HP NFV Director

HP NFV Director

Version 2.0

Installation and Configuration Guide

Edition: 1.0

For the Linux (RHEL6.4) Operating System

December 2014

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.

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, 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 2.0	RHEL Release 6.4

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 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.
${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.

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 two parts:

1. NFVD-Fulfillment
2. NFVD-Assurance

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 v1.1
    - HP UCA Automation Console v1.1
    - 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 v11.24

Note

NFV-D Fulfillment and NFV-D Assurance both require HP Service Activator product. NFV Director 2.0 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 NFVD-Fulfillment and NFVD-Assurance can be either installed; one each for fulfillment, and assurance 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 NFVD Fulfillment components in one system, and NFVD Assurance components in another 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 Assurance components distributed in different systems, such as NFVD Assurance Gateway, UCA Automation, and SiteScope.

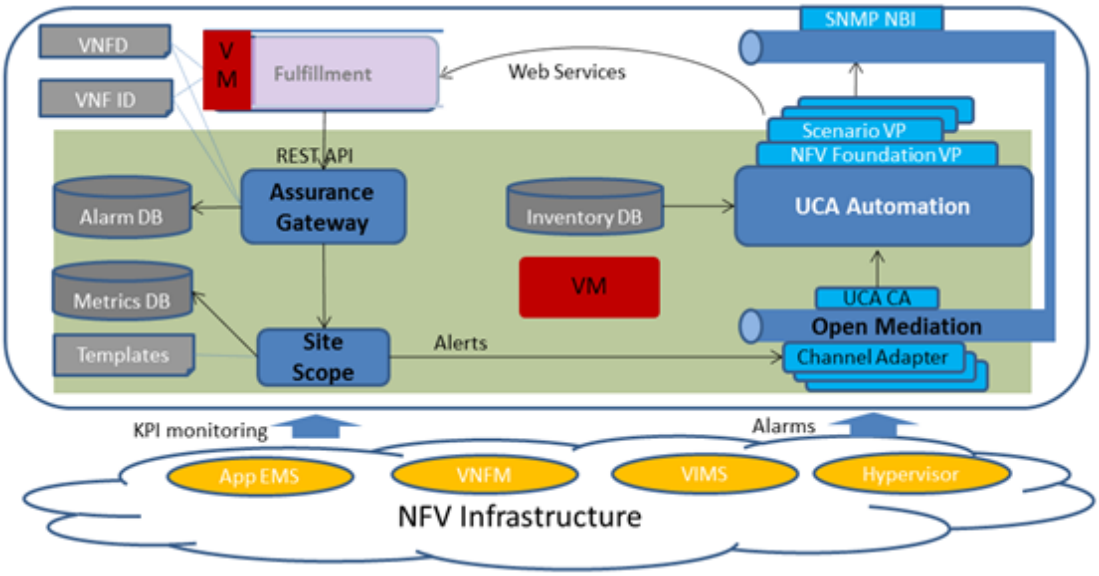

Figure 1 NFVD Deployment Architecture -Single Server

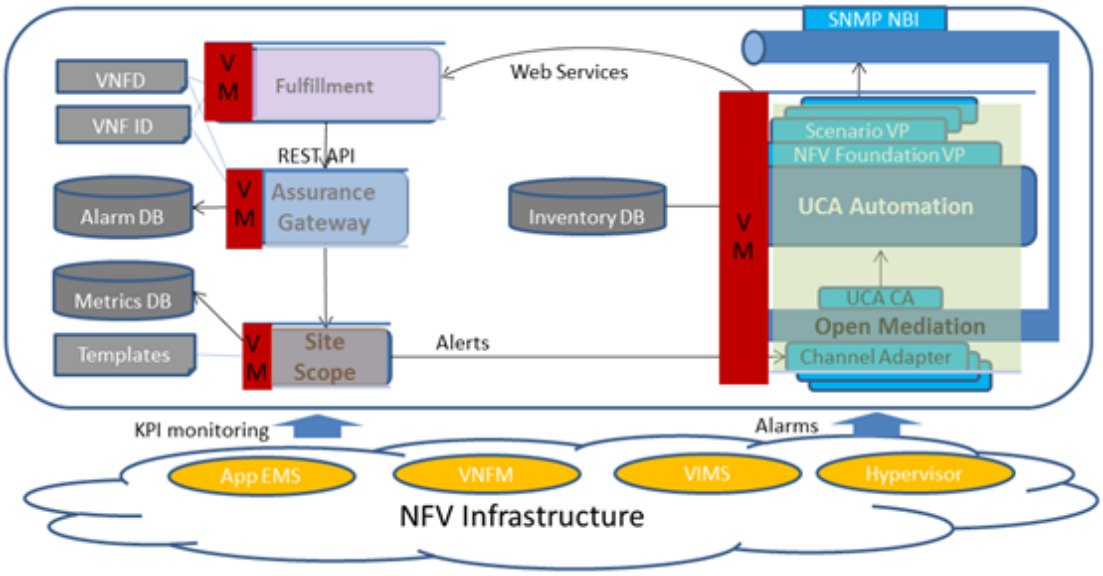

Figure 2 NFVD Deployment Architecture – Distributed

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 Hypervis

VIM TYPE	VERSION	COMPUTE	NETWORKING	STORAGE	MONITORING	IMAGES
						or

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).

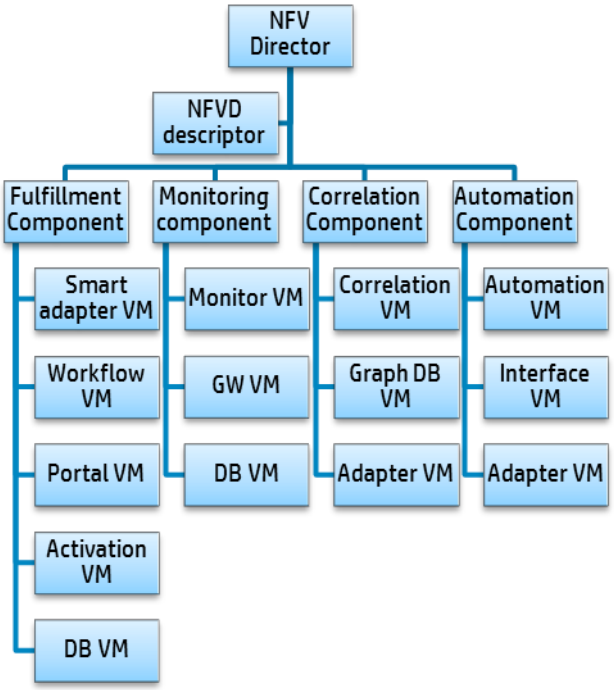

Figure 3 NFV Director sample schema

3.1 NFVD Fulfillment

3.1.1 Hardware requirement

3.1.1.1 For Single server setup

The system must meet the following minimum requirements.

- x86-64 platform
- Red Hat Enterprise Linux 6.4
- The database system requires room for an Oracle or Postgres plus Advanced Server database instance of at least 2 GB, for Service Activator data.

Components	OS	DB	Server	Core	RAM	DISK
HPSA 6.2 EP 6.2 + WSC NFV Director Fulfillment	REDHAT 6.4		VM1 or Blade 1	4 (better 8)	8 (better 16)	140 (better 300)
Fulfillment Database	REDHAT 6.4	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

The specific hardware requirements may vary based on the sizing needed. The system must meet the following recommended requirements:

- x86-64 platform
- Red Hat Enterprise Linux 6.4
- The database system requires room for an Oracle or Postgres Plus Advanced Server database instance of at least 20 GB for Service Activator data.

Components	OS	DB	Server	Core	RAM (GB)	DISK (GB)
Fulfillment FrontEnd	REDHAT 6.4		VM1	8	128	320
Northbound Adapters	REDHAT 6.4		VM2	8	128	320
Fulfillment Automation	REDHAT 6.4		VM3	8	128	320
Southbound Adapters	REDHAT 6.4		VM4	8	128	320

Components	OS	DB	Server	Core	RAM (GB)	DISK (GB)
Fulfillment Database	REDHAT 6.4	Oracle/ PPAS	VM6	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
Java	SE 6 update 37 JDK or later	**NOTE**: Do not use JDK version 7
RHEL	6.4	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

3.2.1.1 For single server setup

If all the components of NFVD Assurance are installed on the same system, then the system must meet the following minimum requirements.

- x86-64 platform
- Red Hat Enterprise Linux 6.4

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

Components	OS	DB	Server	Core	RAM GB	DISK GB
Database		DB Embedded				

Table 7 Assurance single server hardware recommendation

3.2.1.2 For distributed server setup

If the different components of NFVD Assurance are installed on disparate systems, see the following subsections for individual system requirements.

Components	OS	DB	Server	Core	RAM (GB)	DISK (GB)
Assurance Gateway	Red Hat 6.4		VM1	8	128	320
Monitoring (SiteScope)	Red Hat 6.4		VM2	8	128	320
Monitoring Database	Red Hat 6.4		VM3	16	256	2000
Correlation and Automation Engine	Red Hat 6.4		VM4	8	128	320
Correlation Database	Red Hat 6.4	GRAPH DB	VM6	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	V2.0	Uses JBoss 7.1.3
Java JRE/JDK	1.7.0.00 (or later)	
RHEL	6.4	And all available patches

Table 9 NFVD Assurance Gateway Software

Product	Version	Remark
HP UCA for EBC	V3.1	+ Patch UCAEBC31SRVLIN_00005
HP UCA for EBC Topology Extension	V3.1	
UCA Automation Solution	V1.1	
OSS Open Mediation and CA		See Table 11 Open Mediation and Channel

Product	Version	Remark
		Adapters
Java		See Table 8 NFVD Assurance Gateway Software
RHEL		See Table 9 NFVD Assurance Gateway Software

Table 10 UCA Automation software

Product	Version	Remark
OSS Open Mediation	V700	
UCA EBC Channel Adapter	V3.1	
UCA HPSA Channel Adapter	V2.0	
UCA Autoconsole Channel Adapter	V2.0	
Generic SNMP CA	V2.0	
SiteScope Customization for Generic SNMP CA	V2.0	
VMware ESXi Customization for Generic SNMP CA	V2.0	
RHEL		See Table 9 NFVD Assurance Gateway Software.

Table 11 Open Mediation and Channel Adapters

Product	Version	Remark
SiteScope	11.20	+ Patch HPSiS1124_11.24

Table 12 SiteScope Software

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.

Note

For detailed instructions and other installation options, refer to respective product documentation.

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 13 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

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

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

3. 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.

```
# 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;
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 hpsa62.

```
# psql -p 5444 -U enterprisedb -d hpsa -c "create database hpsa62"
# psql -p 5444 -U enterprisedb -d hpsa62 -c "create user NFV WITH PASSWORD 'NFV'"

# psql -p 5444 -U enterprisedb -d hpsa62 -c "GRANT ALL PRIVILEGES ON DATABASE hpsa62 to NFV"

# psql -p 5444 -U enterprisedb -d hpsa -c "ALTER DATABASE hpsa62 OWNER TO NFV"
```

2. Edit the file `pg_hba.conf` to ensure that the database can be accessed remotely.

3. Edit the file `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

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.

4.1.4 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. Export DISPLAY to set the XWindows connection.
2. Go to `/opt/OV/ServiceActivator/bin/` and launch deploymentmanager tool.
3. Set the DB user and password in `System Database Connection` under `Preferences`.
4. Click `OK` to verify.

Note

To launch the deployment manager UI tool, go to the directory `/opt/OV/ServiceActivator/bin`, and then launch the UI. Some issues are observed while deploying solution packs, specifically, when the UI is launched using the absolute path.

```
# cd /opt/OV/ServiceActivator/bin
# ./deploymentmanager
```

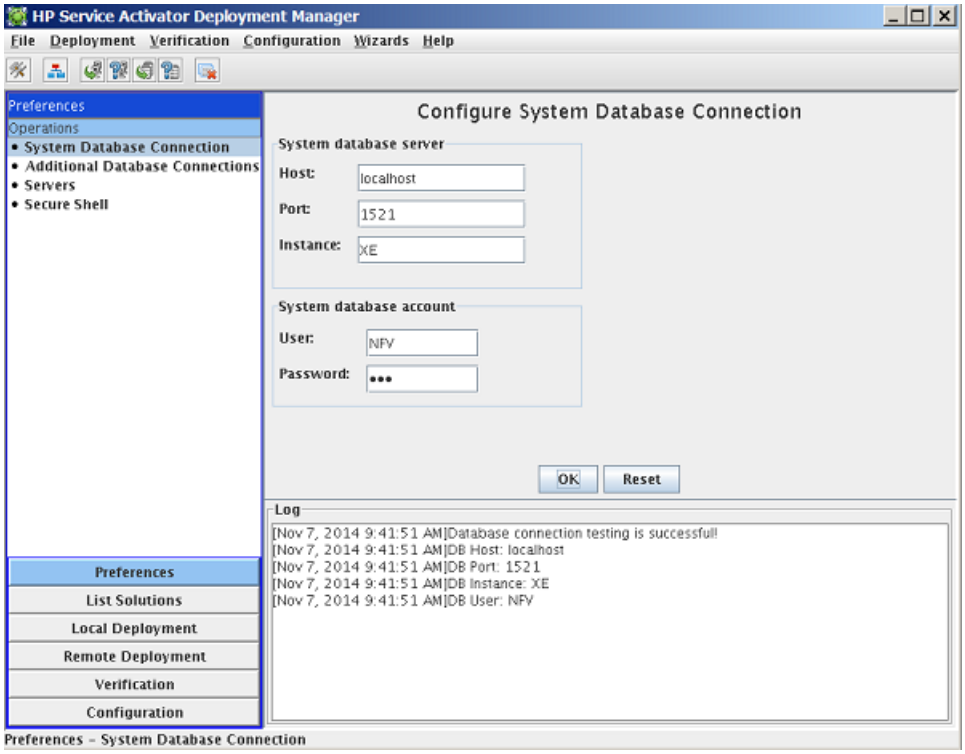

Figure 4 Configure system database connection

5. Select Import Solution option under `Local Deployment` in the UI. Choose `From zip/tar` file and click `Browse…`.

   Select the file `/opt/OV/ServiceActivator/SolutionPacks/CRModel.zip`. Click `Import`.

   When prompted to enter the name of the solution, keep the default name (CRModel) and click `OK` in the `Missing Solution Name` pop-up UI.

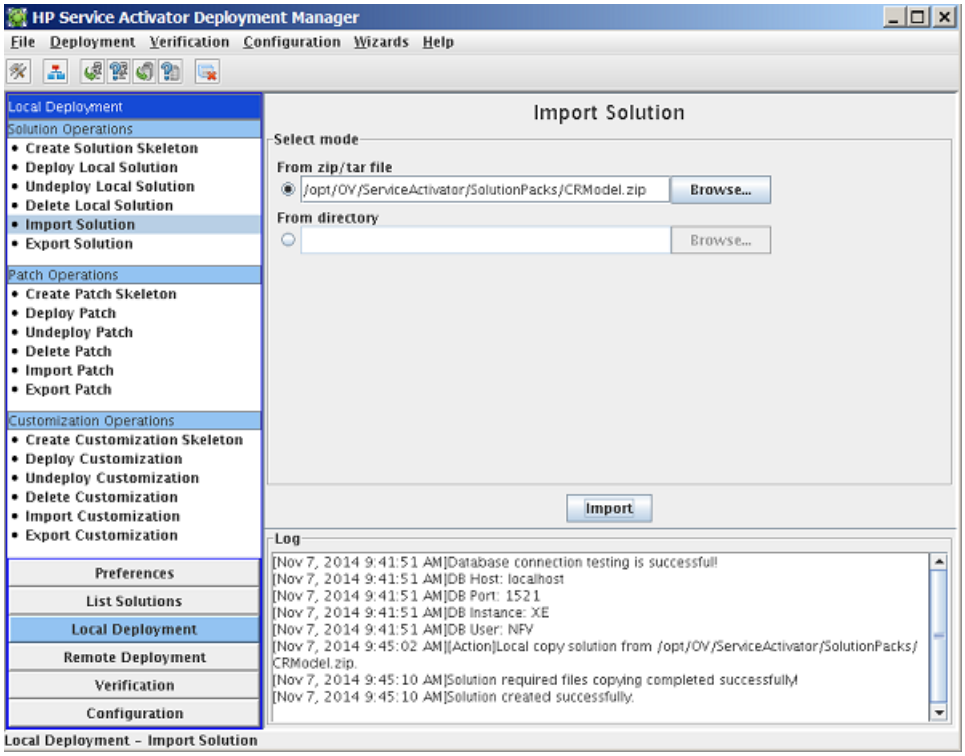

Figure 5 Import HPSA CRModel Solution Pack

6. Select Deploy Local Solution option under Local Deployment in the UI.
7. Select the `Solution Name` CRModel from the drop down list, select an appropriate deployment file, select the `Create inventory tables` checkbox, and then click `Deploy solution`.

   Deployment file is available in `/opt/OV/ServiceActivator/solutions/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 14 Deployment file for CRModel

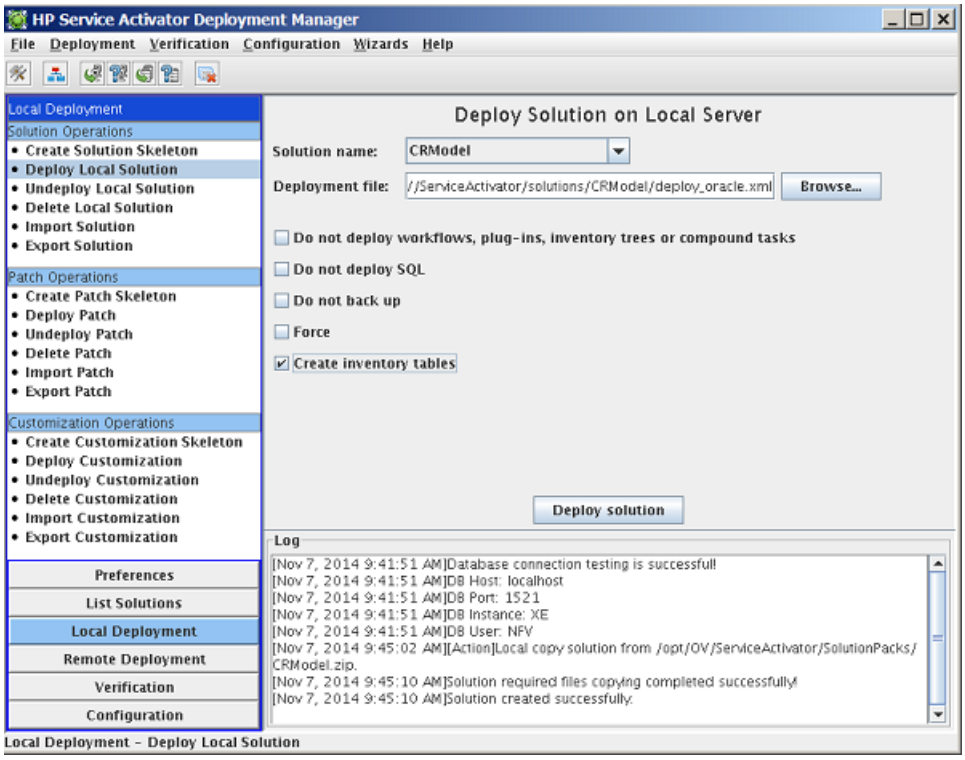

Figure 6 Deploy HPSA CRModel Solution Pack

8. Close the deploymentmanager tool.

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*.

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
```

