NFV Director

Installation, Configuration and Administration Guide

Release 4.1

First Edition

Hewlett Packard
Enterprise

Notices

Legal notice

The information contained herein is subject to change without notice. The only warranties for HPE products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HPE shall not be liable for technical or editorial errors or omissions contained herein.
Printed in the US
Trademarks

Contents

List of tables

List of figures

Preface

About this Guide

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

- Installing and configuring NFVD:
  - Chapter 1: Preparing and checking NFVD environment
  - Chapter 2: Installing NFVD
  - Chapter 3: Post-installation steps

0: • Administering NFVD 4.1:

  - Administering NFVD

This document does not cover the following steps:

- Configuring and administering discovery for NFVD 4.1.
- Configuring NFVD 4.1 optional Software Components (OMi, CMDB).
- Installing NFVD 4.1 resource modelling tool.

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 install, configure and administer NFVD for production environment. It is recommended that the person is knowledgeable in basic Linux and Oracle administration to use this document.

Document History

Edition	Date	Description
1	July 30, 2016	First edition

Table 1: Document history

Chapter 1 Preparing and checking NFVD environment

1.1 Overview

This includes following steps:

- Checking packages availability
- Checking licenses availability
- Checking documentation availability
- Preparing NFVD 4.1 environment
- Checking NFVD 4.1 environment

1.2 Checking packages availability

1.2.1 Checking NFVD packages availability

Make sure you have the following packages available, required for installation:

Package Name	**Reference**
NFVD Installer	nfvd-installer-04.01.000-1.el6.noarch.rpm
NFVD Base Product	NFVD41_BaseProduct.tar
NFVD Software	NFVD41_Software.tar

Table 2 : Required media for installation

1.2.2 Checking SiteScope package availability

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

Make sure you have the following packages available, required for installation:

Package Name	**Reference**
HP SiteScope 11.30 for Linux	HP_SIteScope_11.30_for_Linux_64bit_T8354-15016.zip
HP SiteScope hotfix	sis1131concurrent_templ_deploy_deleteGroupEx.zip

Table 3 : Required media for installation

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

1.2.3 Getting references to software download links

Find hereunder a few useful links regarding components which will not be documented for detailed installation.

Component	**Version/Part Number**
Oracle	http://docs.oracle.com
couchDB	http://docs.couchdb.org

Apache Directory Studio	https://directory.apache.org/studio/
Active Directory schema snap-in installation in Windows 2008R2	http://social.technet.microsoft.com/wiki/contents/articles/10827.install-the-active-directory-schema-snap-in-in-windows-2008-server.aspx
openLDAP	http://docs.adaptivecomputing.com/viewpoint/hpc/Content/topics/1-setup/installSetup/settingUpOpenLDAPOnCentos6.htm

Table 4 : Software download links

1.3 Checking licenses availability

1.3.1 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 5 : Required licenses for installation

Note: Refer to NFVD License Ordering Guide to know how to get the NFVD Base Products commercial licenses.

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

1.3.2 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 6 : Required SiteScope license

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

1.4 Preparing NFVD environment

1.4.1 Preparing configuration of hosts

NFVD deployment encompasses 3 NFVD components:

- NFVD component for Fulfillment (FF).
- NFVD component for Assurance (AA).

- NFVD component for GUI.

In a typical installation for NFVD:

- FF and GUI components are deployed in one Virtual Machine Host with RHEL 6.6 x86_64 deployed in VCenter 5.5U2 VMware infrastructure.
- AA component is deployed in one Virtual Machine Host with RHEL 6.6 x86_64 deployed in VCenter 5.5U2 VMware infrastructure.

Note: Other installation are possible but would require a validation from HPE Services.

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

Naming	Definition
<FF_HOST>	IP address of Host where NFVD component for Fulfillment (FF) is deployed.
<AA_HOST>	IP address of Host where NFVD component for Assurance (AA) is deployed.
<GUI_HOST>	IP address of Host where NFVD component for GUI is deployed.
<INSTALLER_HOST>	IP address of Host where NFVD Installer tool is installed.

Table 7 : Naming convention

In a typical installation for NFVD, <FF_HOST>, <GUI_HOST> and <INSTALLER_HOST> are the same.

NFVD Product also requires **connectivity** to hosts where the following components are deployed:

- DNS server.
- Oracle DB server component (Oracle 11gR2) in order to deploy its data model and store persistent data.
- Server with LDAPv3 implementation. Typical examples are:
  - OpenLDAP server without SSL connection.
  - ActiveDirectory with SSL connection.
- Mail server component.
- VIM Infrastructure (Helion Carrier-Grade 2.0 OpenStack, RedHatOpenStack 7, pure OpenStack Kilo or vCenter 5.5).
- Omi/BSC component (if HPSW is used for discovery).

Note: From NFVD standpoint, there is no constraint on how these components are actually deployed, either through physical or virtual hosts, either collocated or not collocated, as long as they meet connectivity requirements.

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

Naming	Definition
<ORACLE_HOST>	Host IP address of Oracle single-instance server where Oracle component is installed. or Scan IP addresses of Oracle RAC cluster where Oracle component is installed.
<LDAP_HOST>	Host IP address where LDAPv3 server component is reachable.
<OMI_HOST>	Host IP address where OMi/BSC component is reachable.
<MAIL_SERVER_HOST>	Host IP address where Mail Server is reachable.

Table 8 : Product naming convention

1.4.2 Instantiating NFVD VMs in VMware infrastructure

Note: Steps in this chapter can typically be delegated to IT Admin of the VMware infrastructure.

Make sure that that following Virtual Machines are allocated in VMware infrastructure (with VMware Tools installed), can ping each other, can be accessed through ssh, are time-synced and can access yum repo.

Component	Guest OS	IP Address	vCPUs	RAM (GB)	vDisks	Disk size (GB)	
						OS root	NFVD
FF+GUI	RedHat Linux 6.6 x86_64	<FF_HOST> (identical to <GUI_HOST>)	16	32	2	50	100
AA	RedHat Linux 6.6 x86_64	<AA_HOST>	6	24	2	50	150

Table 9 : Typical sizing required per component

Note: Other installations are possible but would require a validation from HPE Services.

Note: In context of custom project, installation can be customized to distribute sub-components (HPSA, HPSA EP, UCA) across several VMs but this requires support from NFVD Team to agree on project-specific customizations, which may require changes to installation scripts.

Find hereunder a typical example for VMware Tools installation on Virtual Machines (once you have selected VM on VCenter with right click→ Guest → Install/Upgrade VMWare Tools):

```
# mkdir /media/cdrom
# mount –t iso9660 /dev/cdrom /media/cdrom
# cd /var/tmp/
# tar –xvzf /media/cdrom/VMwareTools*.tar.gz
# cd vmware-tools-distrib/
# ./vmware-install.pl

[Accept all default values by clicking on Return]

#
```

Find hereunder a typical example of network connectivity:

- /etc/sysconfig/network

```
NETWORKING=yes
HOSTNAME=<[FF|AA|GUI|SITESCOPE]_HOSTNAME>.<NFVD_DOMAIN>
NOZEROCONF=yes
NETWORKING_IPV6=yes
IPV6_AUTOCONF=no
GATEWAY=<NFVD_GATEWAY>
```

Typical example:

```
NETWORKING=yes
HOSTNAME=ducati49.gre.hpecorp.net
NOZEROCONF=yes
NETWORKING_IPV6=yes
IPV6_AUTOCONF=no
GATEWAY=16.16.88.1
```

- /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE="eth0"
```

```
BOOTPROTO="static"
HWADDR="<MAC ADDRESS allocated by VMWare for eth0>"
IPV6INIT="yes"
MTU="1500"
NM_CONTROLLED="yes"
ONBOOT="yes"
TYPE="Ethernet"
IPADDR=<[FF|AA|GUI]_HOST>
NETMASK=<NFVD_NETMASK>
GATEWAY=<NFVD_GATEWAY>
USERCTL=no
```

Typical example:

```
DEVICE="eth0"
BOOTPROTO="static"
HWADDR="00:50:56:B1:3F:98"
IPV6INIT="yes"
MTU="1500"
NM_CONTROLLED="yes"
ONBOOT="yes"
TYPE="Ethernet"
IPADDR=16.16.88.200
NETMASK=255.255.248.0
GATEWAY=16.16.88.1
USERCTL=no
```

- /etc/udev/rules.d/70-persistent-net.rules

```
# This file was automatically generated by the /lib/udev/write_net_rules
# program, run by the persistent-net-generator.rules rules file.
#
# You can modify it, as long as you keep each rule on a single
# line, and change only the value of the NAME= key.

# PCI device 0x15ad:0x07b0 (vmxnet3)
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*", ATTR{address}=="<MAC ADDRESS allocated by VMWare for eth0>",
ATTR{type}=="1", KERNEL=="eth*", NAME="eth0"
```

Typical example:

```
# This file was automatically generated by the /lib/udev/write_net_rules
# program, run by the persistent-net-generator.rules rules file.
#
# You can modify it, as long as you keep each rule on a single
# line, and change only the value of the NAME= key.

# PCI device 0x15ad:0x07b0 (vmxnet3)
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*", ATTR{address}=="00:50:56:b1:3f:98", ATTR{type}=="1", KERNEL=="eth*",
NAME="eth0"
```

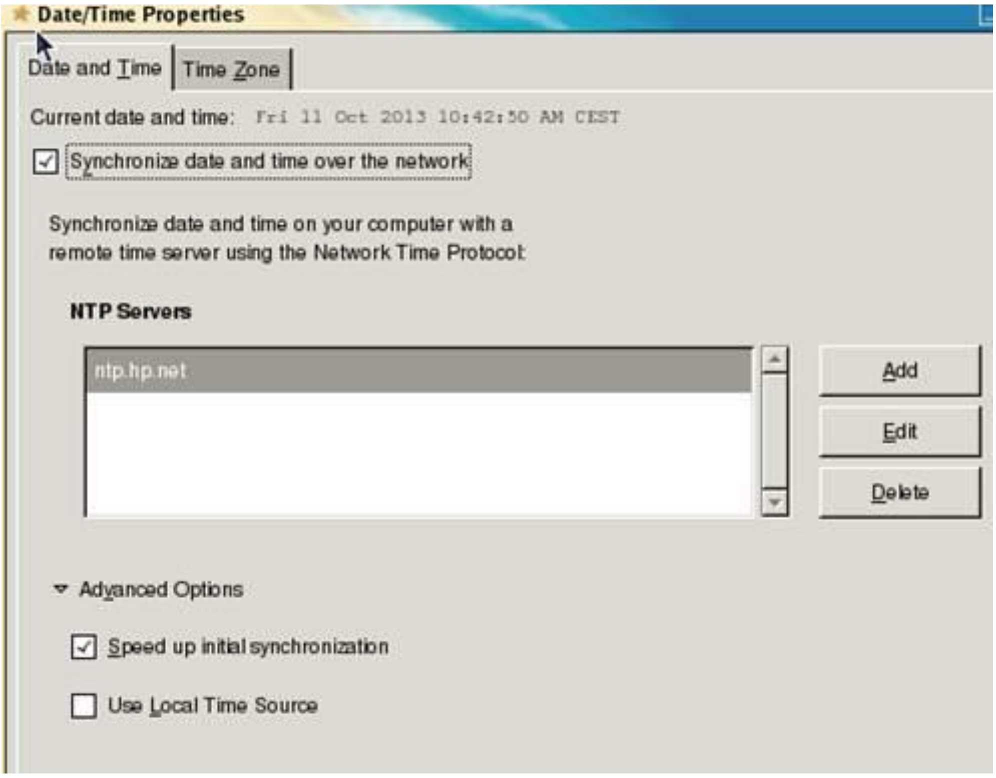
Typical example to enable ssh connectivity: */etc/ssh/sshd_config* file and change the value of *PermitRootLogin* to yes, then restart sshd service:

```
# vi /etc/ssh/sshd_config
....
PermitRootLogin yes
...
# service sshd restart
```

Typical example regarding time-synchronization through NTP:

Invoke *system-config-date* utility, click on “Synchronize date and time over the network”, then reference NTP Server(s).

Typical example:



Current date and time: Fri 11 Oct 2013 10:42:50 AM CEST

☑ Synchronize date and time over the network

Synchronize date and time on your computer with a remote time server using the Network Time Protocol

NTP Servers

ntp.hp.net

Advanced Options

☑ Speed up initial synchronization

□ Use Local Time Source

Figure 1 : Date/Time Properties

Typical example for yum repo:

In order to use yum tool to automatically manage dependencies, there is a need to make sure RedHat Enterprise Linux 6.6 x86_64 distribution is available through a repo.
In order to make it available, one typical example is to mount RHEL 6.6 iso image (or equivalent) and reference it through a repo.

Typical example:

```
# vi /etc/yum.repos.d/redhat.repo

[core]
name=RPM Repository for Red Hat Enterprise Linux $releasever - $basearch - Base OS
baseurl=http://repoman.gre.hpecorp.net/mrepo/rhel6.6-server-$basearch/disc1/Server
enabled=1
gpgcheck=0

[updates]
name= RPM Repository for Red Hat Enterprise Linux $releasever Updates - $basearch - Updates
baseurl=http://linuxcoe.corp.hp.com/LinuxCOE/RedHat-updates-yum/6Server/en/os/$basearch
enabled=0
gpgcheck=0

#
```

1.4.3 Performing basic setup of NFVD VMs

Note: Steps in this chapter can typically be delegated to IT Admin of the VMware infrastructure.

1.4.3.1 Installing RPMs

On: <INSTALLER_HOST>
Login: root

Install following RPMs:

- ksh
- telnet
- libaio-0.3.107-10.el6.x86_64.rpm
- oracle-instantclient11.2-basic-11.2.0.4.0-1.x86_64.rpm
- oracle-instantclient11.2-sqlplus-11.2.0.4.0-1.x86_64.rpm

On: <AA_HOST>, <FF_HOST>, <GUI_HOST>
Login: root

Install following RPMs:

- ksh
- unzip
- dos2unix

On: <GUI_HOST>
Login: root

Install following RPMs:

- openssl
- createrepo
- perl

On: <FF_HOST>
Login: root

Install following RPMs (if you don't have any external SMTP server available):

- postfix

1.4.3.2 Setting up file system layout

Note: Setting up file system layout can be typically handled through *system-config-lvm* utility (installable with yum/rpm).

1.4.3.2.1 Fulfillment host

Typical File System Layout for NFVD FF is following:

vDisk		**Volume Group**		**Logical Volume**		
Id	Size (GB)	Name	Size (GB)	Name	Size (GB)	Mounting Point
2	50	vgFF	50	vgFF-lvolJBoss	10	/opt/HP/jboss

				vgFF-lvolOptSA	20	/opt/OV/ServiceActivator
				vgFF-lvolVarSA	10	/var/opt/OV/ServiceActivator
				vgFF-lvolEtcSA	5	/etc/opt/OV/ServiceActivator

Table 10 : File system layout for NFVD FF

Note: Other installations are possible but would require a validation from HPE Services.

1.4.3.2.2 Assurance host

Typical File System Layout for NFVD AA is following:

vDisk		**Volume Group**		**Logical Volume**		
Id	Size (GB)	Name	Size (GB)	Name	Size (GB)	Mounting Point
2	150	vgAA	150	vgAA-lvolOM	50	/var/opt/openmediation-70
				vgAA-lvolUCA	50	/var/opt/UCA-EBC
				vgAA-lvolAGW	50	/var/opt/HPE/nfvd

Table 11 : File system layout for NFVD AA

Note: Other installations are possible but would require a validation from HPE Services.

1.4.3.2.3 GUI host

Not applicable since there is no dedicated volume group on GUI host for GUI application.

1.4.3.3 Enabling ports

On: <FF_HOST>
Login: root

Make sure the following ports are enabled in */etc/sysconfig/iptables*:

