HPE NFV Director

Administration Guide

Release 4.1

Second 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

List of tables

List of figures

Preface

About this Guide

This document describes the operations related to administration of NFVD 4.1 for a typical standard production environment:

- Administering NFVD 4.1:
  - Chapter 1: NFVD Base Product licenses
  - Chapter 2: Operating NFVD
  - Chapter 3: Securing communication between Fulfillment and Assurance

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 NFVD for production environment. 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	October 14, 2016	First edition

Table 1: Document history

Chapter 1 NFVD 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 NFVD 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 NFVD 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

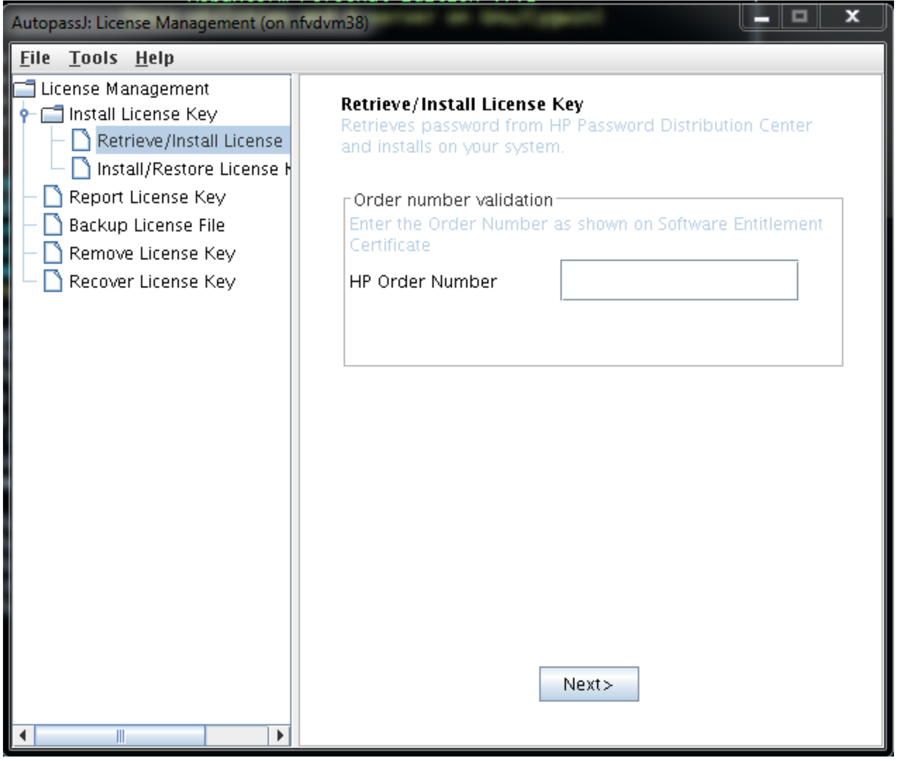
1.3.1.1 Installing HPSA commercial license

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:

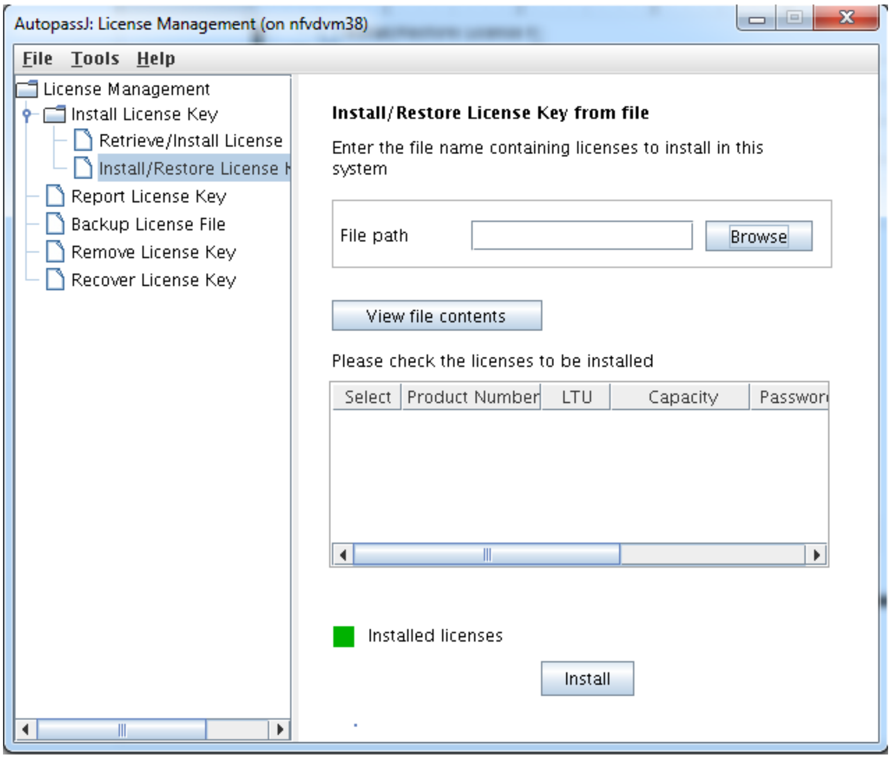


Retrieve/Install License Key
Retrieves password from HP Password Distribution Center and installs on your system.

