



# **HPE NFV Director**

Installation and Configuration Guide

Release 4.2

Second Edition

# Notices

---

## Legal notice

© Copyright 2017 Hewlett Packard Enterprise Development LP

Confidential computer software. Valid license from HPE required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

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

<b>Notices .....</b>	<b>1</b>
<b>Preface.....</b>	<b>6</b>
About this Guide .....	6
Audience .....	6
Document History .....	6
<b>Chapter 1 Preparing and checking NFVD environment .....</b>	<b>7</b>
1.1 Overview .....	7
1.2 Checking packages availability.....	7
1.2.1 Checking NFVD packages availability .....	7
1.2.2 Checking SiteScope package availability.....	7
1.2.3 Prerequisite software .....	7
1.2.3.1 Fulfillment.....	7
1.2.3.2 NFV Director GUI .....	8
1.2.3.3 General .....	8
1.2.3.4 Software links .....	9
1.3 Preparing NFVD environment .....	9
1.3.1 Preparing configuration of hosts.....	9
1.3.2 Instantiating NFVD VMs in VMware infrastructure .....	10
1.3.3 Performing basic setup of NFVD VMs .....	13
1.3.3.1 Installing RPMs.....	14
1.3.3.2 Setting up file system layout.....	14
1.3.3.3 Enabling ports .....	15
1.3.4 Configuring NFVD with LDAPv3 server .....	17
1.3.4.1 Configuring NFVD with openLDAP .....	18
1.3.4.2 Configuring NFVD with ActiveDirectory .....	20
1.3.4.3 Install LDAP from scratch. ....	29
<b>Chapter 2 Installing/Upgrading NFVD .....</b>	<b>35</b>
2.1 Installing a new platform .....	35
2.1.1 Filling in advanced NFVD configuration parameters .....	35
2.1.2 Special case of HA platform installation.....	37
2.2 Upgrading an existing platform .....	37
2.3 Installation tools Overview .....	38
2.4 Troubleshooting Installation/Upgrade .....	39
<b>Chapter 3 Post-installation steps.....</b>	<b>40</b>
3.1 Install Commercial licenses .....	40
3.2 Integrating SiteScope with Assurance Gateway to enable KPI metrics collection.....	40
3.3 Configure the NFVD API to support https. ....	42
3.4 Installing certificate for Active Directory connection .....	43
3.5 Configuring NFVD domain user.....	45
3.6 Verifying NFVD installation .....	45

3.6.1 Access from NFVD GUI .....	45
3.6.2 Verifying objects synchronization of NFVD.....	46
<b>Chapter 4 NFVD Deployment set ups.....</b>	<b>48</b>
4.1 NFV Director Deployment flavors.....	50
4.1.1 NFVD VM View Simplex Flavor.....	51
4.1.2 NFVD VM View Duplex Flavor .....	52
4.1.3 NFVD VM View GR, duplex and duplex flavor Flavor .....	53
4.1.4 NFVD VM View Demo Flavor.....	54
<b>Annex 1: NFVD Module View.....</b>	<b>55</b>
Annex 1.1: NFV Service View. ....	56
Annex 1.2: NFV Module View.....	58
<b>Annex 1.3: NFVD Funtional architecture compared to Openstack .....</b>	<b>58</b>
<b>Annex 2: Subscribing to HPE Security Bulletins.....</b>	<b>59</b>
<b>Annex 3: Generating a self-signed certificate for LDAP.....</b>	<b>60</b>

## List of tables

Table 1: Document history .....	6
Table 2 : Required media for installation .....	7
Table 3 : Required media for installation .....	7
Table 4 : Software download links .....	9
Table 5 : Naming convention .....	9
Table 6 : Product naming convention.....	10
Table 7 : Typical sizing required per component .....	11
Table 8 : File system layout for NFVD FF.....	15
Table 9 : File system layout for NFVD AA .....	15

# List of figures

Figure 1 : Date/Time Properties .....	13
Figure 2 : Double click in Schema shortcut .....	21
Figure 3 : Create Attribute.....	21
Figure 4 : Fill the values for new attribute .....	22
Figure 5 : New attribute 'sshPublicKey' has been created.....	22
Figure 6 : Double click in Schema shortcut .....	23
Figure 7 : Create Class.....	23
Figure 8 : Fill the values for new class .....	24
Figure 9 : Adding a new optional attribute to the new class .....	24
Figure 10 : Adding sshPublicKey attribute.....	25
Figure 11 : sshPublicKey attribute added.....	25
Figure 12 : Schema class ldapPublicKey.....	26
Figure 13 : Configure Active Directory .....	28
Figure 28 : SiteScope Data Integration Preferences.....	41
Figure 29 : UI portal .....	46
Figure 30 : Neo4J after synchronization.....	47
Figure 31 Possible set up for the deployment. ....	49
Figure 32 Level schema of the NFVD deployment. ....	50
Figure 33 NFV Director Deployment Flavors.....	50
Figure 34– Simplex Flavor.....	51
Figure 35– Duplex Flavor.....	52
Figure 36 Legion – GR, duplex & duplex Flavor.....	53
Figure 37 Demo Flavor.....	54
Figure 38 NFV Director Modules and services.....	55
Figure 39 NFVD Service View .....	57
Figure 40 NFVD Module View.....	58
Figure 41 NFVD Architecture VS Openstack Architecture .....	58
Figure 42: HPE Security Bulletins .....	59
Figure 14 : Generating self-signed certificate for LDAP .....	60
Figure 15 : Add Roles Wizard, server roles .....	60
Figure 16 : Add Roles Wizard, role services.....	61
Figure 17 : Server Manager, IIS Manager.....	61
Figure 18 : Server Manager, create Self-Signed Certificate.....	62
Figure 19 : Create Self-Signed Certificate, specify friendly name.....	62
Figure 20 : Export Certificate .....	63
Figure 21 : Run mmc.....	63
Figure 22 : Console1.....	63
Figure 23 : Add Snap-ins.....	64
Figure 24 : Certificates snap-in .....	64
Figure 25 : Select Computer.....	65
Figure 26 : Certificates snap-in .....	65
Figure 27 : AA or Remove Snap-ins .....	66

# Preface

---

## About this Guide

---

This document describes the operations related to installation, configuration and administration of NFVD 4.2 for a typical standard production environment:

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

This document does not cover the steps related to VIM/solution integration, such as:

- Configuring and administering discovery for NFVD 4.2
- Configuring NFVD 4.2 optional Software Components (OMi, CMDB).
- Installing NFVD 4.2 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 and configure 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	16th January, 2017	First edition
2	15 <sup>th</sup> March, 2017	Second Edition. Updates to NFVD deployment set ups

Table 1: Document history

# Chapter 1 Preparing and checking NFVD environment

## 1.1 Overview

This includes following steps:

- Checking packages availability
- Preparing NFVD 4.2 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-04.02.000-1.el6.noarch.rpm
NFVD Base Product	NFVD420_BaseProduct.tar
NFVD Software	NFVD420_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 11.31 for Linux + patches	HP_SiteScope_1131.tar

Table 3 : Required media for installation

### 1.2.3 Prerequisite software

#### 1.2.3.1 Fulfillment

The following table lists the various software components that comprise NFV Director Fulfillment.

Product	Version
Oracle Database	11gR2 / 12c



**NOTE:**

Oracle Database is not included in NFV Director software release. It is mandatory to have Oracle Database.

### 1.2.3.2 NFV Director GUI

The following table lists the various software components that comprise NFV Director GUI.

Product	Version
Apache Couch DB	V1.6.0-1
Graphviz	2.38.0-1
OpenSSL	1.0.1e-42

**NOTE:**

Apache Couch DB as well as Graphviz are not included in NFV Director software release. It is mandatory to have both Apache Couch DB and Graphviz.

### 1.2.3.3 General

NFVD Director must have access to an Oracle database, as well as OpenLdap or Active Directory

Oracle instant client are necessary for the installer.

Component	Version/Part Number
Oracle	11gR2 / 12c oracle-instantclient11.2-sqlplus-11.2.0.4.0-1.x86_64.rpm oracle-instantclient11.2-basic-11.2.0.4.0-1.x86_64rpm
openLDAP	OpenLDAP V3 openldap, openldap-clients RPMs are required for client function openldap-servers if you intend to run a LDAP server.
yum	Access to the RedHat release installation repositories.

**NOTE:**

**oracle-instantclient11.2-sqlplus** and **oracle-instantclient11.2-basic** are not included in NFV Director software release. It is mandatory to have both installed on the installer node prior to NFVD installation.

It is mandatory for yum to be in working order on all the nodes of the platform, with working access to the RedHat release installation repositories (DVD, iso or remote repositories).

### 1.2.3.4 Software links

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

Component	Version/Part Number
Oracle	<a href="http://docs.oracle.com">http://docs.oracle.com</a>
couchDB	<a href="http://docs.couchdb.org">http://docs.couchdb.org</a>
Apache Directory Studio	<a href="https://directory.apache.org/studio/">https://directory.apache.org/studio/</a>
Active Directory schema snap-in installation in Windows 2008R2	<a href="http://social.technet.microsoft.com/wiki/contents/articles/10827.install-all-the-active-directory-schema-snap-in-in-windows-2008-server.aspx">http://social.technet.microsoft.com/wiki/contents/articles/10827.install-all-the-active-directory-schema-snap-in-in-windows-2008-server.aspx</a>
openLDAP	<a href="http://docs.adaptivecomputing.com/viewpoint/hpc/Content/topics/1-setup/installSetup/settingUpOpenLDAPOnCentos6.htm">http://docs.adaptivecomputing.com/viewpoint/hpc/Content/topics/1-setup/installSetup/settingUpOpenLDAPOnCentos6.htm</a>

Table 4 : Software download links

## 1.3 Preparing NFVD environment

### 1.3.1 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 5 : 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 or 12c) in order to deploy its data model and store persistent data.

**Note:** If you want to benefit from Georedundancy capability, it is mandatory that Oracle DB server component be with version Oracle 12c.

- 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 7/8/9, pure OpenStack Kilo/Mitaka/Liberty 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 6 : Product naming convention

**Note:** <FF\_HOST> <AA\_HOST> <GUI\_HOST> <INSTALLER\_HOST> and <ORACLE\_HOST> are expected to answer to a ping.

## 1.3.2 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		vDisks	Disk size (GB)
-----------	----------	------------	-------	--	--------	----------------

				RAM (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 7 : 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:

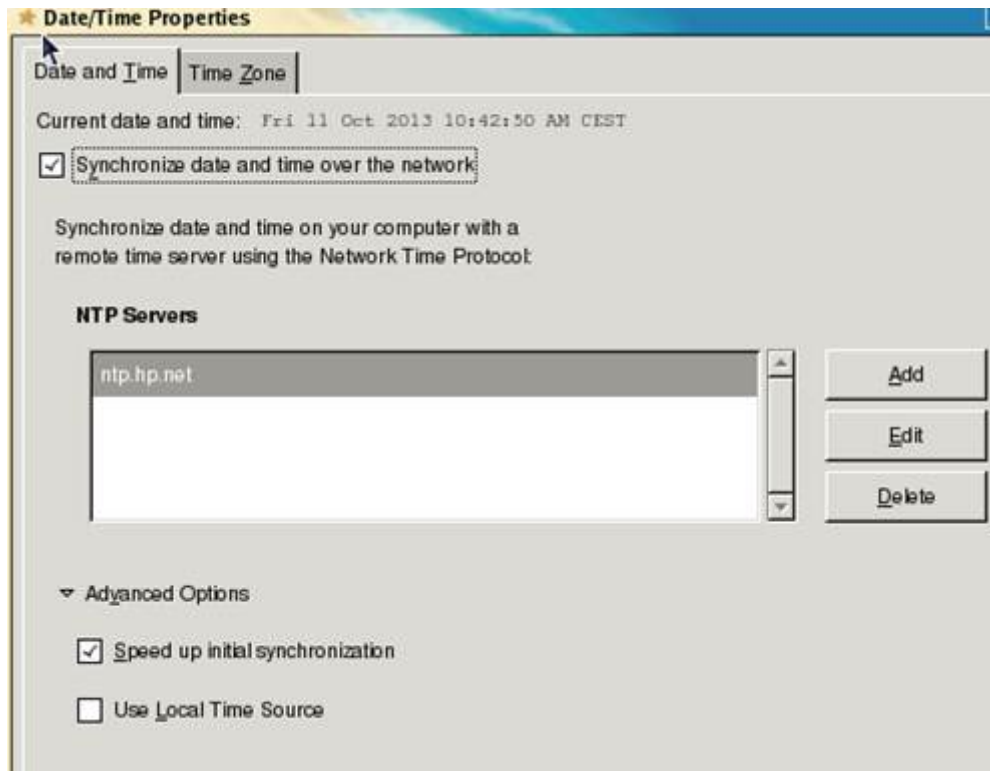


Figure 1 : Date/Time Properties

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 - $basearch - Base OS
baseurl=http://repoman.gre.hp.com/mrepo/rhel6.6-server-$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

#
```

### 1.3.3 Performing basic setup of NFVD VMs

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

### 1.3.3.1 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

### 1.3.3.2 Setting up file system layout

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

### 1.3.3.2.1 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 8 : File system layout for NFVD FF

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

### 1.3.3.2.2 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 9 : File system layout for NFVD AA

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

### 1.3.3.2.3 GUI host

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

### 1.3.3.3 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 <SITESCOPE_CLASSIC_USER_INTERFACE_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 8888 -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
```

## 1.3.4 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 1.3.4.1
- Active Directory : go to section 1.3.4.2

### 1.3.4.1 Configuring NFVD with openLDAP

Skip this part if you use Active Directory.