```
# vi /etc/sysconfig/iptables
....
-A INPUT -p tcp -m tcp -m tcp --dport <HPSA_WEB_SERVER_PORT> -j ACCEPT
-A INPUT -p tcp -m tcp -m tcp --dport <HPSA_RESOURCE_MANAGER_PORT> -j ACCEPT
-A INPUT -p tcp -m tcp -m tcp --dport <HPSA_WORKFLOW_MANAGER_PORT> -j ACCEPT
-A INPUT -p tcp -m tcp -m tcp --dport 1220 -j ACCEPT
-A INPUT -p tcp -m tcp -m tcp --dport 1221 -j ACCEPT
...
```

Typical example:

```
# vi /etc/sysconfig/iptables
....
-A INPUT -p tcp -m tcp -m tcp --dport 8080 -j ACCEPT
-A INPUT -p tcp -m tcp -m tcp --dport 9223 -j ACCEPT
-A INPUT -p tcp -m tcp -m tcp --dport 2000 -j ACCEPT
-A INPUT -p tcp -m tcp -m tcp --dport 1220 -j ACCEPT
-A INPUT -p tcp -m tcp -m tcp --dport 1221 -j ACCEPT
...
```

Apply configuration change:

```
# service iptables restart
```

On: <AA_HOST>
Login: root

Make sure the following ports are enabled in */etc/sysconfig/iptables*:

```
# vi /etc/sysconfig/iptables
....
-A INPUT -p tcp -m tcp -m tcp --dport <UCA_AUTOMATION_CONSOLE_PORT> -j ACCEPT
-A INPUT -p tcp -m tcp -m tcp --dport <UCA_CONSOLE_PORT> -j ACCEPT
-A INPUT -p tcp -m tcp -m tcp --dport <UCA_EBC_JMS_BROKER_PORT> -j ACCEPT
-A INPUT -p tcp -m tcp -m tcp --dport <ACTION_SERVICE_PORT> -j ACCEPT
-A INPUT -p tcp -m tcp -m tcp --dport <HPSA_UCA_AUTOMATION_SYNC_SERVER_PORT> -j ACCEPT
-A INPUT -p tcp -m tcp -m tcp --dport <UCA_AUTOMATION_UI_PORT> -j ACCEPT
-A INPUT -p tcp -m tcp -m tcp --dport <AA_GW_JBOSS_ADMIN_CONSOLE_PORT> -j ACCEPT
-A INPUT -p tcp -m tcp -m tcp --dport <SITESCOPE_PORT> -j ACCEPT
-A INPUT -p tcp -m tcp -m tcp --dport <NEO4J_PORT> -j ACCEPT
...
```

Typical example:

```
# vi /etc/sysconfig/iptables
....
-A INPUT -p tcp -m tcp -m tcp --dport 12500 -j ACCEPT
-A INPUT -p tcp -m tcp -m tcp --dport 8090  -j ACCEPT
-A INPUT -p tcp -m tcp -m tcp --dport 61666 -j ACCEPT
-A INPUT -p tcp -m tcp -m tcp --dport 26700 -j ACCEPT
-A INPUT -p tcp -m tcp -m tcp --dport 8191 -j ACCEPT
-A INPUT -p tcp -m tcp -m tcp --dport 18080 -j ACCEPT
-A INPUT -p tcp -m tcp -m tcp --dport 18888 -j ACCEPT
-A INPUT -p tcp -m tcp -m tcp --dport 7474 -j ACCEPT
...
```

Apply configuration change:

```
# service iptables restart
```

On: <GUI_HOST>
Login: root

Make sure the following ports are enabled in */etc/sysconfig/iptables*:

```
# vi /etc/sysconfig/iptables
....
-A INPUT -p tcp -m tcp -m tcp --dport <UOC_WEB_SERVER_PORT> -j ACCEPT
-A INPUT -p tcp -m tcp -m tcp --dport <COUCHDB_PORT> -j ACCEPT
-A INPUT -p tcp -m tcp -m tcp --dport <IDP_PORT> -j ACCEPT
-A INPUT -p tcp -m tcp -m tcp --dport <IMAGE_UPLOADER_PORT> -j ACCEPT
...
```

Typical example:

```
# vi /etc/sysconfig/iptables
....
-A INPUT -p tcp -m tcp -m tcp --dport 3000 -j ACCEPT
-A INPUT -p tcp -m tcp -m tcp --dport  5984 -j ACCEPT
-A INPUT -p tcp -m tcp -m tcp --dport  38080 -j ACCEPT
-A INPUT -p tcp -m tcp -m tcp --dport  1337 -j ACCEPT
...
```

Apply configuration change:

```
# service iptables restart
```

On: <LDAP_HOST>
Login: root

Make sure the following ports are enabled in */etc/sysconfig/iptables*:

```
# vi /etc/sysconfig/iptables
....
-A INPUT -p tcp -m tcp -m tcp --dport <LDAP_PORT> -j ACCEPT
...
```

Typical example:

```
# vi /etc/sysconfig/iptables
....
-A INPUT -p tcp -m tcp -m tcp --dport 389 -j ACCEPT
...
```

Apply configuration change:

```
# service iptables restart
```

1.4.4 Configuring NFVD with LDAPv3 server

NFVD supports two typical implementations of LDAPv3 Server:

- OpenLDAP without SSL
- ActiveDirectory with SSL

If you have an:

- OpenLDAP : go to section 1.4.4.1
- Active Directory : go to section 1.4.4.2

1.4.4.1 Configuring NFVD with openLDAP

Skip this part if you use Active Directory.

1.4.4.1.1 Prerequisites

- An instantiation of openLDAP with RootDN=nfvd.domain is reachable and its schema can be extended:

On: <LDAP_HOST>
Login: root

- olcDatabase\=\{2\}bdb.ldif file

```
# cd /etc/openldap/slapd.d/cn\=config
# vi olcDatabase\=\{2\}bdb.ldif
[…]
olcSuffix: dc=nfvd,dc=domain
olcRootDN: dc=nfvd,dc=domain
[…]
olcAccess: {0}to attrs=userPassword by self write by dn.base="dc=nfvd,dc=domain" write by
anonymous auth by * none
olcAccess: {1}to * by dn.base="dc=nfvd,dc=domain" write by self write by * read […]
```

- olcDatabase\=\{1\}monitor.ldif file

```
# cd /etc/openldap/slapd.d/cn\=config
# vi olcDatabase\=\{1\}monitor.ldif
```

```
[…]
olcAccess: {0}to *  by dn.base="gidNumber=0+uidNumber=0,cn=peercred,cn=exter
 nal,cn=auth" read  by dn.base="dc=nfvd,dc=domain" read  by * n
 one
[…]
```

- In order to apply the changes, LDAP service has to be restarted:

```
# service slapd restart
```

1.4.4.1.2 Extending openLDAP schema

On: <LDAP_HOST>
Login: root

- Create file */tmp/ldapPublicKey.schema* with content as follows:

```
[root@nfvdvm25 ~]# cd /tmp
[root@nfvdvm25 ~]# vi ldapPublicKey.schema

# octetString SYNTAX
attributetype ( 1.3.6.1.4.1.24552.500.1.1.1.13 NAME 'sshPublicKey'
 DESC 'MANDATORY: OpenSSH Public key'
 EQUALITY octetStringMatch
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.40 )

# printableString SYNTAX yes|no
objectclass ( 1.3.6.1.4.1.24552.500.1.1.2.0 NAME 'ldapPublicKey' SUP top AUXILIARY
 DESC 'MANDATORY: OpenSSH LPK objectclass'
 MAY ( sshPublicKey $ uid )
 )
```

- Create file */tmp/newSchema.conf* with content as follows:

```
 [root@nfvdvm25 ~]# vi newSchema.conf

include /tmp/ldapPublicKey.schema
```

- Create a new directory */tmp/conf.d* where the tool *slaptest* is going to create the necessary files with the schema information to import in the OpenLDAP schema:

```
 [root@nfvdvm25 ~]# mkdir conf.d
```

- Execute the “slaptest” tool:

```
 [root@nfvdvm25 ~]# slaptest -f /tmp/newSchema.conf -F /tmp/conf.d
```

- Edit the generated file “/tmp/conf.d/cn\=config/cn\=schema/cn\=\{0\}ldappublickey.ldif” and delete the following lines:

```
 […]
structuralObjectClass: […]
entryUUID: […]
creatorsName: […]
createTimestamp: […]
entryCSN: […]
modifiersName: […]
modifyTimestamp: […]
[…]
```

In that file change the following lines to:

```
[...]
dn: cn=ldapPublicKey,cn=schema,cn=config
objectClass: olcSchemaConfig
cn: ldapPublicKey
[...]
```

- Import this new object class and attribute to OpenLDAP with the “ldapadd” tool:

```
[root@nfvdvm25 ~]# ldapadd -Y EXTERNAL -H ldapi:/// -f /tmp/conf.d/cn\=config/cn\=schema/cn\=\{0\}ldappublickey.ldif
```

- Restart *slapd* service:

```
[root@nfvdvm25]# service slapd stop
[...]
[root@nfvdvm25]# service slapd start
```

1.4.4.1.3 Importing NFVD structure

As openLDAP schema is extended, next step is to import NFVD structure:

On: <LDAP_HOST>
Login: root

- Create */tmp/structure.ldif* file as follows:

```
[root@nfvdvm25]# vi structure.ldif
version: 1

dn: dc=nfvd,dc=domain
objectClass: dcObject
objectClass: organization
dc: nfvd
o : nfvd

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

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

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

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

- Import the NFVD structure file using *ldapadd* tool:

```
#ldapadd -x -W -D "dc=nfvd,dc=domain" -f structure.ldif
```

1.4.4.2 Configuring NFVD with ActiveDirectory

Skip this part if you use OpenLDAP.

1.4.4.2.1 Prerequisites

- An ActiveDirectory snap-in is reachable and its schema can be extended.

1.4.4.2.2 Extending ActiveDirectory schema

On: <AD_HOST>
Login: root

1.4.4.2.2.1 Attribute ‘sshPublicKey’

1. Double click on AD Schema snap-in

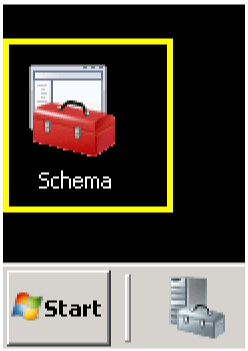
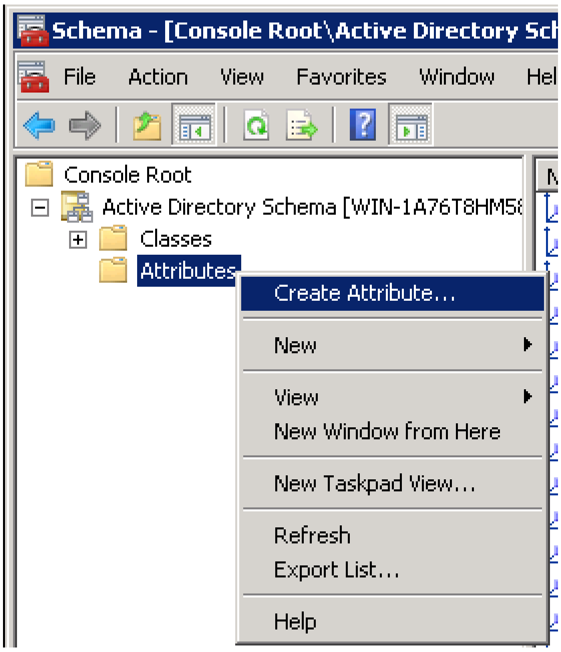


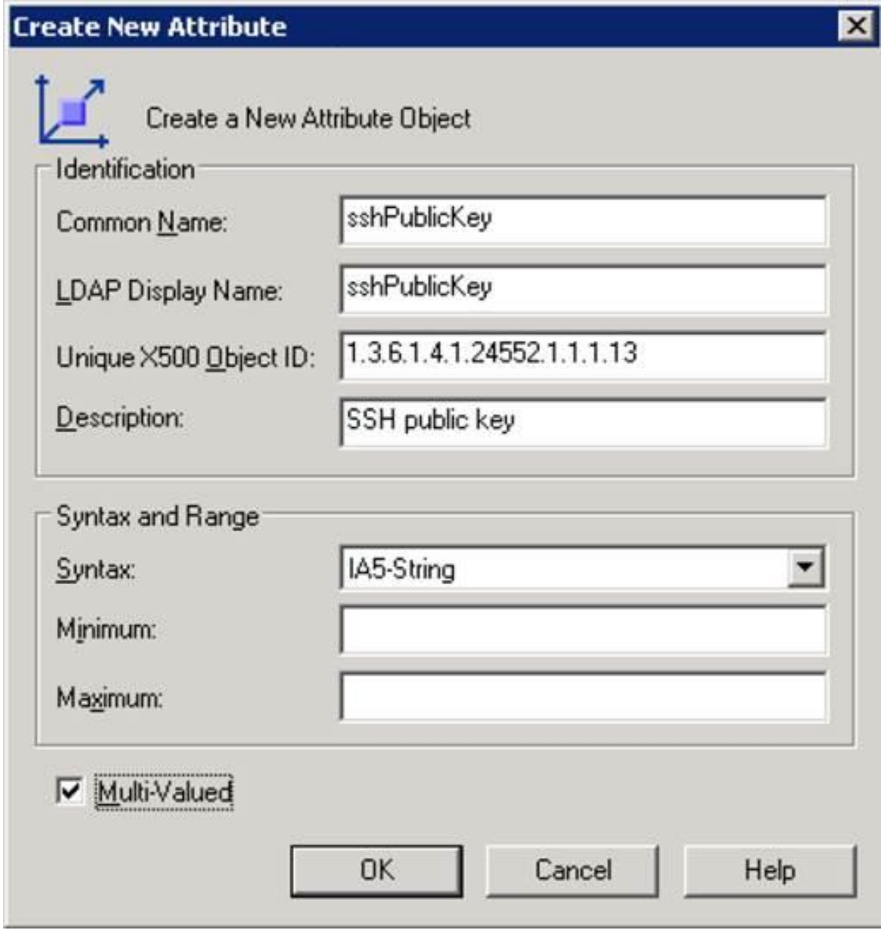
Figure 2 : Double click in Schema shortcut


Schema - [Console Root\Active Directory Sch
File Action View Favorites Window Hel
Console Root
Active Directory Schema [WIN-1A76T8HM58
Classes
Attributes
Create Attribute...
New
View
New Window from Here
New Taskpad View...
Refresh
Export List...
Help

2. Create a new attribute (right button on your mouse over ‘Attributes’)

Figure 3 : Create Attribute

3. Fill the values according to next image:



Common Name: sshPublicKey

LDAP Display Name: sshPublicKey

Unique X500 Object ID: 1.3.6.1.4.1.24552.1.1.1.13

Description: SSH public key

Syntax: IA5-String

Minimum:

Maximum:

