HPE NFV Director

Administration Guide

Release 4.2

Second Edition

Hewlett Packard Enterprise

Notices

Legal notice

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

List of tables

List of figures

Preface

About this Guide

This document describes the operations related to administration of NFVD infrastructure for a typical standard production environment:

- Administering NFVD:
  - Chapter 1: NFV Director Base Product licenses
  - Chapter 2: NFVD Director architecture
  - Chapter 3: Assurance and Fulfillment resynchronization
  - Chapter 4: NFV Director Log management
  - Chapter 5: NFV Director analytics
  - Chapter 6-9 : Securing communication in NFV Director

This document also takes the following assumptions:

- Infrastructure administration tasks are not detailed and handled by a contact identified as “IT Admin”.
- Oracle DBA administration tasks are not detailed and handled by a contact identified as “Oracle DBA”.

Audience

This guide is intended for any stakeholder requiring to administer NFV Director infrastructure. It is recommended that the person is knowledgeable in Linux and Oracle administration to use this document.
NFV Director administrator must have the root access to the NFV D servers, and will be responsible for installation and upgradation of NFV D software.

Document History

Edition	Date	Description
1	February 20, 2017	First edition

Table 1: Document history

Chapter 1 NFV Director Base Product licenses

1.1 Overview

This includes following steps:

- Checking licenses availability
- Managing NFVD Base Products commercial licenses

1.2 Checking licenses availability

1.2.1 Checking NFV Director Base Products licenses availability

Make sure you have the following commercial licenses for NFVD Base Products available, required for installation:

Base Product License	Reference
HPSA Commercial License	HPSA license file
UCA for EBC Commercial License	UCA for EBC license key
UCA Automation Commercial License	UCA Automation license key

Table 2 : Required licenses for installation

Note: For any questions related to NFVD Base Products commercial licenses, please get in touch with the NFV Director product management.

Note: If NFVD Base Products commercial licenses are not available when installing NFVD, they can be installed during the 90-day evaluation license period.

1.2.2 Checking SiteScope license availability

Note: This step can be ignored if NFVD monitoring feature is not required.

Make sure you have the following SiteScope license available:

SiteScope License	Reference
Premium OSI License capacity	SiteScope license file

Table 3 : Required SiteScope license

Note: HP SiteScope 11.30 for Linux package is typically included HP SiteScope 11.30 SW E-Media.

1.3 Managing NFV Director Base Products commercial licenses

You don't have to consider this chapter if you are upgrading from a previous version.

Note: If NFVD Base Products commercial licenses are not available when installing NFVD, they can be installed during the 60-day evaluation license period.

1.3.1 Managing HPSA commercial license

1.3.1.1 Installing HPSA commercial license

On: <FF_HOST>
Login: root

Run /opt/OV/ServiceActivator/bin/checkLicense to check existing license:

```
AutoPass PDF: /etc/opt/OV/ServiceActivator/config/F7wSsMmyZ.txt
AutoPass InstallPath: /etc/opt/OV/ServiceActivator/config
License Type: Instant On
Expiration Date: Sep 13, 2016
Days Remaining: 135
```

Run /opt/OV/ServiceActivator/bin/updateLicense to launch HP Autopass License Tool:

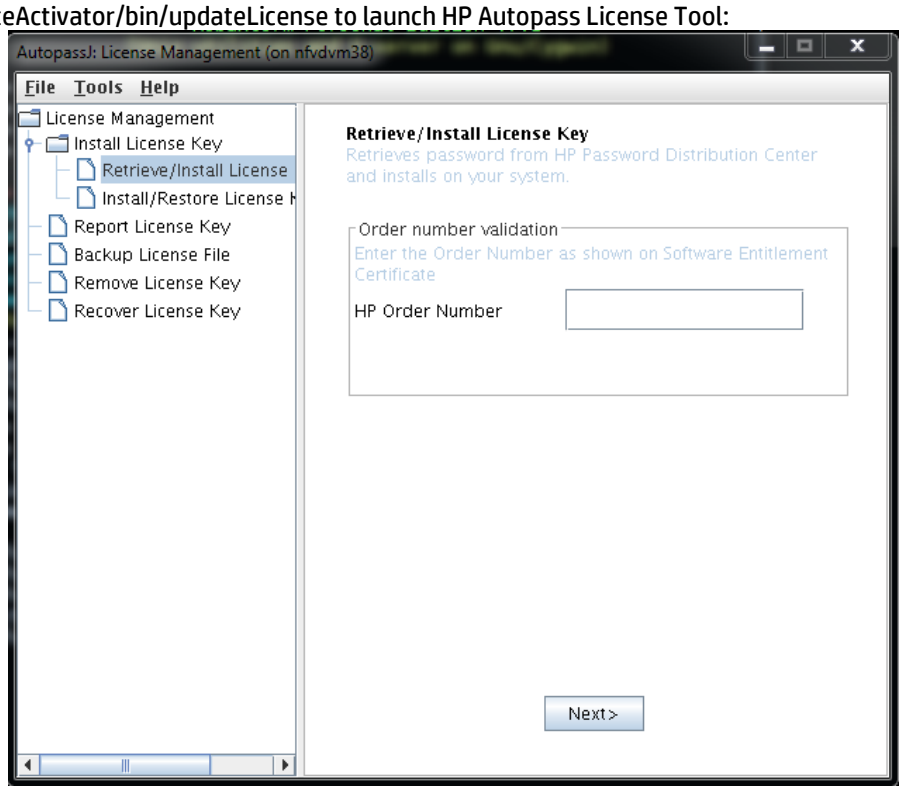


Figure 1 : License Management HPSA

Click on the 'Install/Restore License Key from file', 'Browse' to the license file, and click on 'View file contents', select the license and click on the 'Install' button.

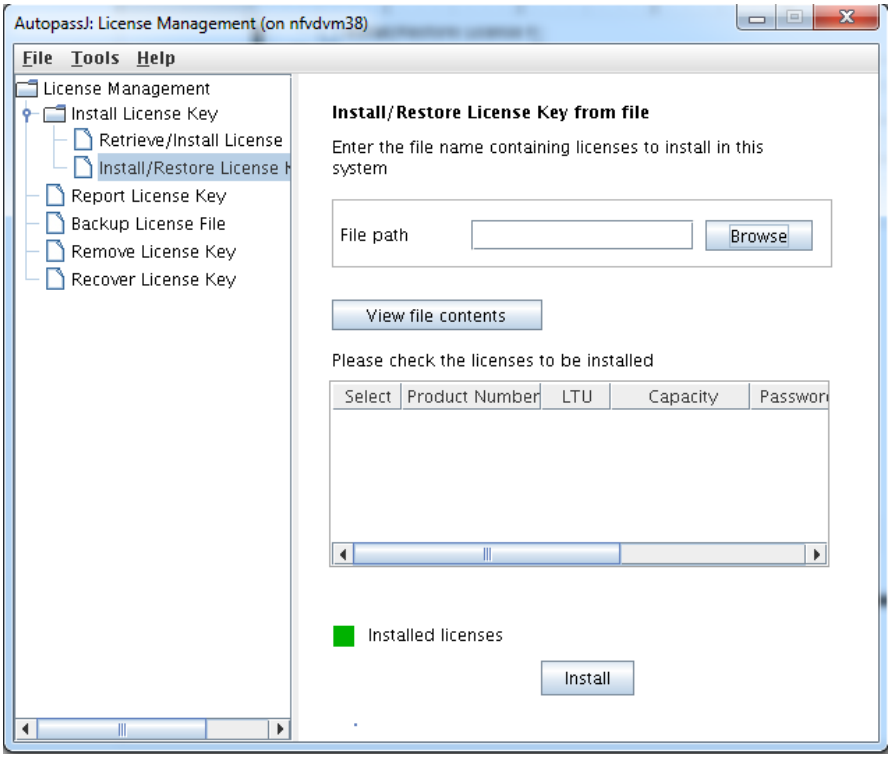


Figure 2 : License Management, install license key from file HPSA

Click on the 'Report License Key' to view the installed license details.

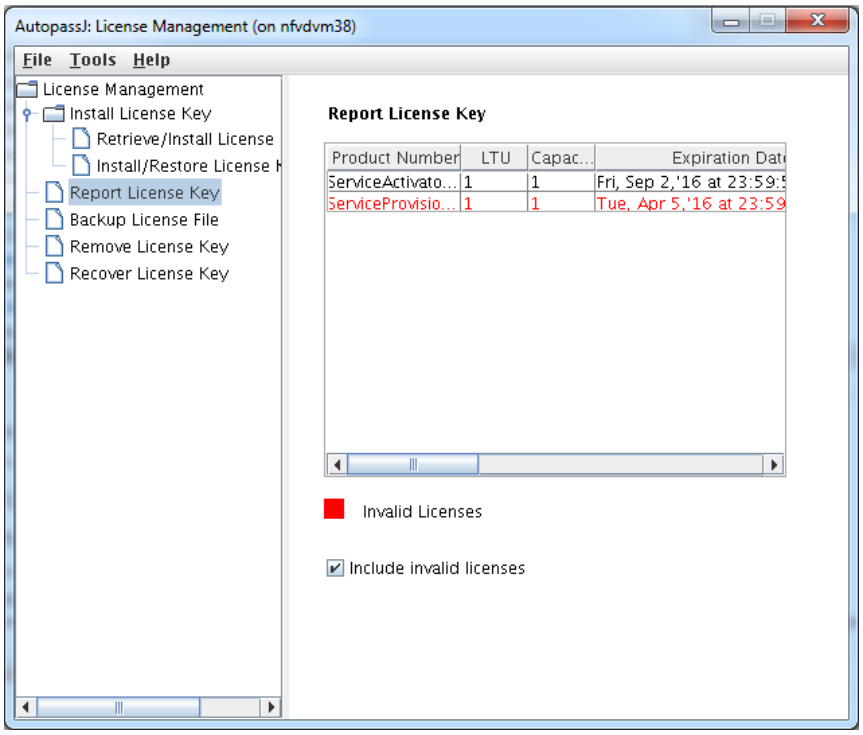


Figure 3 : License Management, report license Key HPSA

1.3.1.2 Verifying HPSA commercial license

On: <FF_HOST>
Login: root

Run */opt/OV/ServiceActivator/bin/checkLicense*:

```
AutoPass PDF: /etc/opt/OV/ServiceActivator/config/F7wSsMmyZ.txt
AutoPass InstallPath: /etc/opt/OV/ServiceActivator/config
License Type: Instant On
Expiration Date: Sep 13, 2016
Days Remaining: 135
```

1.3.2 Managing UCA for EBC commercial license

1.3.2.1 Installing UCA for EBC commercial license

On: <AA_HOST>
Login: root

- Append the UCA for EBC license key(s) to /var/opt/UCA-EBC/instances/default/licenses/license.txt file.
- Restart UCA for EBC Server to apply the changes.

1.3.2.2 Verifying UCA for EBC commercial license

On: <AA_HOST>
Login: root

Upon starting UCA for EBC, open the */var/opt/UCA-EBC/instances/default/logs/uca-ebc.log*, and look for the following pattern to find the license details:

```
Product number       : UCA_Expert_INSTANT-ON
Feature description   : HP OSS UCA Expert Instant-On
License string       : QBKG D9MA H9P9 GHU3 U8A5 HW2N Y9JL KMPL B89H MZVU DXAU 2CSM GHTG L762 CDB6 GVFA LNVT D5K9
EFVW TSNJ N6CJ 6KGC Q9R9 LB2K QAJV QPMZ 58DR RQCE J83M NTQZ 54JB HGWB JK3A 3VEB TTA6 WCDF U2R5 7R39 4QLV
WDWY SXJL JJ4S CZUN XE5Y"HP OSS UCA Expert-90 days Instant-ON License"
Password type        : 0
Feature ID          : 5670
Feature version      : X
IP address          : *.*.*.*
LTU               : 1
Capacity           : 1
Node type(Locking)    : 2
Future date         : Thursday, January 1, 1970 5:30:00 AM IST
Expiration date      : Monday, October 6, 2014 11:59:59 PM IST
Expired            : false
Instant on duration   : 90
IO days remaining     : 15
Host ID            : any
Annotation          : HP OSS UCA Expert-90 days Instant-ON License
Created time        : Friday, September 4, 2009 3:11:12 PM IST
Instant on start date : Wednesday, July 9, 2014 12:00:00 AM IST
```

1.3.3 Managing UCA Automation commercial license

1.3.3.1 Installing UCA Automation commercial license

On: <AA_HOST>
Login: root

- Append the UCA Automation license key to /var/opt/UCA-EBC/instances/default/licenses/license.txt file.
- Restart UCA for EBC Server to apply the changes.

