HPE NFV Director

Release Notes

Release 4.1
First Edition

Hewlett Packard
Enterprise

Notices

Contents

Preface

About this guide

The Release Notes describes critical information related to the HPE NFV Director V4.1 on RHEL 6.6 platform.

Audience

This guide is aimed at Product Users, Solution Architects, System Integrators, Solution Developers, and Software Development Engineers.

For installation details, refer to NFV Director V4.1 Installation, Configuration and Administration Guide

For On boarding VNFs, refer to NFV Director V4.1 VNF On-Boarding Guide

For User guide, refer to NFV Director V4.1 User Guide

For Resource Modeler tool usage, refer to the NFV Director V4.1 Resource Modeler Guide

For NFV Director APIs, refer to the NFV Director V4.1 NFV Director API Guide and NFV Director V4.1 Operations API Guide

For Discovery operations, refer to the NFV Director V4.1 Openstack Discovery Guide and NFV Director V4.1 OMi and uCMDB for NFVD User Guide

For vCenter operations, refer to the NFV Director V4.1 vCenter Resource Modeling Guide

For troubleshooting information, refer to the NFV Director V4.1 Troubleshooting Guide.

Document history

Table 1: Document history

Edition	Date	Description
1.0	30 July 2016	First Edition

Chapter 1
Features

HPE NFV Director provides a common point to ensure consistent management and behavior of VNFs, regardless of the vendor, enabling each VNF to efficiently run on heterogeneous hardware platforms and virtualization environments. The NFV Director automatically manages the end-to-end services across VNF.

The NFV Director is designed to meet the evolving ETSI specifications for the NFV orchestrator. This orchestrator manages and orchestrates virtual network functions and network services, thus providing a global resource management, and consistently applies global, cross-VNF, and VNF-specific policies.

NFV Director provides orchestration of multi-vendor VNFs across multiple VIMs, Multiple sites and multiple organizations providing a single pane of glass to manage resource consumption and quota usage.

1.1 VNF management

- Supports deploying VNF with custom extensions.
- Supports VNF Descriptor by using internal OpenXML-based format.
- Supports versioning VNF—Defined using extensible model with a rich set of pre-defined objects and relationships that can be extended.
- Supports affinity rules (must, must not) on VNF placement—Extensible to support other policies and policies on other objects.
- Supports multiple versions of the same VNF—Extensible to automatically update existing instances.

1.2 NFV monitoring

This module provides the following features:

- Automatic monitoring VNFs, and NFV computes infrastructure with correlation across end-to-end NFV topology.
- Automation rules for actions such as scale-in, scale-out, scale-up, and scale-down.
- Configurable and extensible set of pre-defined monitoring templates.
- Extensible to monitor virtual and physical network infrastructure.
- Easy to add or customize monitoring of any SNMP source.
- Extensible complex monitoring rules and thresholds.

1.3 VIM related features

VIM supports the following features:

- Support for RedHat OpenStack 7.0
- Support for OpenStack Kilo and others on demand.
- Support for HPE Helion Carrier Grade 2.0.
- Support for vCenter 5.5.
- No limitation in terms of number and size of datacenters.
- Affinity rules through the use of resource pools.
- Ability to orchestrate WAN and servers that are not under VIM control.

- Multi-vendor, multi-type VIM through plug-in adaptors. The adaptors can augment VIM capabilities.
- Support for unlimited number of VIMs and underlying virtual resources like VMs and can be from different vendors or of different types.

1.4 Event correlation and autonomous action

The event correlation and autonomous action supports the following features:

- Extensible to correlate events from different sources (VNFM, EMS, Physical resources) and take Automatic actions.
- Configurable simple automated actions (like scale-out if CPU > 80).
- Extensible more complex physical-to-virtual topology-based automated actions.

1.5 General

- Simple Pay as you grow model with very low entry price for PoC.
- Northbound APIs allow Integration with existing OSS.

Chapter 2
New Features/Enhancements

> **NOTE:**
> The V4.1 GA is bringing additional features and fixes compare to the V4.0 GA. It is maintaining the same level of features as the V4.0.1 release
>
> R&D will not provide any installable NFV-D V4.1 images. NFV D must be installed following the instructions provided in the installer, configuration and admin guides.
>
> In NFV Director 4.1, Tenant and VDC are used interchangeably

2.1 Support for Keystone V3

- Support for both OpenStack Keystone V2 and V3

2.2 Support for IPv6

- Discovery support for IPv6 OpenStack
- Deploy VNF on IPv6

2.3 Synchronize monitors in SiteScope

- Out of sync monitors in SiteScope are synchronized with the monitor data in NFV Director Fulfillment.
- When SiteScope template undergoes change in the newer version of NFV Director; the changes are reflected on the monitors that are already deployed in SiteScope.