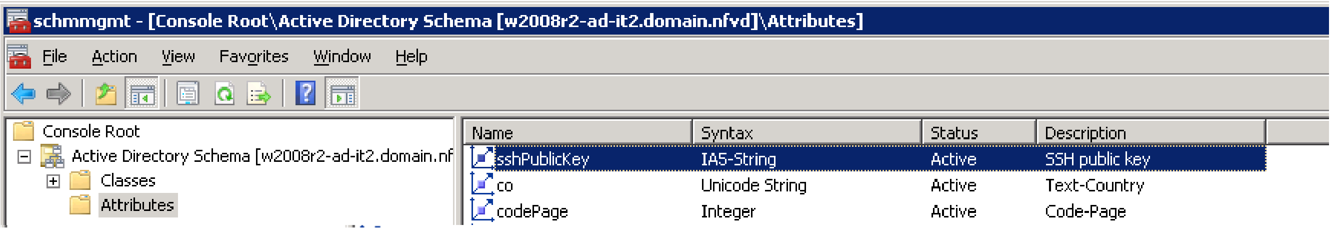
☑ Multi-Valued

Figure 4 : Fill the values for new attribute

The values you have to type are:

- Common name: sshPublicKey
- LDAP Display name: sshPublicKey
- Unique X500 Object ID: 1.3.6.1.4.1.24552.500.1.1.1.13
- Description: SSH public key
- Syntax: IA5-String
- Multi-valued: yes

Click on <OK> button to add the new attribute: a new attribute will be added to your AD Schema.


schmmgmt - [Console Root\Active Directory Schema [w2008r2-ad-it2.domain.nfvd]\Attributes]
File
Action
View
Favorites
Window
Help
Console Root
Active Directory Schema [w2008r2-ad-it2.domain.nf
Classes
Attributes

Name	Syntax	Status	Description
sshPublicKey	IA5-String	Active	SSH public key
co	Unicode String	Active	Text-Country
codePage	Integer	Active	Code-Page

Figure 5 : New attribute ‘sshPublicKey’ has been created

1.4.4.2.2.2 Schema Class ‘ldapPublicKey’

1. (if you have not done before) Double click on AD Schema snap-in

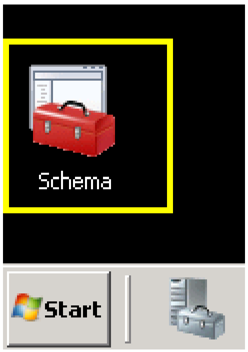


Figure 6 : Double click in Schema shortcut

2. Create a new class (right button on your mouse over 'Classes')

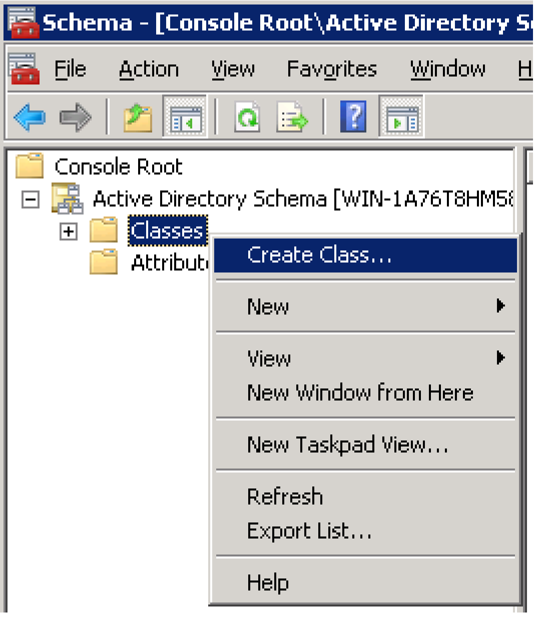
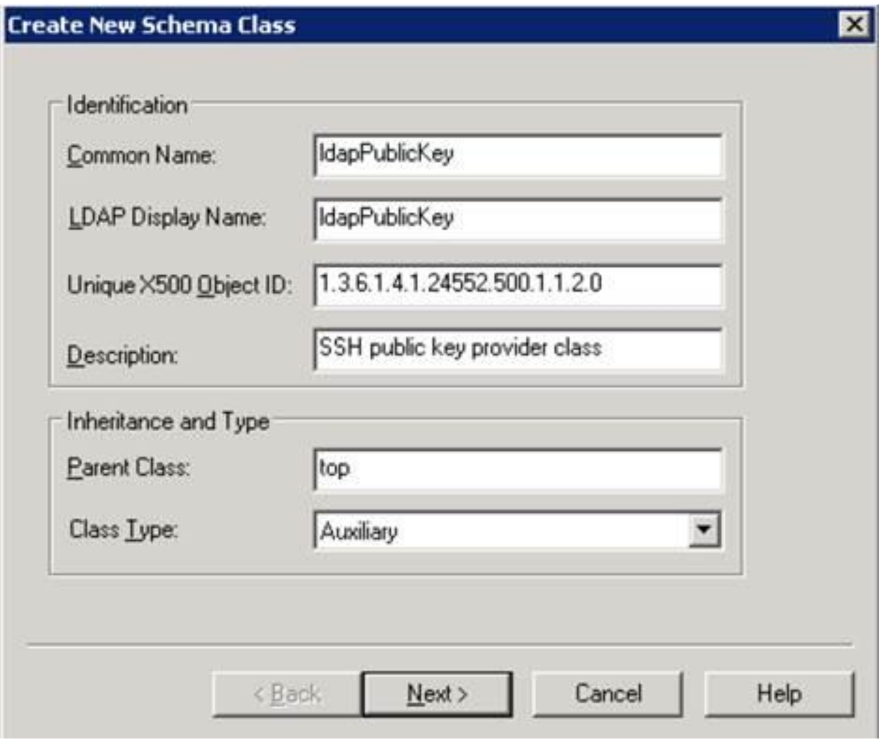


Figure 7 : Create Class

3. Fill the values according to next image



Create New Schema Class

Identification

Common Name: ldapPublicKey

LDAP Display Name: ldapPublicKey

Unique X500 Object ID: 1.3.6.1.4.1.24552.500.1.1.2.0

Description: SSH public key provider class

Inheritance and Type

Parent Class: top

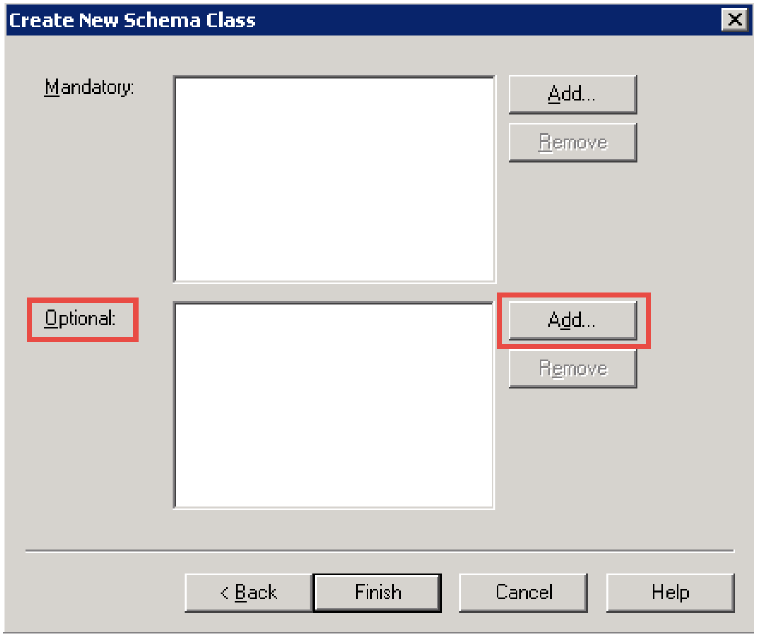
Class Type: Auxiliary

Figure 8 : Fill the values for new class

The values you have to type are:

- Common name: ldapPublicKey
- LDAP Display name: ldapPublicKey
- Unique X500 Object ID: 1.3.6.1.4.1.24552.500.1.1.2.0
- Description: SSH public key provider class
- Parent class: top
- Class type: Auxiliary

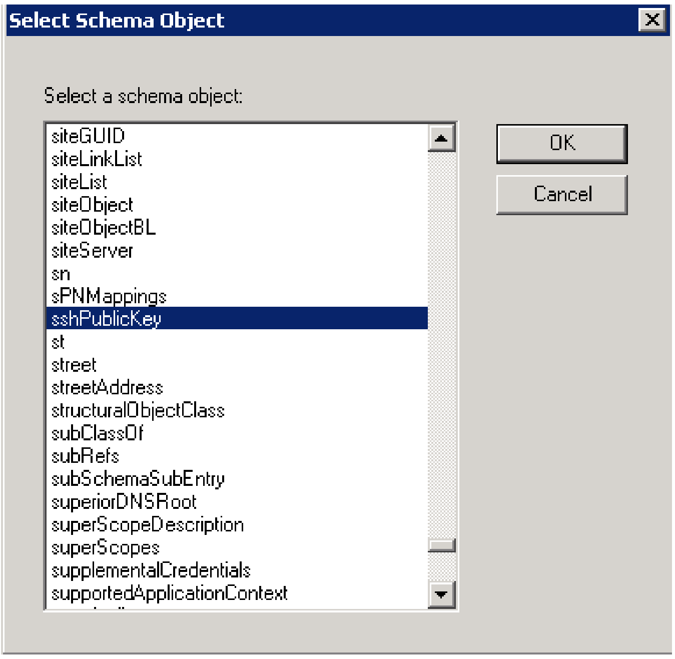
Click on `<Next>` button: you will see the following window:



Create New Schema Class

Figure 9 : Adding a new optional attribute to the new class

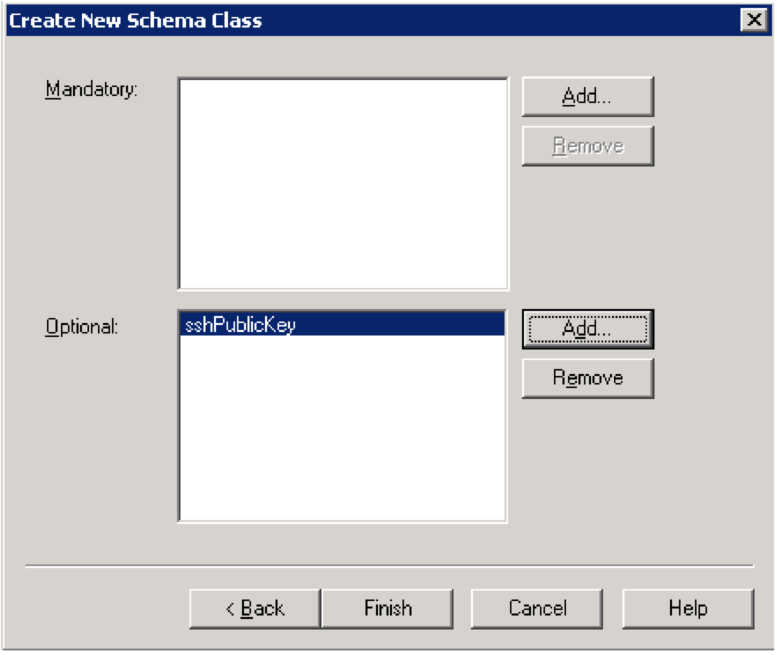
Select the `sshPublicKey` attribute you created in previous section and click `<OK>` button.



Select a schema object:

siteGUID
siteLinkList
siteList
siteObject
siteObjectBL
siteServer
sn
sPNMappings
sshPublicKey
st
street
streetAddress
structuralObjectClass
subClassOf
subRefs
subSchemaSubEntry
superiorDNSRoot
superScopeDescription
superScopes
supplementalCredentials
supportedApplicationContext

Figure 10 : Adding `sshPublicKey` attribute

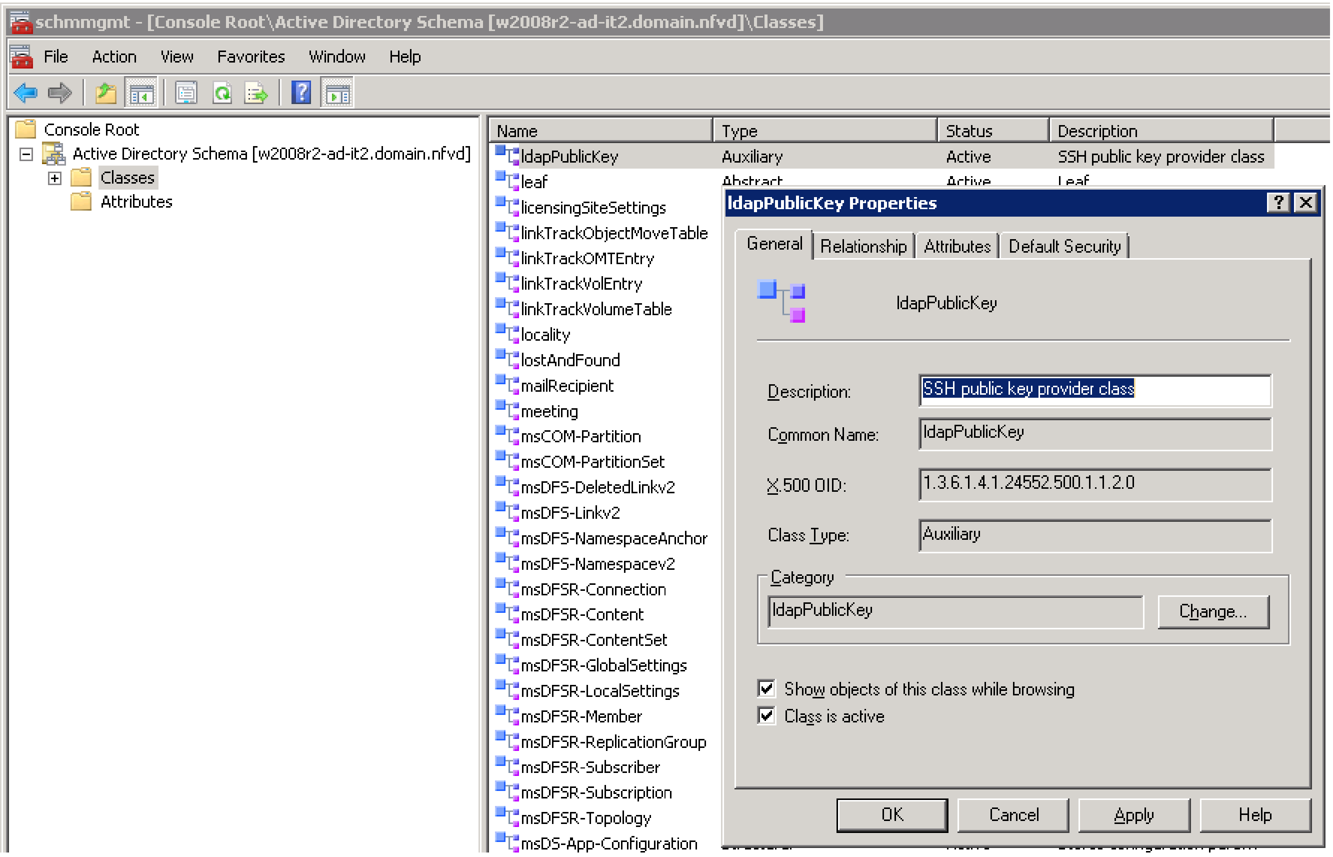


Mandatory:

Optional: sshPublicKey

Figure 11 : `sshPublicKey` attribute added.