#### 1.3.4.1.1 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=external,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
```

#### 1.3.4.1.2 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
```

### 1.3.4.1.3 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
```

## 1.3.4.2 Configuring NFVD with ActiveDirectory

Skip this part if you use OpenLDAP.

### 1.3.4.2.1 Prerequisites

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

### 1.3.4.2.2 Extending ActiveDirectory schema

---

**On:** <AD\_HOST>

**Login:** root

---

#### 1.3.4.2.2.1 Attribute 'sshPublicKey'

1. Double click on AD Schema snap-in

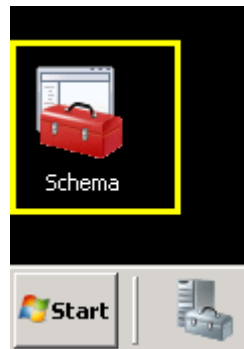
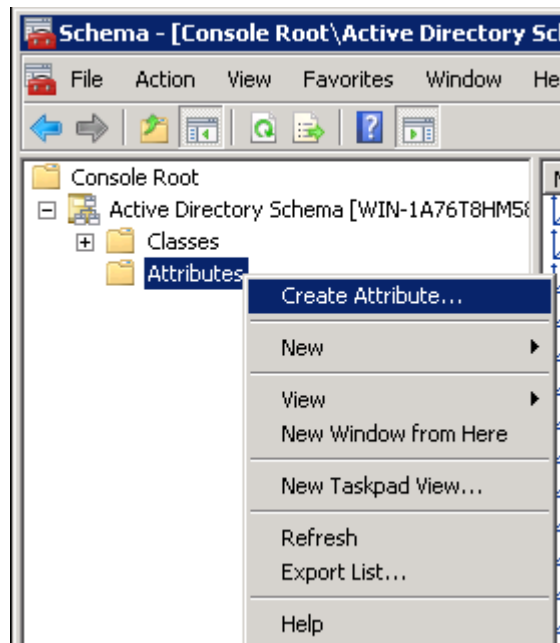


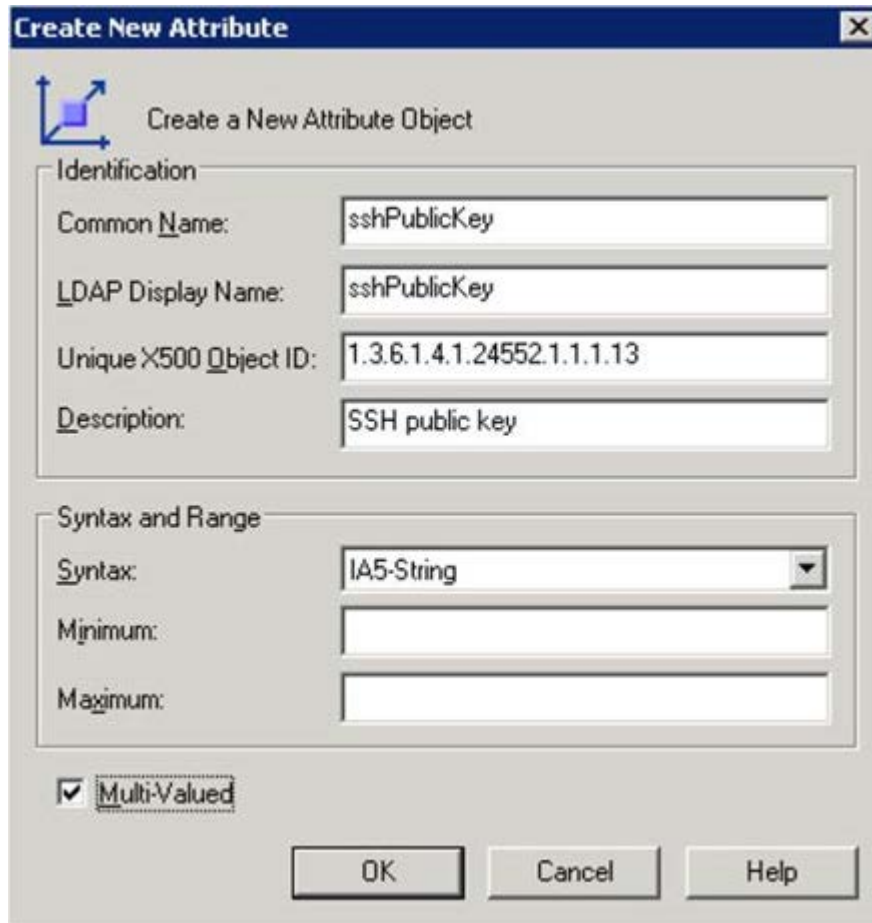
Figure 2 : Double click in Schema shortcut



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

Figure 3 : Create Attribute

3. Fill the values according to next image:



**Create New Attribute**

Create a New Attribute Object

**Identification**

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 and Range**

Syntax: IA5-String

Minimum:

Maximum:

☒ Multi-Valued

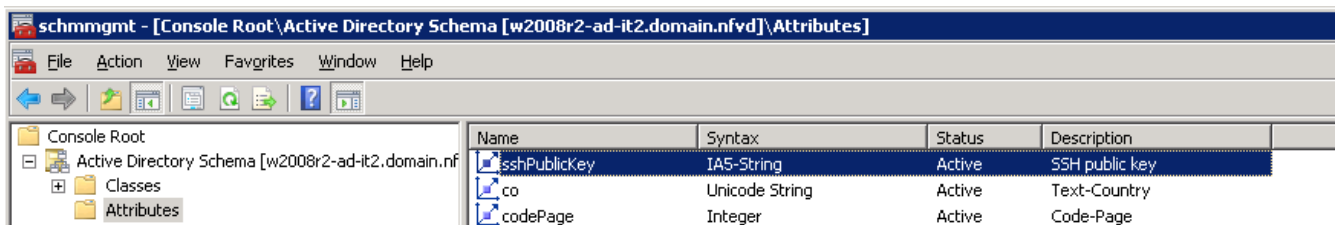
OK Cancel Help

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]

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

#### 1.3.4.2.2.2 Schema Class 'ldapPublicKey'

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

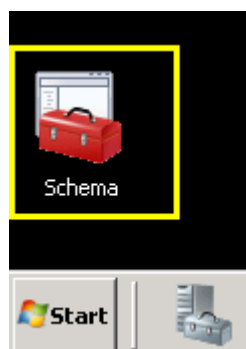


Figure 6 : Double click in Schema shortcut

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

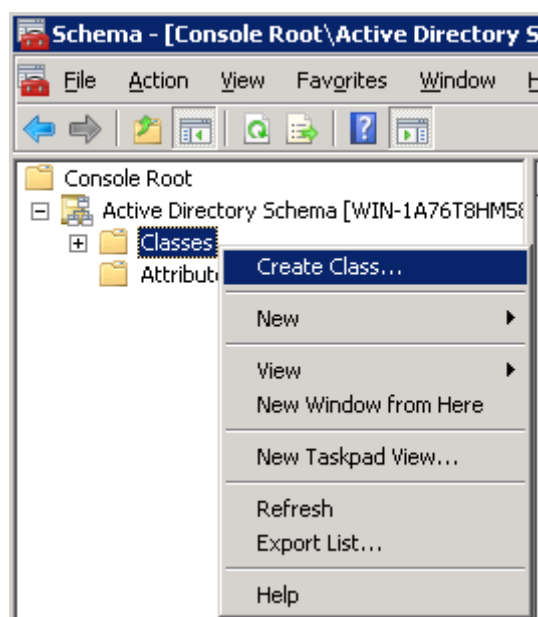
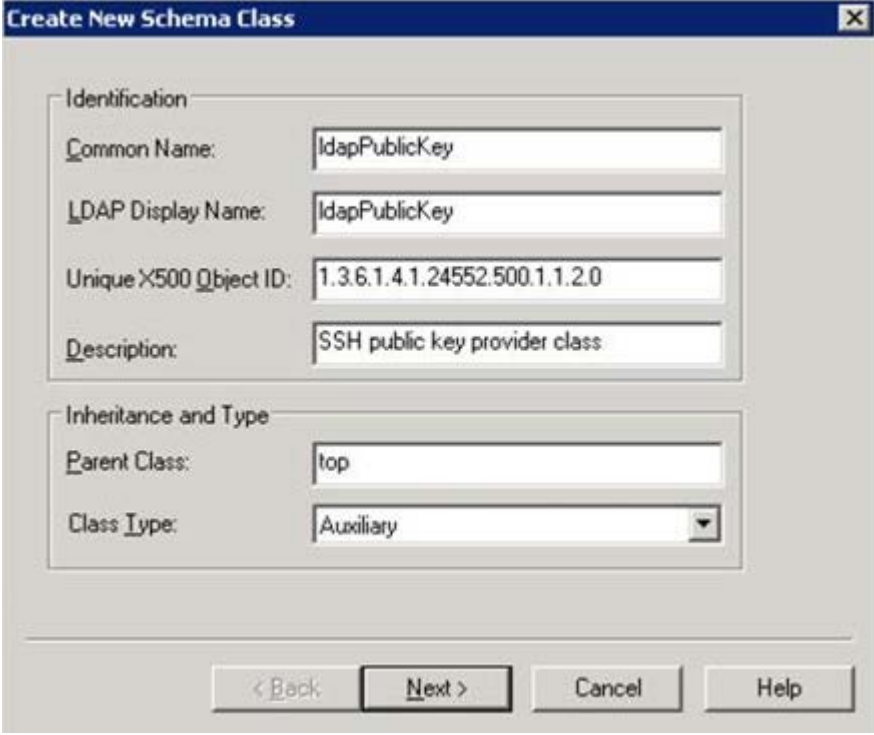


Figure 7 : Create Class

3. Fill the values according to next image





The 'Create New Schema Class' dialog box is shown with the following fields filled:

- 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

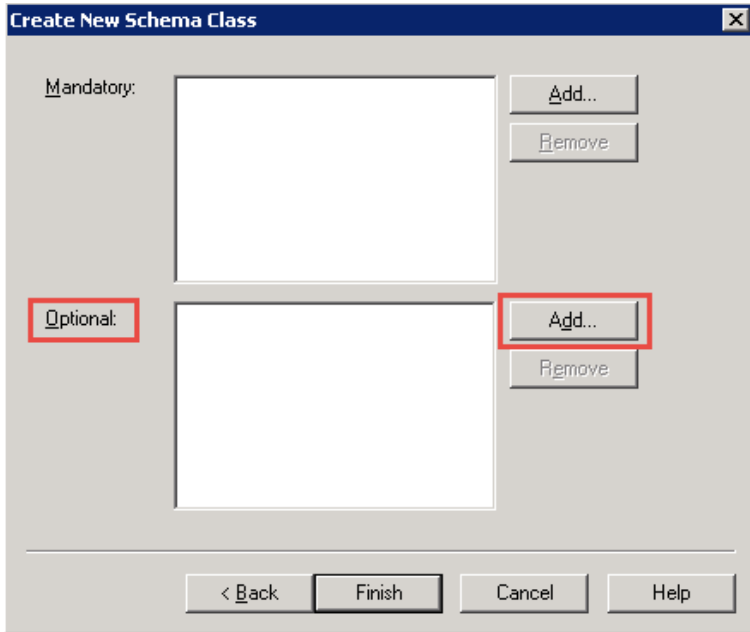
Buttons at the bottom: < Back, Next >, Cancel, Help.

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:



The 'Create New Schema Class' dialog box is shown with the following fields:

- Mandatory:** A large empty text box for mandatory attributes. To its right are 'Add...' and 'Remove' buttons.
- Optional:** A large empty text box for optional attributes. To its right are 'Add...' and 'Remove' buttons. The 'Optional:' label and the 'Add...' button are highlighted with red boxes.

Buttons at the bottom: < Back, Finish, Cancel, Help.

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

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

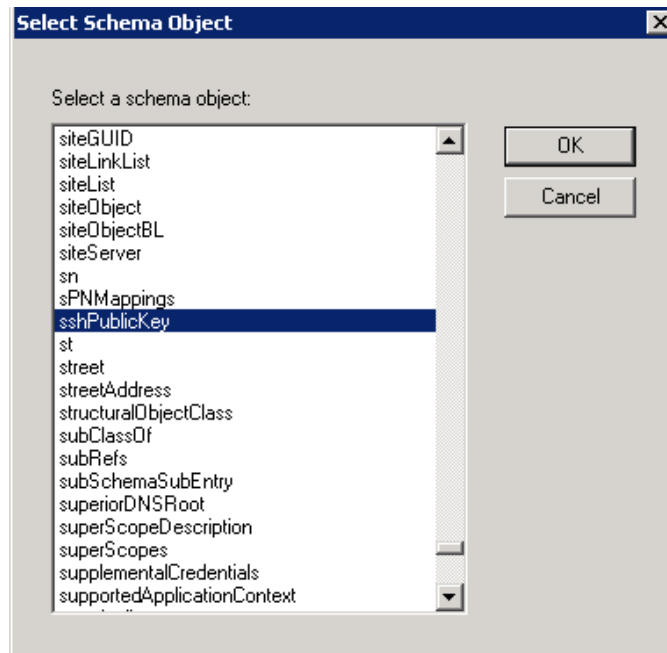


Figure 10 : Adding `sshPublicKey` attribute

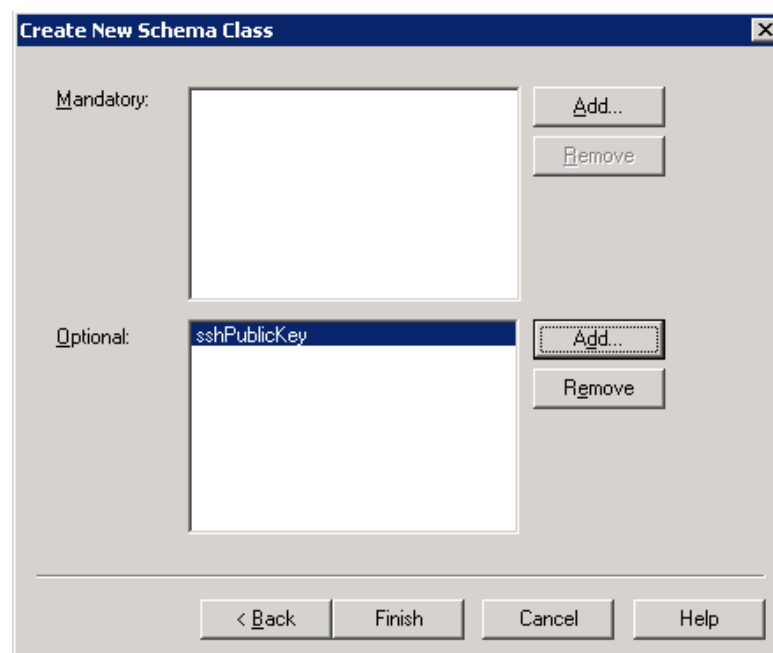


Figure 11 : `sshPublicKey` attribute added.

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

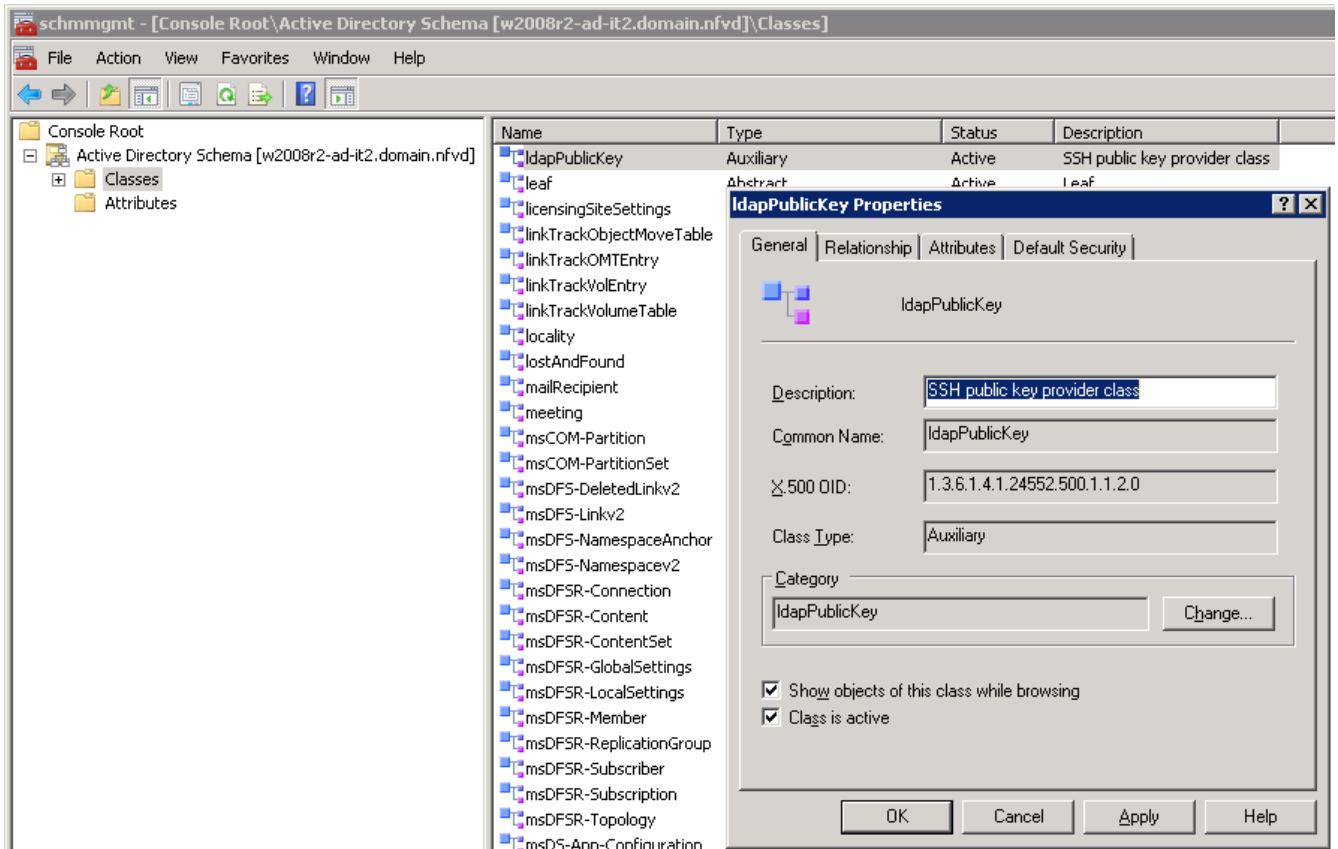


Figure 12 : Schema class ldapPublicKey.

### 1.3.4.2.3 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:

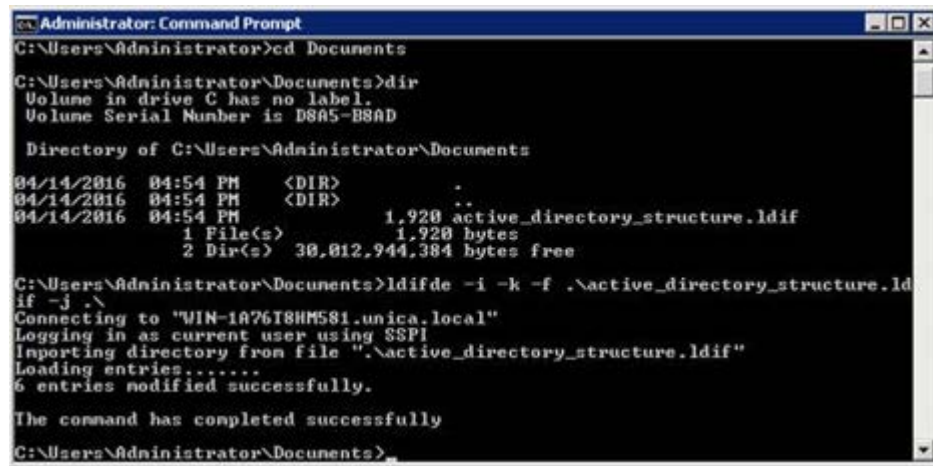


Figure 13 : Configure Active Directory

#### 1.3.4.2.4 Importing private certificate to JBoss VM.

**NOTE:** Import the customer generated private CA certificate in this section.

If the file that contains the customer private 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 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+jCCAeKgAwIBAgIQJfbFmwaf44VPDNYayzzS8zANBgkqhkiG9w0BAQUFADAmMSQwlgYDVQ
QD
ExtXSU4tMUE3NIQ4SE01ODEudW5pY2EubG9jYWwwHhcNMTUxMjlyMTUyMjM5MWhcNMTYxMj
lyMDAw
MDAwWjAmMSQwlgYDVQQDEExtXSU4tMUE3NIQ4SE01ODEudW5pY2EubG9jYWwwggEiMA0GC
SsGSIb3
DQEBAQUAA4IBDwAwggEKAoIBAQDeEiQjZyTKVKKAE8UvTm0HalgMKumm2HnoipfcuErIJ3VBID3
m
42k22QMXHgSW4w+2urZjYztrbGs+d/wEcss7aFSo7/SU7DDI9h4ULgxQ3KSg8ozlg2q93X+oDkN0
AP4muhhw8hmstlVjgrLy2HDBxVe8ruVwaWwCC04ebiOZFKFmdbjfYSJyMQX07tNLkS4jQ88+dT
w
5reqZqfgFu2c45JWN0GBoYz9HTFg7UftWE3i5C5EoKA7qgpWwev/6ZKbbhh7EJfH6Xi300pEqdhB
8Q20x2VCZJ4GAP5/r483XE21sXfKPbgRgeK24XHqHhHonJc9yMsa5m/e/Og/1muMXAgMBAAGjJD
Ai
MAsGA1UdDwQEAWIEMDATBgNVHSUEDDAKBggrBgEFBQcDATANBgkqhkiG9w0BAQUFAAOCAQ
EADmyb
MBQR7+sn0lpcOy4J/jJr4TBMfhxelZ5rjUD3mtGfhCqzVP9xuYycBKPDToVPTi8xW9JZzOWOI8D3
tHBZWRDRciyfYD8uFOc6YotVaWM5Ql410hQ2uxNx6pS0z6+xdccSjjzAbTo3IUSADtm/Vs9YIb3
0HqTS4wgl4rzpBTmLyZiEb891COEO98LWQ28pByyypp2PzIN3te75BIRr2IN70otx57+TsLOuh0P9