2.4 Deploy VNF on VMWare vSphere via vCenter

- Support for VNF deploy on VMWare ESX server using vCenter.

2.5 Support for vCenter VIM

- Orchestration support for vCenter 5.5 VIM

2.6 Support for self-healing

Allows the user to execute a Heal action over a VNF already deployed. Heal operation could be triggered at VNF level or at component level.

2.7 Support for processing policies

Allows the user to execute custom actions during deploy, terminate and/or scale operations of a VNF.

2.8 Support VM order deployment

Allows the user to execute a VNF deployment where each VM will be activated over the VIM with a specific order decided previously by the user.

2.9 NFV Director Browser

The "NFVD Browser" is the tool that allows the user to browse and edit all templates, instances and resources. It also provides a graph view to show the hierarchy of the components.

2.10 NFV Director KPI Dashboard

The "KPI Dashboard" is the tool that allows the user to browse and display KPIs of instances.

Chapter 3 Overview of NFV Director software

This chapter provides overview of various software products included in the NFV Director.

📢 IMPORTANT: For VM resource requirements to setup the below components, refer to the NFV Director Install, Configure and Administrator Guide.

3.1 Fulfillment

📢 IMPORTANT: Fulfillment components are installed on RHEL 6.6 x86_64, and require Java SE 6 update 37 JDK or later (version 6, but not version 7), 32-bit. The 64-bit is not supported.

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

Table 2: NFV Director Fulfillment

Product	Version
HPE Service Activator	V62-1A
HPE SA Patch	V62-1A-9
HPE SA Extension Pack	6.1
HPE SA EP Patch	EP6.1-4
Oracle Database	11gR2

3.2 Assurance

📢 IMPORTANT: Assurance components are installed on RHEL 6.6 x86_64, and require Java 1.7.0.00 or later, 64-bit.

Table 3: NFV Director Assurance Gateway

Product	Version
Assurance Gateway	V4.1

Table 4: NFV Director UCA Automation

Product	Version
HPE UCA for EBC	V3.1
HPE UCA for EBC Patch	UCAEBC31SRVLIN_00007
HPE UCA for EBC Topology Extension	V3.1
HPE UCA for EBC Topology Extension Patch	UCAEBC31TOPOLIN_00001
UCA Automation Solution	V1.2
UCA Automation Patch	EBCATM-12LIN-00001
Open Mediation and Channel Adapters	

Table 5: NFV Director Open Mediation and Channel Adapter

Product	Version
OSS Open Mediation	V700
UCA EBC Channel Adapter	V3.1
UCA HPSA Channel Adapter	V2.0
UCA Autoconsole Channel Adapter	V2.0
Generic SNMP Channel Adapter	V200L01 RevB
SiteScope Customization for Generic SNMP Channel Adapter	V2.0.0 L01 RevC

VMware ESXi Customization for Generic SNMP Channel Adapter	V2.0

Table 6: NFV Director SiteScope

Product	Version
HP SiteScope	11.30
HP SiteScope hotfix	sis1131concurrent_templ_deploy_deleteGroupEx.zip

3.3 NFV Director GUI

Table 7: NFV Director GUI

Product	Version
Apache Couch DB	V1.6.0-1
NodeJS	V0.10.40-1
HPE Unified OSS Console	2.2.9
Graphviz	2.38
OpenSSL	1.0.1e-30

3.4 NFV Director OpenStack Discovery

Table 8: NFV Director OpenStack Discovery

Product	Version
OSS Open Mediation	V700
OpenStack Channel Adapter	1.0.0
Fulfillment Channel Adapter	1.0.0
NFVD Fulfillment	See 3.1
Oracle Database	See 3.1
UCA HPSA Channel Adapter	See 3.2
LDAP (OpenLDAP/ActiveDirectory)	OpenLDAP V3

3.5 NFV Director integration with OMi and BSMC (Optional Component)

Table 9: NFV Director integration with OMi and BSM Connector

Product	Version
OSS Open Mediation	V700
CMDB Channel Adapter	1.0.0
UCA HPSA Channel Adapter	See 3.2
OMi Channel Adapter	1.0.0
NFVD Fulfillment	See 3.1
Oracle Database	See 3.1
OMi	10.00/01
BSM-Connector	10.00
BSM-C for OneView Management Pack (MP)	
OMi Management Pack for HPHelion Carrier Grade (MP)	
OMi Management Pack for Nuage DCN (MP)	