When you click on <Finish> button, a new schema class called ldapPublicKey will be added to your AD Schema.



Name	Type	Status	Description
ldapPublicKey	Auxiliary	Active	SSH public key provider class
leaf	Abstract	Active	Leaf
licensingSiteSettings			
linkTrackObjectMoveTable			
linkTrackOMTEntry			
linkTrackVolEntry			
linkTrackVolumeTable			
locality			
lostAndFound			
mailRecipient			
meeting			
msCOM-Partition			
msCOM-PartitionSet			
msDFS-DeletedLinkv2			
msDFS-Linkv2			
msDFS-NamespaceAnchor			
msDFS-Namespacev2			
msDFSR-Connection			
msDFSR-Content			
msDFSR-ContentSet			
msDFSR-GlobalSettings			
msDFSR-LocalSettings			
msDFSR-Member			
msDFSR-ReplicationGroup			
msDFSR-Subscriber			
msDFSR-Subscription			
msDFSR-Topology			
msDS-App-Configuration			

ldapPublicKey

Description: SSH public key provider class

Common Name: ldapPublicKey

X.500 OID: 1.3.6.1.4.1.24552.500.1.1.2.0

Class Type: Auxiliary

Category: ldapPublicKey

☑ Show objects of this class while browsing

☑ Class is active

Figure 12 : Schema class `ldapPublicKey`.

1.4.4.2.3 Configuring Active Directory

You need to create the NfvdManagement group in your Active Directory importing a LDIF file.
From a command prompt use “ldifde” tool:

```
ldifde -i -k -f .\active_directory_structure.ldif –j .\
```

The file “active_directory_structure.ldif” contains this info:
(Here **DC=<DOMAIN_CONTROLLER_NAME>,DC=<DOMAIN_SUFFIX>** is the Domain Controller name of the Active Directory, for example “DC=domain,DC=nfvd”)

```
version: 1

dn: OU=NfvdManagement,DC=<DOMAIN_CONTROLLER_NAME>
objectClass: organizationalUnit
objectClass: top
instanceType: 4
objectCategory: CN=Organizational-Unit,CN=Schema,CN=Configuration, DC=<DOMAIN_CONTROLLER_NAME>,D
 C=<DOMAIN_SUFFIX>
ou: NfvdManagement
distinguishedName: OU=NfvdManagement,DC=<DOMAIN_CONTROLLER_NAME>
name: NfvdManagement

dn: OU=groups,OU=NfvdManagement,DC=<DOMAIN_CONTROLLER_NAME>
objectClass: organizationalUnit
objectClass: top
instanceType: 4
objectCategory: CN=Organizational-Unit,CN=Schema,CN=Configuration, DC=<DOMAIN_CONTROLLER_NAME> ,D
 C=<DOMAIN_SUFFIX>
ou: groups
distinguishedName: OU=groups,OU=NfvdManagement,DC=<DOMAIN_CONTROLLER_NAME>
name: groups

dn: CN=NfvdManagement,OU=groups,OU=NfvdManagement,DC=<DOMAIN_CONTROLLER_NAME>
objectClass: group
```

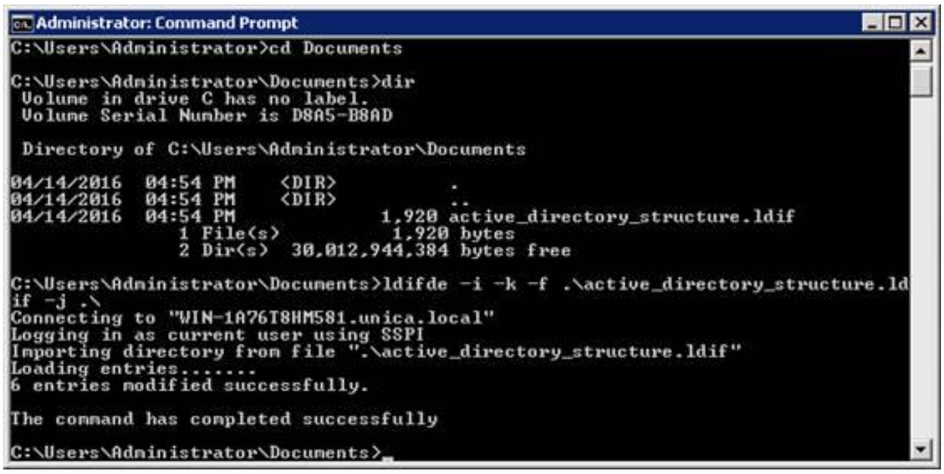
```
objectClass: top
instanceType: 4
objectCategory: CN=Group,CN=Schema,CN=Configuration,DC=<DOMAIN_CONTROLLER_NAME>
cn: NfvdManagement
desktopProfile: domain
distinguishedName: CN=NfvdManagement,OU=groups,OU=NfvdManagement,DC=<DOMAIN_CONTROLLER_NAME>
name: NfvdManagement


dn: OU=profiles,OU=NfvdManagement,DC=<DOMAIN_CONTROLLER_NAME>
objectClass: organizationalUnit
objectClass: top
instanceType: 4
objectCategory: CN=Organizational-Unit,CN=Schema,CN=Configuration, DC=<DOMAIN_CONTROLLER_NAME>,
DC=<DOMAIN_SUFFIX>
ou: profiles
distinguishedName: OU=profiles,OU=NfvdManagement,DC=<DOMAIN_CONTROLLER_NAME>
name: profiles

dn: CN=administrator,OU=profiles,OU=NfvdManagement,DC=<DOMAIN_CONTROLLER_NAME>
objectClass: group
objectClass: top
groupType: -2147483646
instanceType: 4
objectCategory: CN=Group,CN=Schema,CN=Configuration,DC=<DOMAIN_CONTROLLER_NAME>
cn: administrator
distinguishedName: CN=administrator,OU=profiles,OU=NfvdManagement,DC=<DOMAIN_CONTROLLER_NAME>
name: administrator

dn: OU=users,OU=NfvdManagement,DC=<DOMAIN_CONTROLLER_NAME>
objectClass: organizationalUnit
objectClass: top
instanceType: 4
objectCategory: CN=Organizational-Unit,CN=Schema,CN=Configuration, DC=<DOMAIN_CONTROLLER_NAME>,D
 C=<DOMAIN_SUFFIX>
ou: users
distinguishedName: OU=users,OU=NfvdManagement,DC=<DOMAIN_CONTROLLER_NAME>
name: users
```

For example:



```
C:\Users\Administrator>cd Documents

C:\Users\Administrator\Documents>dir
 Volume in drive C has no label.
 Volume Serial Number is D8A5-B8AD

 Directory of C:\Users\Administrator\Documents

04/14/2016  04:54 PM    <DIR>          .
04/14/2016  04:54 PM    <DIR>          ..
04/14/2016  04:54 PM             1,920 active_directory_structure.ldif
               1 File(s)          1,920 bytes
               2 Dir(s)  30,012,944,384 bytes free

C:\Users\Administrator\Documents>ldifde -i -k -f .\active_directory_structure.ld
if -j .\
Connecting to "WIN-1A76T8HM581.unica.local"
Logging in as current user using SSPI
Importing directory from file ".\active_directory_structure.ldif"
Loading entries.......
6 entries modified successfully.

The command has completed successfully

C:\Users\Administrator\Documents>_
```

Figure 13 : Configure Active Directory

1.4.4.2.4 Generating a self-signed certificate for LDAP

In order to make a SSL connection an update to JBoss “standalone.xml” configuration file is needed, then Import a self-signed certificate file generated in AD machine to JBoss java VM.

1. Generate a self-signed certificate.

In Active Directory Windows Machine, select Start button then Administrative tools, and then Server manager…

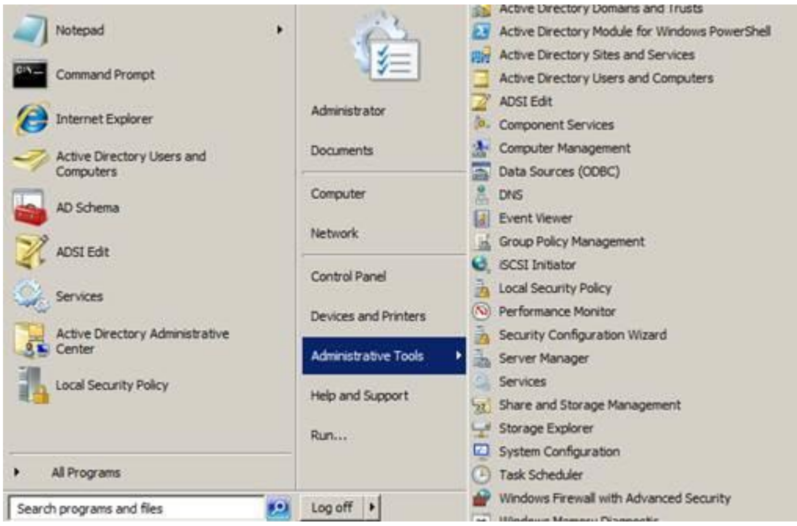
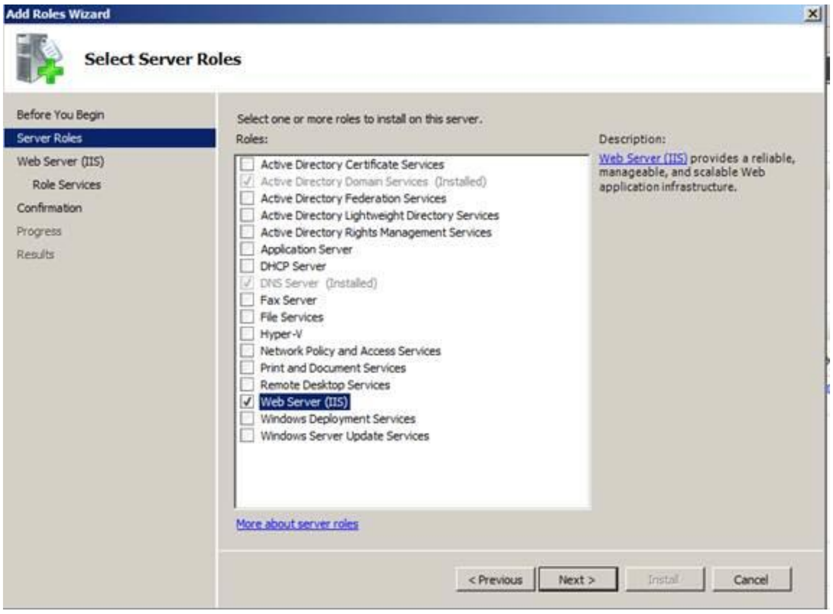


Figure 14 : Generating self-signed certificate for LDAP

In Server Manage, right-click on Roles node and select “Add roles…” click next…
In Add Roles Wizard check Web Server (IIS)… and click next, and then next again



Select Server Roles

Select one or more roles to install on this server.

Roles:

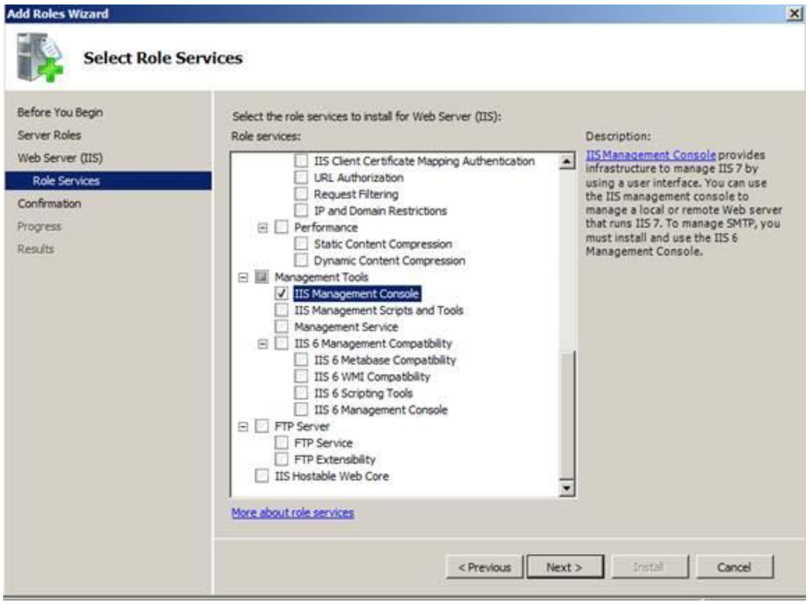
- ☐ Active Directory Certificate Services
- ☑ Active Directory Domain Services (Installed)
- ☐ Active Directory Federation Services
- ☐ Active Directory Lightweight Directory Services
- ☐ Active Directory Rights Management Services
- ☐ Application Server
- ☐ DHCP Server
- ☑ DNS Server (Installed)
- ☐ Fax Server
- ☐ File Services
- ☐ Hyper-V
- ☐ Network Policy and Access Services
- ☐ Print and Document Services
- ☐ Remote Desktop Services
- ☑ Web Server (IIS)
- ☐ Windows Deployment Services
- ☐ Windows Server Update Services

More about server roles

Description:
Web Server (IIS) provides a reliable, manageable, and scalable Web application infrastructure.

Figure 15 : Add Roles Wizard, server roles

In Role Services, deselect all checks and then check Management Tools -> IIS Management Console and then click next



Add Roles Wizard

Select Role Services

Select the role services to install for Web Server (IIS):

Role services:

- □ IIS Client Certificate Mapping Authentication
- □ URL Authorization
- □ Request Filtering
- □ IP and Domain Restrictions
- □ Performance
  - □ Static Content Compression
  - □ Dynamic Content Compression
- ▣ Management Tools
  - ☑ IIS Management Console
  - □ IIS Management Scripts and Tools
  - □ Management Service
  - □ IIS 6 Management Compatibility
    - □ IIS 6 Metabase Compatibility
    - □ IIS 6 WMI Compatibility
    - □ IIS 6 Scripting Tools
    - □ IIS 6 Management Console
- □ FTP Server
  - □ FTP Service
  - □ FTP Extensibility
- □ IIS Hostable Web Core

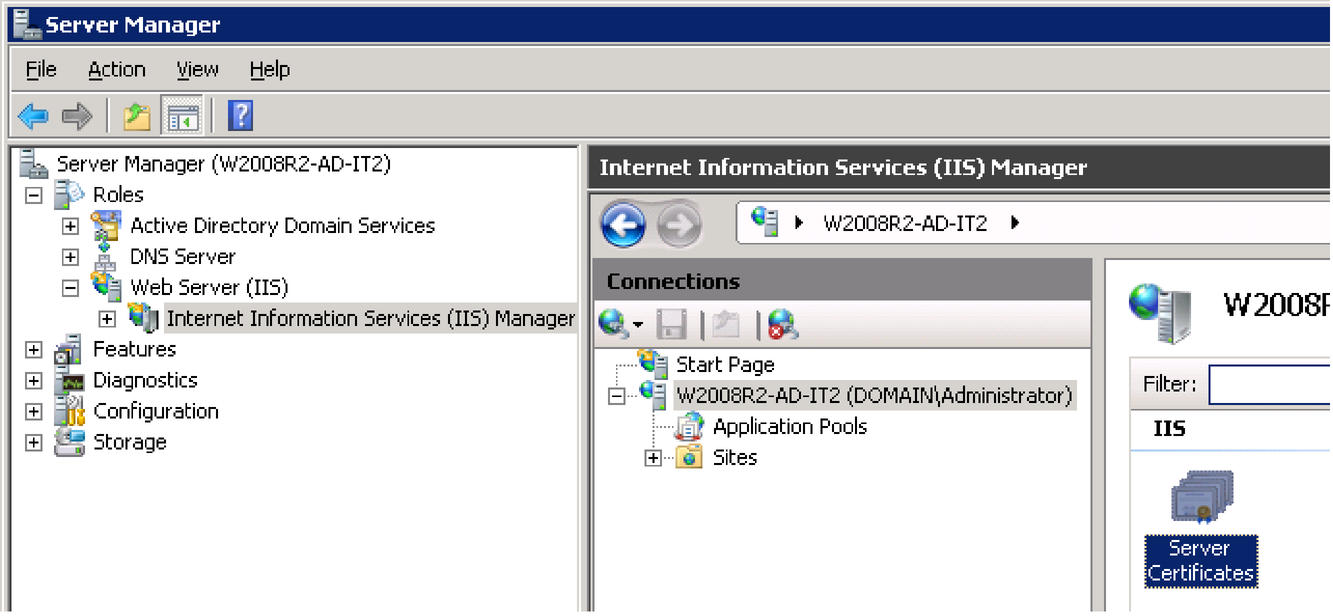
Description:

IIS Management Console provides infrastructure to manage IIS 7 by using a user interface. You can use the IIS management console to manage a local or remote Web server that runs IIS 7. To manage SMTP, you must install and use the IIS 6 Management Console.

