HP NFV Director

HP NFV Director

Version 1.0

Installation Guide

Edition: 1.1

For the Linux (RHEL6.4) Operating System

September 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.

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

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, NOM, Sitescope, HPSA, Oracle/EnterpriseDB, VMware, KVM, OpenStack, 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 1.0	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 V1.0 - Installation Guide*
- *OSS Open Mediation V620L01Installation 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 V3.0 Installation Guide*

Support

Please visit our HP Software Support Online Web site at www.hp.com/go/hpsoftwaresupport 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
${OM_INSTANCE}	/var/opt/openmediation-V62/containers/<instance-#>
${UCA_AUTOMATION_CONSOLE_HOME}	This directory contains the UCA Automation UI deployment. The path refers to /opt/UCA-ATM
${UCA_EBC_HOME}	The root directory of UCA-EBC. The default value is /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

Table 2 Install Location Descriptors

Chapter 1

Introduction

This document describes the procedure for installation and configuration of NFV Director V1.0 product.

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 products:

1. NFV-D Fulfillment
   - HP Service Activator v6.2
     - HP Service Activator Extension Pack v6.1
     - CR Model Solution Pack
     - IPAM Solution Pack
     - MSA Solution Pack
     - GPM Solution Pack
     - NFVDLF Solution Pack
     - NFVModel Solution Pack
     - NFVAutomation Solution Pack
     - OpenStack Client Solution Pack
     - RestPA Solution Pack
2. NFV-D Assurance
   - HP UCA Automation v1.0
     - HP UCA Automation Console v1.0
     - HP Service Activator v6.2
     - HP UCA for EBC v3.0
     - HP UCA for EBC v3.0 Topology Extension
   - OSS Open Mediation v6.2
     - 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
   - Assurance Gateway v1.0
   - Site Scope v11.23

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 NFVD Deployment Architecture – Single Server 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 NFVD Deployment Architecture – Distributed depicts NFVD Assurance components distributed in different systems, such as NFVD Assurance Gateway, UCA Automation, and SiteScope.

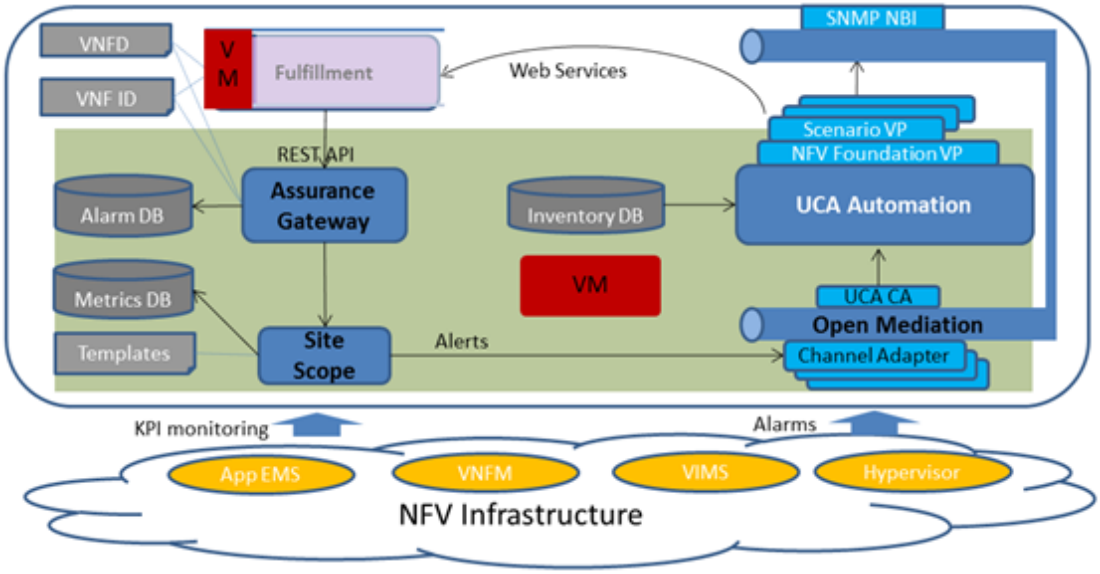


Figure 1 NFVD Deployment Architecture – Single Server

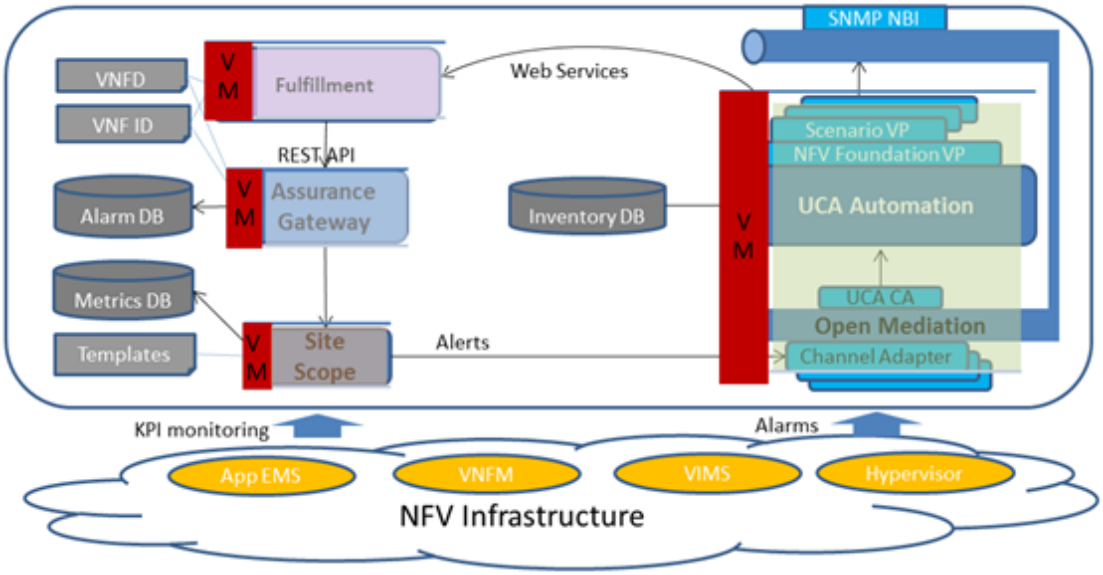


Figure 2 NFVD Deployment Architecture – Distributed

Chapter 2

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).

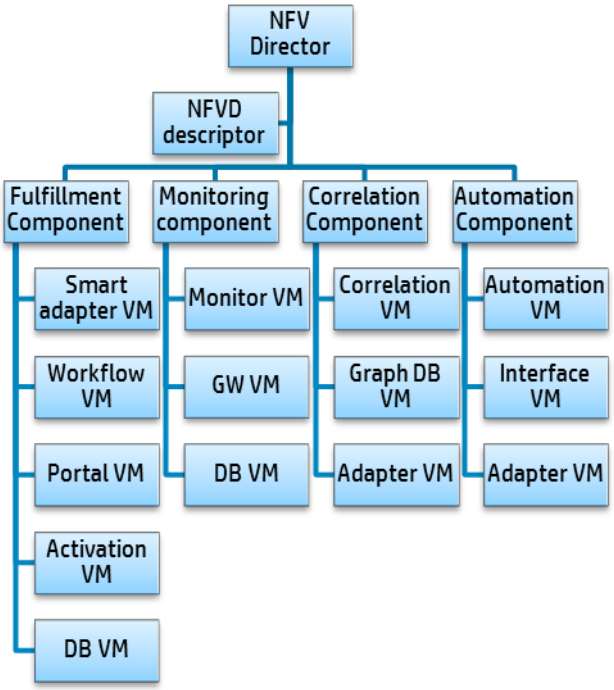


Figure 3 NFV Director sample schema

2.1 NFVD Fulfillment

2.1.1 Hardware requirement

2.1.1.1 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 3 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.

2.1.1.2 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.

Compo-nents	OS	DB	Server	Core	RAM	DISK
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
Fulfillment Database	REDHAT 6.4	Oracle/ PPAS	VM6	16	256	2000

Table 4 Fulfillment distributed setup hardware recommendation

2.1.2 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-2
HP Service Activator Extension Pack	6.1	+ Hotfix EP6.1-1
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 5 NFVD Fulfillment Software requirements

2.2 NFVD Assurance

2.2.1 Hardware requirement

2.2.1.1 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 11.23)	Embedded		VM2	4 (bet-ter 8)	16	146 (better 300)
Monitoring Database (metrics DB)	Embedded	Embedded				
Correlation & Automation Engine	Embedded	Oracle/ PPAS				
Correlation Database	Embedded	GRAPH DB				
		Embedded				

Table 6 Assurance single server hardware recommendation

2.2.1.2 For distributed server setup

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

Compo-nents	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 Engine	Red Hat 6.4		VM4	8	128	320
Automation Engine	Red Hat 6.4		VM5	8	128	320

Correlation Database	Red Hat 6.4	GRAPH DB	VM6	16	256	2000
HPSA 6.2	Red Hat 6.4		VM7	8	128	320
Automation HPSA Database	Red Hat 6.4	Oracle/ PPAS	VM8	8	128	320

Table 7 Assurance distributed server hardware recommendation

2.2.2 Software requirement

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

Product	Version	Remark
Assurance Gateway	V1.0	Uses JBoss 7.1.3
Java	SE 6 update 37 JDK or later	**NOTE:** Do not use JDK version 7
RHEL	6.4	And all available patches

Table 8 NFVD Assurance Gateway Software

Product	Version	Remark
HP UCA for EBC	V3.0	+ Patch UCAEBC30SRVLIN_00006
HP UCA for EBC Topology Extension	V3.0	+ Patch UCAEBC30TOPOLIN_00001
HP UCA Automation Console	V1.0-REV A	+ Patch EBCATMLIN_00001
HP Service Activator	V62-1A	+ Patch V62-1A-2
Oracle database	11g	Either Oracle DB or PPAS
PPAS database	9.2	Either Oracle DB or PPAS
OSS Open Mediation and CA		See Table 10 Open Mediation and Channel Adapters
Java		See Table 8 NFVD Assurance Gateway Software
RHEL		See Table 8 NFVD Assurance Gateway Software

Table 9 UCA Automation software

Product	Version	Remark
OSS Open Mediation	V620-01	+ Patch OSSOPENMEDIATIONLNX_00002
UCA EBC Channel Adapter	V3.0	
UCA HPSA Channel Adapter	V1.0	Available in UCA Automation Patch EBCATMLIN_00001
UCA Autoconsole Channel Adapter	V1.0	Available in UCA Automation Patch EBCATMLIN_00001
Generic SNMP CA	V1.0	
SiteScope Customization for Generic SNMP CA	V1.0	
VMware ESXi Customization for Generic SNMP CA	V1.0	
RHEL		See Table 8 NFVD Assurance Gateway Software

Table 10 Open Mediation and Channel Adapters

Product	Version	Remark
SiteScope	11.20	+ Patch Sitescope11.23_00276

Table 11 SiteScope Software

Chapter 3

Installing and configuring the product

Extract the files contained in JK596-15001 ISO file to a location of your choice (%INSTALLATION_DIR%). The following folder structure is created:

%INSTALLATION_DIR%/ReadMe
%INSTALLATION_DIR%/OpenSource
%INSTALLATION_DIR%/Binaries
%INSTALLATION_DIR%/Documentation

3.1 Installing the NFVD Fulfillment components

For HPSA 6.2-1A installation instructions, see `HP Service Activator Installation Guide Edition: V62-1A`.

For HPSA Hotfix V62-1A-2 installation instructions, see `HPSA Hotfix Installation Guide Edition: V62-1A-2`.

NOTE: After installing HPSA, import and deploy the CRModel solution pack. During the installation of the HPSA Hotfix, choose `Yes` when you are prompted to upgrade the CRModel patch.

3.1.1 HPSA Extension Pack (EP) installation

For HPSA Extension Pack V6.1 installation instructions, see `HPSA Extension Pack Installation Guide Release V6.1`.

For HPSA Extension Pack Hotfix EP6.1-1 installation instructions, see `HPSA Extension Pack Hotfix Installation Guide Edition: EP6.1-1`.

3.1.2 Generate xmaps database model

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

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

3.1.3 Importing and deploying fulfillment solutions and patches

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

- Mount the ISO image `JK596-15001.iso`.
- Go to the `Binaries` directory to find the following RPM file:

  `nfvd-fulfillment-01.00.000-1.el6.noarch.rpm`
- Install the rpm by running the following command:

  `rpm -ivh nfvd-fulfillment-01.00.000-1.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
  - NFVAutomation.zip
  - NFVDLF.zip
  - RESTPA.zip
  - OSPLUGIN.zip

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

3.1.3.1 Importing solution packs

Import the following fulfillment solutions in the sequence as shown below. For instructions on using the Import HPSA Solution, see the Local Solution Deployment Operations section in Using the Deployment Manager chapter of the `HP Service Activator Solution Separation and the Deployment Manager Guide`.

NOTE: In order 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.

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

Table 12 NFVD Fulfillment Solution Pack locations

NOTE: Importing `MSA-1.2.2.zip` prompts a pop-up message that the Solution name `MSA-1.2.2` is missing. Edit the Solution name to `MSA`, and click `OK`.

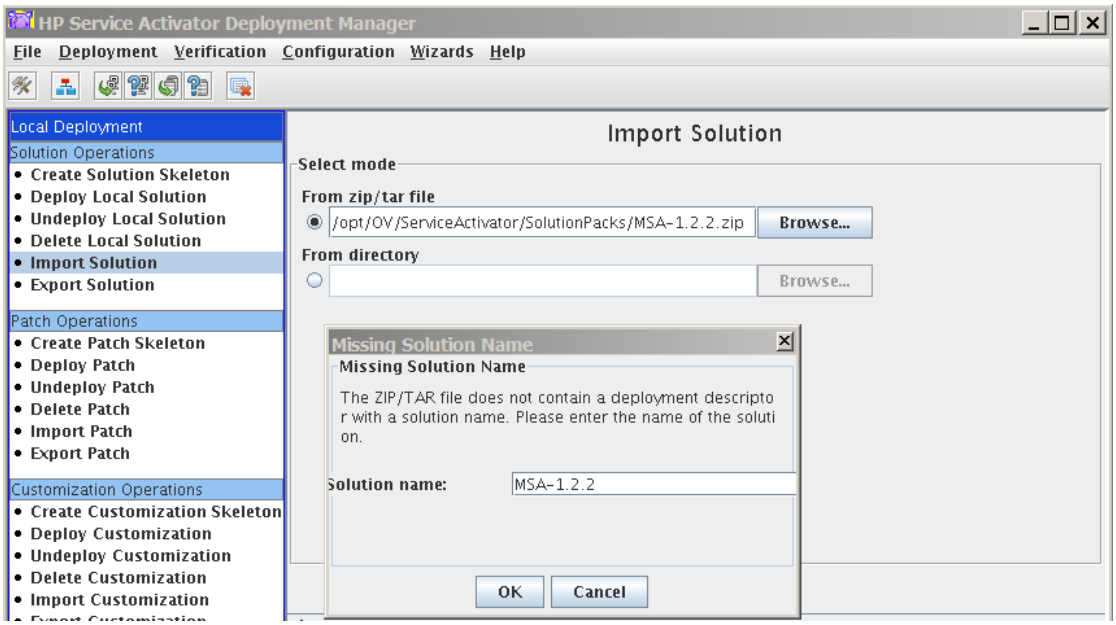


Figure 4 Import MSA Solution Pack

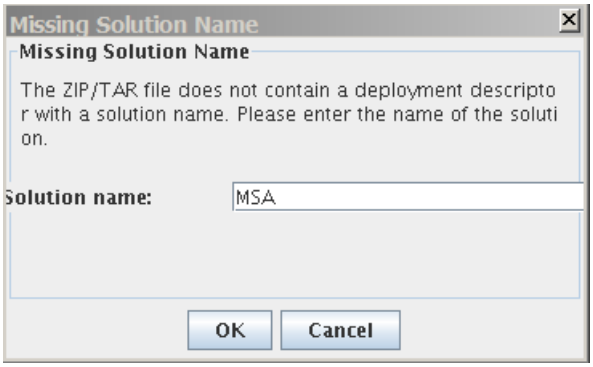


Figure 5 Edit Solution Name MSA-1.2.2 to MSA

NOTE: Importing `NFVAutomation.zip` prompts a pop-up message that the Solution name NFVAutomation is missing. Edit the Solution name to `NFVAuto`, and click `OK`.