3.6 NFV Director integration with DCN (Optional Component)

> 📄 NOTE: NFV Director V4.1 was validated with Alcatel-Lucent Nuage DCN, V3.2.1.1

Table 10: NFV Director Networking

Product	Version
OSS Open Mediation	V700
NFVD Fulfillment	See 3.1
SiteScope	See 3.2
OMi	See 3.5
OMi Management Pack for Nuage DCN (MP)	See 3.5
CMDB Channel Adapter	See 3.5
UCA HPSA Channel Adapter	See 3.2
Generic SNMP Channel Adapter	See 3.2
SiteScope Customization for Generic SNMP Channel Adapter	See 3.2

3.7 NFV Director Integration with Storage (Optional Component)

> 📄 NOTE: NFV Director V4.1 discovers HPE 3PAR Storage. LUN monitoring works with NFV Director only if OS version is 3.2.2 or above.

3.8 Virtual Infrastructure Manager and Hypervisors

The NFV Director supports through a plug-in extension, any type of VIM and even direct connectivity to hypervisor, although the preferred way (provided out-of-the-box) are any OpenStack VIM.

The NFV Director provides an OpenStack southbound interface (Kilo version) that can interface any VIM for supporting that interface.

The NFV director is out-of-the-box multi VIM and selects the VIM depending on the server the VM has been assigned to.

Following Virtual Infrastructure Manager and hypervisors are supported:

- HPE Helion CG 2.0
- OpenStack Kilo
- RedHat OpenStack 7
- VMWare vCenter 5.5

3.9 High Availability Monitoring solution tool

NFV Director V4.1 delivers an example High Availability solution tool. This example tool provides a reference to monitor fulfillment and assurance components.

Chapter 4 Known limitations

CR ID	Comments
2001	**Description:** Only virtual machines deployed by NFV Director on controlled VIM can be managed. **Customer Impact:** Control of the VIM (thru quota management, catalog management) is limited. NFV Director cannot get the virtual machine resources utilized in the VIM, If the virtual machine is not deployed/managed by NFVD. **Workaround:** Make sure that all virtual machines deployed on VIM are deployed by NFV Director.
2217	Stock allocated by a domain manager to an organization is not enforced. **Description:** It is possible for an organization manager to overwrite the quota allocated by a domain manager to its organization without any approval mechanism. **Customer impact:** Domain manager cannot control fully quota used by organization managers. **Workaround:** None. Best practice to be applied as organization manager to not change quota allocated by domain manager.

CR ID	Comments
2385	**Description:** Management of external storage is limited to use of a pre-defined list of Cinder volume types, which have to be explicitly created on Openstack VIM: • Vmware-Quality-A • Kvm-Baremetal-Quality-A • Vmware-Quality-B • Kvm-Baremetal-Quality-B • All-vs-Quality-C Other Cinder volume types defined in VIM are discovered by NFV Director but cannot be used for external storage. **Customer impact:** VIM IT Admin needs to comply with volume types pre-defined by NFV Director. **Workaround:** None.
2441	Limitations on scale-in feature with VNFs having custom monitors. **Description:** When VNFs are deployed with custom monitors, scale-in fails after a scale-out. **Customer impact:** Limitations on scale-in feature. **Workaround:** None.

Chapter 5 Unsupported Features

- Baremetal serves are modeled as physical machines, baremetal cannot be deployed in this release
- NFVD does not support out of the box any vendor VNFM product and VFM need be done through integration.
- Guaranteed mode is only provided as a customization example and is not yet supported.
- The following features are not supported
    - Live migration
    - Evacuate
    - SR-IOV
    - PCI-PT
    - Micro DC management
    - VNF updates (Add Volume, Add Monitors)

Chapter 6
Known problems

CR ID	Comments

2071	**Description:**
	
	Features documented in NFV Director 4.1 User Guide are not available with NFV Director 4.1:
	
	  - Section 3.1.2.2: import/export of component.
	  - Section 2.1.5.3: live Migrate of a Virtual Machine.
	
	Workaround:
	
	Ignore these sections.

