HPE NFV Director

High Availability Installation and Configuration Guide

Release 4.1.1

First Edition

Hewlett Packard
Enterprise

Notices

Legal notice

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

Printed in the US

Trademarks

Linux is the registered trademark of Linus Torvalds in the U.S. and other countries.
Oracle and Java are registered trademarks of Oracle and/or its affiliates.

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

HP-UX Release 10.20 and later and HP-UX Release 11.00 and later (in both 32 and 64-bit configurations) on all HP 9000 computers are Open Group UNIX 95 branded products.

Microsoft®, Internet Explorer, Windows®, Windows Server 2007®, Windows XP®, and Windows 7® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Firefox® is a registered trademark of the Mozilla Foundation.

Google Chrome® is a trademark of Google Inc.

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

EnterpriseDB® is a registered trademark of EnterpriseDB.

Postgres Plus® Advanced Server is a registered U.S. trademark of EnterpriseDB.

UNIX® is a registered trademark of The Open Group.

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

Red Hat® is a registered trademark of the Red Hat Company.

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

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

VMware ESX, VMWare ESXi, VMWare vCenter and VMWare vSphere are either registered trademarks or trademarks of VMware, Inc. in the United States and other jurisdictions.

Contents

Preface

About this Guide

This guide NFVD HA Installation provides all the needed information to have HP NFV Director High Availability solution up and running.

Audience

This guide is intended for any stakeholder requiring to install and configure NFVD for production environment in High Available mode. It is recommended that the person is knowledgeable in basic Linux and Oracle administration to use this document.

Document History

Edition	Date	Description
1	October 15, 2016	First edition

Table 1: Document history

Chapter 1 NFV Director HA installation

1.1 HA Architecture

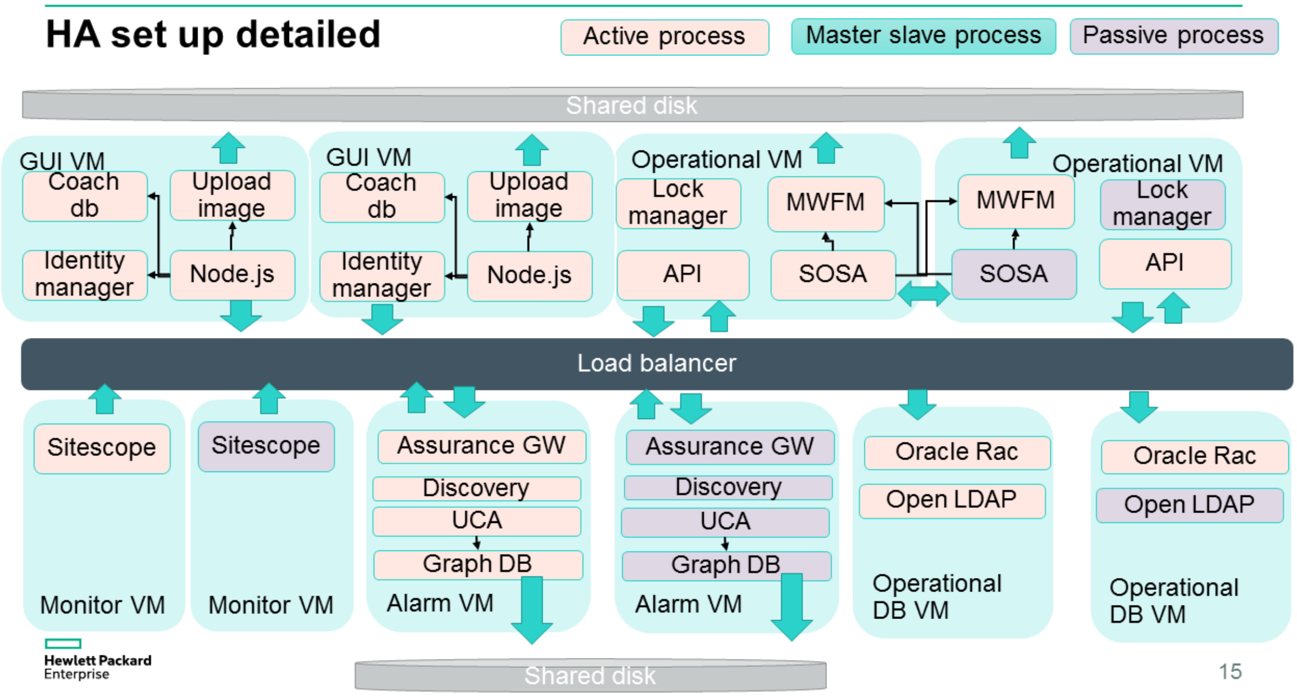
HA architecture is intended set upa at least two copies of each SW process and each VM so on the eventual failure of one process its mirror process takes over.

Ideally all process should be active active with a load balancer in front or a virtual ip so each process is not only protected to an eventual failure but also the load is distributed.

As per today underlaying SW capabilities there are still processes that are active passive.

There can be 3 types of procceses:

1. Active / Active : N processes are active at the same time and a load balancer in front distributes the load (either with stiky session onr round robin mechanism)
2. Active / Passive: Only one process is active and there is one backup process that will wake up on the failure of the second
3. Master / Slave: One processis the master with priority over the others, several slaves have second prority, on the failure of the master one of the slaves can become master



HA set up detailed

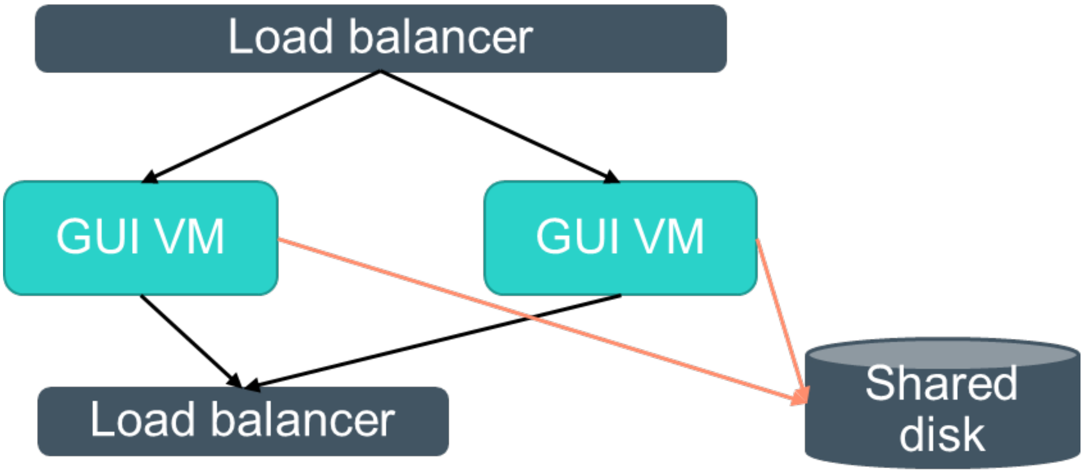
Active process | Master slave process | Passive process

Chapter 2 GUI VM Installation

2.1 Set up

On each GUI virtual machines, the following software should be installed:

- Upload image service
- Node.js
- Identity manger
- Coach db

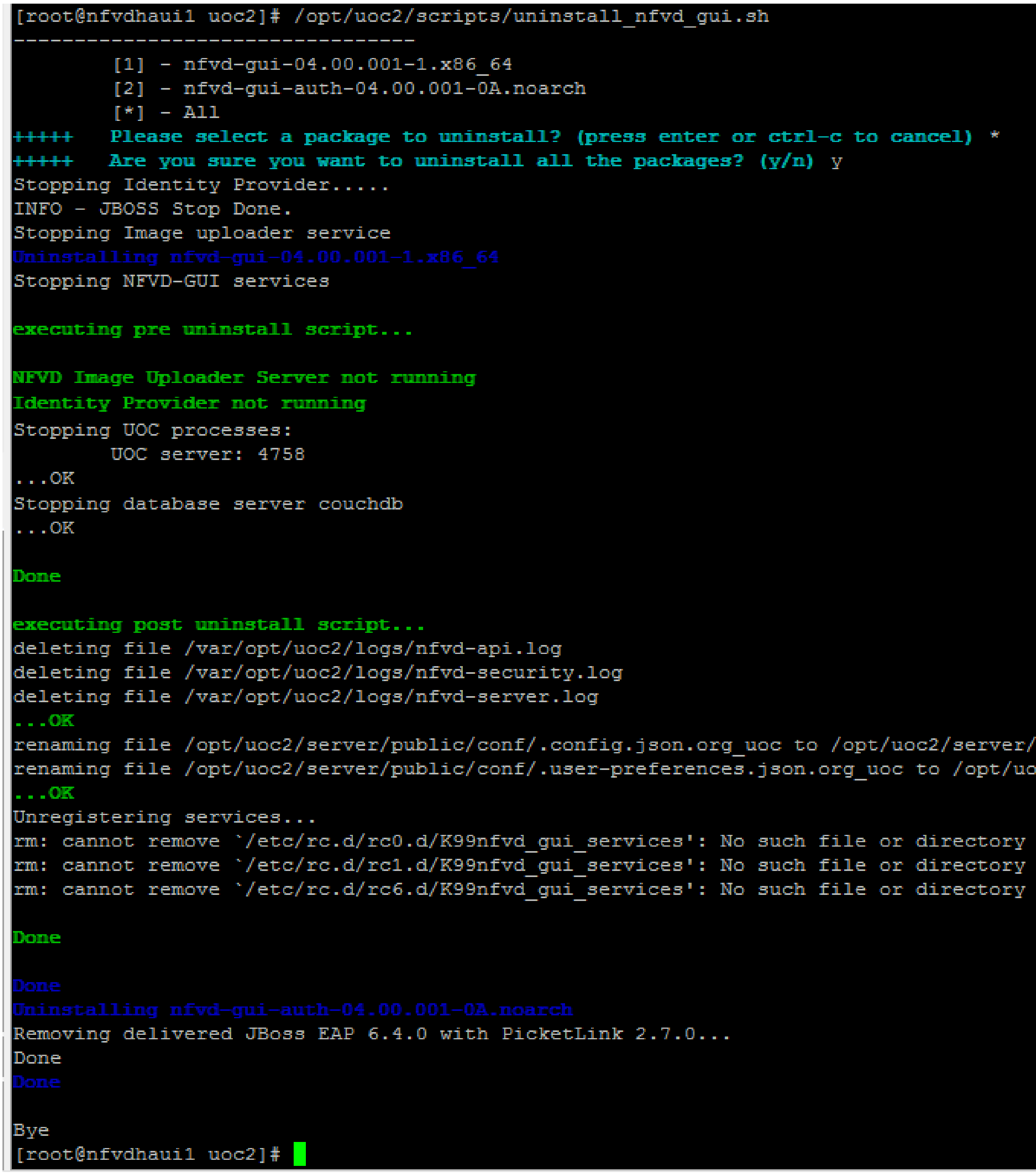


2.2 Upgrading from 4.01 to 4.1

Note: if you are installing NFVD-UI 4.1 on a new VM without 4.01 installed, then skip the "Uninstall" step

As "root"

- Uninstall NFD-UI 4.0.1
  `/opt/uoc2/scripts/uninstall_nfvd_gui.sh`
  Confirm that you want to uninstall All packages and wait for the uninstallation to complete



```
[root@nfvdhaui1 uoc2]# /opt/uoc2/scripts/uninstall_nfvd_gui.sh
---------------------------------
        [1] - nfvd-gui-04.00.001-1.x86_64
        [2] - nfvd-gui-auth-04.00.001-0A.noarch
        [*] - All
+++++   Please select a package to uninstall? (press enter or ctrl-c to cancel) *
+++++   Are you sure you want to uninstall all the packages? (y/n) y
Stopping Identity Provider.....
INFO - JBOSS Stop Done.
Stopping Image uploader service
Uninstalling nfvd-gui-04.00.001-1.x86_64
Stopping NFVD-GUI services

executing pre uninstall script...

NFVD Image Uploader Server not running
Identity Provider not running
Stopping UOC processes:
        UOC server: 4758
...OK
Stopping database server couchdb
...OK

Done

executing post uninstall script...
deleting file /var/opt/uoc2/logs/nfvd-api.log
deleting file /var/opt/uoc2/logs/nfvd-security.log
deleting file /var/opt/uoc2/logs/nfvd-server.log
...OK
renaming file /opt/uoc2/server/public/conf/.config.json.org_uoc to /opt/uoc2/server/
renaming file /opt/uoc2/server/public/conf/.user-preferences.json.org_uoc to /opt/uo
...OK
Unregistering services...
rm: cannot remove `/etc/rc.d/rc0.d/K99nfvd_gui_services': No such file or directory
rm: cannot remove `/etc/rc.d/rc1.d/K99nfvd_gui_services': No such file or directory
rm: cannot remove `/etc/rc.d/rc6.d/K99nfvd_gui_services': No such file or directory

Done

Done
Uninstalling nfvd-gui-auth-04.00.001-0A.noarch
Removing delivered JBoss EAP 6.4.0 with PicketLink 2.7.0...
Done
Done

Bye
[root@nfvdhaui1 uoc2]#
```

- Install NFVD-UI 4.1
  `tar xvf NFVD_UI_KIT-V04.01.000_7_20160719_174735.tar`
  `./nfvd_kit/install_nfvd_gui.sh -a`
  Answer all the questions, and wait for the installation to complete

- Check status of NFVD-UI
  `/opt/uoc2/scripts/monitor`

The linked image cannot be displayed. The file may have been moved, renamed, or deleted. Verify that the link points to the correct file and location.

2.3 Installation differences against non-HA set up

Each GUI VM must be configured the same way
Each GUI VM should acces a shared disk to copy there the uploaded images

Other than that, the installation procedure is not different when installing in HA mode.
Each GUI VM should point to the virtual ip of the Assurance GW and to the virtual IP of the FF API on the load balancer

2.4 Shared disk

The image directory can be configured in /nfs/images

The shared disk can be mounted in 3 ways:

1. Prefered option
   a. An external Cabin provides a single volume through NFS ant both VMs mount the same volume
2. Secon preferred
   a. An external cabin or even openstack cinder provides 2 volumes that are mounted one by each VM
   b. Each VM configured glusterFS to replicate and sync data between the 2 volumes
3. Last option
   a. Each VM defines a volume using the local disk
   b. Each VM configured glusterFS to replicate and sync data between the 2 volumes

2.5 Connectivity and load balancer needs

Each GUI VM should point to the virtual ip of the Assurance GW and to the virtual IP of the FF API on the load balancer
The load balancer should provide a virtual ip in front of the GUI so the end users only see one ip, the sessions for each user must be sticky based on IP

2.6 Monitoring tools

/opt/uoc2/scripts/monitor
This script provides the status of the 4 NFVD-UI components. If all 4 components are up, then it will return
HTTP/1.1 200 NFVD-UI OK

```
Content-Type: text/plain
Content-Length: 23
Connection: close

NFVD-UI is running.
```

If one or more components are down, then it will return
HTTP/1.1 503 NFVD-UI Unavailable
And the list of all unavailable components.

This script can be tested by the load balancer by making a GET request on the UI VM on port 3001
It will return a status code of 200 if the UI VM is up, and 503 otherwise.

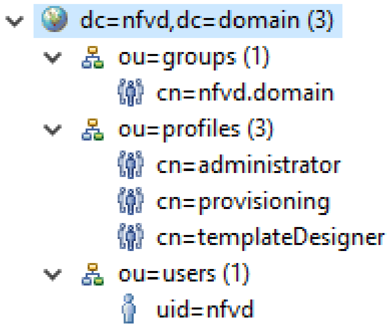
Chapter 3 Operational VMs Installation

3.1 Pre-requisites

This chapter will assume that you already have an Oracle database in a HA configuration (Oracle RAC is recommended) and ready to go, and also an Openldap installed in a multi-master configuration. This guide will not describe the installation of these pre-requisites.

3.2 LDAP structure

For the LDAP, the baseDN of the database needs to be the same as the domain you plan to use. That is, if we plan to use “nfvd.domain” as our domain in NFV-D, a baseDN of “dc=nfvd, dc=domain” should be created before. Also, sshPublicKey attribute should be available in the LDAP installation. Please, refer to OpenLDAP installation notes document provided with NFV-D 4.1 version to meet this pre-requisite. Also, this structure should be already created in the LDAP:



```
dc=nfvd,dc=domain (3)
    ou=groups (1)
        cn=nfvd.domain
    ou=profiles (3)
        cn=administrator
        cn=provisioning
        cn=templateDesigner
    ou=users (1)
        uid=nfvd
```

An example LDIF file is provided here in order to be able to import it structure:

```
version: 1

dn: dc=nfvd,dc=domain
dc: nfvd
o: NFVD Ldap Server
description: NFVD Ldap Server
objectClass: top
objectclass: dcObject
objectclass: organization

dn: ou=users,dc=nfvd,dc=domain
objectClass: top
objectClass: organizationalUnit
ou: users

dn: ou=groups,dc=nfvd,dc=domain
objectClass: top
objectClass: organizationalUnit
ou: groups

dn: cn=nfvd.domain,ou=groups,dc=nfvd,dc=domain
objectClass: top
objectClass: groupOfNames
cn: nfvd.domain
member: uid=default
member: uid=nfvd,ou=users,dc=nfvd,dc=domain
```

```
businessCategory: domain

dn: uid=nfvd,ou=users,dc=nfvd,dc=domain
objectClass: inetOrgPerson
objectClass: ldapPublicKey
objectClass: organizationalPerson
objectClass: person
objectClass: top
cn: name surname
sn: surname
businessCategory: domain
destinationIndicator: nfvd
givenName: name
mail: email@hpe.com
preferredLanguage: en-us
sshPublicKey:: MTIzNTQ2
telephoneNumber: 123546
uid: nfvd
userPassword: {sha}HAhFPdVVl10XVWN9BSVGh7WYX+A=

dn: ou=profiles,dc=nfvd,dc=domain
objectClass: top
objectClass: organizationalUnit
ou: profiles

dn: cn=administrator,ou=profiles,dc=nfvd,dc=domain
objectClass: groupOfNames
objectClass: top
cn: administrator
member: uid=default
member: uid=nfvd,ou=users,dc=nfvd,dc=domain

dn: cn=provisioning,ou=profiles,dc=nfvd,dc=domain
objectClass: groupOfNames
objectClass: top
cn: administrator
member: uid=default
member: uid=nfvd,ou=users,dc=nfvd,dc=domain

dn: cn=templateDesigner,ou=profiles,dc=nfvd,dc=domain
objectClass: groupOfNames
objectClass: top
cn: administrator
member: uid=default
member: uid=nfvd,ou=users,dc=nfvd,dc=domain
```

3.3 Hardware specifications

The recommended hardware specifications for a typical node in HA installation are:

Server	vCPU	Memory	Total OS	Total data
Operational	8	32G	50G	150G

This guide also provides, as a guidance, a mount point list as a example that could be followed to create the appropriate volumes in the VM, although they can be changed if required:

Volume Group	Size	Logical Volume	Mount Point	Size

OS	50G	root	/	10G
		home	/home	5G
		opt	/opt	2G
		usr	/usr	9G
		var	/var	7G
		tmp	/tmp	8.5G
		swap	swap	8G
data	150G	lvolEtcSA	/etc/opt/OV/ServiceActivator	5G
		lvolJBoss	/opt/HP/jboss	10G
		lvolOptNFVD	/opt/HPE/nfvd	5G
		lvolOptSA	/opt/OV/ServiceActivator	20G
		lvolVarSA	/var/opt/OV/ServiceActivator	10G
		<< Free >>	<< Free >>	100G

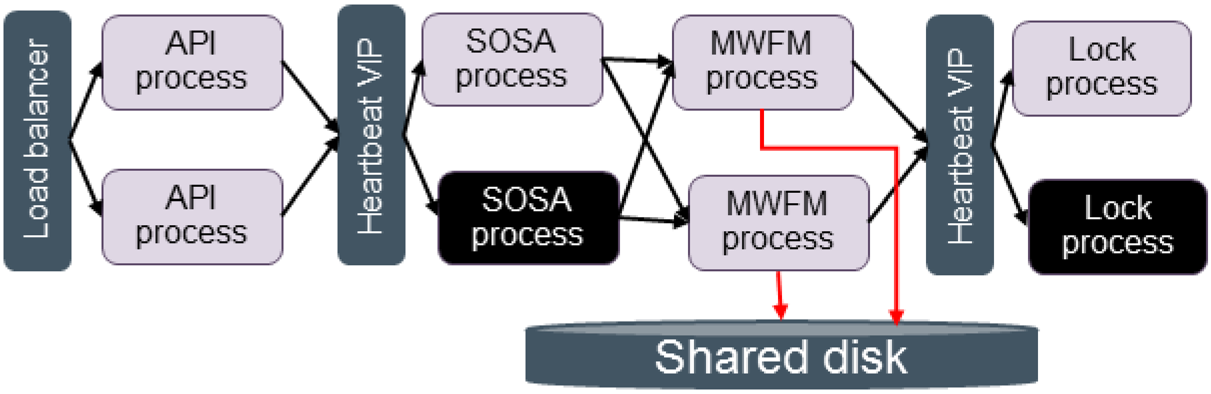
3.4 Base products

This guide will count on the existence of an already installed database cluster, and a HA Openldap installation.

On each Operational virtual machine the following SW should be installed:

- HPSA
  1) Extension packs:
     - SOSA
     - LockManager
- NFV-D solutions
  1) NFV Model (that includes the package to use Operational API)
  2) NFV Automation
  3) Openstack client
  4) DCN client
  5) Vcenter support (optional)

The typical HA configuration for an operational machine would be the following:



The operational API (API from now on) will be accesses through a LoadBalancer (LB) and then we will have two HPSA installations that will provide two separate MWFM processes to run workflows, and SOSA and LockManager will be controlled as cluster resources controlled by Heartbeat (the cluster daemon that will be used in this guide) and a virtual IP will be provided to access both SOSA and LockManager.

3.5 Base product installation

3.5.1 FTP location

You will find all the base products in the following URL:
ftp://nfsgre.gre.hpecorp.net/pub/NFV-DIRECTOR/V4.1/NFVD41_BaseProduct.tar

Download the file (2GB) and extract its content in a folder, for example, ‘`/tmp`’

For Fulfillment component, you will find all the necessary software in ‘`/tmp/BaseProduct/FF`’ folder:

```
[root@ff-node FF]# pwd
/tmp/BaseProduct/FF
[root@ff-node FF]# tree
.
├── alias.xml
├── configuration.xml
├── HPSA
│   ├── EP6.1-2.zip
│   ├── EP6.1-4.zip
│   ├── JK298-15001.iso
│   ├── JK441-15001.iso
│   ├── SAV62-1A-5.zip
│   └── SAV62-1A-9.zip
├── JAVA_ORACLE
│   └── jdk-6u45-linux-x64.bin
├── mwfm.xml
├── nfvd.properties
├── nfv_manager.xml
├── sosa_conf.xml
├── sosa.xml
├── standalone.xml
├── WAQCCR898_populate-catalog-SOSA.sql
└── web.xml
```

3.5.2 Installing Java

HPSA needs Java SE 6.

You will find the binary file in ‘`/tmp/BaseProduct/FF/JAVA_ORACLE/`’:

```
[root@ff-node JAVA_ORACLE]# pwd
/tmp/BaseProduct/FF/JAVA_ORACLE
[root@ff-node JAVA_ORACLE]# tree
.
└── jdk-6u45-linux-x64.bin
```

Copy the file into ‘`/usr/java/`’ folder and install it as follow:

```
[root@ff-node]# cd /usr/java
[root@ff-node]# ./jdk-6u45-linux-x64.bin
```

You will have something like this in '`/usr/java/`' folder:

```
[root@ff-node ~]# ls -lrt /usr/java/
total 8
drwxr-xr-x. 7 root root 4096 Jul 18 10:07 jdk1.6.0_45
lrwxrwxrwx. 1 root root   16 Jul 18 10:08 default -> /usr/java/latest
lrwxrwxrwx. 1 root root   21 Jul 18 10:18 latest -> /usr/java/jdk1.6.0_45
```

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

```
[root@ff-node ~]#  export JAVA_HOME=/usr/jdk1.6.0_45
[root@ff-node ~]#  export PATH=$JAVA_HOME/bin:$PATH:$HOME/bin
```

3.5.3 Database software

HPSA uses Oracle as database (also, it can be installed using Postgres Plus as database).

All what HPSA needs is:

- a user, typically , 'NFV'
- dba permissions and quote unlimited for that user

Once Oracle is setting up and running, you can execute the following commands:

```
[root@ff-node ~]# su - oracle
-bash-4.1$$ sqlplus /nolog

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

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

3.5.4 HP Service Activator installation

To install HPSA, the typical installation should be followed. Only one detail should be taken into account. When doing the configuration in the second node, no database installation should be done. So, the procedure to install it in a HA configuration would be:

- Install HPSA version 6.2-1 rpm provided by NFV-D ISO image.

  All the binaries you will need are located in '`/tmp/BaseProduct/FF/HPSA/`'

```
[root@ff-node HPSA]# pwd
/tmp/BaseProduct/FF/HPSA
[root@ff-node HPSA]# ll
total 1035716
-rwxr-xr-x. 1 root root  16311719 Apr  1 15:22 EP6.1-2.zip
-rw-r--r--. 1 root root  16274740 Jul 13 18:29 EP6.1-4.zip
-rwxr-xr-x. 1 root root 227375104 Apr  1 15:22 JK298-15001.iso
```

```
-rwxr-xr-x. 1 root root 766941184 Apr  1 15:22 JK441-15001.iso
-rwxr-xr-x. 1 root root  16614558 Apr  1 15:22 SAV62-1A-5.zip
-rw-r--r--. 1 root root  17037494 Jul 13 18:29 SAV62-1A-9.zip
```

As root, mount the Service Activator installation compact disk:

```
[root@ff-node HPSA]# pwd
/tmp/BaseProduct/FF/HPSA
[root@ff-node HPSA]#  mkdir -p /tmp/hpsa
[root@ff-node HPSA]#  mount -o loop JK441-15001.iso /tmp/hpsa
[root@ff-node HPSA]# ls -lh /tmp/hpsa
total 10K
dr-xr-xr-x. 4 root root 2.0K Dec 17  2012 Binaries
dr-xr-xr-x. 2 root root 4.0K Oct 23  2013 Documentation
dr-xr-xr-x. 3 root root 2.0K Oct 23  2013 OpenSource
dr-xr-xr-x. 2 root root 2.0K Oct 23  2013 ReadMe
```

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)”*.