Order number validation
Enter the Order Number as shown on Software Entitlement Certificate
HP Order Number

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.



Install/Restore License Key from file

Enter the file name containing licenses to install in this system

File path

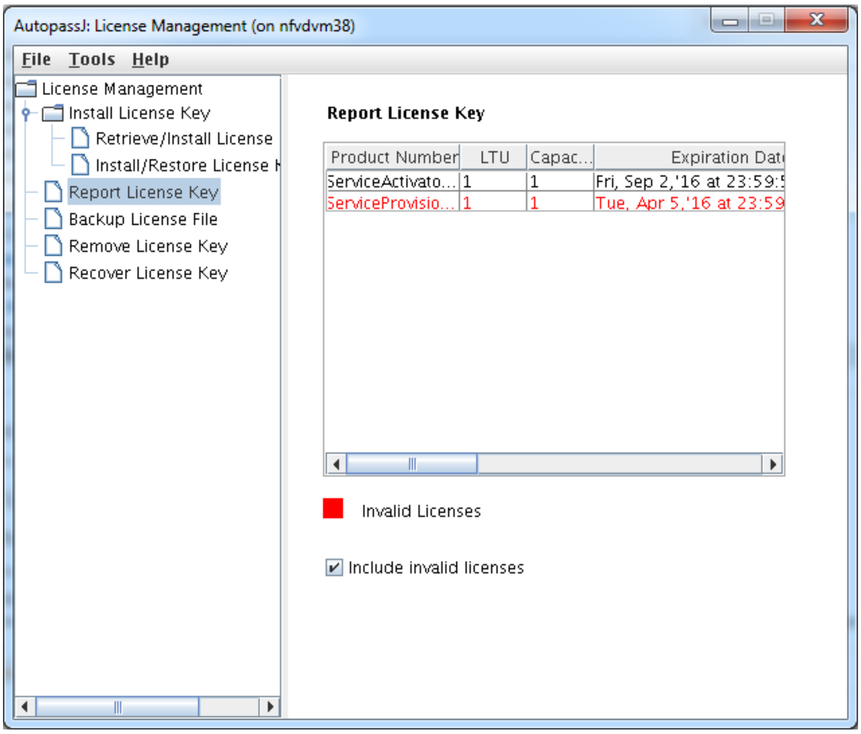
Please check the licenses to be installed

Select	Product Number	LTU	Capacity	Passwor

🟩 Installed licenses

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

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



Report License Key

Product Number	LTU	Capac...	Expiration Date
ServiceActivato...	1	1	Fri, Sep 2,'16 at 23:59:5
ServiceProvisio...	1	1	Tue, Apr 5,'16 at 23:59