1.3.3.2 Verifying UCA Automation commercial license

On: <AA_HOST>
Login: root

Upon starting UCA for EBC, open the */var/opt/UCA-EBC/instances/default/logs/uca-ebc.log*, and look for the following pattern to find the license details

```
Product number       : DesignAssign_INSTANT-ON
Feature description  : HP UCA Automation Instant-On
License string       : YDCE C9AA H9PA 8HU2 V6A4 HW2N Y9JL KMPL B89H MZVU DXAU 2CSM GHTG L762 QF63 W5FA LNVT D5K9
EFVW TSNJ N6CJ 6KGC Q9R9 LB2K QAJV QPMZ 58DR RQCE J83M NTQZ N4RF GGWB ZK3A 3VEB BXKT HDKN 662K HJPA 9VBU 8L24
2VS2 ZLFG KFVG WM3P 48PU BGJ5"HP UCA Automation-60 days Instant-ON License"
Password type        : 0
Feature ID           : 5790
Feature version      : X
IP address           : *.*.*.*
LTU                  : 1
Capacity             : 1
Node type(Locking)   : 1
Future date          : Thursday, January 1, 1970 5:30:00 AM IST
Expiration date      : Thursday, March 19, 2015 11:59:59 PM IST
Expired              : false
Instant on duration  : 60
IO days remaining    : 44
Host ID              : any
Annotation           : HP UCA Automation-60 days Instant-ON License
Created time         : Monday, January 20, 2048 4:04:14 PM IST
Instant on start date : Monday, January 19, 2015 12:00:00 AM IST
```

1.4 Managing SiteScope commercial license

You don't have to consider this chapter if you are upgrading from a previous version.

Note: This step can be ignored if NFVD monitoring feature is not required.

1.4.1 Installing SiteScope commercial license

Note: This is a mandatory step to be executed during installation if NFVD monitoring feature is required.

On: <AA_HOST>
(typical example: http://16.17.100.20:18888/SiteScope)

Login: <SITESCOPE_ADMIN_USER> /<SITESCOPE_ADMIN_PASSWD>
(typical example: admin/admin)

- Click on Preferences > General Preferences > Licenses.
- Click on the 'Select …' option for License file, point to the correct license, and click on 'Import' button

NOTE: You must install the 'Premium Edition OSI license' to enable the SiteScope API features.

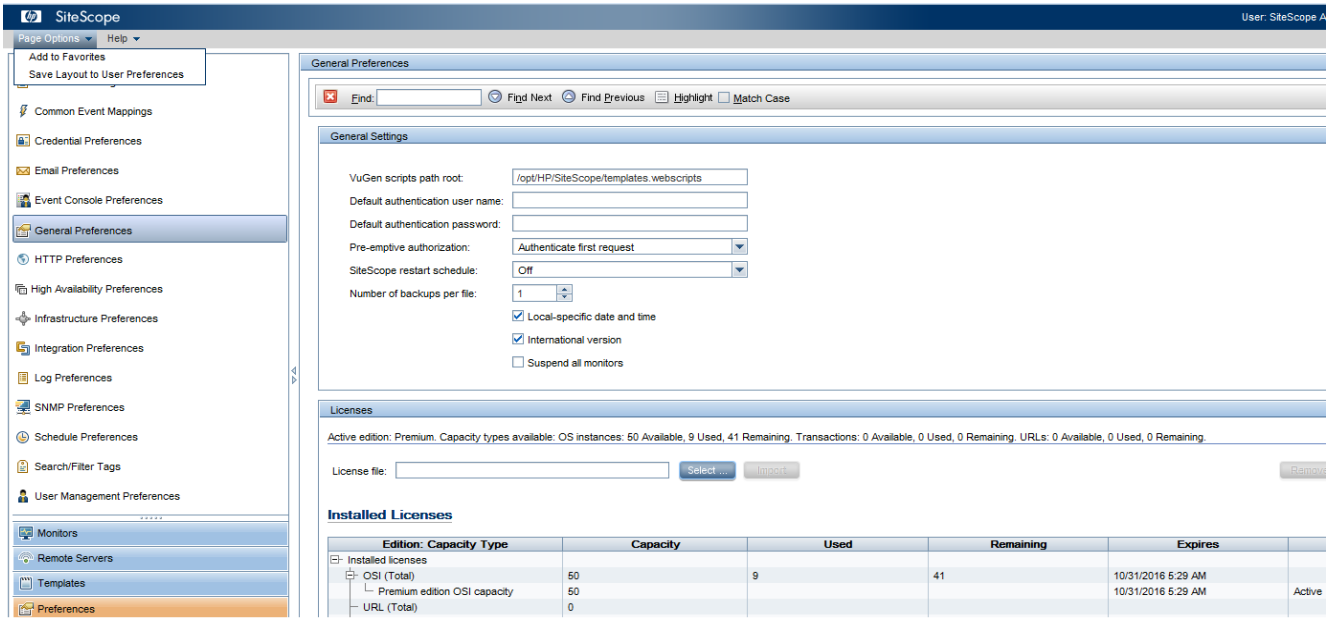


Figure 4 : Sitescope, installing License

1.4.2 Verifying SiteScope commercial license

On: <AA_HOST>
(typical example: http://16.17.100.20:18888/SiteScope)

Login: <SITESCOPE_ADMIN_USER> /<SITESCOPE_ADMIN_PASSWD>
(typical example: admin/admin)

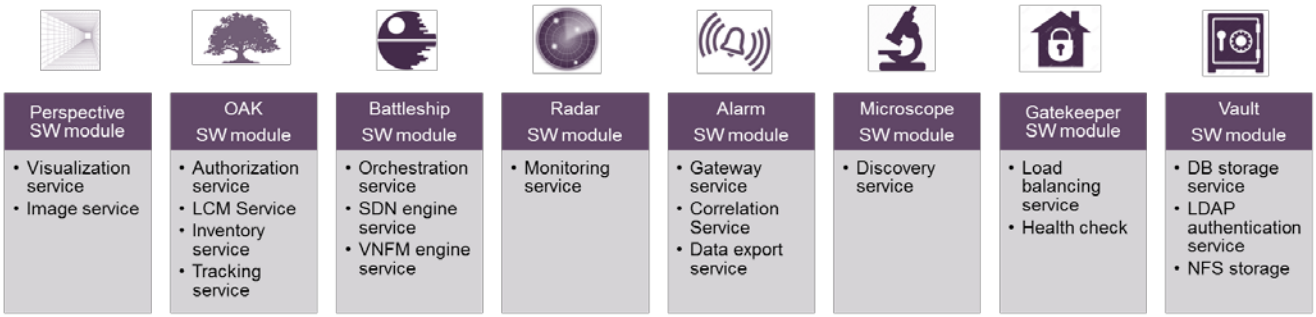
- Click on Preferences > General Preferences > Licenses and check the installed license details.

Chapter 2 NFV Director architecture

This chapter describes the Architecture of NFV director

2.1 NFV Director Architecture

NFV Director provides a set of services that are bundled in different SW modules
NFV Director provides 8 SW modules that can be installed in different deployment flavors
NFV Director provides 18 services that communicate within each other to provide orchestration capabilities



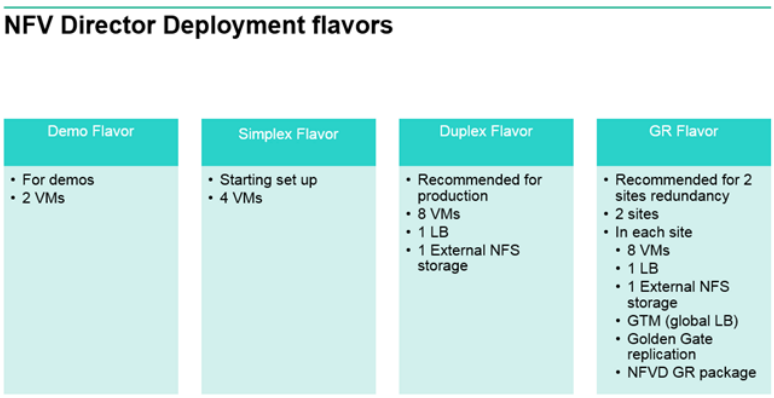
The SW modules are installed in Virtual machines and so NFV Director behaves as a VNF with different deployment flavors.

The Perspective module is normally named as GUI
The grouping of Oak / Battleship and Vaul modules is normally named as Fulfillment
The grouping o Radar / Alarm / Microscope is normally called as Assurance

2.2 NFV Director Deployment flavors

NFV supports 4 out of the box deployment flavors

- Demo flavor
  - Recommeded for demos
- Simplex flavor
  - Recommended for initial set ups and labs
- Duplex flavor
  - Recommended for prodcution
- GR flavor
  - Recommend for Long distance geo redundancy

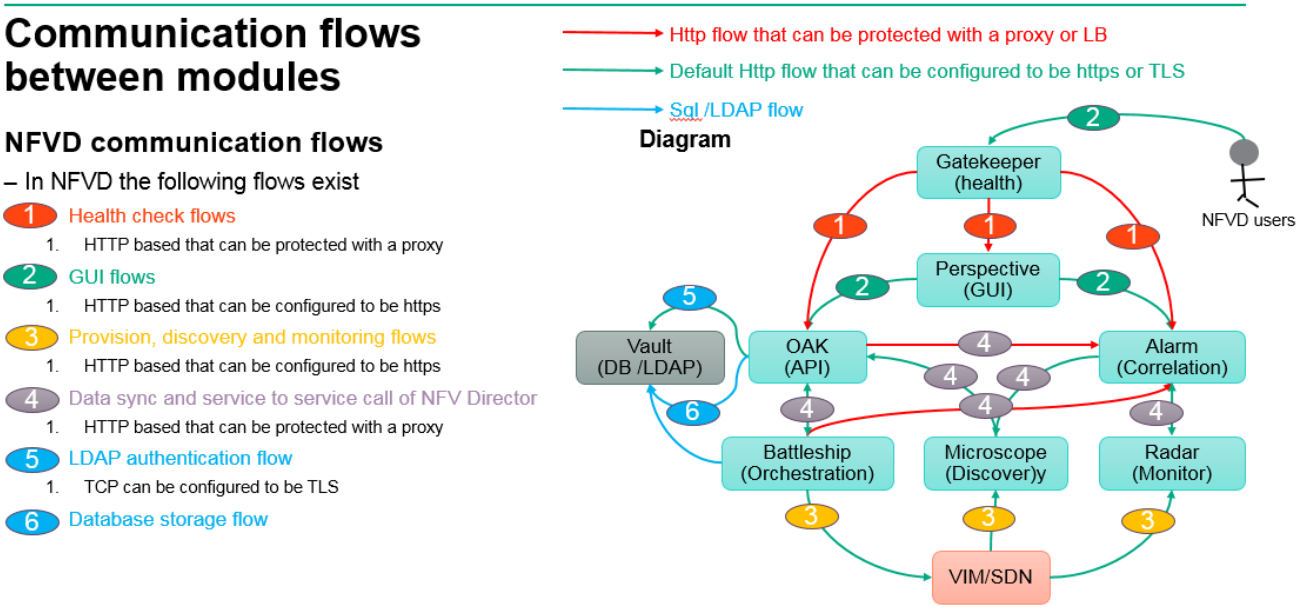


2.3 Security of NFV Director

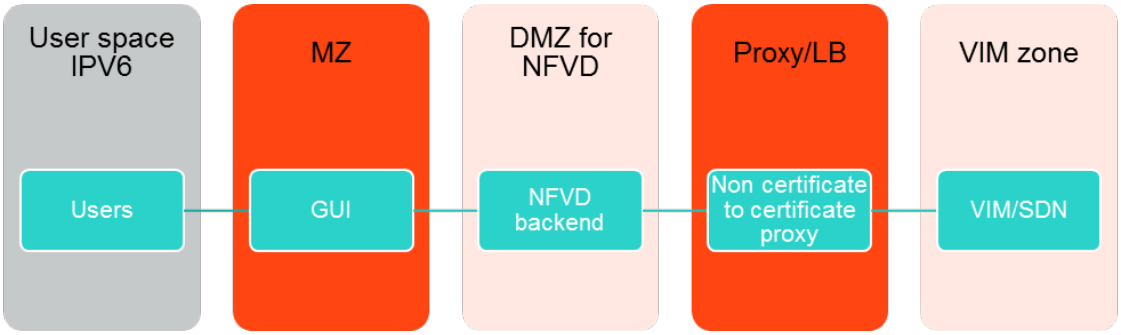
NFV Director is assumed to be deployed in a trusted zone and so it is installed by default with http and ipv4 communications enabled.