```
[root@ff-node HPSA]# cd /tmp/hpsa/Binaries/Unix
[root@ff-node HPSA]# ./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.
```

At this point, HPSA is installed in your virtual machine.

Next step: to configure HPSA.

3.5.4.1 Configuring HP Service Activator

Once the typical HPSA installation has been completed, only one detail has to be taken into account:

When doing the configuration in the second node, no database installation should be done.

So, the procedure to install it in a HA configuration would be:

- Configure the `activatorConfig.xml` file (located in ‘`/etc/opt/OV/ServiceActivator/config/`’) to accommodate the needs.

  As we explained before, we have to configure it to do database configuration only for node 1.

- On node 2, no database configuration is needed.

- Here is depicted an example of the file for both nodes (wildcards are used in the example for you to change to the appropriate values):

  - **Node 1**

```
<?xml version="1.0" encoding="utf-8" ?>
<!DOCTYPE ActivatorConfig SYSTEM "activatorConfig.dtd">

<!--
  ===================================================================
  HP Service Activator configuration file to be read by ActivatorConfig
  ===================================================================
-->

<!-- (C) Copyright 2013 Hewlett-Packard Development Company, L.P. -->

<ActivatorConfig>

  <Mode>
    <!-- Optional Parameters -->
    <Param name="PARTIAL_CONFIGURATION" value="false" /><!-- Set partial or complete configuration
(default: false) -->
    <Param name="BACKUP_AND_REPLACE" value="true" /><!-- If true, backup and replace; otherwise, just
update - ignored for partial configuration (default: true) -->
    <!-- Optional Parameters - mandatory when partial configuration -->
    <Param name="PORT_CONFIGURATION" value="true" />
    <Param name="SSO_CONFIGURATION" value="true/false" /><!-- If true, SSO configuration will be set in
lwsso.xml -->
    <Param name="DB_CONFIGURATION" value="true/false" /><!-- If true, password for data sources will be
updated in standalone.xml -->
    <Param name="JBOSS_MANAGEMENT_CONFIGURATION" value="true/false" />
    <Param name="VIRTUAL_IP_CONFIGURATION" value="false" />
    <Param name="SCRIPTS_CONFIGURATION" value="true/false" />
    <Param name="SSH_CONFIGURATION" value="false" />
  </Mode>

  <!-- Port-Mapping element is optional if you are using default values. -->
  <Port-Mapping>
```

```
    <!-- Optional Parameters -->
    <Param name="MWFM_PORT" value="2000"/><!-- This is the MWFM_PORT default value -->
    <Param name="RM_PORT" value="9223"/><!-- This is the RM_PORT default value -->
    <Param name="DB_PORT" value="1521"/><!-- This is the SYS_DB_PORT default value i.e. Oracle default
port number -->
    <Param name="WEBSERVER_PORT" value="8080"/><!-- This is the WEBSERVER_PORT default value -->
  </Port-Mapping>

  <JBossManagement-Mapping>
    <Param name="MANAGEMENT_REALM_USERNAME" value="<%user>"/><!-- User name for HTTP
connections to JBoss CLI tool -->
    <Param name="MANAGEMENT_REALM_PASSWORD" value="<%password>"/><!-- Clear text password
for HTTP connections to JBoss CLI tool -->
  </JBossManagement-Mapping>

  <SSO-Mapping>
    <!-- Required Parameters -->
    <Param name="SSO_DOMAIN" value="..."/>
    <Param name="SSO_CIPHER_TYPE" value="symmetricBlockCipher"/>
    <Param name="SSO_CIPHER_ALGORITHM" value="AES"/>
    <Param name="SSO_KEY_SIZE" value="256"/>
    <Param name="SSO_INIT_STRING" value="This is a test string"/>
    <Param name="SSO_SESSION_TIMEOUT" value="60"/>
    <Param name="SSO_PROTECTED_DOMAINS" value="..."/>
    <Param name="SSO_LWSSO_LOG_DIRECTORY" value="/var/log"/>
  </SSO-Mapping>

  <!-- Disaster Recovery will be configured in DB only if a virtual IP is also configured -->
  <DisasterRecovery-Mapping>
    <!-- Required Parameters -->
    <Param name="DISASTER_SITE" value="Primary"/>
    <Param name="DISASTER_SITE_NAME" value="<%=@ff_host%>"/>
    <!-- Required Parameters if DR_SITE is Standby -->
    <Param name="DISASTER_DB_USER" value="..."/>
    <Param name="DISASTER_DB_PASSWORD" value="..."/>
    <Param name="DISASTER_DB_HOST" value="..."/>
    <Param name="DISASTER_DB_INSTANCE" value="..."/>
    <Param name="DISASTER_DB_PORT" value="..."/>
  </DisasterRecovery-Mapping>

  <Db-Mapping>
    <!-- Required Parameters -->
    <Param name="DB_HOST" value="<%=@db_host%>"/>
    <Param name="DB_INSTANCE" value="<%dbinstance>"/>
    <Param name="DB_USER" value="<%db_user>"/>
    <Param name="DB_PASSWORD" value="<%db_password>"/>
    <!-- Optional Parameters -->
    <Param name="DB_CREATE" value="true"/><!-- This is the DB_CREATE default value -->
    <Param name="DB_VENDOR" value="Oracle"/> <!—Shoulb be changed to PostgreSQL if used -->
  </Db-Mapping>

  <SysUser-Mapping>
    <!-- Required Parameters -->
    <Param name="SYS_USER" value="admin"/>
    <Param name="SYS_PASSWORD" value="admin123"/>
  </SysUser-Mapping>

  <SecureShell-Mapping>
    <!-- Required Parameters -->
    <Param name="SSH_USERNAME" value="sa_adm"/>
    <Param name="SSH_IDENTITY" value="C:/cygwin/home/sa_adm/.ssh/identity"/>
    <Param name="SSH_BIN_DIR" value=""/>
  </SecureShell-Mapping>
```

```
</ActivatorConfig>
```

- **Node 2**

```
<?xml version="1.0" encoding="utf-8" ?>
<!DOCTYPE ActivatorConfig SYSTEM "activatorConfig.dtd">

<!--
  =================================================================
  HP Service Activator configuration file to be read by ActivatorConfig
  =================================================================
-->

<!-- (C) Copyright 2013 Hewlett-Packard Development Company, L.P. -->

<ActivatorConfig>

  <Mode>
    <!-- Optional Parameters -->
    <Param name="PARTIAL_CONFIGURATION" value="false" /><!-- Set partial or complete configuration (default: false) -->
    <Param name="BACKUP_AND_REPLACE" value="true" /><!-- If true, backup and replace; otherwise, just update - ignored for partial configuration (default: true) -->
    <!-- Optional Parameters - mandatory when partial configuration -->
    <Param name="PORT_CONFIGURATION" value="true" />
    <Param name="SSO_CONFIGURATION" value="true/false" /><!-- If true, SSO configuration will be set in lwsso.xml -->
    <Param name="DB_CONFIGURATION" value="true/false" /><!-- If true, password for data sources will be updated in standalone.xml -->
    <Param name="JBOSS_MANAGEMENT_CONFIGURATION" value="true/false" />
    <Param name="VIRTUAL_IP_CONFIGURATION" value="false" />
    <Param name="SCRIPTS_CONFIGURATION" value="true/false" />
    <Param name="SSH_CONFIGURATION" value="false" />
  </Mode>

  <!-- Port-Mapping element is optional if you are using default values. -->
  <Port-Mapping>
    <!-- Optional Parameters -->
    <Param name="MWFM_PORT" value="2000"/><!-- This is the MWFM_PORT default value -->
    <Param name="RM_PORT" value="9223"/><!-- This is the RM_PORT default value -->
    <Param name="DB_PORT" value="1521"/><!-- This is the SYS_DB_PORT default value i.e. Oracle default port number -->
    <Param name="WEBSERVER_PORT" value="8080"/><!-- This is the WEBSERVER_PORT default value -->
  </Port-Mapping>

  <JBossManagement-Mapping>
    <Param name="MANAGEMENT_REALM_USERNAME" value="<%user>"/><!-- User name for HTTP connections to JBoss CLI tool -->
    <Param name="MANAGEMENT_REALM_PASSWORD" value="<%password>"/><!-- Clear text password for HTTP connections to JBoss CLI tool -->
  </JBossManagement-Mapping>

  <SSO-Mapping>
    <!-- Required Parameters -->
    <Param name="SSO_DOMAIN" value="..."/>
    <Param name="SSO_CIPHER_TYPE" value="symmetricBlockCipher"/>
    <Param name="SSO_CIPHER_ALGORITHM" value="AES"/>
    <Param name="SSO_KEY_SIZE" value="256"/>
    <Param name="SSO_INIT_STRING" value="This is a test string"/>
    <Param name="SSO_SESSION_TIMEOUT" value="60"/>
    <Param name="SSO_PROTECTED_DOMAINS" value="..."/>
    <Param name="SSO_LWSSO_LOG_DIRECTORY" value="/var/log"/>
  </SSO-Mapping>
  <!-- Disaster Recovery will be configured in DB only if a virtual IP is also configured -->
  <DisasterRecovery-Mapping>
    <!-- Required Parameters -->
    <Param name="DISASTER_SITE" value="Primary"/>
    <Param name="DISASTER_SITE_NAME" value="<%=@ff_host%>"/>
    <!-- Required Parameters if DR_SITE is Standby -->
    <Param name="DISASTER_DB_USER" value="..."/>
    <Param name="DISASTER_DB_PASSWORD" value="..."/>
    <Param name="DISASTER_DB_HOST" value="..."/>
    <Param name="DISASTER_DB_INSTANCE" value="..."/>
    <Param name="DISASTER_DB_PORT" value="..."/>
  </DisasterRecovery-Mapping>

  <Db-Mapping>
    <!-- Required Parameters -->
    <Param name="DB_HOST" value="<%=@db_host%>"/>
    <Param name="DB_INSTANCE" value="<%dbinstance>"/>
    <Param name="DB_USER" value="<%db_user>"/>
    <Param name="DB_PASSWORD" value="<%db_password>"/>
    <!-- Optional Parameters -->
    <Param name="DB_CREATE" value="false"/><!-- This is the DB_CREATE default value -->
    <Param name="DB_VENDOR" value="Oracle"/> <!-- Shoulb be changed to PostgreSQL if used -->
  </Db-Mapping>

  <SysUser-Mapping>
    <!-- Required Parameters -->
    <Param name="SYS_USER" value="admin"/>
    <Param name="SYS_PASSWORD" value="admin123"/>
  </SysUser-Mapping>

  <SecureShell-Mapping>
    <!-- Required Parameters -->
    <Param name="SSH_USERNAME" value="sa_adm"/>
    <Param name="SSH_IDENTITY" value="C:/cygwin/home/sa_adm/.ssh/identity"/>
    <Param name="SSH_BIN_DIR" value=""/>
  </SecureShell-Mapping>

</ActivatorConfig>
```

After that, we execute activation in both nodes:

```
[root@ff-node ~]# export JAVA_HOME=”your_java_home”
[root@ff-node ~]#  /opt/OV/ServiceActivator/bin/ActivatorConfig -f
/etc/opt/OV/ServiceActivator/config/activatorConfig.xml
```

Now, we have HPSA installed and configured.

Next step: to install the appropriate patches for HPSA.

To install HPSA patches, you need to have the file “`SAV62-1A-9.zip`”, provided in the NFV-D iso installation.

You will find it in:

```
[root@ff-node ~]# ls -lh /tmp/BaseProduct/FF/HPSA/
total 1012M
-rwxr-xr-x. 1 root root  16M Apr  1 15:22 EP6.1-2.zip
-rw-r--r--. 1 root root  16M Jul 13 18:29 EP6.1-4.zip
-rwxr-xr-x. 1 root root 217M Apr  1 15:22 JK298-15001.iso
-rwxr-xr-x. 1 root root 732M Apr  1 15:22 JK441-15001.iso
-rwxr-xr-x. 1 root root  16M Apr  1 15:22 SAV62-1A-5.zip
```

```
-rw-r--r--. 1 root root  17M Jul 13 18:29 SAV62-1A-9.zip
```

We should unzip this file in a temporary directory, and inside that, we will find a folder called "bin", and inside that folder, you will need to execute this command:

```
[root@ff-node Unix]# mkdir -p /tmp/SAV62-1A-9
[root@ff-node Unix]# cp /tmp/BaseProduct/FF/HPSA/SAV62-1A-9.zip /tmp/SAV62-1A-9/
[root@ff-node Unix]# cd /tmp/SAV62-1A-9/
[root@ff-node SAV62-1A-9]# unzip SAV62-1A-9.zip
[root@ff-node SAV62-1A-9]# cd cd SAV62-1A-9/bin/
[root@ff-node SAV62-1A-9]# bash ./patchmanager install
```

You will be asked a few questions during the install (you can safely answer Yes to every one), and you will need the user and the password of the HPSA database that you provided in `activatorConfig.xml` (typically, 'NFV/NFV').

```
=====================================================================
HP Service Activator Patch Manager version 6.2
HP Service Activator Hotfix V62-1A-9
=====================================================================

Checking files in Hotfix V62-1A-9...
0%....25%....50%....75%....100%
Check successful

Verifying permissions to install Hotfix V62-1A-9...
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-9? [Yes/No] Yes

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

Installing Hotfix V62-1A-9...
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.
```

With that, you will have HPSA installed with the lastest patch.

3.5.4.2 HPSA Extension pack installation

To install HPSA Extension pack, you will need the file “`HPSAEP6.1.zip`” provided in the NFV-D iso installation disk.

You will find it in:

```
[root@ff-node ~]# ls -lh /tmp/BaseProduct/FF/HPSA/
total 1012M
-rwxr-xr-x. 1 root root  16M Apr  1 15:22 EP6.1-2.zip
-rw-r--r--. 1 root root  16M Jul 13 18:29 EP6.1-4.zip
-rwxr-xr-x. 1 root root 217M Apr  1 15:22 JK298-15001.iso
-rwxr-xr-x. 1 root root 732M Apr  1 15:22 JK441-15001.iso
-rwxr-xr-x. 1 root root  16M Apr  1 15:22 SAV62-1A-5.zip
-rw-r--r--. 1 root root  17M Jul 13 18:29 SAV62-1A-9.zip
```

Mount the iso file in a temporal folder:

```
[root@ff-node ~]# mkdir -p /tmp/hpsaep
[root@ff-node bin]# cd /tmp/BaseProduct/FF/HPSA/
[root@ff-node bin]#  mount -o loop JK298-15001.iso /tmp/hpsaep
```

Copy the “`HPSAEP6.1.zip`” file to temporal folder and unzip it.

```
[root@ff-node bin]# mkdir /tmp/ep
[root@ff-node bin]# cp /tmp/hpsaep/Binaries/HPSAEP61.zip /tmp/ep
[root@ff-node bin]# cd /tmp/ep
[root@ff-node ep]# unzip HPSAEP6.1.zip
```

After that, go to the “`bin`” folder, and from that folder, execute:

```
[root@ff-node bin]# cd /tmp/ep/bin/
[root@ff-node bin]# bash ./install install
```

This script will ask a few questions, that you will need to answer (Yes can be safely used) and you will be asked for the HPSA database user and password.

There will also be a question, *“Do you wish to install the database?”* that should be answered:

- *“Yes”* in Node 1,
- *“No”* in Node 2.

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

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

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

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

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

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

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

DB configuration:
  Host   : <db_host>
  Port   : <db_port>
  Instance: <db_instance>
Please enter DB user name: NFV
Please enter DB password : NFV
Success.
Installing database schema...
Do you wish to install the database? [Yes/No] Yes in Node1, No in Node2
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.
```

After that, you will need to install the latest patch for the Extension pack.

The name of the file you need is "`EP6.1-4.zip`", that should be provided along in the NFV-D iso installation disk.

You will find it in:

```
[root@ff-node ~]# ls -lh /tmp/BaseProduct/FF/HPSA/
total 1012M
-rwxr-xr-x. 1 root root  16M Apr  1 15:22 EP6.1-2.zip
-rw-r--r--. 1 root root  16M Jul 13 18:29 EP6.1-4.zip
-rwxr-xr-x. 1 root root 217M Apr  1 15:22 JK298-15001.iso
-rwxr-xr-x. 1 root root 732M Apr  1 15:22 JK441-15001.iso
-rwxr-xr-x. 1 root root  16M Apr  1 15:22 SAV62-1A-5.zip
-rw-r--r--. 1 root root  17M Jul 13 18:29 SAV62-1A-9.zip
```

Copy the "`EP6.1-4.zip`" file to temporal folder and unzip it.

```
[root@ff-node bin]# mkdir /tmp/ep_patch
[root@ff-node bin]# cp /tmp/BaseProduct/FF/HPSA/EP6.1-4.zip /tmp/ep_patch
[root@ff-node bin]# cd /tmp/ep_patch
 [root@ff-node ep]# unzip EP6.1-4.zip
```

After that, edit the file "`/tmp/ep_patch/data/patch/V6.1-3/scripts/install/post/unix`".

```
[root@ff-node ep_patch]# vi /tmp/ep_patch/data/patch/V6.1-3/scripts/install/post/unix
```

Edit the header of this file to read "`#!/bin/ksh`", instead of "`#!/usr/bin/ksh`".

After that, from the "`/tmp/ep_patch/bin/`" directory, execute the following to install the patch:

```
[root@ff-node bin]# cd /tmp/ep_patch/bin/
[root@ff-node bin]# bash ./patchmanager install
```

Again, you will be asked to answer a few questions that can be safely answered as "*Yes*", and the HPSA database user and password.

There will also be a question: *“Do you wish to migrate your system database?”*.

It should be answered:

- *“Yes”* in Node 1,
- *“No”* in Node 2.

```
=====================================================================
HP Service Activator Patch Manager version 6.0
HPSA Extension Pack Hotfix V6.1-4
=====================================================================

Checking files in Hotfix V6.1-4...
0%....25%....50%....75%....100%
Check successful

Verifying permissions to install Hotfix V6.1-4...
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 V6.1-4? [Yes/No] yes

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

Installing Hotfix V6.1-4...
0%....25%....50%....75%....100%
Success.

Migrating system database from original version...
Do you wish to migrate your system database? [Yes/No] Yes for Node1, No for Node2
DB configuration:
  Host    : <db_host>
  Port    : <db_port>
  Instance: <db_instance>
Please enter DB user name: NFV
Please enter DB password : NFV
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.
```

After this procedure, you should have HPSA and Extension packs installed correctly on both machines.

3.5.4.3 Importing dependencies

After applying the HPE Service Activator patch, next task is to import and deploy the *CRModel* solution that is needed for the NFV-D solutions to work properly. The produce to do that is the following (specified by node)

- Node 1

```
[root@ff-node bin]# cd /opt/OV/ServiceActivator/bin
[root@ff-node bin]# echo –ne “CRModel\n” | ./deploymentmanager ImportSolution –file
/opt/OV/ServiceActivator/SolutionPacks/CRModel.zip
[root@ff-node bin]#  /opt/OV/ServiceActivator/bin/deploymentmanager DeploySolution -solutionName
CRModel -deploymentFile /opt/OV/ServiceActivator/solutions/CRModel/deploy_oracle.xml -createTables -
dbUser <db_user> -dbPassword <db_password> –dbHost <db_host> -db <db_instance> -dbPort <db_port>
```

- Node 2

```
[root@ff-node ~]#  cd /opt/OV/ServiceActivator/bin
[root@ff-node ~]#  ./deploymentmanager ImportSolution –file
/opt/OV/ServiceActivator/SolutionPacks/CRModel.zip
[root@ff-node ~]#  /opt/OV/ServiceActivator/bin/deploymentmanager DeploySolution -solutionName
CRModel -deploymentFile /opt/OV/ServiceActivator/solutions/CRModel/deploy_oracle.xml -noSQL -dbUser
<db_user> -dbPassword <db_password>  -dbHost <db_host> -db <db_instance> -dbPort <db_instance> -
noWorkflowsPlugins
```

Following sections describe how to configure the base products to get the desired HA configuration.

3.5.5 Installing NFV-Director operational module

3.5.5.1 Installing RPM file

In **both nodes**, install the RPM by running the following command:

```
[root@ff-node ~]#  rpm -ivh nfvd-fulfillment-04.01.001-1.el6.noarch.rpm
```

3.5.5.2 Copying solutions

In **both nodes**, copy the fulfillment solutions and patches to SolutionPack directory:

```
[root@ff-node ~]#  cp /opt/HPE/nfvd/fulfillment/*.zip /opt/OV/ServiceActivator/SolutionPacks/
```

3.5.5.3 Importing solutions

In **both nodes**, import the fulfillment solutions and patches in the sequence as shown here (*VCENTER* module installation is optional, but it is depicted here for completeness):

```
[root@ff-node ~]#  /opt/OV/ServiceActivator/bin/deploymentmanager ImportSolution -file
/opt/OV/ServiceActivator/SolutionPacks/NFVModel.zip
[root@ff-node ~]#  /opt/OV/ServiceActivator/bin/deploymentmanager ImportSolution -file
/opt/OV/ServiceActivator/SolutionPacks/MSA-1.2.2.zip
[root@ff-node ~]#  /opt/OV/ServiceActivator/bin/deploymentmanager ImportPatch -file
/opt/OV/ServiceActivator/SolutionPacks/MSA1.2.3.zip
[root@ff-node ~]#  /opt/OV/ServiceActivator/bin/deploymentmanager ImportSolution -file
/opt/OV/ServiceActivator/SolutionPacks/NFVAuto.zip
[root@ff-node ~]#  /opt/OV/ServiceActivator/bin/deploymentmanager ImportSolution -file
/opt/OV/ServiceActivator/SolutionPacks/OSPLUGIN.zip
[root@ff-node ~]#  /opt/OV/ServiceActivator/bin/deploymentmanager ImportSolution -file
/opt/OV/ServiceActivator/SolutionPacks/DPLUGIN.zip
[root@ff-node ~]# /opt/OV/ServiceActivator/bin/deploymentmanager ImportSolution -file
/opt/OV/ServiceActivator/SolutionPacks/VCENTER.zip
```

3.5.5.4 Checking Database Configuration (Oracle Only)

In NFVModel solution, there is a SQL script (located in `/opt/OV/ServiceActivator/solutions/NFVModel/etc/sql/` folder) which required to know where database datafiles are located in the ORACLE RAC.

```
[root@ff-node ~]#  cd /opt/OV/ServiceActivator/solutions/NFVModel/etc/sql/
[root@ff-node sql]#  ls -l
-rw-r--r--. 1 root root   158 May 23 11:37 00_create_tablespace.sql
-rw-r--r--. 1 root root    81 May  6 12:59 00_delete_tablespace.sql
-rw-r--r--. 1 root root    66 May  6 12:59 00_delete_user_oracle.sql
-rw-r--r--. 1 root root   306 May  6 12:59 01_create_user_oracle.sql
-rw-r--r--. 1 root root   181 May  6 12:59 01_create_user_ppas.sql
-rw-r--r--. 1 root root  4846 May  6 12:59 02_nfvd_model_delete_oracle.sql
-rw-r--r--. 1 root root  5067 May  6 12:59 02_nfvd_model_delete_ppas.sql
-rw-r--r--. 1 root root 33795 May  6 12:59 03_nfvd_model_create_oracle.sql
-rw-r--r--. 1 root root 33953 May  6 12:59 03_nfvd_model_create_ppas.sql
-rw-r--r--. 1 root root 21260 May  6 12:59 04_nfvd_model_inserts_oracle.sql
-rw-r--r--. 1 root root 22332 May  6 12:59 04_nfvd_model_inserts_ppas.sql
-rw-r--r--. 1 root root 22960 May  6 12:59 populate_catalog_sosa.sql
-rw-r--r--. 1 root root  1978 May  6 12:59 populate_data_example_debug.sql
-rw-r--r--. 1 root root   472 May  6 12:59 populate_default_english_language.sql
-rw-r--r--. 1 root root   360 May  6 12:59 remove_catalog_sosa.sql
-rw-r--r--. 1 root root   232 May  6 12:59 remove_default_english_language.sql
```

To know that path, you have to execute the following query in the database:

```
SQL> select file_name from dba_data_files;

FILE_NAME
--------------------------------------------------------------------------------
+NFV_DATA/xe/users01.dbf
+NFV_DATA/xe/undotbs01.dbf
+NFV_DATA/xe/sysaux01.dbf
+NFV_DATA/xe/system01.dbf
+NFV_DATA/xe/undotbs02.dbf

5 rows selected.
```

The highlighted path is the one that should be taken into account for substitution in the script. That is, the original content of the SQL file `00_create_tablespace.sql` script is:

```
create tablespace NFV_MODEL
datafile '?/dbs/NFVModel_data.dbf'
size 100m autoextend on next 32m maxsize unlimited logging
extent management local;
```

In this example, you would have to modify the content to leave it as as below:

```
create tablespace NFV_MODEL
datafile '+NFV_DATA/xe/NFVModel_data.dbf'
size 100m autoextend on next 32m maxsize unlimited logging
extent management local;
```

3.5.5.5 Deploying solutions

You have to execute only on Node 1 those parameters related to database operations.
This is the order to follow to deploy the solutions:

1) NFVModel solution

- Node 1

```
[root@ff-node ~]#  /opt/OV/ServiceActivator/bin/deploymentmanager DeploySolution -solutionName
NFVModel -deploymentFile /opt/OV/ServiceActivator/solutions/NFVModel/deploy.xml -
createTables -dbUser <hpsa_db_user> -dbPassword <hpsa_db_password> -dbHost <db_host> -db
<db_instance> -dbPort <db_port>
```

- Node 2

```
[root@ff-node ~]#  /opt/OV/ServiceActivator/bin/deploymentmanager DeploySolution -solutionName
NFVModel -deploymentFile /opt/OV/ServiceActivator/solutions/NFVModel/deploy.xml -noSQL -dbUser
<hpsa_db_user> -dbPassword <hpsa_db_password> -dbHost <db_host> -db <db_instance> -dbPort
<db_port>
```

2) MSA solution

- Node 1

```
[root@ff-node ~]#  cd /opt/OV/ServiceActivator/bin
[root@ff-node bin]#  /opt/OV/ServiceActivator/bin/deploymentmanager DeploySolution -solutionName
MSA -deploymentFile /opt/OV/ServiceActivator/solutions/MSA/deployUnix_6_1.xml -createTables -dbUser
<hpsa_db_user> -dbPassword <hpsa_db_password> -dbHost <db_host> -db <db_instance> -dbPort
<db_port>
```

- Node 2

```
[root@ff-node ~]#  cd /opt/OV/ServiceActivator/bin
[root@ff-node bin]#  /opt/OV/ServiceActivator/bin/deploymentmanager DeploySolution -solutionName
MSA -deploymentFile /opt/OV/ServiceActivator/solutions/MSA/deployUnix_6_1.xml -noSQL -dbUser
<hpsa_db_user> -dbPassword <hpsa_db_password> -dbHost <db_host> -db <db_instance> -dbPort
<db_port>
```

3) MSA patch

- Node 1

```
[root@ff-node ~]#  cd /opt/OV/ServiceActivator/bin
[root@ff-node bin]#  /opt/OV/ServiceActivator/bin/deploymentmanager DeployPatch -solutionName MSA -
patchName MSA1.2.3 -deploymentFile /opt/OV/ServiceActivator/solutions/MSA/
patches/MSA1.2.3/deployUnix_6_x.xml -dbUser <hpsa_db_user> -dbPassword <hpsa_db_password> -
dbHost <db_host> -db <db_instance> -dbPort <db_port>
```