```

```

bIBmflBZwCIEHhhD9YzwIHW40HCMf68xav7iYVvelykle+K8hTcbS7OBiQ7x2gXxfai2PsKX9hLf
tNoec5rJtwfFMd3l50WR55T5+scqUeU3nQ==
-----END CERTIFICATE-----
*****

```

### 1.3.4.3 Install LDAP from scratch.

In order to configure the “nfvd” user password we should download all the packages that we are going to need:

1. As “root” user, we will execute the following command:
  - i. `yum -y install openldap openldap-clients openldap-servers`
2. After this we will create a new password , also as root:

```

slappasswd
New password : p@ssw0rd
Re-enter new password : p@ssw0rd
{SSHA}UzXs6I6b8JhK9Xl8jcO/q263jXnk44Vt

```

We should copy the SSHA field, and we will paste the value as the following step describes.

3. Once created the new password we will put our attention in the generated SSHA, we will copy that value and we will configure the new password in the “bdb.ldif” archive, also as root user:

```

cd /etc/openldap/slapd.d/cn\=config
vi olcDatabase\=\{2\}bdb.ldif

cd /etc/openldap/slapd.d/cn\=config
vi olcDatabase\=\{2\}bdb.ldif

olcSuffix: dc=nfvd
olcRootDN: dc=nfvd
olcRootPW: {SSHA}7dRDWUBgt+Xj9jYntIIXq+2HO6UlnAKR

```

4. After the configuration of the “bdb.ldif” we should configure the archive “monitor.ldif”, always as root user.

```

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

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=external,cn=auth" read by
dn.base="dc=nfvd" read by * none

olcAccess: {0}to * by
dn.base="gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth" read by
dn.base="dc=nfvd" read by * none

```

5. After this, we will start the slapd service:

```

[root]# chkconfig slapd on
[root]# service slapd start

```

```
chkconfig slapd on
service slapd start
```

6. We will check the “ldapPublicKey.schema” archive, to check the SSH configuration.

```
cd /tmp
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 )
)
```

7. We will edit the “newSchema.conf” file to include the previously checked “ldapPublicKey.schema”.

```
[root]# vi newSchema.conf

vi newSchema.conf

include /tmp/ldapPublicKey.schema
```

8. Once we have include the file, we will create the folder “conf.d” in order to check the config file previously edited.

```
[root]# mkdir conf.d

mkdir conf.d

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

slaptest -f /tmp/newSchema.conf -F /tmp/conf.d

config file testing succeeded
```

9. Once the testing of the file is succesfull we will check the file “ldapPublickey.ldif”:

```
[root@nfvdvm25 ~]# vi
/tmp/conf.d/cn=config/cn=schema/cn=\{0\}ldapPublickey.ldif

vi /tmp/conf.d/cn=config/cn=schema/cn=\{0\}ldapPublickey.ldif
```

```
# AUTO-GENERATED FILE - DO NOT EDIT!! Use ldapmodify.
# CRC32 39c6db2b
dn: cn=ldapPublicKey,cn=schema,cn=config
objectClass: olcSchemaConfig
cn: ldapPublicKey
olcAttributeTypes: {0}( 1.3.6.1.4.1.24552.500.1.1.1.13 NAME 'sshPublicKey' D
ESC 'MANDATORY: OpenSSH Public key' EQUALITY octetStringMatch SYNTAX 1.3.6.
1.4.1.1466.115.121.1.40 )
olcObjectClasses: {0}( 1.3.6.1.4.1.24552.500.1.1.2.0 NAME 'ldapPublicKey' DE
SC 'MANDATORY: OpenSSH LPK objectclass' SUP top AUXILIARY MAY ( sshPublicKe
y $ uid ) )
```

10. Now, that we have checked it, we will add the configured credentials to the ldap.

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

ldapadd -Y EXTERNAL -H ldapi:/// -f
/tmp/conf.d/cn=config/cn=schema/cn=\{0\}ldapPublicKey.ldif
```

11. After the adding we will edit the file “acme.ldif”, we will make sure that looks as follow.

```
[root@nfvdvm25]# vi acme.ldif

vi acme.ldif

dn: dc=nfvd
objectClass: dcObject
objectClass: organization
dc: nfvd
o : nfvd
```

12. Once the file is checked, and edited if is needed, we will add the file to the ldap

```
[root@nfvdvm25]# ldapadd -x -W -D "dc=nfvd" -f acme.ldif

ldapadd -x -W -D "dc=nfvd" -f acme.ldif
```



The directive “-W” means that a password will be modified, the directive “-D” implies that the file will be bound to the specified “dc”, in this case, “dc=nfvd”, “-f” it will refer to the specific file “acme.ldif”.

13. After we add the file “acme.ldif”, we should edit the file “structure.ldif”, we will check that the file looks like follow:

```
[root@nfvdvm25]# ldapadd -x -W -D "dc=nfvd" -f acme.ldif
```

```
ldapadd -x -W -D "dc=nfvd" -f acme.ldif
```

```
[root@nfvdvm25]# vi structure.ldif
```

```
version: 1
```

```
dn: ou=users,dc=nfvd
```

```
objectClass: top
```

```
objectClass: organizationalUnit
```

```
ou: users
```

```
dn: uid=nfvd,ou=users,dc=nfvd
```

```
objectClass: inetOrgPerson
```

```
objectClass: ldapPublicKey
```

```
objectClass: organizationalPerson
```

```
objectClass: person
```

```
objectClass: top
```

```
cn: name surname
```

```
sn: surname
```

```
businessCategory: domain
```

```
destinationIndicator: nfvd
```

```
givenName: name
```

```
mail: email@hpe.com
```

```
preferredLanguage: en-us
```

```
sshPublicKey:: MTIzNTQ2
```

```
telephoneNumber: 123546
```

```
uid: nfvd
```

```
userPassword:: nfvd
```

```
dn: ou=groups,dc=nfvd
```

```
objectClass: top
```

```
objectClass: organizationalUnit
```

```

ou: groups

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

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

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

```

We will change the “mail: [email@hpe.com](mailto:email@hpe.com)” for a mail address that will serve us to get the info about our nfvd user when it will be created.

14. Once the file “structure.ldif” have been modified we will add it to the ldap.

```

[root@nfvdvm25]# ldapadd -x -W -D "dc=nfvd" -f structure.ldif

ldapadd -x -W -D "dc=nfvd" -f structure.ldif

```

15. Now we will insert some specific lines in the file “module.properties”.

```

cat /opt/uoc2/jboss-eap-
6.4/modules/com/hpe/nfvd/auth/main/conf/module.properties
sed -i 's|nfvd.domain|nfvd|g' /opt/uoc2/jboss-eap-
6.4/modules/com/hpe/nfvd/auth/main/conf/module.properties
cat /opt/uoc2/jboss-eap-
6.4/modules/com/hpe/nfvd/auth/main/conf/module.properties

```

16. After the insertion, we need to restart the “nfvd\_addon\_services”.

```
/opt/uoc2/scripts/nfvd_addon_services restart
/opt/uoc2/scripts/nfvd_addon_services status
```

17. Once restarted, we will make four specific insertions in the “beans.xml” file.