2. As root, mount the Service Activator Extension Pack installation compact disk.

```
# mkdir -p /tmp/hpsaep
# mount -o loop EP61-JK298-15001.iso /tmp/hpsaep
```

3. Copy the HPSAEP61.zip from /tmp/hpsaep/Binary directory and extract.

```
# mkdir /tmp/ep
# cp /tmp/hpsaep/Binary/HPSAEP61.zip /tmp/ep
# cd /tmp/ep
# jar xvf HPSAEP61.zip
```

4. Go to `bin` directory and execute the install script.
   - Type `Yes` when you receive a prompt asking for a confirmation to install.
   - Type the database 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    : xx.xx.xx.xx
  Port    : 1521
  Instance: XE
Please enter DB user name: ABC
Please enter DB password : DEF
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.
```

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. Unzip the patch `zip` file to any location.

```
# jar xvf V6.1-2.zip
```

3. Execute the `patchmanager` script to install the patch.
   - Type `Yes` when asked for confirmation.
   - Type `Yes` when prompted to migrate the database.
   - 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    : xx.xx.xx.xx
  Port    : 1521
  Instance: XE
Please enter DB user name: ABC
Please enter DB password : DEF
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.
```

4.3 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*.

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. Copy the `OM` tar file to `/tmp` directory and extract it.

```
# cp –p openmediation-7.0.0-L.tar /tmp
# cd /tmp
# tar xvf openmediation-7.0.0-L.tar
```

2. 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 15 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

```
# cd /tmp
# tar xvf <kit location>/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`.
4. Set the UCA for EBC environment variables.

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

4.4.3 Installing UCA for EBC Server 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_00005.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 16 UCA for EBC Topology Extension default ports

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

```
#  cd /tmp
# tar xvf <kit location>/uca-ebc-topo-kit-3.1-linux.tar
```

- 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%]
```

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 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.

4.5.2 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-community-1.9.8-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`

   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	URL
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 17 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 7 List of installed channel adapters

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.

```
# cd /tmp
# tar -xvf <kit location>/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
```

2. Replace localhost by IP Address or full DNS name of the system running UCA for EBC Server.
3. Ensure that this value must match the value set for uca.ebc.serverhost in `/var/opt/UCA-EBC/instances/default/conf/uca-ebc.properties`.

4. 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.tar.gz in /tmp.

```
# tar xvf generic-snmp-ca-V200L01.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 V1.1 Installation Guide* .

Component	Default Port	URL
UCA Automation UI	8888	

Table 18 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 (Add your properties after the line #).

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

2. Edit `/var/opt/UCA-EBC/instances/default/conf/uca-ebc.properties` and add the following line at the end (after the above line).

```
<Profile name="ucaatm" displayedName="Decision Tree View" defaultProfile="true">
<DefaultNode>
<Icon>
<MainIcon>images/round.jpg</MainIcon>
<Decorations attributeName="status">
<Decoration attributeValue="Warning">images/warningLarge.png
</Decoration>
<Decoration attributeValue="Failed">images/critical.png
</Decoration>
</Decorations>
</Icon>
```

```
<Text>
<Color>0 0 0</Color>
<Font>SansSerif</Font>
<Size>10</Size>
<Emphasis>plain</Emphasis>
<DisplayedName>[${name}]</DisplayedName>
</Text>
<GetNeighbors automatic="true" level="20">
<Queries>
<Query>
<![CDATA[START startNode = node({nodeID}) MATCH (startNode)<-[relationship]->(endNode) RETURN
startNode, relationship, endNode;]]>
</Query>
</Queries>
</GetNeighbors>
</DefaultNode>
<DefaultRelationship>
<LineType>line</LineType>
<SourceHead>none</SourceHead>
<TargetHead>halffilledarrow</TargetHead>
<DisplayedName>${Type}</DisplayedName>
</DefaultRelationship>
</Profile>
```

4.7.2 Installing UCA Automation Solution

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

```
# mkdir -p /tmp/ucaa
# mount -o loop JK467-15002.iso /tmp/ucaa
```

2. Copy the `UCA_Automation-V1.1-REV_A.noarch.rpm` file to `/tmp` and install the package.

```
# cp UCA_Automation-V1.1-REV_A.noarch.rpm /tmp
# rpm -ivh UCA_Automation-V1.1-REV_A.noarch.rpm
```

```
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!
```

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

4.7.3 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.

```
# 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. Configure UCA HPSA CA.
5. Modify the /var/opt/openmediation-70/ips/uca-hpsa-ca-20/etc/config.properties file.
    - hpsa.host
    - hpsa.port
    - hpsa.userid
    - hpsa.password
6. 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
```

4.7.4 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.

```
# 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. Configure UCA Autoconsole CA.

   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
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
```

4.7.5 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.

4.7.5.1 Deploy HPSA Foundation Solution Pack

1. Copy the /opt/UCA_Automation/UCA_Automation_HPSA_VPs /UCA_HPSA_FoundationVP-V11-1A.zip file to the /opt/OV/ServiceActivator/SolutionPacks directory.
2. Import the Solution Pack UCA_HPSA_FoundationVP-V11-1A.zip.

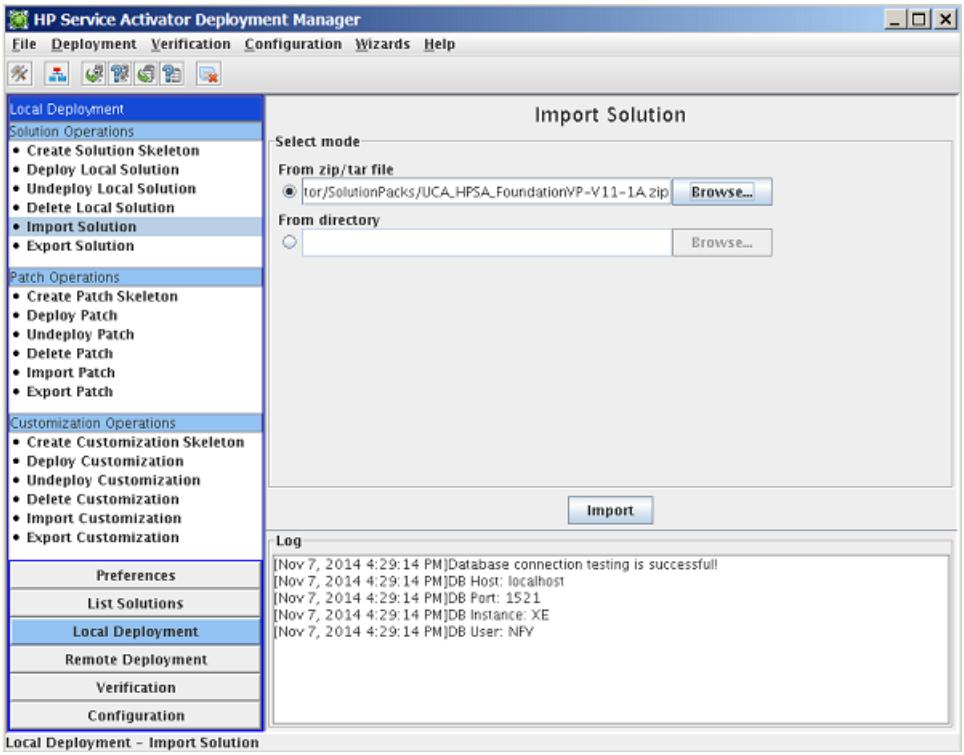

Figure 8 Import UCA Automation foundation solution pack

3. Deploy the Solution Pack UCA. Ensure to check the `Create Inventory Table` check box.

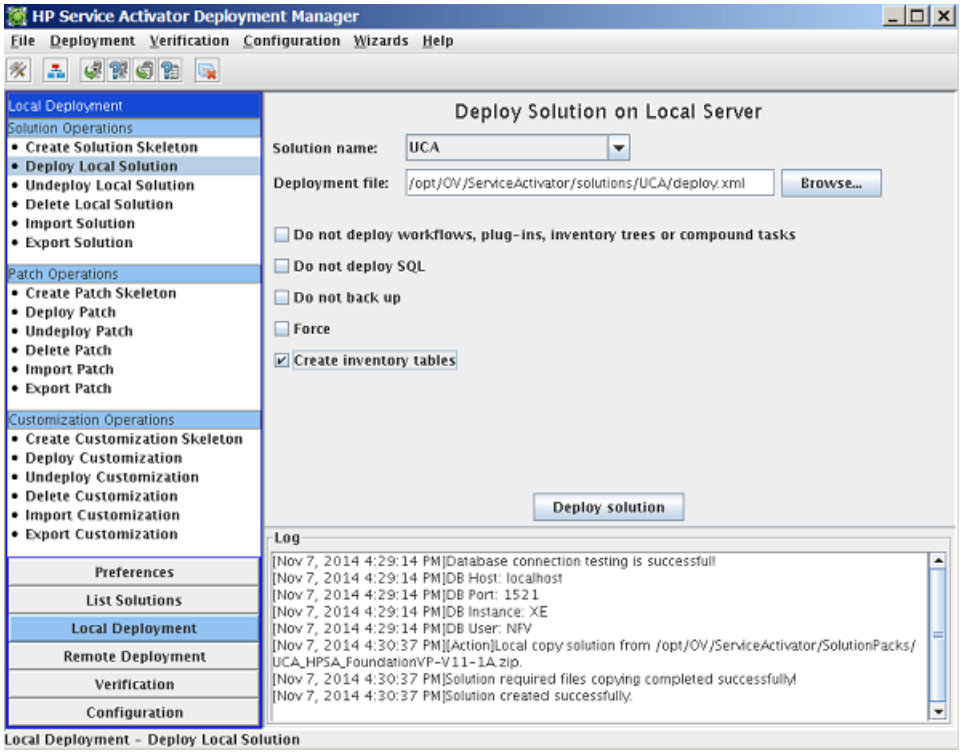

Figure 9 Deploy UCA Automation foundation solution pack

4.7.5.2 Configure HPSA Foundation Solution Pack

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>
```

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

UCA Automation UCA for EBC Foundation Value Pack is available in `/opt/UCA_Automation/UCA_Automation_UCA_VPs` directory.

4.7.6.1 Deploy UCA for EBC Foundation VP

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

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

```
# cp /opt/UCA_Automation/UCA_Automation_UCA_VPs/UCA_Automation_Foundation_UCA-vp-V1.1-1A.zip /var/opt/UCA-EBC/instances/default/valuepacks
# su - uca
$ cd /opt/UCA-EBC/bin
$ ./uca-ebc-admin --deploy -vpn UCA_Automation_Foundation_UCA -vpv V1.1-1A
```

```
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, V1.1-1A, 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-V1.1-1A 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="UCA_Automation_DomainExample_UCA_EV.evaluate" additivity="false">
<level value="TRACE" />
<appender-ref ref="CONSOLE" />
<appender-ref ref="FILE" />
</logger>
```

4.7.6.2 Configure UCA for EBC Foundation VP

1. Edit the /var/opt/UCA-EBC/instances/default/deploy/UCA_Automation_Foundation_UCA-V1.1-1A/conf/UCAAutomation.properties file.
2. Update the localhost 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.
   - For Oracle database, update the following configuration.

```
DB_DRIVER=oracle.jdbc.driver.OracleDriver
DB_URL=jdbc:oracle:thin:@<db-host>:<db-port>:<db>
DB_USER=<db-user>
DB_PASSWORD=<db-user-password>
```

   - For Enterprise database Postgres, update the following configuration.

```
DB_DRIVER=org.postgresql.Driver
DB_URL=jdbc:postgresql://<db-host>:<db-port>/<db>
DB_USER=<db-user>
DB_PASSWORD=<db-user-password>
```

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

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

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

5. Delete the mediation flow in the UCA Automation's UCA for EBC Foundation VP.
6. Start UCA for EBC as `uca` user.

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

7. In the UCA-EBC portal `http://<#UCA EBC Server host>:<#UCA GUI Port>/uca`, log in as admin or admin operator to view the list of VPs.
8. On the left panel, select the UCA_Automation_Foundation_UCA-V1.1-1A → Value Pack and select the Configuration tab.

   It lists the Standard Configuration as follows:

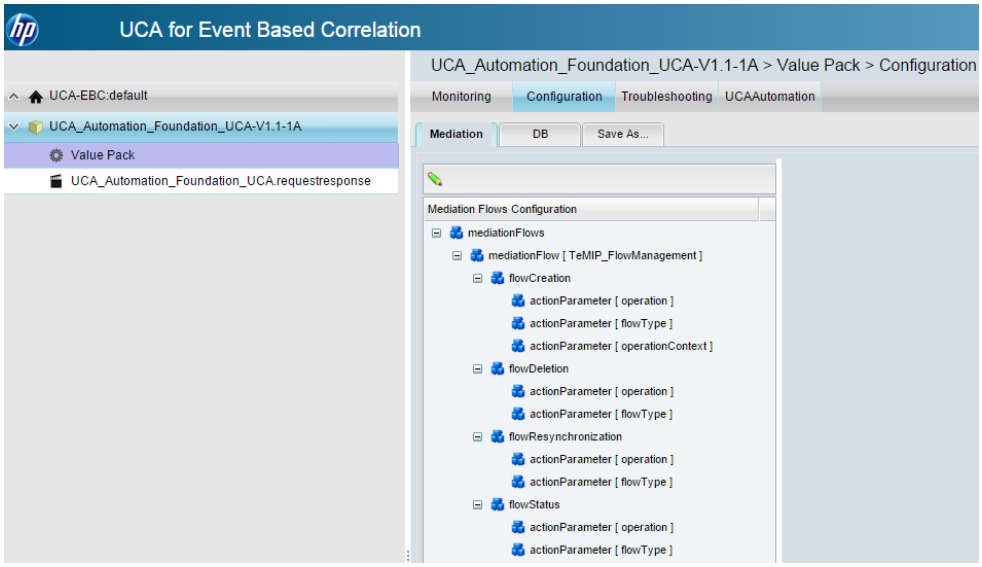

Figure 10 UCA EBC – Open TeMIP mediationFlow tree

9. Select the tree mediation Flows → mediationFlow [TeMIP_FlowManagement].
10. Select the `Edit Configuration` option and click `Remove Entry` to delete this mediationFlow.