- It is assumed that NFVD is installed on a trusted zone (DMZ) where each module can freely talk to each other and can freely talk to VIMs and SDN controllers
- The GUI can be decupled if needed and installed into a more insecure zone if needed and isolate it with a FW/Proxy
- In NFVD the internal communications use user password or token based authentication over an IPV4 network
- If authentication using certificates is needed or connectivity to IPV6 network then a physical or virtual proxy is needed to connect NFVD to the desired destination

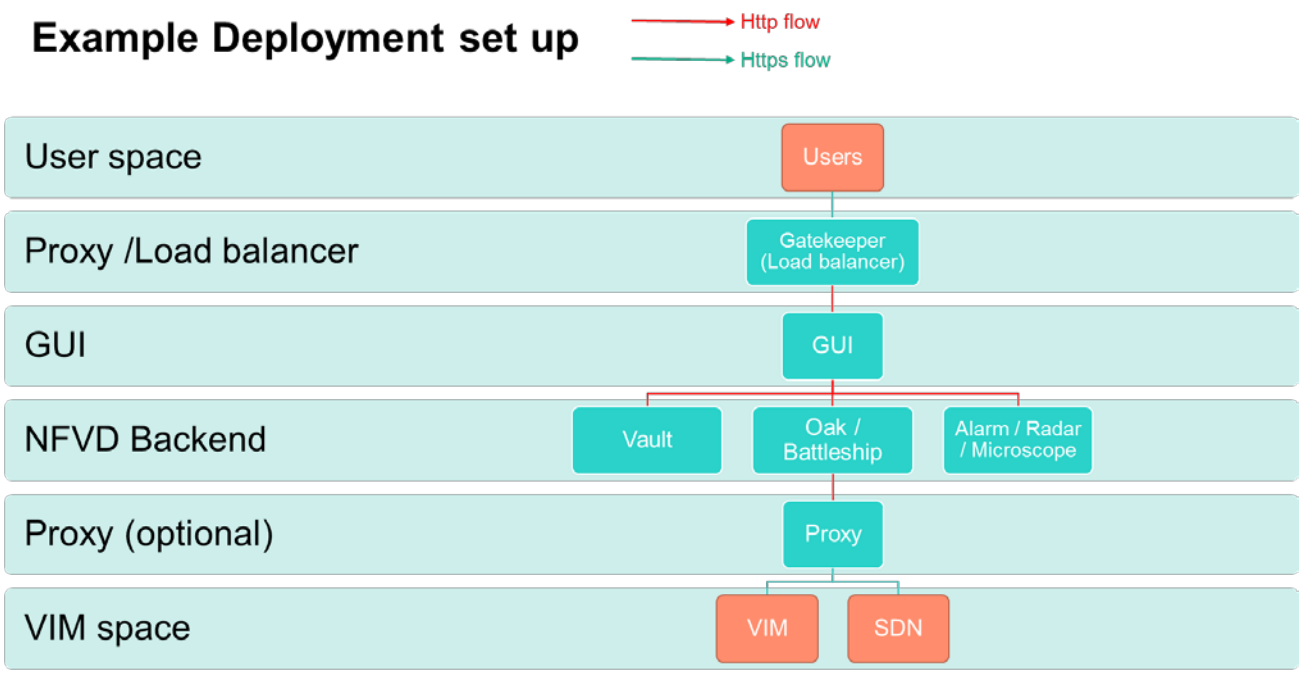
Each module communicates with the other using diffrent security levels (http/https) depending if the comunication is internal between modules or external from NFVD to the VIMs



In order to secure the difrente communication flows is recommended to use an external proxy (or install it collocated with the gatekeeper module) that can translate ipv6 to ipv4 or https to http and vice versa



One typical example is to set up a proxy between the NFVD and the VIMS and between the users and NFVD (it can even be the same physical one) so all the security aspecs are reduced to a single touch point where all https and certificates can be handled without affecting the internals of NFVD.
If needed you will find specific sections over this document about how to configure more https options without the need of a proxy



2.3.1 Increase your security

If you want to increase the security of NFV Director especially after a default installation you will need to:

- Clean up the installation remaining files or protect them at security level as they may contain ip / user password information used during install
- Set up a proxy that isolates all northbound and south bound communications (can be a single SW entity or a pair in HA with a virtual ip or dedicated entities or pairs for northbound and southbound). If needed the same proxy can be used to protect the internal communications between NFVD components as well
    - Within the proxy you can establish
        - IPv6 to/from IPV4 translation if needed
        - Http from /to htpps translation if needed
        - Install and configure CA (customer accepted) certificates so the proxy communicates and authenticates using those certificates even if the communication between NFVD and the proxy is using only http or https without certificates
        - Review the release notes for extra workarounds about known security limitations
        - Follow best practice configurations in the following section

2.3.2 Best practice configurations

2.3.2.1 Verify connectivity and DNS name resolution

- Potential Impact

System will get random errors if connectivity is not in place especially between INTERNAL NFVD components

- Severity **High**
- Description

NFVD components must be able to reach each other as described in the architecture (even if going through a proxy or load balancer
DNS resolution should work to avoid strange behaviors

- Recommended action

Test connectivity within internal components and do not go live if those are not in place
Test DNS resolution and at very least check /etc/hosts and that you are able to ping NFVD elements
Perform same verifications for VIMs/ Datacenters NFVD is going to connect to before going live or before on boarding them into an already live NFVD system

2.3.2.2 Logs

By default the logs are set to debug to allow detect any issue just after the config

- Potential Impact

System might run out of disk space and NFVD platform might be not functional due to disk full.

- Severity **Medium**
- Description

HPSA workflow trace logs is consuming lot of space.
The mwfm_logs.xml (full HPSA workflow trace) can get quickly to 11GB or even more

- Recommended action

Decrease log level and clean logs periodically via cron job.
By default it's better to change the log level to INFORMATIVE.
An example of cron entry:
0 6 * * * /usr/bin/find /var/opt/OV/ServiceActivator/log/<hostname> -mtime +<n> -exec rm "{}" \;
A more complex approach is zip the previous days logs and delete the elders on two different entries on cron.
/usr/bin/find /var/opt/OV/ServiceActivator/log/<hostname> -type f -mmin +1440 -not \(-iname "*\.gz" \) -exec gzip "{}" \;

2.3.2.3 HPSA messages

- Potential Impact: tablespace will be overloaded and the DB could be collapse.

- Severity **High**
- Description: NFVD.MESSAGES are never cleaned on HA environment.
- Recommended action

Use mwfmtool to clean logs periodically via cron job on both HA-FF nodes. As an example:
1 6 * * * /opt/OV/ServiceActivator/bin/mwfmtool DeleteAllMessages -user <hpsa_user>/<hpsa_password> -priorto -3600

2.3.2.4 SOSA history table

- Potential Impact: tablespace will be overloaded and the DB could be collapse. User experience degraded on HPSA-EP web portal

- Severity **High**
- Description: There are not a policy/procedure to rotate SOSA history tables.
- Recommended action

Follow the Sosa documentation to partition history table. Chapter 9.2 Partition History Tables of Sosa.pdf provided by HPSA.

2.3.2.5 Log of "SEVERE" traces for AGW process

- Potential Impact: Monitor Deployment might fail.

- Severity **Medium**
- Description.

Huge amount of "SEVERE" traces

- Recommended action

If too many
Stop AGW process, cleanup neo4j and restart AGW process.
If just install implement a log rotation/delete/backup policy for those logs
An active monetarization of Filesystem could prevent process crashed.

2.3.2.6 Log of "SEVERE" traces for AGW process

- Potential Impact: FF and GUI process may down.

- Severity **High**
- Description: One of the filesystems are every day near 100% Used. At 100% the NFVD process will be unexpected stopped or crashed.

- Recommended action

If just install implement a log rotation/delete/backup policy that fits the amount of disk you have
An active monetarization of Filesystem could prevent process crashed.

2.3.2.7 DB log and archive policies

- Potential Impact: FF and GUI process may down.

- Severity **High**
- Description: file system of DB can be filled with log or archive

- Recommended action

If just install implement a log /archive rotation/delete/backup policy that fits the amount of disk you have
An active monetarization of Filesystem could prevent process crashed

2.3.2.8 Check number of running process

It is needed to check that the number of running processes is the expected one (especially with Lock manager / sosa /AGW / UCA / NOM and graph db)

- Potential Impact: Undefined behavior. (Ex in the case of Lockmanger If the locks are not working the workflow may not be locked so concurrent issues could be found.)

- Severity **High**
- Description: (example nfvdhaff1 is Active and LockManager should be running only on this system. But looks like two stale instances of LockManager are running on nfvdhaff2.)
- Recommended action

Monitors the number of process on each machine to identify if any process started more than once. (Example
Stop all processes on nfvdhaaa2 using nfv-director.sh stop all command.
All NFVD Assurance processes are in Active/Passive mode in HA setup. Only one instance of the process should be running in HA setup.)

2.3.2.9 Check NFVD Fulfilment and Assurance DB are in sync.

- Potential Impact: Monitor deployment might fail.

- Severity **High**
- Description:
  Example

In Simplex Setup the NFVD_SYNCHRONIZATION table shows that there are around 136846 artifacts to be synced.
In HA setup
FF DB: 21303 artifacts
AA DB: 13182 artifacts, more than 30% artifacts not in sync.

- Recommended action

Clean NFVD_SYNCHRONIZATION table and Trigger manual TopologyResync.sh operation and check if they are back in sync.

2.3.2.10 Double Check Openstack.properties file on FF

- Potential Impact: if HPSA change the credential the process may fails.
- Severity **Low**
- Description: Example Openstack.properties missing on HA FF1or misalign with other member of the cluster
- Recommended action
  Create it and or align parameters to be consistent
  On v4.2 onwards this is more important because include more parameters on the HPSA-OpenStack southbound interface.

2.3.2.11 Double Check differences on childWorkflow.properties file

- Potential Impact: Extended mode operation may fail if FF-VM2 process it
- Severity **High**
- Description: differences between HA-FF nodes configuration file
  Example

10.75.14.83//etc/opt/OV/ServiceActivator/config/childWorkflow.properties
include:
WF_TS_VNF_PREVIOUS_VALIDATION_SM=WF_TS_VNF_PREVIOUS_VALIDATION_SM
WF_TS_VNF_PREVIOUS_VALIDATION_VDRA_SM=WF_TS_VNF_PREVIOUS_VALIDATION_SM
WF_TS_VNF_PREVIOUS_VALIDATION_RxGW=WF_TS_VNF_PREVIOUS_VALIDATION_DDE
WF_TS_VNF_PREVIOUS_VALIDATION_VDRA_DDE=WF_TS_VNF_PREVIOUS_VALIDATION_DDE
10.75.14.83//etc/opt/OV/ServiceActivator/config/childWorkflow.properties
Does not have it

- Recommended action

Have the same content in all nodes
Example
Copy the file from 10.75.14.82 node to 10.75.14.83

2.3.2.12 Double check differences Lockmanager start scripts

- Potential Impact: unknown.

- Severity **Medium**
- Description: Not same java parameters are set on HA nodes for Lockmanager
  Example

10.75.14.82//opt/OV/ServiceActivator/EP/LockManager/bin/StartServer.sh
Contains:
JVM_MEMORY="-Xms256M -Xmx256M -Xmn128M"
10.75.14.83//opt/OV/ServiceActivator/EP/LockManager/bin/StartServer.sh
Contains:
JVM_MEMORY="-Xms1024M -Xmx1024M -Xmn512M"
CMD=${CMD}" -server"
["`uname -s`" = "HP-UX"] && CMD=${CMD}" -XdoCloseWithReadPending"

- Recommended action
  The java parameters should be same as in all FF nodes

2.3.2.13 Ensure same java version

- Potential Impact: None

- Severity **Low**
- Description: (example)

Nfvdhaui1 is using JDK 1.7.0_79
Nfvdhaui2 is using JDK 1.7.0_60

- Recommended action

(Example)
JDK used on nfvdhaui1 and nfvdhaui2 should be of same version.
Update nfvdhaui2 to use JDK 1.7.0_79.

2.3.2.14 Monitor NFVD

- Potential Impact: slowness

- Severity **Low**

- Description:

NFVD can handle a certain amount of load based on the sizing if there are peaks of load and system is not well size for those you may expect performance issues potentially even timeouts

- Recommended action

Monitor

- CPU /RAM /disk usage and log that in order to analyze problems even raise alarms to system admin team if usage of any of those reaches 80/85%
- Health of NFVD services and log that in order to analyze problems even raise alarms or send messages to system admin team if any process get stopped (even if the HA mechanism recovers) in order to review the root cause
- Health of NFVD VMs and log that in order to analyze problems even raise alarms or send messages to system admin team if any process get stopped (even if the HA mechanism recovers) in order to review the root cause
- Connectivity to dB and log that in order to analyze problems even raise alarms or send messages to system admin team if any process get stopped (even if the HA mechanism recovers) in order to review the root cause
- Database log and archiving
- LDAP log

Chapter 3 Operating NFV Director

This chapter describes the procedure to manage or administer various components of NFV Director.