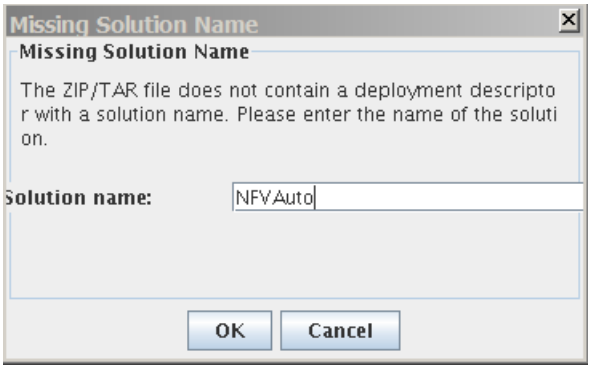


Figure 6 Edit Solution Name NFVAutomation to NFVAuto

NOTE: Importing `AD.zip` prompts a pop-up message that the Solution name `AD` is missing. No need to edit the Solution. Leave it as suggested – `AD`, and click `OK`.

3.1.3.2 Deploying the solutions

Deploy the previously imported Solutions in the same sequence as listed in Importing Solutions section. For instructions on deploying the HPSA solution, deploy solutions; see the Local Solution Deployment Operations section in Using the Deployment Manager chapter of the `HP Service Activator Solution Separation and the Deployment Manager Guide.`

NOTE: Check Create inventory tables option while deploying solution packs.

NOTE: MSA solution pack has a patch. Once you have deployed the MSA solution pack, import and deploy the MSA patch, before deploying any other solution pack. Instructions to import and deploy a HPSA patch is explained in Import MSA patch and Deploy MSA patch sections.

Choose the following file for deployment when prompted:

Solution Pack Name	Database System	File
CRModel	Oracle	deploy_oracle.xml
	PPAS	deploy_ppas.xml
IPAM	Oracle/PPAS	deploy.xml
AD	Oracle/PPAS	deployUnix.xml
MSA Solution Pack	Oracle/PPAS	deployUnix_6_1.xml
MSA Patch	Oracle/PPAS	deployUnix_6_x.xml
NFVModel	Oracle/PPAS	deploy.xml
NFVAutomation	Oracle	Deploy_ORACLE.xml
	PPAS	Deploy_PPAS.xml
NFVDLF	Oracle/PPAS	deploy.xml
RESTPA	Oracle/PPAS	deploy.xml
OSPLUGIN	Oracle/PPAS	deploy.xml

Table 13 NFVD Solution Pack and Patch Deployment Files

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

A sample procedure to deploy the solution is as follows:

- Launch the deploymentmanager tool from `/opt/OV/ServiceActivator/bin/`
- Set the DB user and password in `System Database Connection` under `Preferences`. Click `OK` to verify.
- Select `Deploy Local Solution` option under `Local Deployment` in the UI. Choose the Solution Name from the drop down list, choose an appropriate deployment file, choose the `Create inventory tables` checkbox, and then click `deploy solution`.

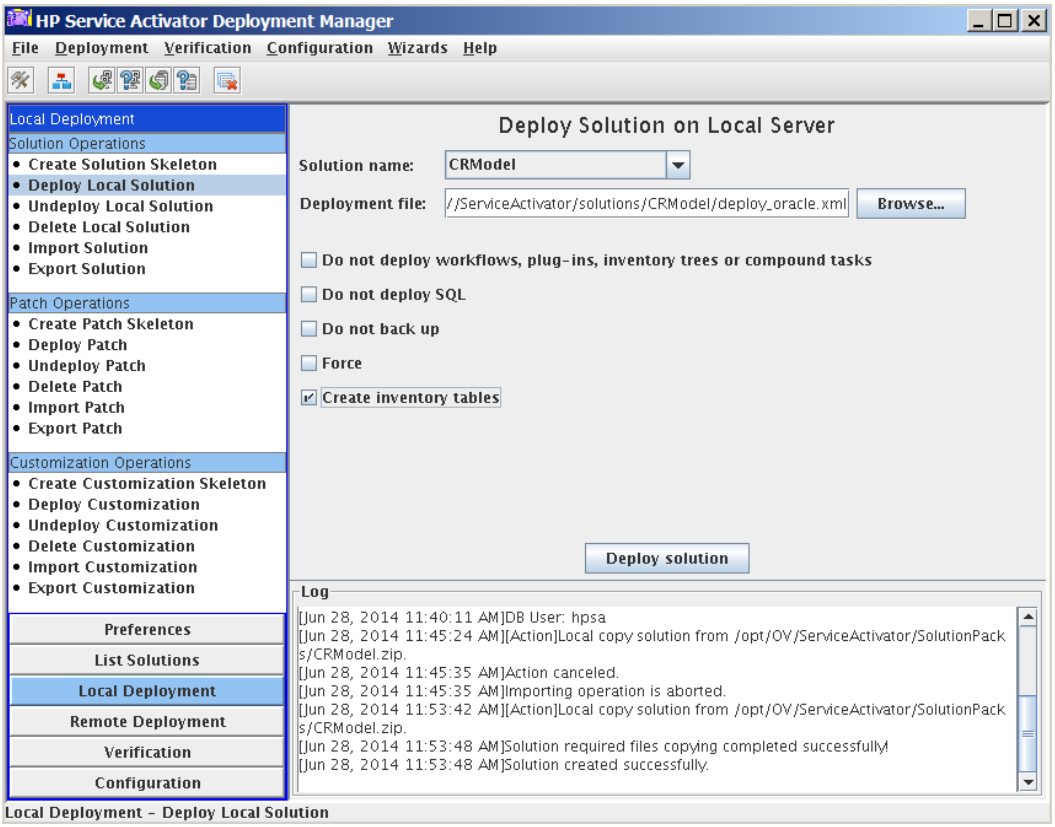


Figure 7 Deploy Solution Pack

3.1.3.3 Import MSA patch

The Solution MSA has a patch. This patch has to be imported and deployed. For instructions on importing a patch, see the Patch Operations section in Using the Deployment Manager chapter of the `HP Service Activator Solution Separation and the Deployment Manager Guide`.

3.1.3.4 Deploy MSA patch

Once the MSA patch has been imported, deploy the patch by following the instructions in Patch Operations section of Using the Deployment Manager chapter of the `HP Service Activator Solution Separation and the Deployment Manager Guide`.

NOTE: Check the `Do not deploy SQL` option in the UI before deploying the MSA patch.

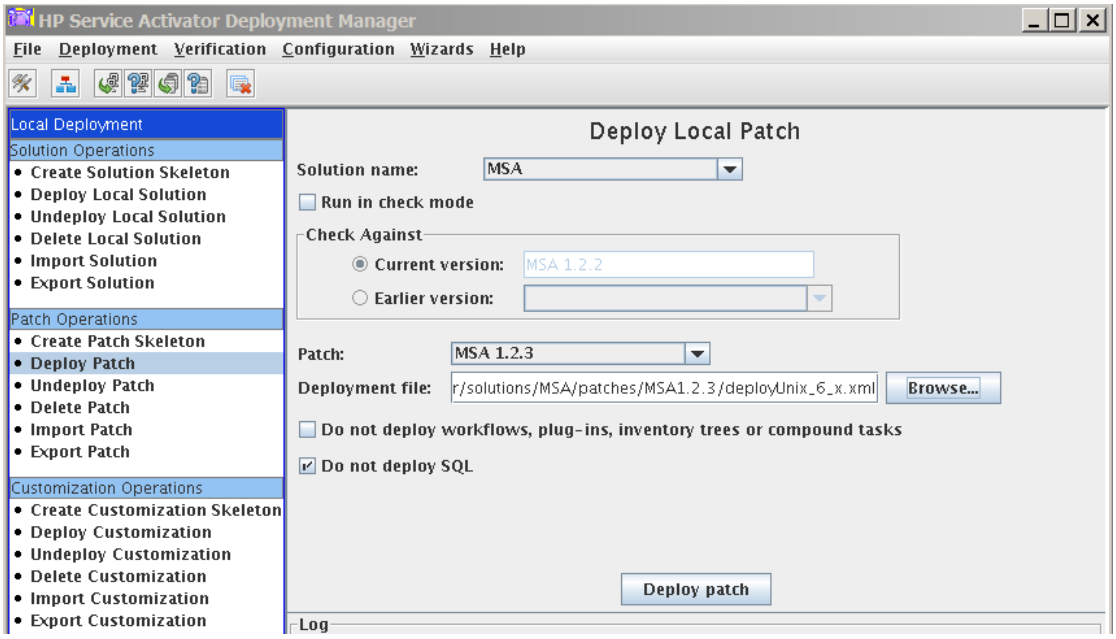


Figure 8 Deploy MSA Patch

3.2 Undeploying and uninstalling the NFVD Fulfillment components

NFVD Fulfillment RPM can be uninstalled by running the `rpm -ev` option.

Run the following command to uninstall the NFVD Fulfillment RPM:

- `rpm -ev nfvd-fulfillment-01.00.000-1.el6.noarch`

In order to undeploy the NFV Director fulfillment Solution Packs, follow the `HP Service Activator Solution Separation and the Deployment Manager Guide.`

You can choose to also delete the Patch and Solution, so that the directory `/opt/OV/ServiceActivator/solutions` also deletes the solution directory completely.

NOTE: Before undeploying the solution packs that have some Patch associated, you must undeploy the patch first. Else, the solution name does not appear in the Undeploy option.

3.3 Configuring the NFVD Fulfillment solution

3.3.1 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`

```
<Module>
```

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

Table 14 mwfm.xml transaction_manager module

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

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

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

```
<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>
```

Table 15 mwfm.xml ConcurrentWorkflowsModule

```
<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>
```

Table 16 mwfm.xml LockModule

```
<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>
```

Table 17 mwfm.xml transaction_manager 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>
```

Table 18 mwfm.xml wsc module

```
<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>
```

Table 19 mwfm.xml NfvManagerModule

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

```
    <Param name="database_module"   value="db"/>
</Module>
```

Table 20 mwfm.xml TMPCModule

```
<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>
```

Table 21 mwfm.xml TMPCModuleRMIAccess Module

```
<Module>
    <Name>sosa_async_responser</Name>
    <Class-Name>com.hp.spain.engine.module.sosa.SosaAsyncResponserImpl</Class-Name>
    <Param name="errors_async_persistence_file" val-
ue="/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>
```

Table 22 mwfm.xml sosa_async_responser Module

Uncomment the existing authenticator module and `add teams_enabled` Param.

```
<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>
```

Table 23 mwfm.xml authenticator Module

3. Create the following folder and file:

```
mkdir /var/opt/OV/ServiceActivator/tmp/wftransactions

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

4. Edit the following file:

```
/etc/opt/OV/ServiceActivator/config/OpenStack.properties
```

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

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

3.3.2 SOSA configurations

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

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

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

If HPSA is using Oracle database:

```
<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=(PROTOCOL=TCP)(
HOST=#db_host)(PORT=#db_port)))(CONNECT_DATA=(SERVICE_NAME=#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>
```

Table 24 sosa.xml NfvManagerModule for Oracle

If HPSA uses Postgres database:

```
<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>
```

Table 25 sosa.xml NfvManagerModule for PPAS

2. 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

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

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

Table 27 sosa.xml sosaModule

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

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

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

```
<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>
```

Table 28 sosa_conf.xml nfvd Queue

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

```
<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>
```

Table 29 sosa_conf.xml basic Queue

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

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

Table 30 sosa_conf.xml NFVD_SA_EXECUTOR

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

```
<ProtocolAdapter class-
Name="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>
```

Table 31 sosa_conf.xml NGWSProtocolAdapter

```
<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>
```

Table 32 sosa_conf.xml ProtocolAdapterRest

Change the following values in `sosa_conf.xml`:

```
<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>
```

Table 33 sosa_conf MWFM_SA_EXECUTOR

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>`

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

```
<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>
```

Table 34 sosa_conf.xml PerformanceStatusManager configuration

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

5. 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`

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

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

Table 35 alias.xml reportmodule

3.3.3 NFVD Fulfillment specific configurations

Edit the following configuration in `nfv_manager.xml` file

Operating System	Path

Linux	`/etc/opt/OV/ServiceActivator/config/nfv_manager.xml`

```
<?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>
                <parame-
ter><name>RedoLogOutputDirectory</name><value>#BI_files_path</value></parameter>
                <parame-
ter><name>RedoLogSaveTimeoutThreshold</name><value>60000</value></parameter>
                <parame-
ter><name>RedoLogSaveCommitSizeThreshold</name><value>1</value></parameter>
                <parame-
ter><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>
                <parame-
ter><name>SOSAFwdUserId</name><value>#assurance_userid</value></parameter>
                <parameter><name>SOSAFwdSaveTimeoutThreshold</name><value>0</value></parameter>
                <parame-
ter><name>SOSAFwdSaveCommitSizeThreshold</name><value>1</value></parameter>
          </parameters>
        </persistence>
      </local>
      <remote>
        <node onError="DISCARD">
          <url>str1234</url>
        </node>
      </remote>
    </configurationType>
  </defaultConfiguration>
</Configuration>
```

Table 36 nfv_manager.xml

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
#assurance_port	NFVD-Assurance notifications WS port. This is the port where NFVD Assurance Gateway JBoss Admin console is listening
#assurance_user	NFVD-Assurance user. Currently not used
#assurance_userid	NFVD-Assurance userid. Currently not used

Table 37 nfv_manager.xml parameters

3.3.4 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

Table 38 Commands to deploy NFVD map

Where:

Variable	Description
#db_user	HPA Database Username
#db _password	HPSA Database clear text 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 39 NFVD Map parameters

3.4 Starting and stopping the NFVD Fulfillment and Extension Pack

3.4.1 Start NFVD Fulfillment

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

3.4.2 Stop NFVD Fulfillment

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

3.4.3 Start/Stop SOSA

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

3.4.4 Start/Stop LockManager

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

3.4.5 Start/Stop ECP

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

3.5 Starting protocol adapters and queues

Once the product is configured, the following actions must be taken.

3.5.1 Start NFVD Fulfillment HPSA and extension pack

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

3.5.2 Enable protocol adapter and queues

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

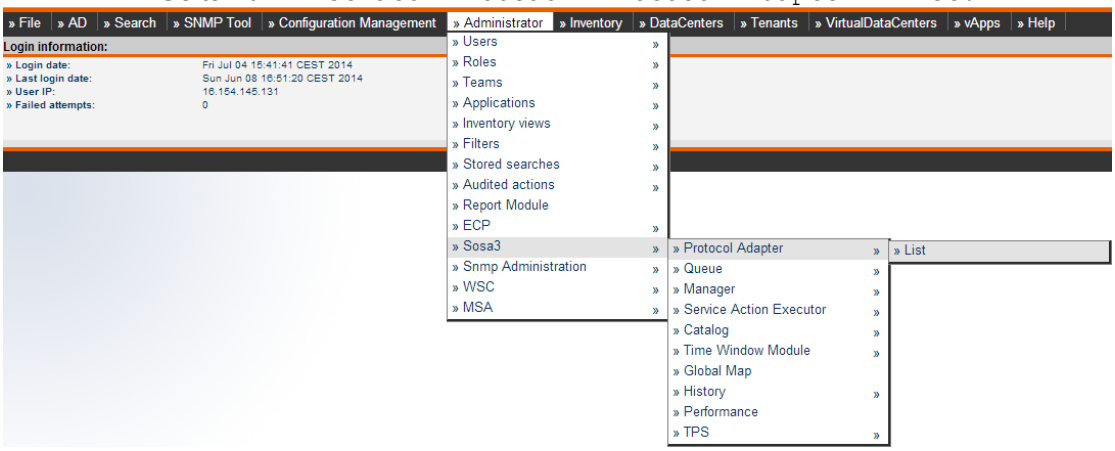


Figure 9 SOSA > Protocol Adapter > List

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

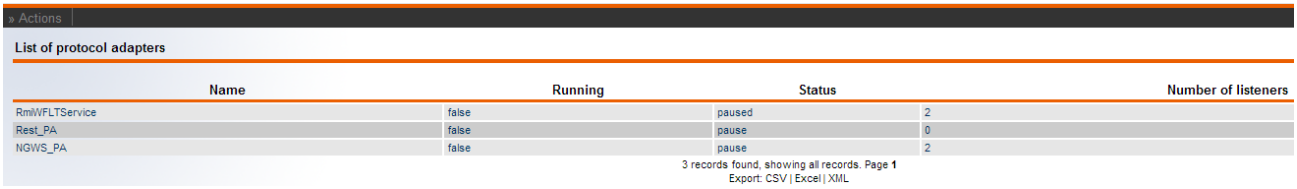


Figure 10 SOSA > Protocol Adapter Status

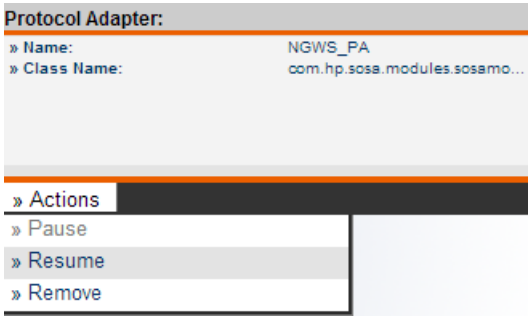


Figure 11 Protocol Adapter Resume Action

- Select `Administrator` → `Sosa3` → `Queue` → `List`.