- Node 2

```
[root@ff-node ~]#  cd /opt/OV/ServiceActivator/bin
[root@ff-node bin]#  /opt/OV/ServiceActivator/bin/deploymentmanager DeployPatch -solutionName MSA -
patchName MSA1.2.3 -deploymentFile
/opt/OV/ServiceActivator/solutions/MSA/patches/MSA1.2.3/deployUnix_6_x.xml -noSQL -dbUser
<hpsa_db_user> -dbPassword <hpsa_db_password> -dbHost <db_host> -db <db_instance> -dbPort
<db_port>
```

4) `NFVAuto` solution

- Node 1

```
[root@ff-node ~]#  cd /opt/OV/ServiceActivator/bin
[root@ff-node ~]#  /opt/OV/ServiceActivator/bin/deploymentmanager DeploySolution -solutionName
NFVAuto -deploymentFile /opt/OV/ServiceActivator/solutions/NFVAuto/deploy_ORACLE.xml -createTables
-dbUser <hpsa_db_user> -dbPassword <hpsa_db_password> -dbHost <db_host> -db <db_instance> -dbPort
<db_port>
```

- Node 2

```
[root@ff-node ~]#  cd /opt/OV/ServiceActivator/bin
[root@ff-node bin]#  /opt/OV/ServiceActivator/bin/deploymentmanager DeploySolution -solutionName
NFVAuto -deploymentFile /opt/OV/ServiceActivator/solutions/NFVAuto/deploy_ORACLE.xml -noSQL -
dbUser <hpsa_db_user> -dbPassword <hpsa_db_password> -dbHost <db_host> -db <db_instance> -dbPort
<db_port>
```

5) `OSPLUGIN` solution

- Node 1

```
[root@ff-node ~]#  cd /opt/OV/ServiceActivator/bin
[root@ff-node bin]# /opt/OV/ServiceActivator/bin/deploymentmanager DeploySolution -solutionName
OSPLUGIN -deploymentFile /opt/OV/ServiceActivator/solutions/OSPLUGIN/deploy.xml -createTables -
dbUser <hpsa_db_user> -dbPassword <hpsa_db_password> -dbHost <db_host> -db <db_instance> -dbPort
<db_port>
```

- Node 2

```
[root@ff-node ~]#  cd /opt/OV/ServiceActivator/bin
[root@ff-node bin]# /opt/OV/ServiceActivator/bin/deploymentmanager DeploySolution -solutionName
OSPLUGIN -deploymentFile /opt/OV/ServiceActivator/solutions/OSPLUGIN/deploy.xml -noSQL -dbUser
<hpsa_db_user> -dbPassword <hpsa_db_password> -dbHost <db_host> -db <db_instance> -dbPort
<db_port>
```

6) `DPLUGIN` solution

- Node 1

```
[root@ff-node ~]#  cd /opt/OV/ServiceActivator/bin
[root@ff-node bin]# /opt/OV/ServiceActivator/bin/deploymentmanager DeploySolution -solutionName
DPLUGIN -deploymentFile /opt/OV/ServiceActivator/solutions/DPLUGIN/deploy.xml -createTables -dbUser
<hpsa_db_user> -dbPassword <hpsa_db_password> -dbHost <db_host> -db <db_instance> -dbPort
<db_port>
```

- Node 2

```
[root@ff-node ~]#  cd /opt/OV/ServiceActivator/bin
[root@ff-node bin]# /opt/OV/ServiceActivator/bin/deploymentmanager DeploySolution -solutionName
DPLUGIN -deploymentFile /opt/OV/ServiceActivator/solutions/DPLUGIN/deploy.xml -noSQL -dbUser
<hpsa_db_user> -dbPassword <hpsa_db_password> -dbHost <db_host> -db <db_instance> -dbPort
<db_port>
```

7) `VCENTER` solution (optional)

- Node 1

```
[root@ff-node ~]#  cd /opt/OV/ServiceActivator/bin
[root@ff-node bin]# /opt/OV/ServiceActivator/bin/deploymentmanager DeploySolution -solutionName
VCENTER -deploymentFile /opt/OV/ServiceActivator/solutions/VCENTER/deploy.xml -createTables -dbUser
<hpsa_db_user> -dbPassword <hpsa_db_password> -dbHost <db_host> -db <db_instance> -dbPort
<db_port>
```

- Node 2

```
[root@ff-node ~]#  cd /opt/OV/ServiceActivator/bin
[root@ff-node bin]# /opt/OV/ServiceActivator/bin/deploymentmanager DeploySolution -solutionName
DPLUGIN -deploymentFile /opt/OV/ServiceActivator/solutions/VCENTER/deploy.xml -noSQL -dbUser
<hpsa_db_user> -dbPassword <hpsa_db_password> -dbHost <db_host> -db <db_instance> -dbPort
<db_port>
```

3.5.5.6 Heartbeat daemon installation

The Heartbeat daemon is needed to clusterize SOSA and LockManager.

As a prerequisite if you are installing in Openstack, it is needed that an IP (it is going to be the VIP for SOSA and LockManager) is associated as an allowed ip for ports of internal network of both machines.

As a reference, here is a list of commands that should be done in Openstack to support that:

```
#Create a port: (Preferrably using an IP from the discovery range)
neutron port-create HA-private  --fixed-ip ip_address=<vip>

#Get the ports Id attached to each server
neutron port-list | grep <internal-ip-vm-1>
neutron port-list | grep <internal-ip-vm-2>

#Attach the new IP to the port on each server
neutron port-update   fc211741-7a10-4ab0-a13b-c1de28aba6df --allowed_address_pairs list=true type=dict
ip_address=<vip>
neutron port-update  c12fefaa-cee1-4913-ade1-620d4b3acc99 --allowed_address_pairs list=true type=dict
ip_address=<vip>
```

It is also needed to configure both VMs with a fixed IP address when creating them in Openstack, and to configure the IP that way in the operating system.

To install heartbeat, all this packages would be needed (provided list is checked against Red Hat Linux 6.6):

```
cifs-utils-4.8.1-20.el6.x86_64.rpm
heartbeat-libs-3.0.4-2.el6.x86_64.rpm
quota-3.17-23.el6.x86_64.rpm
cluster-glue-1.0.5-6.el6.x86_64.rpm
libtalloc-2.1.5-1.el6_7.x86_64.rpm
resource-agents-3.9.5-34.el6.x86_64.rpm
cluster-glue-libs-1.0.5-6.el6.x86_64.rpm
libtdb-1.3.8-3.el6_8.2.x86_64.rpm
samba-client-3.6.23-35.el6_8.x86_64.rpm
```

```
device-mapper-1.02.117-7.el6.x86_64.rpm
libtevent-0.9.26-2.el6_7.x86_64.rpm
samba-common-3.6.23-35.el6_8.x86_64.rpm
device-mapper-event-1.02.117-7.el6.x86_64.rpm
lvm2-2.02.143-7.el6.x86_64.rpm
samba-winbind-3.6.23-35.el6_8.x86_64.rpm
device-mapper-event-libs-1.02.117-7.el6.x86_64.rpm
lvm2-libs-2.02.143-7.el6.x86_64.rpm
samba-winbind-clients-3.6.23-35.el6_8.x86_64.rpm
device-mapper-libs-1.02.117-7.el6.x86_64.rpm
perl-TimeDate-1.16-13.el6.noarch.rpm
tcp_wrappers-7.6-58.el6.x86_64.rpm
device-mapper-persistent-data-0.6.2-0.1.rc7.el6.x86_64.rpm
pytalloc-2.1.5-1.el6_7.x86_64.rpm
tcp_wrappers-libs-7.6-58.el6.x86_64.rpm
heartbeat-3.0.4-2.el6.x86_64.rpm
PyXML-0.8.4-19.el6.x86_64.rpm
```

The init script for both SOSA and LockManager should also be copied to the appropriate place. You should issue this command in your machine:

```
cp /opt/HPE/nfvd/fulfillment/scripts/activator-ep /etc/init.d/
chmod +x /etc/init.d/activator-ep
```

After installation, the following files should be configured:

1. `/etc/ha.d/authkeys`

   The content of this file should be this (with 600 mode):

   ```
   auth 2
   2 sha1 <shared_key>
   ```

   Note: You can create a shared key using any method you know. For example, you can use the following command:

   ```
   [root@ff-node ~]$ dd if=/dev/urandom bs=512 count=1 | openssl md5
   1+0 records in
   1+0 records out
   512 bytes (512 B) copied, 0.000119239 s, 4.3 MB/s
   (stdin)= c9f81b396a4e74278faf02d04c60f16f
   ```

   You should include a shared_key that should be an alphanumerical key and it should be different for each installation.

2. `/etc/ha.d/ha.cf`

   The content of this file should be this:

   ```
   logfile /var/log/heartbeat.log
   logfacility local0
   keepalive 2
   deadtime 30
   initdead 120
   ucast eth0 <other node in the cluster>
   udpport 694
   auto_failback off
   node <node1-hostname>
   ```

```
node <node2-hostname>
```

In a typical installation, you should change the node names with the machine names obtained from executing the command *“uname –n”*

The recommended configuration is to not allow the failback of resources when the primary node goes up again. This can be changed with using the auto_failback configuration to “on”.

3. `/etc/ha.d/haresources`

```
<node1-hostname> IPaddr::<vip>/24/eth0:0 activator-ep
```

The vip should be changed for the one you selected in the previous steps, and you should change the node name with the name of the primary node for your installation.

3.5.6 Persistence for SOSA service orders

By default, SOSA Service Orders for NFVD director are not persistent. So you have to enter in the HPSA database and configure it properly.

```
update catalog_service_order set persistable=1 where service_order_name='NFVD';
```

3.6 Configuring NFV-Director operational module

This section is going to describe what should be done to configuration files in order to obtain adequate performance and HA.
In the guide, there will be references to “password encrypted”. This should be the result of executing this command with the password in clear text:

```
/opt/OV/ServiceActivator/bin/crypt –encrypt <password>
```

3.6.1 JBoss: standalone.conf

Path	File
`/opt/HP/jboss/bin/standalone.conf`	`standalone.conf`

In **both nodes**, you have to change the values for `standalone.conf` file located in `/opt/HP/jboss/bin/` (highlighted):

```
# vi /opt/HP/jboss/bin/standalone.conf
## -*- shell-script -*- ##########################################################
##                                                                          ##
##  JBoss Bootstrap Script Configuration                                    ##
##                                                                          ##
##############################################################################

JVM_MIN_MEMORY=8192M
JVM_MAX_MEMORY=8192M
JVM_THREAD_MEMORY=4096K
```

```
JVM_MAX_PERM_SIZE=1536M

PLATFORM=`uname`
if [ "$PLATFORM" = "HP-UX" ]; then
   PLATFORM_OPTION="-XX:+UseGetTimeOfDay"
elif [ "$PLATFORM" = "Linux" ]; then
   PLATFORM_OPTION="-Djava.security.egd=file:///dev/urandom"
elif [ "$PLATFORM" = "SunOS" ]; then
   PLATFORM_OPTION="-Dsun.security.pkcs11.enable-solaris=false"
fi

rm -f /opt/HP/jboss/standalone/deployments/hpsa.ear.failed
rm -f /opt/HP/jboss/standalone/deployments/hpsa.ear.dodeploy
rm -f /opt/HP/jboss/standalone/deployments/hpsa.ear.deployed
rm -f /opt/HP/jboss/standalone/deployments/hpsa.ear.deploying
touch /opt/HP/jboss/standalone/deployments/hpsa.ear.dodeploy

# Executing standalone.xml script
/opt/OV/ServiceActivator/bin/replaceIP

if [ "x$JBOSS_MODULES_SYSTEM_PKGS" = "x" ]; then
   JBOSS_MODULES_SYSTEM_PKGS="org.jboss.byteman"
fi

#
# Specify options to pass to the Java VM.
#
JAVA_OPTS="-D_HPSA_MAIN_PROCESS_ -Xms$JVM_MIN_MEMORY -Xmx$JVM_MAX_MEMORY -
XX:MaxPermSize=$JVM_MAX_PERM_SIZE -d64 -Djava.awt.headless=true -server -
Xss$JVM_THREAD_MEMORY $PLATFORM_OPTION"
JAVA_OPTS="$JAVA_OPTS -Dorg.jboss.resolver.warning=true -Dsun.rmi.dgc.client.gcInterval=3600000 -
Dsun.rmi.dgc.server.gcInterval=3600000"
JAVA_OPTS="$JAVA_OPTS -Djboss.modules.system.pkgs=$JBOSS_MODULES_SYSTEM_PKGS -
Djava.awt.headless=true"

# Sample JPDA settings for remote socket debugging
#JAVA_OPTS="$JAVA_OPTS -Xrunjdwp:transport=dt_socket,address=8787,server=y,suspend=n"

# Sample JPDA settings for shared memory debugging
#JAVA_OPTS="$JAVA_OPTS -Xrunjdwp:transport=dt_shmem,server=y,suspend=n,address=jboss"

# Allow JProfiler to find its classes
#JAVA_OPTS="$JAVA_OPTS -Djboss.modules.system.pkgs=com.jprofiler"

# Use JBoss Modules lockless mode
#JAVA_OPTS="$JAVA_OPTS -Djboss.modules.lockless=true"
```

3.6.2 JBoss: standalone.xml

Path	File
`/opt/HP/jboss/standalone/configuration/`	`standalone.xml`

- In **both nodes**, add the following block below the `<periodic-rotating-file-handler name=”FILE”>` section.

```
        <periodic-rotating-file-handler name="NFVD_FILE">
            <formatter>
                <pattern-formatter pattern="%d{HH:mm:ss,SSS}|%p|%X{tid}|%m%n"/>
```

```
          </formatter>
          <file relative-to="jboss.server.log.dir" path="nfvd.log"/>
          <suffix value=".yyyy-MM-dd"/>
          <append value="true"/>
        </periodic-rotating-file-handler>

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

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

- In **both nodes**, add the following block in the beginning of the other `<logger category>` blocks.

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

- In **both nodes**, add the following datasource targeting REST API database in the beginning of the `<datasources>` block.

```
          <datasource jta="true" jndi-name="java:/nfvd-DS" pool-name="nfvd-DS" enabled="true" use-java-
context="true" use-ccm="true">
            <connection-
url>jdbc:oracle:thin:@(DESCRIPTION=(LOAD_BALANCE=on)(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCP)(HO
ST=<db_host>)(PORT=<db_port>)))(CONNECT_DATA=(SERVICE_NAME=<db_instance>)))</connection-url>
            <driver>oracle</driver>
            <pool>
              <min-pool-size>1</min-pool-size>
              <max-pool-size>100</max-pool-size>
              <prefill>true</prefill>
```

```
                <use-strict-min>false</use-strict-min>
                <flush-strategy>FailingConnectionOnly</flush-strategy>
            </pool>
            <security>
                <user-name>nfvd</user-name>
                <password>nfvd</password>
            </security>
            <validation>
                <valid-connection-checker class-
name="org.jboss.jca.adapters.jdbc.extensions.oracle.OracleValidConnectionChecker"/>
                <validate-on-match>false</validate-on-match>
                <background-validation>false</background-validation>
                <use-fast-fail>false</use-fast-fail>
            </validation>
        </datasource>
<drivers>
<driver name="oracle" module="com.hp.ov.activator.oracle">
          <xa-datasource-class>oracle.jdbc.driver.OracleDriver</xa-datasource-class>
</driver>
</drivers>
```

- In **both nodes**, replace the `<subsystem xmlns="urn:jboss:domain:resource-adapters:1.0">` block by the following (the important parts are highlighted):

```
    <subsystem xmlns="urn:jboss:domain:resource-adapters:1.0">
        <resource-adapters>
            <resource-adapter>
                <archive>
                    ldap-connector.rar
                </archive>
                <transaction-support>NoTransaction</transaction-support>
                <connection-definitions>
                    <connection-definition class-
name="com.hp.nfv.connector.ldap.jca.LdapManagedConnectionFactory" jndi-name="java:/ldap-DS"
enabled="true" use-java-context="true" pool-name="ldapPool" use-ccm="true">
                        <config-property name="ldapConnTimeout">
                            5000
                        </config-property>
                        <config-property name="connectionValidator">
                            com.hp.nfv.connector.ldap.jca.CustomLdapConnectionValidator
                        </config-property>
                        <config-property name="readTimeout">
                            5000
                        </config-property>
                        <config-property name="validationDN">
                            <base_dn_of_openldap>
                        </config-property>
                        <config-property name="securityCredentials">
                            <password_to_bind_to_openldap>
                        </config-property>
                        <config-property name="providerUrl">
                            ldap://<ldap_host>:<ldap_port>
                        </config-property>
                        <config-property name="securityAuthentication">
                            SIMPLE
                        </config-property>
                        <config-property name="securityPrincipal">
                            <ldap_bind_dn>
                        </config-property>
                        <config-property name="ldapContextFactory">
                            com.sun.jndi.ldap.LdapCtxFactory
                        </config-property>
```

```
          <pool>
            <min-pool-size>1</min-pool-size>
            <max-pool-size>100</max-pool-size>
            <prefill>false</prefill>
            <use-strict-min>false</use-strict-min>
            <flush-strategy>FailingConnectionOnly</flush-strategy>
          </pool>
          <security>
            <application/>
          </security>
          <timeout>
            <blocking-timeout-millis>3000</blocking-timeout-millis>
            <idle-timeout-minutes>0</idle-timeout-minutes>
          </timeout>
          <validation>
            <background-validation>true</background-validation>
            <background-validation-millis>45000</background-validation-millis>
            <use-fast-fail>false</use-fast-fail>
          </validation>
        </connection-definition>
      </connection-definitions>
    </resource-adapter>
  </resource-adapters>
</subsystem>
```

3.6.3 HPE Service Activator: `mwfm.xml`

Path	File
`/etc/opt/OV/ServiceActivator/config/mwfm.xml`	`mwfm.xml`

- In **both nodes**, delete or comment the following configuration:

```
<Module>
  <Name>distribution_module</Name>
  <Class-Name>com.hp.ov.activator.mwfm.engine.module.RoundRobinDistModule</Class-Name>
  <Param name="dispatch_local"  value="true"/>
 </Module>
```

- In **both nodes**, delete or comment the following configuration (if it exists):

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

- In **both nodes**, configure this for KeepAlive module:

```
<Module>
  <Name>keep_alive</Name>
  <Class-Name>com.hp.ov.activator.mwfm.engine.module.KeepAliveModule</Class-Name>
  <Param name="keep_alive_time" value="10000"/>
  <Param name="take_over_time" value="60000"/>
  <Param name="job_startup_retry_count" value="3"/>
  <Param name="job_startup_retry_interval" value="10000"/>
  <Param name="update_heartbeat" value="false"/>
```

```
   <Param name="monitor_wait_interval" value="30000"/>
   <Param name="db_poll_interval" value="10000"/>
   <Param name="retrieve_jobs_buffer_size" value="256"/>
   <Param name="configure_virtual_ip" value="false"/>
   <Param name="auto_virtual_ip_takeover" value="false"/>
   <Param name="virtual_ip_ping_timeout" value="10000"/>
   <Param name="start_watch_dog_process" value="false"/>
   <Param name="watch_dog_poll_interval" value="30000"/>
 </Module>
```

- In **both nodes**, uncomment the existing authenticator module and add `teams_enabled` parameter:

```
 <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>
```

- In **both nodes**, 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>

<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>

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

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

```
<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>

  <Module>
   <Name>sync_module</Name>
   <Class-Name>com.hp.ov.activator.mwfm.engine.module.NFVDSyncModule</Class-Name>
   <Param name="db_cleanup_interval" value="4000"/>
   <Param name="parent_notification_interval" value="4000"/>
   <Param name="wakeup_monitor_interval" value="4000"/>
  </Module>
```

- In **Node 1**, add the following modules between <Engine> </Engine> tag:

```
<Module>
    <Name>LockModule</Name>
    <Class-Name>com.hp.spain.engine.module.lock.manager.LockModule</Class-Name>
    <Param name="locker_name" value="MWFM-<node1_host_name>"/>
    <Param name="locker_service_ip_address" value="<node1_host_name> "/>
    <Param name="unlock_pending_period" value="60000"/>
    <Param name="lock_manager_service_url" value="rmi://<lockmanager-vip-hostname-or-
ip>: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>

  <Module>
     <Name>MailManager</Name>
     <Class-Name>com.hp.spain.engine.module.MailManager</Class-Name>
     <Param name="pop3_server"  value="127.0.0.1"/>
     <Param name="smtp_server"  value="<smtp_server>"/> <!—if you don’t have a relay, you can configure
local delivery>
     <Param name="basedir"  value="/"/>
     <Param name="separator"  value="/"/>
     <Param name="tmpdir"  value="/var/opt/OV/ServiceActivator/tmp"/>
     <Param name="prefix"  value=""/>
     <Param name="notifier"  value="<from_address>"/>
   </Module>
```

- In **Node 2**, add the following modules between <Engine> </Engine> tag:

```
<Module>
    <Name>LockModule</Name>
    <Class-Name>com.hp.spain.engine.module.lock.manager.LockModule</Class-Name>
    <Param name="locker_name" value="MWFM-<node2_host_name>"/>
    <Param name="locker_service_ip_address" value="<node2_host_name> "/>
    <Param name="unlock_pending_period" value="60000"/>
    <Param name="lock_manager_service_url" value="rmi://<lockmanager-vip-hostname-or-
ip>: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>

  <Module>
```

```
    <Name>MailManager</Name>
    <Class-Name>com.hp.spain.engine.module.MailManager</Class-Name>
    <Param name="pop3_server"  value="127.0.0.1"/>
    <Param name="smtp_server"  value="<smtp_server>"/> <!—if you don’t have a relay, you can configure
local delivery>
    <Param name="basedir"  value="/"/>
    <Param name="separator"  value="/"/>
    <Param name="tmpdir"  value="/var/opt/OV/ServiceActivator/tmp"/>
    <Param name="prefix"  value=""/>
    <Param name="notifier"  value="<from_address>"/>
  </Module>
```

In the file /opt/OV/ServiceActivator/EP/LockManager/bin/setenv.sh, add the following line after the line “RMI_HOST=localhost”:

```
RMI_STUB_EXPORT_HOST=<lockmanager-vip-hostname-or-ip>
```

3.6.4 NFV-D properties configuration

Other necessary commands to be executed in both nodes:

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

In **both nodes**, update the file content `/etc/opt/OV/ServiceActivator/config/nfvd.properties` to:

```
X-Auth-Token=3778fe88-e71d-4004-86bc-3188f7fd450b
rest.api.endpoint.key=http://<nfvd-api-vip>:8080
assurance.rest.api.endpoint.key=http://<assurance-api-vip>:18080
assurance.X-Auth-Token=9ea409f5-f69a-4834-b745-8e3099be17a0
```

Execute the following commands in the NFVD database node:

```
update nfvd_configuration set config_value='http://<sosa-vip>:8071' where config_key='sosa.service.url';
update nfvd_configuration set config_value='http:// <assurance-api-vip>:18080' where
config_key='assurance.service.url';
update nfvd_configuration set config_value=<nfvd-api-vip>' where config_key='nfvd.host';
commit;
```

3.6.5 HPE Service Activator: `OpenStack.properties`

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

In **both nodes**, configure following values:

```
mwfwUser=<hpsa_admin_user>
mwfwPassword=<hpsa_admin_password>
```

3.6.6 HPE SA Extension Pack - SOSA: `sosa.sh`

Path	File
`/opt/OV/ServiceActivator/EP/SOSA/bin/`	`sosa.sh`

In **both nodes**, you have to change the values for `sosa.sh` file located in `/opt/OV/ServiceActivator/EP/SOSA/bin/` (highlighted are the changes) :

```
# vi /opt/OV/ServiceActivator/EP/SOSA/bin/sosa.sh
#!/bin/sh

MY_PWD=`pwd`

export BASEDIR=/opt/OV/ServiceActivator/EP/SOSA
cd $BASEDIR

export JAVA_HOME=<java_home>
export JAVADIR=$JAVA_HOME/bin
export CONFDIR=conf
export TMPDIR=tmp
export LOGDIR=log
export PROPERTIES=properties
export LIB=lib


export HPSA_EAR_LIB=/opt/HP/jboss/standalone/deployments/hpsa.ear/lib
export LOG4JFILE=properties/sosa-log4j.properties
export JAVA_DEBUG="-Xdebug -Xrunjdwp:transport=dt_socket,address=8787,server=y,suspend=n"
#export JAVA_VERBOSEGC="-verbose:gc  -Xloggc:$LOGDIR/verbose_sosa3.log.gc -XX:+PrintGCDetails -
XX:+PrintGCTimeStamps"
#export JAVA_VERBOSEGC="-Xverbosegc:file=$LOGDIR/verbose_sosa3.log.gc -XX:+HeapDump"
export JAVA_VERBOSEGC=""
#export JAVA_VERBOSEGC="-XX:+HeapDumpOnOutOfMemoryError -verbose:gc  -
Xloggc:$LOGDIR/verbose_sosa31.log.gc "
#export JAVA_PERFORMANCE="-Xrunhprof:file=$LOGDIR/sosa3.hprof.txt"
#export JAVA_PERFORMANCE="-
Xrunhprof:thread=y,heap=all,depth=8,cutoff=0.0002,doe=y,cpu=times,file=$LOGDIR/sosa3.hprof.txt"
export JAVA_PERFORMANCE=""
export JAVA_XMX="-Xmx2048m"
export JAVA_XMS="-Xms512m"

export SCRIPTNAME=sosa
export CONFIGFILE=$CONFDIR/sosa.xml
export CONFIGFILE_DTD=$CONFDIR/sosa.dtd

export JAVA_OPTS="-D$SCRIPTNAME -Djava.security.policy=$CONFDIR/sosa.policy -
Dlog4j.configuration=$LOG4JFILE $JAVA_XMS $JAVA_XMX $JAVA_VERBOSEGC $JAVA_PERFORMANCE"