Figure 11 Delete TeMIP mediationFlow tree

11. Select Save Modifications to File and Apply them to Value Pack button.

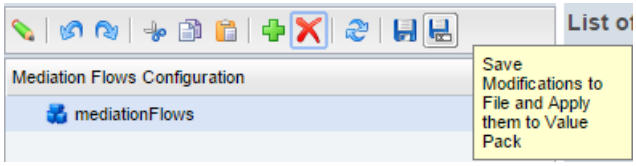

Figure 12 Save and apply changes to VP

4.7.7 HP UCA Automation configuration for NFVD

After installing the HP UCA Automation solution, configure the solution as follows to adapt to the NFVD solution:

1. In the UCA-EBC portal `http://<#UCA EBC Server host>:<#UCA GUI Port>/uca`, login as admin or admin operator.
2. Select UCA_Automation_Foundation_UCA-V1.1-1A.requestresponse→ Configuration → Filter Configuration option.
3. Select the filters → topFilter [Foundation] → allCondition.

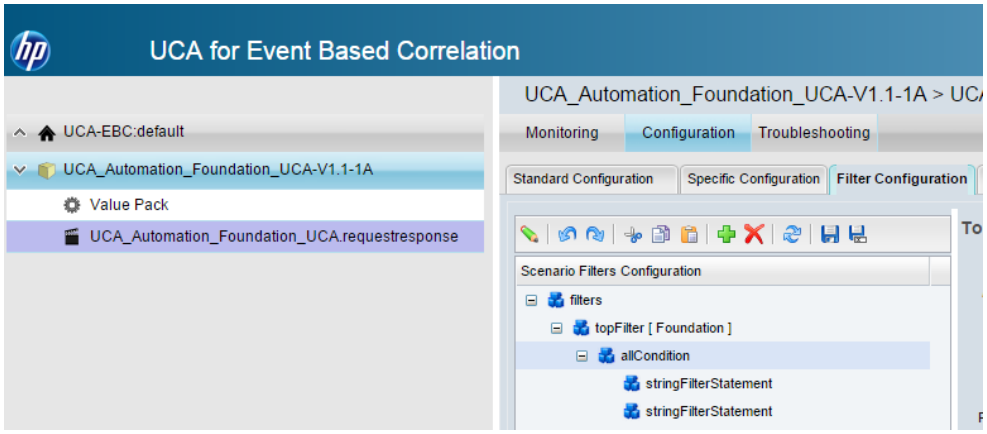

Figure 13 UCA EBC UCA Automation Foundation VP filter

4. Click the `Edit` option, and select `Add new entry` button.

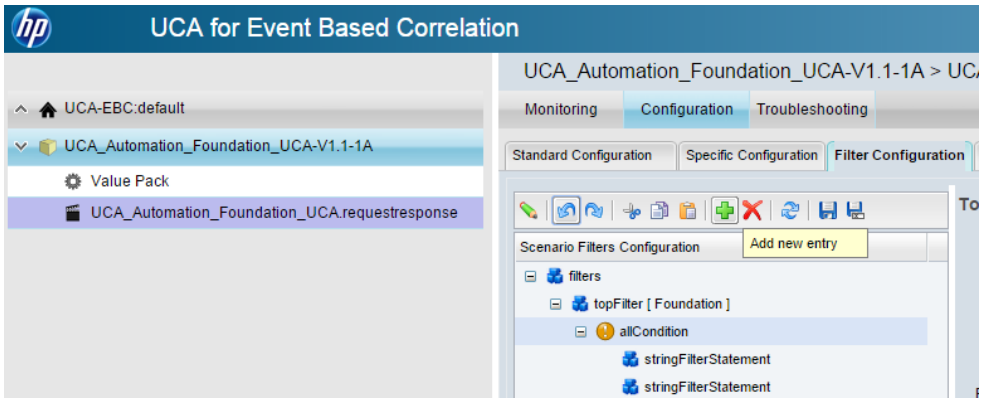

Figure 14 UCA EBC add new filter

5. Select `notCondition` from the drop box, set the check box for `with optional elements`, and click the `Create Entry` button.

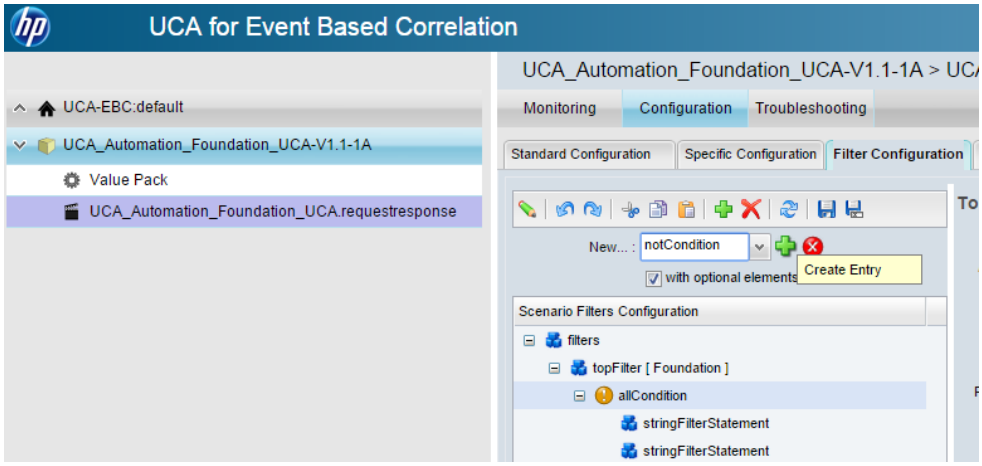

Figure 15 UCA EBC filter create condition

6. Clicking the `Create Entry` button generates five statements under the `notCondition`. They are dateFilterStatement, stringFilterStatement, intFilterStatement, doubleFilterStatement, and instanceOfFilterStatement.

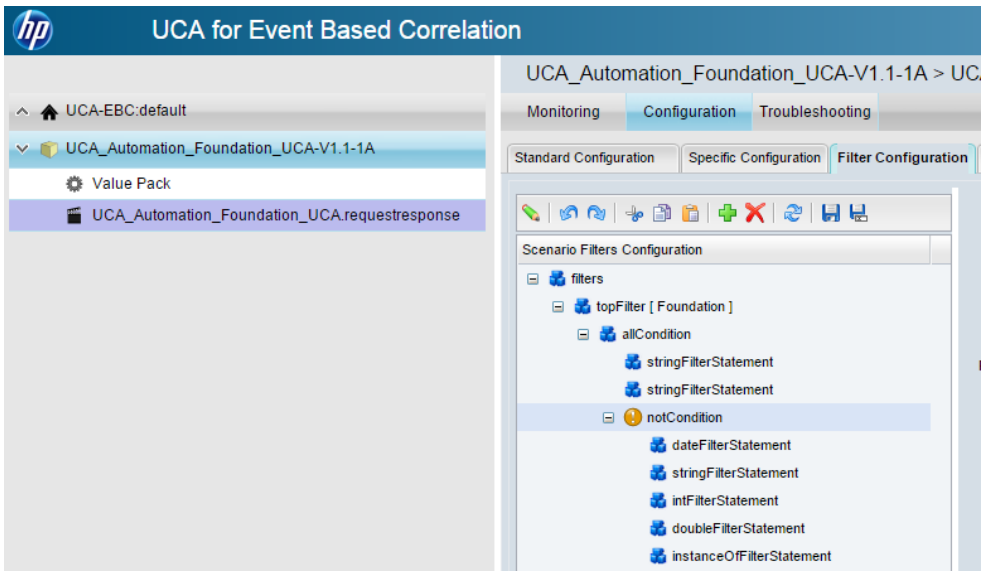

Figure 16 UCA EBC create entry under notCondition

7. Remove all the statements except `stringFilterStatement`.

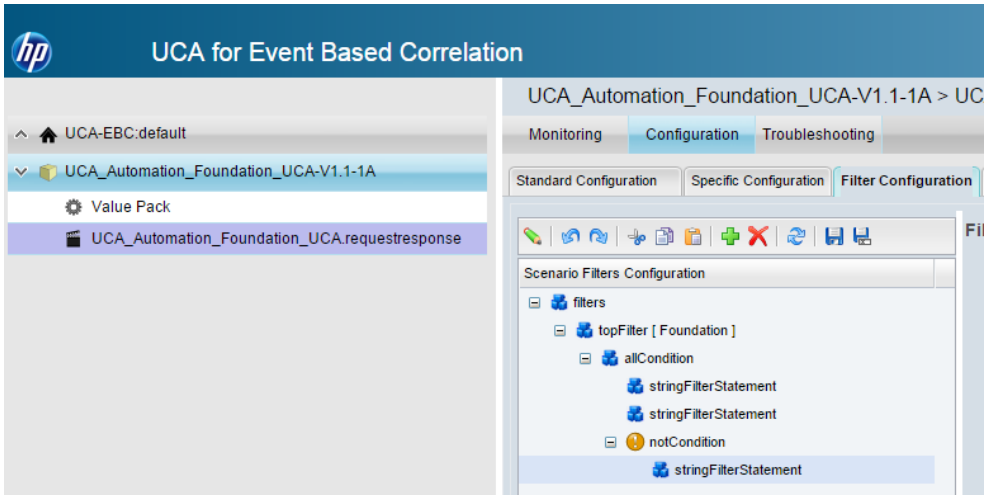

Figure 17 UCA EBC removes unnecessary conditions

8. For the stringFilterStatement, select the fieldname as `additionalText`, operator as `contains` and key in fieldValue as `Publish-VP`. Click `Save Modifications to File` and Apply them to Value Pack.

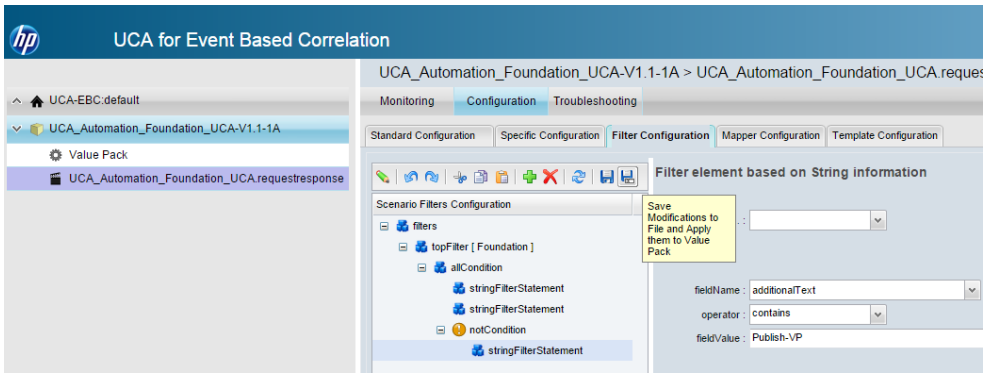

Figure 18 UCA EBC additionalText filter

9. Start the UCA Automation Foundation Value Pack.

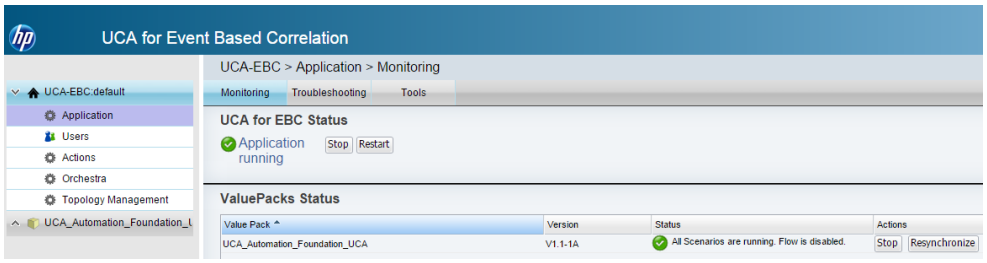

Figure 19 UCA EBC start Value Pack

4.7.7.1 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 19 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_11.20_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 Linux_Setup
# ./HPSiteScope_11.20_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.

   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.
5. Type `Y` when prompted to accept the terms of License Agreement, and press `Enter`.
6. Enter `1` to select `1 - HP SiteScope: ()` as the setup type, and press `Enter`.
7. Enter the number `1` to choose `1 - HP SiteScope(Required)` option, and press `Enter`, in the `Select Features` screen.
8. Press Enter in the Install Requirements screen.

9. Press `Enter` to continue installation in the `Pre-Installation Summary` screen.
10. Type `1` to select the default port 8080 when the port prompt is displayed.
11. Type `2` to change the port and then type a different number in the `change port` prompt.

Note

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

12. Type `1` to leave the license file path empty, when prompted for license file path. License can be applied after completing the installation.
13. Type `1` to select `1 – Do not import: ()` and press `Enter` when prompted to Import Configuration.
14. Type `1` to select `1 – Do not install: ()`, and press `Enter` when prompted to install the HP Operations Agent.

    The console displays the installation parameters for confirmation.
15. Type `1` to proceed with the installation.

    The Installation status message is displayed.

4.8.1 Installing SiteScope patch

Note

Use the following command to launch the installer when you face issues while installing SiteScope on RHEL 6.4:

```
HPSiS1124_11.24_setup.bin LAX_VM <Path to 64 bit
JVM>/bin/java -i console.
```

As root user, run the installer.

```
# ./HPSiS1124_11.24_setup.bin -i console
```

Rest of the installation process is almost similar to the base product installation process.

Note

The port set in the SiteScope 11.20 gets reset to `8080` when we install the patch. Run `/opt/HP/SiteScope/bin/config_tool.sh -i console Change Ports` option to set the desired SiteScope user interface port. Do not change the other ports – choose the default values.

4.9 Starting and stopping base products

Note

Make sure to start OM with Java 7. OM might not work as expected if started with Java 6.

Product	Start	Stop	Remark
SiteScope	/opt/HP/SiteScope/start	/opt/HP/SiteScope/stop	Path: /opt/HP/Sitescope
UCA EBC	/opt/UCA-	/opt/UCA-	Run the start/stop

Product	Start	Stop	Remark
Server	EBC/bin/uca-ebc start	EBC/bin/uca-ebc stop	commands as 'uca' user. Path: /opt/UCA-EBC
HPSA	/etc/init.d/activator start	/etc/init.d/activator stop	status and restart are other options. Path: /opt/OV/ServiceActivator, /etc/opt/OV/ServiceActivator, /var/opt/OV/ServiceActivator /opt/HP/jboss
Oracle	/etc/init.d/oracle start	/etc/init.d/oracle stop	status and restart are other options.
PPAS	/etc/init.d/ppas-9.2 start	/etc/init.d/ppas-9.2 stop	status and restart are other options.
OM	/opt/openmediation-70/bin/nom_admin --start-container –all	/opt/openmediation-70/bin/nom_admin --shutdown-container –all	
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	Path: /opt/HP/nfvd/tpp

Table 20 NFVD Assurance start/stop scripts

Chapter 5

Installing and configuring the NFVD product

Extract the files contained in the JK765-15001 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%/Binaries
%INSTALLATION_DIR%/Documentation

Table 21 ISO image directories

5.1 Installing the NFVD Fulfillment solution

5.1.1 Generate xmaps database model

Run the following SQL script in your HPSA database installation instance:

```
/var/opt/OV/ServiceActivator/xmaps/xmaps.sql
```

5.1.2 Importing and deploying fulfillment solutions and patches

NFVD Fulfillment solution is available as nfvd-fulfillment-02.00.000-1.el6.noarch.rpm.

The following sections explain the installation and configuration process.

1. Mount the ISO image `JK765-15001.iso`.
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-02.00.000-1.el6.noarch.rpm
   ```

   The following HPSA Solution packs are extracted into `/opt/HP/nfvd/fulfillment` directory.

   - IPAM.zip
   - AD.zip
   - MSA-1.2.2.zip
   - MSA1.2.3.zip Patch

- NFVModel.zip
- NFVAuto.zip
- NFVDLF.zip
- RESTPA.zip
- OSPLUGIN.zip
- NFVMPLUGIN.zip
- VNFMANPA.zip

Follow the instructions in the subsequent sections to setup the NFVD Fulfillment solution.

5.1.2.1 Importing solution packs

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

Solution Pack Zip	Solution/Patch	File Location
IPAM.zip	Solution	/opt/HP/nfvd/fulfillment
AD.zip	Solution	/opt/HP/nfvd/fulfillment
MSA-1.2.2.zip	Solution	/opt/HP/nfvd/fulfillment
MSA1.2.3.zip (Patch)	Patch	/opt/HP/nfvd/fulfillment
NFVModel.zip	Solution	/opt/HP/nfvd/fulfillment
NFVAuto.zip	Solution	/opt/HP/nfvd/fulfillment
NFVDLF.zip	Solution	/opt/HP/nfvd/fulfillment
RESTPA.zip	Solution	/opt/HP/nfvd/fulfillment
OSPLUGIN.zip	Solution	/opt/HP/nfvd/fulfillment
NFVMPLUGIN.zip	Solution	/opt/HP/nfvd/fulfillment
VNFMANPA.zip	Solution	/opt/HP/nfvd/fulfillment

Table 12 NFVD Fulfillment solution pack and patch locations

1. Export DISPLAY to set the XWindows connection.
2. Go to `/opt/OV/ServiceActivator/bin/` and launch deploymentmanager tool.
3. Set the DB user and password in `System Database Connection` under `Preferences`.
4. Click `OK` to verify.

Note

To launch the deployment manager UI tool, go to the directory

`/opt/OV/ServiceActivator/bin`, and then launch the UI.
Some issues are observed while deploying solution packs, specifically, when the UI is launched using the absolute path.