```
sed -i 's|<class>com.hp.spain.nfvd.idm.service.decorator.OMIU|<!--
<class>com.hp.spain.nfvd.idm.service.decorator.OMIU|g'
/opt/HP/jboss/standalone/deployments/nfvd.ear/nfvd-modules-ext-2.0.0-
SNAPSHOT.jar/META-INF/beans.xml

sed -i
's|OMIProfileManagementServiceDecorator</class>|OMIProfileManagementServiceDec
orator</class>-->|g' /opt/HP/jboss/standalone/deployments/nfvd.ear/nfvd-
modules-ext-2.0.0-SNAPSHOT.jar/META-INF/beans.xml

sed -i 's|<alternat|<!--<alternat|g'
/opt/HP/jboss/standalone/deployments/nfvd.ear/nfvd-modules-ext-2.0.0-
SNAPSHOT.jar/META-INF/beans.xml

sed -i 's|</alternatives>|</alternatives>-->|g'
/opt/HP/jboss/standalone/deployments/nfvd.ear/nfvd-modules-ext-2.0.0-
SNAPSHOT.jar/META-INF/beans.xml

cat /opt/HP/jboss/standalone/deployments/nfvd.ear/nfvd-modules-ext-2.0.0-
SNAPSHOT.jar/META-INF/beans.xml
```

18. After the insertion we will edit the “standalone.xml”, in the path “/opt/uoc2/jboss-eap-6.4/standalone/configuration/standalone.xml”

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

```
<config-property name="validationDN">
    DC=nfvd,DC=domain
</config-property>
<config-property name="securityCredentials">
    secret
</config-property>
```

We will assure that the “securityCredentials” has the value “secret”.

19. Once the file has been edited we will restart the LDAP services

```
service slapd restart
```

## Chapter 2 Installing/Upgrading NFVD

### 2.1 Installing a new platform

This section only applies to an installation from scratch.

If you want to upgrade from a previous version, please refer to section 2.2 “Upgrading an existing platform” below

---

**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-04.01.001-1.el6.noarch.rpm file and install it:

```
# rpm -ivh nfvd-installer-04.02.000-1.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).

If platform to be installed is:

- either a simplex (non-HA) platform,
- or a primary platform of a HA configuration (refer to HA Solution Guide for more details):

execute the following command:

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

If platform to be installed is:

- or a secondary platform of a HA configuration (refer to HA Solution Guide for more details):

execute the following command:

```
# /opt/HPE/nfvd/install/nfvd-install.sh -s /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 2.1.1 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 execute steps described in Chapter 3 “Post-installation steps”.

#### 2.1.1 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_ansi/group_vars/all` file, contact NFVD Team.

## 2.1.2 Special case of HA platform installation.

There are many prerequisites for HA installation. Please consult “*NFVD High Availability Solution Guide*”

## 2.2 Upgrading an existing platform

This section describes the procedure to upgrade from a previous version of NFVD (4.0.0 or 4.1 or 4.1.1 or 4.1.2) to 4.2.

---

**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-04.02.000-1.el6.noarch.rpm` file and install it:

```
# rpm -Uvh --force nfvd-installer-04.02.000-1.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`).

If the currently installed version has no customized Definitions or Components, please execute the following command:

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

If the currently installed version was customized with some specific Definitions or Components, please execute the following command:

```
# /opt/HPE/nfvd/install/nfvd-install.sh -c <custom_files_dir> /kits/archives
```

Where

<custom\_files\_dir> is a directory containing customized files (Components, Definitions, Instances) replacing files from the kits. The directory content must match the same structure as in /opt/OV/ServiceActivator/solutions/NFVModel/etc/LoadXML

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).

All questions already asked by a previous installation will be automatically filled.

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

At this point, if you choose 'y', then the installer will continue with the upgrade

As soon as the installation is complete (it usually takes around 25 minutes), you are done!

You don't have to consider any step related to license installation (previous licenses are still valid) or post installation.

## 2.3 Installation tools Overview

There are two main installation tools, the install script and the reconfigure script.

The install script allows installation and upgrade of platforms in both Simplex and Ha mode.

```
# /opt/HPE/nfvd/install/nfvd-install.sh -h
Installer/Upgrader tool for NFVD
Usage:
  nfvd-install.sh [options] <kit_directory>

options:
  -p          : Install or Upgrade a primary platform (for HA configurations)
  -s          : Install or Upgrade a secondary platform (for HA configurations)
  -c <custom_files_dir> : Directory containing customized files (Components, Definitions,
Instances)
                                replacing files from the kits. The directory content must match the
                                structure in /opt/OV/ServiceActivator/solutions/NFVModel/etc/LoadXML/
  -m <module_name>    : Specific module(s) to install. Module name is one of : FF AA UI
sitescope
                                Multiple values allowed (e.g.: -m FF -m UI)
                                All modules will be installed by default when none are specified.
  -v          : Run IVP
  -u          : Upgrade mode only
  -n          : Skip checking of prerequisites
  -h          : Displays this usage message
  -r          : Force resuming previous installation
  -f          : Force a new installation
```

The reconfigure tool allows reconfiguration of IP addresses and setup of VIP addresses for HA

```
# /opt/HPE/nfvd/install/nfvd-reconfigure.sh -h
IP addresses "reconfigurator" for NFVD
Usage:
  nfvd-reconfigure.sh [options]

options:
  -s          : Reconfigure IPs of a secondary platform (for HA configurations)
  -p          : Reconfigure IPs of a primary platform (for HA configurations)
```

-h	: Displays this usage message
-r	: Force resuming previous configuration
-n	: Skip checking of prerequisites
-l	: Skip landscape reloading
-f	: Skip fulfillment ha setting

## 2.4 Troubleshooting Installation/Upgrade

---



---

**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 explicitly 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*



## Chapter 3 Post-installation steps

You can directly go to “3.6 Verifying NFVD installation” if you are upgrading from a previous version.

### 3.1 Install Commercial licenses

Refer to NFV Director Administration Guide, “NFVD Base Product licenses”.

### 3.2 Integrating SiteScope with Assurance Gateway to enable KPI metrics collection

**On:** <AA\_HOST>

**Login:** root

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

In order to enable KPI data collection from SiteScope, perform the following steps.

```
# 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 <agw_url> -tagname <tagname>
```

**Typical example:**

```
# cd /opt/HPE/nfvd/templates/bin/

# If Assurance Gateway in HTTP mode
# ./dataintegration_tool_sitescope.sh -lwssopath /var/opt/HPE/nfvd/conf/lwssofmconf.xml -
host <SIS_HOST> -port 18888 -uname admin -pass admin -dname DefaultSis-AGW-INTG -url
http://<AA_HOST>:18080/nfvd/kpimetrics -tagname NFVD

# If Assurance Gateway in HTTPS mode
# ./dataintegration_tool_sitescope.sh -lwssopath /var/opt/HPE/nfvd/conf/lwssofmconf.xml -
host <SIS_HOST> -port 18888 -uname admin -pass admin -dname DefaultSis-AGW-INTG -url
https://<AA_HOST>:18443/nfvd/kpimetrics -tagname NFVD
```


**Note:** reportInterval is a parameter that can be passed to dataintegration\_tool\_sitescope.sh, by default it is set to 60 seconds. SiteScope posts KPI data to Assurance which is exported to csv file and stored in neo4j. The frequency of the data to be posted is based on the reportInterval value. It is recommended to set the value of reportInterval to the monitor frequency which is having a least value.

Eg: Assume we have 3 monitors with monitor frequency 300,600,250 seconds. It is recommended to set the reportInterval to 250 seconds.

Once the above tool is executed successfully, the same can be verified or updated in SiteScope portal.

- Click on Preferences > Integration Preferences.

- A record by name '<diname>' will be created. Open the same.

 Edit Data Integration Preferences

### General Settings

\* Name: DefaultSis-AGW-INTG

Description:

### Data Integration Preferences Settings

\* Receiver URL:

Encoding:

\* Reporting interval (seconds):

Time synchronization interval (minutes):

☐ GZIP compression

☐ Include additional data

☐ Error on redirect

\* Request timeout (seconds):

\* Connection timeout (seconds):

Number of retries:

☐ Authentication when requested

☐ Disable integration

### Web Server Security Settings

### Proxy Server Settings

### Reporting Tags

Use SiteScope tags to define the data that is reported in the integration. Select or add a tag to identify groups and monitors whose data is forwarded to the receiving application. (Ensure that this tag is also selected for the relevant groups or monitors.)

[Add Tag](#)

You can manage existing tags from Preferences > Search/Filter Tags.

- ☐ DATACENTER
- ☐ Monitor Deployment Wizard
- ☐ NETWORK\_SERVICE
- ☒ NFVD
- ☐ SELF\_MONITOR

Figure 14 : SiteScope Data Integration Preferences

### 3.3 Configure the NFVD API to support https.

In this section we will expose how to configure the typical installation of NFV-Director solution to support https protocol, the configuration should take place in the machine where the solution is installed, in case the different functional parts of the solution were installed in more than one machine, this configuration should take place in the FullFillment machine.

We assume as starting point that:

- The user is using Red Hat 6.6.
- The user already have a certificate to use.
- The user already have a key to use.

The configuration steps are :

The user will locate the file “standalone.xml” in the following path:

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

Once we have the file located, we will edit the file adding the following line:

```
<connector name="ajp" protocol="AJP/1.3" scheme="http" socket-binding="ajp"/>
```

Just under the line: <connector name="http" protocol="HTTP/1.1" scheme="http" socket-binding="http"/>

After we finish the edition of the file, we will save the file, and continue with the following steps:

- The user will restart the JBoss service using the following command:

```
service activator start
```

- Install apache server and mod\_ssl using the command below:

```
Yum install httpd mod_ssl
```

- Place the certificate in the directory: /etc/pki/tls/certs and the key in the folder: /etc/pki/tls/private directories
- Go to /etc/httpd/conf.d/ssl.conf and comment all the lines that are not commented between :

```
"<VirtualHost _default_:443>"
.....
"</VirtualHost>"
```

Now we need to create a new file in the path : /etc/httpd/conf.d with following content, you should replace the text with <> with your own values, the key is assumed not to contain a passphrase.

```
<VirtualHost *:80>
  ServerName <Your server name>

  RewriteEngine On
  RewriteCond %{HTTPS} off
  RewriteRule ^ https://%{Your HTTP_HOST}%{Your REQUEST_URI}
</VirtualHost>

<VirtualHost *:443>
  SSLEngine on
  SSLProtocol all -SSLv2 -SSLv3

  ServerName <Your server name>
  SSLCertificateFile /etc/pki/tls/certs/<Your certificate>
  SSLCertificateKeyFile /etc/pki/tls/private/<Your Key>
  SSLCipherSuite DEFAULT:!EXP:!SSLv2:!DES:!IDEA:!SEED:+3DES

  ProxyRequests Off
  ProxyPreserveHost On

  ErrorLog /var/log/httpd/nfvd_error.log
  CustomLog /var/log/httpd/nfvd.log combined
```

```
<Proxy *>
    Order deny,allow
    Allow from all
</Proxy>

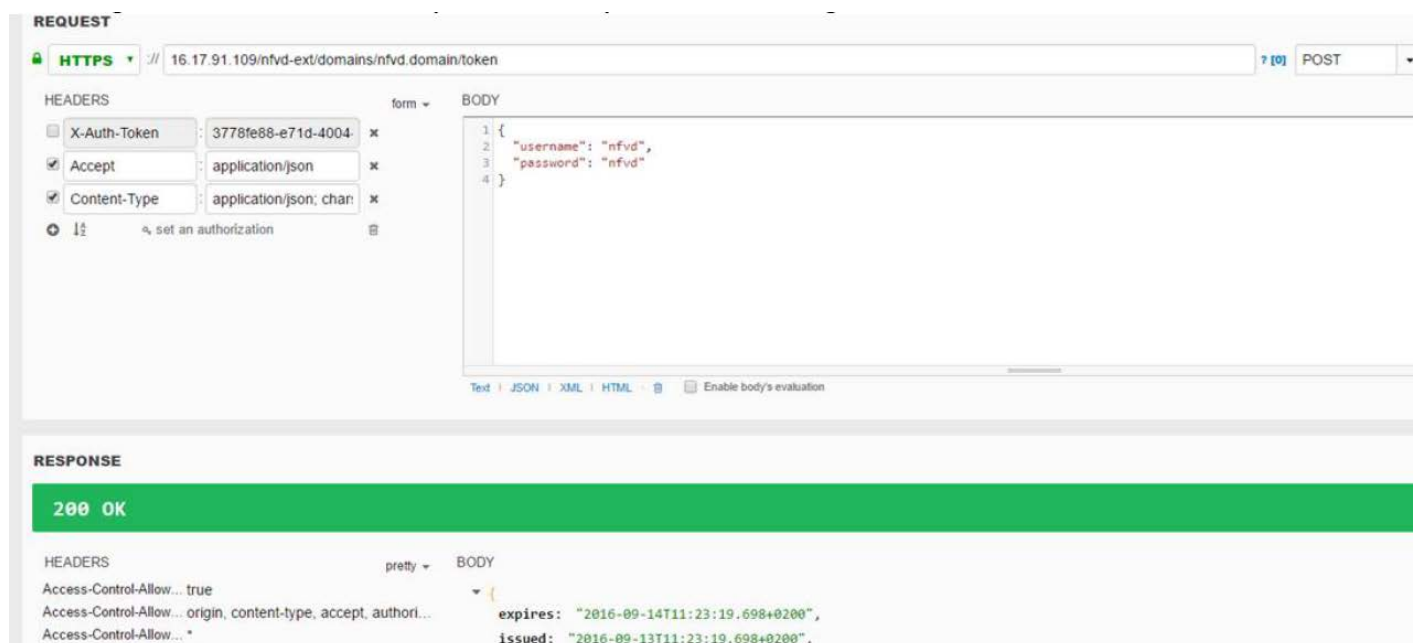
ProxyPass / ajp://localhost:8009/
ProxyPassReverse / ajp://localhost:8009/
</VirtualHost>
```

Once we have created and stored the file we will restart our Apache server:

```
service httpd restart
```

Once this configuration is finished, you should be able to do requests to:  
[https://<your\\_server\\_ip>/nfvd\(-ext\).](https://<your_server_ip>/nfvd(-ext).)