#CLASSPATH=$SOSA_CLASSPATH:.:$PROPERTIES:$CONFDIR:$HPSA_EAR_LIB/sosa.jar:$HPSA_EAR_LIB/mwfm
.jar:$HPSA_EAR_LIB/activator_utils.jar:$HPSA_EAR_LIB/resmgr.jar:$HPSA_EAR_LIB/inventoryruntime.jar:$H
PSA_EAR_LIB/ep-utils.jar:$HPSA_EAR_LIB/commons-codec-1.5.jar:$HPSA_EAR_LIB/sosa-hibernate.jar
CLASSPATH=$SOSA_CLASSPATH:.:$PROPERTIES:$CONFDIR:$HPSA_EAR_LIB/sosa.jar:$HPSA_EAR_LIB/mwfm.j
ar:$HPSA_EAR_LIB/activator_utils.jar:$HPSA_EAR_LIB/resmgr.jar:$HPSA_EAR_LIB/inventoryruntime.jar:$HP
SA_EAR_LIB/ep-utils.jar:$HPSA_EAR_LIB/commons-codec-1.5.jar:$HPSA_EAR_LIB/sosa-
hibernate.jar:$HPSA_EAR_LIB/axiom-api-1.2.13.jar:$HPSA_EAR_LIB/axiom-impl-
1.2.13.jar:$HPSA_EAR_LIB/axis2-adb-1.6.2.jar:$HPSA_EAR_LIB/axis2-kernel-1.6.2.jar:$HPSA_EAR_LIB/axis2-
transport-http-1.6.2.jar:$HPSA_EAR_LIB/axis2-transport-local-1.6.2.jar:$HPSA_EAR_LIB/commons-codec-
1.5.jar:$HPSA_EAR_LIB/commons-httpclient-3.1.jar:$HPSA_EAR_LIB/httpcore-4.2.1.jar:$HPSA_EAR_LIB/mail-
1.4.5.jar:$HPSA_EAR_LIB/neethi-3.0.2.jar:$HPSA_EAR_LIB/wsdl4j-1.6.2.jar:$HPSA_EAR_LIB/XmlSchema-
1.4.7.jar
```

```
for file in $LIB/*.jar
do
   CLASSPATH=$CLASSPATH:$file
done

if [ "$1" = "start" ]
then
      echo Starting $SCRIPTNAME
      echo  "$JAVADIR/java $JAVA_OPTS -classpath $CLASSPATH com.hp.sosa.Main start $CONFIGFILE
$CONFIGFILE_DTD >$LOGDIR/$SCRIPTNAME.stdout 2> $LOGDIR/$SCRIPTNAME.stderr "
      $JAVADIR/java $JAVA_OPTS -classpath $CLASSPATH com.hp.sosa.Main start $CONFIGFILE
$CONFIGFILE_DTD >$LOGDIR/$SCRIPTNAME.stdout 2> $LOGDIR/$SCRIPTNAME.stderr & echo $!>
$TMPDIR/$SCRIPTNAME.pid
elif [ "$1" = "startdebug" ]
then
      echo Starting $SCRIPTNAME
      echo  "$JAVADIR/java $JAVA_DEBUG $JAVA_OPTS -classpath $CLASSPATH com.hp.sosa.Main start
$CONFIGFILE $CONFIGFILE_DTD >$LOGDIR/$SCRIPTNAME.stdout 2> $LOGDIR/$SCRIPTNAME.stderr "
      $JAVADIR/java $JAVA_DEBUG $JAVA_OPTS -classpath $CLASSPATH com.hp.sosa.Main start $CONFIGFILE
$CONFIGFILE_DTD >$LOGDIR/$SCRIPTNAME.stdout 2> $LOGDIR/$SCRIPTNAME.stderr & echo $!>
$TMPDIR/$SCRIPTNAME.pid

elif [ "$1" = "stop" ]
then
      echo Stoping $SCRIPTNAME
      echo $JAVADIR/java -D$SCRIPTNAME -Dlog4j.configuration=$LOG4JFILE -classpath $CLASSPATH
com.hp.sosa.Main stop
      $JAVADIR/java -D$SCRIPTNAME -Dlog4j.configuration=$LOG4JFILE -classpath $CLASSPATH
com.hp.sosa.Main stop
elif [ "$1" = "restart" ]
then
      echo Stoping $SCRIPTNAME
      echo $JAVADIR/java -D$SCRIPTNAME -Dlog4j.configuration=$LOG4JFILE -classpath $CLASSPATH
com.hp.sosa.Main stop
      $JAVADIR/java -D$SCRIPTNAME -Dlog4j.configuration=$LOG4JFILE -classpath $CLASSPATH
com.hp.sosa.Main stop
      echo Starting $SCRIPTNAME
      echo  "$JAVADIR/java $JAVA_OPTS -classpath $CLASSPATH com.hp.sosa.Main start $CONFIGFILE
$CONFIGFILE_DTD >$LOGDIR/$SCRIPTNAME.stdout 2> $LOGDIR/$SCRIPTNAME.stderr "
      $JAVADIR/java $JAVA_OPTS -classpath $CLASSPATH com.hp.sosa.Main start $CONFIGFILE
$CONFIGFILE_DTD >$LOGDIR/$SCRIPTNAME.stdout 2> $LOGDIR/$SCRIPTNAME.stderr & echo $!>
$TMPDIR/$SCRIPTNAME.pid
elif [ "$1" = "restartdebug" ]
then
      echo Stoping $SCRIPTNAME
      echo $JAVADIR/java -D$SCRIPTNAME -Dlog4j.configuration=$LOG4JFILE -classpath $CLASSPATH
com.hp.sosa.Main stop
      $JAVADIR/java -D$SCRIPTNAME -Dlog4j.configuration=$LOG4JFILE -classpath $CLASSPATH
com.hp.sosa.Main stop
      echo Starting $SCRIPTNAME
      echo  "$JAVADIR/java $JAVA_DEBUG $JAVA_OPTS -classpath $CLASSPATH com.hp.sosa.Main start
$CONFIGFILE $CONFIGFILE_DTD >$LOGDIR/$SCRIPTNAME.stdout 2> $LOGDIR/$SCRIPTNAME.stderr "
      $JAVADIR/java $JAVA_DEBUG $JAVA_OPTS -classpath $CLASSPATH com.hp.sosa.Main start $CONFIGFILE
$CONFIGFILE_DTD >$LOGDIR/$SCRIPTNAME.stdout 2> $LOGDIR/$SCRIPTNAME.stderr & echo $!>
$TMPDIR/$SCRIPTNAME.pid

elif [ "$1" = "test" ]
then
      echo Testing $SCRIPTNAME
      #echo $JAVADIR/java -D$SCRIPTNAME -Dlog4j.configuration=$LOG4JFILE -classpath $CLASSPATH
com.hp.sosa.Main test
      $JAVADIR/java -D$SCRIPTNAME -Dlog4j.configuration=$LOG4JFILE -classpath $CLASSPATH
com.hp.sosa.Main test
```

```
else
      echo "Usage: start|startdebug|stop|test"
fi

cd $MY_PWD
```

3.6.7 HPE SA Extension Pack - SOSA: `sosa.xml`

Path	File
`/opt/OV/ServiceActivator/EP/SOSA/conf/`	`sosa.xml`

In **both nodes**, the content for file `/opt/OV/ServiceActivator/EP/SOSA/conf/sosa.xml` is:

```
# cat /opt/OV/ServiceActivator/EP/SOSA/conf/sosa.xml
<?xml version="1.0" encoding="utf-8" ?>
<Modules>
      <Module name="sosaModule" className="com.hp.sosa.modules.sosamodule.SosaModule">
            <Parameter name="sosa.conf.file" value="conf/sosa_conf.xml" />
            <Parameter name="sosa.conf.dtd.file" value="conf/sosa_conf.dtd" />
            <Parameter name="jetty.start" value="true" />
      </Module>
      <Module name="timeWindowModule"
className="com.hp.sosa.modules.timewindowmodule.TimeWindowModule">
            <Parameter name="db.pool.name" value="db_time_window_module" />
            <Parameter name="db.user" value="<HPSA_database_user>" />
            <Parameter name="db.password" value="<HPSA_database_password_encrypted>" />
            <Parameter name="db.jdbc.driver" value="oracle.jdbc.driver.OracleDriver" />
            <Parameter name="db.url"
value="jdbc:oracle:thin:@(DESCRIPTION=(LOAD_BALANCE=on)(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCP)(
HOST=<db_host>)(PORT=<db_port>)))(CONNECT_DATA=(SERVICE_NAME=<db_instance>)))" />
            <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" />
      </Module>

</Modules>
```

3.6.8 HPE SA Extension Pack - SOSA: `sosa_conf.xml`

Path	File
`/opt/OV/ServiceActivator/EP/SOSA/conf/`	`sosa_conf.xml`

- In **both nodes**, the `<Queues>` section has to be:

```
<Queues>
      <Queue name="basic" className="com.hp.sosa.modules.sosamodule.queues.basic.BasicQueue" >
         <Parameter name="queue.threads" value="1"/>
         <Parameter name="queue.maxparallelism" value="10"/>
         <Sae name="MWFM_SA_EXECUTOR" medium_load="100" load_threshold="0"/>
          <Sae name="MWFM_SA_EXECUTOR_STANDBY" medium_load="100" load_threshold="0"/>
      </Queue>
```

```
    <Queue name="mailqueue" className="com.hp.sosa.modules.sosamodule.queues.basic.BasicQueue" >
      <Parameter name="queue.threads" value="5"/>
      <Parameter name="queue.max.parallelism" value="2"/>
      <Sae name="MWFM_SA_EXECUTOR" medium_load="100" load_threshold="0"/>
      <Sae name="MWFM_SA_EXECUTOR_STANDBY" medium_load="100" load_threshold="0"/>
    </Queue>

    <Queue name="priority" className="com.hp.sosa.modules.sosamodule.queues.priority.PriorityQueue"
>
         <Parameter name="queue.threads" value="1"/>
         <Parameter name="queue.priorities" value="4"/>
         <Parameter name="queue.group" value="true"/>
         <Parameter name="queue.group.max.num" value="10"/>
         <Parameter name="queue.group.max.time" value="3000"/>
         <Sae name="MWFM_SA_EXECUTOR" medium_load="100" load_threshold="0"/>
         <Sae name="MWFM_SA_EXECUTOR_STANDBY" medium_load="100" load_threshold="0"/>
    </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>-->
</Queues>
```

- In **both nodes**, the `<ServiceActionExecutors>` section has to be:

```
  <ServiceActionExecutors>
         <ServiceActionExecutor name="MWFM_SA_EXECUTOR"
className="com.hp.sosa.modules.sosamodule.executors.mwfm.MwfmServiceActionExecutor"
max_parallelism="0">
                  <Parameter name="host" value="<node1_hostname>"/>
                  <Parameter name="port" value="2000"/>
                  <Parameter name="user" value="<hpsa_admin_user>"/>
                  <Parameter name="password" value="<hpsa_admin_password_encrypted>"/>
                  <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>
  <ServiceActionExecutor name="MWFM_SA_EXECUTOR_STANDBY"
className="com.hp.sosa.modules.sosamodule.executors.mwfm.MwfmServiceActionExecutor"
max_parallelism="0">
      <Parameter name="host" value="<node2_hostname>"/>
      <Parameter name="port" value="2000"/>
      <Parameter name="user" value="<hpsa_admin_user>"/>
      <Parameter name="password" value="<hpsa_admin_password_encrypted>"/>
      <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>
<!--<ServiceActionExecutor name="NFVD_SA_EXECUTOR" class-
Name="com.hp.sosa.modules.sosamodule.executors.nfvd.ServiceActionExecutorNFVD" max_parallelism="0"
/>-->
</ServiceActionExecutors>
```

- In **both nodes**, add the following Protocol Adapter configuration between `<ProtocolAdapters>` and `</ProtocolAdapters>` tag:

```
<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>
```

- In **both nodes**, add this section under <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>
```

- In **both nodes**, comment or remove (if it exists) the following content:

```
<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>

<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>
```

3.6.9 HPE SA Extension Pack - SOSA: `alias.xml`

Path	File

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

In **both nodes**, add the following entry between `<alias-definition> </alias-definition>` tag:

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

3.6.10 HPE SA Extension Pack - SOSA: `sosa_action_saver.xml`

Path	File
`/opt/OV/ServiceActivator/EP/SOSA/conf/`	`sosa_action_saver.xml`

In **both nodes**, the content for file `/opt/OV/ServiceActivator/EP/SOSA/conf/sosa_action_saver.xml` should be:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<SosaAction>
<Managers>
            <Manager name="HISTORY" status="resume"/>
            <Manager name="PERFORMANCE_STATUS" status="resume"/>
</Managers>
<ProtocolAdapters>
            <ProtocolAdapter name="RmiWFLTService" status="resume"/>
            <ProtocolAdapter name="RMI_PA" status="pause"/>
            <ProtocolAdapter name="NGWS_PA" status="resume"/>
</ProtocolAdapters>
<Queues>
            <Queue name="basic" status="unlock.open"/>
            <Queue name="priority" status="unlock.open"/>
            <Queue name="mailqueue" status="unlock.open"/>
</Queues>
<ServiceActionExecutors>
            <ServiceActionExecutor name="MWFM_SA_EXECUTOR" status="unlock"/>
            <ServiceActionExecutor name="MWFM_SA_EXECUTOR_STANDBY" status="unlock"/>
</ServiceActionExecutors>
</SosaAction>
```

3.6.11 HPE SA Extension Pack - SOSA: `hbm_persistence.cfg.xml`

Path	File
`/opt/OV/ServiceActivator/EP/SOSA/conf/`	`hbm_persistence.cfg.xml`

In **both nodes**, configure the database connection in `<session-factory>` section:

```
[...]
```

```
<session-factory>
        <!-- Database connection settings -->
        <property name="hibernate.connection.driver_class">oracle.jdbc.driver.OracleDriver</property>
        <property
name="hibernate.connection.url">jdbc:oracle:thin:@(DESCRIPTION=(LOAD_BALANCE=on)(ADDRESS_LIST=(A
DDRESS=(PROTOCOL=TCP)(HOST=<db_host>)(PORT=<db_port>)))(CONNECT_DATA=(SERVICE_NAME=<db_in
stance>)))</property>
        <property name="hibernate.connection.username"><hpsa_db_user></property>
        <property name="hibernate.connection.password"><hpsa_db_password_encrypted></property>
[...]
```

3.6.12 HPE SA Extension Pack - SOSA: `hbm_mixedpersistence.cfg.xml`

Path	File
`/opt/OV/ServiceActivator/EP/SOSA/conf/`	`hbm_mixedpersistence.cfg.xml`

In **both nodes**, configure the database connection in `<session-factory>` section:

```
[...]
<session-factory>
        <!-- Database connection settings -->
        <property name="hibernate.connection.driver_class">oracle.jdbc.driver.OracleDriver</property>
        <property
name="hibernate.connection.url">jdbc:oracle:thin:@(DESCRIPTION=(LOAD_BALANCE=on)(ADDRESS_LIST=(A
DDRESS=(PROTOCOL=TCP)(HOST=<db_host>)(PORT=<db_port>)))(CONNECT_DATA=(SERVICE_NAME=<db_in
stance>)))</property>
        <property name="hibernate.connection.username"><hpsa_db_user></property>
        <property name="hibernate.connection.password"><hpsa_db_password_encrypted></property>
[...]
```

3.6.13 HPE SA Extension Pack - SOSA: `hbm_history.cfg.xml`

Path	File
`/opt/OV/ServiceActivator/EP/SOSA/conf/`	`hbm_history.cfg.xml`

In **both nodes**, configure the database connection in `<session-factory>` section:

```
[...]
<session-factory>
        <!-- Database connection settings -->
        <property name="hibernate.connection.driver_class">oracle.jdbc.driver.OracleDriver</property>
        <property
name="hibernate.connection.url">jdbc:oracle:thin:@(DESCRIPTION=(LOAD_BALANCE=on)(ADDRESS_LIST=(A
DDRESS=(PROTOCOL=TCP)(HOST=<db_host>)(PORT=<db_port>)))(CONNECT_DATA=(SERVICE_NAME=<db_in
stance>)))</property>
        <property name="hibernate.connection.username"><hpsa_db_user></property>
        <property name="hibernate.connection.password"><hpsa_db_password_encrypted></property>
[...]
```

3.6.14 HPE SA Extension Pack - SOSA: `hibernate_persistence_hsqldb.cfg.xml`

Path	File
`/opt/OV/ServiceActivator/EP/SOSA/conf/`	`hibernate persistence hsqldb.cfg.xml`

In **both nodes**, configure the database connection in `<session-factory>` section:

```
[…]
<session-factory>
                <!-- Database connection settings -->
                <property name="hibernate.connection.driver_class">oracle.jdbc.driver.OracleDriver</property>
                <property
name="hibernate.connection.url">jdbc:oracle:thin:@(DESCRIPTION=(LOAD_BALANCE=on)(ADDRESS_LIST=(A
DDRESS=(PROTOCOL=TCP)(HOST=<db_host>)(PORT=<db_port>)))(CONNECT_DATA=(SERVICE_NAME=<db_in
stance>)))</property>
                <property name="hibernate.connection.username"><hpsa_db_user></property>
                <property name="hibernate.connection.password"><hpsa_db_password_encrypted></property>
[…]
```

3.6.15 HPE SA Extension Pack - SOSA: `sosa-util.properties.xml`

Path	File
`/opt/OV/ServiceActivator/EP/SOSA/properties/`	`sosa-util.properties`

In **both nodes**, configure the RMI server IP address:

```
#############
# SOSA UTIL #
#############


rmi.server.ip=<sosa-vip-hostname-or-ip>
rmi.server.port=1119
rmi.server.wait.msg=100
rmi.server.wait.retries=100
[…]
```

3.6.16 HPE SA Extension Pack - SOSA: `sosa.sh`

Path	File
`/opt/OV/ServiceActivator/EP/SOSA/bin/`	`sosa.sh`

In both nodes, we need to change the sosa startup script to add a java configuration property when it starts. So we have to add the highlighted lines to the script:

```
#!/bin/sh

MY_PWD=`pwd`

export BASEDIR=/opt/OV/ServiceActivator/EP/SOSA
cd $BASEDIR

export JAVA_HOME=/usr/java/default
export JAVADIR=$JAVA_HOME/bin
export CONFDIR=conf
export TMPDIR=tmp
export LOGDIR=log
export PROPERTIES=properties
export LIB=lib


export HPSA_EAR_LIB=/opt/HP/jboss/standalone/deployments/hpsa.ear/lib
export LOG4JFILE=properties/sosa-log4j.properties
export JAVA_DEBUG="-Xdebug -Xrunjdwp:transport=dt_socket,address=8787,server=y,suspend=n"
#export JAVA_VERBOSEGC="-verbose:gc  -Xloggc:$LOGDIR/verbose_sosa3.log.gc -XX:+PrintGCDetails -
XX:+PrintGCTimeStamps"
#export JAVA_VERBOSEGC="-Xverbosegc:file=$LOGDIR/verbose_sosa3.log.gc -XX:+HeapDump"
export JAVA_VERBOSEGC=""
#export JAVA_VERBOSEGC="-XX:+HeapDumpOnOutOfMemoryError -verbose:gc  -
Xloggc:$LOGDIR/verbose_sosa31.log.gc "
#export JAVA_PERFORMANCE="-Xrunhprof:file=$LOGDIR/sosa3.hprof.txt"
#export JAVA_PERFORMANCE="-
Xrunhprof:thread=y,heap=all,depth=8,cutoff=0.0002,doe=y,cpu=times,file=$LOGDIR/sosa3.hprof.txt"
export JAVA_PERFORMANCE=""
export JAVA_XMX="-Xmx2048m"
export JAVA_XMS="-Xms512m"

export SCRIPTNAME=sosa
export CONFIGFILE=$CONFDIR/sosa.xml
export CONFIGFILE_DTD=$CONFDIR/sosa.dtd
export RMI_HOSTNAME=<sosa-vip-hostname-or-ip>

export JAVA_OPTS="-D$SCRIPTNAME -Djava.security.policy=$CONFDIR/sosa.policy -
Dlog4j.configuration=$LOG4JFILE $JAVA_XMS $JAVA_XMX $JAVA_VERBOSEGC $JAVA_PERFORMANCE -
Djava.rmi.server.hostname=${RMI_HOSTNAME}"
```

3.6.17 HPE SA Extension Pack - LockManager: `StartServer.sh`

Path	File
`/opt/OV/ServiceActivator/EP/LockManager/bin/`	`StartServer.sh`

In **both nodes**, you have to change the values for `StartServer.sh` file located in `/opt/OV/ServiceActivator/EP/LockManager/bin/`:

```
# vi /opt/OV/ServiceActivator/EP/LockManager/bin/StartServer.sh
#!/bin/sh

. /opt/OV/ServiceActivator/EP/LockManager/bin/setenv.sh

echo "Starting RMI service ${RMI_SERVICE} on rmi://${RMI_HOST}:${RMI_PORT}/${RMI_SERVICE_NAME}"

JVM_MEMORY="-Xms1024M -Xmx1024M -Xmn512M"
#JVM_PROF="-Xeprof:inlining=disable"
```

```
# HPjmeter
#SHLIB_PATH=${SHLIB_PATH}:/opt/hpjmeter/lib/PA_RISC2.0
#HPJMETER_OPTS=" -Xbootclasspath/a:/opt/hpjmeter/lib/agent.jar -Xrunjmeter "
#export SHLIB_PATH

JAVA_OPTS="${JVM_MEMORY} ${HPJMETER_OPTS} ${JVM_PROF}"

CMD=${JAVA_HOME}"/bin/java"
CMD=${CMD}" "${JAVA_OPTS}
CMD=${CMD}" -server"
[ "`uname -s`" = "HP-UX" ] && CMD=${CMD}" -XdoCloseWithReadPending"
CMD=${CMD}" -Djava.hp.spain.process.id=${RMI_SERVICE}"
CMD=${CMD}" -Djava.rmi.server.codebase=file:${RMI_PUB_DIR}/"
CMD=${CMD}" -Djava.rmi.server.logCalls=false"
CMD=${CMD}" -Djava.rmi.server.hostname=${RMI_STUB_EXPORT_HOST}"
CMD=${CMD}" -Djava.security.policy=${CFG_DIR}/${RMI_SERVICE_NAME}.policy"
CMD=${CMD}" -classpath "${CLASSPATH}
CMD=${CMD}" "${RMI_SERVICE}" "${RMI_HOST}" "${RMI_PORT}" "${BASE_DIR}

${CMD} > ${LOG_DIR}/${RMI_SERVICE_NAME}.stdout 2>${LOG_DIR}/${RMI_SERVICE_NAME}.stderr &

echo "Saving pid in ${BASE_DIR}/tmp/lckmgr.pid"
echo $! > ${BASE_DIR}/tmp/lckmgr.pid

echo "Done. Check ${LOG_DIR} for details."
```

3.6.18 HPE SA Extension Pack - LockManager: `LockManager.properties`

Path	File
`/opt/OV/ServiceActivator/EP/LockManager/conf/`	`StartServer.sh`

In **both nodes**, configure database parameters:

```
#
#Generic parameters
#
LOCK_PENDING_PERIOD = 5000
LOCK_PENDING_TIMEOUT = 600000
DEAD_LOCK_RISK_THRESHOLD_TIME = 60000
KEY_MONITOR_WAIT_TIMEOUT = 0
ADMINISTRATOR_LOCKER_NAMES = SUPERLOCKER_WEB_1, SUPERLOCKER_WEB_2, SUPERLOCKER_CMD

#
#File persistence parameters
#
#PERSISTENCE_CLASS = com.hp.spain.lock.manager.FileDataSource
#PERSISTENCE_DIR_PATH = /opt/OV/ServiceActivator/EP/LockManager/data

#
#Database persistence parameters
#
PERSISTENCE_CLASS = com.hp.spain.lock.manager.JdbcDataSource
POOL_JDBCDRIVER = oracle.jdbc.driver.OracleDriver
POOL_MAXACTIVE = 20
DATABASE_CONNECTION_URI =
jdbc:oracle:thin:@(DESCRIPTION=(LOAD_BALANCE=on)(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCP)(HOST=<db_host>)(PORT=<db_port>)))(CONNECT_DATA=(SERVICE_NAME=<db_instance>)))
```

```
USERNAME = <hpsa_db_user>
PASSWORD = <hpsa_db_password_encrypted>

#
#Tracking parameters
#
LOG_MAX_FILE_SIZE = 5242880
LOG_MAX_NUM_FILES = 10
LOG_PATTERN = %d [%t] %-5p %c\{1} - %m %n
LOG_LEVEL = DEBUG

POOL_MANAGE_ABANDONED = false
POOL_ABANDONED_TIMEOUT = 300
```

3.6.19 HPSA Extension Pack web: `sosa3.properties`

Path	File
`/opt/HP/jboss/standalone/deployments/hpsa.ear/ep.war/properties/`	`Sosa3.properties`

In case you want the EP web to work, you need to change this file in both nodes to:

```
sosamanager.service.host = <sosa-vip-hostname-or-ip>
sosamanager.service.port = 1119
sosamanager.service.name = SosaClient
timewindowmanager.service.name = TimeWindowService

dir.sosa.history.images.path = /opt/HP/jboss/standalone/deployments/hpsa.ear/ep.war/images/sosa-web/

persistence.service.timerefresh = 5000

sosa.history.serviceaction.column0=type
sosa.history.serviceaction.column1=service
sosa.history.serviceaction.column2=action
sosa.history.serviceaction.column3=protocolAdapterName
sosa.history.serviceaction.column4=queueName
sosa.history.serviceaction.column5=userName
sosa.history.serviceaction.column6=code
sosa.history.serviceaction.column7=sosaCode
sosa.history.serviceaction.column8=sosaDescription
sosa.history.serviceaction.column9=id
sosa.history.serviceaction.column10=creationDate
sosa.history.serviceaction.column11=finishDate
```

3.7 Monitoring tools

The HA monitoring scripts are part of the RPM and they will be located under the folder */opt/HPE/nfvd/fulfillment/scripts/*.

All the configuration changeable for a script will be available as a variable in the header of the script. There will be two different pairs of scripts:

- **nfvd_jboss_restart.sh**: this script can stop and start the Jboss instance of a machine.

By default, it logs to *
/var/opt/OV/ServiceActivator/log/nfvd_checker/nfvd_jboss_restart.log*

- **nfvd_jboss_check.sh**: this script will be responsible of checking the existence of the Jboss process that is serving both MWFM and FF API.

  If the jboss process is not present, it will invoke the restart script to try to start the Jboss process, maximum 3 times.

  After the third time, it will log a failure and it will not try to start Jboss anymore.
  By default, it logs to*/var/opt/OV/ServiceActivator/log/nfvd_checker/nfvd_jboss_check.log*. Number of retries will be stored in */var/opt/OV/ServiceActivator/tmp/jboss_retries* by default.

- **nfvd_sosa_lm_restart.sh:** this script can stop and start SOSA and LockManager locally in the machine.

  By default, it logs to
  /var/opt/OV/ServiceActivator/log/nfvd_checker/nfvd_sosa_lm_restart.log.

- **nfvd_sosa_lm_check.sh**: this script will be responsible of checking the existence of the SOSA and LockManager processes in an active/passive HA configuration.

  If the any of the processes are not present, it will invoke the restart script to try to start them, maximum 3 times.

  After the third time, it will log a failure and it will not try to start Jboss anymore.

  By default, it logs to
  /var/opt/OV/ServiceActivator/log/nfvd_checker/ nfvd_sosa_lm_check.log.

  Number of retries will be stored in */opt/OV/ServiceActivator/EP/SOSA/tmp/sosa_retries* for SOSA, and */opt/OV/ServiceActivator/EP/LockManager/tmp/lock_manager_retries* for LockManager, by default.

3.7.1 Configuration

To install these scripts, you will need to place an entry in the crontab (execute ‘`crontab -e`’) for the HPSA installation user, like this:

```
*/5  *  *  *  * /opt/HPE/nfvd/fulfillment/scripts/nfvd_sosa_lm_check.sh
*/5  *  *  *  * /opt/HPE/nfvd/fulfillment/scripts/nfvd_jboss_check.sh
```

After that, we need to give them execution permissions:

```
chmod +x /opt/HPE/nfvd/fulfillment/scripts/*.sh
```

3.8 Shared disk (Image service – GUI)

GUI and Fulfillment need to share a folder in which all the images will be stored.

A NFS server is needed (typically in same virtual machine as openLDAP server) as pre-requiste.

NFS server configuration is out of the scope of this document.

You can follow instructions in some places in Internet like:

> Quick NFS Server configuration on Redhat 7 Linux System
> https://linuxconfig.org/quick-nfs-server-configuration-on-redhat-7-linux

3.8.1 NFS configuration in Fulfillment

You need to install the following packages in Fulfillment nodes in order to be able to mount the NFS exported directories shared by NFS server.