```
# cd /opt/OV/ServiceActivator/bin
# ./deploymentmanager
```

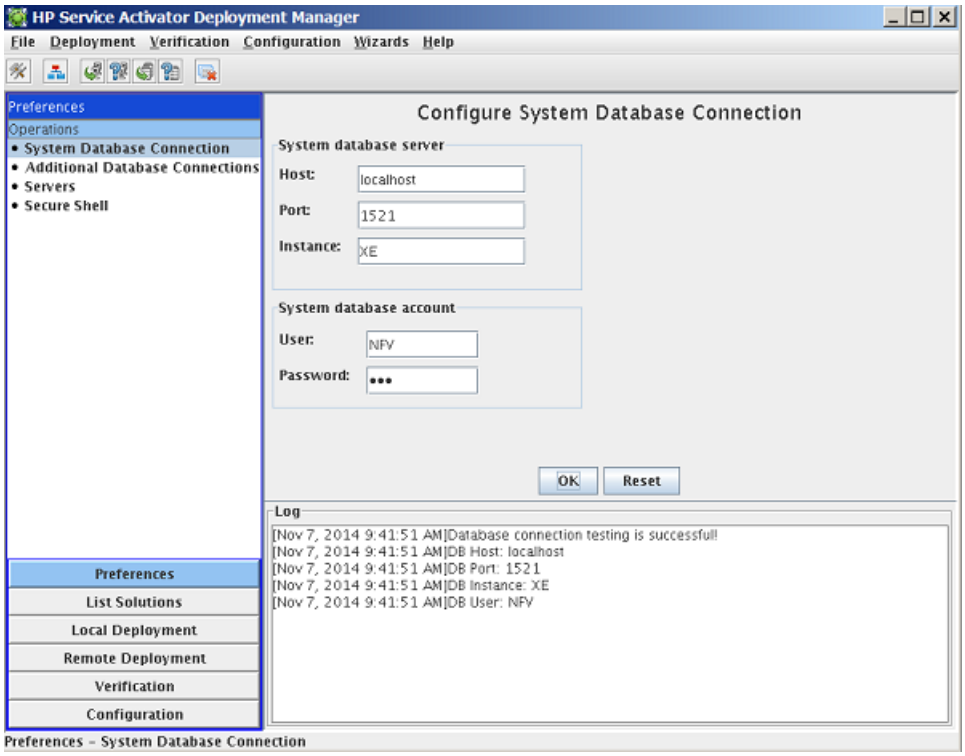

Figure 20 Configure DB connections in deployment manager

5. Select `Import Solution` option under `Local Deployment` in the UI.
6. Select `From zip/tar file` and click the `Browse…` button.

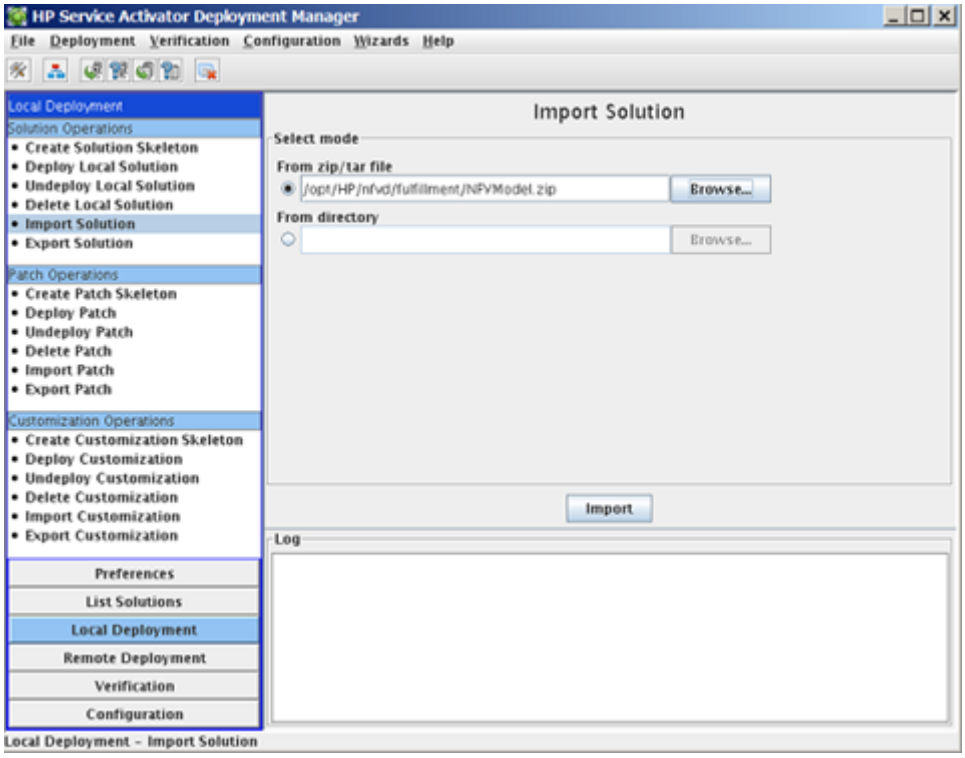

Figure 21 Import solution pack in deployment manager

7. Click the `Import` button for each of the following ZIP files (solution packs) in `/opt/HP/nfvd/fulfillment` directory.
    - IPAM.zip
    - AD.zip
    - MSA-1.2.2.zip (See the following **NOTE** before importing MSA)
    - NFVModel.zip
    - NFVAuto.zip
    - NFVDLF.zip
    - RESTPA.zip
    - OSPLUGIN.zip
    - NFVMPLUGIN.zip
    - VNFMANPA.zip
8. After importing all the solution packs, import the MSA patch (MSA.1.2.3.zip).
9. Select `Import patch` option under `Local Deployment` in the UI.
10. Select the Patch `MSA1.2.3.zip` and then click `Import patch`.

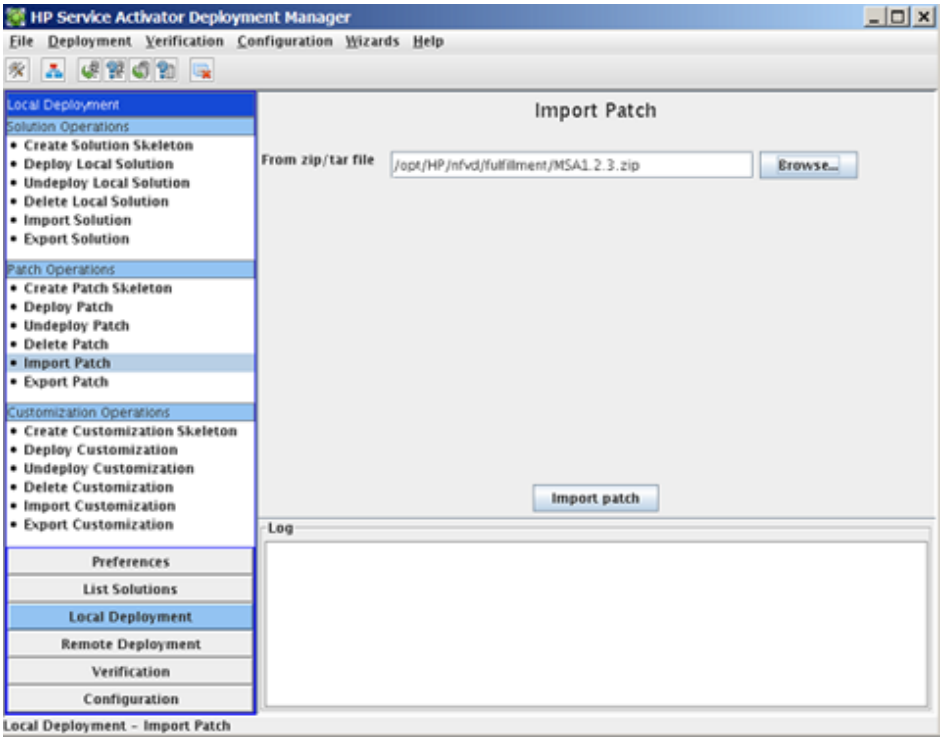

Figure 22 Import patch in deployment manager

5.1.2.2 Deploying the solutions

For each solution pack listed in the following table, read the NOTEs before deploying the solutions.

Note

Check `Create inventory tables` option while deploying solution packs.

Verify if there is execute permission for the `.sh` files in `/opt/OV/ServiceActivator/solutions/<SolutionName>/*directories`. If not add `+x` permissions, before deploying. This issue is observed in the **IPAM** solution pack.

Select the following file for deployment when prompted:

Solution Pack Name	Database System	File
IPAM	Oracle/PPAS	deploy.xml
AD	Oracle/PPAS	deploy.xml
MSA Solution Pack	Oracle/PPAS	deploy.xml
MSA Patch	Oracle/PPAS	deploy.xml
NFVModel	Oracle/PPAS	deploy.xml
NFVAuto	Oracle	deploy_ORACLE.xml
	PPAS	deploy_PPAS.xml
NFVDLF	Oracle/PPAS	deploy.xml
RESTPA	Oracle/PPAS	deploy.xml
OSPLUGIN	Oracle/PPAS	deploy.xml

NFVMPLUG	Oracle/PPAS	deploy.xml
VNFMANPA	Oracle/PPAS	deploy.xml

Table 22 NFVD Solution Pack and Patch Deployment Files

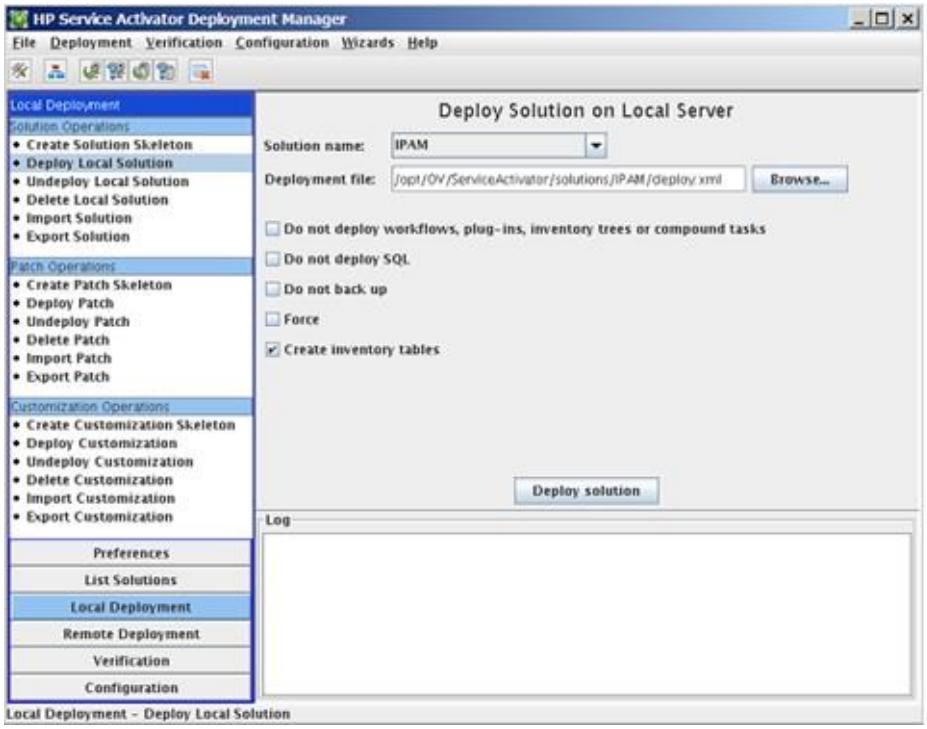

Figure 23 Deploy solution in deployment manager

5.1.2.3 Deploy MSA patch

Select Deploy Patch option under Local Deployment in the UI. Choose the Solution Name MSA from the drop down list, choose an appropriate deployment file, check the Do not deploy SQL checkbox, and then click deploy patch.

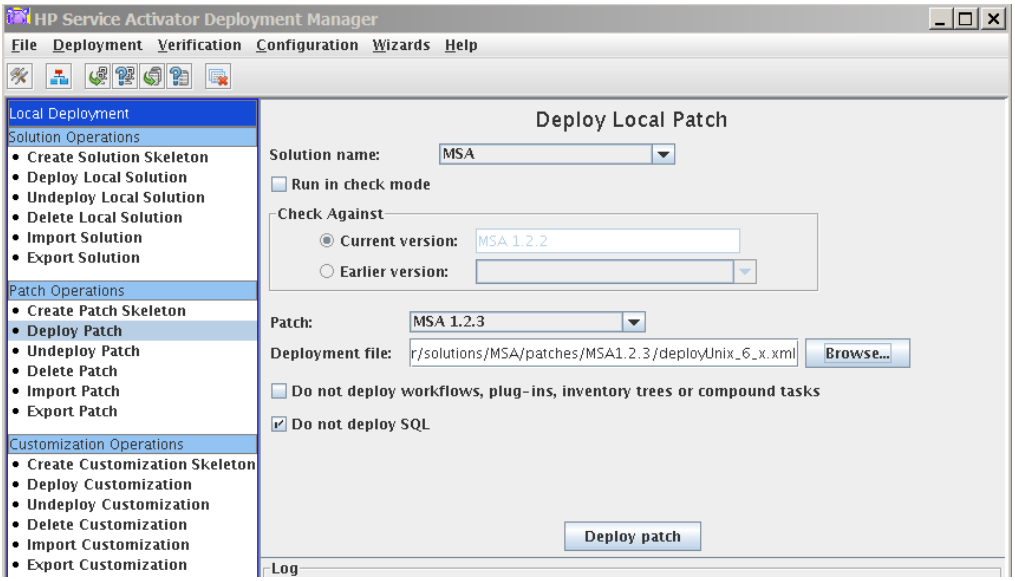

Figure 24 Deploy MSA Patch

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 23 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 24 mwfm.xml path

3. 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>
```

4. 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>
```

5. Create the following folder and file:

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

6. 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
```

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 25 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_serv
ice_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>
```

   - 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://#dbhost:#dbport/#db_service_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>
```

3. 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_service_name	Service name of the instance of HPSA Database

Table 26 sosa.xml NfvManagerModule parameters

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

sosa.xml sosaModule

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

5. Include the following configuration into `sosa_conf.xml` file.

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

Table 27 sosa_conf.xml path

6. 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>
```

7. 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>
```

8. 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" />
```

9. 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>
```

10. Change 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 28 sosa_conf MWFM_SA_EXECUTOR variables

11. 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.

12. 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 29 alias.xml path

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

alias.xml reportmodule

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

13. 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 30 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 31 web.xml orchestrator

14. 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 32 configuration.xml path

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

Create the following directory.

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

5.2.3 NFVD Fulfillment specific configurations

1. Create the following directory:

Operating System	Path
Linux	`/var/opt/OV/ServiceActivator/log/NFVModel/`

Table 33 NFVModel directory

2. Edit the following configuration in `nfv_manager.xml` file

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

Table 34 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/ae-
services- impl/NGWSServiceService/NGWSServiceImpl</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.
#assurance_user	NFVD-Assurance user. Currently not used.
#assurance_userid	NFVD-Assurance user ID. Currently not used.

Table 35 nfv_manager.xml parameters

5.2.4 Deploying NFVD maps

Use Diagram Deployer to deploy the NFV Director maps by executing the following commands on the HPSA server:

```
cd /opt/OV/ServiceActivator/bin/
./DiagramDeployer -deploy -dbHost #db_host -dbName #db_service_name -dbPort #db_port -dbUser #db_user
-dbPassword #db_password
/opt/OV/ServiceActivator/solutions/NFVModel/etc/config/xmaps/ARTIFACT_TEMPLATES.xml
./DiagramDeployer -deploy -dbHost #db_host -dbName #db_service_name -dbPort #db_port -dbUser #db_user
-dbPassword #db_password
/opt/OV/ServiceActivator/solutions/NFVModel/etc/config/xmaps/ARTIFACT_INSTANCES.xml
```

Variable	Description
#db_user	HPA Database Username
#db_password	HPSA Database clear text password.

Variable	Description
#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_service_name	Service name of the instance of HPSA Database.

Table 36 NFVD Map 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.