The image below shows an example of this request over a configured machine:



### 3.4 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 1.3.4.2.4 "Importing private 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+jCCAeKgAwIBAgIQfbFmwaf44VPDNYayzS8zANBgkqhkiG9w0BAQUFADAmMSQwlgYDVQ
QD
ExtXSU4tMUE3NIQ4SE01ODEudW5pY2EubG9jYWwwHhcNMTUxMjlyMTUyMjM5WWhcNMTYxMj
lyMDAw
MDAwWjAmMSQwlgYDVQDEExtXSU4tMUE3NIQ4SE01ODEudW5pY2EubG9jYWwwggEiMA0GC
SgGSlb3
DQEBAQUAA4IBDwAwggEKAoIBAQDeEiQJZYtkVKKAE8UvTm0HalgMKumm2HnoipfcuErIJ3VBID3
m
42k22QMXHgSW4w+2urZjYZtrbGs+d/wEc5s7aFSo7/SU7DDI9h4ULgxQ3KSg8ozlg2q93X+oDkN0
AP4muhhw8hmstlvjgrLy2HDBxVe8ruVwaWwCC04ebIOZFKFmdbjfySJyMQX07tNLkS4jQ88+dT
w
5reqZqfgFu2c45JWNOGBoYz9HTFg7UftWE3i5C5EoKA7qgpWwev/6ZKbbhh7EJfH6Xi300pEqdhB
8Q20x2VCZJ4GAP5/r483XE21sXfKPbgRgeK24XHQHhHonJc9yMsa5m/e/Og/1muMXAgMBAAGjJD
Ai
MAsGA1UdDwQEAwIEMDATBgNVHSUEDDAKBggrBgEFBQCcDATANBgkqhkiG9w0BAQUFAAOCAQ
EADmyb
MBQR7+sn0lpcOy4J/jJr4TBMfhxeIZ5rjUD3mtGfhCqzVP9xuYycBKPDToVPTi8xW9JZzOWOI8D3
tHBZWRDRciyfyD8uFOc6YotVaWM5Ql410hQ2uxNx6pS0z6+xdccSjjzAbTo3lUSADtm/Vsv9YIb3
OHqTS4wgl4rzpBTmLyZiEb891COEO98LWQ28pByyyp2PzIN3te75BlRr2IN70otx57+TsLOuh0P9
bIBmflBZwCIEHhD9YzwlHW40HCMf68xav7iYVvelykle+K8hTcbS70BiQ7x2gXxfai2PsKX9hLf
tNoec5rJtwfFMd3l50WR55T5+scqUeU3nQ==
-----END CERTIFICATE-----
*****
```

- Stop and restart Fulfillment host.

**Note:** Refer to NFV Director Administration Guide “*Administering NFVD*” for full description of steps to start, stop and check status of NFVD components.

## 3.5 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/HPE/nfvd/bin/nfvd_createUser.sh -d <NFVD_DOMAIN_NAME> -e
<NFVD_DOMAIN_USER_EMAIL> <NFVD_DOMAIN_USER>

Typical Example:

# /opt/HPE/nfvd/bin/nfvd_createUser.sh -d nfvd.domain -e localuser@localhost.localdomain
nfvd
```

## 3.6 Verifying NFVD installation

### 3.6.1 Access from NFVD GUI

---

[http://<GUI\\_HOST>:3000/login](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!)

---

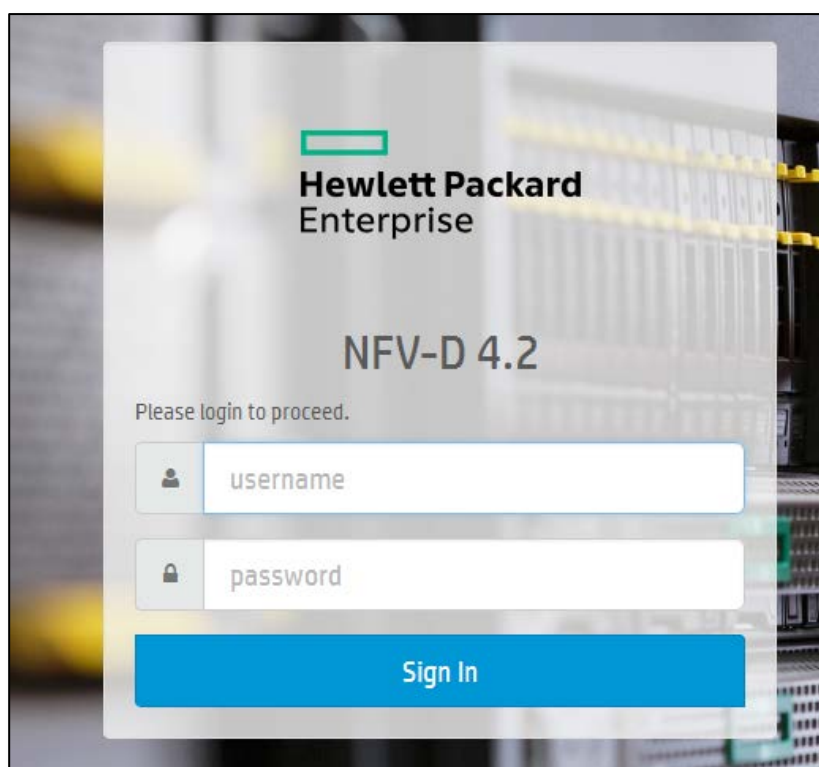


Figure 15 : UI portal

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

### 3.6.2 Verifying objects synchronization of NFVD

---

[http://<AA\\_HOST>:7474/webadmin](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.

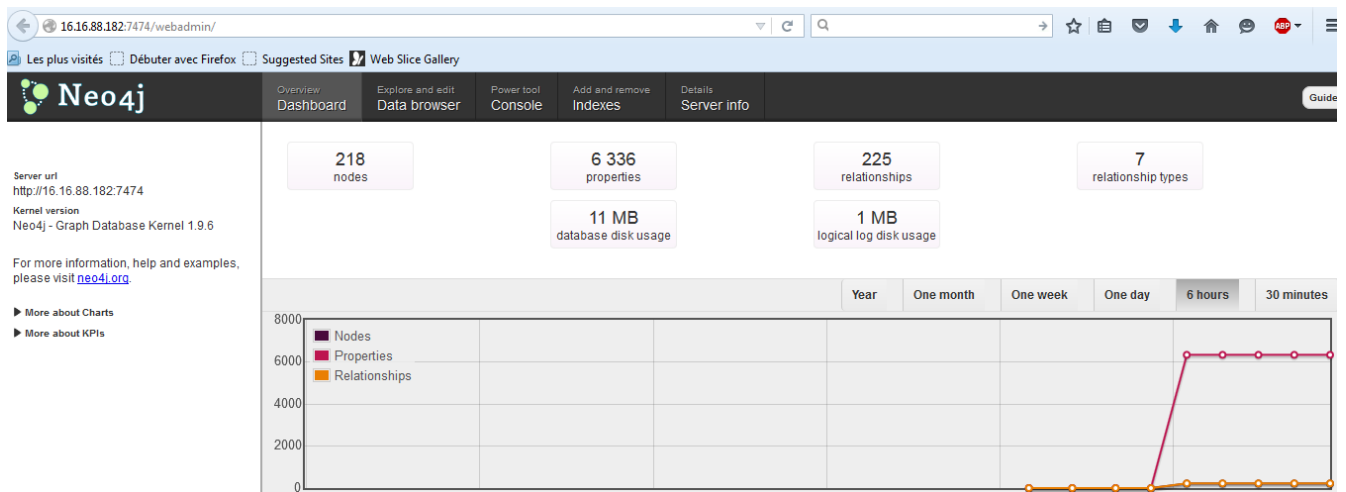


Figure 16 : Neo4J after synchronization

If this last checking is OK, then:

**CONGRATULATIONS, YOU HAVE SUCCESSFULLY INSTALLED AND CONFIGURED NFVD !!!**

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

Typical next step is to integrate NFVD with an infrastructure/VIM (refer to “VIM Integration Guide” document for more details).



## Chapter 4 NFVD Deployment set ups

---

NFV Director can be deployed in several ways where 4 main deployment flavors are the standard ones:

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

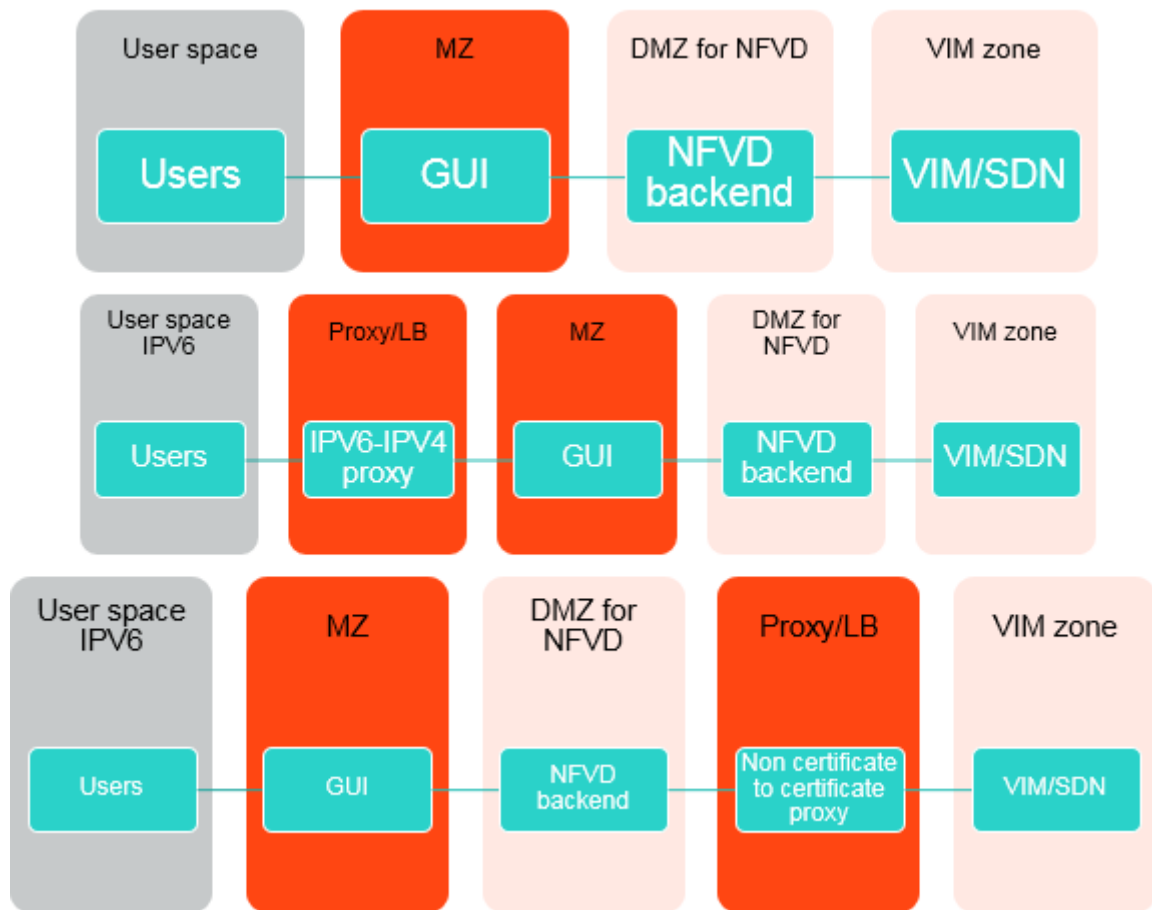


Figure 17 Possible set up for the deployment.

The image below describe the standard deployment set up for NFVD.

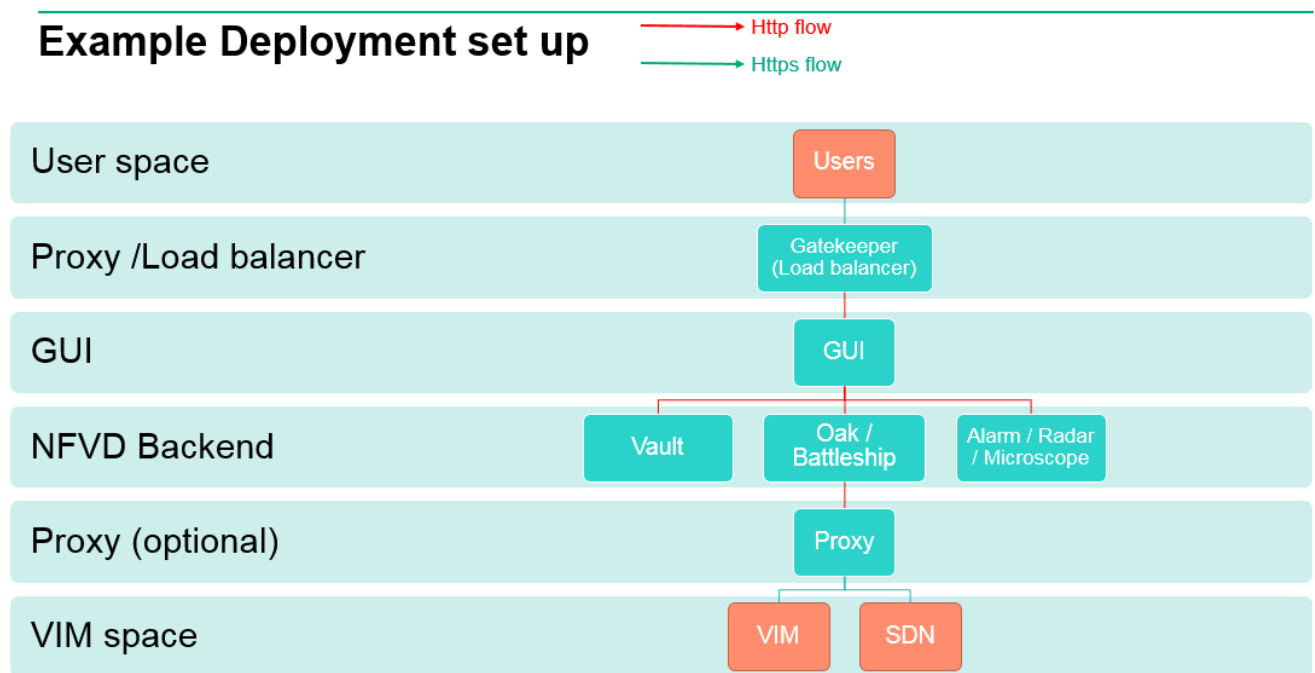


Figure 18 Level schema of the NFVD deployment.