2205	**Description:** When using "Delete Image" action to delete image, image is deleted from NFV Director portal but remains on file system. **Customer impact:** Housekeeping of file system is not automatic and requires to be done by explicitely removing file on file system. Impact is minor as long as there is still enough space on file system. **Workaround:** On NFV-Director Virtual Machine Fulfillment/GUI, login as root: Remove unused images from file system in: */var/opt/uoc2/server/public/addons/plugins/nfvd_portal/image_repository*
2347	**Description:** When scale-out is invoked, new VM has same name as the one in Base Component. **Customer impact:** Operability issue for management of VMs deployed/scaled by NFV Director. **Workaround:** None.

CR ID	Comments
2425	**Description:** There are corner cases related to job rollback management where virtual network are not visible in VDC Manager but still visible in Openstack. **Customer impact:** Operability issue: Inconsistency between status displayed in NFVD VDC Manager and Openstack. **Frequency:** Low **Workaround:** Do the clean-up in Openstack.
2434	**Description:** Use of nfvd_createVIM.sh command line with -discoverTenant option may lead to corrupted discovery. **Customer impact:** Inconsistent catalog management on NFV Directory. **Workaround:** Do not use -discoverTenant option when invoking nfvd_createVIM.sh command line.
2440	**Description:** Deletion of servers in Datacenter is not properly discovered by incremental discovery. This may lead to artifacts still being managed in NFVD but not available anymore as physical resources on datacenter. **Customer impact:** Datacenter resources are not properly discovered by NFV Director in case of server deletion. **Workaround:** None.

CR ID	Comments
2464	**Description:** No monitors are deployed when added to VNF in VDC Manager before deploying the VNF. **Customer impact:** Limitation on "add monitor" capability. **Workaround:** Monitors have to be added during design phase (in VNF Component and VNF Designer) instead of doing this in VDC Manager.
2466	**Description:** Failure when deploying VNF composed of VNFC (2 VMs) with monitoring. **Customer impact:** Limitation on capability to deploy VNF with monitoring. **Workaround:** Design monitors at VM level instead of VNFC.
2496	**Description:** Failure when deploying VDC in VCenter when ESXi is described with IP address. **Customer impact:** Limitations on capability to deploy VDC in VCenter infrastructure. **Workaround:** Describe ESXi with FQDN instead of IP address.

Chapter 7
Known deprecations

- GPM has been deprecated and so the VNFM interaction it provided
- VNFM integration will be ported in future versions to align with new API and multitenancy model
- SOSA, ECP and Lock Manager are still present but will be deprecated in the future, and locking and queue mechanism will be ported accordingly

Chapter 8 Verifying HPE Signatures

NOTE:
- If you do not already have GnuGP installed, you will have to download and install it. For information about obtaining and installing GnuGP, see http://www.gnupg.org
- The wget utility may not be available in the system by default. Install it using yum install

8.1 Verifying signature for NFV-D FF and AA components

These NFV-D components are digitally signed and accompanied by a set of GnuPG keys.

On: <FF_HOST>
<AA_HOST>
Login: root

8.1.1 Importing HPE public key

Perform the following steps to import the HPE public key needed for verifying the integrity of the delivered product:

- Create a directory where the HPE public keys will be stored:

```
# mkdir -p signcheck
```

- Download the compressed HPE GPG Public Key, and extract the keys:

```
# cd signcheck
# wget -P signcheck/ https://ftp.hp.com/pub/keys/HPE-GPG-Public-Keys.tar.gz
```

- Uncompress and extract the file content in signcheck directory

```
# gunzip HPE-GPG-Public-Keys.tar.gz
# tar xvf HPE-GPG-Public-Keys.tar
```

We get a list of HPE Public Certificates.

- Run the gpg import command to import the public certificate 2BAF2262.pub:

```
# gpg --import signcheck/2BAF2262.pub
```

- Configure level of trust for the imported key:

```
# gpg --edit-key 2BAF2262

gpg (GnuPG) 2.0.14; Copyright (C) 2009 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
pub  2048R/2BAF2262  created: 2015-12-10  expires: 2025-12-07  usage: SCEA
                     trust: unknown       validity: unknown
[ unknown] (1). Hewlett Packard Enterprise Company RSA-2048-14 <signhp@hpe.com>
Command> trust
```

```
pub  2048R/2BAF2262  created: 2015-12-10  expires: 2025-12-07  usage: SCEA
                          trust: unknown       validity: unknown
[ unknown] (1). Hewlett Packard Enterprise Company RSA-2048-14 <signhp@hpe.com>
Please decide how far you trust this user to correctly verify other users' keys
(by looking at passports, checking fingerprints from different sources, etc.)

  1 = I don't know or won't say
  2 = I do NOT trust
  3 = I trust marginally
  4 = I trust fully
  5 = I trust ultimately
  m = back to the main menu
Your decision? 5
Do you really want to set this key to ultimate trust? (y/N) y
pub  2048R/2BAF2262  created: 2015-12-10  expires: 2025-12-07  usage: SCEA
                          trust: ultimate      validity: unknown
[ unknown] (1). Hewlett Packard Enterprise Company RSA-2048-14 <signhp@hpe.com>
Please note that the shown key validity is not necessarily correct
unless you restart the program.
Command> quit
```