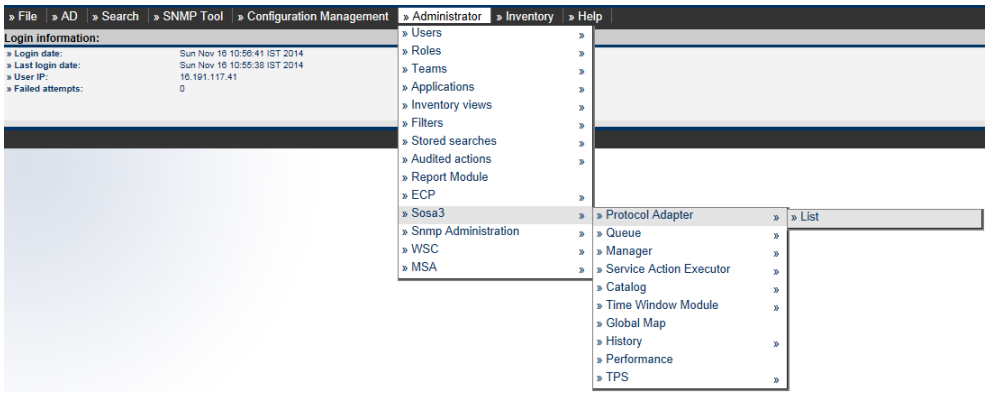

Figure 25 SOSA > Protocol Adapter > List

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

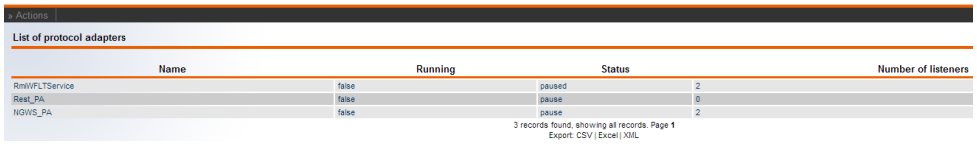

Figure 26 SOSA > Protocol Adapter Status

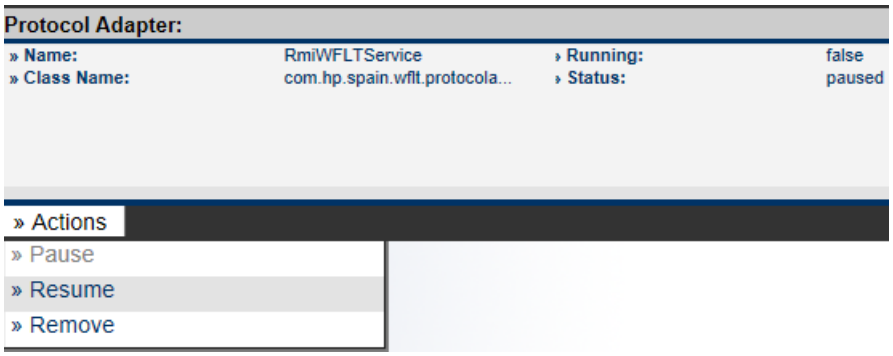

Figure 27 Protocol Adapter Resume Action

5. Select Administrator → Sosa3 → Queue → List.

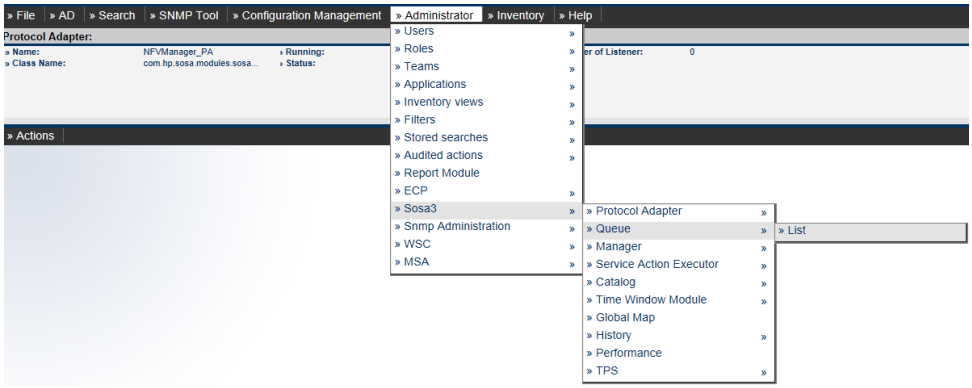

Figure 28 SOSA > Queue > List

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

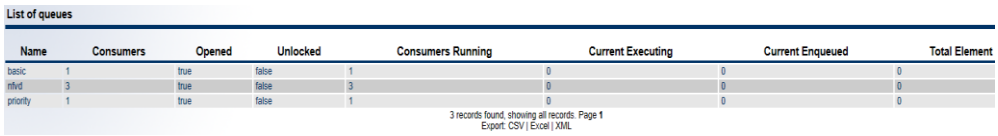

Figure 29 SOSA Queue list

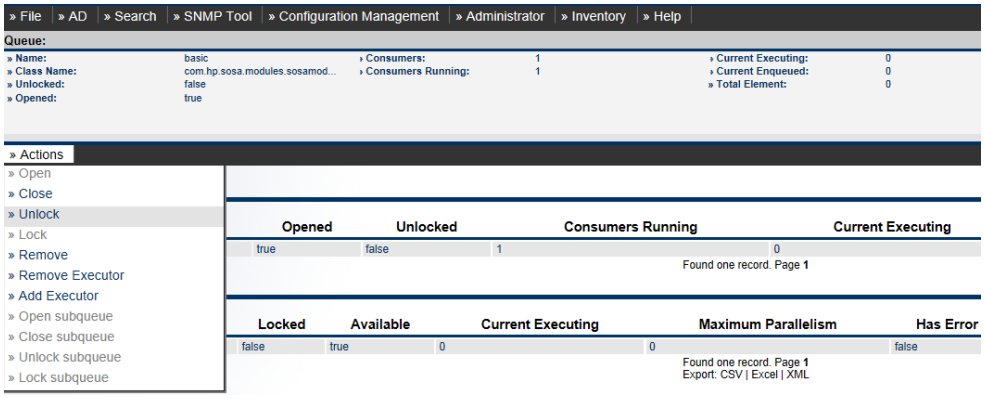

Figure 30 Queue Unlock

5.4.3 Load artifact definitions

The NFVD Fulfillment solution requires the default artifact definitions to be loaded to properly manage VNF and all its components:

1. Open a Web Browser and type HPSA UI (http://<#hpsa system>:<#hpsa port>/activator).
2. Login using your HPSA username/password.

Figure 31 NFVD Fulfillment Login

3. Open the NFVModel/NFVDView Inventory Tree View.

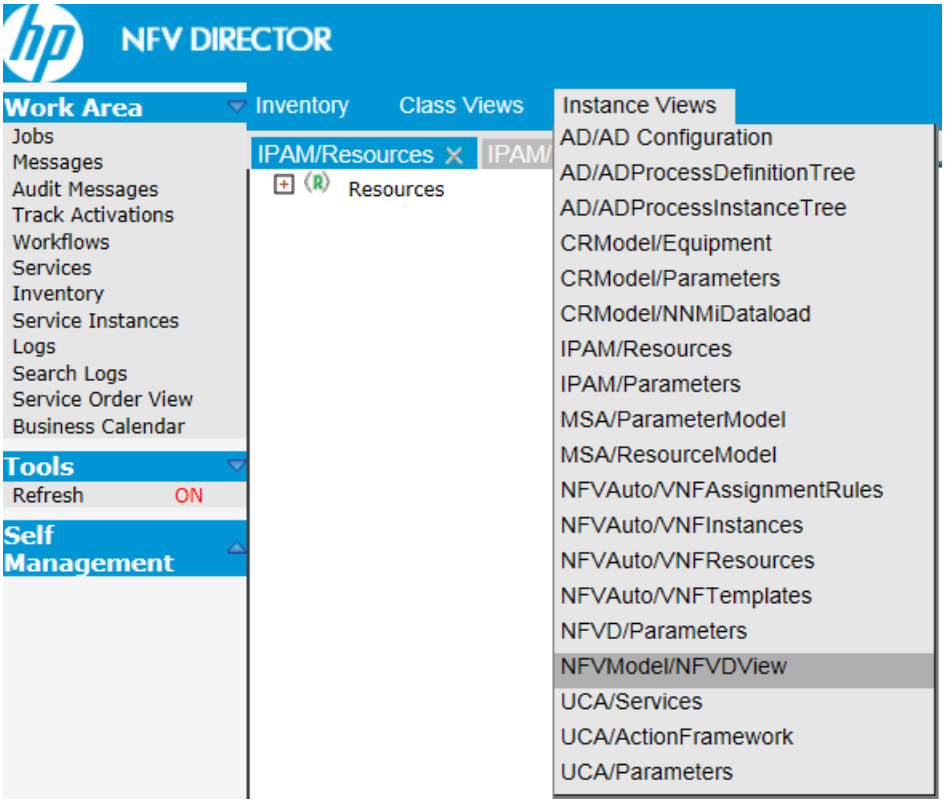

Figure 32 NFVD Fulfillment Inventory List

4. Right click Artifact Definitions branch, and select Multiple Upload Artifact Definition.

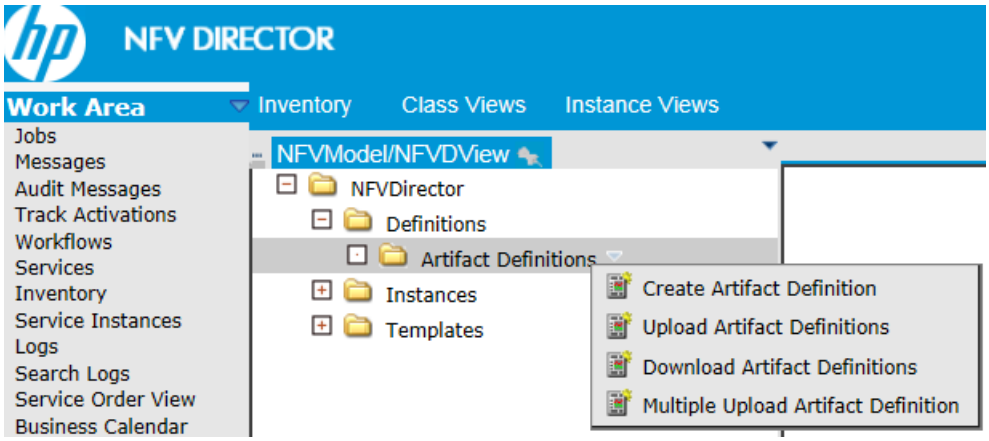

Figure 33 Multiple Upload Artifact Definition

5. Click Browse and select all artifact definitions in the /opt/OV/ServiceActivator/solutions/NFVModel/etc/LoadXML/DEFINITIONS/ARTIFACTS/*xml file.

Note

Use Mozilla Firefox to perform this operation. If you are using the browser in a remote system, you will need to transfer the artifact definitions from `/opt/OV/ServiceActivator/solutions/NFVModel/etc/LoadXML/DEFINITIONS/ARTIFACTS/*xml` location.

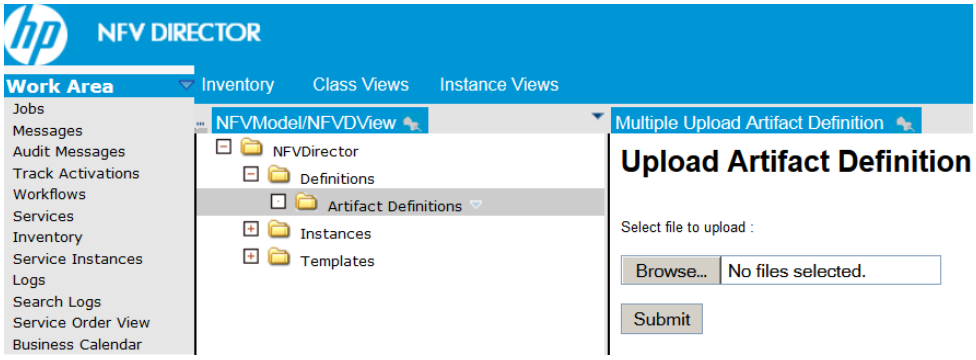

Figure 34 Select Artifact Definitions

6. Click `Submit`.

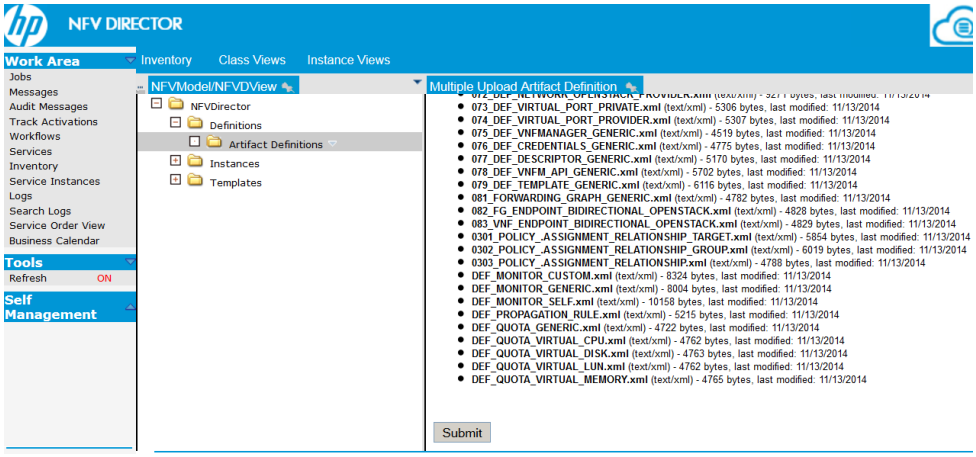

Figure 35 Upload Selected Artifact Definitions

7. Repeat the same process for the following files:

   /opt/OV/ServiceActivator/solutions/NFVModel/etc/LoadXML/DEFINITIONS/RELATIONSHIPS/*.xml

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

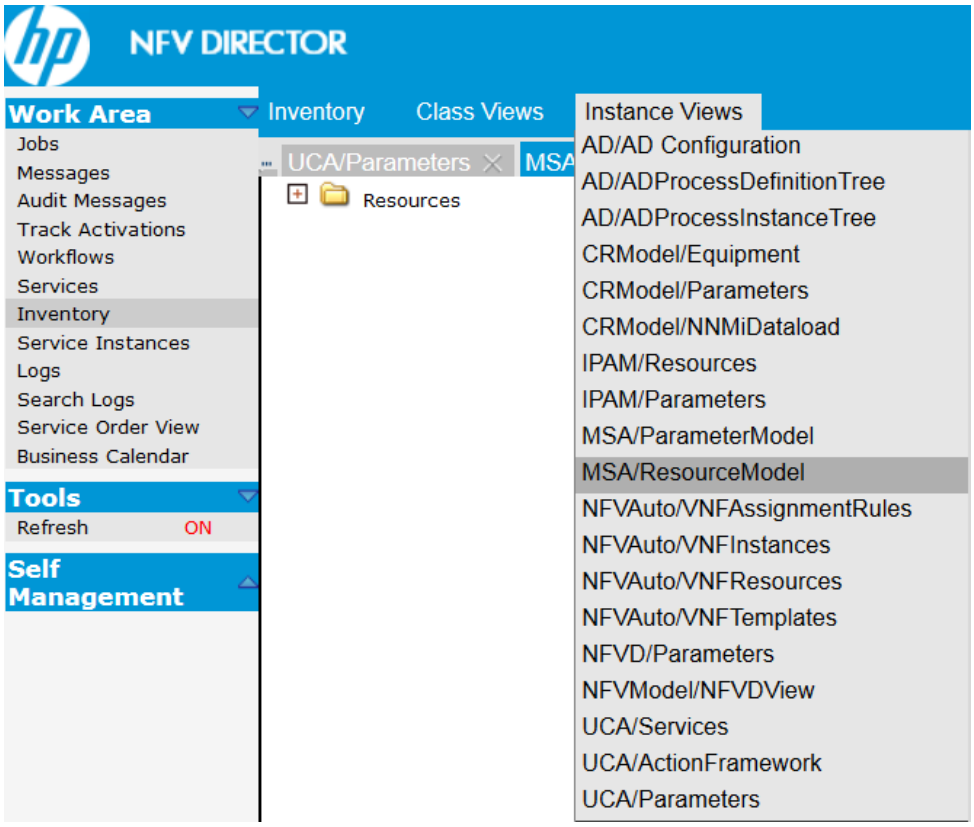

Figure 36 MSA Resource Model Inventory Model

4. Navigate through the tree until you find EndPoint:

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

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

   http://<#assurance_host>:<#port>/ae-services-impl/NGWSServiceService/NGWSServiceImpl

   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`.