3.1 Start/Stop/Status of NFV Director components

Most standard administration operations such as “start”, “stop”, “restart”, “status” can be done with a unique tool installed on all hosts of the NFVD platform in: /opt/HPE/nfvd/bin/nfv-director.sh.

```
# /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
```

3.2 Platform healthcheck

For verifying various base product versions, refer to Troubleshooting Guide

- To check memory information of the system, run
  - cat /proc/meminfo
  - egrep --color 'Mem|Cache|Swap' /proc/meminfo
  - free -m
- To check CPU information of the system, run
  - cat /proc/cpuinfo
  - mpstat -P ALL
  - ps -eo pcpu,pid,user,args | sort -k 1 -r | less
- Firewall commands

```
service iptables [stop | start | status]
chkconfig iptables --list
```

- To increase the number of open files

```
cat /proc/sys/fs/file-max
# To increase max number of open files,
vi /etc/sysctl.conf
fs.file-max = 100000
```

3.3 Backup and recovery

It is recommended to take backup of the following directories and files:

3.3.1 Base product licenses

On: <FF_HOST>

1. /etc/opt/OV/ServiceActivator/config/license.txt

On: <AA_HOST>

1. /opt/HP/SiteScope/conf/license/lic_v2.txt
2. /var/opt/UCA-EBC/instances/default/licenses/license.txt

3.3.2 Data directories

On: <AA_HOST>

1. /var/opt/UCA-EBC/instances/default/neo4j
2. /opt/HP/SiteScope/bin/config_tool.sh -i console – Choose the option to export.

On: <FF_HOST>

1. For Oracle database data backup, refer to Oracle documents

3.4 Audit tool

This tool counts the number of objects managed by NFVD:

- Catalog objects: VNFs , VNF Components , Virtual Machines , Virtual Networks , Monitors
- Physical objects: Data Centers , Servers , CPUs , Cores
- Virtual objects: Organizations , VDCs , VNF Groups , VNFs , VNF Components , Virtual Machines , Virtual Cores , Virtual Networks , Monitors

```
/opt/HPE/nfvd/bin/nfvd_audit.sh -h
Audit tool for NFVD
Usage:
        nfvd_audit.sh [options]

options:
        -d DB Host : Database host (default=localhost)
        -p DB Port : Database port (default=1521)
        -n DB Name : Database name (default=XE)
        -h                  : Displays this usage message
        -v                  : Verbose mode
```

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

At 2016-12-01 09:31:19, NFVD database (localhost) contains the following objects:
```

```
Category        Type                        Nb
--------------- ------------------- ----------
Catalog         VNFs                         1
Catalog         VNF Components               1
Catalog         Virtual Machines             2
Catalog         Virtual Networks             2
Catalog         Monitors                     6
Physical        Data Centers                 0
Physical        Servers                      0
Physical        CPUs                         0
Physical        Cores                        0
Virtual         Organizations                0
Virtual         VDCs                         0
Virtual         VNF Groups                   0
Virtual         VNFs                         0
Virtual         VNF Components               0
Virtual         Virtual Machines             0
Virtual         Virtual Cores                0
Virtual         Virtual Networks             0
Virtual         Monitors                     0
```

3.5 What to do when NFVD server password is changed?

When the system password hosting the NFVD components are changed, the updated password must be reflected in the NFVD solution. Following NFVD system password changes will require updates in the NFVD solution:

- FF_HOST
- AA_HOST
- GUI_HOST
- ORACLE_HOST

1. Login to NFVD GUI as domain user
2. Navigate to Instances menu
3. Select VNFs, and select the VNF of category NFVD
4. Choose all the impacted VNF Components, and open them.
    a. If password is changed in FF_HOST, typically, you would need to update HPSA, SOSA, ECP, LockMgr VNF_COMPONENT
    b. If password is changed in AA_HOST, typically, you would need to update NOM, NEO4J, DefaultSitescope, UCA, AssuranceGateway VNF_COMPONENT
    c. If password is changed in GUI_HOST, typically, you would need to update COUCHDB and UOC VNF_COMPONENT
    d. If password is changed in ORACLE_HOST, typically, you would need to update the VNF_COMPONENT XE
5. Choose the ACTION > Edit > CONNECTION
6. Update the hostPassword with encrypted password value. Password encryption can be done using the below script that is present on <FF_HOST>:
   cd /opt/HPE/nfvd/fulfillment/scripts/ ./ encryption.sh -o encrypt -p <password>
7. Click on Update button.

3.6 What to do when database password is changed?

Following NFVD components are impacted when database password is changed.

1. Update the VNF COMPONENT XE CONNECTION.appPassword attribute using the procedure given in the section “What to do when NFVD server password is changed?”
2. In AA_HOST, update /opt/HP/jboss/standalone/configuration/standalone.xml datasource “nfvd-DS”, <security><password> attribute to reflect the updated password. Restart Assurance Gateway application.

3.7 What to do when VIM password is changed?

1. Navigate to ‘Virtual Infrastructure Manager’ Instance in the NFVD GUI, and edit the CREDENTIALS > Password attribute with encrypted password value, using the procedure given in the section “What to do when NFVD server password is changed?”

Chapter 4 Assurance and Fulfillment resynchronization

4.1 Resync topology between Fulfillment and Assurance

The tool `TriggerTopologyReSync.sh` synchronizes the data between Fulfillment and Assurance. By default, the script works in https mode. In case http mode is required, use '-m http' option.

```
# 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>>
```

4.2 Resync monitors between Fulfillment/Assurance and SiteScope

You can start monitors resync between Fulfilment/Assurance and SiteScope by executing the script `TriggerSiteScopeReSync.sh`. By default, the script works in https mode. In case http mode is required, use '-m http' option.

```
# cd /opt/HPE/nfvd/bin
# ./TriggerSiteScopeReSync.sh –m http

Usage: TriggerSiteScopeReSync.sh [OPTIONS...]
 -h <<Hostname or IPADDRESS of Assurance Gateway>>
 -p <<Assurance Gateway JBOSS PORT>>
 -m <<https or http>>
 -s <<SiteScope Host>>
 -t <<VIRTUAL_MACHINE KVM CPU ex:>>
```

Chapter 5 NFV Director Log management

5.1 NFV Director log files

Various NFV Director component log files and their locations are as follows:

1. Fulfillment

Application	Log
HP Service Activator JBoss	/opt/HP/jboss/standalone/log/server.log
NFV Director	/opt/HP/jboss/standalone/log/nfvd*.log
HP Service Activator	/var/opt/OV/ServiceActivator/log/<host> - mwfm*.log - resmgr*.log

2. GUI

Application	Log
UOC	/var/opt/uoc2/logs/ - server.log - sessions.log
NFV Director	/var/opt/uoc2/logs/ - nfvd*.log

3. Assurance

Application	Log
SiteScope	/opt/HP/SiteScope/logs/ - SiteScope*.log
UCA EBC	/var/opt/UCA-EBC/instances/default/logs - uca-ebc*.log
Open Mediation	/var/opt/openmediation-70/log - nom_admin.log
Open Mediation Service Mix	/var/opt/openmediation-70/containers/instance-0/data/log - servicemix*.log
Assurance Gateway JBoss	/opt/HPE/nfvd/tpp/jboss/standalone/log - server.log
Assurance Gateway NFV Director	/var/opt/HPE/nfvd/log - nfv-director*.log

Regular archival/cleanup of these logs is recommended to avoid filling up the disk space.

You can use the RHEL command ‘df -h’ to get file system disk space usage.

By default SiteScope Self Monitor VNF Component for log_monitor is disabled. If it is enabled, SiteScope may return a "java.lang.OutOfMemoryError" error when the memory allocated to SiteScope runs out.
In order to overcome this issue, any of the following steps can be adopted :

1. Increase the amount of memory availalble to SiteScope, i.e. Java virtual memory of sitescope.
2. It may be necessary to change the behavior of the application generating the log file to create a new log file when it reaches a certain size to keep SiteScope from using all available memory, i.e. need to rotate the log file size
3. Additional fix can be Do not enable all monitors log_monitor, i.e. allow logging for certain components only.

Chapter 6 NFV Director analytics

On: <AA_HOST>
Login: root

By default, NFV Director analytics and capacity calculation features are disabled.
In order to enable analytics in NFV D, set STARTUP_ANALYTICS to TRUE in /var/opt/HPE/nfvd/conf/nfvd.properties.
In order to enable capacity calculation in NFV D, set CAPACITY_CALCULATION to TRUE in /var/opt/HPE/nfvd/conf/nfvd.properties.

The topology files are created in CSV format and exported to the following location: `/var/opt/HP/nfvd/DataDirectory/Topology.`
The format of the csv file name will be:
`TOPOLOGY_<ARTIFACTFAMILY><ARTIFACTCATEGORY>_<HOST>_<TIMESTAMP>.csv.`
Assurance receives notifications from Fulfillment for many artifacts, but the `.csv` files are not generated for all the artifacts. The `.csv` files are generated only for the artifact families and categories configured in the `nfvd-analytics.properties` file. A default set of artifact families are configured in the `nfvd-analytics.properties` file. If we need to export any other artifacts then it has to be configured in nfvd-analytics.properties, The format to specify the artifacts to be exporte dis export. <ArtifactFamily>.<ArtifactCateogry>.<CategoryLabel>.<AttributeLabel>=true

Example:
`export.VIRTUAL_MACHINE.GENERIC.GENERAL.NAME=true`

Any valid artifact can be exported. Set the export.<ArtifactFamily>.<ArtifactCateogry>.<CategoryLabel>.<AttributeLabel>=true

Example:
`export.MONITOR.GENERIC.GENERAL.NAME=true`

6.1 Export topology

The tool TriggerExportAllTopology.sh dumps the Assurance data into CSV format for consumption by analytics. By default, the script works in https mode. In case http mode is required, use '-m http' option.

```
# cd /opt/HPE/nfvd/bin
# ./TriggerExportAllTopology.sh –m http

Usage: TriggerExportAllTopology.sh [OPTIONS...]
 -h <<Hostname or IPADDRESS of Assurance Gateway>>
 -p <<Assurance Gateway JBOSS PORT>>
 -m <<https or http>>
```

6.2 Capacity recalculation utility

The tool TriggerCapacityRecalculation.sh tool calculates the free, available, and used resources in the infrastructure. By default, the script works in https mode. In case http mode is required, use '-m http' option.

```
# 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>>
```

6.3 Export KPI metrics

The metrics information generated from SiteScope are exported to a `.csv` file and the file will be present in the following directory:
`/var/opt/HPE/nfvd/DataDirectory/Metrics`
The metrics information is triggered from SiteScope for a predefined interval. Please refer to the installation guide for more details.
By default NFVD doesn't export KPI Metrics to CSV files, If you need to export KPI Metricis to CSV files then set STARTUP_ANALYTICS=TRUE in /var/opt/HPE/nfvd/conf/nfvd.properties. By default KPI Metrics will be updated to Neo4j and UPDATE_MONITOR_KPI_VALUE will be TRUE.
If the KPI Metrics should not be updated to Neo4j then set UPDATE_MONITOR_KPI_VALUE=false in /var/opt/HPE/nfvd/conf/nfvd.properties.

The following table lists the columns in the `.csv` file.

Table 4: KPI metrics fileds

Field	Field name	Description/Comment
1	`COLLECTOR`	The application collecting the data, which is always SiteScope.
2	`COLLECTOR HOST`	SiteScope hostname.
3	`GROUP NAME`	Name of the Group.
4	`GROUP DESCRIPTION(OPTIONAL)`	Group description, if entered for the group.
6	`TYPE`	Type of the Monitor e.g. Memory, CPU, Custom Monitor, etc.
7	`TARGET`	Monitored remote server.
8	`TARGET IP`	IP address of the monitored remote server.
9	`TIMESTAMP`	Time of the measurement.
10	`MONITOR QUALITY`	Status as determined by the monitor's thresholds. Possible values: • 0 – no data (no thresholds defined)

		• 1 – informational (good) • 2 –warning • 3 – critical
11	SOURCE TEMPLATE NAME	Name of the source template.
12	MONITOR NAME	User-defined monitor name.
13	MONITOR DESC(OPTIONAL)	Monitor description, if entered for the monitor.
14	VM ARTIFACT ID	ARTIFACT ID of the VM.
15	HYPERVISOR ID	ARTIFACT ID of the Hypervisor.
16	VIM ID	ARTIFACT ID of the VIM.
17	COUNTER 1 QUALITY	Status of the counter as determined by the counter's threshold. Possible values: • 0 – no data (no thresholds defined) • 1 – informational (good) • 2 – warning • 3 – critical
18	COUNTER 1 STATUS (OPTIONAL)	
19	COUNTER1 DESCRIPTION(OPTIONAL)	Monitor description, if entered for the monitor.
20	COUNTER 1 NAME	Counter name.
21	COUNTER 1 VALUE	Counter value.
22	COUNTER 2 QUALITY	
23	COUNTER 2 STATUS	
24	COUNTER2 DESCRIPTION	
25	COUNTER2 NAME	

The following example shows a sample `.csv` file.