🟥 Invalid Licenses

☑ Include invalid licenses

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

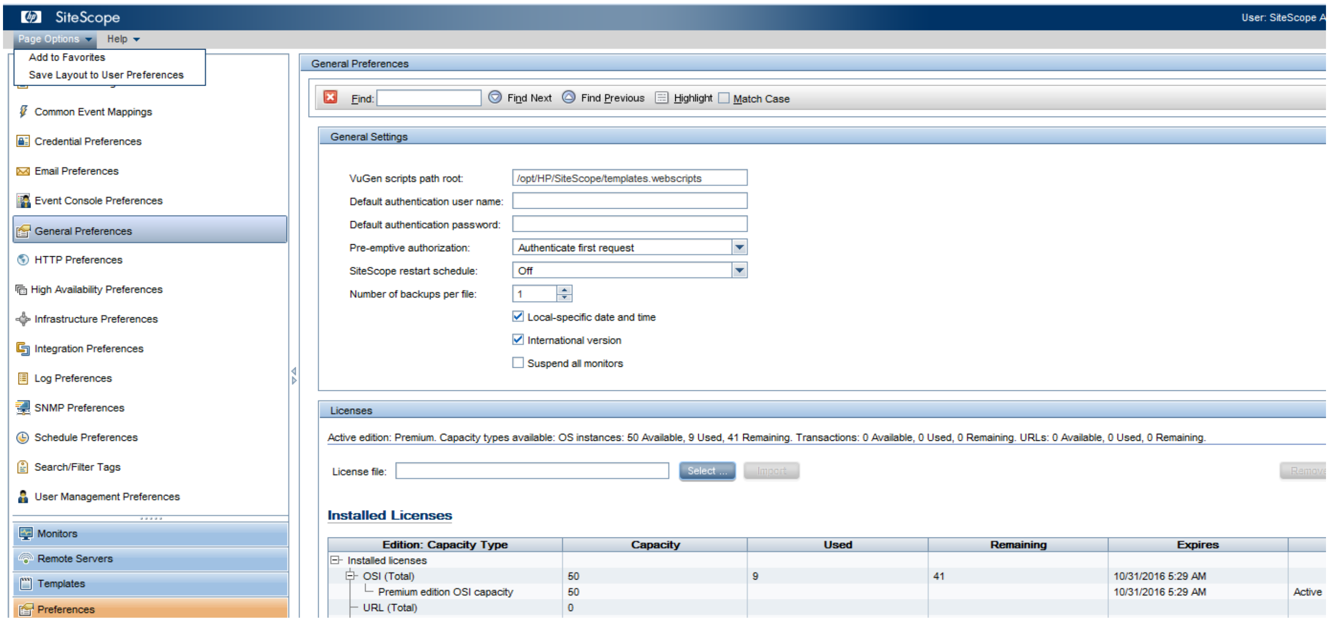
Note: This is a mandatory step to be executed during installation if NFVD monitoring feature is required.

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.



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

Active edition: Premium. Capacity types available: OS instances: 50 Available, 9 Used, 41 Remaining. Transactions: 0 Available, 0 Used, 0 Remaining. URLs: 0 Available, 0 Used, 0 Remaining.

License file:

Installed Licenses

Edition: Capacity Type	Capacity	Used	Remaining	Expires	
Installed licenses					
OSI (Total)	50	9	41	10/31/2016 5:29 AM	
Premium edition OSI capacity	50			10/31/2016 5:29 AM	Active
URL (Total)	0				

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 Operating NFVD

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

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
```

Chapter 3 NFV D Log management

3.1 NFV D log files

Various 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.

Chapter 4 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

4.1 Support utility for diagnostics

The tool *supportability_snapshot.sh* tool aggregates NFV Director log and configuration files, so that it can be sent for analysis.

```
# cd /opt/HPE/nfvd/agw/tools
# ./supportability_snapshot.sh
```

4.2 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>>
```

4.3 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>>
```

4.4 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>>
```

4.5 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

Usage : nfvd_assurance_logger.sh -l < production | troubleshoot > [ optionals ]
 where optionals include:
  -h <ip-address | localhost>      localhost is default host.
  -p <port number>                 19999 is default port.
```

The tool *setAGWLogLevel.sh* can be used to change the logging level

```
# cd /opt/HPE/nfvd/bin
# ./setAGWLogLevel.sh –l <FATAL|ERROR|SEVERE|FINEST|FINER|FINE|TRACE|CONFIG|DEBUG|WARN|INFO> [optionals]
 where optionals include:
  -h <ip-address | localhost>      localhost is default host.
  -p <port number>                 19999 is default port.
                                   Note: SEVERE level is internally ERROR level
```

Chapter 5 Securing communication between Fulfillment and Assurance

By default, the communication between Fulfillment and Assurance is using the HTTP protocol. If you want to secure this communication with HTTPS (SSL), please follow the instructions below:

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

5.1 Create Java keystore for Assurance

```
# 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>
```

Note:
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
```

5.2 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:/opt/HPE/nfvd/tpp/jboss/standalone/configuration/sample.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="${VAULT::keystore_pass::password::NmZiYmRmOGQtMTYzZS00MjE3LTllODMtZjI4OGM2NGJmODM4TElO
RV9CUkVBS3ZhdWx0}"
                          certificate-key-file="${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

Note: Refer to *"Section **Error! Reference source not found. Error! Reference source not found.**"* for full description of steps to start, stop and check status of NFVD components.

5.3 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.

Generate a public key

Note

Assurance Keystore is already generated in step1.

Location: `/home/rahulv/assuranceKeystore.jks`

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

```
keytool -export -keystore /home/rahulv/Assurance.jks -alias vault -file AssurancePub.cer
```

5.3.1 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.

5.3.2 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 5.3.1) 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

5.3.3 SiteScope

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

5.3.4 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=/home/rahulv/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>
```

5.4 Enabling secure connection in Fulfillment

On: <FF_HOST>
Login: root

- Stop HPSA
- 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