6. Set timeout to 600000.

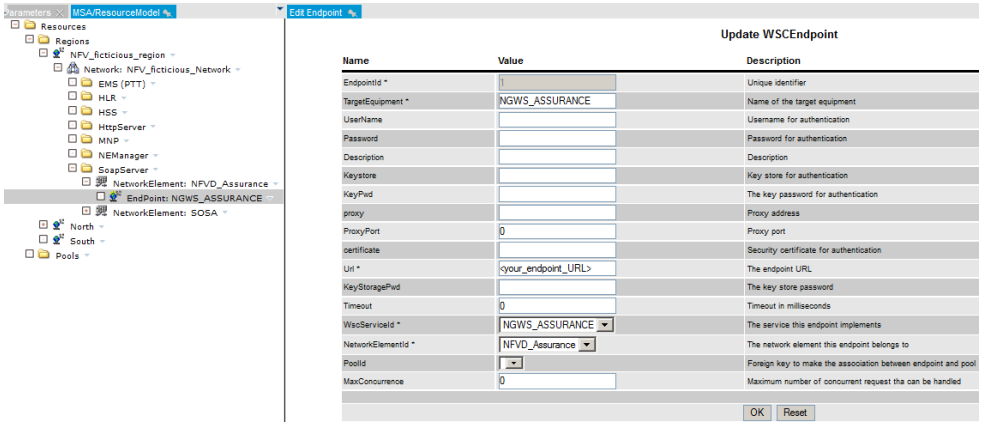

Figure 37 Edit NGWS_Assurance URL and timeout

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 JK765-15001.iso.
2. Go to the `Binaries` directory to find the following NFVD Assurance specific RPM files:
   - nfvd-assur-gw-base-02.00.000-1.el6.noarch.rpm
   - nfvd-assur-gw-tpp-02.00.000-1.el6.noarch.rpm
   - nfvd-assur-gw-core-02.00.000-1.el6.noarch.rpm
   - nfvd-correlation-02.00.000-1.el6.noarch.rpm
   - nfvd-monitors-02.00.000-1.el6.noarch.rpm

Note

Install the five 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-02.00.000-1.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-02.00.000-1.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-02.00.000-1.el6.noarch.rpm
```

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

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

3. Verify if the package is successfully installed:

```
# rpm –-qa | grep –i nfvd
```

```
nfvd-assur-gw-base-02.00.000-1.el6.noarch
```

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-02.00.000-1.el6.noarch.rpm`.

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

1. Transfer the file `nfvd-assur-gw-tpp-02.00.000-1.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-02.00.000-1.el6.noarch.rpm
```

   This command installs the package under `/opt/HP/nfvd/tpp` directory.

3. Verify if the package is successfully installed:

```
# rpm -qa | grep –i nfvd
```

```
nfvd-assur-gw-tpp-02.00.000-1.el6.noarch
```

5.5.3 Installing Assurance gateway core

The NFVD Assurance gateway is available as `nfvd-assur-gw-core-02.00.000-1.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-02.00.000-1.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-02.00.000-1.el6.noarch.rpm
```

   This command installs the package under `/opt/HP/nfvd/tpp/jboss/standalone/deployments` directory.

3. Verify if the package is successfully installed:

```
nfvd-assur-gw-core-02.00.000-1.el6.noarch
```

5.5.3.1 Artifact definition and relation notification

When the NFVD Fulfillment creates, modifies, or deletes any artifact definition or any relationship, notification is sent to the NFVD Assurance gateway.

Assurance gateway takes appropriate create, modify, or delete operation in the Neo4J graph database.

The details to access the Neo4J graph database is maintained in the property file: `/var/opt/HP/nfvd/conf/nfvd-endpoints.xml`

```
<TopologyDB>
    <Instance>
      <host>localhost</host>
      <port>7474</port>
      <db>db</db>
      <data>data</data>
      <protocol>http</protocol>
    </Instance>
</TopologyDB>
```

Update the host and port values to reflect the Neo4J graph DB.

Other attributes related to Neo4J graph DB are maintained in nfvd.properties. These need not be modified.

```
#cache related requests
#cacheEnabled = (true)/(false), to enable/disable assurance graph database cache
cacheEnabled = false
#size of the cache, maximum number of objects in the cache at a time.
maxCacheSize = 10000
```

5.5.3.2 Synchronize NFVD Assurance and Fulfillment

When the NFVD Assurance Gateway application starts, there may be a need to synchronize with NFVD Fulfillment on the infrastructure operations that Fulfillment carried out and Assurance may have missed out.

This can be achieved by the resynch functionality of NFVD Assurance gateway. After starting, Assurance gateway reads the parameters in the file: `/var/opt/HP/nfvd/conf/nfvd.properties` to determine whether to sync at start up. If the flag `RESYNC_AT_STARTUP` is set to `true`, Assurance gateway makes the web service call exposed by Fulfillment to get the details and synchronizes the topology database.

```
# Configure RESYNC_AT_STARTUP as true/yes, for synchronization during Assurance startup
RESYNC_AT_STARTUP=false
# Fulfillment URL connection timeout limit in millisecond, default 1.5 min
FULFILLMENT_CONNECTION_TIMEOUT=90000
# Fulfillment URL response for query timeout limit in millisecond, default 1.5 min
FULFILLMENT_RESPONSE_TIMEOUT=90000
```

You can perform the Resync operation manually as well. Set the `RESYNCH_AT_STARTUP` value to `false`. For more details, see the *HP NFV Director User Guide*.

Required information for accessing the fulfillment URL is available in the `nfvd-endpoints.xml` file.

```
<Fulfillment>
    <Instance>
      <url>http://localhost:8071/ngws/service?wsdl</url>
    </Instance>
</Fulfillment>
```

Modify the URL to update the hostname of the fulfillment server.

5.5.3.3 Life Cycle alarms

Life Cycle alarms are published to the OM bus. The OM server and ActiveMQ ports can be configured in `/var/opt/HP/nfvd/conf/alarms.properties`.

The default ActiveMQ port is defined in `/var/opt/openmediation-70/containers/instance-0/conf/ servicemix.properties`.

```
ALARM_PUBLISHED_URL=failover:(tcp://localhost:10000)?timeout=4000
ALARM_PUBLISHED_TOPIC_NAME=com.hp.openmediation.alarms
ALARM_MAX_BLOCK_QUEUE_SIZE=1024
```

Modify the `ALARM_PUBLISHED_URL` to reflect the OM server. The timeout attribute in the URL is the time (in milli seconds) to connect to the OM topic, failing which, JMS exception will be thrown.

Multiple end points (OM) can be configured as follows:

```
ALARM_PUBLISHED_URL=failover:(tcp://host1:10000, tcp://host2:10000)?timeout=4000
```

In this URL, `host1` and `host2` are the two end points.

5.5.3.4 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-2.0/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-2.0/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:

`/var/opt/UCA-EBC/instances/default/deploy/UCA_NFVD_StatePropagation-2.0/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
```

Note

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

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-02.00.000-1.el6.noarch.rpm` RPM file.

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

1. Transfer the file `nfvd-correlation-02.00.000-1.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-02.00.000-1.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-02.00.000-1.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-V20-1A.zip`
   - `UCA_NFVD_ProblemDetection_Valuepack-vp-2.0.zip`
   - `UCA_NFVD_PublishToNomBus-vp-2.0.zip`
   - `UCA_NFVD_StatePropagation-vp-2.0.zip`

5.5.4.1 Installing UCA Automation NFVD HPSA SP

1. Import the Solution Pack using the `HPSA deploymentmanager` tool.
2. Deploy the NFVD Solution Pack using the `HPSA deploymentmanager` tool.
3. 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 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 2.0
```

```
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, 2.0, 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 2.0
```

```
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, 2.0, 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 2.0
```

```
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, 2.0, 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
```

2. Start the Value Packs.

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

```
$ ./uca-ebc-admin --start -vpn UCA_NFVD_ProblemDetection_Valuepack -vpv 2.0
```

```
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, 2.0, all scenarios ]
INFO  - Logging to org.slf4j.impl.Log4jLoggerAdapter(org.mortbay.log) via org.mortbay.log.Slf4jLog
INFO  - Status: [ UCA_NFVD_ProblemDetection_Valuepack, 2.0, all scenarios ]Value pack has been
successfully started. Status of the value pack: Running
```

```
$ ./uca-ebc-admin --start -vpn UCA_NFVD_PublishToNomBus -vpv 2.0
```

```
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, 2.0, all scenarios ]
INFO  - Logging to org.slf4j.impl.Log4jLoggerAdapter(org.mortbay.log) via org.mortbay.log.Slf4jLog
INFO  - Status: [ UCA_NFVD_PublishToNomBus, 2.0, all scenarios ]Value pack has been successfully started.
Status of the value pack: Running
```

```
$ ./uca-ebc-admin --start -vpn UCA_NFVD_StatePropagation -vpv 2.0
```

```
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, 2.0, all scenarios ]
INFO  - Logging to org.slf4j.impl.Log4jLoggerAdapter(org.mortbay.log) via org.mortbay.log.Slf4jLog
INFO  - Status: [UCA_NFVD_StatePropagation, 2.0, all scenarios ]Value pack has been successfully started.
Status of the value pack: Running
```

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-02.00.000-1.el6.noarch.rpm` RPM file.

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

1. Transfer the file `nfvd-monitors-02.00.000-1.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-monitors-02.00.000-1.el6.noarch.rpm
```

3. Verify if the package is successfully installed:

```
# rpm –-qa | grep –i nfvd
```

```
nfvd-monitors-02.00.000-1.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.

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
```

   If the SiteScope application is running, you cannot run the script.

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:

   http://<#SiteScope Host>:<SiteScope UI port>/SiteScope/servlet/Main.

2. Select the **Accept untrusted SSL certificates** checkbox in the General Settings tab under Preferences → Infrastructure Preferences.

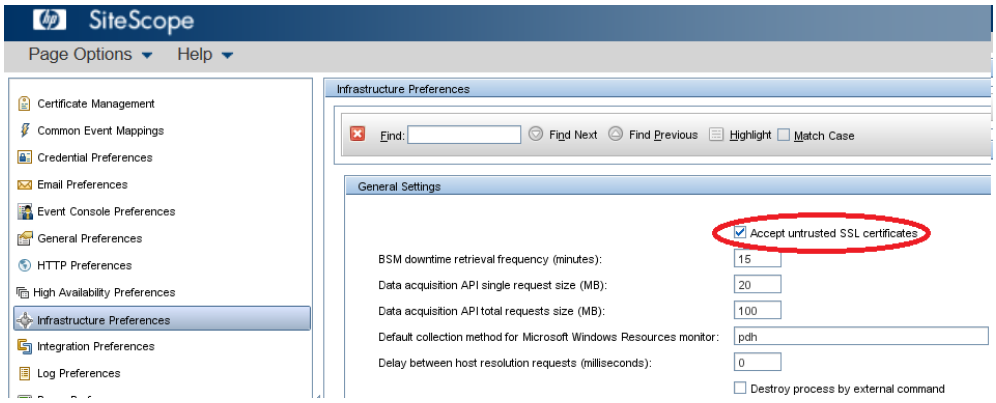

Figure 38 SiteScope > Infrastructure Preferences > General Settings

3. 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.

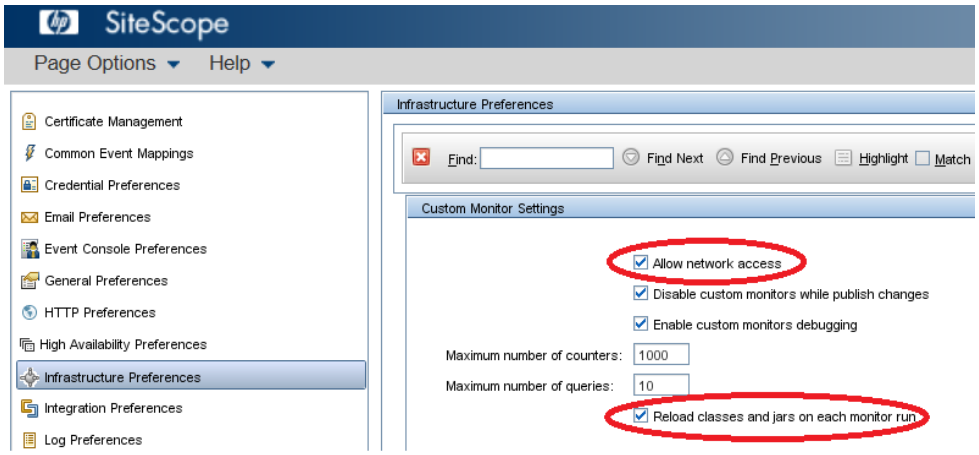

Figure 39 SiteScope > Infrastructure Preferences > Custom Monitor Settings

4. Save the configuration.

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

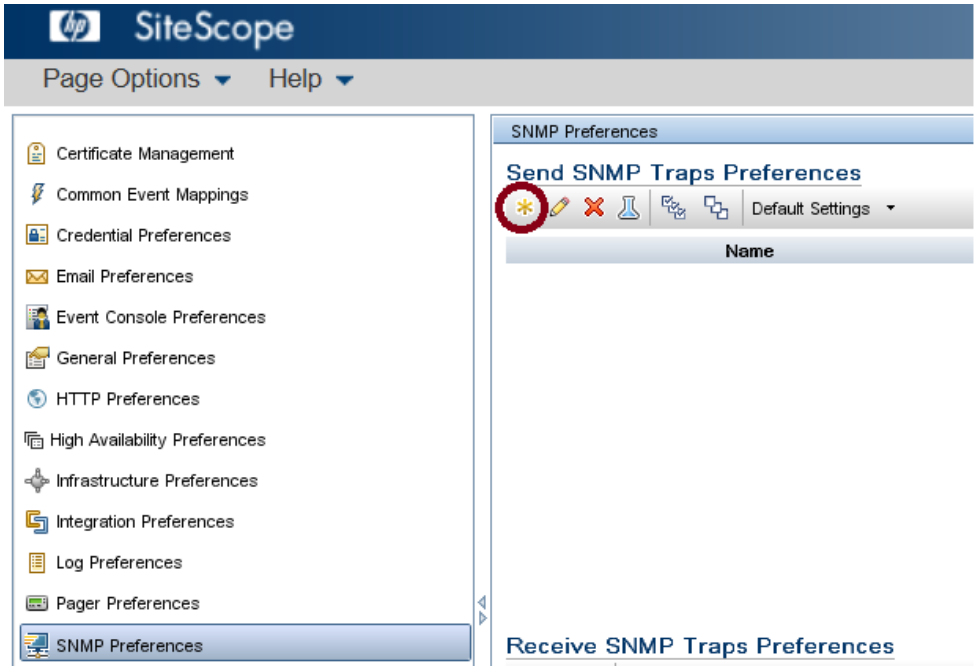

Figure 40 SiteScope > SNMP Preferences

6. Enter the details in the SNMP Trap window that opens.
   - Make sure to enter the Enterprise-specific SNMP trap ID as `11` 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.

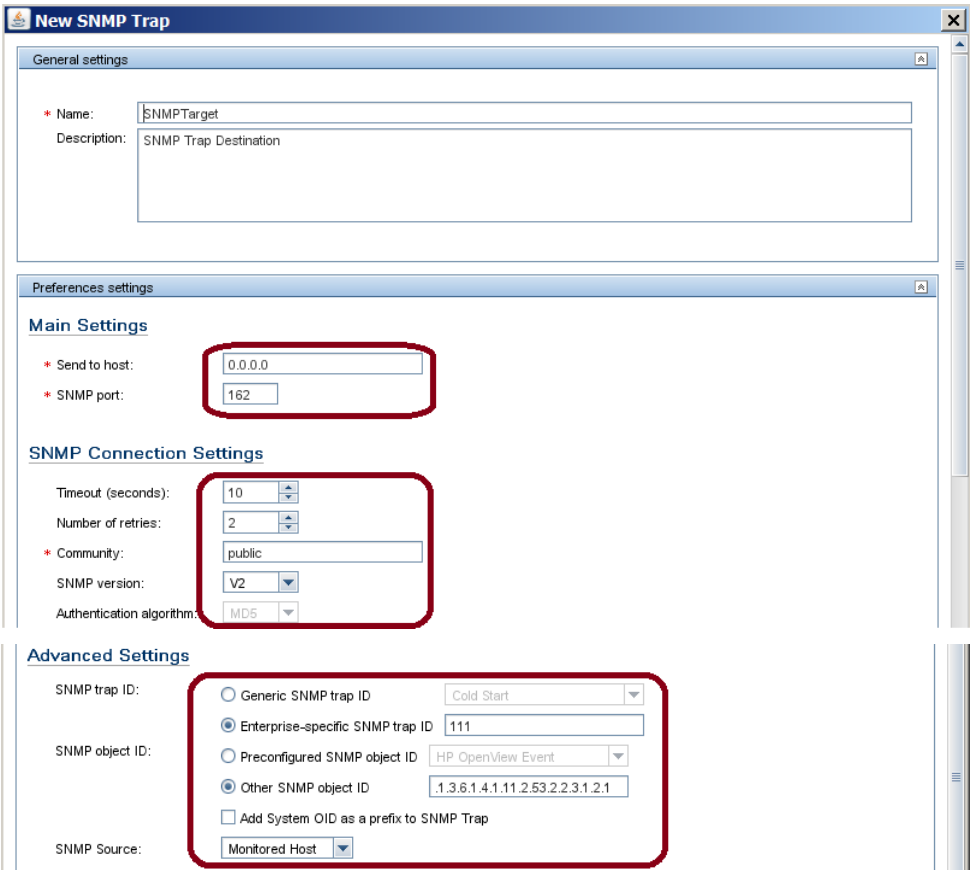

Figure 41 SiteScope > SNMP Preferences > New SNMP Trap

7. Click `OK`.

   You can see an entry created in the `SNMP Preferences` page.