```
COLLECTOR,COLLECTOR HOST,General.Name,GROUP DESCRIPTION,TYPE,TARGET,TARGET
IP,TIMESTAMP,MONITOR QUALITY,SOURCE TEMPLATE NAME,MONITOR
DESC,MONITOR_TYPE,MONITOR_ARTIFACT_ID,MONITORED_ENTITY_ID,MONITORED_ENTITY_FAMILY,MONITORED_
ENTITY_CATEGOORY,VM_HYPERVISOR_ID,VM_VIM_ID,COUNTER NAME1,COUNTER VALUE1,COUNTER STATUS
1,COUNTER DESCRIPTION1,COUNTER QUALITY1,COUNTER NAME2,COUNTER VALUE2,COUNTER STATUS
2,COUNTER DESCRIPTION2,COUNTER QUALITY2,COUNTER NAME3,COUNTER VALUE3,COUNTER STATUS
3,COUNTER DESCRIPTION3,COUNTER QUALITY3,COUNTER NAME4,COUNTER VALUE4,COUNTER STATUS
4,COUNTER DESCRIPTION4,COUNTER QUALITY4,COUNTER NAME5,COUNTER VALUE5,COUNTER STATUS
5,COUNTER DESCRIPTION5,COUNTER QUALITY5,COUNTER NAME6,COUNTER VALUE6,COUNTER STATUS
6,COUNTER DESCRIPTION6,COUNTER QUALITY6,COUNTER NAME7,COUNTER VALUE7,COUNTER STATUS
7,COUNTER DESCRIPTION7,COUNTER QUALITY7,COUNTER NAME8,COUNTER VALUE8,COUNTER STATUS
8,COUNTER DESCRIPTION8,COUNTER QUALITY8,COUNTER NAME9,COUNTER VALUE9,COUNTER STATUS
9,COUNTER DESCRIPTION9,COUNTER QUALITY9,COUNTER NAME10,COUNTER VALUE10,COUNTER STATUS
10,COUNTER DESCRIPTION10,COUNTER QUALITY10
SiteScope,nfvdvm31,VIRTUAL_MACHINE OPENSTACK CPU,(MONITOR_ARTIFACT_ID=0aad1b44-8301-49c5-
ad17-a771d58f208e)(MONITOR_TYPE=CPU)(MONITORED_ENTITY_ID=4e93e066-e084-4949-bdf6-
a017dd236b00)(MONITORED_ENTITY_FAMILY=VIRTUAL_MACHINE)(MONITORED_ENTITY_CATEGORY=GENERIC)(VM
_HYPERVISOR_ID=7d941343-0170-4317-909a-71a413ca57b6)( VM_VIM_ID=7d941343-0170-4317-909a-
```

```
71a413ca57b6)(counterName=cpu_usage_average),Custom Monitor,nfvdvm31,unknown host,2015-06-
18T11:21:48.887+0000,3,NFVDirector/VIRTUAL_MACHINE/OPENSTACK/CPU,7d941343-0170-4317-909a-
71a413ca57b6,null,Custom Monitor,0aad1b44-8301-49c5-ad17-a771d58f208e,4e93e066-e084-4949-
bdf6-a017dd236b00,VIRTUAL_MACHINE,null,7d941343-0170-4317-909a-71a413ca57b6,7d941343-0170-
4317-909a-71a413ca57b6,cpu_usage_average,No data,0,null,3
```

Chapter 7 Securing communication with GUI

By default, the communication between Fulfillment and Assurance is using the HTTP protocol.

Note:
It is recommended to use customer generated private certificates for secure communication.

Note:
Configuration steps using a sample certificate for illustration purpose is described in Annex 1: "Securing communication with sample certificate".

7.1 Configuring GUI to use Secure Socket Layer protocol:

Refer to the following sections in HPE Unified OSS Console 2.3.0 Installation and Configuration Guide

- 17.11 Secure Socket Layer (SSL/TLS)

7.2 Enabling secure connection in GUI:

On: <GUI_HOST>
Login: uoc

➢ Step 1: create the key and certificate request

```
openssl genrsa -des3 -out server.key 2048

        Generating RSA private key, 2048 bit long modulus
        ..............................................................+++
        .........+++
        e is 65537 (0x10001)
        Enter pass phrase for server.key: <pwd_server_key_value>
        Verifying - Enter pass phrase for server.key: <pwd_server_key_value>

openssl req -new -key server.key -out server.csr
        Enter pass phrase for server.key: <pwd_server_key_value>
        You are about to be asked to enter information that will be incorporated
        into your certificate request.
        What you are about to enter is what is called a Distinguished Name or a DN.
        There are quite a few fields but you can leave some blank
        For some fields there will be a default value,
        If you enter '.', the field will be left blank.
        -----
        Country Name (2 letter code) [XX]: <enter_value>
        State or Province Name (full name) []:<enter_value>
        Locality Name (eg, city) [Default City]: <enter_value>
        Organization Name (eg, company) [Default Company Ltd]: <enter_value>
        Organizational Unit Name (eg, section) []:<enter_value>
        Common Name (eg, your name or your server's hostname) []:<enter_value>
        Email Address []:
```

```
        Please enter the following 'extra' attributes
        to be sent with your certificate request
        A challenge password []:
        An optional company name []:


mv server.key server.key.org
openssl rsa -in server.key.org -out server.key
        Enter pass phrase for server.key.org: <pwd_server_key_value>
        writing RSA key
```

- Step 2: Create certicate using the certificate request server.cr that has been created
- Step 3: copy the key, request and certificate to /var/opt/uoc2/server/public/ssl/
- Step 4: Convert x509 Cert and Key to a pkcs12 file

```
cd /var/opt/uoc2/server/public/ssl

openssl pkcs12 -export -in server.crt -inkey server.key -out server.p12 -name idpcert -CAfile ca.crt -caname root
        Note: Make sure you put a password on the p12 file - otherwise you'll get a null reference exception when you try to
import it.

        Enter Export Password: <p12_pwd>
        Verifying - Enter Export Password: <p12_pwd>
```

- Step 5: Convert the pkcs12 file to a java keystore

```
keytool -importkeystore -deststorepass <idp_ks_pwd> -destkeypass <idp_ks_pwd> -destkeystore
/var/opt/uoc2/server/public/ssl/idpcertstore.jks -srckeystore server.p12 -srcstoretype PKCS12 -srcstorepass <p12_pwd> -alias idpcertks
```

- Step 6: Create JBOSS Vault and Vault keystore

```
keytool -genseckey -alias vault -storetype jceks -keyalg AES -keysize 128 -storepass <vault_ks_pass> -keypass <vault_ks_pass> -keystore
/var/opt/uoc2/server/public/ssl/vault-jks.keystore
```

- Step 7: Add secure value to vault keystore

```
/opt/uoc2/jboss-eap-6.4/bin/vault.sh -k /var/opt/uoc2/server/public/ssl/vault-jks.keystore -p <vault_ks_pass> -e /var/opt/uoc2/server/public/ssl
-s 24681359 -i 88 -v vault -b idpjks -a pwd -x <idp_ks_pwd>

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

         JBoss Vault

        JBOSS_HOME: /opt/uoc2/jboss-eap-6.4

        JAVA: /usr/lib/jvm/jre-1.8.0-openjdk.x86_64/bin/java

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

        Mar 14, 2017 1:29:26 PM org.picketbox.plugins.vault.PicketBoxSecurityVault init
        INFO: PBOX000361: Default Security Vault Implementation Initialized and Ready
        Secured attribute value has been stored in vault.
        Please make note of the following:
        ********************************************
```

```
        Vault Block:idpjks
        Attribute Name:pwd
        Configuration should be done as follows:
        VAULT::idpjks::pwd::1
        ************************************************
        Vault Configuration in configuration file:
        ************************************************
        ...
        </extensions>
        <vault>
          <vault-option name="KEYSTORE_URL" value="/var/opt/uoc2/server/public/ssl/vault-jks.keystore"/>
          <vault-option name="KEYSTORE_PASSWORD" value="<masked_ vault_ks_pass>"/>
          <vault-option name="KEYSTORE_ALIAS" value="vault"/>
          <vault-option name="SALT" value="24681359"/>
          <vault-option name="ITERATION_COUNT" value="88"/>
          <vault-option name="ENC_FILE_DIR" value="/var/opt/uoc2/server/public/ssl/"/>
        </vault>
        <management> ...
        ************************************************



/opt/uoc2/jboss-eap-6.4/bin/vault.sh -k /var/opt/uoc2/server/public/ssl/vault-jks.keystore -p <vault_ks_pass> -e /var/opt/uoc2/server/public/ssl
-s 24681359 -i 88 -v vault -b idpjks -a ks -x /var/opt/uoc2/server/public/ssl/idpcertstore.jks

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

        JBoss Vault

        JBOSS_HOME: /opt/uoc2/jboss-eap-6.4

        JAVA: /usr/lib/jvm/jre-1.8.0-openjdk.x86_64/bin/java

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

        Mar 14, 2017 2:07:15 PM org.picketbox.plugins.vault.PicketBoxSecurityVault init
        INFO: PBOX000361: Default Security Vault Implementation Initialized and Ready
        Secured attribute value has been stored in vault.
        Please make note of the following:
        ************************************************
        Vault Block:idpjks
        Attribute Name:ks
        Configuration should be done as follows:
        VAULT::idpjks::ks::1
        ************************************************
        Vault Configuration in configuration file:
        ************************************************
        ...
        </extensions>
        <vault>
          <vault-option name="KEYSTORE_URL" value="/var/opt/uoc2/server/public/ssl/vault-jks.keystore"/>
         <vault-option name="KEYSTORE_PASSWORD" value="<masked_ vault_ks_pass>"/>
         <vault-option name="KEYSTORE_ALIAS" value="vault"/>
        <vault-option name="SALT" value="24681359"/>
        <vault-option name="ITERATION_COUNT" value="88"/>
        <vault-option name="ENC_FILE_DIR" value="/var/opt/uoc2/server/public/ssl/"/>
        </vault><management> ...
        ************************************************



/opt/uoc2/jboss-eap-6.4/bin/vault.sh -k /var/opt/uoc2/server/public/ssl/vault-jks.keystore -p <vault_ks_pass> -e /var/opt/uoc2/server/public/ssl
-s 24681359 -i 88 -v vault -b idpjks -a ksalias -x idpcertks

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

```
JBoss Vault

JBOSS_HOME: /opt/uoc2/jboss-eap-6.4

JAVA: /usr/lib/jvm/jre-1.8.0-openjdk.x86_64/bin/java

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

Mar 14, 2017 2:08:06 PM org.picketbox.plugins.vault.PicketBoxSecurityVault init
INFO: PBOX000361: Default Security Vault Implementation Initialized and Ready
Secured attribute value has been stored in vault.
Please make note of the following:
********************************************
Vault Block:idpjks
Attribute Name:ksalias
Configuration should be done as follows:
VAULT::idpjks::ksalias::1
********************************************
Vault Configuration in configuration file:
********************************************
...
</extensions>
<vault>
  <vault-option name="KEYSTORE_URL" value="/var/opt/uoc2/server/public/ssl/vault-jks.keystore"/>
  <vault-option name="KEYSTORE_PASSWORD" value="<masked_ vault_ks_pass>"/>
  <vault-option name="KEYSTORE_ALIAS" value="vault"/>
  <vault-option name="SALT" value="24681359"/>
  <vault-option name="ITERATION_COUNT" value="88"/>
  <vault-option name="ENC_FILE_DIR" value="/var/opt/uoc2/server/public/ssl/"/>
</vault><management> ...
********************************************
```

- Step 8: Update UOC, couchDB and JBOSS configuration files

- UOC

```
vi /var/opt/uoc2/server/public/conf/config.json

        "server" : {
                "protocol" : "https",
                "port" : "3443",
                "privateKey" : "server.key",
                "certificate" : "server.crt",
                "secureProtocol" : "TLSv1_method"
        },

        "saml" : {
                "idp" : {
                        "entryPoint" : "https://<hostname>:38443/idp",
                        "identifierFormat" : "urn:oasis:names:tc:SAML:2.0:nameid-format:entity",
                        "certificate" : "server.crt",
                        "acceptedClockSkewMs" : -1
                },

                "sp" : {
                        "issuer" : "https:// <hostname>:3443",
                        "privateKey" : "server.key"
                },
```

```
                "signature" :  false ,
                "encryption" :  false,
                "postAuthCallback" :  "nfvd-post-authentication-module"
        },
```

- couchDB

On: <GUI_HOST>
Login: couchdb

To use the same certificate and key as UOC you need to copy them to a write and read access permission directory for user coucdb

```
mkdir /opt/couchdb/var/config/couchdb/ssl

cp /var/opt/uoc2/server/public/ssl/server.crt /var/opt/uoc2/server/public/ssl/server.key /opt/couchdb/var/config/couchdb/ssl
```