## 4.1 NFV Director Deployment flavors.

The Flavors of the NFV Director are:

### NFV Director Deployment flavors

Demo Flavor	Simplex Flavor	Duplex Flavor	GR Flavor
<ul style="list-style-type: none"> <li>• For demos</li> <li>• 2 VMs</li> </ul>	<ul style="list-style-type: none"> <li>• Starting set up</li> <li>• 4 VMs</li> </ul>	<ul style="list-style-type: none"> <li>• Recommended for production</li> <li>• 8 VMs</li> <li>• 1 LB</li> <li>• 1 External NFS storage</li> </ul>	<ul style="list-style-type: none"> <li>• Recommended for 2 sites redundancy</li> <li>• 2 sites</li> <li>• In each site               <ul style="list-style-type: none"> <li>• 8 VMs</li> <li>• 1 LB</li> <li>• 1 External NFS storage</li> </ul> </li> <li>• GTM (global LB)</li> <li>• Golden Gate replication</li> <li>• NFVD GR package</li> </ul>

Figure 19 NFV Director Deployment Flavors.

### 4.1.1 NFVD VM View Simplex Flavor

#### NFVD VM View Simplex flavor

GUI VM	Fulfillment VM	Assurance VM	DB VM
<ul style="list-style-type: none"> <li>• GUI module</li> </ul>	<ul style="list-style-type: none"> <li>• API Module</li> <li>• Fulfillment Module</li> </ul>	<ul style="list-style-type: none"> <li>• Discovery Module</li> <li>• Monitor Module</li> <li>• Alarm Module</li> </ul>	<ul style="list-style-type: none"> <li>• DB (oracle / postgresql) module</li> <li>• LDAP (openldap or active directory) module</li> </ul>

Figure 20– Simplex Flavor.

For production is recommended to use a duplex flavor with full HA capabilities:

- 2x GUI VM in HA including
  - GUI module
- 2x Fulfillment VM in HA including
  - API Module
  - Fulfillment Module
- 2x Assurance VM in HA including
  - Discovery Module
  - Monitor Module
  - Alarm Module
- 2x DB VM in HA including
  - DB (oracle / postgresql) module
  - LDAP (openldap or active directory) module
- 1x Load balancer (can be a VM with apache proxy or F5)
  - Health service module
- 1x external NFS storage

## 4.1.2 NFVD VM View Duplex Flavor

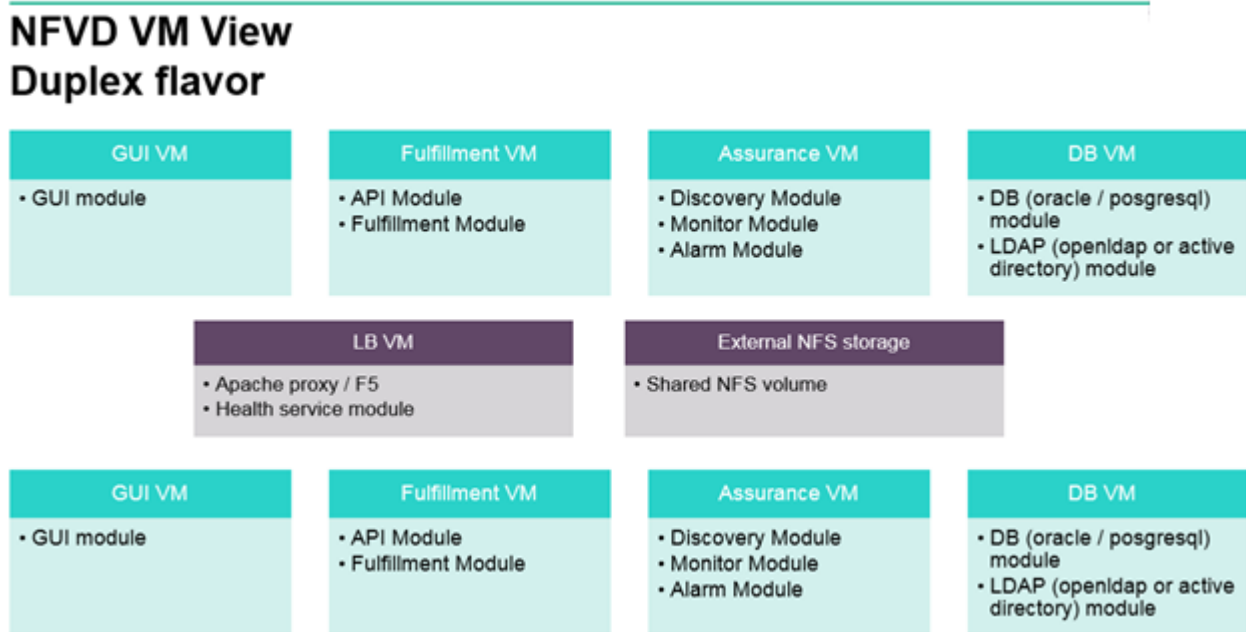


Figure 21– Duplex Flavor.

For long distance Geo redundancy a more advance set up is need and it is recommended to use to full duplex installations with Global load balancing of the traffic

- Each site with
  - 2x GUI VM in HA including
    - GUI module
  - 2x Fulfillment VM in HA including
    - API Module
    - Fulfillment Module
  - 2x Assurance VM in HA including
    - Discovery Module
    - Monitor Module
    - Alarm Module
  - 2x DB VM in HA including
    - DB (oracle RAC) module
    - LDAP (openldap or active directory) module
    - Oracle Golden Gate replication
  - 2x Load balancer (can be a VM with apache proxy or F5)
    - Health service module
  - 1x external NFS storage
  - 2x Global site Load balancers (can be a VM with apache proxy or F5)

### 4.1.3 NFVD VM View GR, duplex and duplex flavor Flavor

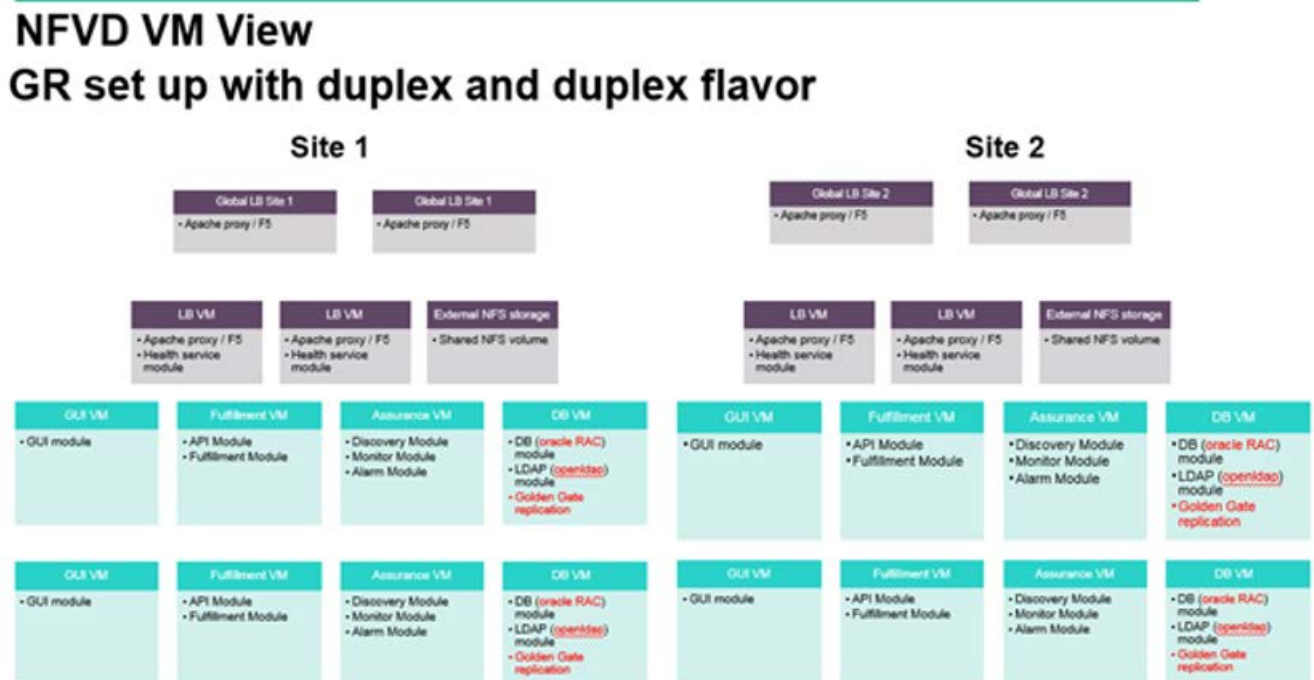


Figure 22 Legion – GR, duplex & duplex Flavor.

It is of course possible to collocate any of those modules (even the level of one VM) but that is NOT recommended for any production set up without proper Technical sizing and assessment

Typical demo set up due to simplicity is composed by two VMs using minimal set up and even non commercial options (as oracle XE)

oracle XE can run well for small demos but it has the well documented by oracle performance and scalability limitations so do not expect high performance with oracle XE.

#### 4.1.4 NFVD VM View Demo Flavor

##### NFVD VM View

##### Demo flavor

FF Demo VM	AA Demo VM
<ul style="list-style-type: none"><li>• GUI module</li><li>• API Module</li><li>• Fulfillment Module</li><li>• DB (<u>oracle</u> /<u>Oracle XE</u> / <u>posgresql</u>) module</li><li>• LDAP (<u>openldap</u>) module</li></ul>	<ul style="list-style-type: none"><li>• Discovery Module</li><li>• Monitor Module</li><li>• Alarm Module</li></ul>

Figure 23 Demo Flavor.

## Annex 1: NFVD Module View

NFV Director is composed of several Modules (each module providing one or more services):

### NFV Director modules and services

NFV Director provides a set of services that are bundled in different SW modules

NFV Director provides 8 SW modules that can be installed in different deployment flavors

NFV Director provides 18 services that communicate within each other to provide orchestration capabilities

GUI Module	API Module	Fulfillment Module	Monitor Module	Alarm module	Discovery Module	Platform Health	Storage Module
<ul style="list-style-type: none"> <li>• Visualization service</li> <li>• Image service</li> </ul>	<ul style="list-style-type: none"> <li>• Authorization service</li> <li>• LCM Service</li> <li>• Inventory service</li> <li>• Tracking service</li> </ul>	<ul style="list-style-type: none"> <li>• Orchestration service</li> <li>• SDN engine service</li> <li>• VNFM engine service</li> </ul>	<ul style="list-style-type: none"> <li>• Monitoring service</li> </ul>	<ul style="list-style-type: none"> <li>• Gateway service</li> <li>• Correlation Service</li> <li>• Data export service</li> </ul>	<ul style="list-style-type: none"> <li>• Discovery service</li> </ul>	<ul style="list-style-type: none"> <li>• Load balancing service</li> <li>• Health check</li> </ul>	<ul style="list-style-type: none"> <li>• DB storage service</li> <li>• LDAP authentication service</li> <li>• NFS storage</li> </ul>

Figure 24 NFV Director Modules and services

- GUI Module
  - Providing:
    - Visualization service
    - Image Service
- API Module
  - Providing
    - Authorization Service
    - Inventory Service
    - Catalog Service
    - NFVD entities Service
    - Orchestration LCM Service
    - Tracking service
- Fulfilment Module
  - Providing
    - Orchestration engine service
    - VNFM engine service
    - SDN engine service
- Discovery Module
  - Providing
    - Openstack discovery service
    - Vcenter discovery service



- Monitor Module
  - Providing
    - Monitoring service
- Alarm Module
  - Providing
    - Gateway Service
    - Correlation engine service
    - Data export service
- Platform Health Module (only for HA and GR installations)
  - Providing
    - NFV Director site health service

And make use of some 3rparty modules

- DB (oracle / postgresql) module
  - Providing
    - Data storage service
- LDAP (openldap or active directory) module
  - Providing
    - Authentication service
- Load balancer for HA and GR (in HA and GR installations)
  - Providing
    - Load balancing capabilities.

## Annex 1.1: NFV Service View.

---

It is recommended to install those modules in separate Virtual machines and review you security needs to proper configure each module

Simplex Flavor deployment of NFVD for an initial set up or complex demos/POC is composed of 4 virtual machines

- GUI VM including
  - GUI module
- Fulfillment VM including
  - API Module
  - Fulfillment Module
- Assurance VM including
  - Discovery Module
  - Monitor Module
  - Alarm Module

- DB VM including
  - DB (oracle / postgresql) module
  - LDAP (openldap or active directory) module.