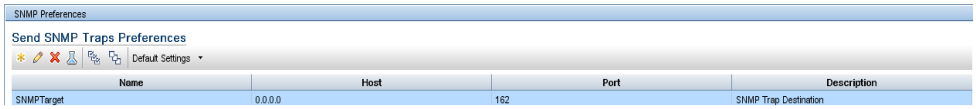

Figure 42 SiteScope > SNMP Preferences >Send SNMP Trap Preferences

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

Figure 43 SiteScope > Import Template

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

   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` location.

10. Click `OK` to import the templates.

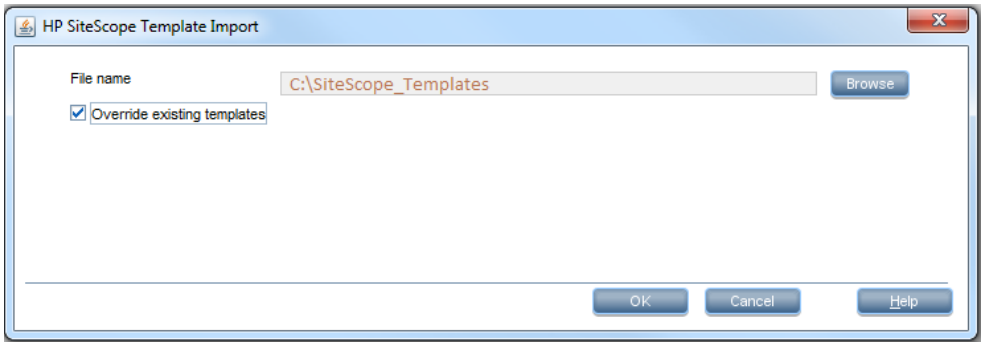

Figure 44 SiteScope > Import Template SiteScope_Templates

11. Select the `Preferences context` → `Search/Filter Tags` → `Select New Tag` icon, enter the details as shown in the following Screen shot, and click the `OK` button.

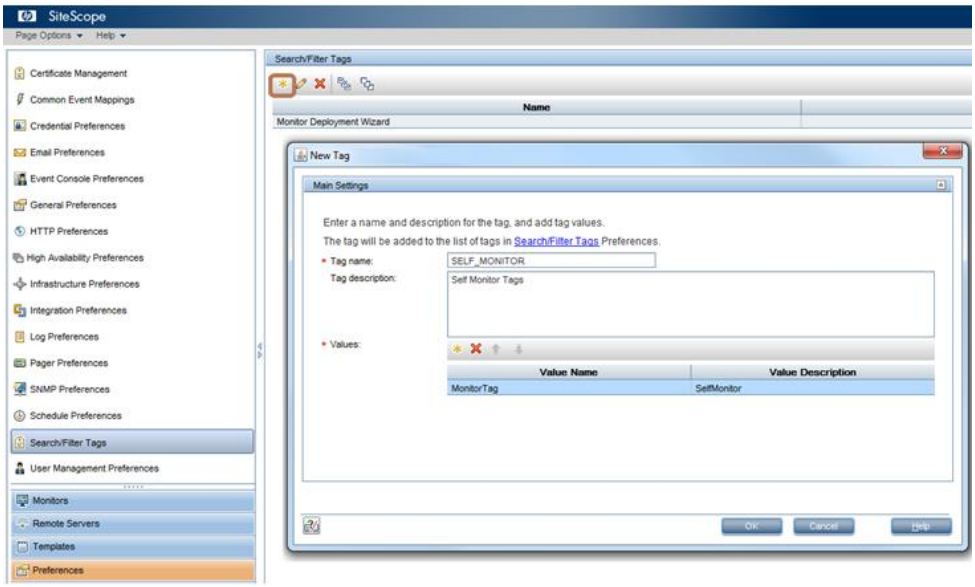

Figure 45 Search/Filter Tags

A new entry is created as shown in the following image.

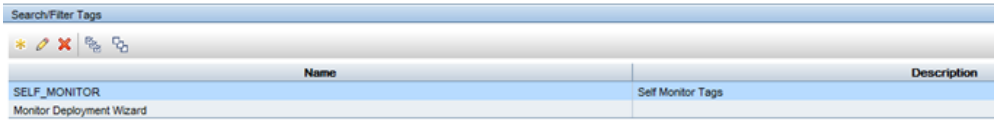

Figure 46 New Search/Filter Tag

Repeat the above steps for SelfMonitor_Sitescope_Templates also.

You can see the imported templates under `NFVD_SELF_MONITORS` and `NFVDDirector`.

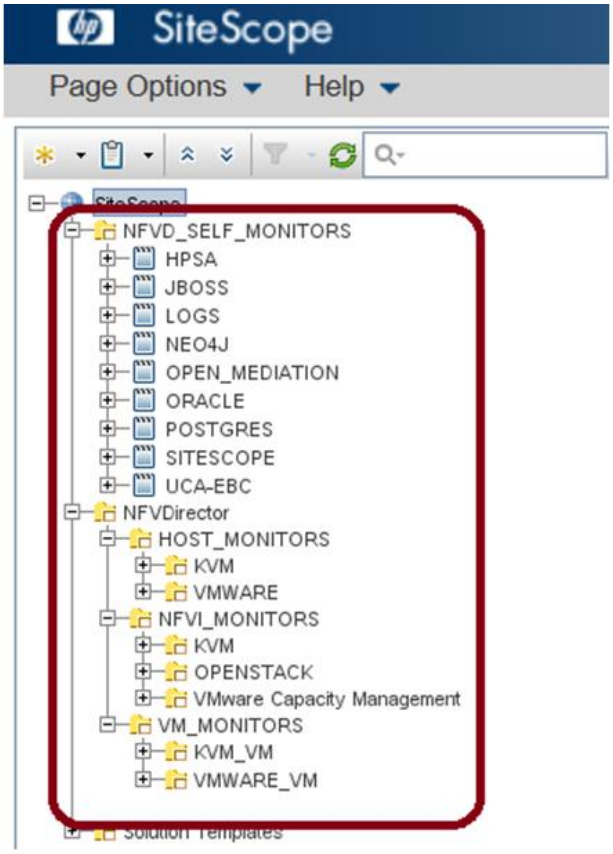

Figure 47 SiteScope > NFVDirector Template listing

12. From the imported templates, select the `VM_MONITORS` tree and select `Import`→`Content Package` option.

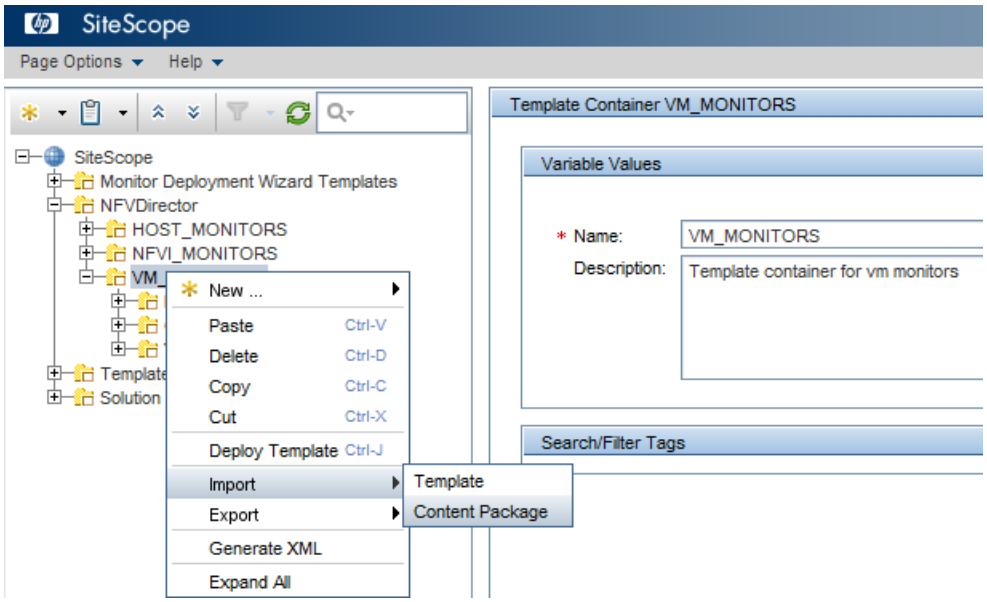

Figure 48 SiteScope > Import Content Package

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

    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` location.

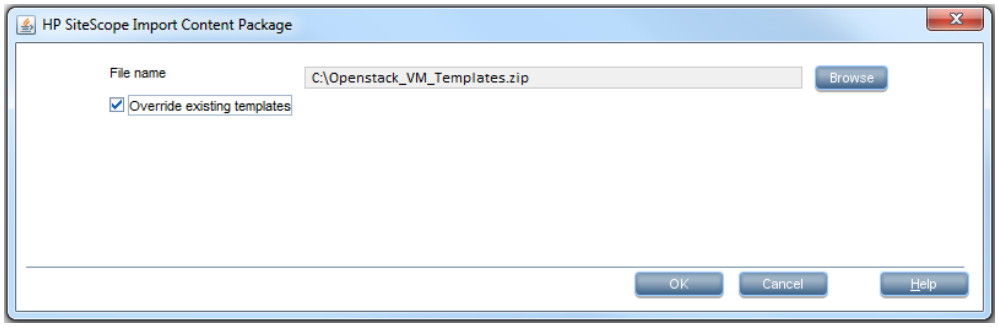

Figure 49 SiteScope > Import Content Package Openstack_VM_Templates.zip

14. After importing, the `Openstack` templates are listed under `OPENSTACK_VM` tree.

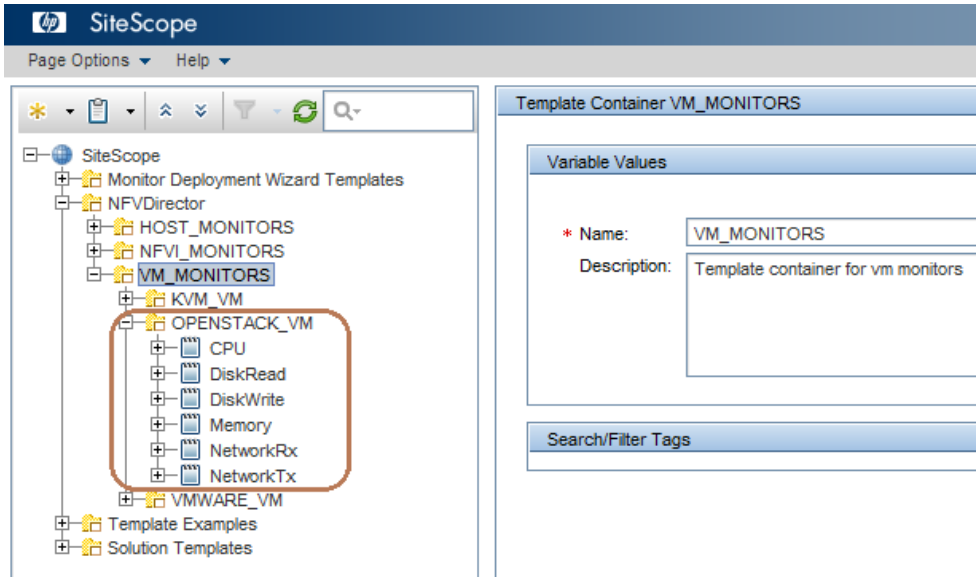

Figure 50 SiteScope > NFVDirector Templates > OpenStack Templates

15. Restart the SiteScope.

5.5.6.3 Assurance gateway configuration for SiteScope

Modify the `/var/opt/HP/nfvd/conf/nfvd-endpoints.xml` file to reflect the SiteScope host, user, password, and port.

```
<Sitescope>
    <Instance>
            <host>localhost</host>
            <user></user>
            <password></password>
        <port>18088</port>
    </Instance>
</Sitescope>
```

Note

The user and password values must reflect the SiteScope administrator credentials.

When self-monitoring is required for NFVD components, assurance gateway checks the graph DB for the NFVD component at a frequency defined by the

`SELF_MONITORS_RUN_FREQUENCY` in the `nfvd.properties` file. By default, the value is set to 15 minutes.

```
SELF_MONITORS_RUN_FREQUENCY=15
```

5.5.6.4 Enabling database logging on SiteScope

Note

The respective database drivers must be available in the directory :

/opt/HP/SiteScope/java/lib/ext

SiteScope has a provision to store the monitor logs into the database.

1. You can enable this optional feature by running the following script: `/opt/HP/nfvd/bin/metricsDBConfig.sh`

   Before running this script, stop the SiteScope application. It creates a database table `SITESCOPELOG`, which enables the logging preferences.

   Before running this script, edit the script to update database details such as DB host, port, SID, user, and password.

   - If the database to be used is Oracle, modify the following details:

```
oracleDBHost="127\.0\.0\.1"
oracleDBPort="1521"
oracleSID="orcl"
oracleDBUser="oracle"
oracleDBPasswd="oracle"
```

   - If the database to be used is PPAS, modify the following details:

```
postGresDBHost="127\.0\.0\.1"
postGresDBPort="5444"
postGresDBName="postgres"
postGresDBUser="postgres"
postGresDBPasswd="postgres"
```

   - If any other database is used, enter the required details when prompted.

2. After running the script, start SiteScope and log into the portal.
3. Go to `Preferences` →`Log Preferences` to verify whether the Database Logging Preferences are set.

   A sample preference setting is shown in the following figure:

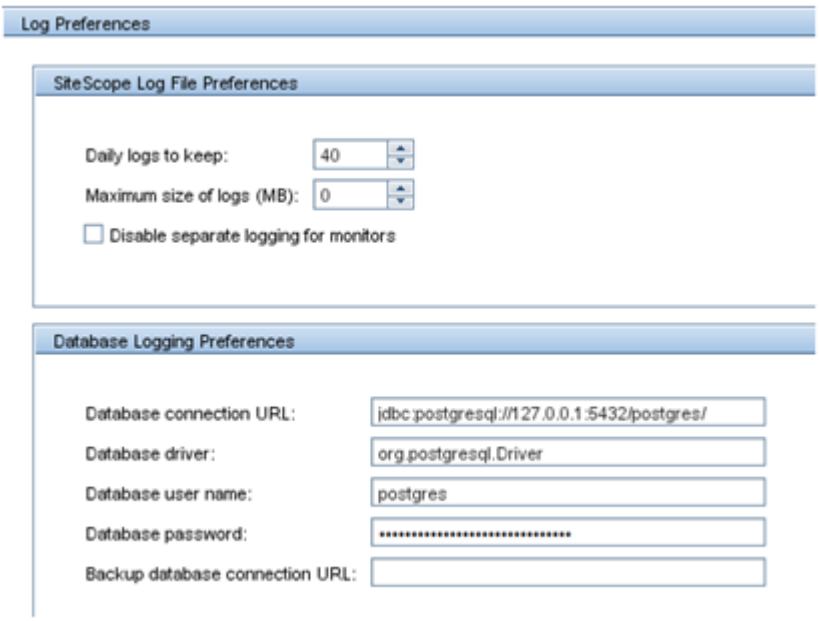

Figure 51 SiteScope > Log Preferences

5.6 Stop and Start NFVD Assurance gateway

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.
- 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.

5.7 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-02.00.000-1.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.

5.7.1 Undeploy the NFVD Fulfillment patches

1. Before undeploying the solution packs, you must delete the patches associated with solution packs.
2. To undeploy the patches for NFVD solution packs, click the `Undeploy Patch` option under `Local Deployment`.
3. Select the solution name as `MSA` from the drop-down list
4. Select the `Do not undeploy SQL` checkbox.
5. Click the `Undeploy patch` button.