Enable https connection

```
vi /opt/couchdb/var/config/couchdb/local.ini


        [ssl]
        cert_file = /opt/couchdb/var/config/couchdb/ssl/server.crt
        key_file = /opt/couchdb/var/config/couchdb/ssl/server.key

        [daemons]
        ; enable SSL support by uncommenting the following line and supply the PEM's below.
        ; the default ssl port CouchDB listens on is 6984
        httpsd = {couch_httpd, start_link, [https]}
```

Disable http connection

```
vi /opt/couchdb/etc/couchdb/default.ini

        [daemons]
        …
        ; httpd={couch_httpd, start_link, []}
        …
```

- JBOSS

On: <GUI_HOST>
Login: uoc

Retrieve the fault configuration from the step 7 output

```
vi /opt/uoc2/jboss-eap-6.4/standalone/configuration/standalone.xml
```

Add vault configuration

```
...
</extensions>

<vault>
  <vault-option name="KEYSTORE_URL" value="/var/opt/uoc2/server/public/ssl/vault-jks.keystore"/>
  <vault-option name="KEYSTORE_PASSWORD" value="<masked_ vault_ks_pass>"/>
  <vault-option name="KEYSTORE_ALIAS" value="vault"/>
  <vault-option name="SALT" value="24681359"/>
  <vault-option name="ITERATION_COUNT" value="88"/>
  <vault-option name="ENC_FILE_DIR" value="/var/opt/uoc2/server/public/ssl/"/>
</vault>

<management>
...
```

Replace http by https connector

```
<subsystem xmlns="urn:jboss:domain:web:2.2" default-virtual-server="default-host" native="false">
        <connector name="https" protocol="HTTP/1.1" scheme="https" socket-binding="https" enable-lookups="false"
secure="true">
                <ssl name="jboss-ssl" key-alias="${VAULT::idpjks::ksalias::1}" password="${VAULT::idpjks::pwd::1}"
certificate-key-file="${VAULT::idpjks::ks::1}" protocol="TLSv1"/>
        </connector>
        <virtual-server name="default-host" enable-welcome-root="true">
                <alias name="localhost"/>
                <alias name="example.com"/>
        </virtual-server>
</subsystem>
```

- Step 9: restart GUI services

On: <GUI_HOST>
Login: root

```
service nfvd_gui_services restart
```

Chapter 8 Securing communication with Fulfillment

On: <FF_HOST>
Login: root

8.1 Configuring Fulfillment to use Secure Socket Layer Protocol

Refer to the following sections in HPE Service Activator V62-1A Installation Guide for the RHEL:

- D Security Considerations
- E Configuring Service Activator to Use Secure Socket Layer (SSL) Protocol.

8.2 Enabling secure connection in Fulfillment

- Stop HPE Service Activator
- Edit the file */etc/opt/OV/ServiceActivator/config/nfvd.properties*

```
assurance.rest.api.endpoint.key=https://<<AA_HOST>>:18443
```

On: <INSTALLER_HOST>
Login: root

- Create the script update_http.sql in /tmp/

```
cd /tmp

vi update_https.sql

update NFVD_CONFIGURATION set CONFIG_VALUE='https://<<AA_HOST>>:18443' where
CONFIG_KEY='assurance.service.url';
quit;
/
```

- Launch the command :

```
sqlplus64 -L "nfvd/nfvd@//<<DB_HOST>>:<<DB_PORT>>/<<DB_NAME>>" @./update_https.sql
```

On: <FF_HOST>
Login: root

- Edit the file /etc/opt/OV/ServiceActivator/config/nfv_manager.xml

```
…

<parameter><name>SOSAFwdEndpoint</name><value> http://<<AA_HOST>>:18080/ae-services-
impl/NGWSServiceService/NGWSServiceImpl</value></parameter>

…
```

- Start HPSA

Chapter 9 Securing communication with Assurance

By default, the communication between Fulfillment and Assurance is using the HTTP protocol.

Note:
It is recommended to use customer generated private certificates for secure communication. Contact your certificate authority to create a new certificate.

Note:
All certificates refered for illustration in the following sections are assumed to be customer generated private certificates which is available in a truststore.

9.1 Prerequisites for secure communication

Once Assurance Gateway is running in SSL mode, all client accessing AGW through REST API should contain public certificate exposed by AGW, in their respective java Trust Stores.

Export public key

Executing below command gives a valid public certificate (AssurancePub.cer) to be used by AGW clients.

```
keytool -export -keystore ${user.home}/opensslKeys/KEYTOOL/assuranceKeystore.jks -alias vault -file AssurancePub.cer
    where
    Assurnace.jks is the truststore containing cutomer generated private certificate
```

9.1.1 Enabling secure connection in Assurance

On: <AA_HOST>
Login: root

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

- Setup keystore password by invoking command */opt/HPE/nfvd/tpp/jboss/bin/vault.sh*. Reply to interactive questions with answers in red:

```
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: ${user.home}/opensslKeys/KEYTOOL/assuranceKeystore.jks
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
```

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 and Update the <vault> and <connector> tags as explained below:

```
<?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="${user.home}/opensslKeys/KEYTOOL/assuranceKeystore.jks"/>
     <vault-option name="KEYSTORE_PASSWORD" value="MASK-3y28rCZlcKR"/>
     <vault-option name="KEYSTORE_ALIAS" value="vault"/>
     <vault-option name="SALT" value="124345678"/>
     <vault-option name="ITERATION_COUNT" value="50"/>
     <vault-option name="ENC_FILE_DIR" value="${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="${VAULT::keystore_pass::password::NmZiYmRmOGQtMTYzZS00MjE3LTllODMtZjI4OGM2NGJmODM4TElORV9CUkVBS3ZhdWx0}"
                        certificate-key-file="${user.home}/opensslKeys/KEYTOOL/assuranceKeystore.jks"/>  <!--(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>
```

- Start Assurance Gateway

9.1.2 Fulfillment

- Copy assurance SSL public certificate (AssurancePub.cer) from AGW box to FF Box. (copy to /tmp)

- Create a new java trustore for fulfilment or use one if already created. Post that import the AGW certificate (AssurancePub.cer) in truststore.

Below command creates new Trust Store (FFTrustStore.jts) and imports AGW public certificate in the same.

```
# cd /opt/HP/jboss/bin/
# keytool -import -file /tmp/AssurancePub.cer -alias assuranceCA -keystore FFTrustStore.jts
(Password be asked for new Trust Store. Remember the same as same will be used while referring truststore)
e.g. <ffTrustPass>
```

- In /opt/HP/jboss/bin/standalone.conf, add one more java option as below:

```
# vi /opt/HP/jboss/bin/standalone.conf

< ADD BELOW LINE AT END OF FILE >
JAVA_OPTS="$JAVA_OPTS -Djavax.net.ssl.trustStore={DEPLOY_ROOT}/opt/HP/jboss/bin/ FFTrustStore.jts
 -Djavax.net.ssl.trustStorePassword=ffTrustPass"
```

- Restart Fulfilment.

9.1.3 UCA for EBC

- Copy assurance SSL public certificate (AssurancePub.cer) from AGW box to UCA-EBC Box. (copy to /tmp)

- In case UCA-EBC is on same machine as Fulfilment, then same Truststore (Refer 9.1.1) can be referred. Else Follow below step:

  This command creates new Trust Store (UCATrustStore.jts) and imports AGW public certificate in the same.

```
# cd {DEPLOY_ROOT}/var/opt/UCA-EBC/instances/default/conf/
# keytool -import -file AssurancePub.cer -alias assuranceCA -keystore UCATrustStore.jts
(Password be asked for new Trust Store. Remember the same as same will be used while referring truststore)
e.g. <ucaTrustPass>
```

- Update JVM Arguments, to consider the trustsore (UCATrustStore.jts) while starting.

```
# cd {DEPLOY_ROOT /var/opt/UCA-EBC/instances/default/conf
# vi uca-ebc.options

Add below line in file
JVM_OPTS="$JVM_OPTS -Djavax.net.ssl.trustStore=/opt/HPE/nfvd/tpp/jboss/standalone/configuration/FTStore.jts -
Djavax.net.ssl.trustStorePassword= ucaTrustPass”
```

- Restart uca-ebc

9.1.4 SiteScope

Sitescope has mechanism to pull the certificate automatically. So no changes required specific to SSL communication with AGW.

9.1.5 Discovery (User End Point Trigger)

1. Enable HTTPS

a) reconciliation-endpoints.properties

Location: /opt/openmediation-70/ips/fulfillment-ca-10/etc/config/reconciliation-endpoints.properties

```
# vi /opt/openmediation-70/ips/fulfillment-ca-10/etc/config/reconciliation-endpoints.properties
[...]
#HTTP URL
#recon.rest.endpoint=http://0.0.0.0:18989/
#HTTPS URL
recon.rest.endpoint=https://0.0.0.0:18999/
httpj.port=18999
httpj.sec.keystore.type=JKS
httpj.sec.keystore.file=/opt/HPE/nfvd/tpp/jboss/standalone/configuration/sample.jks
httpj.sec.keystore.password=samplePass
#httpj.sec.truststore.type=JKS
#httpj.sec.truststore.file=/tmp/assuranceKeystore.jks
#httpj.sec.truststore.password=samplePass
```

b) reconciliaition-rest-route.xml

Location: /opt/openmediation-70/ips/fulfillment-ca-10/etc/routeContexts/external-discovery-trigger-routes/reconciliation-rest-route.xml
import resource block:

```
# vi /opt/openmediation-70/ips/fulfillment-ca-10/etc/routeContexts/external-discovery-trigger-routes/https-server-config.xml

<beans
[...]
   <!-- HTTPS -->
   <import resource="file:${ca.cfg.dir}/routeContexts/external-discovery-trigger-routes/https-server-config.xml" />
   <!-- HTTPS -->
[...]
</beans>
```

c) https-server-config.xml

Location: /opt/openmediation-70/ips/fulfillment-ca-10/etc/routeContexts/external-discovery-trigger-routes/https-server-config.xml
File content httpj:engine-factory block should be exactly as below:
(Note: sec: trusManagers and sec:cipherSuitesFilter are optional)

```
# vi /opt/openmediation-70/ips/fulfillment-ca-10/etc/routeContexts/external-discovery-trigger-routes/https-server-config.xml

<beans
[...]
<httpj:engine-factory bus="cxf">
```

```
    <httpj:engine port="${rest.endpoint.https.port}">
      <httpj:tlsServerParameters>
        <sec:keyManagers keyPassword="${httpj.sec.keystore.password}">
          <sec:keyStore type="${httpj.sec.keystore.type}" password="${httpj.sec.keystore.password}"
file="${httpj.sec.keystore.file}"/>
        </sec:keyManagers>
        <sec:clientAuthentication want="false" required="false"/>
      </httpj:tlsServerParameters>
    </httpj:engine>
  </httpj:engine-factory>
</beans>
```

2. Disable HTTPS/ Enable HTTP

a) reconciliation-endpoints.properties

Location: /opt/openmediation-70/ips/fulfillment-ca-10/etc/config/reconciliation-endpoints.properties

```
# vi /opt/openmediation-70/ips/fulfillment-ca-10/etc/config/reconciliation-endpoints.properties

[…]
#HTTP URL
recon.rest.endpoint=http://0.0.0.0:18989/
#HTTPS URL
#recon.rest.endpoint=https://0.0.0.0:18999/
#httpj.port=18999
#httpj.sec.keystore.type=JKS
#httpj.sec.keystore.file=/opt/HPE/nfvd/tpp/jboss/standalone/configuration/sample.jks
#httpj.sec.keystore.password=samplePass
#httpj.sec.truststore.type=JKS
#httpj.sec.truststore.file=/opt/HPE/nfvd/tpp/jboss/standalone/configuration/sample.jks
#httpj.sec.truststore.password=samplePass
```

b) reconciliation-rest-route.xml

Comment https completely:
Location: */opt/openmediation-70/ips/fulfillment-ca-10/etc/routeContexts/external-discovery-trigger-routes/reconciliation-rest-route.xml*

```
# vi /opt/openmediation-70/ips/fulfillment-ca-10/etc/routeContexts/external-discovery-trigger-
routes/reconciliation-rest-route.xml

[…]
<!-- HTTPS -->
 <!-- <import resource="file:${ca.cfg.dir}/routeContexts/external-discovery-trigger-routes/https-server-
config.xml" /> -->
 <!-- HTTPS -->
```

c) https-server-config.xml

Location: */opt/openmediation-70/ips/fulfillment-ca-10/etc/routeContexts/external-discovery-trigger-routes/https-server-config.xml*
Property file content should be exactly as below:

```
# vi /opt/openmediation-70/ips/fulfillment-ca-10/etc/routeContexts/external-discovery-trigger-routes/https-
server-config.xml
<beans
[…]
<httpj:engine-factory bus="cxf">
     <httpj:engine port="${rest.endpoint.https.port}">
       <httpj:tlsServerParameters>
         <sec:keyManagers keyPassword="${httpj.sec.keystore.password}">
```

```
            <sec:keyStore type="${httpj.sec.keystore.type}" password="${httpj.sec.keystore.password}"
file="${httpj.sec.keystore.file}"/>
          </sec:keyManagers>
          <sec:clientAuthentication want="false" required="false"/>
        </httpj:tlsServerParameters>
      </httpj:engine>
    </httpj:engine-factory>
</beans>
```