Figure 16 : Add Roles Wizard, role services

In Confirmation step click “Install” and then “Close”.

Now in Server Manager window expand “Web Server (IIS)” node and select “Internet Information Services (IIS) Manager” node.
In the window on the right select “<machine-name>(DOMAIN\Administrator)” node and then double-click on “Server Certificates” icon:



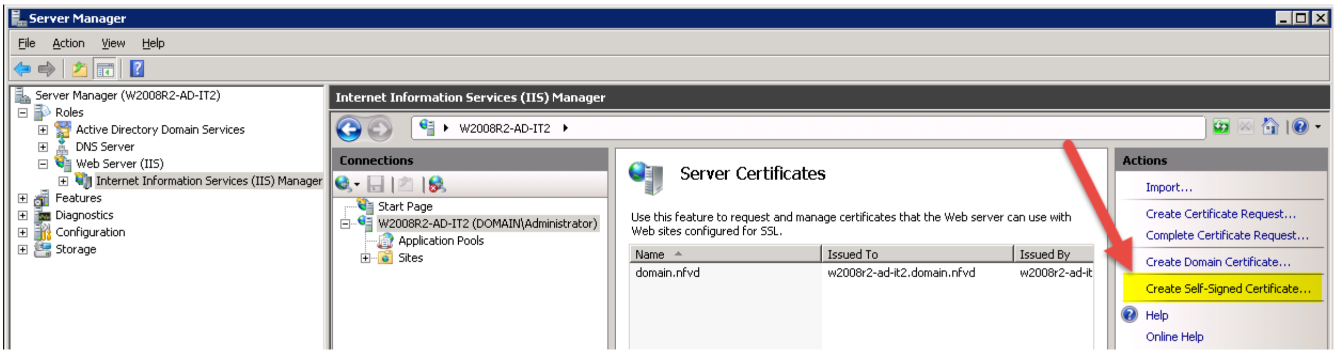
- Server Manager (W2008R2-AD-IT2)
  - Roles
    - Active Directory Domain Services
    - DNS Server
    - Web Server (IIS)
      - Internet Information Services (IIS) Manager
  - Features
  - Diagnostics
  - Configuration
  - Storage

Internet Information Services (IIS) Manager

- Start Page
- W2008R2-AD-IT2 (DOMAIN\Administrator)
  - Application Pools
  - Sites

Figure 17 : Server Manager, IIS Manager

In “Server Certificates” frame click on “Create Self-Signed Certificate…” on the right (“Actions” frame)

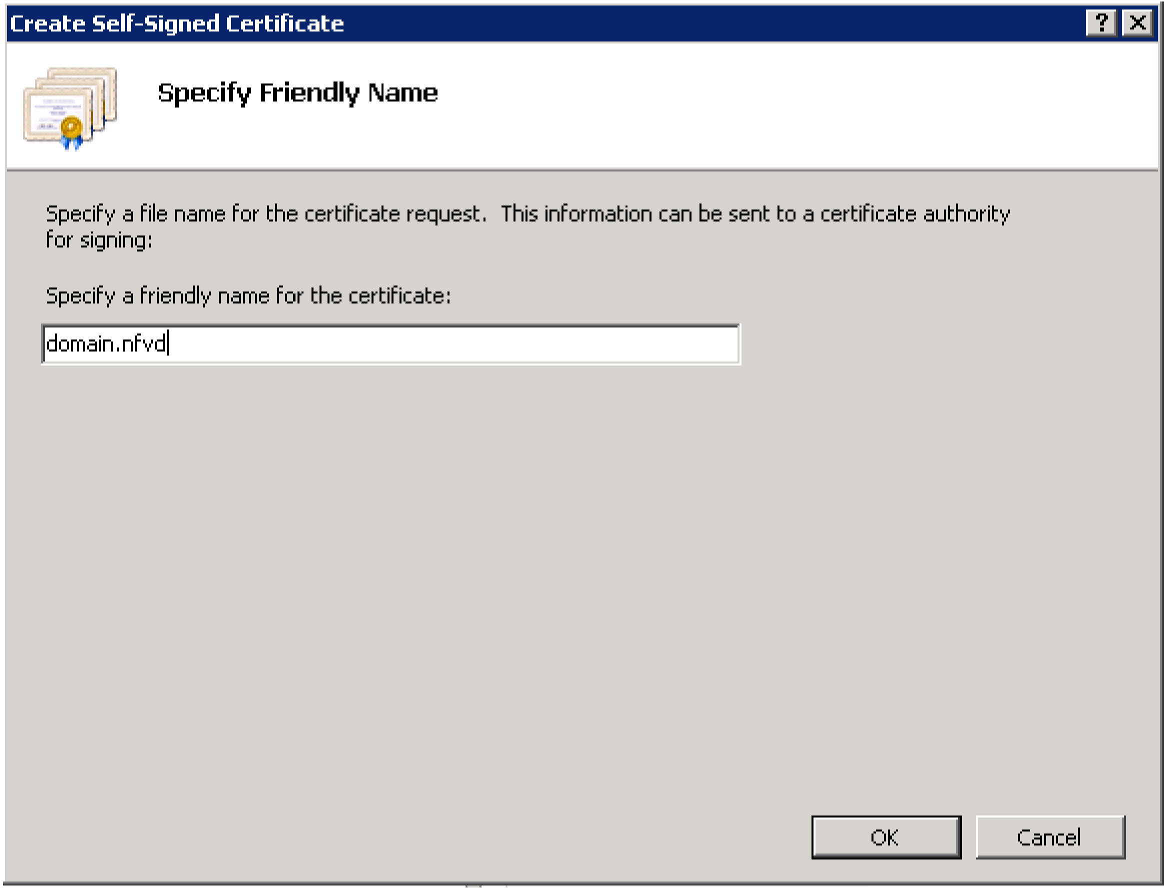

Server Manager
File Action View Help
Server Manager (W2008R2-AD-IT2)
Roles
Active Directory Domain Services
DNS Server
Web Server (IIS)
Internet Information Services (IIS) Manager
Features
Diagnostics
Configuration
Storage
Internet Information Services (IIS) Manager
W2008R2-AD-IT2
Connections
Start Page
W2008R2-AD-IT2 (DOMAIN\Administrator)
Application Pools
Sites
Server Certificates
Actions
Import...
Create Certificate Request...
Complete Certificate Request...
Create Domain Certificate...
Create Self-Signed Certificate...
Help
Online Help

Use this feature to request and manage certificates that the Web server can use with Web sites configured for SSL.

Name	Issued To	Issued By
domain.nfvd	w2008r2-ad-it2.domain.nfvd	w2008r2-ad-it

Figure 18 : Server Manager, create Self-Signed Certificate

In “Create Self-Signed Certifcate” window, type a friendly name for the file name and click “OK”…



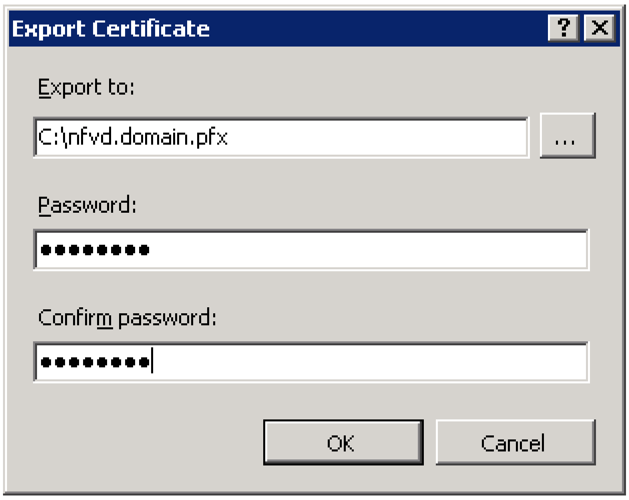
Specify a file name for the certificate request. This information can be sent to a certificate authority for signing:

Specify a friendly name for the certificate:

domain.nfvd

Figure 19 : Create Self-Signed Certificate, specify friendly name

Now, right click on the new certificate created and select “Export…”…
On “Export Certificate” dialog select a directory to export the certificate and then a password and click “OK”…



Export to:

C:\nfvd.domain.pfx

Password:

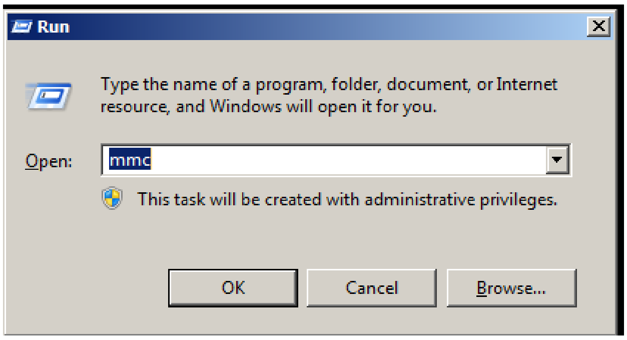
●●●●●●●●●

Confirm password:

●●●●●●●●●

Figure 20 : Export Certificate

In Active Directory Windows machine, select Start menu and then type “run”, then type “mmc”



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: mmc

This task will be created with administrative privileges.

Figure 21 : Run mmc

In console root window select File-> Add/Remove Snap-in...

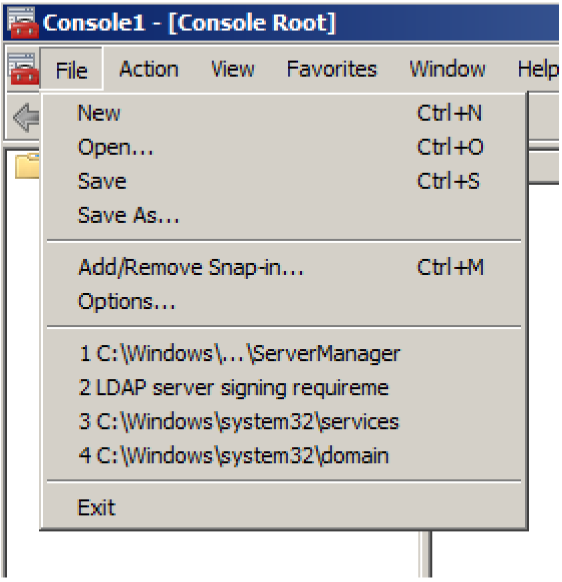
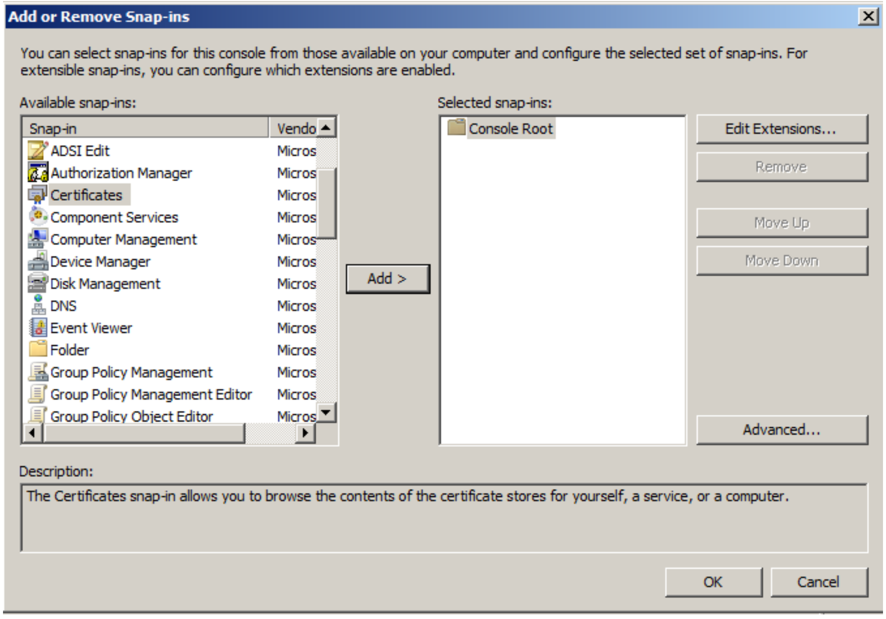

Console1 - [Console Root]
File
Action
View
Favorites
Window
Help
New Ctrl+N
Open... Ctrl+O
Save Ctrl+S
Save As...
Add/Remove Snap-in... Ctrl+M
Options...
1 C:\Windows\...\ServerManager
2 LDAP server signing requireme
3 C:\Windows\system32\services
4 C:\Windows\system32\domain
Exit

Figure 22 : Console1

In “Add or Remove Snap-ins” dialog select “Certificates”, then “Add->”, then check “Service Account”, then click “Next”...



Add or Remove Snap-ins

You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Available snap-ins:

Snap-in	Vendo
ADSI Edit	Micros
Authorization Manager	Micros
Certificates	Micros
Component Services	Micros
Computer Management	Micros
Device Manager	Micros
Disk Management	Micros
DNS	Micros
Event Viewer	Micros
Folder	Micros
Group Policy Management	Micros
Group Policy Management Editor	Micros
Group Policy Object Editor	Micros

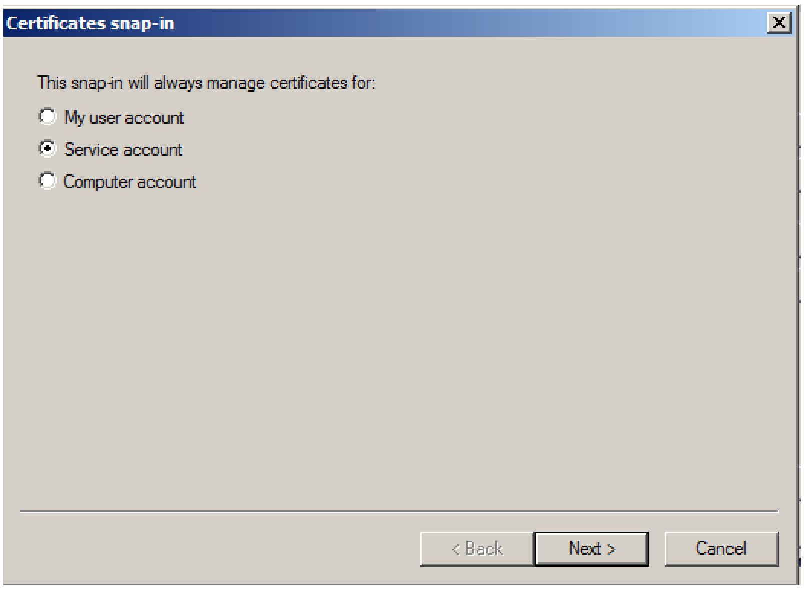
Selected snap-ins:

Console Root

Description:

The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.