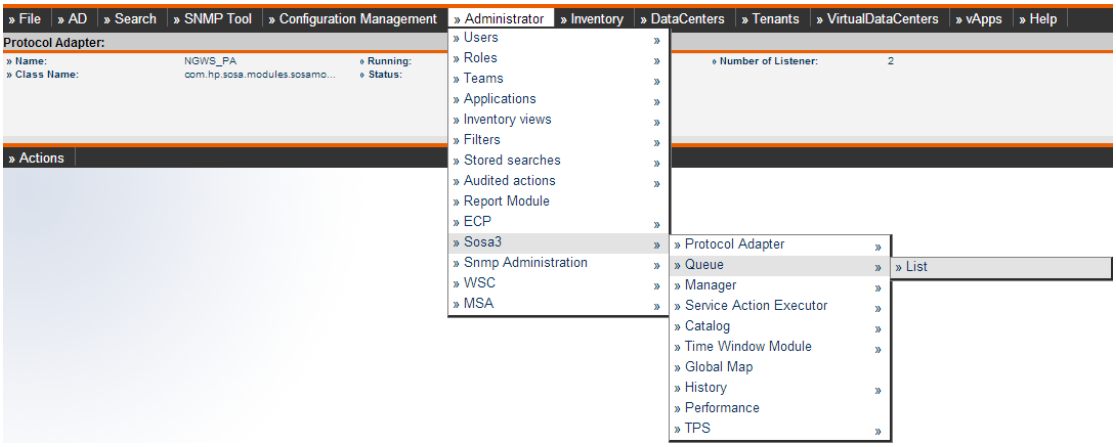


Figure 12 SOSA > Queue > List

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

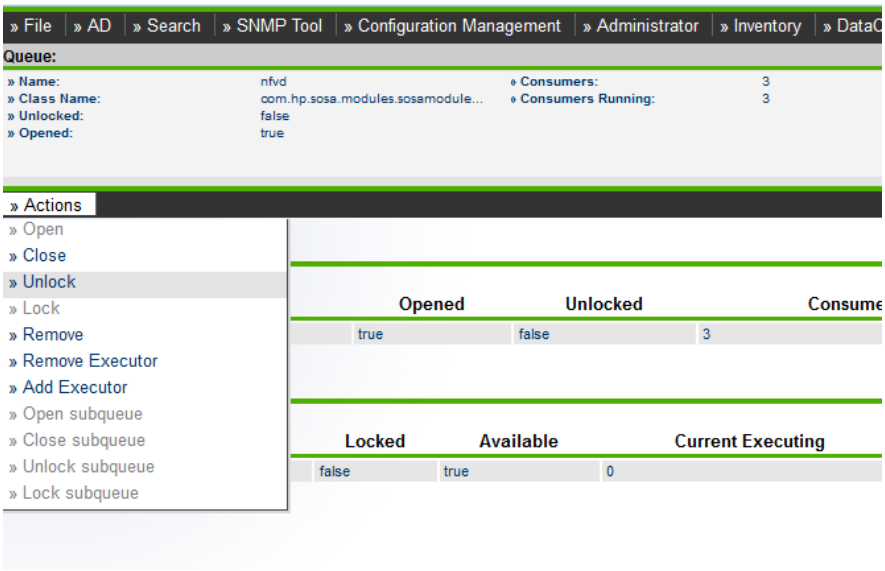
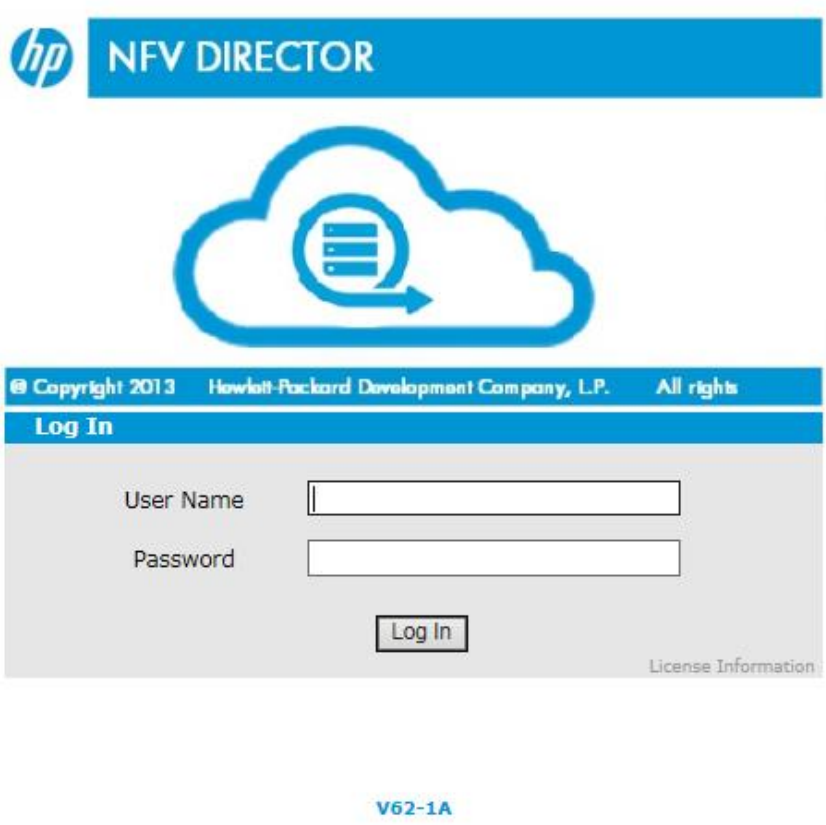


Figure 13 Queue Unlock

3.5.3 Load artifact definitions

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

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



V62-1A

Figure 14 NFVD Fulfillment Login

- Open the NFVModel/NFVDView Inventory Tree View.

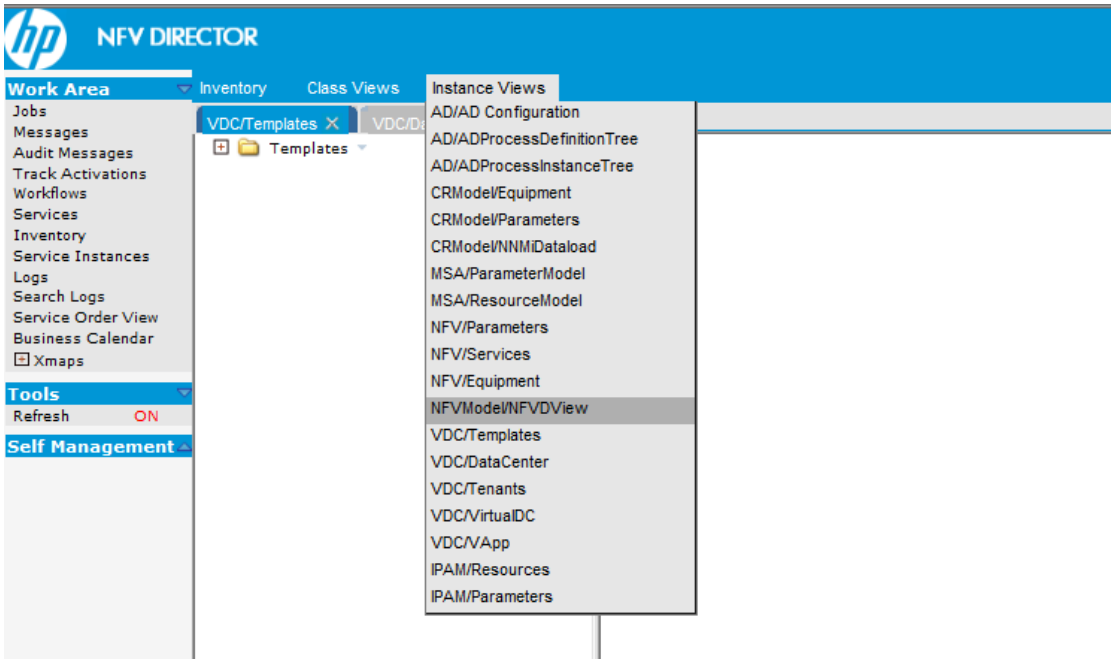


Figure 15 NFVD Fulfillment Inventory List

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

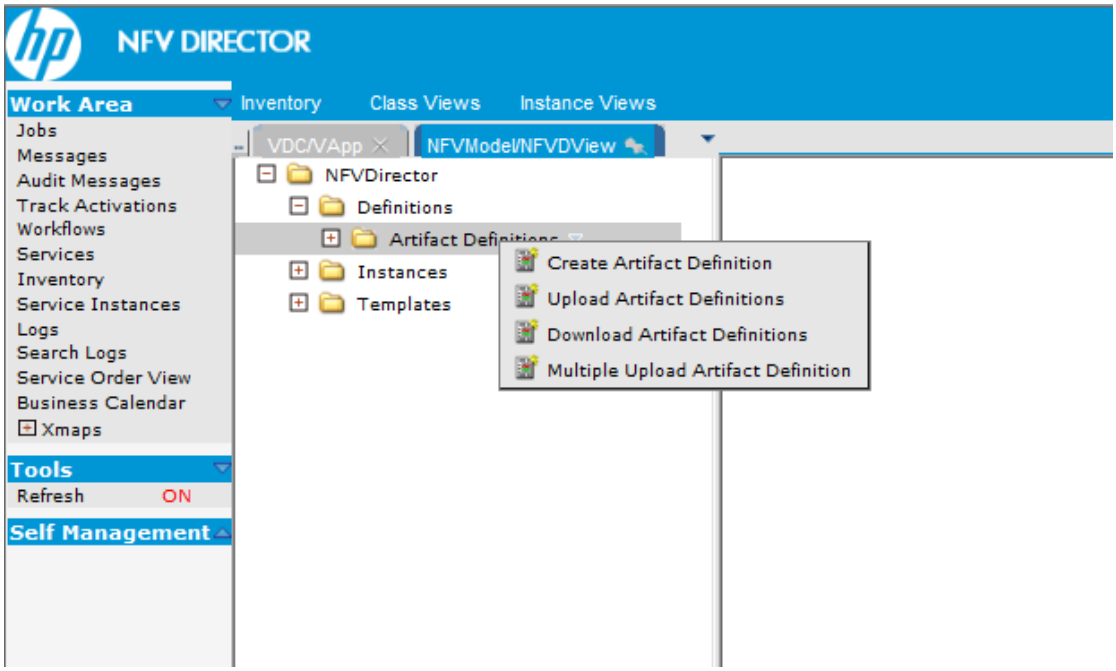


Figure 16 Multiple Upload Artifact Definition

- Click `Browse` and select all artifact definitions in:

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

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.

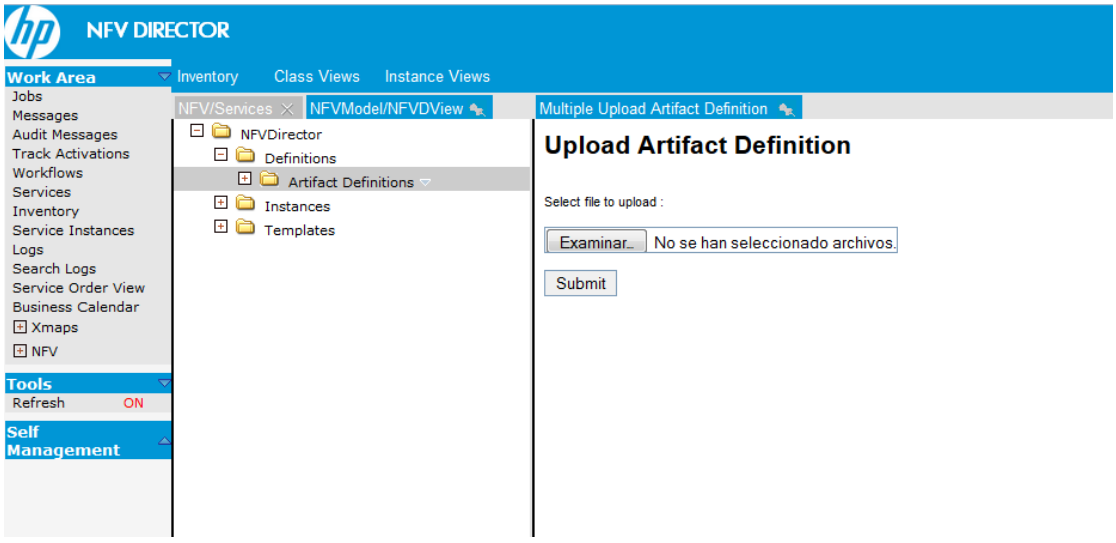


Figure 17 Select Artifact Definitions

- Click `Submit`.

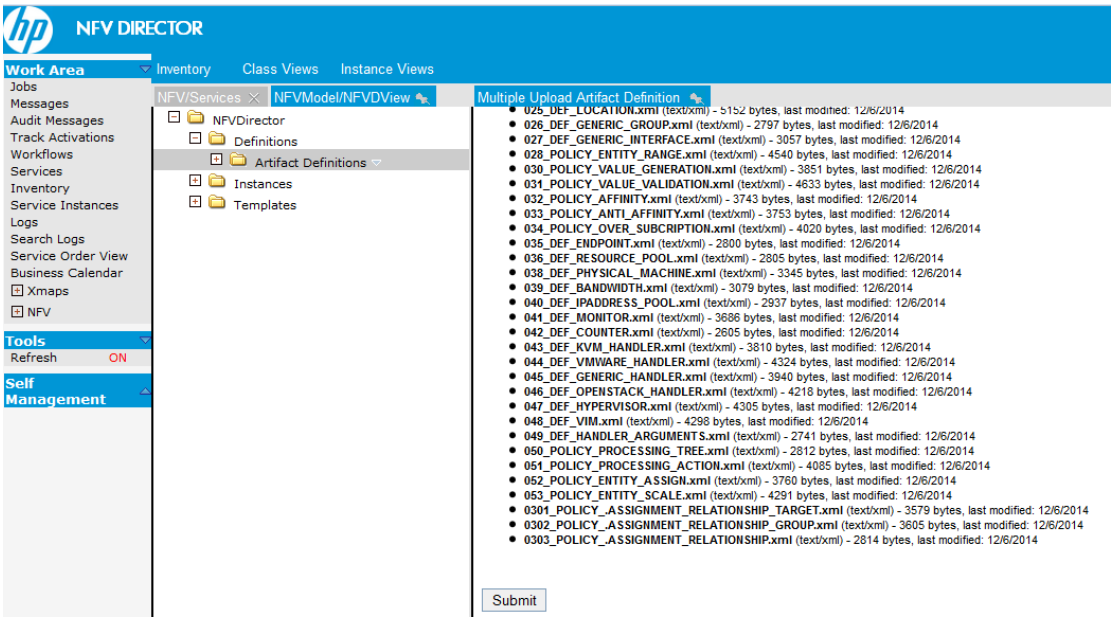


Figure 18 Upload Selected Artifact Definitions

- Repeat the same process for the following files:

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

3.5.4 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:

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

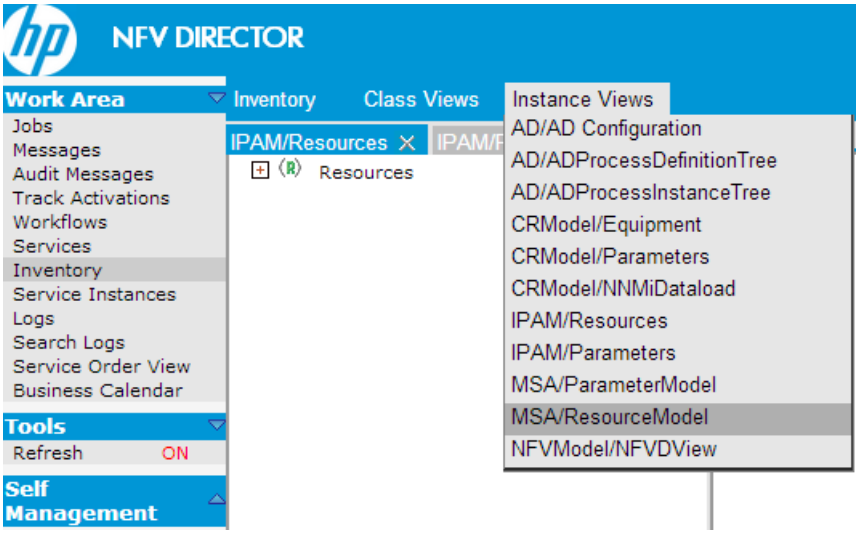


Figure 19 MSA Resource Model Inventory Model

- 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

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

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

- Set `timeout` to `600000`.