3. Truststore Configuration (optional)

NOTE: Optional configuration for truststore if required can be done

a) reconciliation-endpoints.properties

Location: /opt/openmediation-70/ips/fulfillment-ca-10/etc/config/reconciliation-endpoints.properties

```
# vi /opt/openmediation-70/ips/fulfillment-ca-10/etc/config/reconciliation-endpoints.properties
[…]
#HTTP URL
#recon.rest.endpoint=http://0.0.0.0:18989/
#HTTPS URL
recon.rest.endpoint=https://0.0.0.0:18999/
httpj.port=18999
httpj.sec.keystore.type=JKS
httpj.sec.keystore.file=/opt/HPE/nfvd/tpp/jboss/standalone/configuration/sample.jks
httpj.sec.keystore.password=samplePass
httpj.sec.truststore.type=JKS
httpj.sec.truststore.file=/opt/HPE/nfvd/tpp/jboss/standalone/configuration/sample.jks
httpj.sec.truststore.password=samplePass
```

b) reconciliaition-rest-route.xml

Location: /opt/openmediation-70/ips/fulfillment-ca-10/etc/routeContexts/external-discovery-trigger-routes/reconciliation-rest-route.xml
import resource block:

```
# vi /opt/openmediation-70/ips/fulfillment-ca-10/etc/routeContexts/external-discovery-trigger-routes/https-
server-config.xml
<beans
[…]
  <!-- HTTPS -->
  <import resource="file:${ca.cfg.dir}/routeContexts/external-discovery-trigger-routes/https-server-
config.xml" />
  <!-- HTTPS -->
[…]
</beans>
```

c) Changes in https-server-config.xml

Location: /opt/openmediation-70/ips/fulfillment-ca-10/etc/routeContexts/external-discovery-trigger-routes/https-server-config.xml

```
# vi /opt/openmediation-70/ips/fulfillment-ca-10/etc/config/https-server-config.xml
[…]
<httpj:engine-factory bus="cxf">
    <httpj:engine port="${rest.endpoint.https.port}">
      <httpj:tlsServerParameters>
        <sec:keyManagers keyPassword="${httpj.sec.keystore.password}">
          <sec:keyStore type="${httpj.sec.keystore.type}" password="${httpj.sec.keystore.password}"
file="${httpj.sec.keystore.file}"/>
        </sec:keyManagers>
        <sec:trustManagers>
          <sec:keyStore type="${httpj.sec.truststore.type}" password="${httpj.sec.truststore.password}"
file="${httpj.sec.truststore.file}"/>
```

```
            </sec:trustManagers>
            <!--<sec:cipherSuitesFilter>
               <sec:include>.*_WITH_3DES_.*</sec:include>
               <sec:include>.*_WITH_DES_.*</sec:include>
               <sec:exclude>.*_WITH_NULL_.*</sec:exclude>
               <sec:exclude>.*_DH_anon_.*</sec:exclude>
            </sec:cipherSuitesFilter>-->
            <sec:clientAuthentication want="false" required="false"/>
         </httpj:tlsServerParameters>
      </httpj:engine>
   </httpj:engine-factory>
```

Chapter 10 Securing communication between OpenStack and SiteScope

10.1 Enabling SSL communication between OpenStack and SiteScope

The following changes are required to enable SSL communication in OpenStack components:

- Obtain X.509 Certificate.
- Configure the X.509 Certificate in OpenStack by adding the following parameters to the `/etc/keystone.conf` file.

```
[ssl]
enable = True
certfile = <path to keystone.pem>
keyfile = <path to keystonekey.pem>
ca_certs = <path to ca.pem>
cert_required = True
```

Where

- `certfile` is the path to the Identity Service public certificate file.
- `keyfile` is the path to the Identity Service private certificate file. If you include the private key in the `certfile` parameter, you can omit the `keyfile`.
- `ca_certs` is the path to the CA trust chain.
- `cert_required` indicates whether the client certificate is required.

10.2 Enabling SSH between OpenStack and SiteScope

On: <AA_HOST>
Login: root

SSH communication is required to execute NFVI script monitors. Follow these steps to enable SSH communication.

1. Log in to the SiteScope machine as root user and execute the following command to generate the key.

   ```
   # ssh-keygen -t rsa
   ```

```
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
```

```
The key fingerprint is:
87:bc:83:12:6e:e4:db:18:ed:85:43:8c:31:47:53:fc root@osskemp1
The key's randomart image is:
+--[ RSA 2048]----+
|      oo.        |
|     . ..        |
|    o .  .       |
|     * . .E      |
|    + o S .      |
|   + + o o       |
|    * = +        |
|   . B o .       |
|    o o          |
+-----------------+
#
```

2. The generated public key is stored in the `/root/.ssh/id_rsa.pub` file. Check the contents of the `id_rsa.pub` file by executing the following command:

   ```
   # cat /root/.ssh/id_rsa.pub
   ```

```
ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAQEA1YWKnVXx3QPHTU8YGLpZFk8CblLJVHLLC+Uez6gZmoT+f1Vlz8nuKGbLFdTpFFHS
v5g3iiEODAzSPRohAfmtdYfcyHkyN5PKdU8aRhv4dgTkeKS19okGcuXC8RAlaGeC9pOxTFtx8+mwbnzZEoVLWYiNJ+3l
BeE5J3D9ePn7Y4Cxqs7f6oHOZiGn93wptnnkTjQBWjqEeWLbQTYdyPA07MvIzy8Qur1BQrTb8MyyzyTOz3nEjrd9YFmj
+khyqz1W6y0CIshCDJELQ8YmONcpoE9pHDba1sXVDVqUCWlZ67fx5vYxKa1QehlEl6t/2GE55CJtk34mBxc/o/PlkucC
SQ== root@host
#
```

3. Copy the `id_rsa.pub` file to the `/root/.ssh/` folder on the OpenStack machine.
4. Check if the `authorized_keys` file exists in the `/root/.ssh` folder. If the file does not exist, then create it by using the following command.

   ```
   touch authorized_keys
   ```

5. Append the contents of the `id_rsa.pub` to file to the `authorized_keys` file using the following command.

   ```
   # cat id_rsa.pub >> authorized_keys
   ```

6. Exit and try log in to the OpenStack Machine from the SiteScope Machine using SSH. If SSH has been configured correctly, log in should not require a password.
7. Repeat Steps 3 to 6 for all the OpenStack Nodes.

Chapter 11 Assurance configuration checker tool

This tool is useful for detecting and reporting most of common misconfigurations in NFVD which are required for normal working of Assurance.

Note: It is recommended to run this tool after any update to NFVD systems and for troubleshooting issues in NFVD functioning.

11.1 Introduction

This tool will check most common configuration problems identified as follows:

1. Assurance gateway process status
2. Missing JDBC settings for Alarm DB connection
3. Validation of assurance gateway jboss configuration i.e. standalone.xml file validation
   a. Jar file entry
   b. DB connection entry
   c. Protocol validation
4. UCA Value packs status check
5. KPI display rest service check
6. Fulfillment connection and status check
7. Self-Management Entities check
   a. VNF_COMPONENT Assurance
   b. VNF_COMPONENT Neo4j
   c. VNF_COMPONENT Site scope & Site scope license sync
   d. VNF_COMPONENT NOM
   e. VNF_COMPONENT UCA
8. Assurance endpoint configuration in fulfilment, (password less ssh login is required)
9. Assurance endpoint entries in Database of Fulfillment
10. Assurance and Fulfillment data synchronization
11. Discovery configuration and status check (Openstack CA, Fulfillment CA status check)

11.2 Usage

This tool is installed in the following location:
/opt/HPE/nfvd/bin/config_checker.sh
on assurance VM.

Dependencies jar files /opt/HPE/nfvd/lib

1. AssuranceConfigChecker.jar
2. oracle_jdbc.jar
3. uca-expert-engine-3.1.7.jar

Usage :

```
# /opt/HPE/nfvd/bin/config_checker.sh --help

Usage: config_checker.sh [options]
 where -options include:
 OPTIONAL:
   -l   enable or disable
        enable - will enable console logging in detail
        disable - will disable console logging in detail
```

Config checker without any parameters:

```
# /opt/HPE/nfvd/bin/config_checker.sh

-   Checking status of Assurance                                                    :[Ok]
-   Checking Assurance protocol(http) entry in Assurance standalone.xml             :[Ok]
-   Checking jar file entry in Assurance standalone.xml                             :[Ok]
-   Checking database entry in Assurance standalone.xml                             :[Ok]
-   Checking status of Fulfillment                                                  :[Ok]
-   Checking the entry of Assurance gateway in Fulfillment self management         :[Ok]
-   Checking the entry of NEO4J in Fulfillment self management                      :[Ok]
-   Checking the entry of  SiteScope in Fulfillment self management                 :[Ok]
-   Checking SiteScope License                                                      :[Ok]
-   Checking Assurance entries in Fulfillment nfvd.properties, Fulfillment Database, Assurance &
Fulfillment Sync :[Ok]
-   Checking the status of the KPI Rest Call                                        :[Ok]
-   Checking status of value packs                                                  :[Ok]
-   Total number of value packs running                                             :[7]
-   Checking consistency of uca host,port in the UCA config files                   :[Ok]
================================================================================
config_checker.sh execution ended sucessfully
For more details; Please Check /tmp/config_check.log file
================================================================================
```