```
[root@ff-node ~]# yum install nfs-utils rpcbind
```

After that, start RPC service:

```
[root@ff-node ~]# service rpcbind start
```

Create a folder in your filesystem and mount the NFS exported directory:

```
[root@ff-node ~]# mkdir -p /mnt/nfs
[root@ff-node ~]# mount <NFS_server_IP>:<NFS_folder_shared_by_NFS_server> /mnt/nfs
```

If your server is, for example, 10.75.14.23, and it shares the '`/opt/nfs`' folder, you will have to execute the following:

```
[root@ff-node ~]# mount 10.75.14.23:/opt/nfs /mnt/nfs
```

If you want your Fulfillment nodes mount the NFS exported directory after reboot, you will have to add an entry in your `/etc/fstab` file like this:

```
10.75.14.23:/opt/nfs          /mnt/nfs  nfs        defaults              0 0
```

As Fulfillment nodes (`root` user) will read/write in that NFS folder as well as `uoc` user (GUI nodes) you have to keep in mind some considerations about folder permissions in that folder.

You can decide the best approach for read/write processes between Fulfillment (`root` user) and GUI (`uoc` user) nodes in that NFS shared folder.

One solution could be the following:

1) In NFS server, add a '`uoc`' user

```
[root@hpe-nfs-server ~]# adduser uoc
```

2) The uid (user ID) and gid (group ID) for that uoc user in NFS server has to be the same like in both UI nodes.

   In UI nodes, you can find the uid/gid for uoc user in `/etc/passwd`:

```
[root@nfvdhaui1 ~]# cat /etc/passwd
[…]
uoc:x:50010:4012::/export/home/uoc:/bin/bash
```

3) Go to `/etc/passwd` file, in NFS server, and search the uoc line. Modify that line with correct uid/gid you get from UI nodes:

```
uoc:x:50010:4012::/home/uoc:/bin/bash
```

4) Change (recursively) folder/files permissions (in GUI nodes) for the NFS shared folder

```
[root@nfvdhaui1 ~]# chown -R uoc.root /nfs/
[root@nfvdhaui2 ~]# chown -R uoc.root /nfs/
```

Once you have completed all the previous steps, your Fulfillment nodes (`root` user) will be able to write/read into NFS shared folder as well as GUI nodes (`uoc` user).

In GUI nodes, you will have to update Image service configuration file according to NFS shared folder:

```
[uoc@nfvdhaui1 ~]$ vi /opt/uoc2/image-uploader-service/config/application.js
module.exports.application = {

  nfvdEndPoint : 'http://nfvdhaff1:8080/nfvd',
  FINAL_PATH : '<NFS_shared_folder>',
  TMP_PATH : '.tmp/uploads',
  SUPER_TOKEN : '3778fe88-e71d-4004-86bc-3188f7fd450b',
  MAX_BYTES: 100000000000
};
```

Chapter 4 Monitor VMs Installation

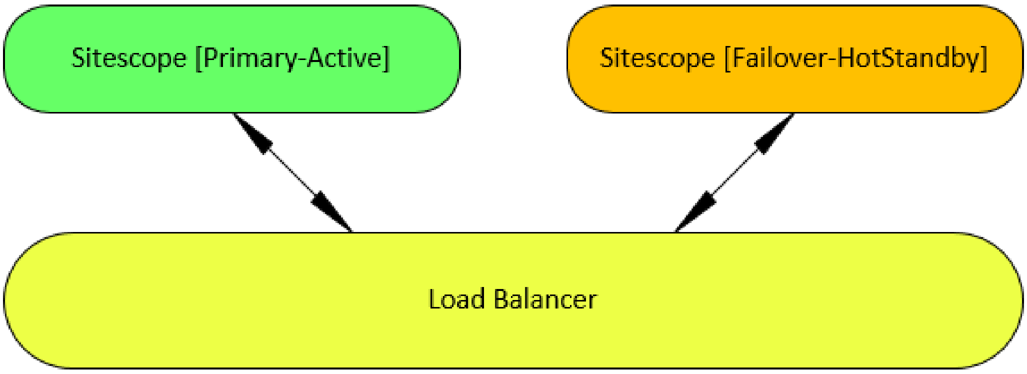
4.1 Pre-requisites:

1. All system and network configurations must be appropriate, for eg: hosts file entries, DNS configuration, NTP configurations, network connectivity, Disk volumes/partitioning in the below 'Hardware Specifications'.
2. Valid Premium licenses for Sitescope must be procured
3. It is recommended to have a complete High Availability solution for NFVD. By default NFVDirector may provide a few HA monitoring utilities which have limited features which are explained in the '4.1.1 Monitoring Tools' section.
4. Sitescope uses a pre-bundled Java installation

4.2 Set up

On each Monitor virtual machine install the following SW should be installed:

- Sitescope v11.30 and a patch v11.31



In the remaining part of the document, the following naming convention is used:

Naming	**Definition**
<PRIMARY_HOST>	Host that will act as Primary Host.
<SECONDARY_HOST>	Host that will act as Secondary Host [FailOver].
<ASSURANCE_GW_VIP>	Host for Assurance Gateway Load Balancer.

A Sample IP usage can be -

Naming	Hostname	Internal IP	Virtual IP
<PRIMARY_HOST>	nfvdhasi1	192.168.11.131	
<SECONDARY_HOST>	nfvdhasi2	192.168.11.132	
<Sitescope_VIP>	nfvdhasi-vip		10.100.62.134

Content for /etc/hosts file (both nodes):

```
# cat /etc/hosts
127.0.0.1   localhost localhost.localdomain localhost4
localhost4.localdomain4      nfvdhasi1
::1         localhost localhost.localdomain localhost6
localhost6.localdomain6
10.100.62.205   nfvddb-scan.elabs.hpe.com
192.168.11.131  nfvdhasi1
192.168.11.132  nfvdhasi2
192.168.11.114  nfvdhaaa-vip
10.100.62.130   openldap-vip
192.168.11.119  lockmanager-vip
192.168.11.119  sosa-vip
192.168.11.113  nfvd-api-vip
```

Note: Ensure to replace nfvdhasi1 to nfvdhasi2 in the the secondary

Hardware specifications are:

Server	**Internal IP**	**Flavor**	**vCPU**	**Memory**	**Total Ceph OS**	**Total Ceph APP**	**Total Shared**
nfvdhasi1	192.168.11.131	nfvd.ha.large	10	32G	50G	150G	-
nfvdhasi2	192.168.11.132	nfvd.ha.large	10	32G	50G	150G	-
Volume Group	Size	Logical Volume		Mount Point			Size
rhel	50G	Root		/			10G
		Home		/home			5G
		Opt		/opt			2G
		Usr		/usr			9G
		Var		/var			7G
		tmp		/tmp			8.5G
		swap		swap			8G
vgSI	150G	lvOptSI		/opt/HP/SiteScope			50G
		lvVarSI		/var/opt/HP/SiteScope			50G
		lvShSI		/var/opt/OV/shared			10G
		<< Free >>		<< Free >>			40G

On each Operational virtual machine install the following SW should be installed:
Sitescope Primary
Sitescope Secondary

4.3 Installation differences against non HA set up

Each Primary Monitor VM must be installed & configured as in the below mentioned steps

4.3.1 Each Secondary Monitor VM must be installed & configured as in the below mentioned steps for failover Mode

4.4 SiteScope High Availability setup

4.4.1 This involves the following steps in general:

4.4.2 Install SiteScope on a node [Virtual Machine] to act as primary SiteScope

4.4.3 Install SiteScope (same version as in step 1) as Failover SiteScope on another node identified for this purpose.

4.4.4 Installing SiteScope on primary node

Component	**Default Port**	**URL**
SiteScope User Interface	8080	http://<IPOrHostname>:8080/SiteScope
Tomcat shutdown	28005	
Tomcat AJP connector	28009	
JMX console port	28006	
Classic user interface	8888	
Classic user interface (secure) SSL port	8443	https://<IPOrHostname>:8443/SiteScope
SNMP Destination port	162	

Table: SiteScope default ports

Note

- Using SiteScope port as 8080 may clash with HPSA port which is also 8080 by default.
- The destination Port 162 must be opened up to receive SNMP traps.

For NFVDirector, the below steps are used for installation

1. As root user, run the installer.

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

2. Enter the number `2` to choose `2 – English` as the locale and press `Enter. [In case of any other locale, choose the relevant option]`

3. Press `Enter` when prompted for confirmation.

4. Press `Enter` to continue in the Introduction screen.

5. The text of the license agreement is displayed. The SiteScope License Agreement requires several pages to display. Read each page as it is presented. Press `Enter` to continue to the next page.

6. Type `Y` when prompted to accept the terms of License Agreement, and press `Enter`.

7. Enter `1` to select `1 - HP SiteScope: ()` as the setup type, and press `Enter`.

8. Enter the number `1` to choose `1 – HP SiteScope(Required)` option, and press `Enter`, in the `Select Features` screen.

9. Press Enter in the Install Requirements screen.

10. Press `Enter` to continue installation in the `Pre-Installation Summary` screen.

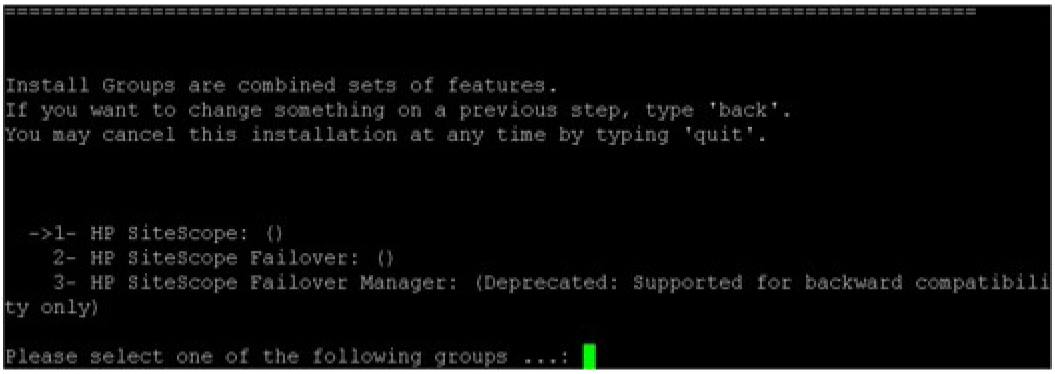
11. Type `1` to select the default port 8080 when the port prompt is displayed.

12. Type `2` to change the port and then type a different number in the `change port` prompt.

4.4.5 Installing SiteScope on failover node

Repeat the instructions as provided in Installing SiteScope on primary node. However, read the Notes below before proceeding with the installation.

Note:
Exercise caution on to choose the right options here for failover server setup.
Enter 2 among the options to select HP SiteScope Failover: () to install SiteScope on Failover server, and press Enter. Below screen shows the configuration window sample.



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


Install Groups are combined sets of features.
If you want to change something on a previous step, type 'back'.
You may cancel this installation at any time by typing 'quit'.



  ->1- HP SiteScope: ()
    2- HP SiteScope Failover: ()
    3- HP SiteScope Failover Manager: (Deprecated: Supported for backward compatibili
ty only)

Please select one of the following groups ...:
```

4.5 Sitescope Patch Installation

4.5.1 Install a sitescope patch: “sis1131concurrent_templ_deploy_deleteGroupEx.zip”.

This patch consists in a zip file containing some java classes under `com/mercury/sitescope` and the instructions are very minimalistic:
To apply the hotfix, perform the below steps -

1. Stop SiteScope if started up – *‘/etc/init.d/sitescope stop’*
2. Copy com folder from the attached zip to <SiS_HOME>\WEB-INF\classes

4.6 Install NFVD Sitescope Monitors and configuration

Note: Perform this operation on both nfvdhasi1 and nfvdhasi2

```
rpm -ivh nfvd-assur-gw-base-(version number).noarch.rpm
rpm -ivh nfvd-monitors-(version number).noarch.rpm
rpm -ivh nfvd-installer-(version number).noarch.rpm
rpm -ivh nfvd-ha-example-04.01.000-1.el6.noarch.rpm
```

Stop Sitescope

```
/opt/HP/SiteScope/stop
```

Import Sitescope templates

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

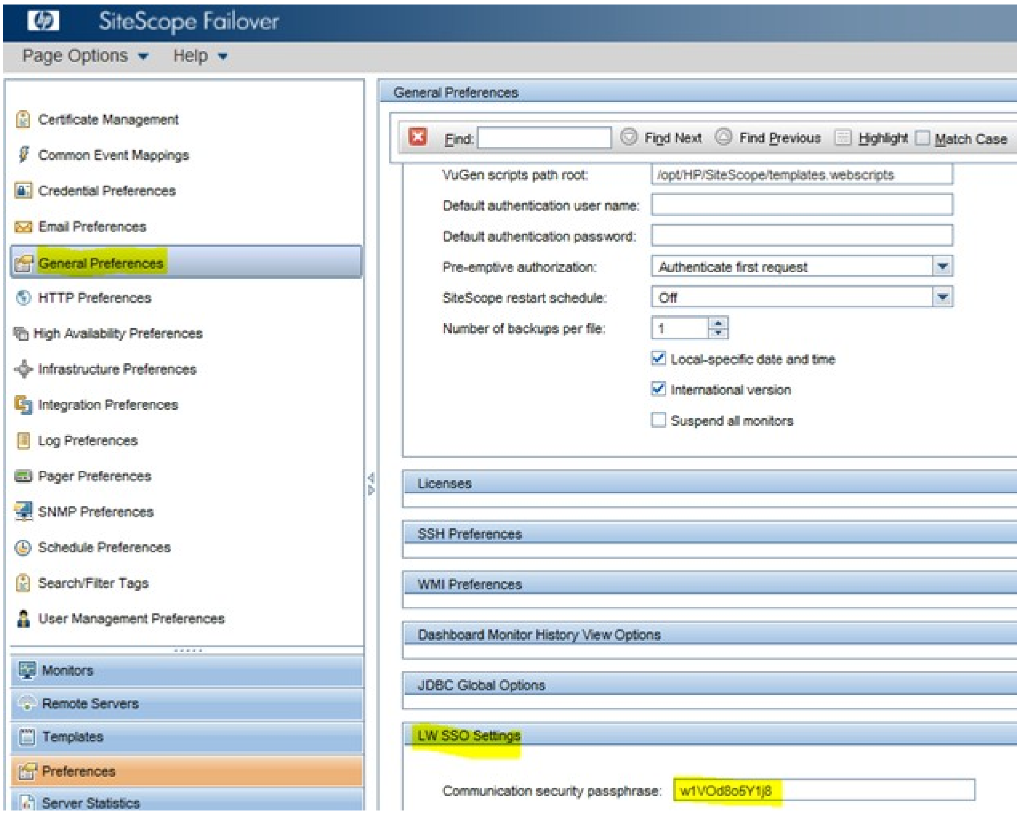
Start Sitescope

```
/opt/HP/SiteScope/start
```

4.7 Configuring SiteScope Failover node

Configure Lightweight Single Sign-on (LWSSO) for Authentication as follows:

1. Access the primary SiteScope user interface.
2. Select Preferences > General Preferences > LW SSO Settings. Copy the text from the Communication security passphrase field.
3. Access the SiteScope Failover user interface.
4. Navigate to Preferences > General Preferences > LW SSO Settings. Paste the communication security passphrase, and then click Save. Restart SiteScope Failover.



VuGen scripts path root: /opt/HP/SiteScope/templates.webscripts

Default authentication user name:

Default authentication password:

Pre-emptive authorization: Authenticate first request

SiteScope restart schedule: Off

Number of backups per file: 1

☑ Local-specific date and time

☑ International version

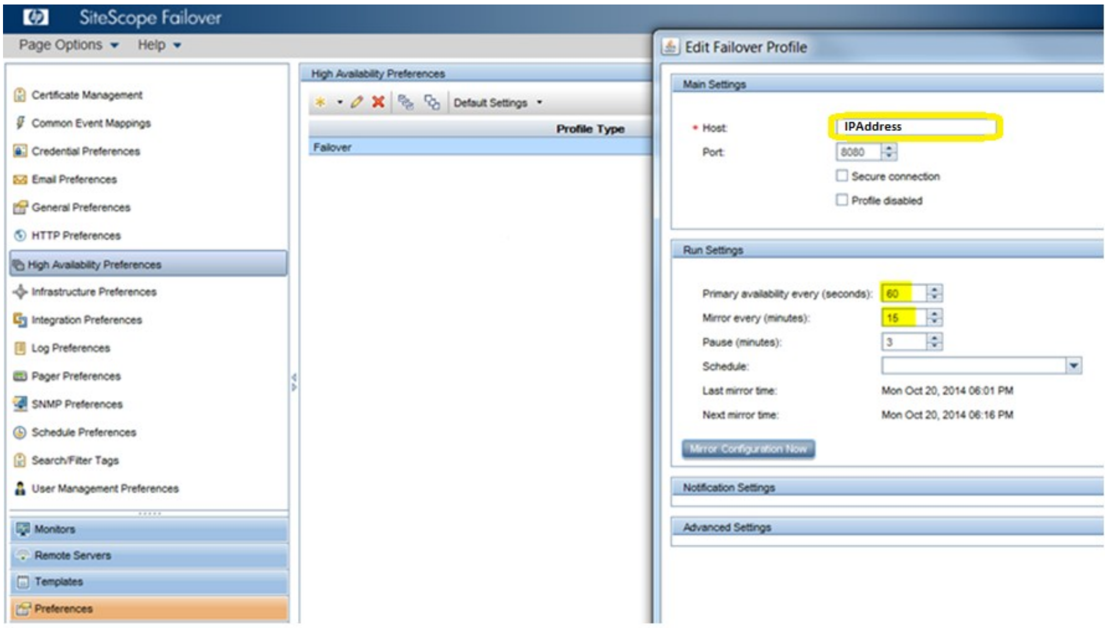
□ Suspend all monitors

Communication security passphrase: w1VOd8o5Y1j8

Figure 2 SiteScope Failover LW-SSO Setting

4.7.1 Create a new Failover Profile

In the Failover node UI, go to Preferences > High Availability Preferences.
In the right panel, click New Profile to open the New Failover Profile dialog.
Specify the settings as required [sample in screenshot below], and then click OK,
The value "Host" is the IP address of the Primary SiteScope.



* Host: IPAddress

Port: 8080

□ Secure connection

□ Profile disabled

Primary availability every (seconds): 60

Mirror every (minutes): 15

Pause (minutes): 3

Schedule:

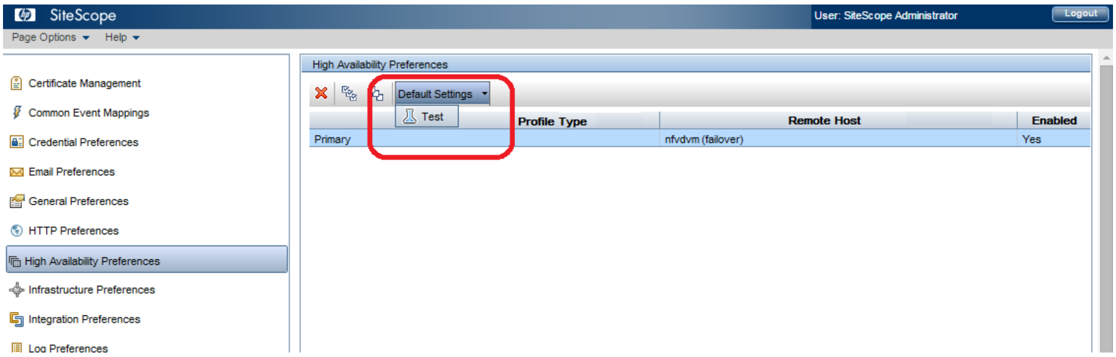
Last mirror time: Mon Oct 20, 2014 06:01 PM

Next mirror time: Mon Oct 20, 2014 06:16 PM

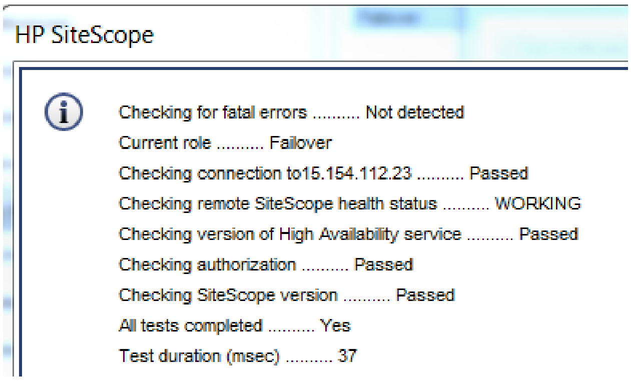
Figure 3 SiteScope Failover Profile Preferences

4.7.2 Verify Failover node settings

Login to SiteScope UI using Primary node IP. Go to Preferences > High Availability Preferences. Select Default Settings > Test.



	Profile Type	Remote Host	Enabled
Primary		nfvdvm (failover)	Yes



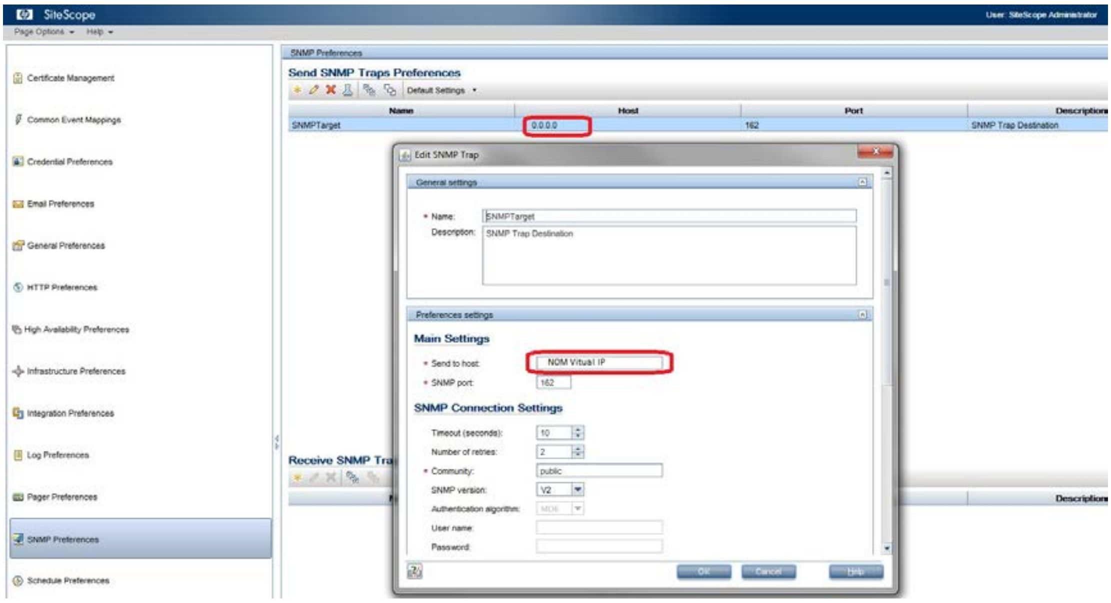
```
Checking for fatal errors .......... Not detected
Current role .......... Failover
Checking connection to15.154.112.23 .......... Passed
Checking remote SiteScope health status .......... WORKING
Checking version of High Availability service .......... Passed
Checking authorization .......... Passed
Checking SiteScope version .......... Passed
All tests completed .......... Yes
Test duration (msec) .......... 37
```

Figure 4 SiteScope Failover setup verification

Note
Perform the import operation first on Primary node followed by Failover node

4.8 Configure OpenMediation Endpoint in SiteScope

Login to SiteScope UI using Primary node IP. Go to Preferences > SNMP Preferences. Edit the SNMPTarget entry and provide the Virtual IP [nfvdhaaa-vip] configured for OM and click OK button. Perform the same steps on the Failover node also.



Send SNMP Traps Preferences

Name	Host	Port	Description
SNMPTarget	0.0.0.0	162	SNMP Trap Destination

Edit SNMP Trap

General settings

* Name: SNMPTarget

Description: SNMP Trap Destination

Preferences settings

Main Settings

* Send to host: NOM Vitual IP

* SNMP port: 162

SNMP Connection Settings

Timeout (seconds): 10

Number of retries: 2

* Community: public

SNMP version: V2

Authentication algorithm: MD5

User name:

Password:

4.9 Shared disk

The sitescope full system directory can be configured in …

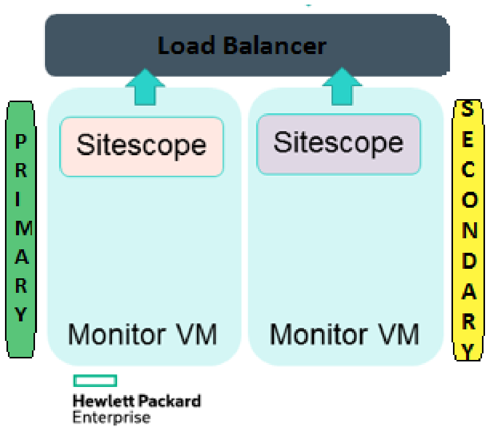
```
There is no requirement of a shared disk for sitescope
```

Each sitescope will be accesing the filesystem

1. Option 1
   a. An external cabin or even openstack cinder provides 2 volumes that are mounted one by each VM
2. Option 2
   a. Each VM defines a volume using the local disk

4.10 Connectivity and load balancer needs

The Loadbalancer hosts the VIP for Sitescope and redirects requests to Primary and then Secondary on a Priority basis.