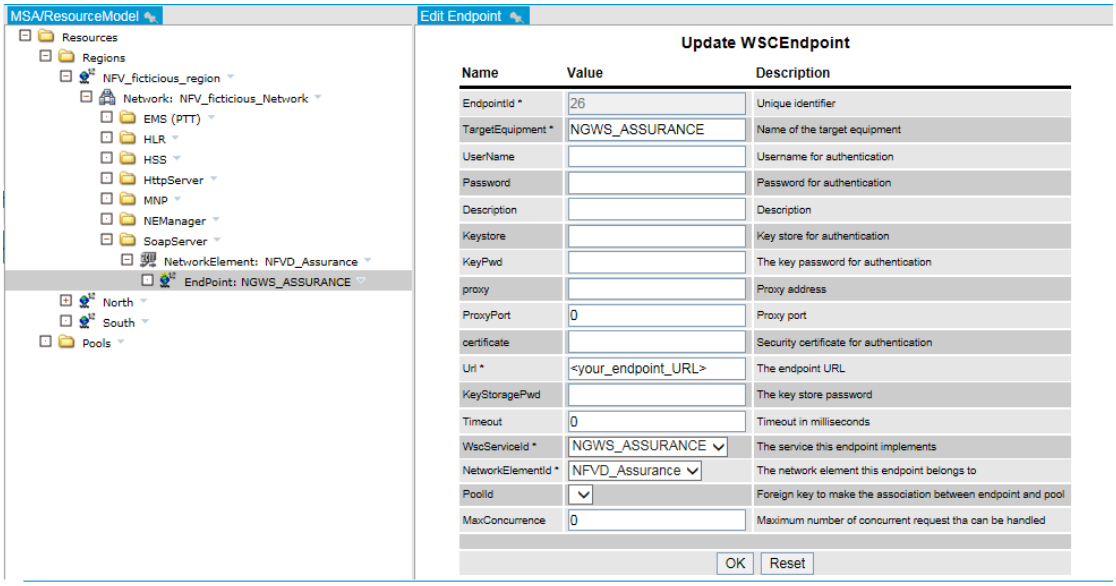


Figure 20 Edit NGWS_Assurance URL and timeout

3.6 Installing the NFVD Assurance base products

The following table summarizes the various ports used by the different components in NFVD Assurance. You may want to keep it handy and write down the details during deployment for future reference. Note that the below ports are mentioned only for illustration.

Product	Component	Example Port	URL
Sitescope	SiteScope User Inter-face	8088	http://<host or IP>:<Port>/SiteScope. Run /opt/HP/SiteScope/bin/config_tool.sh to change ports.
	Tomcat shutdown	28005	
	Tomcat AJP connector	28009	
	JMX console port	28006	
	Classic user interface	8888	
	Classic user interface (secure)		
	SSL port	8443	
UCA EBC Server	UCA-EBC JMS Broker port	61666	
	UCA-EBC JMX RMI port	1100	
	UCA GUI port	8090	http://<host or IP>:<Port>/#EXPERT:APPLICATION:MONITORING

UCA-EBC Topology Extension	Neo4J Rest http/GUI http	7474	http://<host or IP>:<Port>/webadmin
	Neo4J backup port	6362	
HPSA	Workflow Manager port	2000	
	Resource Manager port	9223	
	System DB listener port	1521/5444	1521 for Oracle/5444 for PPAS
	Web Server port	9090	http://<host or IP>:<port>/ activator/jsp/login.jsp
UCA Automation	Jetty Server hosting UI	9080	http://<host or IP>:<port>/ UCAAutomation
	Shutdown Jetty server	8079	
UCA Autoconsole CA	UCA automation port	12500	
	UCA Console port	9080	Same as UCA Automation "Jetty Server hosting UI" port
UCA EBC CA	UCA EBC JMS broker port	61666	
	Action Service port	26700	
UCA HPSA CA	HPSA UCA Automation Sync Service port	8191	
Generic SNMP CA	SNMP trap receiver	162	
JBoss NFVD Assurance	JBoss HTTP connection	18080	http://<host or IP>:<Port>
	JBoss AS remoting	9999	
	JBoss AS remoting	4447	
	JBoss AS Management Admin console	9990	Management access: <User> / <Password>

Table 40 NFVD Assurance ports

NOTE : Both HPSA and NFVD Assurance run on JBoss. To avoid port conflict with HPSA JBoss, if deployed on the same server, NFVD Assurance ports are reconfigured in the `/opt/HP/nfvd/bin/nfvd_agw_env.sh`.

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.

Product	Start	Stop	Remark
Sitescope	/opt/HP/SiteScope/start	/opt/HP/SiteScope/stop	Path: /opt/HP/Sitescope
UCA EBC Server	/opt/UCA-EBC/bin/uca-ebc start	/opt/UCA-EBC/bin/uca-ebc stop	Run the start/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
UCA Automation	/opt/UCA-ATM/bin/ucautomation-ui start	/opt/UCA-ATM/bin/ucautomation-ui stop	Path: /opt/UCA-ATM
NOM	/opt/openmediation-V62/bin/nom_admin --start-container –all	/opt/openmediation-V62/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

Table 41 NFVD Assurance start/stop scripts

3.6.1 HP UCA automation

NOTE: After installing HP UCA Automation V1.0, follow Chapter 3 of `UCA Automation Installation Guide`, and then install the UCA Automation mandatory patch EBCATMLIN_00001, and then proceed with deployment and configuration steps, by following the patch installation guide EBCATMLIN_00001.txt.

For HP UCA Automation V1.0 installation instructions, see the `HP UCA Automation V1.0 - Installation Guide V1.1.`

Installation of HP UCA Automation product involves the installation of products as listed in **Table 9 UCA Automation software**.

For UCA Automation patch EBCATMLIN_00001 installation, see the Patch Installation Guide EBCATMLIN_00001.txt

3.6.1.1 HP UCA Automation configuration for NFVD

Once HP UCA Automation solution and patch has been installed, configure the solution as follows to adapt to the NFVD solution:

1. Install the HP UCA Automation Foundation VP by placing the VP in the `/var/opt/UCA-EBC/instances/default/valuepacks` directory. In the UCA-EBC portal http:// <#UCA EBC Server host>:<#UCA GUI Port>/#EXPERT:APPLICATION:MONITORING, login as admin or admin operator to view the list of VPs.

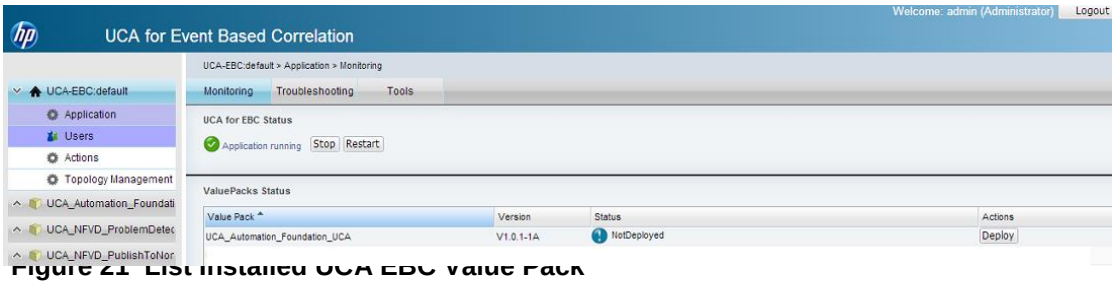


Figure 21 List installed UCA EBC Value Pack

2. Deploy the HP UCA Automation Foundation VP, by clicking the `Deploy` button.

Figure 22 List Deployed UCA EBC Value Pack

3. Select `UCA_Automation_Foundation_UCA-V1.0.1-1A` → `Value Pack` → `Configuration` option. It lists the Standard Configuration as follows:

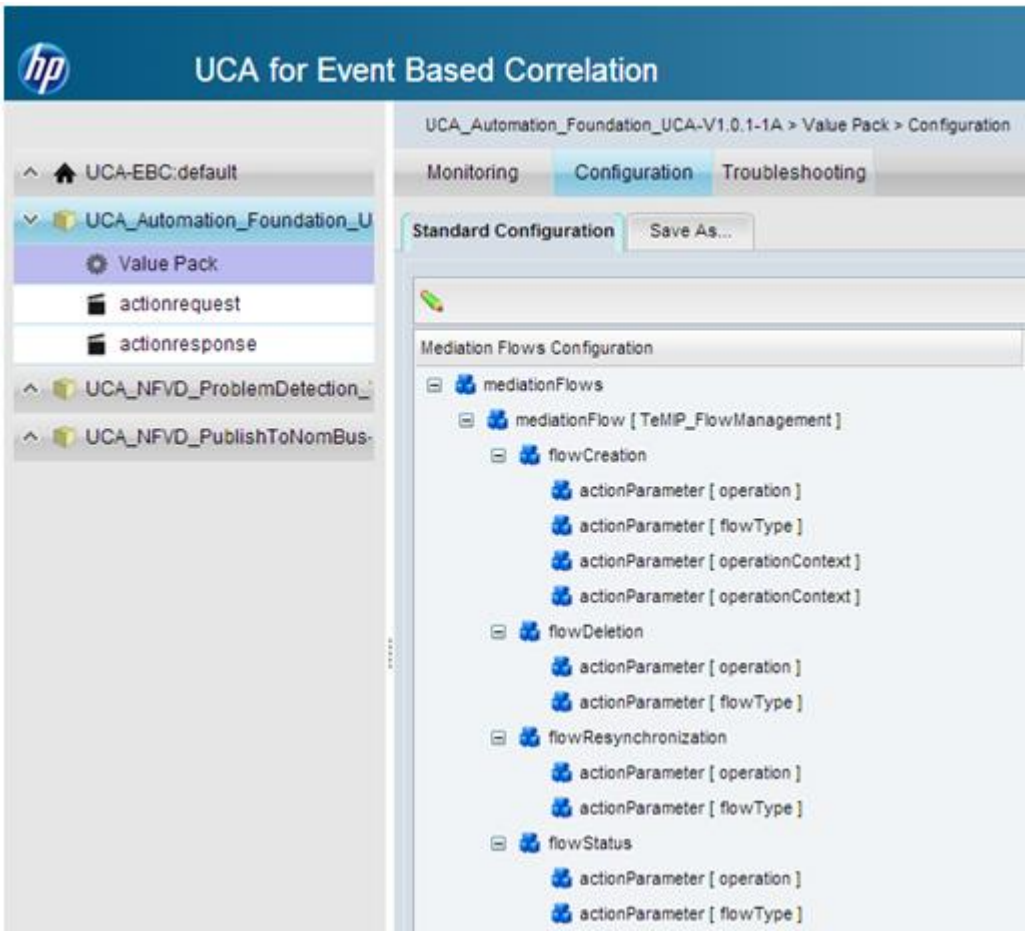


Figure 23 UCA EBC –TeMIP mediationFlow

4. Select the `tree mediation Flows` → `mediationFlow [TeMIP_FlowManagement]`. Choose the `Edit` option, and click `Delete` to delete this mediationFlow.

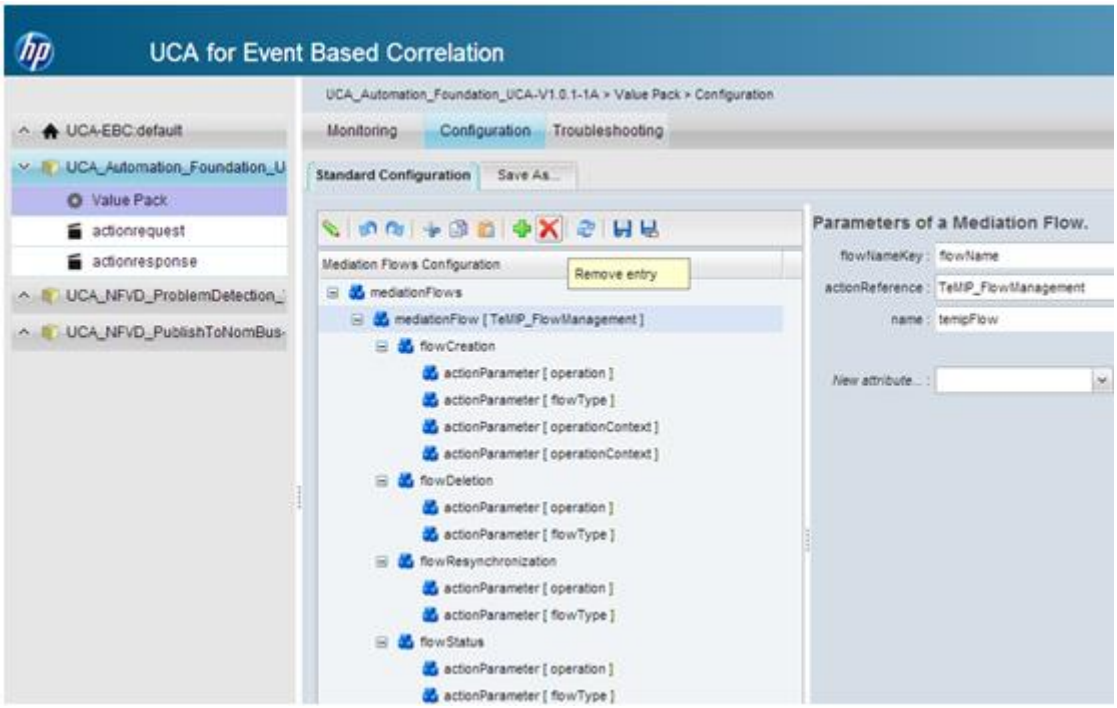


Figure 24 UCA EBC Remove TeMIP mediationFlow

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

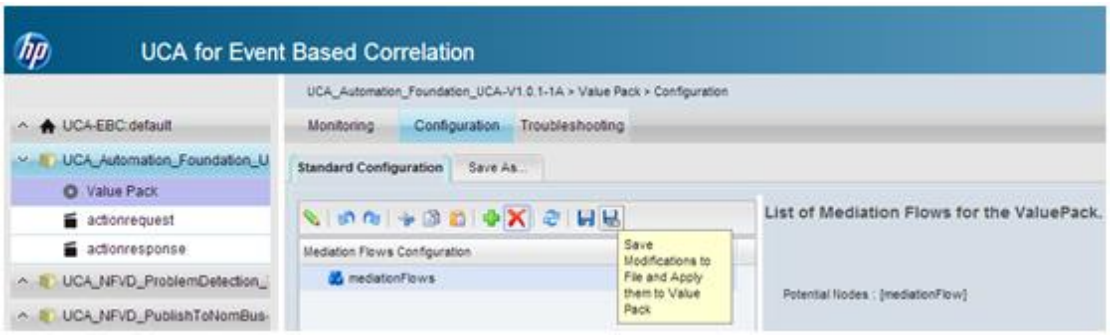


Figure 25 UCA EBC save modification

6. Now, select `UCA_Automation_Foundation_UCA-V1.0.1-1A` → `Action-request` → `Filter Configuration` option. Choose the `filters` → `topFilter [Foundation]` → `allCondition`.