Figure 23 : Add Snap-ins



Certificates snap-in

This snap-in will always manage certificates for:

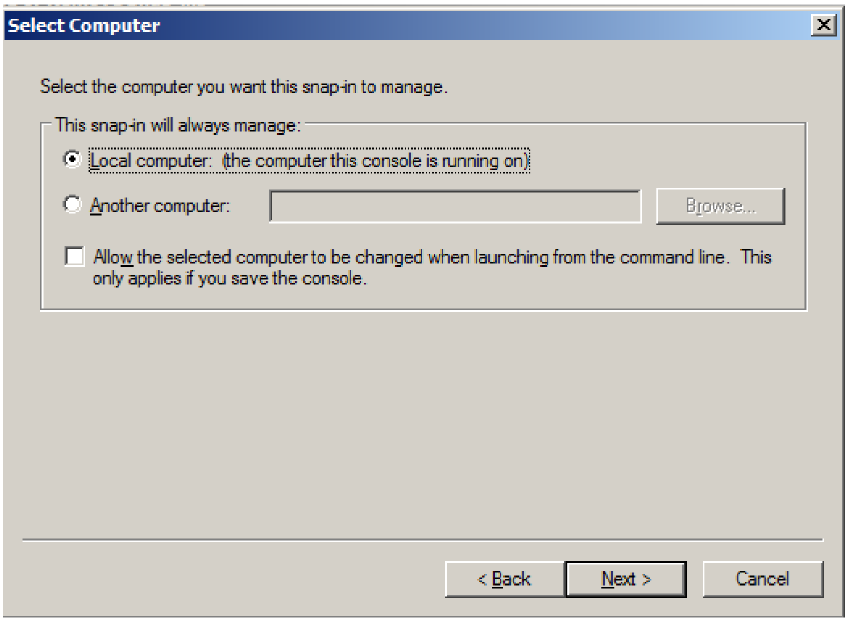
○ My user account

● Service account

○ Computer account

Figure 24 : Certificates snap-in

In “Select Computer” dialog select “Local computer”, then click “Next”



Select Computer

Select the computer you want this snap-in to manage.

This snap-in will always manage:

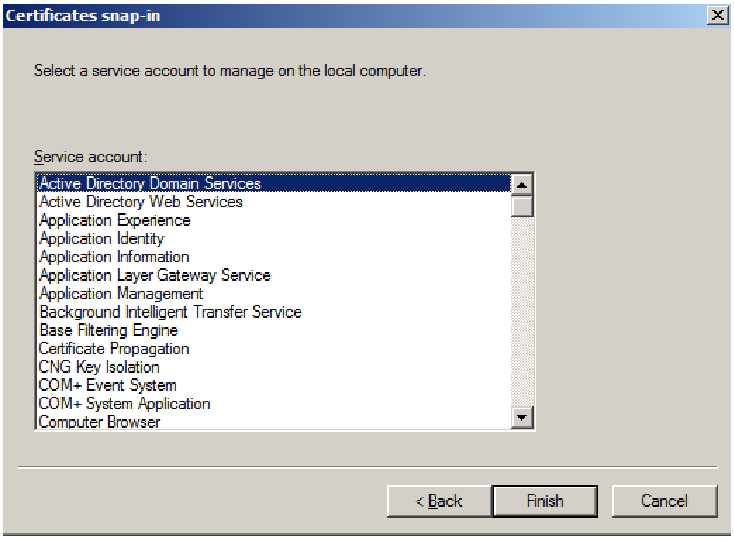
● Local computer: (the computer this console is running on)

○ Another computer:

□ Allow the selected computer to be changed when launching from the command line. This only applies if you save the console.

Figure 25 : Select Computer

In “Certificates snap-in” dialog select “Active Directory Domain Services” service account… and then click “Finish”



Certificates snap-in

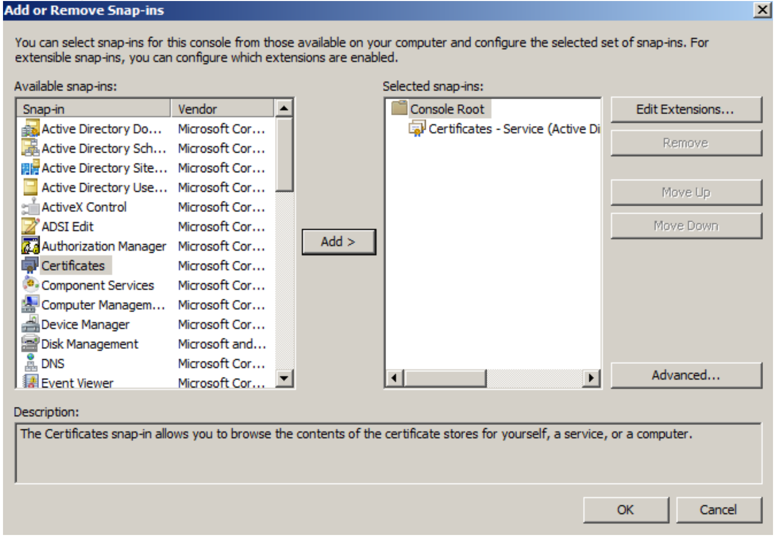
Select a service account to manage on the local computer.

Service account:

- Active Directory Domain Services
- Active Directory Web Services
- Application Experience
- Application Identity
- Application Information
- Application Layer Gateway Service
- Application Management
- Background Intelligent Transfer Service
- Base Filtering Engine
- Certificate Propagation
- CNG Key Isolation
- COM+ Event System
- COM+ System Application
- Computer Browser

Figure 26 : Certificates snap-in

In “Add or Remove Snap-ins” dialog click “OK”…



Add or Remove Snap-ins

You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Available snap-ins:

Snap-in	Vendor
Active Directory Do...	Microsoft Cor...
Active Directory Sch...	Microsoft Cor...
Active Directory Site...	Microsoft Cor...
Active Directory Use...	Microsoft Cor...
ActiveX Control	Microsoft Cor...
ADSI Edit	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificates	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Device Manager	Microsoft Cor...
Disk Management	Microsoft and...
DNS	Microsoft Cor...
Event Viewer	Microsoft Cor...

Selected snap-ins:

- Console Root
  - Certificates - Service (Active Di

Description:

The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.

Figure 27 : AA or Remove Snap-ins

1.4.4.2.5 Importing certificate to JBoss VM.

If the file that contains the self-signed certificate is named, for example, “nfvd.pfx” and the password for that file is “1234”…

Use *keytool* utility to import the certificate and reply to interactive questions with answers in red:

```
# /opt/java1.6/bin/keytool -importkeystore –srckeystore nfvd.pfx -srcstoretype pkcs12 -destkeystore
/opt/java1.6/jre/lib/security/cacerts -deststoretype JKS –noprompt
Enter destination keystore password: changeit
Enter source keystore password: 1234
Entry for alias 6ff943a2-aa90-4fbc-84eb-c51d1325ed5f successfully imported.
Import command completed:  1 entries successfully imported, 0 entries failed or cancelled
```

The self-signed certificate is imported in “cacerts” file:

```
******************************************
Alias name: 6ff943a2-aa90-4fbc-84eb-c51d1325ed5f
Creation date: Dec 22, 2015
Entry type: PrivateKeyEntry
Certificate chain length: 1
Certificate[1]:
-----BEGIN CERTIFICATE-----
MIIC+jCCAeKgAwIBAgIQJfbFmwaf44VPDNYayzzS8zANBgkqhkiG9w0BAQUFADAmMSQwIgYDVQQD
ExtXSU4tMUE3NlQ4SE01ODEudW5pY2EubG9jYWwwHhcNMTUxMjIyMTUyMjM5WhcNMTYxMjIyMDAw
MDAwWjAmMSQwIgYDVQQDExtXSU4tMUE3NlQ4SE01ODEudW5pY2EubG9jYWwwggEiMA0GCSqGSIb3
DQEBAQUAA4IBDwAwggEKAoIBAQDeEiQjZYTkVKKAE8UvTm0HaIgMKumm2HnoipfcuErIJ3VBlD3m
42k22QMXHgSW4w+2urZjYZtrbGs+d/wEcss7aFSo7/SU7DDl9h4ULgxQ3KSg8ozIg2q93X+oDkN0
AP4muhhw8hmstlVjgrpLy2HDBxVe8ruVwaWwCC04ebIOZFKFmdbjfYSJyMQX07tNLkS4jQ88+dTw
5reqZqfgFu2c45JWNOGBoYz9HTFg7UftWE3i5C5EoKA7qgpWwev/6ZKbbhh7EJfH6Xi300pEqdhB
8Q20x2VCZJ4GAP5/r483XE21sXfKPbgRgeK24XHQhHonJc9yMsa5m/e/Og/1muMXAgMBAAGjJDAi
MAsGA1UdDwQEAwIEMDATBgNVHSUEDDAKBggrBgEFBQcDATANBgkqhkiG9w0BAQUFAAOCAQEADmyb
MBQR7+sn0lpcOy4J/jJr4TBMfhxeIZ5rjUD3mtGfhCqzVP9xuYycBKPDTovPTi8xW9JZzOWOl8D3
tHBZWRDRciyfyD8uFOc6YotVaWM5Ql410hQ2uxNx6pS0z6+xdccSjjzAbTo3lUSADtm/VSv9YIb3
0HqTS4wgI4rzpBTmLyZiEb891COEO98LWQ28pByyyp2PzIN3te75BlRr2lN70otx57+TsLOuh0P9
bIBmfLBZwCIEHhhD9YzwlHW40HCMf68xav7iYVvelykIe+K8hTcbS7OBiQ7x2gXxfai2PsKX9hLf
tNoec5rJtwtFMd3l50WR55T5+scqUeU3nQ==
-----END CERTIFICATE-----
******************************************
```

Chapter 2 Installing NFVD

2.1 Installing NFVD Installer RPM

On: <INSTALLER_HOST>
Login: root

Copy NFVD installer in a repository directory (typical example: /kits/archives). Go to the directory where you copied the nfvd-installer-04.01.000-1.el6.noarch.rpm file and install it:

```
# rpm -ivh nfvd-installer-04.01.000-1.el6.noarch.rpm
```

Make sure that all required archives (see sections 1.2.1 and 1.2.2) are copied in the same directory (typical example: /kits/archives).

2.2 Installing a new platform

On: <INSTALLER_HOST>
Login: root

Execute the following command:

```
# /opt/HPE/nfvd/install/nfvd-install.sh /kits/archives
```

The installer automatically unpacks the necessary archives and will start asking some questions about the hostnames of the systems composing your platform, the discovery mode (use of OMi/uCMDB or not) and some Oracle DB and LDAP parameters. You will also have to enter the root password of each of your systems in order to configure the SSH access (required by the installer).

Once all data are entered, the installer asks: "*Do you want to continue with installation*".

At this point, if you choose '*y*', then the installer will continue with all default values for the ports, credentials, user names…
If you want to specify different values, refer to section 2.2.1 below in order to change some specific values.
When this is done, you can answer 'y' to resume the installation.

As soon as the installation is complete (it usually takes around 2 hours), please refer to sections 0 and 2.5 to install commercial licenses and to Chapter 3 "Post-installation steps" to execute post installation steps.

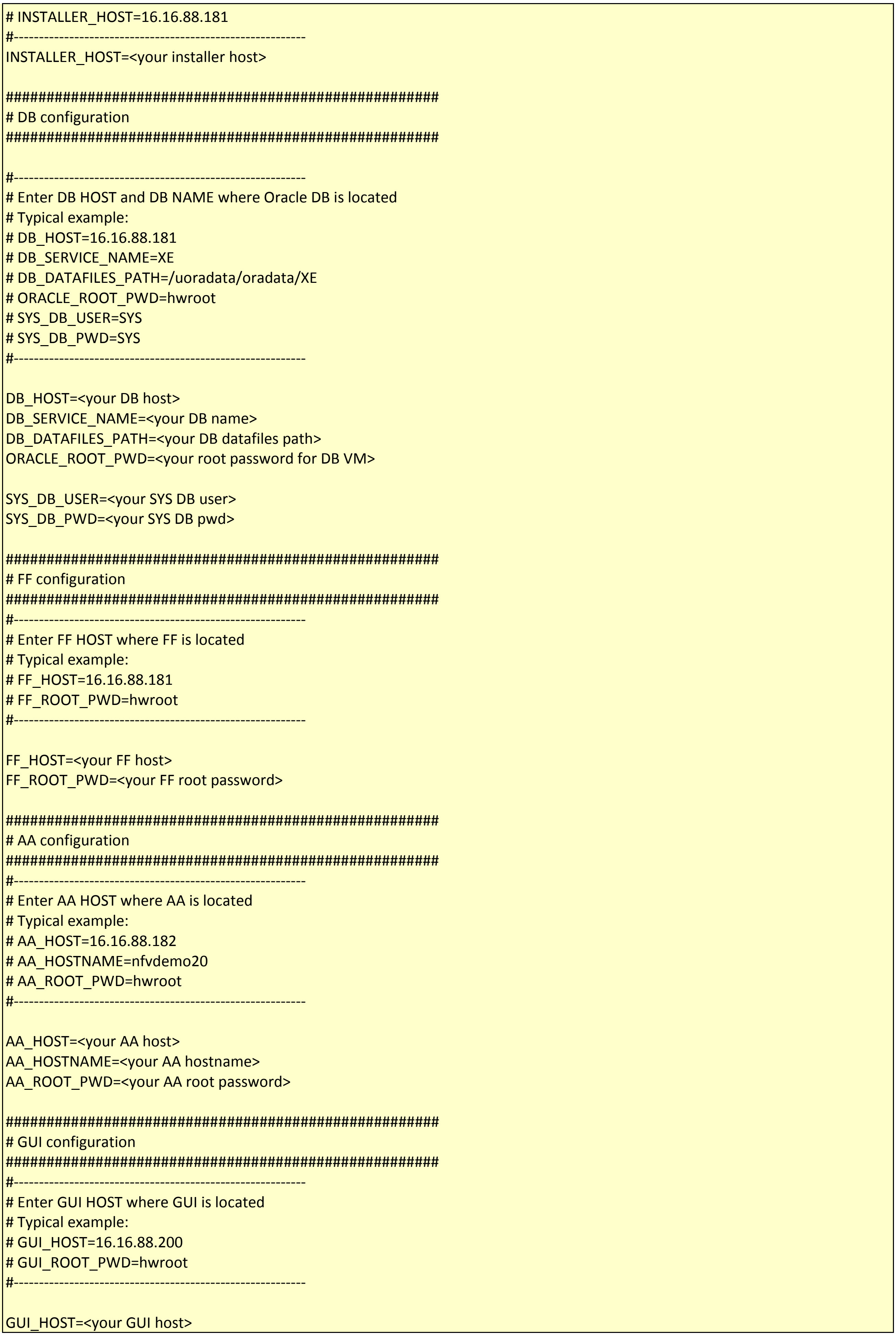
2.2.1 Filling in advanced NFVD configuration parameters