Install xinetd-2.3.14-39.el6_4.x86_64.rpm in both the sitescope nodes

Edit /etc/services to have the below config at the end of the file, save and quit

```
sischkprm      8898/tcp            # sischkprm
```

Edit/ Create file - /etc/xinetd.d/sischkprm to have the below config at the end of the file, save and quit.

```
# default: on
# description: sischkprm
service sischkprm
{
      flags         = REUSE
      socket_type    = stream
      port          = 8898
      wait          = no
      user          = root
      server        = /opt/HPE/nfvd/solutions/ha-example/sis_check_primary.sh
      log_on_failure  += USERID
      disable        = no
      only_from      = 0.0.0.0/0
      per_source      = UNLIMITED
}
```

Restart xinetd

```
/etc/init.d/xinetd restart
```

4.10.1 Verify sitescope health service

On running the below checks in both the sitescope VMs, the outputs must be as below, else it indicates some issue in configuration

Check 1: Ports must be open

```
netstat -an | grep 8898
tcp       0      0 :::8898                  :::*                    LISTEN
```

Check 2:

```
[root@nfvdhasi1 ~]# wget http://nfvdhasi1:8898
--2016-08-09 01:50:35--  http://nfvdhasi1:8898/
Resolving nfvdhasi1... 127.0.0.1, 192.168.11.131
Connecting to nfvdhasi1|127.0.0.1|:8898... connected.
HTTP request sent, awaiting response... 200 NFVD SiteScope OK
Length: 25 [text/plain]
```

```
Saving to: “index.html”

100%[===================================================================
=======>] 25        --.-K/s   in 0s

2016-08-09 01:50:35 (5.14 MB/s) - “index.html” saved [25/25]

[root@nfvdhasi1 ~]# cat index.html
SiteScope is running.
```

4.11 Monitoring tools

sis_check.sh is an independent script registered to cron and triggered at regular intervals to check and ensure that the Sitescope process is OK of Sitescope on Primary and Secondary Node

The behavior of the script will be the following:

- If the machine is primary, it will check that sitescope processes are running.
- If the machine is standby, the script will do nothing.
- The script will end

Location of script: /opt/HPE/solutions/ha-example

4.11.1 Crontab monitoring entries in RHEL OS

1. Edit crontab using below command, add the entry in Sitescope VMs, save & quit [wq!]

```
crontab -e
*/5 * * * * /opt/HPE/solutions/ha-example/sis_check.sh
```

Note: The numeric highlighted in red – 5 is the frequency of the scripts to be triggered in minutes. It can be modified as per requirement. Please refer to man crontab for more inputs.

2. Provide execute permissions

```
chmod +x /opt/HPE/solutions/ha-example/sis_check.sh
```

3. Configure Virtual or Floating IP [set variables – SIS_VIP=192.x.x.x] in the script – ‘sis_check.sh’ before deploying them in the above mentioned location

4.11.2 Disable monitoring job

Edit crontab using below command, add comment or add ‘#’ entry in Assurance VMs and save->Quit [wq!]

```
crontab -e
#*/5 * * * * /opt/HPE/solutions/ha-example/sis_check.sh
```

Note: In case the cron job is still not stopped post the above change, a restart or the crond service can be performed as - /etc/init.d/crond restart

4.12 Administrative Operations:

Use the nfv-director.sh script located in /opt/HPE/nfvd/bin to start/stop or check status of any NFVD or assurance components as well

Check processes Status

```
/opt/HPE/nfvd/bin/nfv-director.sh status
```

Start Processes

```
/opt/HPE/nfvd/bin/nfv-director.sh start
```

Stop Processes

```
/opt/HPE/nfvd/bin/nfv-director.sh stop
```

Action with individual Processes

```
    # /opt/HPE/nfvd/bin/nfv-director.sh -h

    Administration tool for the NFVD solution

    Usage:

    [options] [-c nfvdComponent] <action>

    where action is one of start | stop | restart | status

    options:

-c nfvdComponent : NFVD Component on which the action is applied

One of: activator | sosa | ecpool | lockmgr | openmediation | sitescope | uca-
ebc | nfvd-agw | couchdb | uoc | idp | imageuploader

If not specified, the specified action applies to all installed NFVD components

-h : Displays this usage message

-v : Verbose mode
```

Chapter 5 Alarm VMs Installation

5.1 Pre-requisites

1. All system and network configurations must be appropriate, for eg: hosts file entries, DNS configuration, NTP configurations, network connectivity, Disk volumes/partitioning as mentioned in below *'Hardware Specifications'*.
2. Licenses for UCA-EBC and UCA-Automation must be procured
3. It is recommended to have a complete High Availability solution for NFVD. By default NFVDirector may provide a few HA monitoring utilities which have limited features covered as part of monitoring tools.
4. Oracle Database for usage
5. Java 1.7 [JAVA_HOME] for all products except for HPSA-UCA-Automation which requires Java 1.6 [JAVA6_HOME] should be installed

5.2 Set up

In the remaining part of the document, the following naming convention is used:

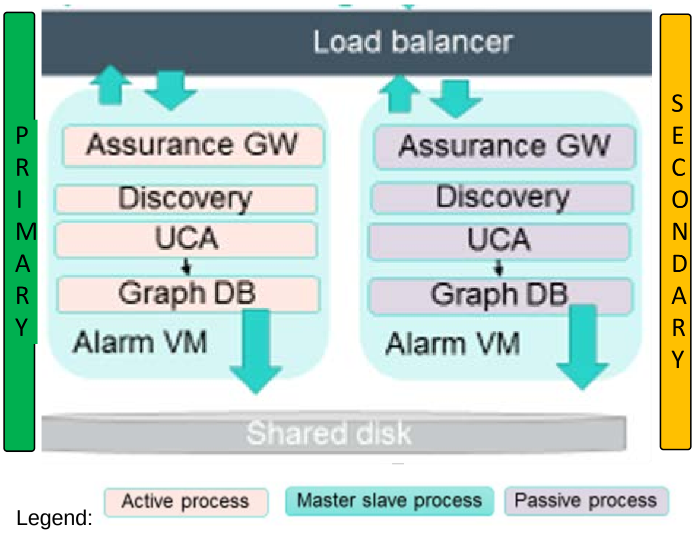
Naming	**Definition**
<PRIMARY_HOST>	Host that will act as Primary Host.
<SECONDARY_HOST>	Host that will act as Secondary Host.
<ORACLE_HOST>	Oracle RAC cluster where Oracle component is installed.
<SITESCOPE_VIP>	Host for Sitescope Load Balancer.

Sample IP-hostname configuration can be:

Naming	Hostname	Internal IP	Virtual IP
<PRIMARY_HOST>	nfvdhaaa1	192.168.11.121	
<SECONDARY_HOST>	nfvdhaaa2	192.168.11.122	
<ASSURANCE_GW_VIP>	assurance-gw-vip		192.168.11.114
<HB_VIP>			192.168.11.221

Content for /etc/hosts file (both nodes):

```
# cat /etc/hosts
127.0.0.1    localhost localhost.localdomain localhost4
localhost4.localdomain4      nfvdhaaa1
::1          localhost localhost.localdomain localhost6
localhost6.localdomain6
10.100.62.205   nfvddb-scan.elabs.hpe.com
192.168.11.121  nfvdhaaa1
192.168.11.122  nfvdhaaa2
192.168.11.114  nfvdhaaa-vip
192.168.11.113  nfvd-api-vip
10.100.62.134   nfvdhasi-vip
```



Server	**Internal IP**	**Flavor**	**vCPU**	**Memory**	**Total Ceph OS**	**Total Ceph APP**	**Total Shared**
nfvdhaaa1	192.168.11.121	nfvd.ha.large.largeram	10	64G	50G	150G	200G
nfvdhaaa2	192.168.11.122	nfvd.ha.large.largeram	10	64G	50G	150G	
Volume Group	Size	Logical Volume		Mount Point			Size
rhel	50G	root		/			10G
		home		/home			5G
		opt		/opt			2G
		usr		/usr			9G
		var		/var			7G
		tmp		/tmp			8.5G
		swap		swap			8G
vgAA	200G	lvolOM		/var/opt/openmediation-70			50G
		lvolUCA		/var/opt/UCA-EBC			50G
		lvolAGW		/var/opt/HPE/nfvd			50G
		lvolOptOM		/opt/openmediation-70			10G
		lvolOptUCA		/opt/UCA-EBC			5G
		lvolOptUCAA		/opt/UCA_Automation			5G
		lvolOptNFVD		/opt/HPE/nfvd			5G
		<< Free >>		<< Free >>			25G
NFS	1024G	NFS:/nfs-shares/images		/nfs/images			1024G

5.2.1 Installing Java

1. Navigate to /<PathTo>/BaseProduct/AA/JAVA,
2. Extract the tar file - jdk-7u60-linux-x64.tar.gz using –

```
cp jdk-7u60-linux-x64.tar.gz /usr/java
tar -xvf jdk-7u60-linux-x64.tar.gz
```

3. 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
```

5.3 Open Mediation High Availability setup

5.3.1 Installing Open Mediation on Primary node

5.3.1.1 Installing Open Mediation

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

```
# mkdir -p /tmp/nfvd
cd <PathOfNFVD_ISO_File>
tar -xvf NFVD40_BaseProduct.tar
cd /var/KITS/NFVD40-KIT/BaseProduct/AA/OPEN_MEDIATION
```

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

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

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

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

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

5.3.1.2 Setup Open Mediation

1. Comment out the lines in file - /opt/openmediation-70/bin/nom_install as below save and quit.

```
31 #      test ! -e "$path_nom_var_dir" \
32 #     || error_and_exit "NOM variable files directory $path_nom_var_dir already
                   exists"
```

Note: The above is necessary as a directory/volume - /var/opt/openmediation-70 is pre-created and we cannot proceed without this mandatory workaround

2. `Press [Enter]key` when prompted with confirmation to install.
3. `Press [Enter]key` when prompted for OM installation directory [/opt]:
4. `Press [Enter]key` 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):
[/var/opt/openmediation-70]  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.
```

5.3.2 Installing Open Mediation on Failover node

Installation OM on Failover node, same procedure as above can be used

Note

Configurations related to OM HA setup are explained as part of UCA-EBC HA setup in below sections.

5.4 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:8090/uca`
UCA-EBC JMX RMI port	1100	
UCA for EBC GUI port	8090	

5.4.1 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 /var/KITS/NFVD40-KIT/BaseProduct/AA/UCA
# cp uca-ebc-server-kit-3.1-linux.tar  /tmp
# cd /tmp
# tar xvf uca-ebc-server-kit-3.1-linux.tar
# ./install-uca-ebc.sh
```

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

           Installation of HP Unified Correlation Analyzer
                        For
                  Event Based Correlation

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

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

*          UCA EBC Server                                                    *
*                                                                            *
******************************************************************************

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

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

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

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

5.4.2 Installing UCA for EBC Server patch

5.4.2.1.1 Note

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

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

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

3. Login as root user
4. Go to EPatch kit directory

5. Run the command :

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

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

5.5 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	

UCA for EBC Topology Extension default ports

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

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

5.5.1 Installing UCA for EBC Topology Extension

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

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

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

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

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

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


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

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

*          UCA EBC Topology Extension                                  *
*                                                              *
 *******************************************************************************

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

5.5.2 Installing UCA for EBC Topology Extension Patch

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

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

5.5.3 Use 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.

5.5.4 Use an external topology server

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

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

1. Download Neo4J 1.9 Enterprise Edition from `http://www.neo4j.com`
2. Transfer the archive to a location where you want to install Neo4J, and extract.

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

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

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

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

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

5. Manually copy the following files to the Neo4J topology server `plugins` directory:

   - `/opt/UCA-EBC/lib/opencsv-2.3.jar`
   - `/opt/UCA-EBC/lib/scalalogging-slf4j_2.10-1.0.1.jar`
   - `/opt/UCA-EBC/lib/uca-ebc-topology-dataload-3.1.jar`
   - `/opt/UCA-EBC/lib/config-0.5.2.jar`

6. The following commands will start/stop/check status of Neo4J respectively.

   - `/home/neo4j/neo4j-enterprise-1.9.9/bin/neo4j start`
   - **`/home/neo4j/neo4j-enterprise-1.9.9/bin/neo4j stop`**
   - **`/home/neo4j/neo4j-enterprise-1.9.9/bin/neo4j status`**

Note

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

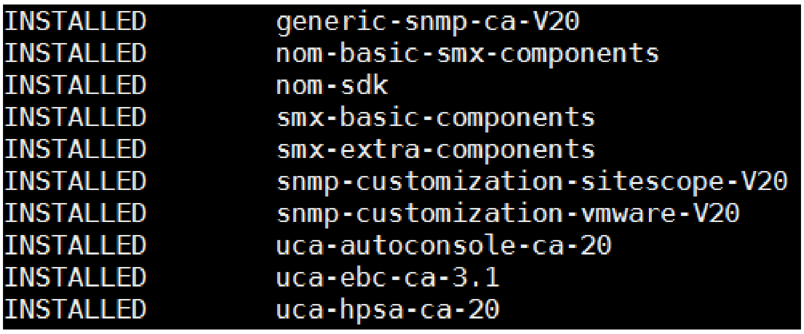
5.6 Installing Channel Adapters

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

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

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
```

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

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

5.6.1 Installing UCA for EBC CA

5.6.1.1.1.1 Run the installation script

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

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

5.6.1.1.3 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%]
```

5.6.1.2 Install UCA for EBC CA on OSS OM

5.6.1.2.1 Run the following command.

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

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

5.6.1.2.2 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
```

5.6.1.3 Install UCA for EBC CA on OSS OM container

5.6.1.3.1 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
```

5.6.1.3.2 Verify that the installation was successful.

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

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

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

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

5.6.1.3.2.2 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
```

5.6.1.4 Configure UCA for EBC CA

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

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

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

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

Restart the container.

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

5.6.1.5 Deploy UCA for EBC CA on OSS OM container

5.6.1.5.1 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
```

5.6.1.5.2 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
```

5.6.2 Installing Generic SNMP CA

Run the installation script

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

```
cd /var/KITS/NFVD40-KIT/BaseProduct/AA/CHANNEL_ADAPTERS
# tar xvf generic-snmp-ca-V200L01-RevB.tar.gz
# cd /tmp/generic-snmp-ca-V20
```

5.6.2.1 Install Generic SNMP CA in OM container

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
```

5.6.2.2 Deploy Generic SNMP CA in OM container

Check if container instance has started.

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

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

Start the container instance, if it is not running.

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

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
```

5.6.3 Installing SiteScope Customization for Generic SNMP CA

Run the installation script

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

```
cd /var/KITS/NFVD40-KIT/BaseProduct/AA/CHANNEL_ADAPTERS
# tar xvf snmp-customization-sitescope-V200L01-RevC.tar.gz
# cd /tmp/snmp-customization-sitescope-V20
```

5.6.3.1 Install SiteScope customization

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
```

5.6.3.2 Deploy the SiteScope customization within OM container

Check if the container instance has started.

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

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

Start the container instance, if it is not running.

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

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
```

5.6.4 Installing VMWare ESXi Customization for Generic SNMP CA

Run the install script

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

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

5.6.4.1 Install VMWare ESXi Customization for Generic SNMP CA

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
```

5.6.4.2 Deploy the VMWare ESXi customization within OM container

Check if the container instance has started.

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

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

Start the container instance, if it is not running.

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

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
```

5.7 Installing UCA Automation

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

Component	**Port to use**
UCA Automation UI	8090

5.7.1 Configure HP UCA for EBC

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

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

1. Restart UCA for EBC server.

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

```
# mkdir -p /tmp/ucaa
cd /var/KITS/NFVD40-KIT/BaseProduct/AA/UCA
# mount -o loop JP245-15001.iso /tmp/ucaa
cd /tmp/ucaa
```

3. Verify that the environment variable UCA_EBC_HOME is set to UCA-EBC Home Directory.

4. Copy the uca-automation-kit-1.2-linux.tar file to `/tmp` and install the package.

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

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

The package is installed under `/opt/UCA_Automation` directory.

5.7.2 Installing UCA Automation Patch

5.7.3 Note

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

1. As uca user, stop UCA for EBC.

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

2. As root, install the patch package

```
cd /var/KITS/NFVD40-KIT/BaseProduct/AA/UCA
# rpm -ivh EBCATM-12LIN-00003.noarch.rpm
```

It installs the package under the directory /opt/UCA_Automation/Patches/EBCATM12LIN_00003/UCA_Automation_UCA_VPs

1. Undeploy the UCA_Automation_Foundation_UCA-V1.2.2-1A and deploy the UCA_Automation_Foundation_UCA-vp-V1.2.3-1A contained in the Patch.

Stop and undeploy UCA-FVP

```
cd /opt/UCA-EBC/bin
./uca-ebc-admin --stop -vpn UCA_Automation_Foundation_UCA-vp -vpv 1.2.1-1A
./uca-ebc-admin --undeploy -vpn UCA_Automation_Foundation_UCA-vp -vpv 1.2.1-1A
rm -rf /var/opt/UCA-EBC/instances/default/valuepacks/UCA_Automation_Foundation_UCA-vp-V1.2.3-1A.zip
```

Copy the FVP patch to UCA-EBC

```
cp
${UCA_AUTOMATION_HOME}/Patches/EBCATM12LIN_00003/UCA_Automation_UCA_VPs/UCA_Automation
_Foundation_UCA-vp-V1.2.3-1A.zip /var/opt/UCA-EBC/instances/default/valuepacks
```

2. UCA_Automation_ChannelAdapters:

1. Edit the Foundation value pack version in config.properties in the ${NOM_INSTANCE}/ips/uca-autoconsole-ca-20/etc

uca.console.service=UCA_Automation_Foundation_UCA-V1.2.3-1A-UCAAutomation/UCAService

2. Undeploy and deploy the Automation Console Channel Adapter.

```
%nom_admin --undeploy-ip-in-container uca-autoconsole-ca-20
%nom_admin --deploy-ip-in-container uca-autoconsole-ca-20
```

3. Edit the Foundation value pack version in uca.ebc.properties in the ${UCA_EBC_DATA}/instances/default/conf/ UCA_Automation_Foundation_UCA-V1.2.3-1A-UCAAutomation-webapp-parameters=username=${user},userrole=${role}

4. Edit any Routes involving Foundation value pack. Modify the Foundation Value Pack version in ${UCA_EBC_INSTANCES}/conf/OrchestraConfiguration.xml file

5.7.4 Install NOM Channel Adapters

5.7.4.1 Installing UCA HPSA CA

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

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

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

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

```
# rpm -ivh --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
```

a. Modify the /var/opt/openmediation-70/ips/uca-hpsa-ca-20/etc/config.properties file.

i. hpsa.host= nfvdhaff-vip

ii. hpsa.port

iii. hpsa.userid

iv. hpsa.password

b. 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
```

5.7.4.2 Installing UCA Automation Console CA

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

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

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

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

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

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
```

Modify /var/opt/openmediation-70/ips/uca-autoconsole-ca-20/etc/config.properties.

uca.uca-automation.host

uca.uca-automation.port

uca.console.host

uca.console.port

uca.console.service=UCA_Automation_Foundation_UCA-V1.2.3-1A-UCAAutomation/UCAService

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
```

5.7.5 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.

5.7.5.1 Install, Import and Deploy HPSA Foundation Solution Pack

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

```
# scp /opt/UCA_Automation/UCA_Automation_HPSA_VPs/UCA_HPSA_FoundationVP-V12-1A.zip
user@nfvdhaff1:/opt/OV/ServiceActivator/SolutionPacks
```

Go to /opt/OV/ServiceActivator/bin directory.

Run the following command to import UCA solution pack.

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

Run the following command to deploy UCA.

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

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

NOTE: Run the above command on the Secondary node with -noSQL as an option

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

5.7.5.2 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 ]

nfvdhaa-vip

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
```

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://nfvdhaa-vip:8090/UCA_Automation_Foundation_UCA-V1.2.3-1A-
      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"/>
```

5.7.6 Installing UCA Automation’s UCA for EBC Foundation Value Pack

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

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

5.7.6.1 Deploy UCA for EBC Foundation VP

1. Copy the file - /opt/UCA_Automation/Patches/EBCATM12LIN_00001/UCA_Automation_UCA_VPs/UCA

_Automation_Foundation_UCA-vp-V1.2.1-1A.zip file to the /var/opt/UCA-EBC/instances/default/valuepacks directory.

```
# cp /opt/UCA_Automation/Patches/EBCATM12LIN_00001/UCA_Automation_UCA_VPs/UCA_Automation_Fou
n    dation_UCA-vp-V1.2.3-1A.zip /var/opt/UCA-EBC/instances/default/valuepacks
```

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

```
# su - uca
$ cd /opt/UCA-EBC/bin
$ ./uca-ebc-admin --deploy -vpn UCA_Automation_Foundation_UCA -vpv V1.2.3-1A
```

```
INFO  - Running Java HotSpot(TM) 64-Bit Server VM Version 1.7.0_60 (from Java(TM) SE Runtime
Environment, Oracle Corporation)
INFO  - Deploying [ UCA_Automation_Foundation_UCA, V1.2.3-1A, all scenarios ]
INFO  - Logging to org.slf4j.impl.Log4jLoggerAdapter(org.mortbay.log) via org.mortbay.log.Slf4jLog
INFO  - Value Pack name: UCA_Automation_Foundation_UCA-V1.2.3-1A has been successfully deployed
```

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

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

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

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

```
</logger>

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

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

5.7.6.2 Configure UCA for EBC Foundation VP

1. Edit the /var/opt/UCA-EBC/instances/default/deploy/UCA_Automation_Foundation_UCA-V1.2.3-1A/conf/UCAAutomation.properties file.
2. Update the localhost and port with UCA for EBC server hostname and port.

```
ucaebc_tomsawyer_port=http://nfvdhaaa-vip:8090/graphdisplay/?username=root&nodeId=0&profile=ucaatm
```

3. Update the database. Add # to the beginning of the lines or comment out for non relevant database details.

For Oracle database, update the following configuration.

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

4. Edit the /var/opt/UCA-EBC/instances/default/deploy/UCA_Automation_Foundation_UCA-V1.2.3-1A/conf/ExternalActionConfig.xml file.

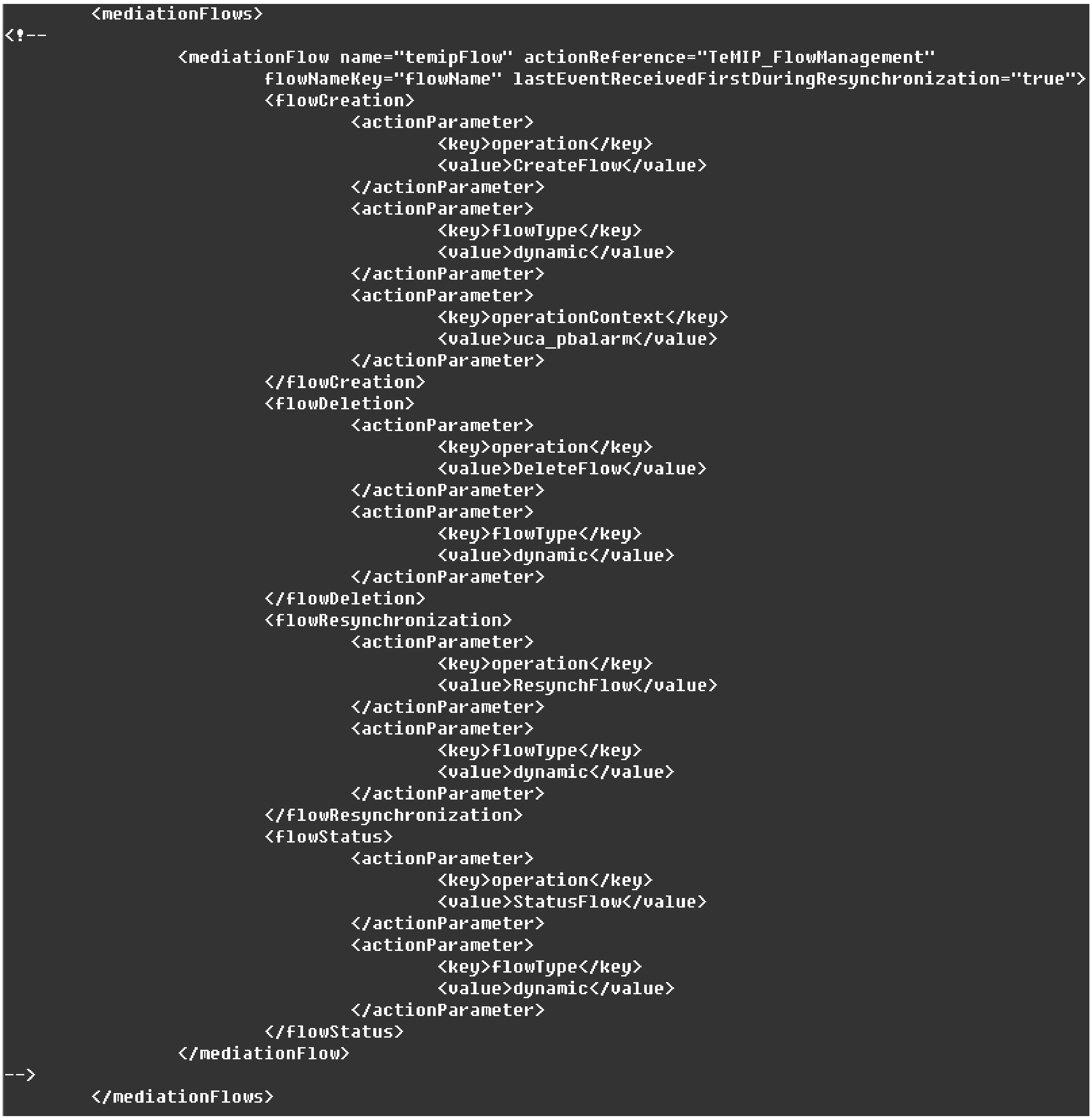
5. Update the localhost and port with UCA for EBC server hostname and port.

```
<consoleurl>
http://nfvdhaaa-vip:8090/UCA_Automation_Foundation_UCA-V1.2.3-1A-UCAAutomation/UCAService
</consoleurl>
  <!-- Foundation Value pack details  -->
 <valuepacks>
       <valuepack name="FVP">
              <vpName>UCA_Automation_Foundation_UCA</vpName>
              <version>V1.2.3-1A</version>
              <scenarioName>UCA_Automation_Foundation_UCA.requestresponse</scenarioName>
             </valuepack>
 </valuepacks>
```

6. Configure mediation flow in UCA for EBC Foundation VP

   Edit the file /var/opt/UCA-EBC/instances/default/deploy/UCA_Automation_Foundation_UCA-V1.2.3-1A/conf/ValuePackConfiguration.xml

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



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

Update UCA Auto Foundation VP ValuePackConfiguration.xml

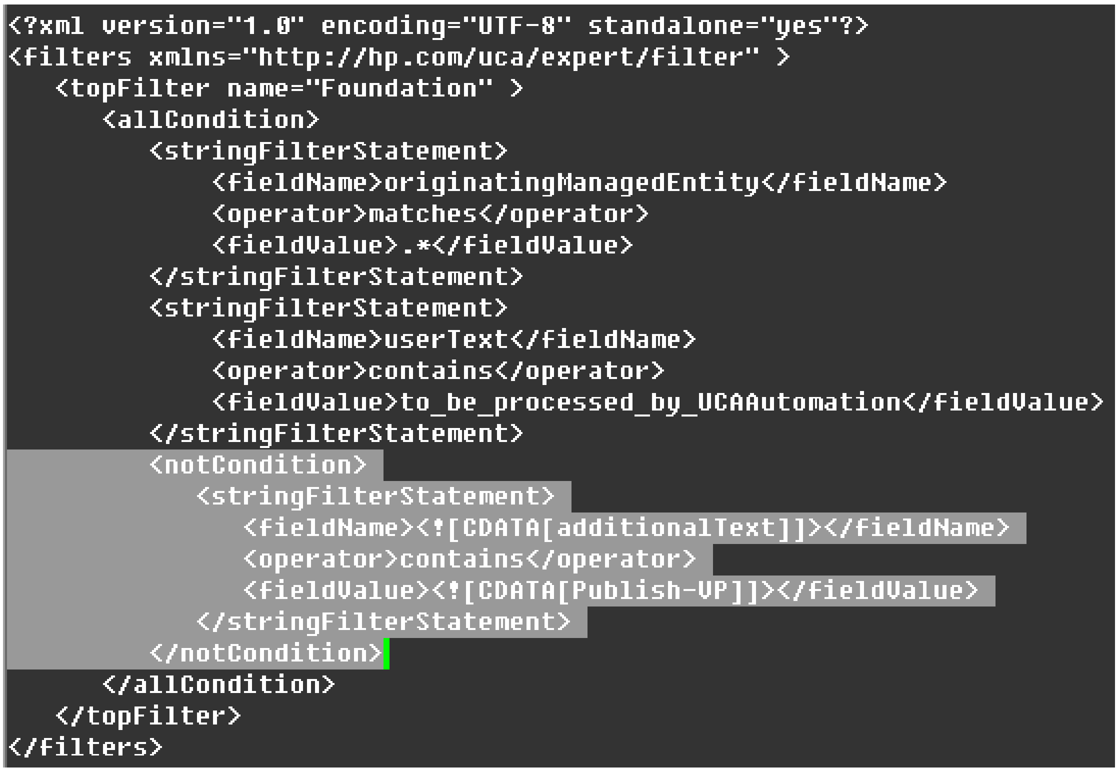
Save the file.