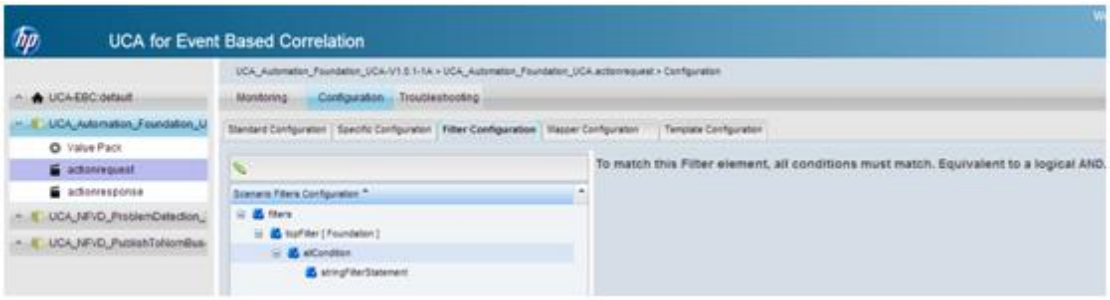


Figure 26 UCA EBC UCA Automation Foundation VP filter

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

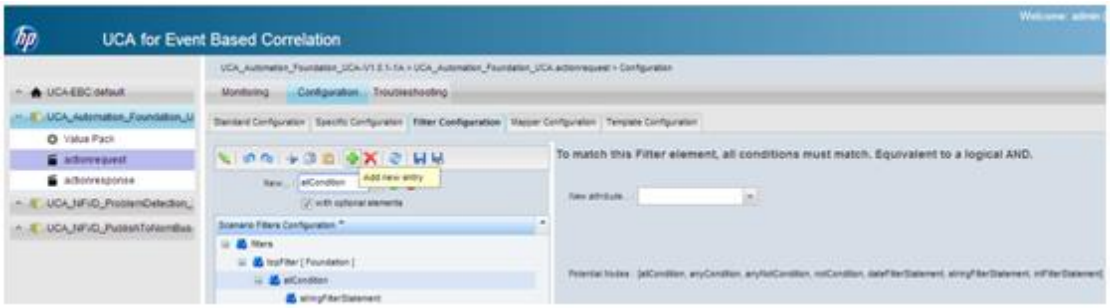


Figure 27 UCA EBC add new filter

8. Select `notCondition` from the drop box, set the radio button for `with optional element`, and click the `Create Entry` button.

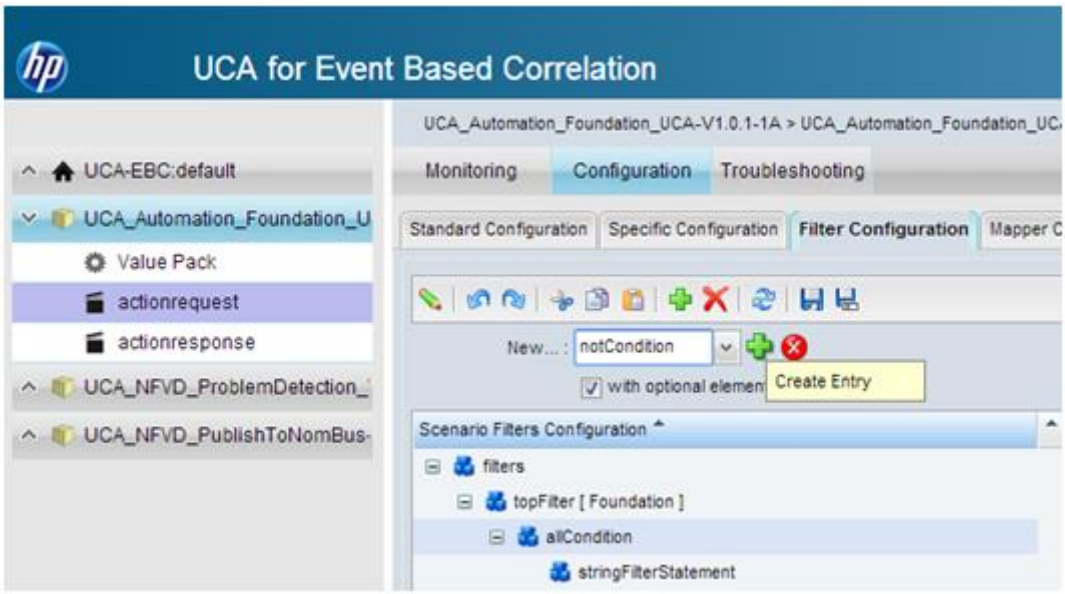


Figure 28 UCA EBC filter create condition

9. Clicking the `Create Entry` button generates three statements under the `notCondition`. They are `dateFilterStatement`, `intFilterStatement` and `stringFilterStatement`.

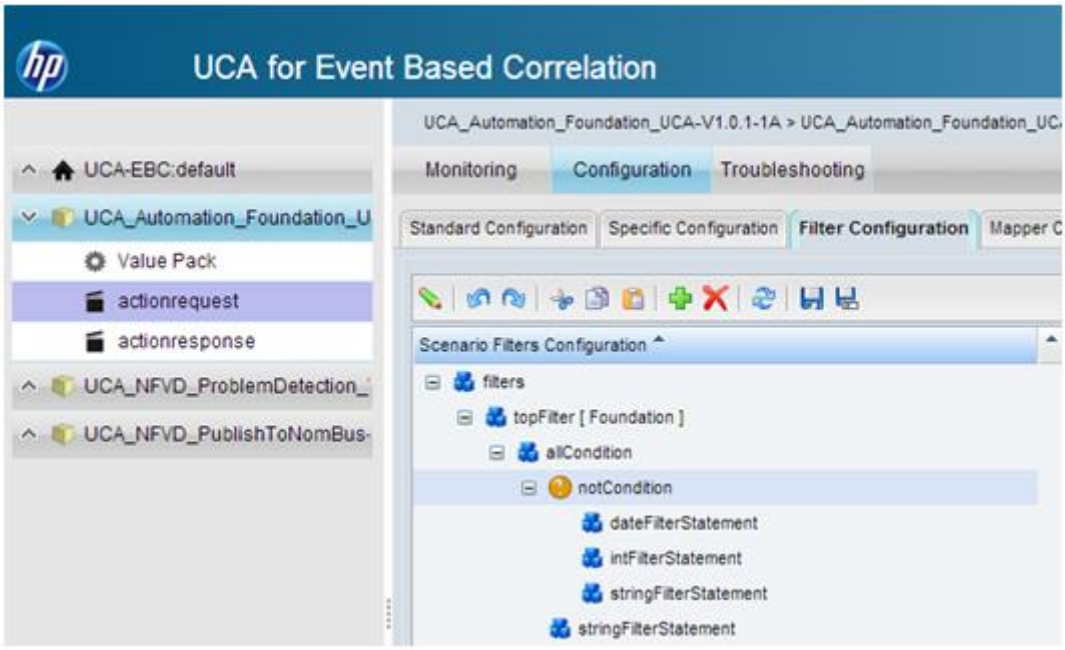


Figure 29 UCA EBC create entry under notCondition

10. Select the `dateFilterStatement` and the `intFilterStatement` and remove them.

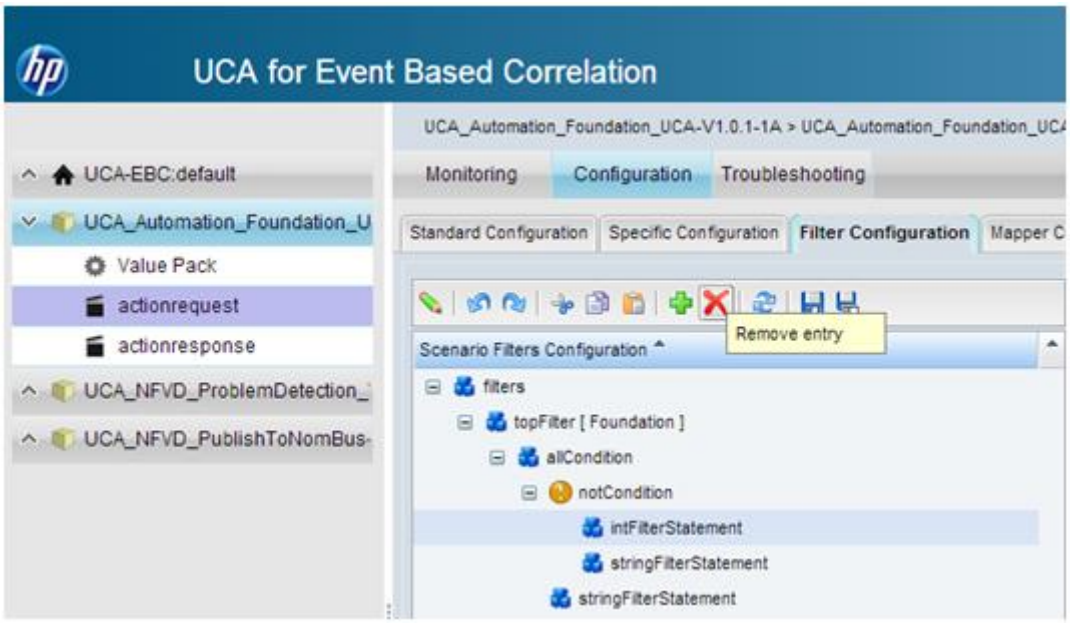


Figure 30 UCA EBC remove unnecessary conditions

11. For the stringFilterStatement, select the `fieldname` as `additionalText`, `operator` as `contains` and key in `fieldValue` as `Publish-VP`.

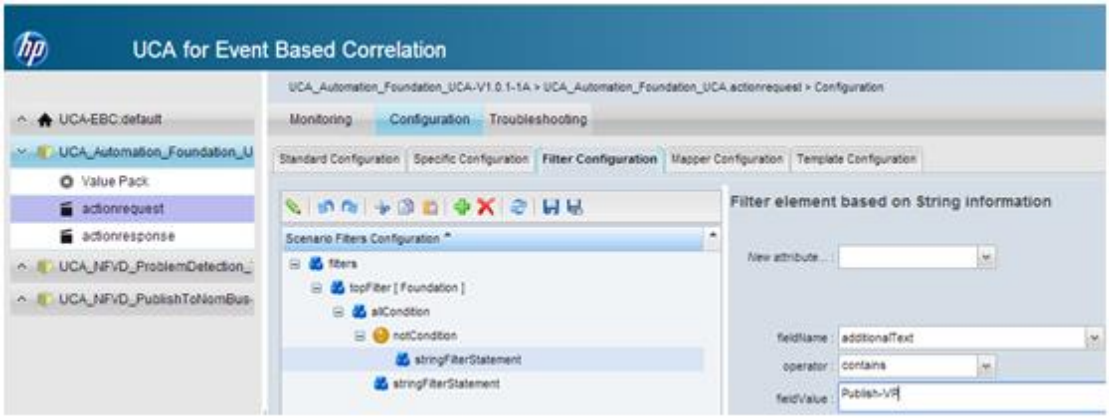


Figure 31 UCA EBC additionalText filter

12. Click `Save Modifications` to File and Apply them to Value Pack.

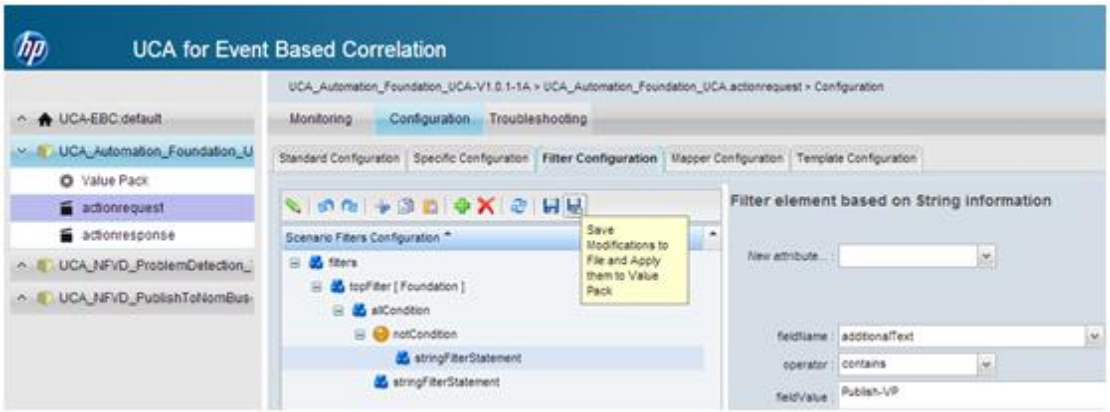


Figure 32 UCA EBC Save filter

13. Start the UCA Automation Foundation Value Pack.

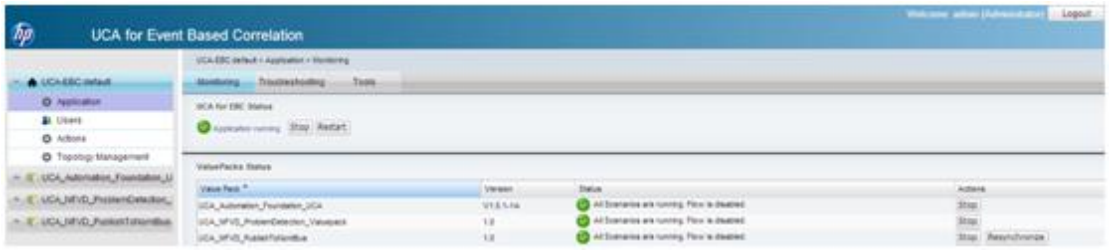


Figure 33 UCA EBC start Value Pack

3.6.1.2 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:

```
<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>
```

3.6.2 Generic SNMP channel adapter

For Generic SNMP Channel Adapter installation instructions, see `NOM Installation and Configuration Guide` and `Generic SNMP CA Installation Guide Version V100L01.`

3.6.2.1 Generic SNMP CA SiteScope customization

For Generic SNMP Channel Adapter SiteScope Customization installation, see `Open Mediation HP SiteScope Customization for Generic SNMP CA Installation and Configuration Guide Version V100L01.`

3.6.2.2 Generic SNMP CA VMware ESXi customization

For Generic SNMP Channel Adapter VMware ESXi Customization installation, see `Open Mediation HP VMware ESXi Customization for Generic SNMP CA Installation and Configuration Guide Version V100L01.`

All the installed packages in NOM are listed as follows:

```
# ./nom_admin --list-ip
INSTALLED       generic-snmp-ca-V10
INSTALLED       nom-basic-smx-components
INSTALLED       nom-basic-smx-components-sdk
INSTALLED       nom-sdk
INSTALLED       smx-basic-components
INSTALLED       smx-extra-components
INSTALLED       snmp-customization-sitescope-V10
INSTALLED       snmp-customization-vmware-V10
INSTALLED       uca-autoconsole-ca-V10
INSTALLED       uca-ebc-ca-3.0
INSTALLED       uca-hpsa-ca-V10
```

Figure 34 List of Channel Adapters

3.6.3 HP SiteScope

For HP SiteScope 11.23 installation instructions, see `HP SiteScope Release Notes.`

Follow the HP SiteScope patch installation instructions to install the HP SiteScope patch.

NOTE: 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` OR install the `32-bit X11` libraries on the system. Example: `libX11-1.5.0-4.el6.i686`, `libX11-common-1.5.0-4.el6.noarch`.

3.7 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.

- Mount the ISO image `JK596-15001.iso`.
- Go to the `Binaries` directory to find the following NFVD Assurance specific RPM files:
  - `nfvd-assur-gw-base-01.00.000-1.el6.noarch.rpm`
  - `nfvd-assur-gw-tpp-01.00.000-1.el6.noarch.rpm`
  - `nfvd-assur-gw-core-01.00.000-1.el6.noarch.rpm`
  - `nfvd-correlation-01.00.000-1.el6.noarch.rpm`
  - `nfvd-monitors-01.00.000-1.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.

3.7.1 Installing assurance gateway scripts

The NFVD Assurance Gateway scripts are available as `nfvd-assur-gw-base-01.00.000-1.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-01.00.000-1.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-01.00.000-1.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-01.00.000-1.el6.noarch
```

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

3.7.2 NFVD Assurance third-party products

NFVD Assurance Third-Party Products is available as `nfvd-assur-gw-tpp-01.00.000-1.el6.noarch.rpm`.

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

1. Transfer the file `nfvd-assur-gw-tpp-01.00.000-1.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-01.00.000-1.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-base-01.00.000-1.el6.noarch
 nfvd-assur-gw-tpp-01.00.000-1.el6.noarch
```

3.7.3 Installing Assurance gateway core

The NFVD Assurance gateway is available as nfvd-assur-gw-core-01.00.000-1.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-01.00.000-1.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-01.00.000-1.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:

```
# rpm –-qa | grep nfvd
nfvd-assur-gw-base-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
```

NOTE: Both HPSA and NFVD Assurance run on JBoss. To avoid port conflict with HPSA JBoss, if deployed on the same server, NFVD Assurance ports in are reconfigured in the `/opt/HP/nfvd/bin/nfvd_agw_env.sh`.
If you wish to change the NFVD Assurance ports, edit the `/opt/HP/nfvd/bin/nfvd_agw_env.sh`, and restart the NFVD Assurance gateway application.

```
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
```

3.7.3.1 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/topology.properties`

```
# The Neo4J Db connection protocol
neo4j.protocol=http
# Specify the HTTP server port and host supporting data, administrative, and UI access
neo4j.host=localhost
neo4j.port=7474

# For Neo4J data retrievals
neo4j.db=db
neo4j.data=data

# Used for Junit
neo4j.host.test=localhost
neo4j.port.test=17373
```

Figure 35 topology.properties

Update the neo4j.host, neo4j.port attribute values in the topology.properties to reflect the Neo4J graph DB host and port respectively.