## NFVD Service View

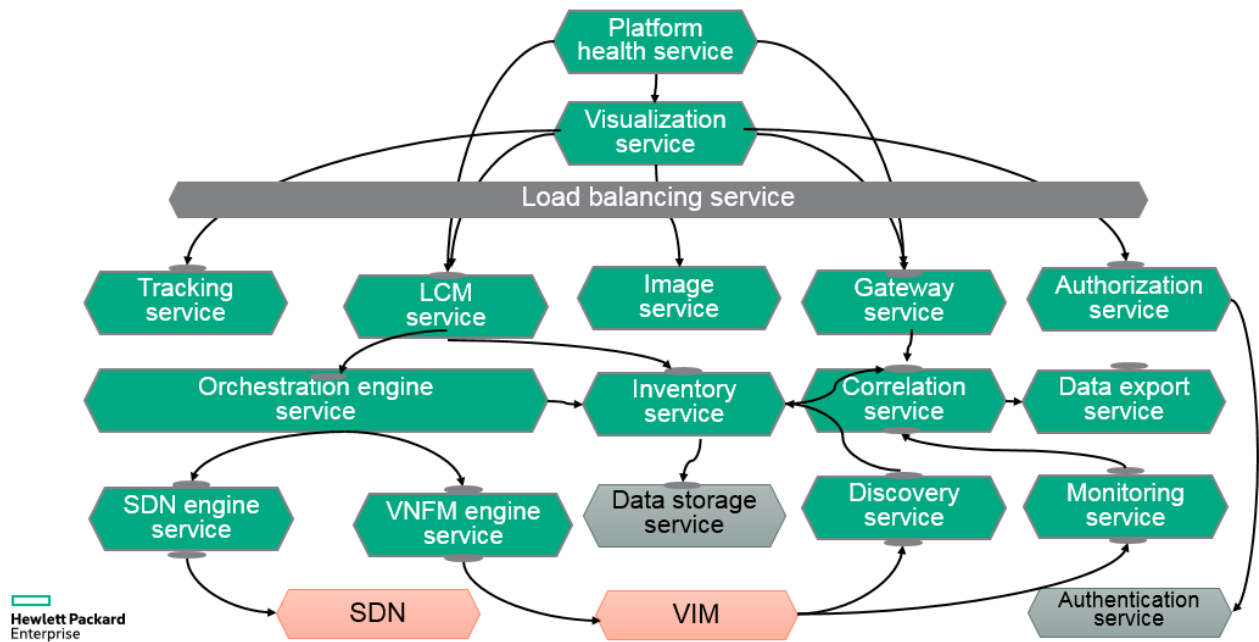


Figure 25 NFVD Service View

## Annex 1.2: NFV Module View.

### NFVD Module View

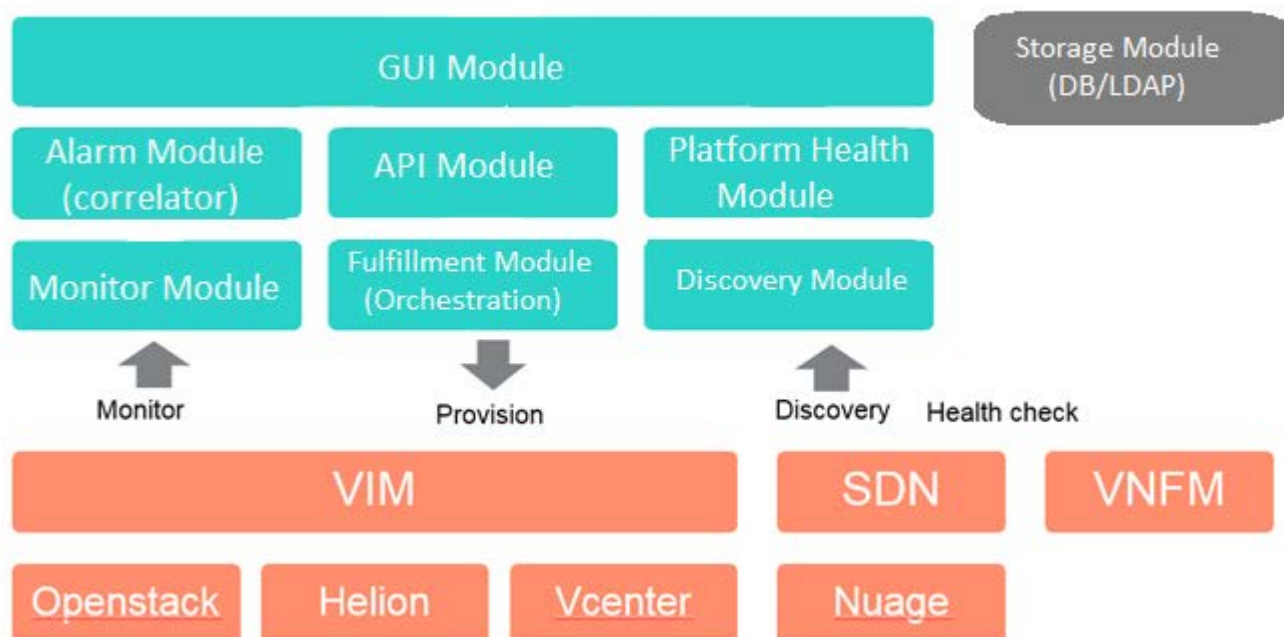


Figure 26 NFVD Module View

## Annex 1.3: NFVD Funtional architecture compared to Openstack

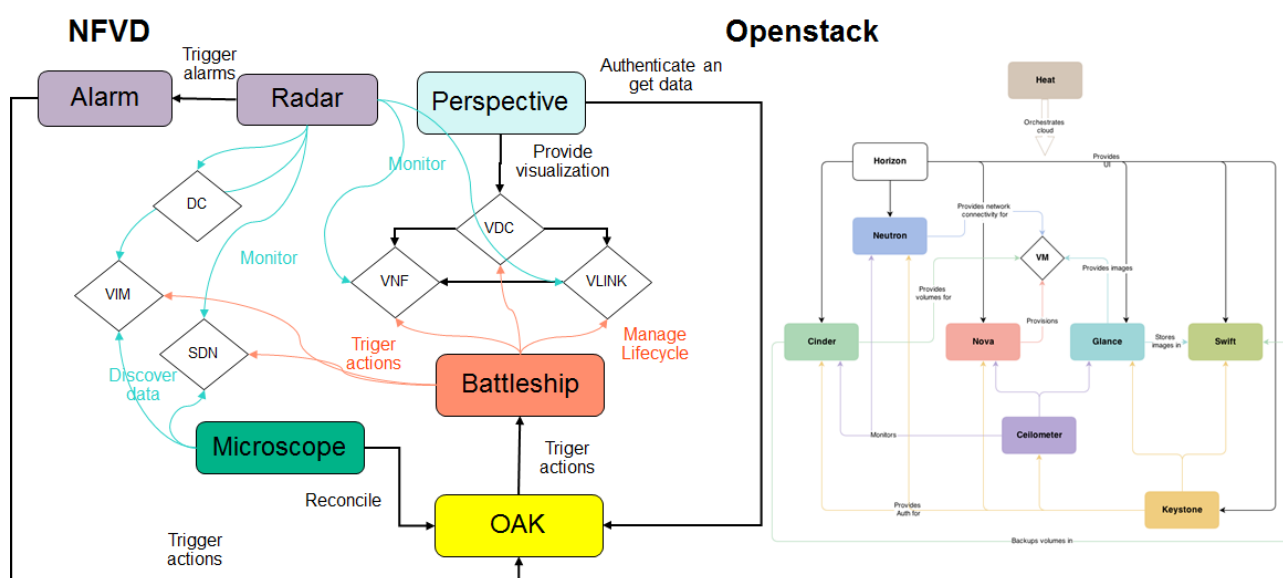


Figure 27 NFVD Architecture VS Openstack Architecture

## Annex 2: Subscribing to HPE Security Bulletins

### Procedure for Subscribing to Security Bulletins

1. Open a browser to go to the HPE Updates page  
[http://www.hpe.com/support/Subscriber\\_Choice](http://www.hpe.com/support/Subscriber_Choice)
2. Do one of the following:
  - Sign in if you are a registered customer.
  - Enter your email address to sign-up now.
3. Select the following fields
  - Product Category: Enterprise Software
  - Product Family: CMS SW Products
  - Select the product – HP Network Function Virtualization Director Software Series
  - Click Subscribe

### Products

Simple search SAID

Choose a product category

Enterprise Software

or search



Choose a product family

CMS SW Products

Select your products (Hold down the CTRL key and click to make multiple selections OR hold down the Shift key and click to select an entire list.)

HP Network Application Software Series  
 HP Network Application Term Software Series  
**HP Network Function Virtualization Director Software Series**  
 HP Network Node Management Software Series  
 HP Open Mediation Software Series  
 HP OpenCall Convergent Communication Platform Software Series  
 HP OpenCall Media Platform Software Series  
 HP OpenView OSI Transport Services Software Series

**Add selected products**

Figure 28: HPE Security Bulletins

## Annex 3: Generating a self-signed certificate for LDAP

**NOTE:** This section provides an illustration on how to generate a self-signed certificate for LDAP. It is recommended to use the customer provided private certificate, and not the self-signed certificate.

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...

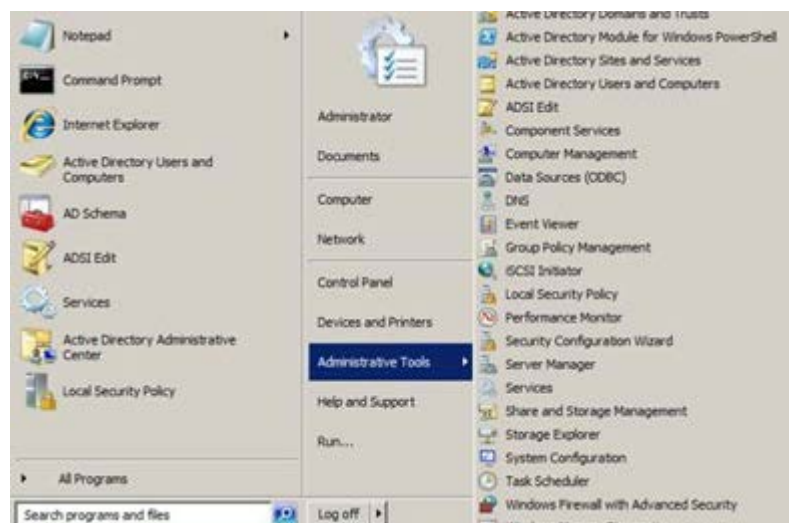


Figure 29 : Generating self-signed certificate for LDAP

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



Figure 30 : Add Roles Wizard, server roles

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

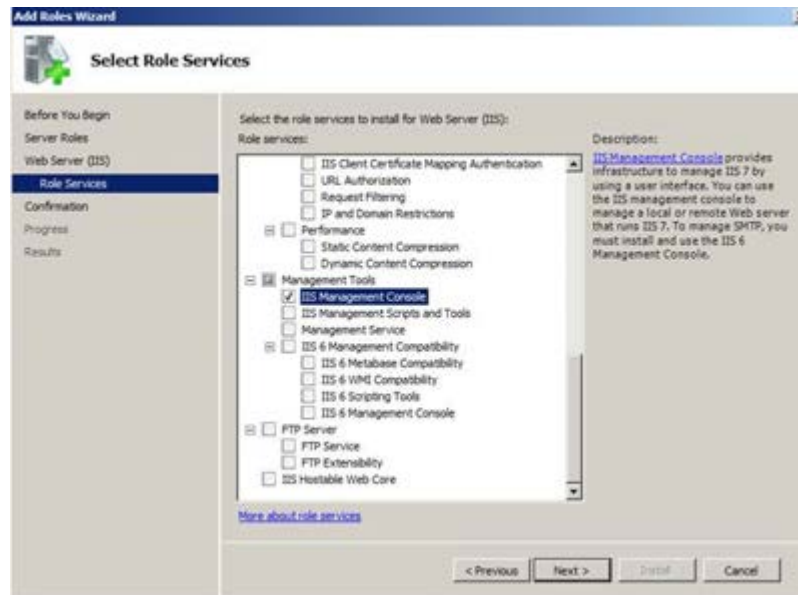


Figure 31 : Add Roles Wizard, role services

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:

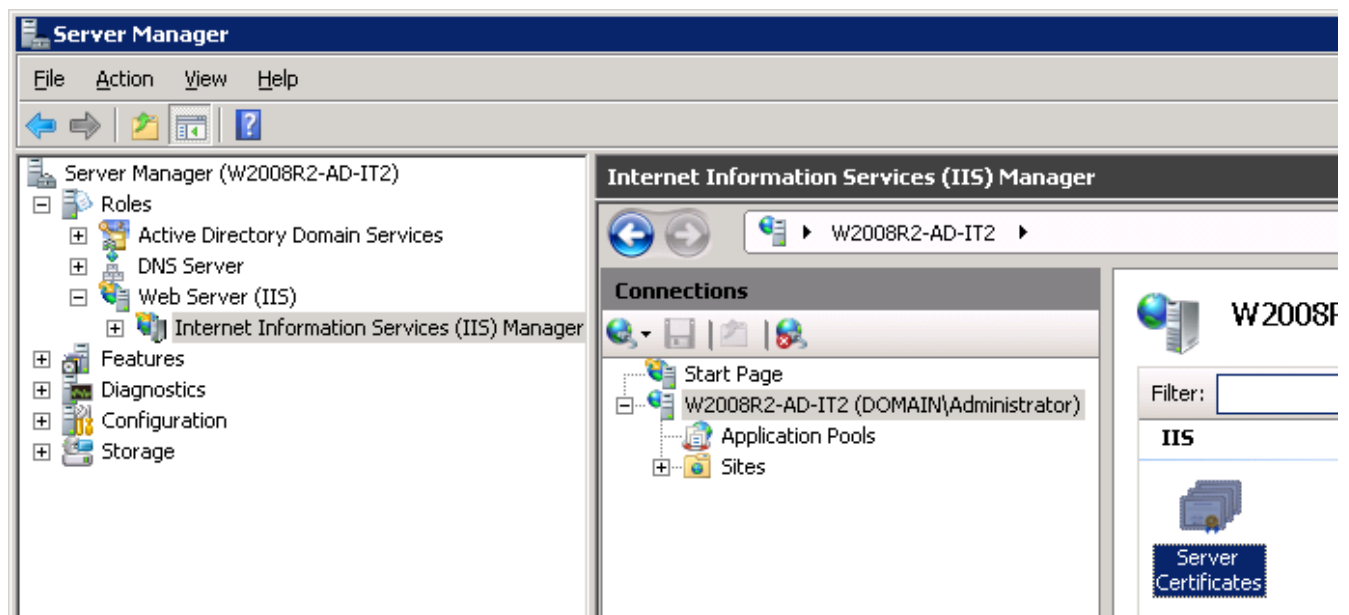


Figure 32 : Server Manager, IIS Manager

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

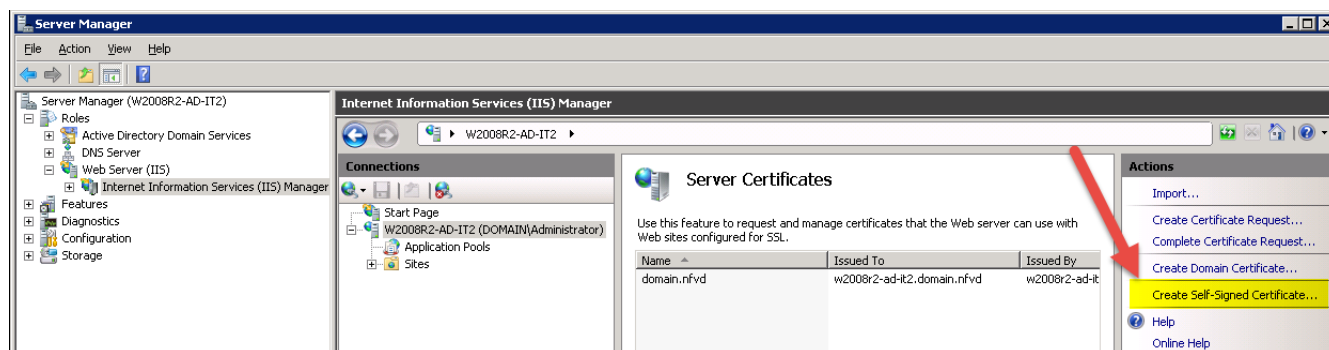


Figure 33 : Server Manager, create Self-Signed Certificate

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

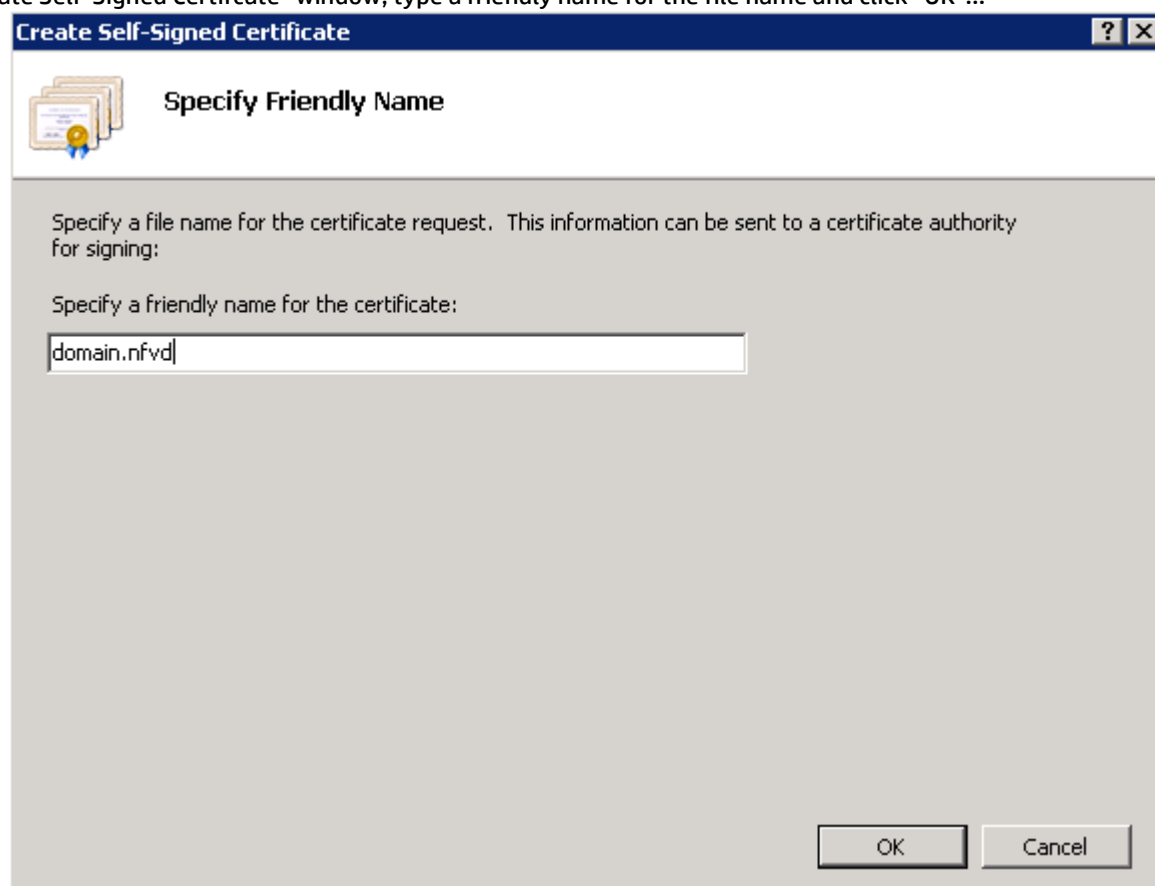


Figure 34 : Create Self-Signed Certificate, specify friendly name

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”...

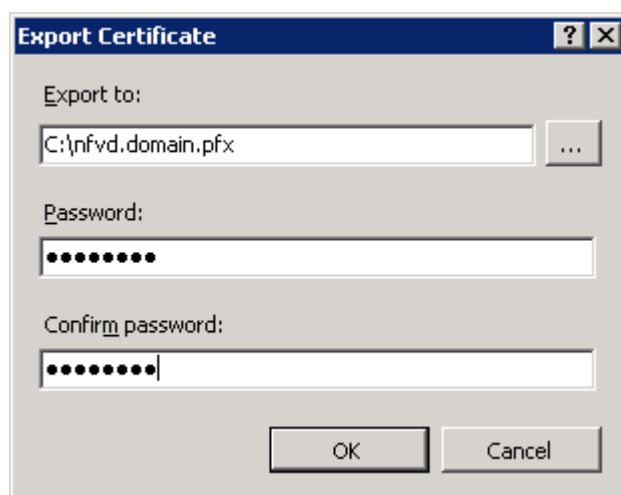


Figure 35 : Export Certificate

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

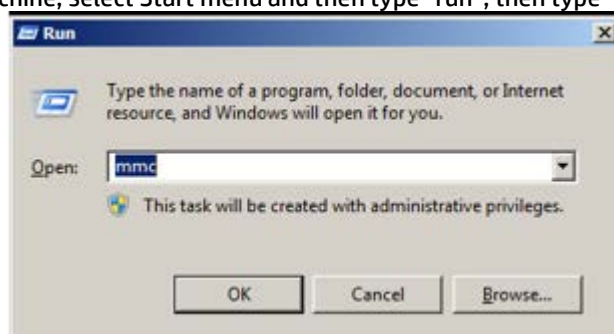


Figure 36 : Run mmc

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

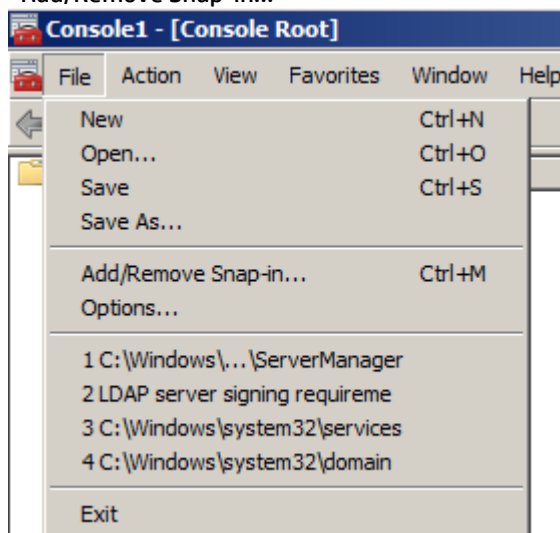


Figure 37 : Console1

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



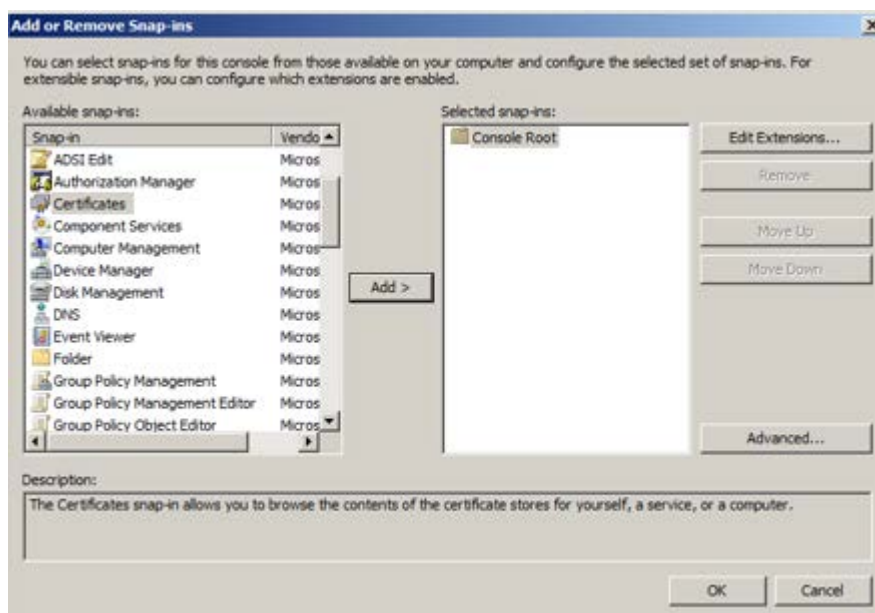


Figure 38 : Add Snap-ins

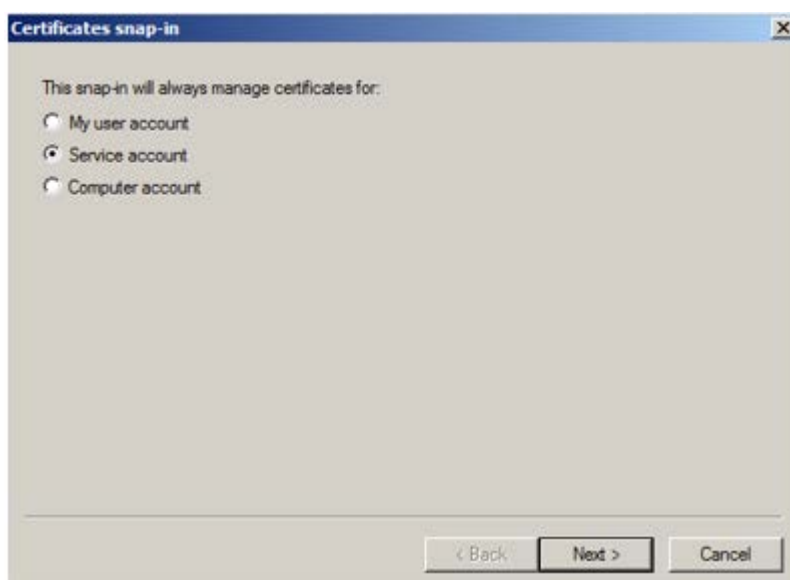


Figure 39 : Certificates snap-in

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

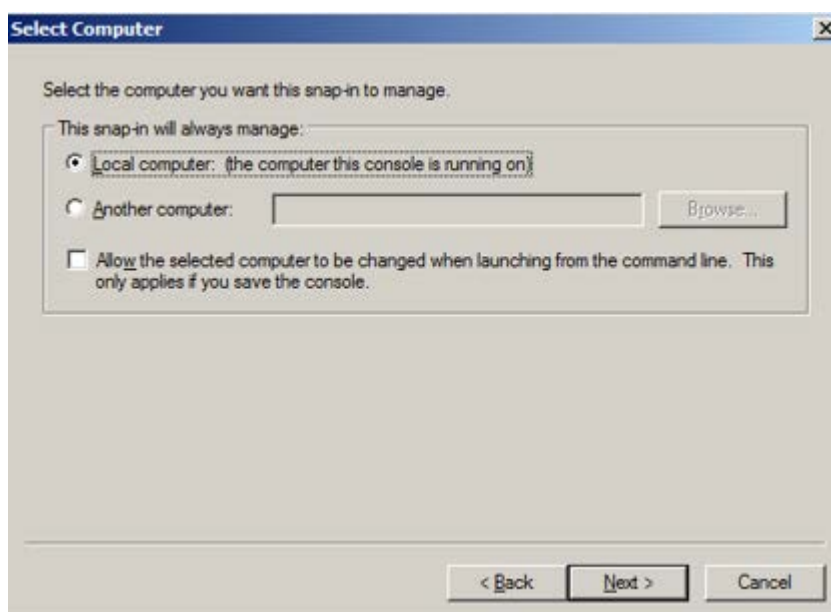


Figure 40 : Select Computer

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

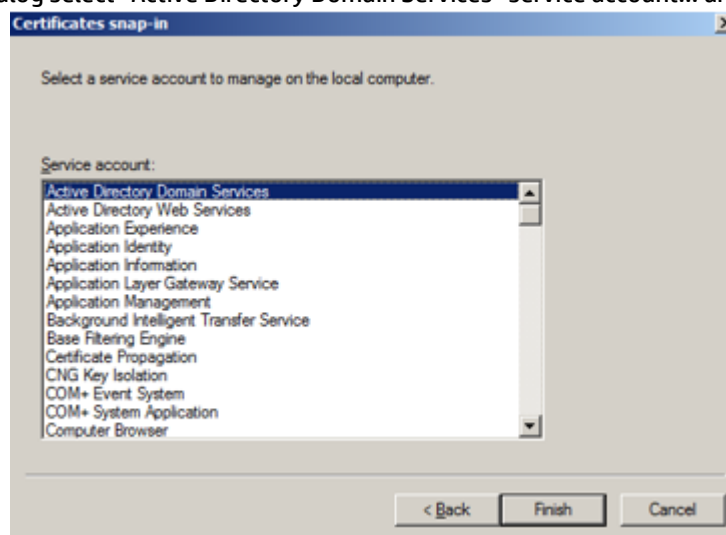


Figure 41 : Certificates snap-in

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

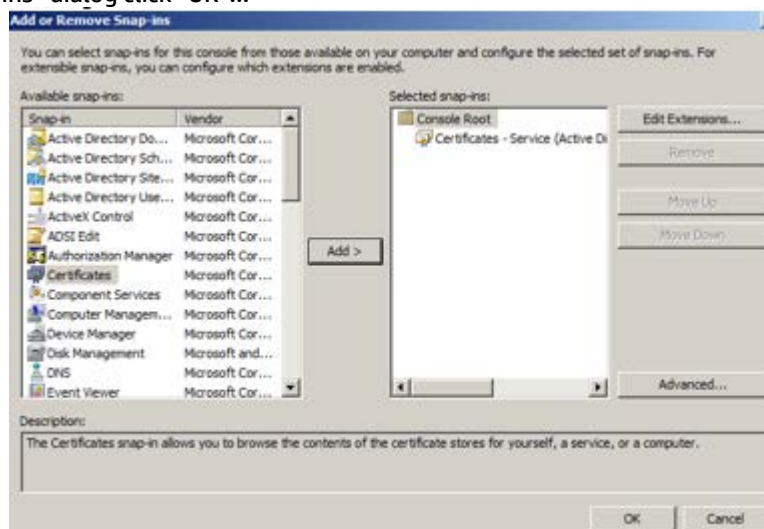


Figure 42 : AA or Remove Snap-ins