7. Filter Configuration in UCA Automation for NFVD

   a. Edit the file /var/opt/UCA-EBC/instances/default/deploy/UCA_Automation_Foundation_UCA-V1.2.3-1A/requestresponse/filters.xml

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

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



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

UCA EBC – Update UCA Auto Foundation VP filter.xml

b.Save the file.

c. Start the UCA Automation Foundation Value Pack.

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

```
$ ./uca-ebc-admin --start -vpn UCA_Automation_Foundation_UCA -vpv V1.2.3-1A
```

```
INFO - Running Java HotSpot(TM) 64-Bit Server VM Version 1.7.0_65 (from Java(TM) SE Runtime
Environment, Oracle Corporation)
INFO  - Starting [ UCA_Automation_Foundation_UCA, V1.2.3-1A, all scenarios ]
INFO  -  Logging  to  org.slf4j.impl.Log4jLoggerAdapter(org.mortbay.log)  via  org.mortbay.log.Slf4jLog
INFO - Status: [ UCA_Automation_Foundation_UCA, V1.2.3-1A, all scenarios ]Value pack has been
successfully started. Status of the value pack: Running
```

8. 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://nfvdhaaa-vip:18192/uca/mediation/action/ActionService?WSDL"
         brokerURL="failover://tcp://localhost:10000">
       <Action actionReference="NFV_Action_localhost">
             <ServiceName>alertService</ServiceName>
             <NmsName>localhost</NmsName>
         </Action>
</MediationValuePack>
```

Chapter 6 Install NFVD solution

6.1 Install NFVD RPMs

Source the RPMs & install them using below commands in the same order

Note

In case of a distributed/HA setup ensure to copy the rpms to the respective destination along with the rpm – ‘nfvd-assur-gw-base-(version number).noarch.rpm’.

Eg: nfvd-correlation(version number).noarch can be uninstalled where the product uca-ebc is installed and nfvd-alarms-omi(version number).noarch and so on

```
rpm -ivh nfvd-assur-gw-base-(version number).noarch.rpm
rpm -ivh nfvd-assur-gw-tpp-(version number).noarch.rpm
rpm -ivh nfvd-assur-gw-core-(version number).noarch.rpm
rpm -ivh nfvd-correlation-(version number).noarch.rpm
rpm -ivh nfvd-discovery-common-(version number).noarch.rpm
rpm -ivh nfvd-discovery-cmdb-(version number).noarch.rpm
rpm -ivh nfvd-alarms-omi-(version number).noarch.rpm
rpm -ivh nfvd-installer-(version number).noarch.rpm
rpm -ivh nfvd-ha-example-(version number).noarch.rpm
```

6.2 Install Open Mediation CAs

Install the various NFVD Channel Adapters based on need. Eg: If OMi is being used with discovery, both omi CA and CMDB CA have to be installed, else if Helion/Helion Carrier Grade/ Openstack discovery is required just the openstack CA has to be installed. Else all CAs can be used if OMi-RTSM discovery and openstack flavour discoveries are to be supported.

6.2.1 Setup OMI CA

Step-1: Unzip

```
unzip -d /opt/openmediation-70/ips/ /opt/HPE/nfvd/discovery/omi/omi-ca-1.0.0.zip
```

Step-2: Install the CA in openmediation container

```
nom_admin --install-ip omi-ca-10
```

Step-3: Install CA in nom-container (default container 0)

```
nom_admin --install-ip-in-container 0 omi-ca-10
```

Step-4: Edit CA properties

Edit the file /var/opt/openmediation-70/containers/instance-0/ips/omi-ca-10/etc/omi-nfvd.properties

```
omi.rest.endpoint=http://nfvdhaaa-vip:17870
```

Step-5 : Deploy CA in openmediation container

```
nom_admin --deploy-ip-in-container 0 omi-ca-10
```

6.2.2 Setup CMDB CA

When NFVD is discovering resources via HPSW/OMi

Step-1 : Unzip

```
unzip -d /opt/openmediation-70/ips/  /opt/HPE/nfvd/discovery/cmdb/cmdb-ca-1.0.0.zip
```

Step-2 : Install the CA in openmediation container

```
nom_admin --install-ip cmdb-ca-10
```

Step-3 : Install CA in nom-container (default container 0)

```
nom_admin --install-ip-in-container 0 cmdb-ca-10
```

Step-4 : Edit CA properties

Edit the file /var/opt/openmediation-70/containers/instance-0/ips/cmdb-ca-10/etc/endpoints-config.properties

```
omi.protocol=http
omi.host=nfvdhaaa-vip
omi.port=80
omi.username=<OMI_API-Access_Username>
omi.password=<OMI_ API-Access_Password>
```

Step-5 : Edit TQL endpoint.

Note

Use the variable values as – 'NFVD_TOPOLOGY' query to get all DataCenters and fulfillment channel adapter will reconcile any datacentre details.

Eg: Assume a datacentre with name as DC2 and it is required to discover or update just the DC2 details, then the query value must be - NFVD_TOPOLOGY_DC2

Edit the file /var/opt/openmediation-70/containers/instance-0/ips/cmdb-ca-10/etc/endpoints-config.properties

```
# comma separated named query name in omi
named.queries.dump=NFVD_TOPOLOGY

#Live Topology
#comma separated named query name in omi
named.queries.live=NFVD_TOPOLOGY
```

Step-6 : Deploy CA in openmediation container

```
nom_admin --deploy-ip-in-container 0 cmdb-ca-10
```

6.2.3 Setup Fulfillment CA

Step-1: Unzip

```
unzip -d /opt/openmediation-70/ips/  /opt/HPE/nfvd/discovery/common/fulfillment-ca-1.0.0.zip
```

Step-2: Install the CA in openmediation container

```
nom_admin --install-ip fulfillment-ca-10
```

Step-3: Install CA in nom-container (default container 0)

```
nom_admin --install-ip-in-container 0 fulfillment-ca-10
```

Step-4: Edit CA properties

Edit the file /var/opt/openmediation-70/containers/instance-0/ips/fulfillment-ca-10/etc/config/reconciliation-endpoints.properties to modify the below items as required

```
#Fulfillment rest endpoint protocol http/https
rest.protocol=http

#Fulfillment rest endpoint ipaddress/hostname
rest.endpoint= nfvdhaff-vip

#Fulfillment rest endpoint port
rest.port=8080
```

```
#Reconciliation CA rest endpoint for sending trigger message, port has to be changed each container deployment.
recon.rest.endpoint=http://0.0.0.0:18989

#Reconciliation data log folder for artifact-relationship instances.
log.file.folder=/var/tmp

#Reconciliation interval
rest.endpoint.polling.interval=36000s

#REST/LOG OPTION to be triggered for Reconciliation(Only One Option can be enabled)
REST_CALL=TRUE
LOG_ENTRY=TRUE
```

Step-5: On deploying FF-CA, will also trigger discovery, by using below command:

```
cd /opt/open-mediation/bin
./nom_admin --deploy-ip-in-container fulfillment-ca-10
```

6.2.4 Setup Openstack CA

In case where CMDB is not available and NFVD is working directly with Openstack, this CA needs to be installed and configured.

Step-1: Unzip

```
unzip -d /opt/openmediation-70/ips/  /opt/HPE/nfvd/discovery/common/openstack-ca-1.0.0.zip
```

Step-2: Install the CA in openmediation container

```
nom_admin --install-ip openstack-ca-10
```

Step-3: Install CA in nom-container (default container 0)

```
nom_admin --install-ip-in-container 0 openstack-ca-10
```

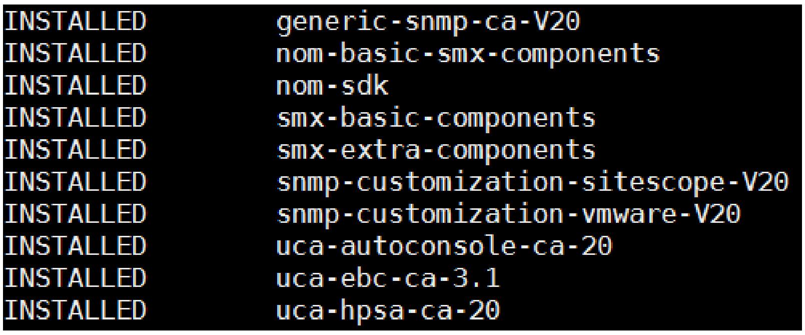
Step-4 : Deploy CA in openmediation container

```
nom_admin --deploy-ip-in-container 0 openstack-ca-10
nom_admin --list-ip-in-container
```

Note: Follow the same procedure on both Primary and Failover nodes. Ensure to mention Endpoint details with the virtualIP value for all the CAs as mentioned in the previous sections

Note: After successfully installing all Channel Adapters, verify the same by running the command on both primary and failover nodes

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



```
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
```

6.3 Edit the NFVD SolutionPack properties for integration with FF

Note: Based on the configuration of Assurance gateway, the port can be 18080[http] or 8443[https] can be updated in the below property

Login to Fulfillment VM
EDIT /etc/opt/OV/ServiceActivator/config/nfvd.properties

```
rest.api.endpoint.key=http://nfvdhaff-vip:8080
assurance.rest.api.endpoint.key=http://nfvdhaaa-vip:<port>
```

6.4 Deploy and Start UCA-EBC VPs

Note: This step can optionally be performed using UCA-EBC GUI for Deploy and start actions

6.4.1 Deploy UCA_EBC VALUE PACKS

```
cd /opt/UCA-EBC/bin
./uca-ebc-admin --deploy -vpn UCA_NFVD_ProblemDetection_Valuepack -vpv 4.1.1
./uca-ebc-admin --deploy -vpn UCA_NFVD_PublishToNomBus -vpv 4.1.1
./uca-ebc-admin --deploy -vpn UCA_NFVD_StatePropagation -vpv 4.1.1
./uca-ebc-admin --deploy -vpn UCA_NFVD_Evaluate_Valuepack -vpv 4.1.1
./uca-ebc-admin --deploy -vpn UCA_NFVD_Persistence_Valuepack -vpv 4.1.1
./uca-ebc-admin --deploy -vpn UCA_NFVD_Migration_Valuepack -vpv 4.1.1
```

6.4.2 Configure Value Packs in UCA-EBC

Note

Based on the configuration of Assurance gateway, the port can be 18080[http] or 8443[https] can be updated in the below property files for the Value Packs. Also ensure to update the http or https as per requirement

6.4.2.1 Configure Assurance_Gateway_Rest_URL in Persistence VP

Edit /var/opt/UCA-EBC/instances/default/deploy/UCA_NFVD_Persistence_Valuepack-4.1.1/conf/persistence.properties

```
Assurance_Gateway_Rest_URL=http://nfvdhaaa-vip:<Port>
```

6.4.2.2 Configure Assurance_Gateway_Rest_URL in Evaluate VP

Edit /var/opt/UCA-EBC/instances/default/deploy/UCA_NFVD_Evaluate_Valuepack-4.1.1/conf/evaluate.properties

```
Assurance_Gateway_Rest_URL=http://nfvdhaaa-vip:<Port>
```

6.4.2.3 Configure Assurance_Gateway_Rest_URL in PD VP

Edit /var/opt/UCA-EBC/instances/default/deploy/UCA_NFVD_ProblemDetection_Valuepack-4.1.1/conf/cypher.property

```
Assurance_Gateway_Rest_URL=http://nfvdhaaa-vip:<Port>
```

6.4.2.4 Configure Assurance & Fulfillment endpoints in State_propagation VP

Edit /var/opt/UCA-EBC/instances/default/deploy/UCA_NFVD_StatePropagation-4.1.1/conf/statepropagation.property

```
#The URL for fulfillment for state propagation
#The URL for NFVD database
NFVD_DB_URL=http://nfvdhaaa-vip:7474/db/data
#Set if alarm after STP needs to be published to NOM Bus. value true/false
FULFILLMENT_URL=http:// nfvdhaff-vip:8080
ENABLE_FF_UPDATE=true
ASSURANCE_REST_URL=http://nfvdhaaa-vip:<Port>
```

6.4.3 Start UCA_EBC VALUE PACKS

```
./uca-ebc-admin --start -vpn UCA_NFVD_ProblemDetection_Valuepack -vpv 4.1.1
./uca-ebc-admin --start -vpn UCA_NFVD_PublishToNomBus -vpv 4.1.1
./uca-ebc-admin --start -vpn UCA_NFVD_StatePropagation -vpv 4.1.1
./uca-ebc-admin --start -vpn UCA_NFVD_Evaluate_Valuepack -vpv 4.1.1
./uca-ebc-admin --start -vpn UCA_NFVD_Persistence_Valuepack -vpv 4.1.1
./uca-ebc-admin --start -vpn UCA_NFVD_Migration_Valuepack -vpv 4.1.1
```

6.5 UCA Automation – HPSA Solution Packs Installation

Note: Follow the same procedure on both Primary and Failover nodes except the below listed Note.

Note: During deployment of HPSA Foundation Solution pack in the **nodes** using Deployment Manager, make sure the checkboxes shown in below screen are always checked and others unchecked. A sample deployment window on other nodes is depicted below

6.5.1 Copy HPSA NFVD Solution pack

Note: The below solution pack can be copied to HPSA/Fulfillment machine or the correlation rpm can be installed on a Fulfillment VM which has HPSA installed and configured. This can be performed from one host only, say - primary

```
cp /opt/HPE/nfvd/correlation/UCA_AUTOMATION_HPSA_NFVD_VP*.zip /opt/OV/ServiceActivator/SolutionPacks
```

Here source path is on assurance machine and destination path in on HPSA/FF machine

6.5.2 Import NFVD Solution Pack

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

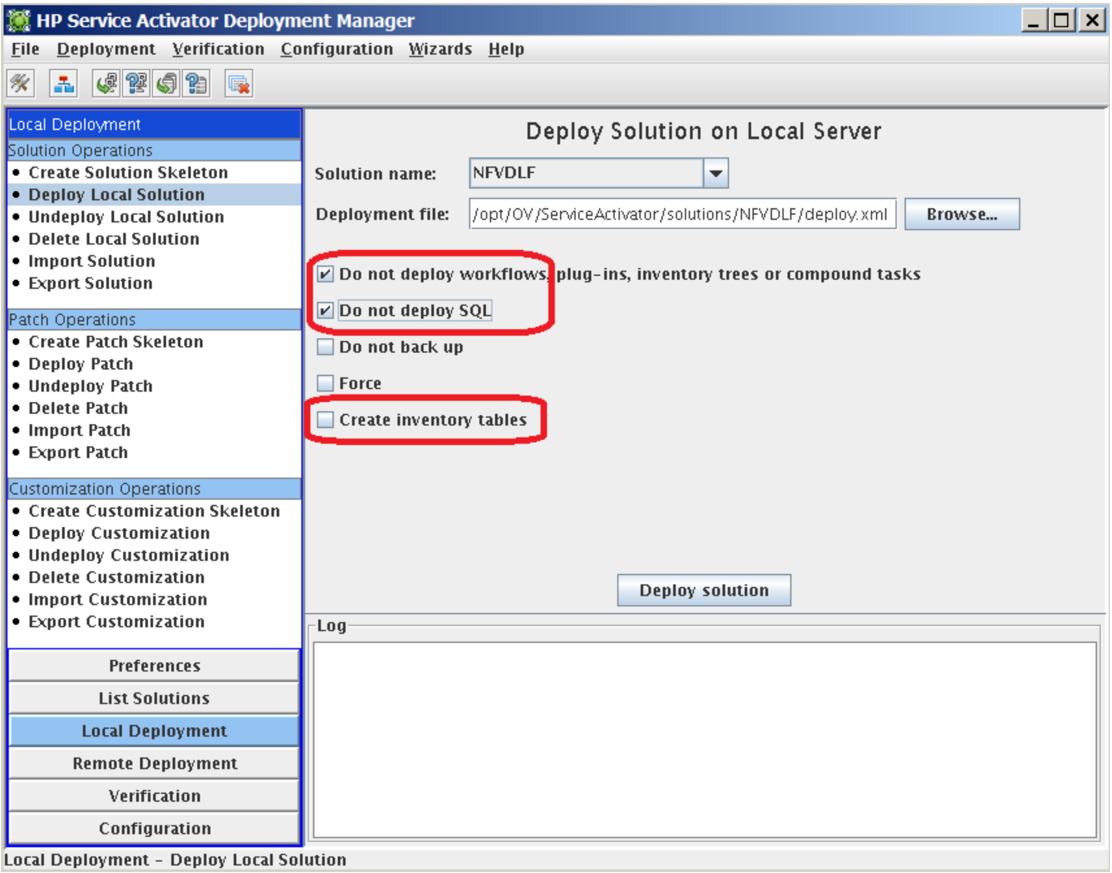
```
./deploymentmanager ImportSolution -file  /opt/OV/ServiceActivator/SolutionPacks/UCA_AUTOMATION_HPSA_NFVD_VP-V40-
1A.zip
```

6.5.3 Deploy NFVD Solution Pack

If the database used by HPSA is on the local machine, the below can be used.

```
./deploymentmanager DeploySolution -solutionName NFVD -deploymentFile /opt/OV/ServiceActivator/solutions/NFVD/deploy.xml
-createTables
```

In case the Database used by HPSA is on a remote host, the below command can be used with appropriate values highlighted in red.



Deploy Solution on Local Server

Solution name: NFVDLF

Deployment file: /opt/OV/ServiceActivator/solutions/NFVDLF/deploy.xml

☑ Do not deploy workflows, plug-ins, inventory trees or compound tasks

☑ Do not deploy SQL

□ Do not back up

□ Force

□ Create inventory tables

Local Deployment – Deploy Local Solution

Alternately, the commadline tool can be used to deploy the solution pack

- <PRIMARY_HOST> node

```
# cd /opt/OV/ServiceActivator/bin
# /opt/OV/ServiceActivator/bin/deploymentmanager DeploySolution -solutionName NFVD
-deploymentFile /opt/OV/ServiceActivator/solutions/NFVD/deploy.xml -createTables -
dbUser NFV -dbPassword NFV -dbHost nfvddb-scan -db XE -dbPort 1521
```

- <SECONDARY_HOST> node

```
# cd /opt/OV/ServiceActivator/bin
# ./deploymentmanager ImportSolution –file
/opt/OV/ServiceActivator/SolutionPacks/UCA_HPSA_FoundationVP-V12-1A.zip
# /opt/OV/ServiceActivator/bin/deploymentmanager DeploySolution -solutionName NFVD
-deploymentFile /opt/OV/ServiceActivator/solutions/NFVD/deploy.xml -
noWorkflowsPlugins  -noSQL -dbUser NFV -dbPassword NFV -dbHost nfvddb-scan -db XE
-dbPort 1521
```

In the Fulfillment VM, edit the host details in the below file - /opt/OV/ServiceActivator/solutions/NFVD/etc/config/nfvd_config.properties

```
sosa_service_url=http://FFHostnameOrIP_OR_nfvdhaff-api-vip:8080/nfvd/operations
```

6.6 Assurance Gateway setup

Note: Follow the same procedure on both Assurance nodes.

6.6.1 SSL Communication with AGW

Note: Please note that this is a one-time configuration. If this configuration already exists, please ignore

6.6.1.1 Configuring SSL on JBoss Web

Once below steps are done, from NFVD, we need to update <PORT> to access https AGW url.
Port used for HTTP = 18080
Port used for HTTPS = 18443

Reference: https://developer.jboss.org/wiki/JBossAS7ConfiguringSSLOnJBossWeb

Create a Keystore file and store it in a known location. It is important to keep track of the keystore password and the alias.

Now create a KeyStore certificate along with a keypair using the JDK KeyTool.

Note:
In keytool-genkey-alias command,
- keystore takes key store path
- alias is the alias name.

```
$ keytool -genkey -alias vault -keyalg RSA -keystore /home/anil/vault/vault.keystore
Enter keystore password:
Re-enter new password:
What is your first and last name?
  [Unknown]:  Anil S
What is the name of your organizational unit?
  [Unknown]:  JBoss
What is the name of your organization?
  [Unknown]:  RedHat
What is the name of your City or Locality?
  [Unknown]:  Chicago
What is the name of your State or Province?
  [Unknown]:  IL
What is the two-letter country code for this unit?
  [Unknown]:  US
Is CN=Anil S, OU=JBoss, O=RedHat, L=Chicago, ST=IL, C=US correct?
  [no]:  yes

Enter key password for <tomcat>
        (RETURN if same as keystore password):
```

I used the password "mykeystore". In this case, the key alias is tomcat.

Then to encrypt the password use vault.sh present in ASSURANCE_JBOSS_BIN.

6.6.1.2 Password Mask Connector Keystore

Note: Masking a Keystore password is optional and not mandatory for functioning of the product

When you want to mask the keystore password in the ssl subelement of the connector setting.

Note: Reference – Vault read on the Vault in JBoss AS7.1 at https://community.jboss.org/wiki/JBossAS7SecuringPasswords

Note:

- In *Enter Keystore URL:* (key store path)
- Enter Keystore password: <KEY Store password>
- Enter Keystore alias: alias name used in keystore generation
- Please enter attribute value: KEY Store password

```
 bin/util$ sh /opt/HPE/nfvd/tpp/jboss/bin/vault.sh
=========================================================================

  JBoss Vault

  JBOSS_HOME: /home/anil/as7/jboss-as/build/target/jboss-as-7.1.0.Final-SNAPSHOT

  JAVA: /usr/java/jdk1.6.0_30/bin/java

  VAULT Classpath: /home/anil/as7/jboss-as/build/target/jboss-as-7.1.0.Final-
SNAPSHOT/modules/org/picketbox/main/*:/home/anil/as7/jboss-as/build/target/jboss-as-7.1.0.Final-
SNAPSHOT/modules/org/jboss/logging/main/*:/home/anil/as7/jboss-as/build/target/jboss-as-7.1.0.Final-
SNAPSHOT/modules/org/jboss/common-core/main/*:/home/anil/as7/jboss-as/build/target/jboss-as-7.1.0.Final-
SNAPSHOT/modules/org/jboss/as/security/main/*
=========================================================================

**********************************
****  JBoss Vault ********
**********************************
Please enter a Digit::   0: Start Interactive Session  1: Remove Interactive Session  2: Exit
0
Starting an interactive session
Enter directory to store encrypted files (end with either / or \ based on Unix or Windows:/home/anil/vault/
Enter Keystore URL:/home/anil/vault/vault.keystore
Enter Keystore password:
Enter Keystore password again:
Values match
Enter 8 character salt:12345678
Enter iteration count as a number (Eg: 44):50

Please make note of the following:
********************************************
Masked Password:MASK-5WNXs8oEbrs  (to be used in <vault> block of standalone.xml)
salt:12345678  (to be used in <vault> block of standalone.xml)
Iteration Count:50   (to be used in <vault> block of standalone.xml)
********************************************

Enter Keystore Alias:vault
Jan 24, 2012 10:23:26 AM org.jboss.security.vault.SecurityVaultFactory get
INFO: Getting Security Vault with implementation of org.picketbox.plugins.vault.PicketBoxSecurityVault
Obtained Vault
Intializing Vault
Jan 24, 2012 10:23:26 AM org.picketbox.plugins.vault.PicketBoxSecurityVault init
INFO: Default Security Vault Implementation Initialized and Ready
Vault is initialized and ready for use
Handshake with Vault complete
Please enter a Digit::   0: Store a password  1: Check whether password exists  2: Exit
0
Task:  Store a password
Please enter attribute value:   <KEY Store password>
Please enter attribute value again:
Values match
Enter Vault Block:keystore_pass
Enter Attribute Name:password
Attribute Value for (keystore_pass, password) saved
```

```
Please make note of the following:
********************************************
Vault Block:keystore_pass
Attribute Name:password
Shared Key:NmZiYmRmOGQtMTYzZS00MjE3LTllODMtZjI4OGM2NGJmODM4TElORV9CUkVBS3ZhdWx0
Configuration should be done as follows:
VAULT::keystore_pass::password::NmZiYmRmOGQtMTYzZS00MjE3LTllODMtZjI4OGM2NGJmODM4TElORV9CUkVBS3ZhdWx0  (this
is used in <connector> of standalone.xml file)
********************************************

Please enter a Digit::   0: Store a password  1: Check whether password exists  2: Exit
2
anil@sadbhav:~/as7/jboss-as/build/target/jboss-as-7.1.0.Final-SNAPSHOT/bin/util$
```

Note: The attribute value was given as "mykeystore". This is what we are trying to mask.

Edit the file /var/opt/HPE/nfvd/conf/standalone.xml
Update the standalone.xml for the <vault> and <connector> tag details as explained below -

Now my standalone.xml contains the following settings:

```
<?xml version='1.0' encoding='UTF-8'?>

<server name="sadbhav" xmlns="urn:jboss:domain:1.1" xmlns:xsd="http://www.w3.org/2001/XMLSchema-instance">

  <extensions>
   ...
   </extensions>

 <vault>
      <vault-option name="KEYSTORE_URL" value="${user.home}/vault/vault.keystore"/>
      <vault-option name="KEYSTORE_PASSWORD" value="MASK-3y28rCZlcKR"/>
      <vault-option name="KEYSTORE_ALIAS" value="vault"/>
      <vault-option name="SALT" value="12438567"/>
      <vault-option name="ITERATION_COUNT" value="50"/>
      <vault-option name="ENC_FILE_DIR" value="${user.home}/vault/"/>
   </vault>
   ....