3.7.3.2 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. On start up, Assurance gateway reads the parameters in the file: `/var/opt/HP/nfvd/conf/fulfillment.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.

1. Modify the value set at `RESYNC_AT_STARTUP` to `true` to resynchronize at start up.
2. Modify the value `127.0.0.1` set in the `FULFILLMENT_URL` to point to NFVD Fulfillment system.
3. Modify the value `FULFILLMENT_CONNECTION_TIMEOUT`, to set the connection time limit for the given fulfillment URL (value in milliseconds).
4. Modify the value `FULFILLMENT_RESPONSE_TIMEOUT`, to set the web response time limit for the configured fulfillment URL (value in milliseconds).

```
# Configure RESYNC_AT_STARTUP as true/yes, for synchronization during Assurance startup
RESYNC_AT_STARTUP=false
# Provide the fulfillment URL to sync the data
FULFILLMENT_URL=http://127.0.0.1:8071/ngws/service?wsdl
# 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
```

Figure 36 fulfillment.properties

Resync operation can be performed manually as well. Set the `RESYNCH_AT_STARTUP` value to `false`.

For details, see the HP NFV Director User Guide 1.1.

3.7.4 Installing UCA automation NFVD packs

The UCA Automation NFVD correlation value packs (UCA-EBC) and domain solution packs (HPSA) is available as `nfvd-correlation-01.00.000-1.el6.noarch.rpm` RPM file.

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

- Transfer the file `nfvd-correlation-01.00.000-1.el6.noarch.rpm` to a RHEL system, and place it under a directory:

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

  `# rpm -ivh nfvd-correlation-01.00.000-1.el6.noarch.rpm`

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

```
# rpm –-qa | grep –i nfvd

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

- Go to the directory `/opt/HP/nfvd/correlation`.
  There is one HPSA NFVD domain Solution Pack, and two UCA for EBC Value Packs in the directory.

  - `UCA_AUTOMATION_HPSA_NFVD_VP-V10-1A.zip`
  - `UCA_NFVD_ProblemDetection_Valuepack-vp-1.0.zip`
  - `UCA_NFVD_PublishToNomBus-vp-1.0.zip`

3.7.4.1 Installing UCA Automation NFVD HPSA SP

- Copy the `UCA_AUTOMATION_HPSA_NFVD_VP-V10-1A.zip` to `/opt/OV/ServiceActivator/SolutionPacks`.
- Import the Solution Pack using the `HPSA deploymentmanager` tool. It can be verified by checking that the directory `NFVD` has been created in `/opt/OV/ServiceActivator/solutions` directory.
- It creates NFVD solution under `/opt/OV/ServiceActivator/solutions` directory.
- Deploy the Solution Pack using the `HPSA deploymentmanager` tool.

Once the UCA Automation HPSA Solution Packs for NFVD are deployed, we get the following Inventory views in the HPSA inventory.

Figure 37 UCA Automation HPSA Inventory View

- Open the `UCA/Parameters → Parameters → Workflow` templates to view the workflow being invoked for the identified NFVD Action.
  When the UCA Automation Console invokes the UCA Automation HPSA via the NOM bus, the requests are made to the workflow listed in the file `/var/opt/openmediation-V62/containers/instance-0/ips/uca-hpsa-ca-V10/etc/config.properties → hpsa.controller.workflow.name` attribute. It is `UCAController` in this case.
  `UCAController` workflow in turn calls the workflow as configured in the `UCA/Parameters → Workflow` templates for each action. It is fixed as `NFVD_Controller` in this case.

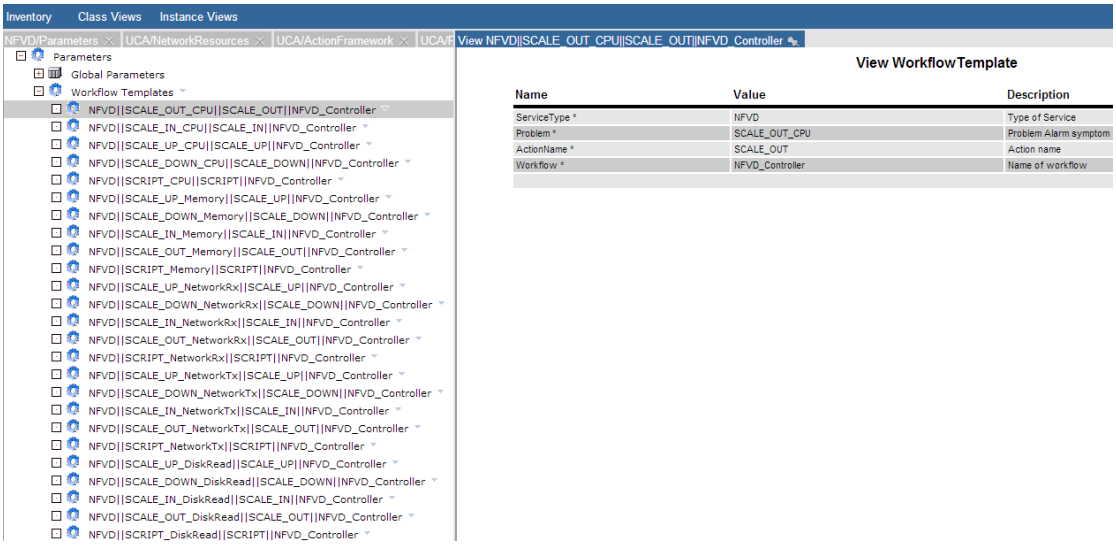


Figure 38 UCA Automation HPSA – UCA/Parameters > Workflow

- Open the `UCA/ActionFramework → Diagnostics Actions Framework → Problems` to view the mapping between Problem and NFVD Action.

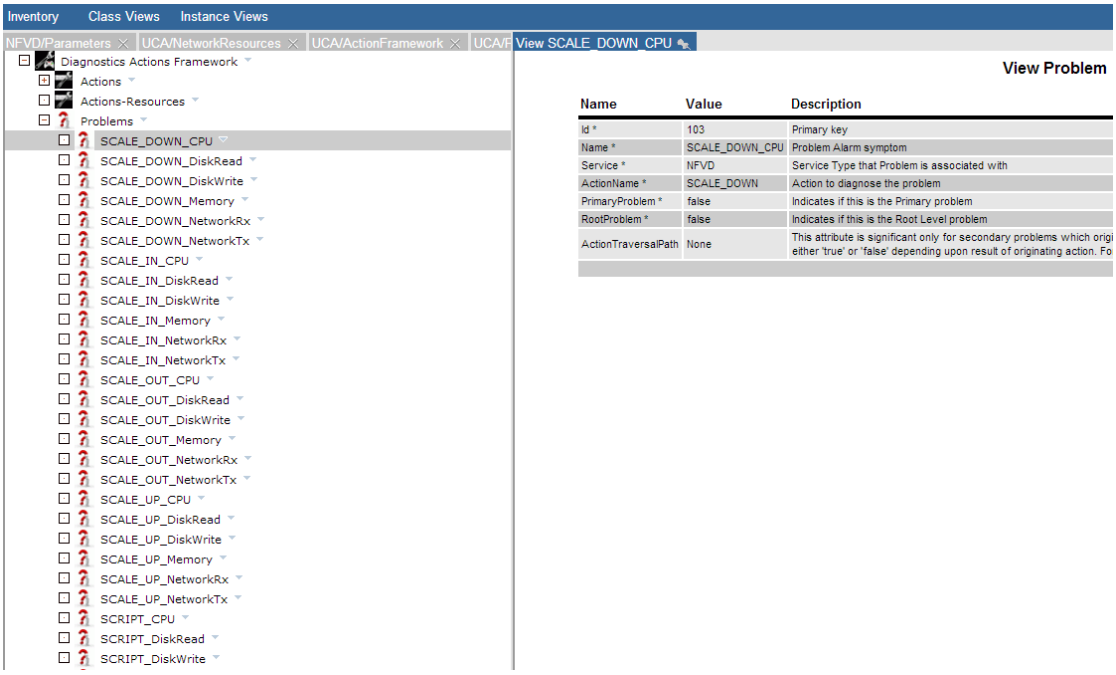


Figure 39 View UCA/ActionFramework > Diagnostics Actions Framework > Problems

- Open the `UCA/ActionFramework → Diagnostics Actions Framework → Actions` to see list of NFVD Actions.

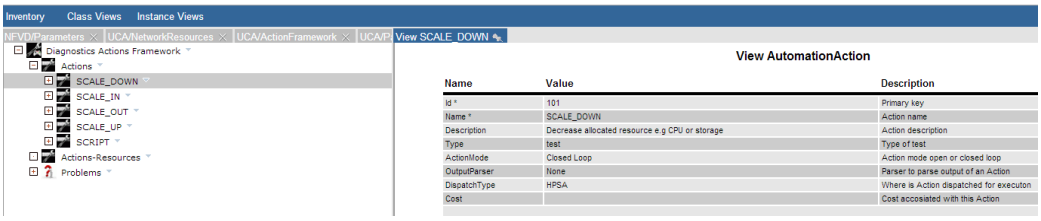


Figure 40 View UCA/ActionFramework > Diagnostics Actions Framework > Actions

The workflow `NFVD_Controller` calls the child workflow as listed in the `NFVD/Parameters → Parameters → Workflow templates` for each Action. These workflows make appropriate NBI call to NFVD Fulfillment solution based on the type of action, as shown in the following two scenarios.

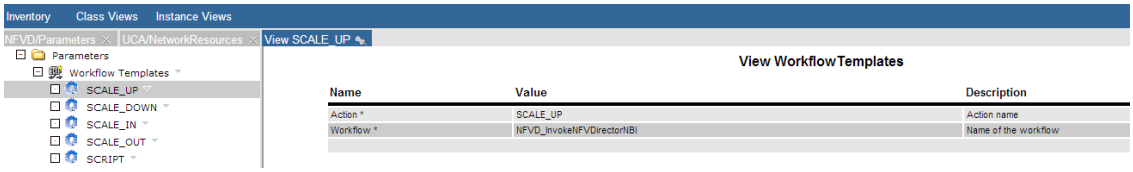


Figure 41 NFVD/Parameters > Parameters > Workflow templates with NBI action

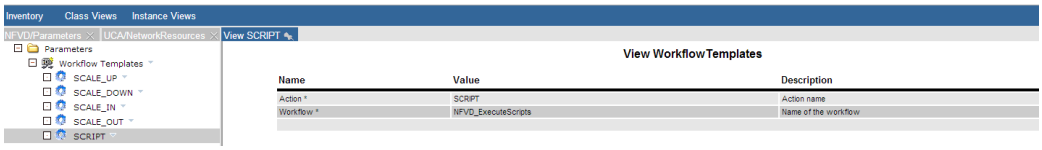


Figure 42 NFVD/Parameters > Parameters > Workflow templates with Script action

- The workflows `NFVD_InvokeNFVDirectorNBI` and `NFVD_ExecuteScripts` make use of the `${ACTIVA-TOR_OPT}/solutions/NFVD/etc/config/nfvd_config.properties` to invoke the NFVD Fulfillment webservice calls to request for VM operations.
- Modify only 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://<#NFVD Fulfillment Server>: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
```

3.7.4.2 Installing UCA automation NFVD UCA for EBC value packs

Note: See HP UCA Automation configuration for NFVD for UCA for EBC GUI options to deploy and start Value Packs. The following description explains the command line options.

1. Install the Value Packs.

   Copy the two UCA for EBC value packs `UCA_NFVD_ProblemDetection_Valuepack-vp-1.0.zip` and `UCA_NFVD_PublishToNomBus-vp-1.0.zip` to `${UCA_EBC_INSTANCE}/valuepacks` directory on the UCA for EBC system.

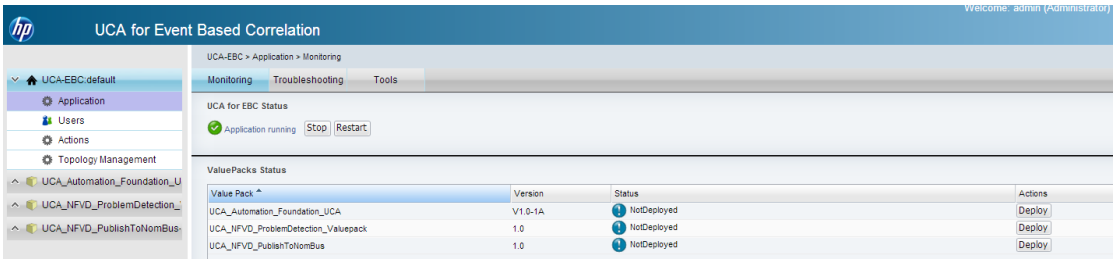


Figure 44 UCA EBC Install Value packs

2. Deploy the Value Packs.

   Deploy the Value Packs listed above into the `${UCA_EBC_INSTANCE}/deploy` directory using `uca-ebc-admin` administration tool.
   As UCA user, deploy the two Value Packs.

```
# cd /var/opt/UCA-EBC/instances/default/valuepacks/
# ls
UCA_Automation_Foundation_UCA-vp-V1.0-1A.zip  UCA_NFVD_ProblemDetection_Valuepack-vp-1.0.zip  UCA_NFVD_PublishToNomBus-vp-1.0.zip
# su - uca
$ cd /opt/UCA-EBC/bin/
$ ./uca-ebc-admin --deploy -vpn UCA_NFVD_ProblemDetection_Valuepack -vpv 1.0
INFO  - Value Pack name: UCA_NFVD_ProblemDetection_Valuepack-1.0 has been successfully deployed
$ ./uca-ebc-admin --deploy -vpn UCA_NFVD_PublishToNomBus -vpv 1.0
INFO  - Value Pack name: UCA_NFVD_PublishToNomBus-1.0 has been successfully deployed
```

Figure 45 UCA EBC Deploy Value Packs

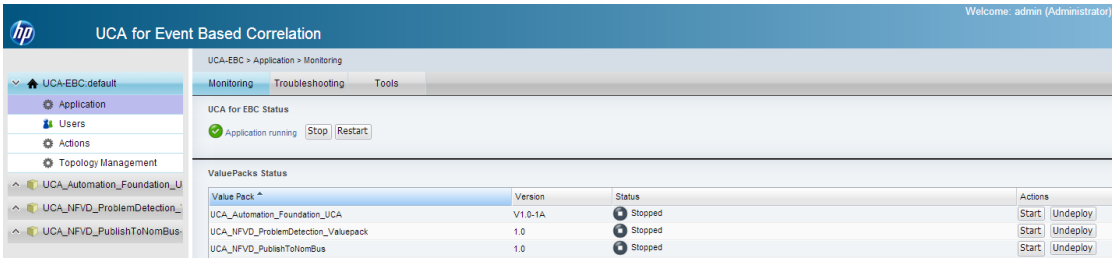


Figure 46 UCA EBC List Value packs

3. Start the Value Packs.

   If UCA for EBC is stopped, restarting UCA for EBC will load all value packs deployed in the `${UCA_EBC_INSTANCE}/deploy` folder.
   If UCA for EBC is running, use `uca-ebc-admin` option to start the VPs.

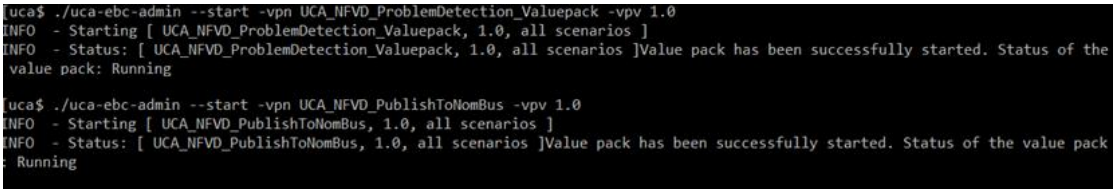


Figure 47 UCA EBC Start Value Packs

3.7.5 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-01.00.000-1.el6.noarch.rpm RPM file.