Skip this part if you plan to use the default values for the ports, credentials, user names…

On: <INSTALLER_HOST>
Login: root

Edit */var/opt/HPE/nfvd/install/NFVD_var* topology information file and update values between brackets with the topology information:

```
########################################################
# GENERIC CONFIG
########################################################
#-------------------------------------------------------
# Enter INSTALLER_HOST of NFV-D platform
# Typical example:
```



```
# INSTALLER_HOST=16.16.88.181
#---------------------------------------------------------
INSTALLER_HOST=<your installer host>

######################################################
# DB configuration
######################################################

#---------------------------------------------------------
# Enter DB HOST and DB NAME where Oracle DB is located
# Typical example:
# DB_HOST=16.16.88.181
# DB_SERVICE_NAME=XE
# DB_DATAFILES_PATH=/uoradata/oradata/XE
# ORACLE_ROOT_PWD=hwroot
# SYS_DB_USER=SYS
# SYS_DB_PWD=SYS
#---------------------------------------------------------

DB_HOST=<your DB host>
DB_SERVICE_NAME=<your DB name>
DB_DATAFILES_PATH=<your DB datafiles path>
ORACLE_ROOT_PWD=<your root password for DB VM>

SYS_DB_USER=<your SYS DB user>
SYS_DB_PWD=<your SYS DB pwd>

######################################################
# FF configuration
######################################################
#---------------------------------------------------------
# Enter FF HOST where FF is located
# Typical example:
# FF_HOST=16.16.88.181
# FF_ROOT_PWD=hwroot
#---------------------------------------------------------

FF_HOST=<your FF host>
FF_ROOT_PWD=<your FF root password>

######################################################
# AA configuration
######################################################
#---------------------------------------------------------
# Enter AA HOST where AA is located
# Typical example:
# AA_HOST=16.16.88.182
# AA_HOSTNAME=nfvdemo20
# AA_ROOT_PWD=hwroot
#---------------------------------------------------------

AA_HOST=<your AA host>
AA_HOSTNAME=<your AA hostname>
AA_ROOT_PWD=<your AA root password>

######################################################
# GUI configuration
######################################################
#---------------------------------------------------------
# Enter GUI HOST where GUI is located
# Typical example:
# GUI_HOST=16.16.88.200
# GUI_ROOT_PWD=hwroot
#---------------------------------------------------------

GUI_HOST=<your GUI host>
```

```
GUI_ROOT_PWD=<your GUI root password>

#######################################################
# DISCOVERY MODE
#######################################################
#-------------------------------------------------------
# Enter the Discovery mode
# TWO VALUES:
# OPENSTACK -> if you use Openstack for discovery
# HPSW -> if you use HP Software (cmdb, OMI)

DISCOVERY_MODE=OPENSTACK
```

Note: If you wish to perform advanced configuration by updating */var/opt/HPE/nfvd/install/repo_ansible/group_vars/all* file, contact NFVD Team.

2.3 Troubleshooting Installation

On: <INSTALLER_HOST>
Login: root

In case of failure, the installer exits, displaying the messages explaining what caused trouble.

When the blocking problem is fixed, the installation or upgrade can be resumed by calling:

```
# /opt/HPE/nfvd/install/nfvd-install.sh /kits/archives
```

You will have to answer "*We have detected existing installation files .. Do you want to resume it?*".

The installer from there will explicitely skip all steps previously done, and resume work from only the last failing step.

A complete, detailed installer log is always available in */tmp/nfvd_install.log*, and the particular trace of the step that caused failure in */tmp/nfvd_install_last.log*

2.4 Managing NFVD Base Products commercial licenses

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

2.4.1 Managing HPSA commercial license

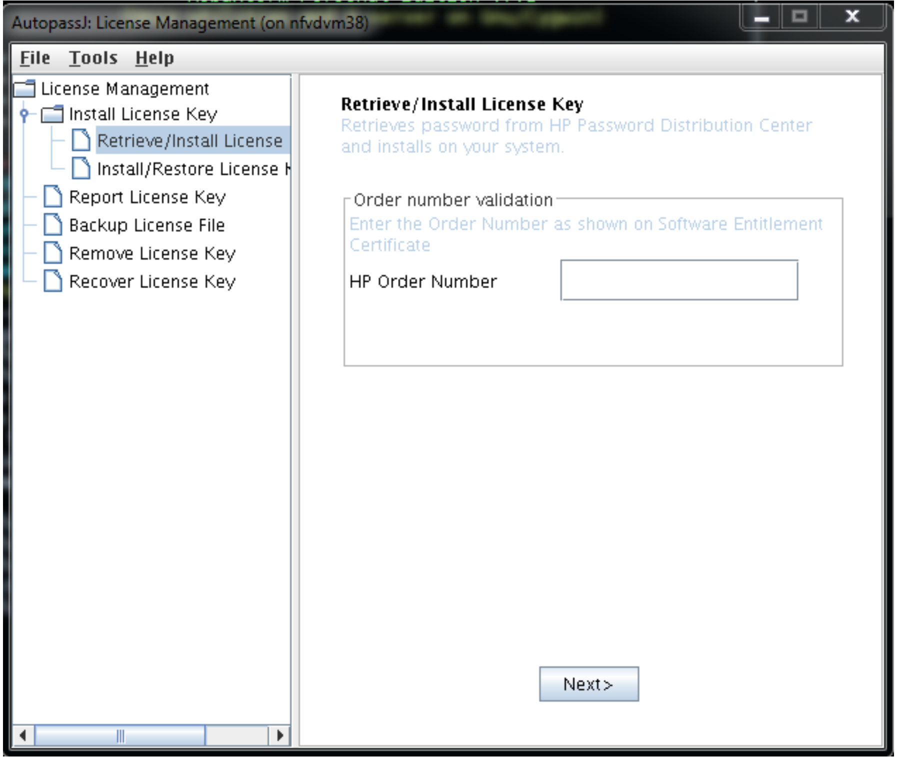
2.4.1.1 Installing HPSA commercial license

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.

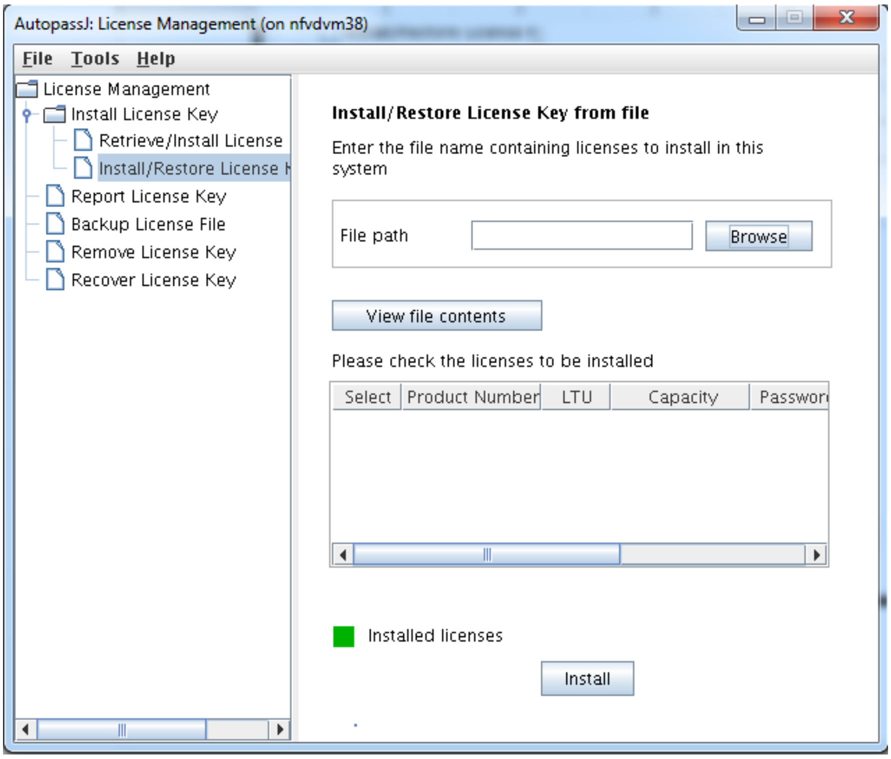
Order number validation

Enter the Order Number as shown on Software Entitlement Certificate

HP Order Number

Figure 28 : 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

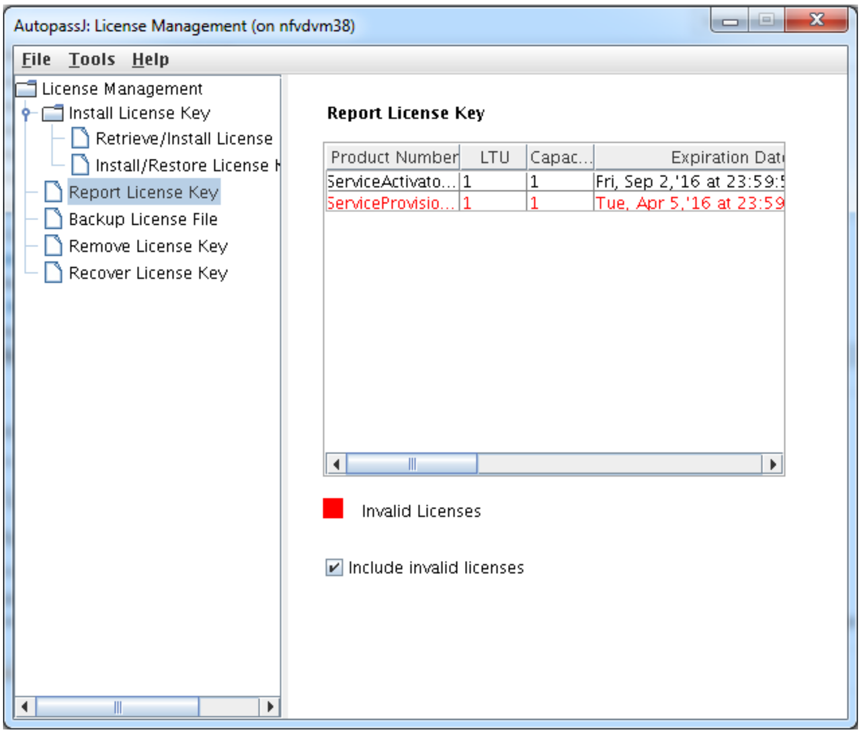
Please check the licenses to be installed

Select	Product Number	LTU	Capacity	Passwor

🟩 Installed licenses

Figure 29 : 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 Dat
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 30 : License Management, report license Key HPSA

2.4.1.2 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
```

2.4.2 Managing UCA for EBC commercial license

2.4.2.1 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.

2.4.2.2 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
```

2.4.3 Managing UCA Automation commercial license

2.4.3.1 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.

2.4.3.2 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
```

2.5 Managing SiteScope commercial license

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

2.5.1 Installing SiteScope commercial license

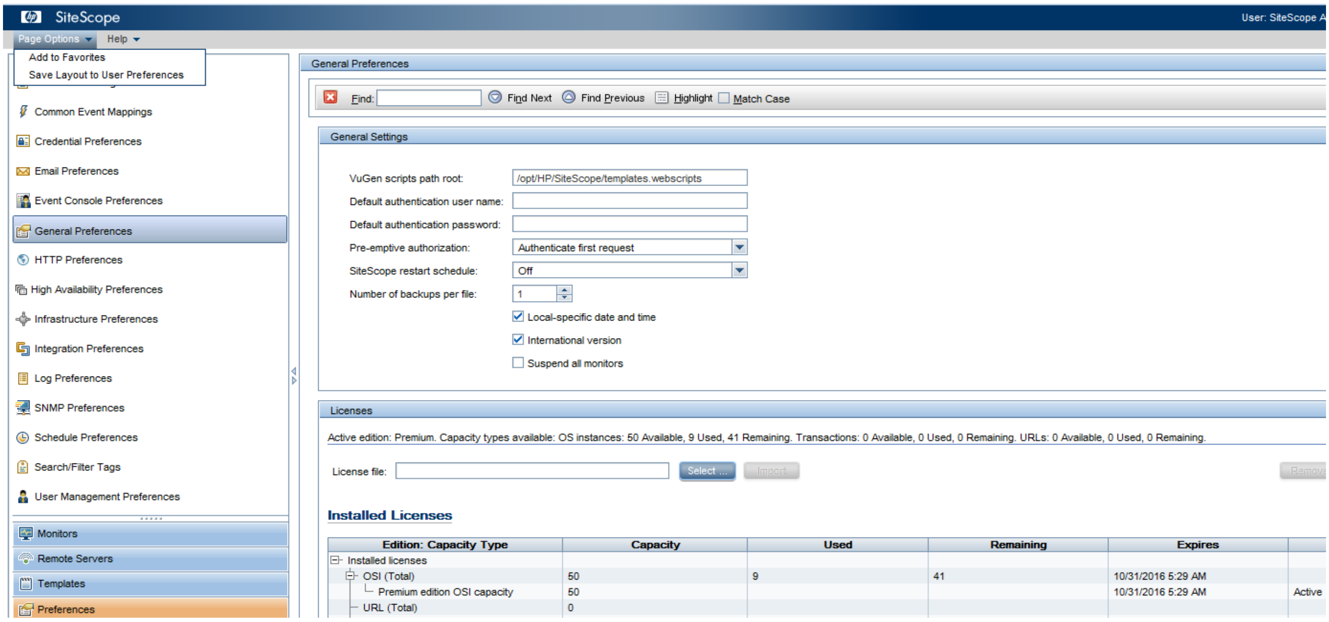
Note: This is a mandatory step to be executed during installation if NFVD monitoring feature is required.

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.



General Preferences

General Settings

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

Licenses

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 31 : Sitescope, installing License

2.5.2 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 3 Post-installation steps

3.1 Installing certificate for Active Directory connection

On: <FF_HOST>
Login: root

When your LDAP Vendor is Active Directory, the default configuration uses a SSL connection (port 636) between NFVD and AD server.
In this case, you need to import into your NFVD VM the CA Certificate from your AD server.
Refer to section 1.4.4.2.5 “Importing certificate to JBoss VM.

Standard procedure to import the CA certificate is shown below:

```
/opt/java1.6/bin/keytool -importkeystore -srckeystore my_ca_cert.pfx -srcstoretype pkcs12 -destkeystore
/opt/java1.6/jre/lib/security/cacerts -deststoretype JKS -noprompt
```

where:

/opt/java1.6	: path where your Java version is located
my_ca_cert.pfx	: file that contains the CA certificate from your AD server
/opt/java1.6/jre/lib/security/cacerts	: keystore where the CA cert will be sotred

Example output:

```
[root@my_vm ~]# /opt/java1.6/bin/keytool -importkeystore –srckeystore emea.local.pfx -srcstoretype pkcs12 -destkeystore
/opt/java1.6/jre/lib/security/cacerts -deststoretype JKS –noprompt
Enter destination keystore password: changeit
Enter source keystore password: 1234
Entry for alias 6ff943a2-aa90-4fbc-84eb-c51d1325ed5f successfully imported.
Import command completed:  1 entries successfully imported, 0 entries failed or cancelled
```

Here,
+ "changeit" is the password for cacerts file in your VM
+ "1234" is the certificate file password

You can list all the imported CA Certs using the following command:

```
/opt/java1.6/jre/bin/keytool keytool -list -v -keystore /opt/java1.6/jre/lib/security/cacerts
```

It will show entries similar to this:

```
********************************************
Alias name: 6ff943a2-aa90-4fbc-84eb-c51d1325ed5f
Creation date: Dec 22, 2015
Entry type: PrivateKeyEntry
Certificate chain length: 1
Certificate[1]:
-----BEGIN CERTIFICATE-----
MIIC+jCCAeKgAwIBAgIQJfbFmwaf44VPDNYayzzS8zANBgkqhkiG9w0BAQUFADAmMSQwIgYDVQQD
ExtXSU4tMUE3NlQ4SE01ODEudW5pY2EubG9jYWwwHhcNMTUxMjIyMTUyMjM5WhcNMTYxMjIyMDAw
MDAwWjAmMSQwIgYDVQQDExtXSU4tMUE3NlQ4SE01ODEudW5pY2EubG9jYWwwggEiMA0GCSqGSIb3
DQEBAQUAA4IBDwAwggEKAoIBAQDeEiQjZYTkVKKAE8UvTm0HaIgMKumm2HnoipfcuErIJ3VBlD3m
42k22QMXHgSW4w+2urZjYZtrbGs+d/wEcss7aFSo7/SU7DDl9h4ULgxQ3KSg8ozIg2q93X+oDkN0
AP4muhhw8hmstlVjgrpLy2HDBxVe8ruVwaWwCC04ebIOZFKFmdbjfYSJyMQX07tNLkS4jQ88+dTw
5reqZqfgFu2c45JWNOGBoYz9HTFg7UftWE3i5C5EoKA7qgpWwev/6ZKbbhh7EJfH6Xi300pEqdhB
8Q20x2VCZJ4GAP5/r483XE21sXfKPbgRgeK24XHQhHonJc9yMsa5m/e/Og/1muMXAgMBAAGjJDAi
MAsGA1UdDwQEAwIEMDATBgNVHSUEDDAKBggrBgEFBQcDATANBgkqhkiG9w0BAQUFAAOCAQEADmyb
MBQR7+sn0lpcOy4J/jJr4TBMfhxeIZ5rjUD3mtGfhCqzVP9xuYycBKPDTovPTi8xW9JZzOWOl8D3
tHBZWRDRciyfyD8uFOc6YotVaWM5Ql410hQ2uxNx6pS0z6+xdccSjjzAbTo3lUSADtm/VSv9YIb3
0HqTS4wgI4rzpBTmLyZiEb891COEO98LWQ28pByyyp2PzIN3te75BlRr2lN70otx57+TsLOuh0P9
```

```
bIBmfLBZwCIEHhhD9YzwlHW40HCMf68xav7iYVvelykIe+K8hTcbS7OBiQ7x2gXxfai2PsKX9hLf
tNoec5rJtwtFMd3l50WR55T5+scqUeU3nQ==
-----END CERTIFICATE-----
*******************************************
```

- Stop and restart Fulfillment host.

Note: Refer to *"Section 4.1* - Operating NFVD*"* for full description of steps to start, stop and check status of NFVD components.

3.2 Configuring NFVD domain user

On: <FF_HOST>
Login: root

As a starting point to log into the UI, you need to create a User at Domain level
Execute the following command to create a domain user called 'nfvd' (with password Welcome2016!)

```
# /opt/OV/ServiceActivator/solutions/NFVModel/etc/scripts/nfvd_createUser.sh -d <NFVD_DOMAIN_NAME> -e
<NFVD_DOMAIN_USER_EMAIL> <NFVD_DOMAIN_USER>

Typical Example:
# /opt/OV/ServiceActivator/solutions/NFVModel/etc/scripts/nfvd_createUser.sh -d nfvd.domain -e
localuser@localhost.localdomain nfvd
```

3.3 Configuring NFVD with SiteScope

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

On: <AA_HOST>
Login: root

Stop Sitescope

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

Import Sitescope templates

```
# cp -p /opt/HPE/nfvd/templates/config_tool_params.txt  /opt/HP/SiteScope/examples/silent_config_tool/
cp: overwrite `/opt/HP/SiteScope/examples/silent_config_tool/config_tool_params.txt'? y
# /opt/HPE/nfvd/bin/sitescope_config_import.sh
```

Start Sitescope (you may wait a couple of minutes before you get the message that SiteScope is started):

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


SiteScope started as a background process
#
```

3.4 Verifying NFVD installation

3.4.1 Access from NFVD GUI

http://<GUI_HOST>:3000/login
(Typical example: http://16.16.88.200:3000/login)

Login: <NFVD Domain User> / <Password NFVD Domain User>
(Typical example: nfvd/Welcome2016!)

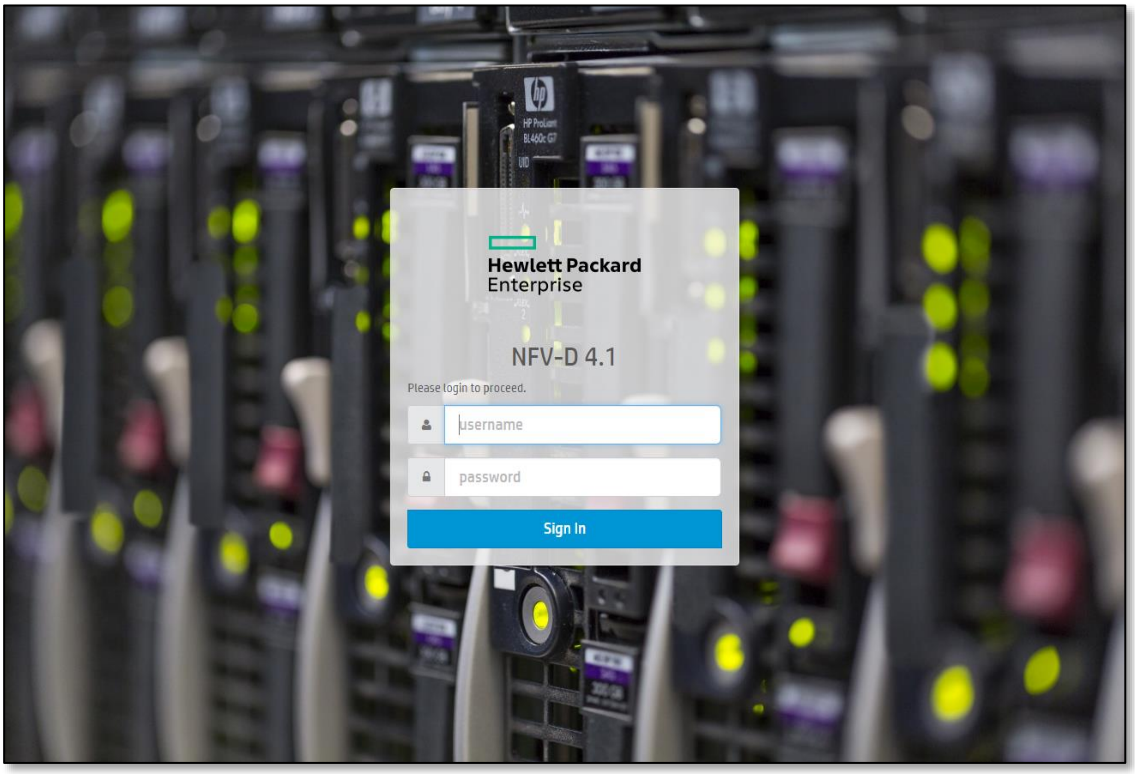


Figure 32 : UI portal

Once logged on, the workspaces available for NFVD Domain user profile are displayed.

3.4.2 Verifying objects synchronization of NFVD

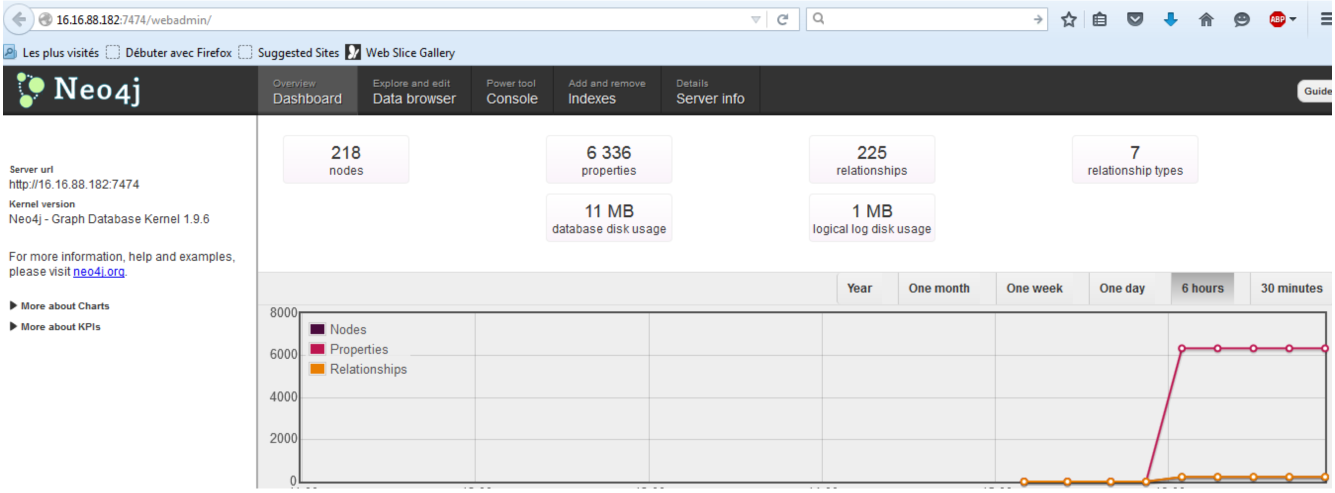
http://<AA_HOST>:7474/webadmin

(typical example: http://16.16.88.200:7474/webadmin)

NFVD components store persistent objects as follows:

- In Oracle database for NFVD Fulfillment component.
- In Neo4J database for NFVD Assurance component.

The run-time objects synchronization process between NFVD Fulfillment and Assurance components is automatically triggered when the Assurance Gateway is started. In order to verify successful completion of synchronization process, Neo4J database content can be checked:
If the number of nodes, properties and relationships is higher than 1, synchronization was successfully done.



218 nodes | 6 336 properties | 225 relationships | 7 relationship types
11 MB database disk usage | 1 MB logical log disk usage

Server url
http://16.16.88.182:7474
Kernel version
Neo4j - Graph Database Kernel 1.9.6

For more information, help and examples, please visit neo4j.org.

Figure 33 : Neo4J after synchronization

Check also JBOSS log files on Fulfillment host:

On: <FF_HOST>
Login: root

- Check */opt/HP/jboss/standalone/log/nfvd.log* file for following entry:

```
Element for synchornize:0
```

If this last checking is OK, then:

CONGRATULATIONS, YOU HAVE SUCCESSFULLY INSTALLED NFVD 4.1 !!!

Note: It is recommended to backup NFVD at that step.

3.5 Next step: configuring NFVD with infrastructure/VIM

NFVD can interoperate with 2 categories of infrastructure/VIM: Openstack and vCenter.

3.5.1 Importing VIM certificate to SiteScope

If the VIM (vCenter, RHOS, pure OpenStack, HCG) services are https enabled, it is mandatory to import the VIM certificate into SiteScope.

In order to import VIM certificate into SiteScope, following is the process:

1. Access the VIM say - HCG-openstack in a browser (eg: Mozilla firefox)
2. If the certificate is already saved in the local keystore/registry, access in browser Options -> Advanced -> Certificates -> View Certificates -> Servers tab and select appropriate certificate used by the VIM in list(eg., H13-HCG-IP)
3. Alternately, in case of a first time user access of VIM, when the certificate challenge is thrown, select View Certificate >> Details
4. Export the certificate as a file to a local system.
5. Login to Sitescope.
6. Navigate to -> preferences -> Certificate Management -> import the certificate saved in the local system

3.5.2 Running VIM Discovery

- For an Openstack, discovery of physical and virtual resources (also referenced as 'Resource Tree') can be done in two ways:
  - *OpenStack-based discovery*: Please refer to *NFV Director Openstack Discovery Guide*
  - *HPSW-based discovery* (using OMi and uCMDB): Please refer to *NFV Director Omi and uCMDB for NFVD User Guide*
- For a vCenter, there is no automatic discovery. The resource tree must be manually created and uploaded to NFVD
  - Please refer to *NFV Director vCenter Resource Modeling Guide*

Chapter 4 Administering NFVD

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

4.1 Operating NFVD

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
```

4.2 Running NFVD Assurance component utilities

NFVDirector is a solution encompassing a vast range of features and technologies. Given the vastness of the solution, there is a need to make the product user friendly. To accommodate the feature access a few utilities are provided as below.

On: <AA_HOST>
Login: root

4.2.1 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
```

4.2.2 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>>
```

4.2.3 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>>
```

4.2.4 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>>
```

4.2.5 Changing Assurance Gateway logging level

The tool *nfvd_assurance_logger.sh* can be used to set the Assurance Gateway logging level to production or troubleshooting level.

```
# cd /opt/HPE/nfvd/bin
# ./nfvd_assurance_logger.sh -level <production | troubleshoot>
```

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

```
# cd /opt/HPE/nfvd/bin
# ./setAGWLogLevel.sh –l <ERROR|DEBUG|FINEST|FINER|FINE|TRACE|CONFIG|INFO|WARN|FATAL>
```

4.2.6 Integrating SiteScope with Assurance Gateway to enable KPI metrics collection

In order to enable KPI data collection from SiteScope, perform the following steps. This is an optional step.

1. Login to SiteScope.
2. From Preferences > General Preferences > LW SSO Settings, copy the value in ‘Communication security passphrase’.
3. Edit the file /var/opt/HP/nfvd/conf/lwssofmconf.xml and enter the value of ‘Communication security passphrase’ to initString attribute. Save the file.
4. Use this saved file as one of the input parameter in the dataintegration_tool_sitescope.sh script.

```
# cd /opt/HPE/nfvd/templates/bin
# ./dataintegration_tool_sitescope.sh -lwssopath <lwssofmconf.xml path> -host <Sitescope-
hostnameOrIP> -port <Sitescope-port> -uname <SitescopeAdminUsername> -pass
<SitescopeAdminPassword> -dname <diname> -url <url> -tagname <tagname>
```

Typical example:

```
# cd /opt/HPE/nfvd/templates/bin/
# ./dataintegration_tool_sitescope.sh -lwssopath /var/opt/HPE/nfvd/conf/lwssofmconf.xml -
host localhost -port 18888 -uname admin -pass admin -dname DefaultSis-AGW-INTG -url
https://localhost:18443/nfvd/kpimetrics -tagname NFVD
```

Appendix ASecuring 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

A.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
```

A.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 4.1* Operating NFVD*"* for full description of steps to start, stop and check status of NFVD components.

A.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
```

A.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.

A.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 A.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

A.3.3 SiteScope

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

A.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)

<u>NOTE: Optional configuration for truststore if required can be done</u>

a) reconciliation-endpoints.properties

<u>Location</u>: /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

<u>Location</u>: /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

<u>Location</u>: /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>
```

A.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