Logger file and –l enable optional parameter

When option ”–l enable” is used more verbose details are printed on the console.

```
# vi /tmp/config_check.log
and
#/opt/HPE/nfvd/bin/config_checker.sh –l enable
-   Checking status of Assurance
        :[Ok]
    Assurance started
    extracting assurance gateway [http | https] protocol from
/opt/HPE/nfvd/tpp/jboss/standalone/configuration/standalone.xml... http [Ok]
-   Checking Assurance protocol(http) entry in Assurance standalone.xml                    :[Ok]
    http entry configured in Assurance standalone.xml file is correct
-   Checking jar file entry in Assurance standalone.xml                                        :[Ok]
    jar file under /opt/HPE/nfvd/tpp/jboss/standalone/deployments/ is matching with standalone.xml
configuration
-   Checking database entry in Assurance standalone.xml                                        :[Ok]
    Created database connection successfully
-   Checking status of Fulfillment
        :[Ok]
    Fulfillment host(15.154.112.28) is reachable
-   Checking the entry of Assurance gateway in Fulfillment self management                 :[Ok]
    Assurance IP/HOST(15.154.112.28)/PORT() configured in VNF_COMPONENT:ASSURANCE_GATEWAY is correct
-   Checking the entry of NEO4J in Fulfillment self management                                 :[Ok]
    Neo4J URL http://15.154.112.28:7474/db/data configured in VNF_COMPONENT:NEO4J is reachable
-   Checking the entry of  SiteScope in Fulfillment self management                        :[Ok]
    SIS URL(http://15.154.112.28:18888/SiteScope) configured in VNF_COMPONENT:SITESCOPE is reachable
-   Checking SiteScope License
        :[Ok]
     SiteScope license is valid
    Extracting NOM_HOST,NOM_ARTIFACTID entries of NOM in Fulfillment self management
    extracted 15.154.112.28 , 819582eb-4f35-49a1-b857-e0284c3c701a
    Extracting UCA_HOST,UCA_PORT entries of UCA in Fulfillment self management
    extracted 15.154.112.28 , 8090 entries of UCA in Fulfillment self management
    Extracting HPSA_HOST,HPSA_PORT,HPSA_HOST_USER entries of HPSA in Fulfillment self management
    extracted 15.154.112.28,8080,root entries of HPSA in Fulfillment self management
    Extracting ORACLE_HOST,ORACLE_PORT entries of Oracle in Fulfillment self management
    extracted 15.154.112.28,1521 entries of Oracle in Fulfillment self management
-   Checking Assurance entries in Fulfillment nfvd.properties, Fulfillment Database, Assurance &
Fulfillment Sync :
    /opt/HP/jboss/standalone/configuration/standalone.xml...copied
    /etc/opt/OV/ServiceActivator/config/nfvd.properties...copied
```

```
    Checking Assurance host in assurance.rest.api.endpoint.key in Fulfillment
/etc/opt/OV/ServiceActivator/config/nfvd.properties.... [Ok]
    Checking Assurance port in assurance.rest.api.endpoint.key in Fulfillment
/etc/opt/OV/ServiceActivator/config/nfvd.properties.... [Ok]
    Checking Assurance token in assurance.X-Auth-Token in Fulfillment
/etc/opt/OV/ServiceActivator/config/nfvd.properties.... [Ok]
    Please wait, proceeding to check Fulfillment and Assurance Syncronization....
    Checking assurance.service.mode in NFVD_CONFIGURATION table.... [Ok]
    Checking Assurance host in assurance.service.url in NFVD_CONFIGURATION table.... [Ok]
    Checking Assurance port in assurance.service.url in NFVD_CONFIGURATION table.... [Ok]
    Checking Assurance token in assurance.token in NFVD_CONFIGURATION table.... [Ok]
    Checking NFVD_SYNCHRONIZATION table for Fulfillment and Assurance sync.... [Ok]
    Fulfillment and Assurance Syncronization Established successfully


    Assurance entries in Fulfillment nfvd.properties, Fulfillment Database,  Assurance & Fulfillment
Sync : [Ok]


-   Checking the status of the KPI Rest Call
       :[Ok]
-   Checking status of value packs
       :[Ok]
-   Total number of value packs running                                                    :[7]
Value pack: UCA_NFVD_StatePropagation-4.2.0 [Running] All Scenarios are running. Flow is disabled.
Value pack: UCA_NFVD_Persistence_Valuepack-4.2.0 [Running] All Scenarios are running. Flow is disabled.
Value pack: UCA_NFVD_PublishToNomBus-4.2.0 [Running] All Scenarios are running. Flow is disabled.
Value pack: UCA_NFVD_Migration_Valuepack-4.2.0 [Running] All Scenarios are running. Flow is disabled.
Value pack: UCA_NFVD_Evaluate_Valuepack-4.2.0 [Running] All Scenarios are running. Flow is disabled.
Value pack: UCA_Automation_Foundation_UCA-V1.2.3-1A [Running] All Scenarios are running. Flow is
disabled.
Value pack: UCA_NFVD_ProblemDetection_Valuepack-4.2.0 [Running] All Scenarios are running. Flow is
disabled.
-   Checking consistency of uca host,port in the UCA config files              :
--------------------------------------------------------------------------------

    /var/opt/UCA-EBC/instances/default/conf/uca-ebc.properties
Line 7:uca.ebc.serverhost=0.0.0.0
Checking UCA_HOST=15.154.112.28 in uca.ebc.serverhost=0.0.0.0
Ok: [0.0.0.0] AA_HOST=15.154.112.28, UCA_HOST=15.154.112.28

Config : [Ok]

--------------------------------------------------------------------------------
    /var/opt/openmediation-70/containers/instance-0/ips/uca-ebc-ca-3.1/etc/uca-ebc-ca.properties
Line 2:uca.ebc.jms.broker.host=15.154.112.28

Checking UCA_HOST=15.154.112.28 in uca.ebc.jms.broker.host=15.154.112.28
Ok: [15.154.112.28]

Line 6:action-service.host=15.154.112.28

Checking UCA_HOST=15.154.112.28 in uca.ebc.jms.broker.host=15.154.112.28
Ok: [15.154.112.28]

Config : [Ok]

--------------------------------------------------------------------------------
    /var/opt/UCA-EBC/instances/default/deploy/UCA_Automation_Foundation_UCA-V1.2.3-
1A/conf/ExternalActionConfig.xml
Found: <consoleurl>http://15.154.112.28:8090/UCA_Automation_Foundation_UCA-V1.2.3-1A-
UCAAutomation/UCAService</consoleurl>

Checking UCA_HOST=15.154.112.28 in <consoleurl>[...]</consoleurl>
Ok: [15.154.112.28]
```

```
Checking UCA_Automation_Foundation_UCA-Version=V1.2.3-1A in <consoleurl>[...]</consoleurl>
Ok: [V1.2.3-1A]

Checking UCA_Automation_Foundation_UCA-Version=V1.2.3-1A in <version>V1.2.3-1A</version>
Ok: [V1.2.3-1A]

Config : [Ok]

--------------------------------------------------------------------------------
    /var/opt/UCA-EBC/instances/default/deploy/UCA_Automation_Foundation_UCA-V1.2.3-
1A/conf/UCAAutomation.properties
Checking UCA_HOST=15.154.112.28 in java.naming.provider.url=15.154.112.28
Ok: [15.154.112.28]

Checking UCA_HOST=15.154.112.28 in
UCACONSOLE_CA_URL=http://15.154.112.28:12500/UCAAutomationConsoleService/UCAAutomationConsoleService
Ok: [15.154.112.28]

Checking UCA_HOST=15.154.112.28 in
ucaebc_tomsawyer_port=http://15.154.112.28:8090/graphdisplay/?username=root&nodeId=0&profile=ucaatm
Ok: [15.154.112.28]

Info: Line 11:DB_DRIVER=oracle.jdbc.driver.OracleDriver
Info: Line 12:DB_URL=jdbc:oracle:thin:@15.154.112.28:1521:XE
Info: Line 13:DB_USER=NFV
Info: Line 14:DB_PASSWORD=NFV

Config : [Ok]

--------------------------------------------------------------------------------
    /var/opt/openmediation-70/containers/instance-0/ips/uca-autoconsole-ca-20/etc/config.properties
Checking UCA_HOST=15.154.112.28 in uca.uca-automation.host=0.0.0.0
Ok: [0.0.0.0]

Checking UCA_Automation_Foundation_UCA-Version=V1.2.3-1A in
uca.console.service=UCA_Automation_Foundation_UCA-V1.2.3-1A-UCAAutomation/UCAService
Ok: [V1.2.3-1A]

Checking UCA_HOST=15.154.112.28 in uca.console.host=15.154.112.28
Ok: [15.154.112.28]

Config : [Ok]

--------------------------------------------------------------------------------
    /var/opt/openmediation-70/containers/instance-0/ips/uca-hpsa-ca-20/etc/config.properties
1. Checking FF_HOST=15.154.112.28 in hpsa.host=15.154.112.28,2. In case UCA_HOST=FF_HOST then
hpsa.host=0.0.0.0 is allowed
Ok: [15.154.112.28] FF_HOST=15.154.112.28, UCA_HOST=15.154.112.28

Checking FF_PORT=8080 in hpsa.port=8080
Ok: [8080]

Info: Line 4:hpsa.userid=admin
Info: Line 12:hpsa.uca-automation.sync-service.host=0.0.0.0

Checking hpsa.uca-automation.sync-service.port != 8090 in hpsa.uca-automation.sync-service.port=8191
Ok: [8191]

Config : [Ok]

--------------------------------------------------------------------------------
    /etc/opt/OV/ServiceActivator/config/mwfm.xml
/etc/opt/OV/ServiceActivator/config/mwfm.xml...copied

Found:
```

```
<Param name="url"  value="http://15.154.112.28:8090/UCA_Automation_Foundation_UCA-V1.2.3-1A-
UCAAutomation/UCAService"/>

Checking UCA_HOST=15.154.112.28 in <Param name="url"  value=[...]"/>
Ok: [15.154.112.28]

Checking UCA_PORT=8090 in <Param name="url"  value=[...]"/>
Ok: [8090]

Checking UCA_Automation_Foundation_UCA-Version=V1.2.3-1A in <Param name="url"  value=[...]"/>
Ok: [V1.2.3-1A]

Config : [Ok]

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

Checking Assurance Rest URL Entry with http is uncommented : Ok

Checking AA_HOST=15.154.112.28 in Line 2:Assurance_Gateway_Rest_URL=http://15.154.112.28:18080
[15.154.112.28] : Ok

Config : [Ok]

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

Checking Assurance Rest URL Entry with http is uncommented : Ok

Checking AA_HOST=15.154.112.28 in Line 19:Assurance_Gateway_Rest_URL=http://15.154.112.28:18080
[15.154.112.28] : Ok

Config : [Ok]

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

Checking Assurance Rest URL Entry with http is uncommented : Ok

Checking AA_HOST=15.154.112.28 in Line 8:ASSURANCE_REST_URL=http://15.154.112.28:18080
[15.154.112.28] : Ok

Config : [Ok]

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

Checking Assurance Rest URL Entry with http is uncommented : Ok

Checking AA_HOST=15.154.112.28 in Line 2:Assurance_Gateway_Rest_URL=http://15.154.112.28:18080
[15.154.112.28] : Ok


Config : [Ok]

--------------------------------------------------------------------------------
    /var/opt/UCA-EBC/instances/default/conf/OrchestraConfiguration.xml
Found:
Line 7:<ValuePackNameVersion>UCA_NFVD_Persistence_Valuepack-4.2.0</ValuePackNameVersion>
Line 16:<ValuePackNameVersion>UCA_NFVD_ProblemDetection_Valuepack-4.2.0</ValuePackNameVersion>
Line 25:<ValuePackNameVersion>UCA_NFVD_StatePropagation-4.2.0</ValuePackNameVersion>
Line 34:<ValuePackNameVersion>UCA_NFVD_Migration_Valuepack-4.2.0</ValuePackNameVersion>
```

```
Line 44:<ValuePackNameVersion>UCA_NFVD_ProblemDetection_Valuepack-4.2.0</ValuePackNameVersion>
Line 53:<ValuePackNameVersion>UCA_Automation_Foundation_UCA-V1.2.3-1A</ValuePackNameVersion>
Line 63:<ValuePackNameVersion>UCA_Automation_Foundation_UCA-V1.2.3-1A</ValuePackNameVersion>
Line 69:<ValuePackNameVersion>UCA_NFVD_Evaluate_Valuepack-4.2.0</ValuePackNameVersion>
Line 79:<ValuePackNameVersion>UCA_NFVD_Migration_Valuepack-4.2.0</ValuePackNameVersion>
Line 88:<ValuePackNameVersion>UCA_Automation_Foundation_UCA-V1.2.3-1A</ValuePackNameVersion>

Checking UCA_NFVD_Persistence_Valuepack in <ValuePackNameVersion>[...]</ValuePackNameVersion>
Count is [1]/1 with version 4.2.0 : Ok

Checking UCA_NFVD_Migration_Valuepack in <ValuePackNameVersion>[...]</ValuePackNameVersion>
Count is [2]/2 with version 4.2.0 : Ok

Checking UCA_NFVD_ProblemDetection_Valuepack in <ValuePackNameVersion>[...]</ValuePackNameVersion>
Count is [2]/2 with version 4.2.0 : Ok

Checking UCA_NFVD_StatePropagation in <ValuePackNameVersion>[...]</ValuePackNameVersion>
Count is [1]/1 with version 4.2.0 : Ok

Checking UCA_NFVD_Evaluate_Valuepack in <ValuePackNameVersion>[...]</ValuePackNameVersion>
Count is [1]/1 with version 4.2.0 : Ok

UCA_Automation_Foundation_UCA in <ValuePackNameVersion>[...]</ValuePackNameVersion>
Count is [3]/3 with version V1.2.3-1A : Ok
Config : [Ok]

consistency of uca host,port in the UCA config files : [Ok]

================================================================================
config_checker.sh execution ended sucessfully
================================================================================
```

Annex 1: Securing communication using sample certificate

This chapter illustrates the configuration steps required to use sample certificate for secure communication.

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 key pair using the JDK "keytool".

Note:
In keytool-genkey-alias command,
-keystore takes key store path
-alias is the alias name
-ext is provided with SAN (Subject Alternative Names)

This keytool is used in Java 1.7 environment

Annex 1.1: Create Java keystore for Assurance

Note:
While creating Java keystore for Assurance, in case a product accessing Assurance API is installed on same box, then "localhost" / "127.0.0.1" needs to be added in the SAN while creating java Keystore.
e.g.

keytool -genkey -alias assuranceKeystore -keyalg RSA –keystore /opt/HPE/nfvd/tpp/jboss/standalone/configuration/sample.jks -ext san=ip:<assurance_server_ip>,ip:127.0.0.1,dns:localhost

```
# keytool -genkey -alias assuranceKeystore -keyalg RSA -keystore /opt/HPE/nfvd/tpp/jboss/standalone/configuration/sample.jks -ext san=ip:<assurance_server_ip>

Enter keystore password: <password_for_keystore: e.g. assurancePwd>
Re-enter new password: < assurancePwd >
What is your first and last name?
  [Unknown]:  Assurance Certificate
What is the name of your organizational unit?
  [Unknown]:  CMS
What is the name of your organization?
  [Unknown]:  HPE
What is the name of your City or Locality?
  [Unknown]:  Bangalore
What is the name of your State or Province?
  [Unknown]:  Karnataka
What is the two-letter country code for this unit?
  [Unknown]:  IN
Is CN=Rahul Verma, OU=CMS, O=HPE, L=Bangalore, ST=Karnataka, C=IN correct?
  [no]:  yes

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