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

1. Transfer the file `nfvd-monitors-01.00.000-1.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-01.00.000-1.el6.noarch.rpm
```

   This command:

   - Copies `config_tool_params.txt to /opt/HP/nfvd/templates`. Manually copy it to `<SITESCOPE_HOME>/examples/silent_config_tool` directory.
   - Copies SiteScope jars to `/opt/HP/nfvd/newconfig`. Manually copy them to `<SITESCOPE_HOME>/java/lib/ext` directory.

3. Verify if the package is successfully installed:

```
# rpm –-qa | grep –i nfvd
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
```

3.7.6 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.

3.7.6.1 Manual import

Take the following steps in order to perform manual import of SiteScope templates and configurations:

1. Login to Sitescope: http://<#SiteScope Host>:<SiteScope User Interface port>/SiteScope/servlet/Main.
2. Navigate to `Preferences → Infrastructure Preferences → General Settings` tab and check the `Accept untrusted SSL certificates` option if unchecked.

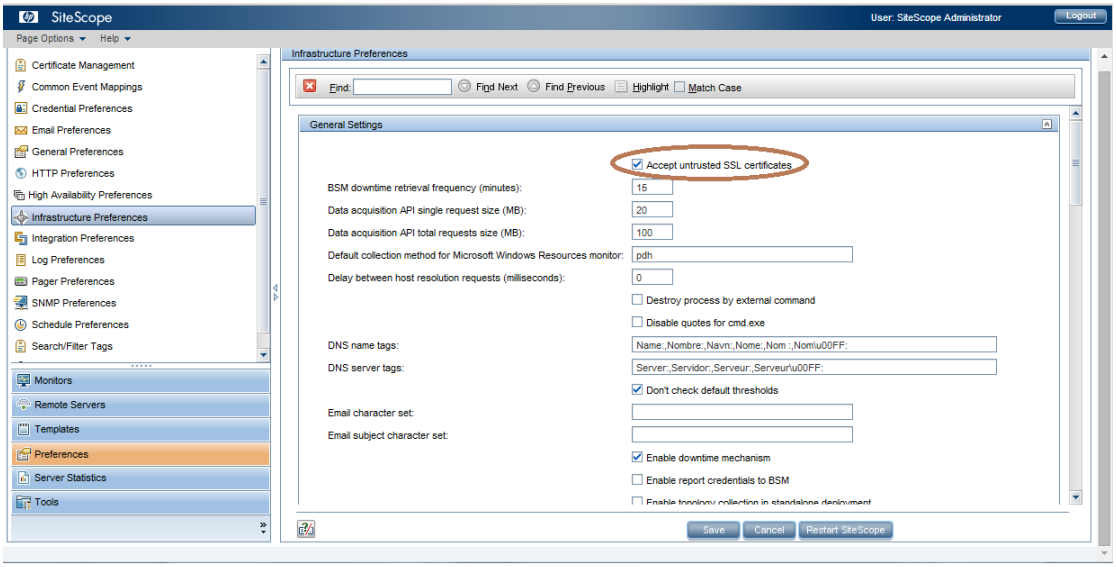


Figure 48 SiteScope > Infrastructure Preferences > General Settings

3. Navigate to `Preferences → Infrastructure Preferences → Custom Monitor Settings` tab and check the `Allow Network Access` and `Reload classes and jars on each monitor run` checkboxes.

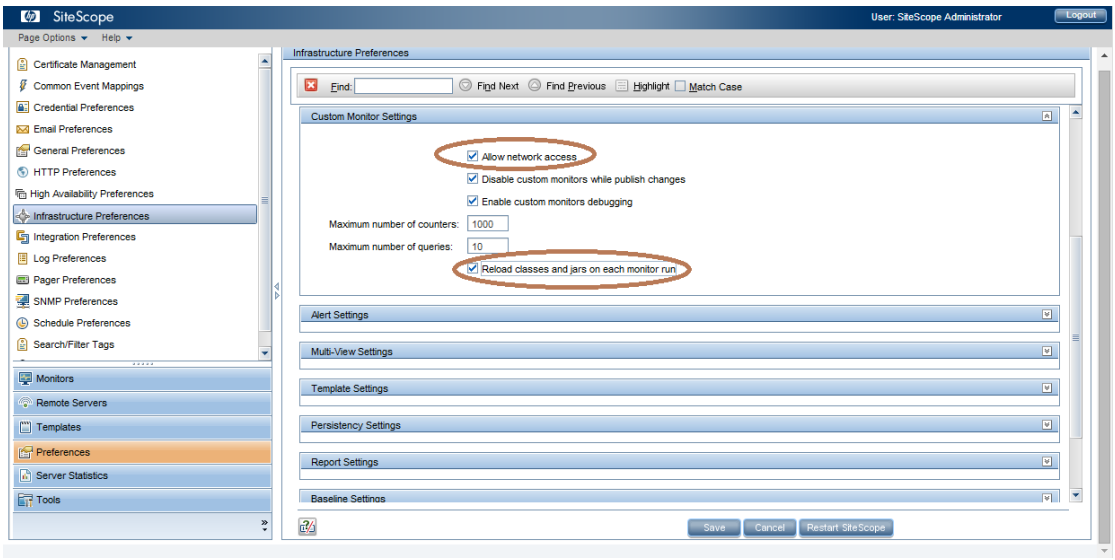


Figure 49 SiteScope > Infrastructure Preferences > Custom Monitor Settings

4. Save the configuration.
5. Navigate to `Preferences → SNMP Preferences` → Select New icon

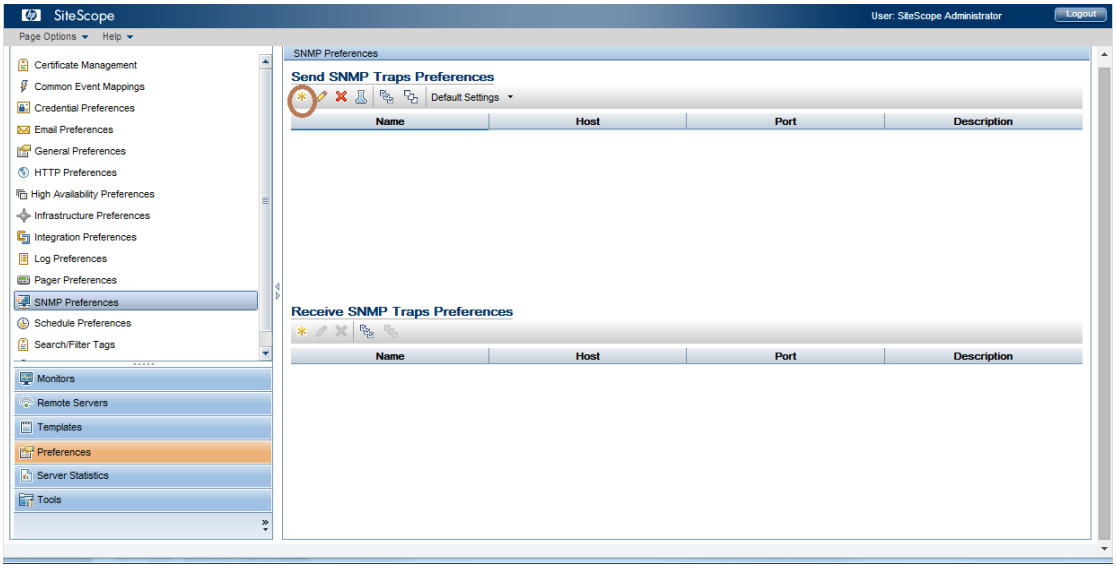


Figure 50 SiteScope > SNMP Preferences

6. Fill in the details in the SNMP Trap window that opens. Make sure to key in 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.

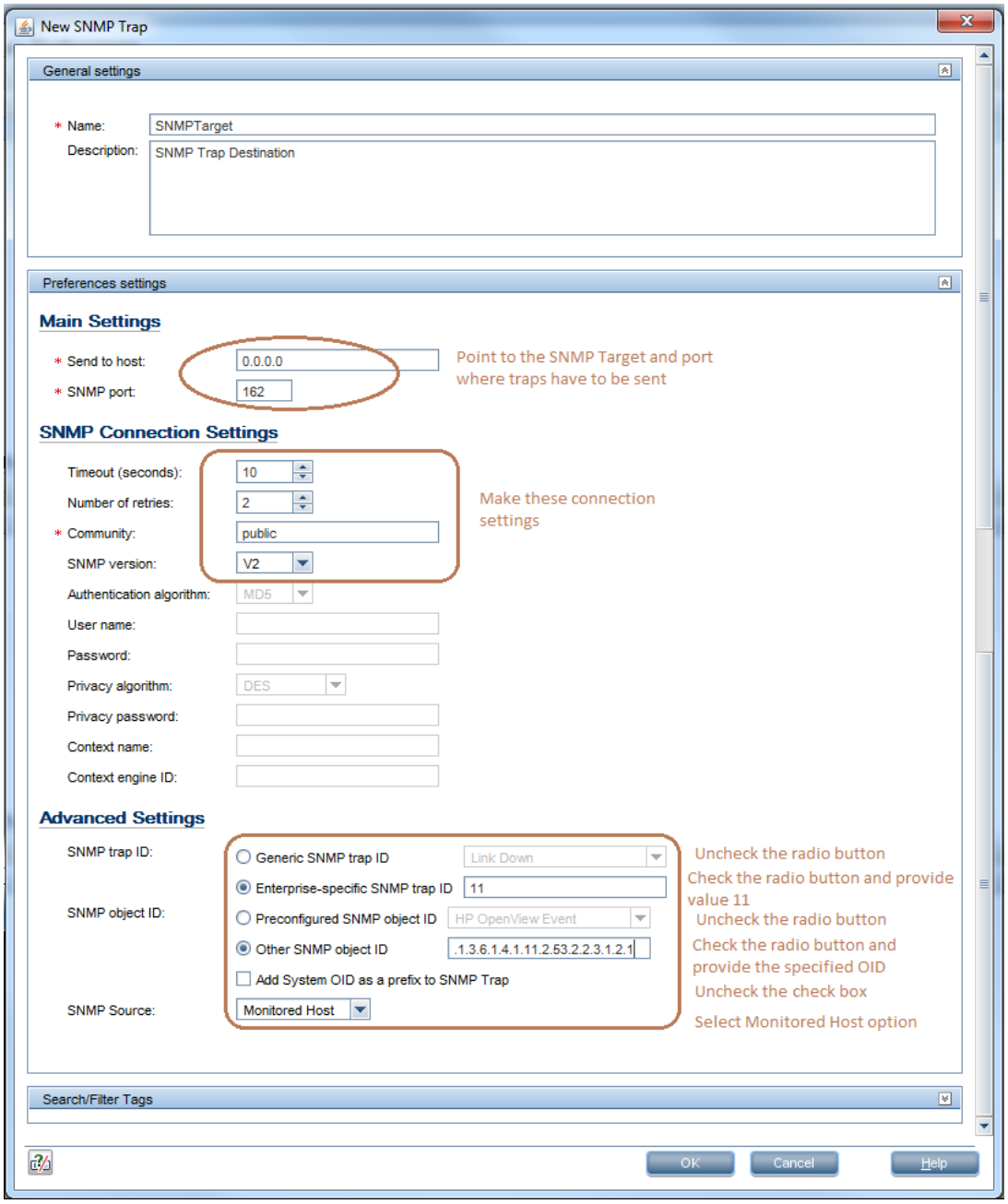


Figure 51 SiteScope > SNMP Preferences > New SNMP Trap

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

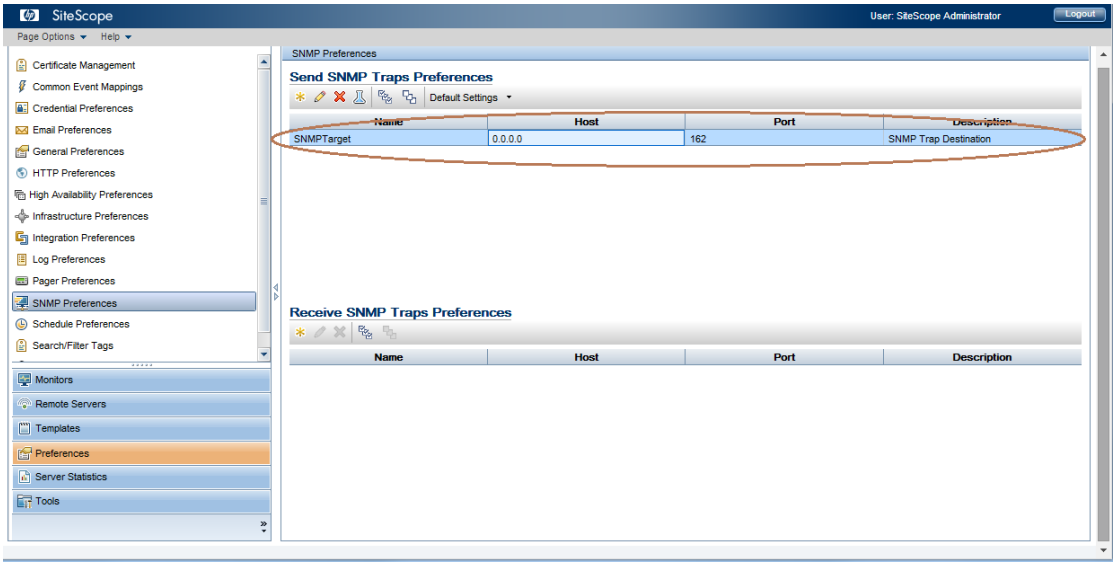


Figure 52 SiteScope > SNMP Preferences >Send SNMP Trap Preferences

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

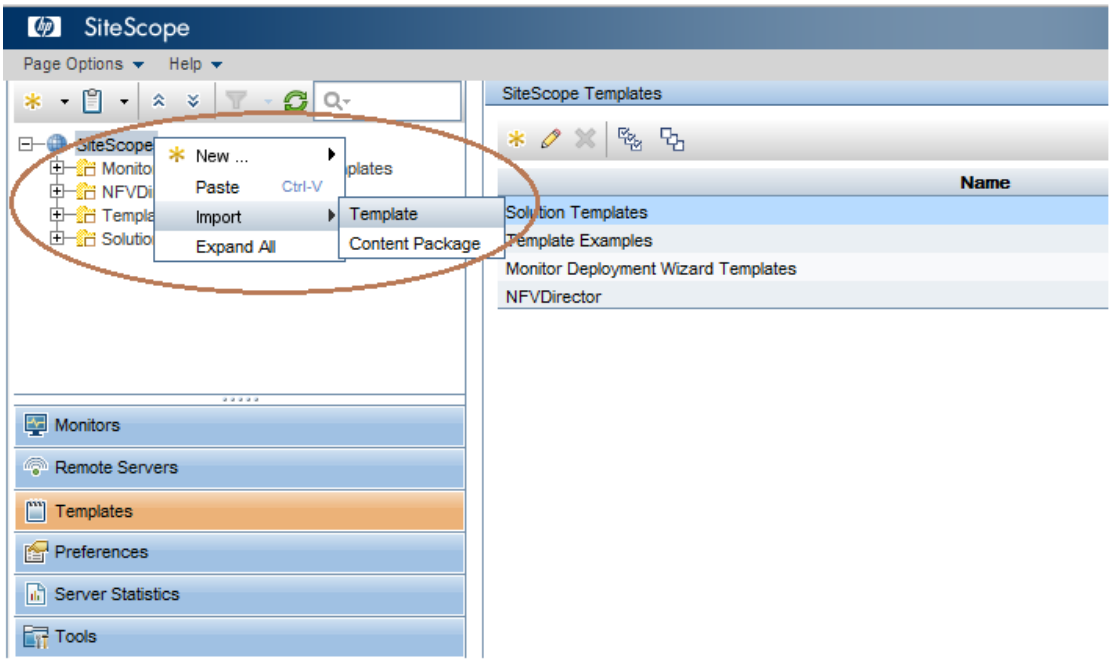


Figure 53 SiteScope > Import Template

9. Browse to the location where the file SiteScope_Templates is placed and choose the same. If you have launched the browser from your Desktop system, you may have to transfer the SiteScope_Templates from the system where you have installed the RPM from the `/opt/HP/nfvd/templates` location.

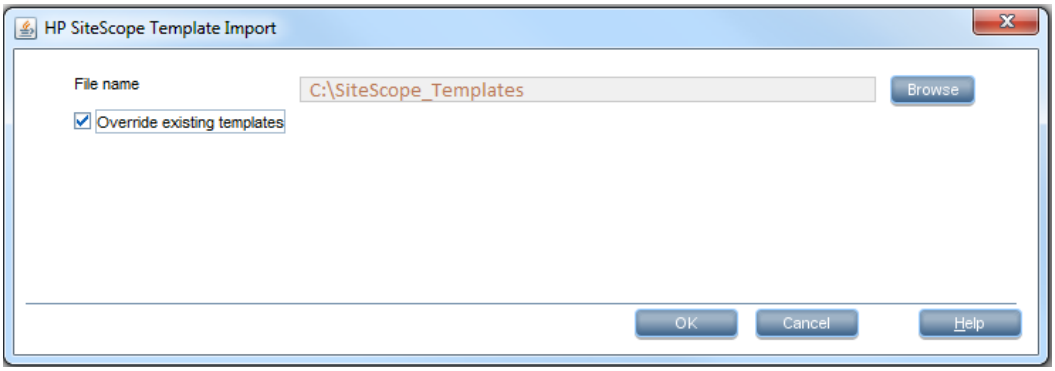


Figure 54 SiteScope > Import Template SiteScope_Templates

10. Click `OK` to import the templates. You will see the imported templates under NFVD directory.

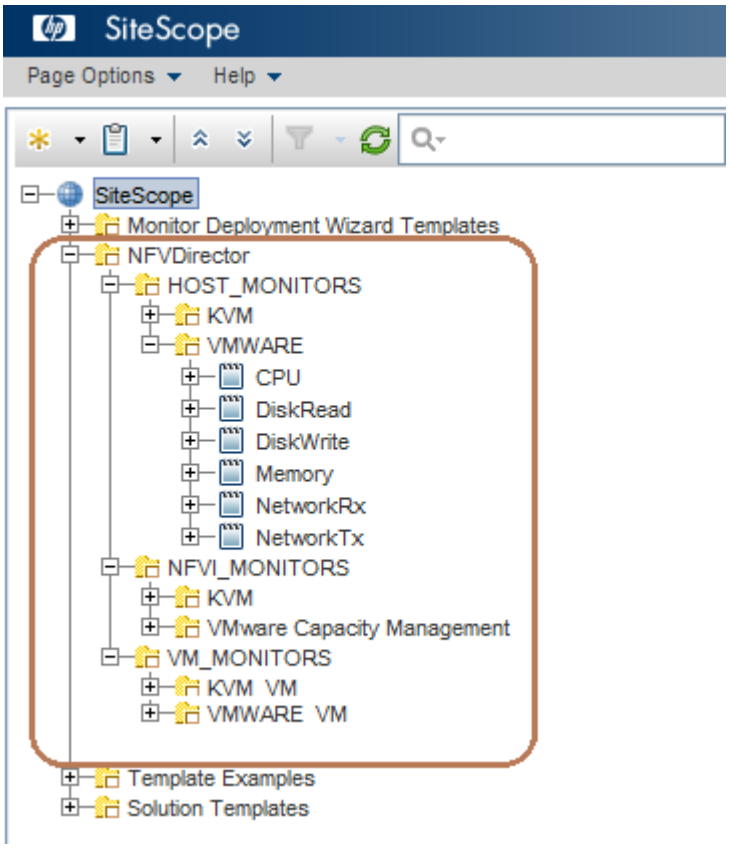


Figure 55 SiteScope > NFVDirector Template listing

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

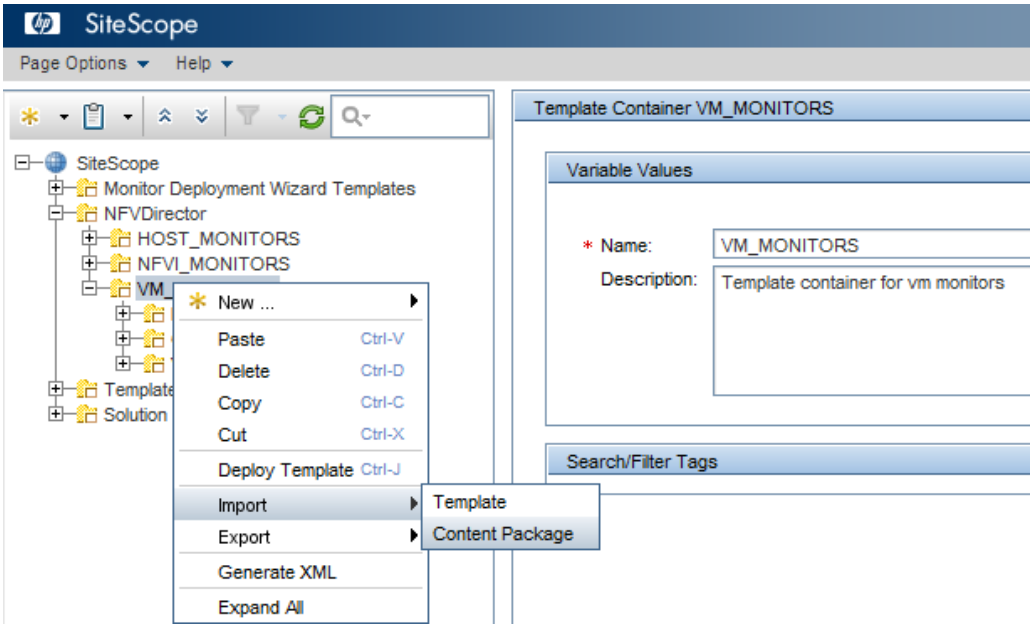


Figure 56 SiteScope > Import Content Package

12. Browse and point to the `Openstack_VM_Templates zip` file and click `OK`. If you have launched the browser from your Desktop system, you may have to transfer the SiteScope_Templates from the system where you have installed the RPM from the `/opt/HP/nfvd/templates` location.

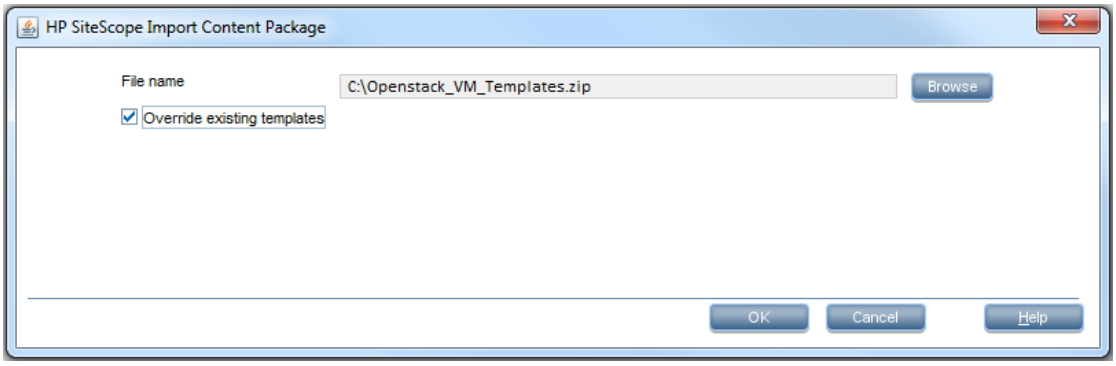


Figure 57 SiteScope > Import Content Package Openstack_VM_Templates.zip

13. Once imported, `Openstack` templates will be listed under `OPENSTACK_VM` tree.

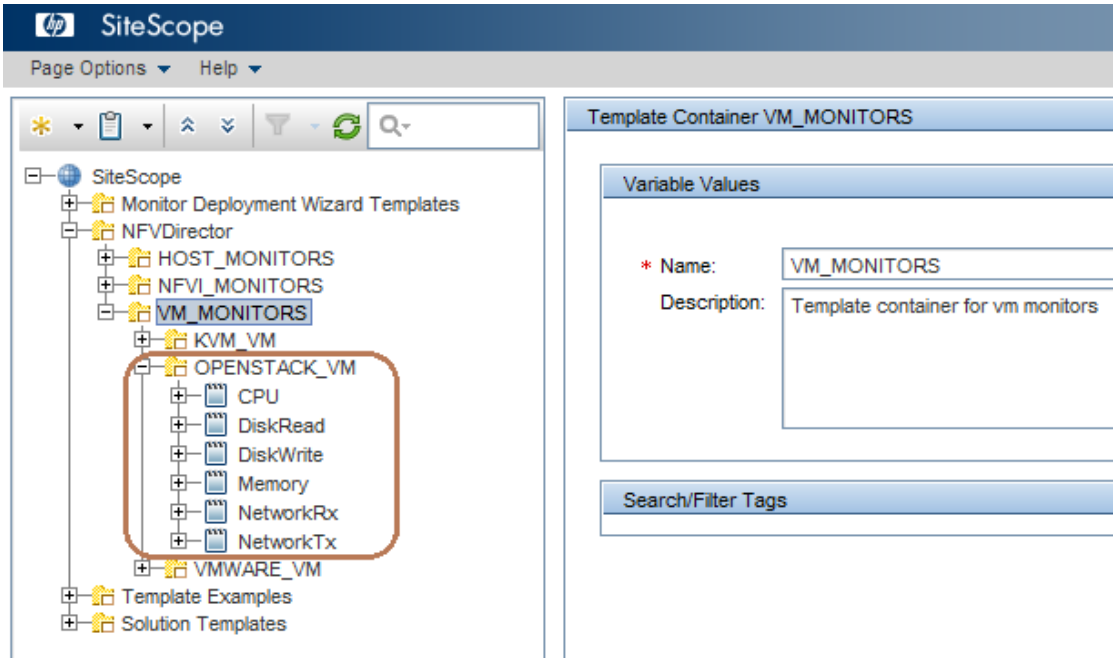


Figure 58 SiteScope > NFVDirector Templates > OpenStack Templates

14. Restart SiteScope.

3.7.6.2 Automatic import

NOTE: If the automatic import script is executed, you will need to reapply the license file again and the existing administrator credentials will be erased.

In order to automatically import all the settings that were carried out during Manual Import, Automatic Import of SiteScope template and configuration can be performed. However, it is advisable to perform automatic import only if it is a new SiteScope installation as it would overwrite any other configurations already performed on SiteScope, including overwriting the administrator username and password.

Automatic import can be performed by running the following command:

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

Script would not be executed if the SiteScope application is running.

3.7.6.3 Assurance gateway configuration for SiteScope

The file `/var/opt/HP/nfvd/conf/monitoring.properties` must be edited to set the following attributes:

- sitescope.login – SiteScope Administrator user name
- sitescope.password – SiteScope Administrator password
- sitescope.host – SiteScope server
- sitescope.port – SiteScope port