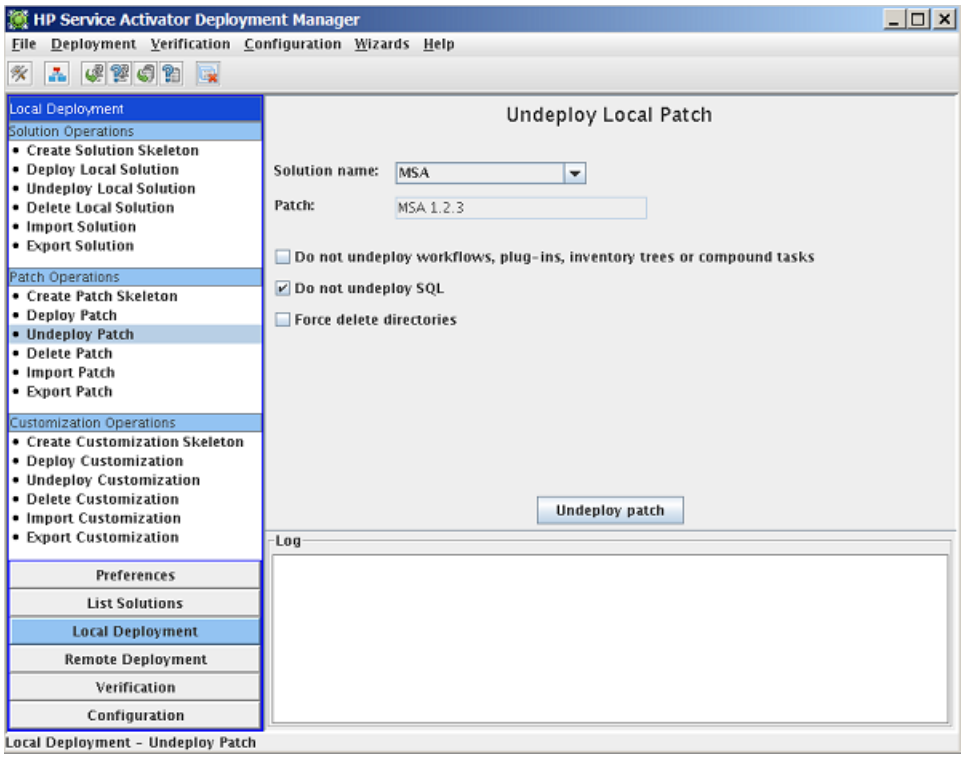

Figure 52 Undeploy patch in deployment manager

5.7.2 Undeploy the NFVD Fulfillment solution packs

Select Local Deployment -> Undeploy Local Solution.

In the `Solution name` drop down list, various solution names are listed.

Repeat the following steps for different solution packs to undeploy them in the sequence mentioned here.

- VNFMANPA
- NFVMPLUGIN
- OSPLUGIN
- RESTPA
- NFVDLF

- NFVAuto
- NFVModel
- MSA
- AD
- IPAM
- CRModel

1. Select the solution pack from the drop-down list.
2. Select the Delete inventory tables and Force delete directories checkboxes and click the Undeploy solution button.

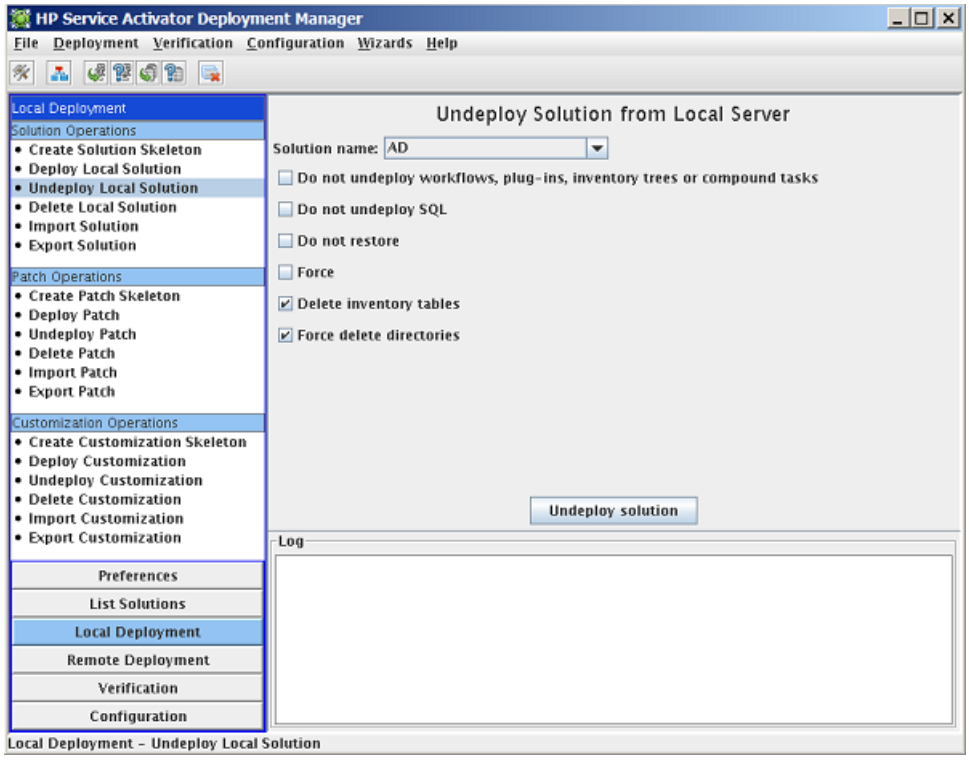

Figure 53 Undeploy solution in deployment manager

3. Select `Local Deployment` -> `Delete Local Solution`. Choose the solution name that was undeployed in the previous step, and click `Delete solution` button.

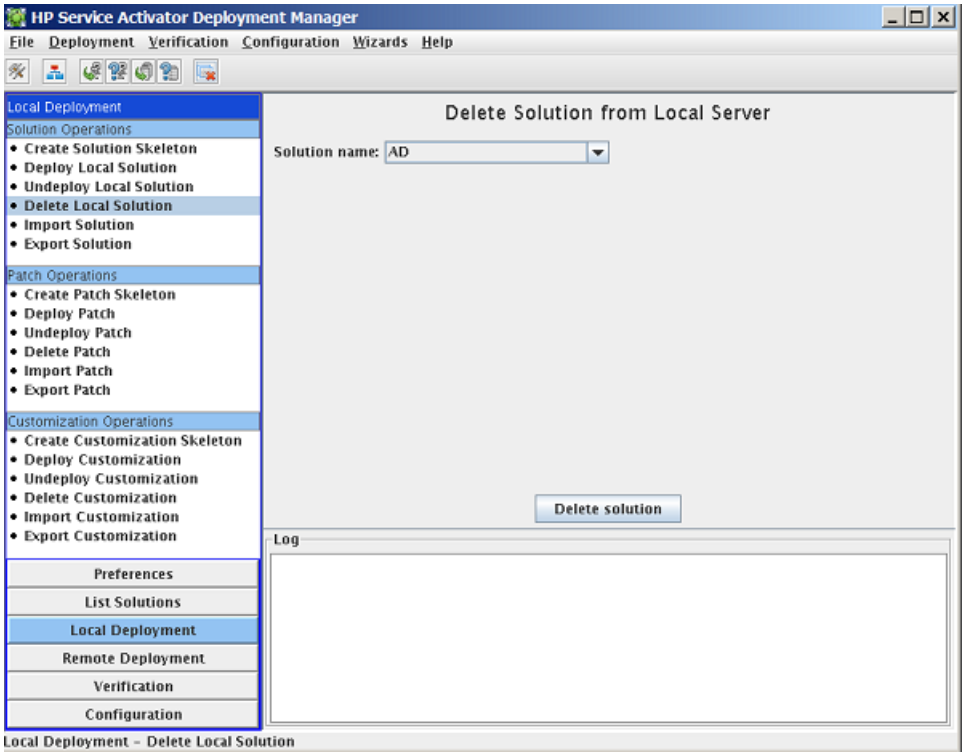

Figure 54 Delete solution in deployment manager

5.8 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-02.00.000-1.el6.noarch
# rpm -ev nfvd-assur-gw-tpp-02.00.000-1.el6.noarch
# rpm -ev nfvd-monitors-02.00.000-1.el6.noarch
# rpm -ev nfvd-correlation-02.00.000-1.el6.noarch
# rpm -ev nfvd-assur-gw-base-02.00.000-1.el6.noarch
```

2. Manually remove the following directories:
   - `/opt/HP/nfvd`
   - `/var/opt/HP/nfvd`

Note

Uninstalling the `nfvd-monitors-02.00.000-1.el6.noarch` does not remove the configuration settings performed on the SiteScope system.

5.9 Various log file locations in NFVD

Product	Logs Location
SiteScope	/opt/HP/SiteScope/logs/
HPSA	/var/opt/OV/ServiceActivator/log/<hostname>

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

Table 38 Various log locations

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

Chapter 6

Upgrading to NFVD V2.0

If you have NFVD V1.0 or NFVD V1.0.1 installed in your system, this chapter provides process to upgrade the solution.

First step is to upgrade the base products, and second step is to upgrade the NFVD solution. Note that there is no data migration supported from NFVD V1.0 or NFVD V1.0.1 to NFVD V2.0. This means that any Artifact Definition, Template, or Instance created in previous versions must be deleted and recreated in NFVD V2.0. Also, any Virtual Machine created in the infrastructure must be deleted and recreated.

6.1 Upgrading the base products

Following base products were upgraded in NFVD V2.0, as compared to NFVD V1.0 or NFVD V1.0.1

Product	Component	New Version	Old Version
NFVD	Solution	V2.0	V1.0 or V1.0.1
HPSA	Hotfix	SAV62-1A-5	SAV62-1A-2
HPSA Extension Pack	Hotfix	EP6.1-2	EP6.1-1
OM	Base Product	7.0.0	V620-01
Channel Adapter	UCA EBC CA	V3.1	V3.0
Channel Adapter	UCA HPSA CA	V2.0	V1.0
Channel Adapter	UCA Autoconsole CA	V2.0	V1.0
Channel Adapter	Generic SNMP CA	V2.0	V1.0
Channel Adapter	SiteScope Customization for Generic SNMP CA	V2.0	V1.0
Channel Adapter	VMWare ESXi Customization for Generic SNMP CA	V2.0	V1.0
HP UCA for EBC Topology Extension	Base Product	V3.1	V3.0
HP UCA for EBC	Base Product	V3.1	V3.0
HP UCA Automation	Base Product	V1.1	V1.0-REV A
SiteScope	Patch	HPSiS1124_11	SiteScope11.23_

Product	Component	New Version	Old Version
		.24	00276

Table 39 Base products upgraded in NFVD 2.0

6.1.1 Uninstalling HP Service Activator

6.1.1.1 Remove HP Service Activator

Follow the procedure mentioned here to remove the HP Service Activator.

1. Run the `remove.serviceactivator` command to remove the installation.

```
# cd /opt/OV/ServiceActivator/bin/
# ./remove.serviceactivator
```

2. Manually remove the following directories:
   - `/opt/OV/ServiceActivator`
   - `/opt/HP/jboss`
   - `/var/opt/OV/ServiceActivator`
   - `/etc/opt/OV/ServiceActivator`

6.1.1.2 Remove the database

To drop the database configured for the HP Service Activator, follow the instructions provided in the section 4.1 Installing HP Service Activator and section 4.2 Installing HP Service Activator Extension Pack.

6.1.2 Uninstalling Channel Adapters on OM 6.2

It involves the following phases:

- Uninstall Channel Adapters
- Uninstall OM 6.2
- Install OM 7.0.0
- Install Channel Adapters

Following subsection describes the process to uninstall the Channel Adapters. For instructions on installing OM and Channel Adapters, refer to sections 4.3, 4.6, 4.7.3, 4.7.4 respectively.

6.1.2.1 Uninstall Channel Adapters

Ensure that OM container is running.

Run the following commands in sequence for each Channel Adapter.

```
# /opt/openmediation—V62/bin/nom_admin --undeploy-ip-in-container 0 <CA>
# /opt/openmediation-V62/bin/nom_admin --remove-ip-in-container 0 <CA>
# /opt/openmediation-V62/bin/nom_admin --remove-ip <CA>
# rm –rf /opt/openmediation-V62/ips/<CA>
```

Where `CA` represents the following channel adapters:

- generic-snmp-ca-V10
- snmp-customization-sitescope-V10
- snmp-customization-vmware-V10

- uca-autoconsole-ca-V10
- uca-hpsa-ca-V10
- uca-ebc-ca-3.0

6.1.3 Uninstalling OM V6.2

Uninstall the OM V620-01.

```
# /opt/openmediation-V62/bin/nom_admin --undeploy-ip-in-container 1 smx-basic-components
# /opt/openmediation-V62/bin/nom_admin --remove-ip-in-container 1 smx-basic-components
# /opt/openmediation-V62/bin/nom_admin --remove-ip smx-basic-components
# /opt/openmediation-V62/bin/nom_admin --undeploy-ip-in-container 1 nom-basic-smx-components
# /opt/openmediation-V62/bin/nom_admin --remove-ip-in-container 1 nom-basic-smx-components
# /opt/openmediation-V62/bin/nom_admin --remove-ip nom-basic-smx-components
# /opt/openmediation-V62/bin/nom_admin --undeploy-ip-in-container 1 smx-extra-components
# /opt/openmediation-V62/bin/nom_admin --remove-ip-in-container 1 smx-extra-components
# /opt/openmediation-V62/bin/nom_admin --remove-ip smx-extra-components
# /opt/openmediation-V62/bin/nom_admin --shutdown-container --all
# /opt/openmediation-V62/bin/nom_admin --remove-container --all
# /opt/openmediation-V62/bin/nom_install --remove
# /opt/openmediation-V62/bin/nom_admin
# rpm -e ngossnom-basic-smx-components-V620-01
# rpm -e ngosssmx-extra-components-V620-01
# rpm -e ngossopenmediation-V620-01
```

Follow the instructions in section 4.3 to install OM 7.0.0.

6.1.4 Uninstalling UCA for EBC Topology Extension 3.0

Run the following commands:

```
# /opt/UCA-EBC/bin/uninstall-uca-ebc-topology
```

Enter the number `0` and press `Enter` when prompted with `Enter the index number of UCA-EBC TOPOLOGY version to un-install.`

6.1.5 Uninstalling UCA for EBC 3.0

1. Run the following commands:

```
# /opt/UCA-EBC/bin/uninstall-uca-ebc
```

2. Enter the number `0` and press `Enter`, when prompted with `Enter the index number of UCA-EBC version to un-install.`

6.1.6 Uninstalling UCA Automation 1.0

Run the following commands to uninstall the packages.

```
# rpm -ev UCA_Automation_Console-V1.0-REV_A.noarch
#  rpm -ev UCA_Automation-V1.0-REV_A.noarch
```

6.1.6.1 Undeploy UCA Automation HPSA SP

1. Undeploy the solution pack UCA using the deploymentmanager tool.

   Select the `Delete Inventory tables` option.

2. Delete the solution UCA using the deploymentmanager tool.
3. Edit `/etc/opt/OV/ServiceActivator/config/mwfm.xml`

   Remove the following text from the file.

```
<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" value="com.hp.ov.activator.mwfm.engine.module.WeightedEngineQueue"/>
</Module>
```

6.1.7 Upgrading SiteScope

Follow the instructions in section 4.8.1 to upgrade to SiteScope 11.24.

6.2 Upgrading the NFVD solutions

1. Run the following commands to get the version of NFVD installed.

```
# rpm –qa | grep -i nfvd
```

   - NFVD V1.0.1 is installed if we get the following output.

```
nfvd-assur-gw-base-01.00.001-1.el6.noarch
nfvd-correlation-01.00.001-1.el6.noarch
nfvd-assur-gw-core-01.00.001-1.el6.noarch
nfvd-assur-gw-tpp-01.00.001-1.el6.noarch
nfvd-monitors-01.00.001-1.el6.noarch
nfvd-fulfillment-01.00.001-1.el6.noarch
```

   - NFVD V1.0 is installed if we get the following output.

```
nfvd-assur-gw-base-01.00.000-1.el6.noarch
nfvd-correlation-01.00.000-1.el6.noarch
nfvd-assur-gw-core-01.00.000-1.el6.noarch
nfvd-assur-gw-tpp-01.00.000-1.el6.noarch
nfvd-monitors-01.00.000-1.el6.noarch
nfvd-fulfillment-01.00.000-1.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. Install the new NFVD solutions.

Chapter 7

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.

7.1 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
```

7.2 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.

7.2.1 Red Hat Enterprise Linux 6.4

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>
```

The `<Binary File>` is one of the following:

Binary File	Component Name
nfvd-assur-gw-tpp-02.00.000-1.el6.noarch.rpm	NFVD Assurance 3rd party products
nfvd-assur-gw-core-02.00.000-1.el6.noarch.rpm	NFVD Assurance Gateway
nfvd-assur-gw-base-02.00.000-1.el6.noarch.rpm	NFVD Start/Stop Scripts
nfvd-correlation-02.00.000-1.el6.noarch.rpm	UCA Automation NFVD domain solution packs
nfvd-monitors-02.00.000-1.el6.noarch.rpm	SiteScope NFVD monitors
nfvd-fulfillment-02.00.000-1.el6.noarch.rpm	NFV Director Fulfillment solution packs

Table 40 Binaries List for Signature

2. Look for the following output from the gpg command:

```
gpg: Good signature from "Hewlett-Packard Company RSA (HP Codesigning Service)"
```