8.1.2 Verifying signature

> 📄 NOTE: Repeat the below steps for the following package:
> nfvd-correlation-04.01.000-1.el6.noarch.rpm
> nfvd-assur-gw-base-04.01.000-1.el6.noarch.rpm
> nfvd-assur-gw-core-04.01.000-1.el6.noarch.rpm
> nfvd-assur-gw-tpp-04.01.000-1.el6.noarch.rpm
> nfvd-monitors-04.01.000-1.el6.noarch.rpm
> nfvd-alarms-omi-04.01.000-1.el6.noarch.rpm
> nfvd-discovery-cmdb-04.01.000-1.el6.noarch.rpm
> nfvd-discovery-common-04.01.000-1.el6.noarch.rpm
> nfvd-fulfillment-04.01.000-1.el6.noarch.rpm
> nfvd-installer-04.01.000-1.el6.noarch.rpm
> NFVD Resource Modeler-win32.win32.x86_64.zip

- Run the gpg verify command to verify the signature file

```
# gpg --verify <package_name>.sig <package_name>
```

- If signature verification completed successfully, the command output will contain the following lines:

```
gpg: Signature made <DATE> using RSA key ID 2BAF2262
gpg: checking the trustdb
gpg: 3 marginal(s) needed, 1 complete(s) needed, PGP trust model
gpg: depth: 0  valid:  1  signed:  0  trust: 0-, 0q, 0n, 0m, 0f, 1u
gpg: next trustdb check due at 2025-12-07
gpg: Good signature from "Hewlett Packard Enterprise Company RSA-2048-14 <signhp@hpe.com>"
```

8.2 Verifying Signature for NFV-D GUI component

On: <GUI_HOST>

Login: root

8.2.1 Importing HPE public key

> 📄 **NOTE:**
> If <FF_HOST> and <GUI_HOST> are collocated, this section may have been run already.

Perform the following steps to import one of HPE public keys that is needed for verifying the integrity of the delivered product:

- Create a directory where the HPE public keys will be stored:

```
# mkdir -p signcheck
```
- Download the compressed HPE GPG Public Key, and extract the keys.

```
# cd signcheck
# wget -P signcheck/ https://ftp.hp.com/pub/keys/HPE-GPG-Public-Keys.tar.gz
```
- Uncompress and extract the file content in signcheck directory

```
# gunzip HPE-GPG-Public-Keys.tar.gz
# tar xvf HPE-GPG-Public-Keys.tar
```

We get a list of HPE Public Certificates.

Run the rpm import command to import the public certificate 2BAF2262.pub:

```
# rpm --import signcheck/2BAF2262.pub
```

8.2.2 Verifying signature

- In the location where UI RPM exists, run the rpm verify command to verify the nfvd-ui rpm file

```
# rpm -Kv nfvd-gui-04.01.000-1.el6.x86_64.rpm
```

- Check the command output. If signature verification completed successfully, the command output will contain the following lines:

```
nfvd-gui-04.01.000-1.el6.x86_64.rpm:
Header V3 RSA/SHA256 Signature, key ID 2baf2262: OK
Header SHA1 digest: OK (3d2584cb02f0fc393e65240890c305095a914ee5)
V3 RSA/SHA256 Signature, key ID 2baf2262: OK
MD5 digest: OK (e5de3f7f18ddc2ef7f92ff8a8be3965c)
```

- Run the rpm verify command to verify the nfvd-ui identity provider rpm file:

```
# rpm -Kv nfvd-gui-auth-04.01.000-1.el6.x86_64.rpm
```

- If signature verification completed successfully, the command output will contain the following lines:

```
nfvd-gui-auth-04.01.000-1.el6.x86 64.rpm:
Header V3 RSA/SHA256 Signature, key ID 2baf2262: OK
Header SHA1 digest: OK (45eae139d81b6e8ed26bb5f21a37411b3bd9d401)
V3 RSA/SHA256 Signature, key ID 2baf2262: OK
MD5 digest: OK (ab42d0f1284f0bf1fd5a87efb37df202)
```