   ....
      <subsystem xmlns="urn:jboss:domain:web:1.1" native="false" default-virtual-server="default-host">
         <connector name="http" protocol="HTTP/1.1" scheme="http" socket-binding="http"/>  <!-- (This tag is sufficient if you just
need http, and not https) ->
         <connector name="https" protocol="HTTP/1.1" scheme="https" socket-binding="https" enable-
lookups="false" secure="true">
            <ssl password="${VAULT::keystore_pass::password::NmZiYmRmOGQtMTYzZS00MjE3LTllODMtZjI4OGM2NGJmODM4TElO
RV9CUkVBS3ZhdWx0}"
                              certificate-key-file="/home/anil/opensslKeys/KEYTOOL/https.keystore"/>   <!--(This is the Keystore URL path) -
>
         </connector>
         <virtual-server name="default-host" enable-welcome-root="true">
            <alias name="localhost"/>
            <alias name="example.com"/>
         </virtual-server>
      </subsystem>

  ....
```

Comment or uncomment the ssl/non-ssl communication with AGW as below based on the mode of usage -
<!-- WARNING: Enabling the below configuration might expose data transactions between Assurance gateway and an external interface communicator-->
<!-- DISCLAIMER: HPE cannot be responsible for any loss of data or property in any way due to enablement of this feature -->

Note: In case SSL mode has to be used, please specify the values of password and certificate-key-file as shown below

```
<!-- <connector name="http" protocol="HTTP/1.1" scheme="http" socket-binding="http"/> -->
<!-- <connector name="https" protocol="HTTP/1.1" scheme="https" socket-binding="https" enable-lookups="false" secure="true">
        <ssl password="${<FINAL_PASSWORD_GIVEN_USING_VAULT>}"
                certificate-key-file="<PATH_TO_KEYSTORE_FILE_WITH_NAME>"/>
    </connector>
-->
```

6.6.2 Data Source Configuration to Assurance Gateway for AlarmDB

Note: Please note that this is a one-time configuration. If this configuration already exists, please ignore

Edit the file /var/opt/HPE/nfvd/conf/standalone.xml

6.6.2.1 Properties CONFIGURATION

Edit /var/opt/HPE/nfvd/conf/nfvd.properties

```
FULFILLMENT_REST_URL=http://<Fulfillment_Host-Or-IP>:8080
…
…
…

#Option to configure number of items to retrieved from fulfilment in each paginated rest call during topololgy resync. This number can be tuned based on the memory/ram of the system, max number of parallel connections to neo4j etc. Default value is set to 100.
TOPOLOGY_RESYNC_NUMBER_OF_PAGINATION_ITEMS=100

#This property controls the alarm persistence in JMS
ALARM_JMS_PERSISTENCE_FLAG=false

# This property controls the FF notifications persistence in JMS queue
NOTIFICATION_JMS_PERSISTENCE_FLAG=false

#This property controls the FF Notifications Persistence in Oracle/Potsgres DB
NOTIFICATION_DB_PERSISTENCE=false

#This property controls the Alarms activity to the DataBase
ALARM_DB_PERSISTENCE_FLAG=true

#Option to switch on/off capacity calculation as and when notification are received from fulfilment. Default value is set to true. Possible values: true/false
CAPACITY_CALCULATION=TRUE
```

Note: Any other configurations of the assurance gateway can also be enabled here, for eg: analytics, timeouts, etc.

6.6.2.2 Oracle Datasource

Pre-requisite: Ensure disk space is available

a) Copy database driver

Note

- Oracle JDBC driver needs to be downloaded from the manufacturers site [NFVDv4.0 supports Oracle database 11g]; After download, rename it to oracle_jdbc.jar and it has to be placed in /opt/HPE/nfvd/tpp/jboss/standalone/deployments directory. It can be found at the manufacturers web site.

- Alternately this file can be copied from the FulFillment VM from /opt/HP/jboss/modules/com/hp/ov/activator/oracle/main/oracle_jdbc.jar to /opt/HPE/nfvd/tpp/jboss/standalone/deployments directory

Note

- Hibernate decides which Database Schema to persist based on user-name, password provided in datasource.

Copy /opt/HP/jboss/modules/com/hp/ov/activator/oracle/main/oracle_jdbc.jar to /opt/HPE/nfvd/tpp/jboss/standalone/deployments folder

```
cp /opt/HP/jboss/modules/com/hp/ov/activator/oracle/main/oracle_jdbc.jar /opt/HPE/nfvd/tpp/jboss/standalone/deployments
```

Note

Please do not change the jndi name in datasource.

b) To CREATE database schema and USER follow these steps:

Note

Please note that it is a one time creation and not necessary to perform for every upgrade

1) Login to VM where Oracle database is installed
2) su - oracle
3) . /u01/app/oracle/product/11.2.0/xe/bin/oracle_env.sh
4) sqlplus /nolog
5) conn / as sysdba
6) Execute the below SQL commands

```
create tablespace NFV_ALARM datafile '/u01/app/oracle/product/11.2.0/xe/dbs/NFVALARM_data.dbf' size 100m autoextend on next 32m maxsize unlimited logging;
CREATE USER nfvAlarm IDENTIFIED BY nfvAlarm DEFAULT TABLESPACE NFV_ALARM TEMPORARY TABLESPACE temp QUOTA UNLIMITED ON NFV_ALARM;
GRANT create session TO nfvAlarm;
GRANT alter session TO nfvAlarm;
GRANT create table TO nfvAlarm;
GRANT create sequence TO nfvAlarm;
```

Note

<NFV_ALARM, NFVALARM_data.dbf, nfvAlarm> here are examples, which can be customized as required.

c) Add the following data source in - /var/opt/HPE/nfvd/conf/standalone.xml under the datasources tag.

```
<datasource jta="true" jndi-name="java:/assurance-DS" pool-name="assurance-DS" enabled="true" use-java-context="true" use-ccm="true">
                <connection-url>jdbc:oracle:thin:@(DESCRIPTION=(LOAD_BALANCE=off)(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCP)(HOST=localhost)(PORT=1521)))

(CONNECT_DATA=(SERVICE_NAME=XE)))</connection-url>
                <driver-class>oracle.jdbc.driver.OracleDriver</driver-class>
                <driver>oracle_jdbc.jar</driver>
                <pool>
                   <min-pool-size>0</min-pool-size>
                   <max-pool-size>5</max-pool-size>
                   <prefill>true</prefill>
                   <use-strict-min>false</use-strict-min>
                   <flush-strategy>FailingConnectionOnly</flush-strategy>
                </pool>
```

```
      <security>
        <user-name>nfvAlarm</user-name>
        <password>nfvAlarm</password>
      </security>
      <validation>
        <check-valid-connection-sql>SELECT 1 from DUAL</check-valid-connection-sql>
        <validate-on-match>false</validate-on-match>
        <background-validation>false</background-validation>
        <use-fast-fail>false</use-fast-fail>
      </validation>
    </datasource>
```

Chapter 7 NFVD Assurance Component Utilities

NFVDirector is a solution encompassing a vast range of features and technologies. Given the vastness of the solution, there is a need to make the product user friendly. To accommodate the feature access a few utilities are provided as below.

On: <AA_HOST>
Login: root

7.1 Support utility for diagnostics

The tool *supportability_snapshot.sh* tool aggregates NFV Director Assurance log and configuration files, so that it can be sent for analysis.

Note: This tool requires the ‘zip’ package (e.g. zip-3.0-1.el6.x86_64) to be installed on your system.

```
# cd /opt/HPE/nfvd/agw/tools
# export UCA_EBC_DATA=/var/opt/UCA-EBC
# export path_nom_var_dir=/var/opt/openmediation-70
# ./supportability_snapshot.sh
```

7.2 Capacity recalculation utility

The tool *TriggerCapacityRecalculation.sh* tool calculates the free, available, and used resources in the infrastructure.

```
# cd /opt/HPE/nfvd/bin
# ./TriggerCapacityRecalculation.sh -m http

Usage: TriggerCapacityRecalculation.sh [OPTIONS...]
 -h <<Hostname or IPADDRESS of Assurance Gateway>>
 -p <<Assurance Gateway JBOSS PORT>>
 -m <<https or http>>
```

7.3 Assurance and Fulfillment resynchronization tool

The tool *TriggerTopologyReSync.sh* synchronizes the data between Fulfillment and Assurance:

```
# cd /opt/HPE/nfvd/bin
# ./TriggerTopologyReSync.sh -m http

Usage: TriggerTopologyReSync.sh [OPTIONS...]
 -h <<Hostname or IPADDRESS of Assurance Gateway>>
 -p <<Assurance Gateway JBOSS PORT>>
 -m <<https or http>>
```

7.4 Dump topology tool

The tool *TriggerDumpAllTopology.sh* dumps the Assurance data into CSV format for consumption by analytics

```
# cd /opt/HPE/nfvd/bin
# ./TriggerDumpAllTopology.sh -m http

Usage: TriggerDumpAllTopology.sh [OPTIONS...]
 -h <<Hostname or IPADDRESS of Assurance Gateway>>
 -p <<Assurance Gateway JBOSS PORT>>
 -m <<https or http>>
```

7.5 Changing Assurance Gateway logging level

The tool *nfvd_assurance_logger.sh* can be used to set the Assurance Gateway logging level to production or troubleshooting level.

```
# cd /opt/HPE/nfvd/bin
# ./nfvd_assurance_logger.sh -level <production | troubleshoot>
```

The tool *setAGWLogLevel.sh* can be used to change the logging level

```
# cd /opt/HPE/nfvd/bin
# ./setAGWLogLevel.sh –l <ERROR|DEBUG|FINEST|FINER|FINE|TRACE|CONFIG|INFO|WARN|FATAL|SEVERE>
```

7.6 Integrating SiteScope with Assurance Gateway to enable KPI metrics collection

In order to enable KPI data collection from SiteScope, perform the following steps on both the nodes. This is an optional step.

```
# cd /opt/HPE/nfvd/templates/bin
# ./dataintegration_tool_sitescope.sh -lwssopath <lwssofmconf.xml path> -host <Sitescope-hostnameOrIP> -port <Sitescope-port> -uname <SitescopeAdminUsername> -pass <SitescopeAdminPassword> -dname <diname> -url <Receiverurl> -tagname <tagname>
```

Typical example:

```
# cd /opt/HPE/nfvd/templates/bin/
# ./dataintegration_tool_sitescope.sh -lwssopath /var/opt/HPE/nfvd/conf/lwssofmconf.xml -host localhost -port 18888 -uname admin -pass admin -dname DefaultSis-AGW-INTG -url http://localhost:18080/nfvd/kpimetrics -tagname NFVD
```

7.7 Importing VIM certificate to SiteScope

If the VIM (vCenter, RHOS, pure OpenStack, HCG) services are https enabled, it is mandatory to import the VIM certificate into SiteScope.

In order to import VIM certificate into SiteScope, following is the process:

1. Access the VIM say - HCG-openstack in a browser (eg: Mozilla firefox)
2. If the certificate is already saved in the local keystore/registry, access in browser Options -> Advanced -> Certificates -> View Certificates -> Servers tab and select appropriate certificate used by the VIM in list(eg., H13-HCG-IP)
3. Alternately, in case of a first time user access of VIM, when the certificate challenge is thrown, select View Certificate >> Details

4. Export the certificate as a file to a local system.
5. Login to Sitescope.
6. Navigate to -> preferences -> Certificate Management -> import the certificate saved in the local system

7.8 Installation differences against non HA set up

```
The differences are explained in detail, where as the common steps are mentioned as to
be referred to the HPE NFVD I&C Guide
         The NFVD Instances need to have HA Instances modelled for all NFVD VNFC or
atleast for Assurance Gateway and Sitescope [as in below attached File] inorder to
achieve self-monitoring and DB sync between assurance & Fulfillment
```

7.9 Shared disk

The image directory can be configured in …

```
The ${UCA_EBC_DATA}/var/opt/UCA-EBC directory has to be shared or has to be in sync for
the HA VMs with UCA-EBC
```

The /var/opt/UCA-EBC directory must be in sync for both the VMs.

The shared disk can be mounted in 3 ways:

4. Prefered option
   a. An external Cabin provides a single volume through NFS ant both VMs mount the same volume
5. Second preferred
   a. An external cabin or even openstack cinder provides 2 volumes that are mounted one by each VM
   b. Each VM configured glusterFS to replicate and sync data between the 2 volumes
6. Last option
   a. Each VM defines a volume using the local disk
   b. Each VM configured glusterFS to replicate and sync data between the 2 volumes

7.10 Connectivity and load balancer needs

```
Both Primary and secondary assurance VMs must have a full duplex communication
with the load balancer. The Load balancer will listen to a certain port bound
to a virtual IP to service requests.
```

7.11 Monitoring tools

```
aa_check.sh is an independent script registered to cron and triggered at
regular intervals to check the process status. It has to be used with the Load
balancer.
```

Location: /opt/HPE/nfvd/bin

7.11.1 Enable HA Monitoring job

1. Crontab entries in RHEL OS

Edit crontab using below command, add the entry in Assurance VMs and save->Quit [wq!]

```
crontab –e
MAILTO=""
*/5 * * * * /opt/HPE/solutions/ha-example/aa_check.sh
```

Note: The numeric highlighted in red – 5 is the frequency of the scripts to be triggered in minutes. It can be modified as per requirement. Please refer to man crontab for more inputs.

2. Modify Execution permissions

```
chmod +x /opt/HPE/solutions/ha-example/aa_check.sh
```

3. Edit the aa_check.sh and set the variable value of <HB_VIP> for AGW_VIP. Eg: AGW_VIP=192.168.11.221, save and quit [:wq! In vim editor]

7.12 Heartbeat daemon installation

The heartbeat daemon is needed to clusterize assurance products. As a prerequisite if you are installing in Openstack, it is needed that an IP (it is going to be the VIP for assurance) is associated as an allowed ip for ports of internal network of both machines. As a reference, here is a list of commands that should be done in Openstack to support that:

```
#Create a port: (Preferrably using an IP from the discovery range)
neutron port-create HA-private  --fixed-ip ip_address=<vip>

#Get the ports Id attached to each server
neutron port-list | grep <internal-ip-vm-1>
neutron port-list | grep <internal-ip-vm-2>

#Attach the new IP to the port on each server
neutron port-update   fc211741-7a10-4ab0-a13b-c1de28aba6df --
allowed_address_pairs list=true type=dict ip_address=<vip>
neutron port-update  c12fefaa-cee1-4913-ade1-620d4b3acc99 --
allowed_address_pairs list=true type=dict ip_address=<vip>
```

To install heartbeat, all this packages would be needed (provided list is checked against Red Hat Linux 6.6):

```
cifs-utils-4.8.1-20.el6.x86_64.rpm
heartbeat-libs-3.0.4-2.el6.x86_64.rpm
quota-3.17-23.el6.x86_64.rpm
cluster-glue-1.0.5-6.el6.x86_64.rpm
libtalloc-2.1.5-1.el6_7.x86_64.rpm
resource-agents-3.9.5-34.el6.x86_64.rpm
cluster-glue-libs-1.0.5-6.el6.x86_64.rpm
libtdb-1.3.8-3.el6_8.2.x86_64.rpm
samba-client-3.6.23-35.el6_8.x86_64.rpm
device-mapper-1.02.117-7.el6.x86_64.rpm
libtevent-0.9.26-2.el6_7.x86_64.rpm
samba-common-3.6.23-35.el6_8.x86_64.rpm
device-mapper-event-1.02.117-7.el6.x86_64.rpm
lvm2-2.02.143-7.el6.x86_64.rpm
samba-winbind-3.6.23-35.el6_8.x86_64.rpm
device-mapper-event-libs-1.02.117-7.el6.x86_64.rpm
lvm2-libs-2.02.143-7.el6.x86_64.rpm
samba-winbind-clients-3.6.23-35.el6_8.x86_64.rpm
device-mapper-libs-1.02.117-7.el6.x86_64.rpm
perl-TimeDate-1.16-13.el6.noarch.rpm
tcp_wrappers-7.6-58.el6.x86_64.rpm
device-mapper-persistent-data-0.6.2-0.1.rc7.el6.x86_64.rpm
pytalloc-2.1.5-1.el6_7.x86_64.rpm
tcp_wrappers-libs-7.6-58.el6.x86_64.rpm
heartbeat-3.0.4-2.el6.x86_64.rpm
PyXML-0.8.4-19.el6.x86_64.rpm
```

The init script for assurance should also be copied to the appropriate place. You should issue the below commands in your machine:

```
cp /opt/HPE/nfvd/bin/nfvd /etc/init.d/
chmod +x /etc/init.d/nfvd
```

Note: If the preference is to set default runlevel operations for the NFVD VM, the below commands have to be executed. This however is subject to the HA clustering software.

```
chkconfig --add nfvd
chkconfig --level 345 nfvd on
chkconfig --list | grep nfvd
```

After installation, the following files should be configured:

1. Create and edit /etc/ha.d/authkeys using below commands

```
: > /etc/ha.d/authkeys
chmod 0600 /etc/ha.d/authkeys
printf "auth 2\n2 sha1 %s\n" "$(head -c 12 /dev/urandom | base64)" >
/etc/ha.d/authkeys
```

Include a shared_key that should be an alphanumerical key and it should be different for each installation. The shared key must be present in both the primary and secondary setups

2. Edit /etc/ha.d/ha.cf

   The content of this file should be this:

```
logfile /var/log/heartbeat.log
logfacility local0
keepalive 2
deadtime 30
initdead 120
ucast eth0 <other node in the cluster>
udpport 694
auto_failback off
node nfvdhaaa1
node nfvdhaaa2
```

   In a typical installation, you should change the node names with the machine names obtained from executing the command *“uname –n”*
   The recommended configuration is to not allow the failback of resources when the primary node goes up again. This can be changed with using the auto_failback configuration to “on”.

3. Edit /etc/ha.d/haresources

```
nfvdhaaa1 nfvdhaaa-vip nfvd
```

   The vip should be changed for the one you selected in the previous steps, and you should change the node name with the name of the primary node for your installation.

2. Start heartbeat process

```
/etc/init.d/heartbeat start
```

7.13 Disable HA and monitoring job

1. Edit crontab using below command, add comment or add '#' entry in Assurance VMs and save->Quit [wq!]

```
crontab -e
#*/5 * * * * /opt/HPE/solutions/ha-example/aa_check.sh
```

Note: In case the cron job is still not stopped post the above change, a restart or the crond service can be performed as - /etc/init.d/crond restart

2. Stop heartbeat process

```
/etc/init.d/heartbeat stop
```

Chapter 8 Administrative Operations:

8.1 NFVD Processes usage

Use the nfv-director.sh script located in /opt/HPE/nfvd/bin to start/stop or check status of any assurance components

Check processes Status

```
/opt/HPE/nfvd/bin/nfv-director.sh status
```

Start Processes

```
/opt/HPE/nfvd/bin/nfv-director.sh start
```

Stop Processes

```
/opt/HPE/nfvd/bin/nfv-director.sh stop
```

Action with individual Processes

```
/opt/HPE/nfvd/bin/nfv-director.sh -c [ activator | sosa | ecpool | lockmgr | openmediation | sitescope | uca-ebc | nfvd-agw | couchdb | uoc | idp | imageuploader ] [start|stop|status|restart]
```

8.2 Enable-Disable crontab mails

It has been observed that for each cronjob trigger a mail is sent to the user and overtime the disk storage is full. Hence below procedure is to enable/disable mails for crontab.

Enable mailing:
Edit crontab using below command, comment out ‘MAILTO=”” entry as a first line and save->Quit [wq!]

```
crontab -e
#MAILTO=””
```

Disable mailing:
Edit crontab using below command, uncomment or add the ‘MAILTO=”” entry as a first line and save->Quit [wq!]

8.3 HA Landscape Configuration:

8.3.1 Pre-requisites:

1. UOC and related processes must be up and running with the NFVD components installed
2. The fulfillment setup and related components has to be up and running.
3. The Assurance setup and related components has to be up and running.

8.3.2 Sample NFVD HA Landscape to be loaded to Fulfillment

Below is an example of a part of the NFVD Landscape looks like for ASSURANCE GATEWAY component. This sample NFVD Landscape is provided as part of installation in Assurance Gateway including all of the NFVD VNFC components.

The sample instance needs to be loaded in NFVD, for the self-monitoring capability to work.

```
cd /opt/OV/ServiceActivator/solutions/NFVModel/etc/LoadXML/INSTANCES/NFVD_INSTANCES
cp NFVD_LANDSCAPE_SAMPLE_ORACLE_localhost.xml NFVD_LANDSCAPE.xml
```

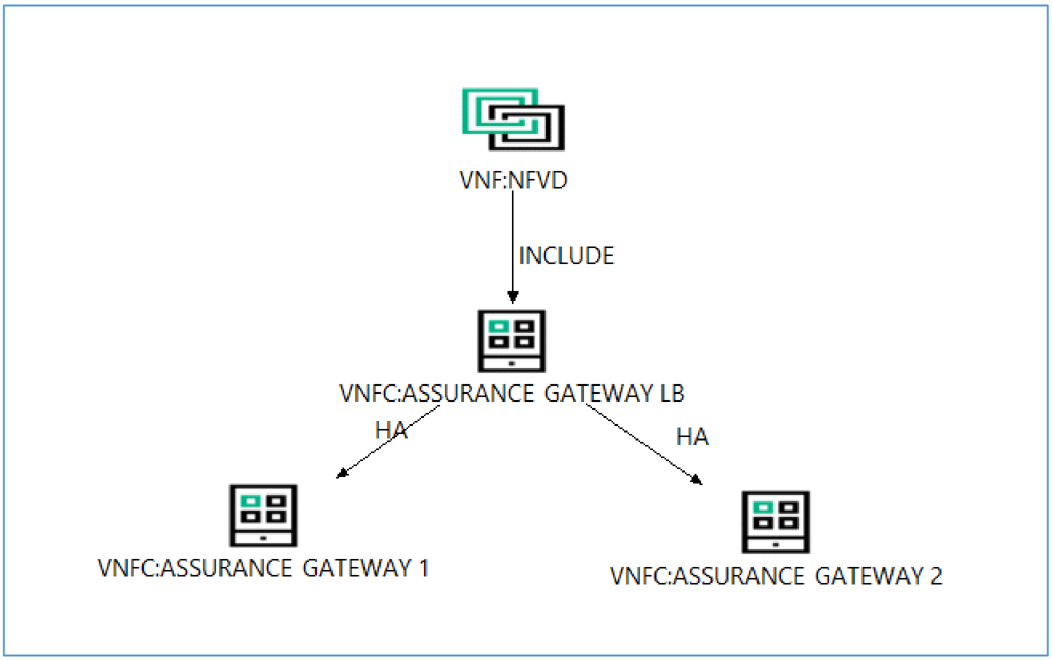
```
chmod +x UploadNfvdInstances.sh
./UploadNfvdInstances.sh
```

8.3.3 Configuration

Configuration needs to be done for self-monitoring support for High Availability to work in Assurance Gateway.

Below are the steps for configuration that needs to be done.

1. Login to NFVD GUI as a domain user or as any user which has access to the instances
2. Access Instances >> VNF_COMPONENT from the dropdown
3. One can find 3 instances of VNF_COMPONENY of category ASSURANCE_GATEWAY.
4. Select/Search and click on VNF_COMPONENT - ASSURANCE_GATEWAY
5. From the Actions dropdown, click on EDIT
6. Ensure to input the Virtual IP, port for the Parent VNFC [LB – Load Balancer] and below details for both the Primary and Secondary nodes



7. EDIT the details of the VNF_COMPONENTS, especially the GENERAL category which has Name, Description, type, IS_PRIMARY and so on. Similarly update CONNECTION details for host [IP or FQDN hostname], port, hostuser, hostpassword, username, userpassword and any other details as required, MONITOR >> Enabled, LOG_MONITOR [Remove path of log to disable log monitoring].
8. Click on update to save the changes
9. Repeat the above procedure from steps 2 to 6 for all VNF_COMPONENTS –
   a. NEO4J
   b. UCA
   c. OPENMEDIATION
   d. SITESCOPE
   e. ORACLE
   f. SOSA
   g. HPSA

   h. ECP

   i. COUCHDB

   j. UOC

   k. LOCKMANAGER

10. Input only 1 node [say nfvdhasi1] of Sitescope as IS_DEFAULT=true and IS_PRIMARY=true, the rest of the VNFC:Sitescopes must have IS_DEFAULT=false and IS_PRIMARY=false
11. Set Mode [ACTIVE-ACTIVE, ACTIVE-PASSIVE] at the Parent VNFC level LB
12. Ensure to specify the DNS registered Fully Qualified Domain Names [FQDN] for the hosts
13. It is recommended to add any relevant details for other categories, for example – DATA_INTEGRATION if it is required for sitescope or MONITOR details [frequency in seconds and Enabled – set to true or false as per requirement]; edit LOG_MONITOR properties – LogPath, LogFile and LogPattern for any of the NFVD Components.
14. The resync may take quite sometime depending on the number of instances. One quick way to check if sync is achieved is by checking the /opt/HPE/nfvd/tpp/jboss/standalone/log/server.log where Assurance queries details from Fulfillment and /opt/HP/jboss/standalone/log/nfvd.log which has information about sync with assurance. Search string in nfvd.log – “Element for synchornize:0”. The value must always be ‘0’ [zero]. Also a login to neo4j and the number of nodes must be > 1

Note:

1. In cases where the DNS registration of hosts is not present, an alternate is to specify alias entries in /etc/hosts, but it is recommended to always have the DNS setup so as to prevent multiple other issues which arise due to non-standard usage of a network.

2. Troubleshooting the sync functionality has multiple approaches which will be covered in the Troubleshooting guide in a broad manner

3. In some cases due to known issues in java, the hostname may not be identified consistently. To resolve this issue, grep for “Attributes” in /opt/HPE/nfvd/tpp/jboss/standalone/log/server.log.* file and use the entries suggested in the latest part of the log to enter the host details of assurance gateway in NFVD GUI. **Command** – ‘*grep Attributes /opt/HPE/nfvd/tpp/jboss/standalone/log/server.log.**’