```
#Hypervisor Properties

## The VMWARE_Handler property indicates the attribute in the Virtual Machine from where the VM name has to be used
## by the Assurance Gateway for deploying the monitor
VMWARE_Handler=HYPERVISOR.NAME

## The KVM_Handler property indicates the attribute in the Virtual Machine from where the VM name has to be used
## by the Assurance Gateway for deploying the monitor
KVM_Handler=HYPERVISOR.NAME

## The OPENSTACK_Handler property indicates the attribute in the Virtual Machine from where the VM name has to be used
## by the Assurance Gateway for deploying the monitor
OPENSTACK_Handler=HYPERVISOR.ID

## In the absence of above Handler properties, GENERAL.NAME attribute in the Monitor Handler of the VNFD will be
## used to identify the VM name for deploying the monitor

## The KVM_HOSTNAME property indicates the attribute in the KVM host from where the host name has to be used by
## the Assurance Gateway for deploying the monitor
KVM_HOSTNAME=HYPERVISOR.HOSTNAME

## The VMWARE_HOSTNAME property indicates the attribute in the VMWare host from where the host name has to be
## used by the Assurance Gateway for deploying the monitor
VMWARE_HOSTNAME=HYPERVISOR.HOSTNAME

# Specify the Sitescope login details
sitescope.login=
sitescope.password=
# Specify the sitescope server port and host
sitescope.host=localhost
sitescope.port=8088
# Configure if SSL is required
sitescope.useSSL=false
```

Figure 59 monitoring.properties

3.7.6.4 Enabling database logging on SiteScope

1. SiteScope has a provision to store the monitor logs into the database. It is an optional feature that can be enabled by running the following script:

   `/opt/HP/nfvd/bin/metricsDBConfig.sh`

   Before running this script, SiteScope application must be stopped. It would create a database table `SITESCOPELOG`, which enables the logging preferences.

2. Once you run the script, start SiteScope and login to the portal.
3. Go to `Preferences` → `Log Preferences` to verify that the Database Logging Preferences has been set.

A sample preference setting is as shown in the following figure:

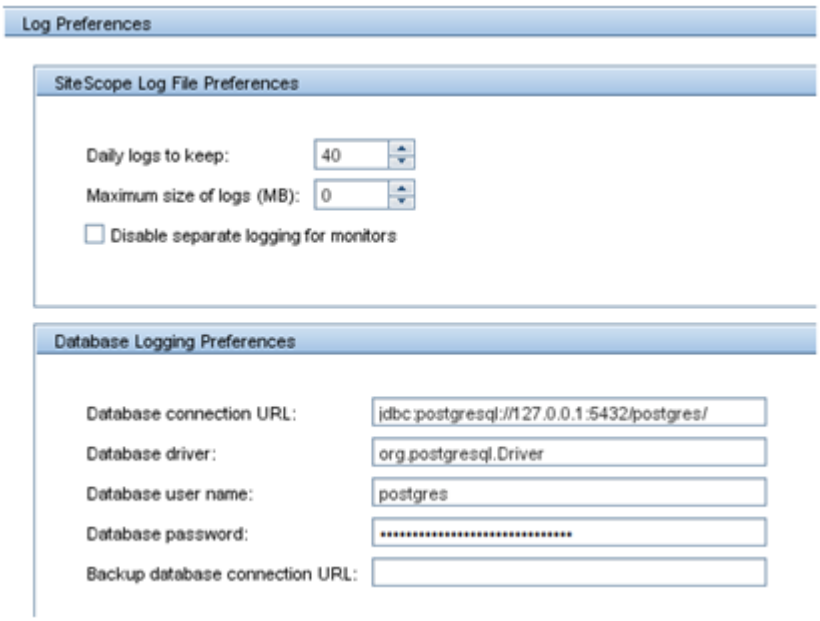


Figure 60 SiteScope > Log Preferences

3.8 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 | ppasdb | openmediation
| sitescope | uca-ebc | uca-atm | 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.

3.9 Uninstalling the NFVD Assurance solution

NFVD Assurance RPMs can be uninstalled by running the `rpm -ev` option.

Run the following commands to uninstall the various NFVD Assurance solutions:

- rpm -ev nfvd-assur-gw-core-01.00.000-1.el6.noarch
- rpm -ev nfvd-assur-gw-tpp-01.00.000-1.el6.noarch
- rpm -ev nfvd-monitors-01.00.000-1.el6.noarch
- rpm -ev nfvd-correlation-01.00.000-1.el6.noarch
- rpm -ev nfvd-assur-gw-base-01.00.000-1.el6.noarch

Note that uninstalling the `nfvd-monitors-01.00.000-1.el6.noarch` does not remove the configuration settings performed on the SiteScope system.

3.10 Various log file locations in NFVD Assurance

Product	Logs Location
Sitescope	/opt/HP/SiteScope/logs/
HPSA	/var/opt/OV/ServiceActivator/log/<hostname>
HPSA	/opt/HP/jboss/standalone/log/
UCA-EBC	/var/opt/UCA-EBC/instances/default/logs/
Open Mediation	/var/opt/openmediation-V62/log/
Open Mediation Service Mix	/var/opt/openmediation-V62/containers/instance-<#>/data/log
UCA Automation	/var/opt/UCA-ATM/logs/
NFVD Assurance Gateway	/opt/HP/nfvd/tpp/jboss/standalone/log

Table 42 Various log locations

NOTE: Periodic cleanup or archiving of the log files in the above directories is recommended.

Chapter 4

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.

4.1 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. Log in 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
```

4.2 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.

4.2.1 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>
```

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

Binary File	Component Name
nfvd-assur-gw-tpp-01.00.000-1.el6.noarch.rpm	NFVD Assurance 3rd party products

nfvd-assur-gw-core-01.00.000-1.el6.noarch.rpm	NFVD Assurance Gateway
nfvd-assur-gw-base-01.00.000-1.el6.noarch.rpm	NFVD Start/Stop Scripts
nfvd-correlation-01.00.000-1.el6.noarch.rpm	UCA Automation NFVD domain solution packs
nfvd-monitors-01.00.000-1.el6.noarch.rpm	SiteScope NFVD monitors
nfvd-fulfillment-01.00.000-1.el6.noarch.rpm	NFV Director Fulfillment solution packs

Table 43 Binaries List for Signature

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

```
gpg: Good signature from "Hewlett-Packard Company (HP Code
signing Service)"
```