HP NFV Director

HP NFV Director

Version 3.0

High Availability Installation and Configuration Guide

Edition: 1.0

For Linux (RHEL 6.6) Operating System

June 2015

Legal Notices

Warranty

The information contained herein is subject to change without notice. The only warranties for HP 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. HP shall not be liable for technical or editorial errors or omissions contained herein.

License Requirement and U.S. Government Legend

Confidential computer software. Valid license from HP 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.

Copyright Notices

Trademark Notices

Adobe®, Acrobat® and PostScript® are trademarks of Adobe Systems Incorporated.

Red Hat® and the Red Hat "Shadow Man" logo are registered trademarks of Red Hat, Inc. in the United States and other countries.

Linux is a registered trademark of Linus Torvalds.

Microsoft®, Windows® and Windows NT® are U.S. registered trademarks of Microsoft Corporation.

Oracle® is a registered U.S. trademark of Oracle Corporation, Redwood City, California.

X/Open® is a registered trademark, and the X device is a trademark of X/Open Company Ltd. in the UK and other countries.

Java™ is a trademark of Oracle and/or its affiliates.

Firefox® is a registered trademark of the Mozilla Foundation.

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

Contents

Tables

Figures

Preface

This manual describes the pre-installation requirements and provides the installation instructions for Network Function Virtualization Director (NFVD) in High Available mode. It also encompasses the configuration and management guide.

Intended Audience

The audience for this guide is the System Integrators (SI) and NFV Director administrators. They must have the knowledge of clustering software like RedHat Cluster Suite, Oracle RAC and traffic management using load balancers, data management using shared disk.

Software Versions

The term UNIX is used as a generic reference to the operating system, unless otherwise specified.

The software versions referred to in this document are as follows:

Product Version	**Supported Operating systems**
HP NFV Director 3.0	RHEL Release 6.6

Table 1 Software Versions

Typographical Conventions

`Courier Font`:

- Source code and examples of file contents.
- Commands that you enter on the screen.
- Pathnames
- Keyboard key names

Italic Text:

- Filenames, programs and parameters.
- The names of other documents referenced in this manual.

Bold Text:

To introduce new terms and to emphasize on important words.

Associated Documents

The following documents contain useful reference information:

References

- HP UCA Automation - Installation Guide
- OSS Open Mediation Installation and Configuration Guide
- OM Generic SNMP CA Installation and Configuration Guide
- OM SiteScope Customization for Generic SNMP CA Installation and Configuration Guide
- OM VMware ESXi Customization for Generic SNMP CA Installation and Configuration Guide
- HP SiteScope Deployment Guide
- HP Service Activator Installation Guide
- HP Service Activator Solution Separation and Deployment Manager Guide
- Unified Correlation Analyzer for Event Based Correlation Installation Guide
- *HP Unified OSS Console Installation Guide*
- HP NFV Director Installation and Configuration Guide

Support

Visit our HP Software Support Online Web site at https://softwaresupport.hp.com for contact information, and details about HP Software products, services, and support.

The software support area of the Software Web site includes the following:

- Downloadable documentation.
- Troubleshooting information.
- Patches and updates.
- Problem reporting.
- Training information.
- Support program information.

Install Location Descriptors

The following names are used throughout this guide to define install locations.

Descriptor	What the Descriptor represents
${NOM_INSTANCE}	/var/opt/openmediation-70/containers/<instance-#>
${UCA_EBC_HOME}	The root directory of UCA-EBC. The default value is /opt/UCA-EBC.
${UCA_EBC_DATA}	The data directory of UCA-EBC. Default value is /var/opt/UCA_EBC.
${UCA_EBC_INSTANCES}	This directory may contain multiple instances of UCA-EBC where the value packs are deployed. The path refers to ${UCA_EBC_DATA}/instances/default.
${ACTIVATOR_OPT}	The base install of Service Activator. The UNIX® location is /opt/OV/ServiceActivator.
${ACTIVATOR_ETC}	The install location of specific Service Activator files. The UNIX location is /etc/opt/OV/ServiceActivator.
$ACTIVATOR_VAR	The install location of specific Service Activator files. The UNIX location is /var/opt/OV/ServiceActivator
$JBOSS_HOME	The install location for JBoss. The UNIX location is /opt/HP/jboss
${NFVD_AGW_HOME}	The install base location of Assurance Gateway. The default UNIX location is /opt/HP/nfvd.
${SOSA_HOME}	The install base location of SOSA. The default UNIX location is ${ACTIVATOR_OPT}/EP/SOSA.
${ECP_HOME}	The install base location of Equipment Connections Pool. The default UNIX location is ${ACTIVATOR_OPT}/EP/ECP.
${SITESCOPE_HOME}	The root directory of SiteScope. The default value is /opt/HP/SiteScope.

Table 2 Install Location Descriptors

Chapter 1

Introduction

This document describes the procedure for installation and configuration of NFV Director Product in High Available mode.

1.1 Getting Started

Installation of NFV Director in High Available mode is primarily driven by the HA support provided by the underlying components involved in the NFV Director solution.

This document provides instructions to setup various underlying components in HA mode to support the deployment architecture as depicted in the next section.

1.2 Deployment Architecture

Figure 1 depicts the NFV Director High Available deployment architecture for local and geo-redundant modes.

In the Figure,

- Site 1 represents the primary site and is active
- Site 2 represents the backup site and is passive. Site 2 becomes active when Site 1 goes down
- Traffic is routed to the active site (Site 1 or Site 2) by an external component using a load balancer/traffic manager (global).

Note

Development and validation of external component is not in scope of NFV Director

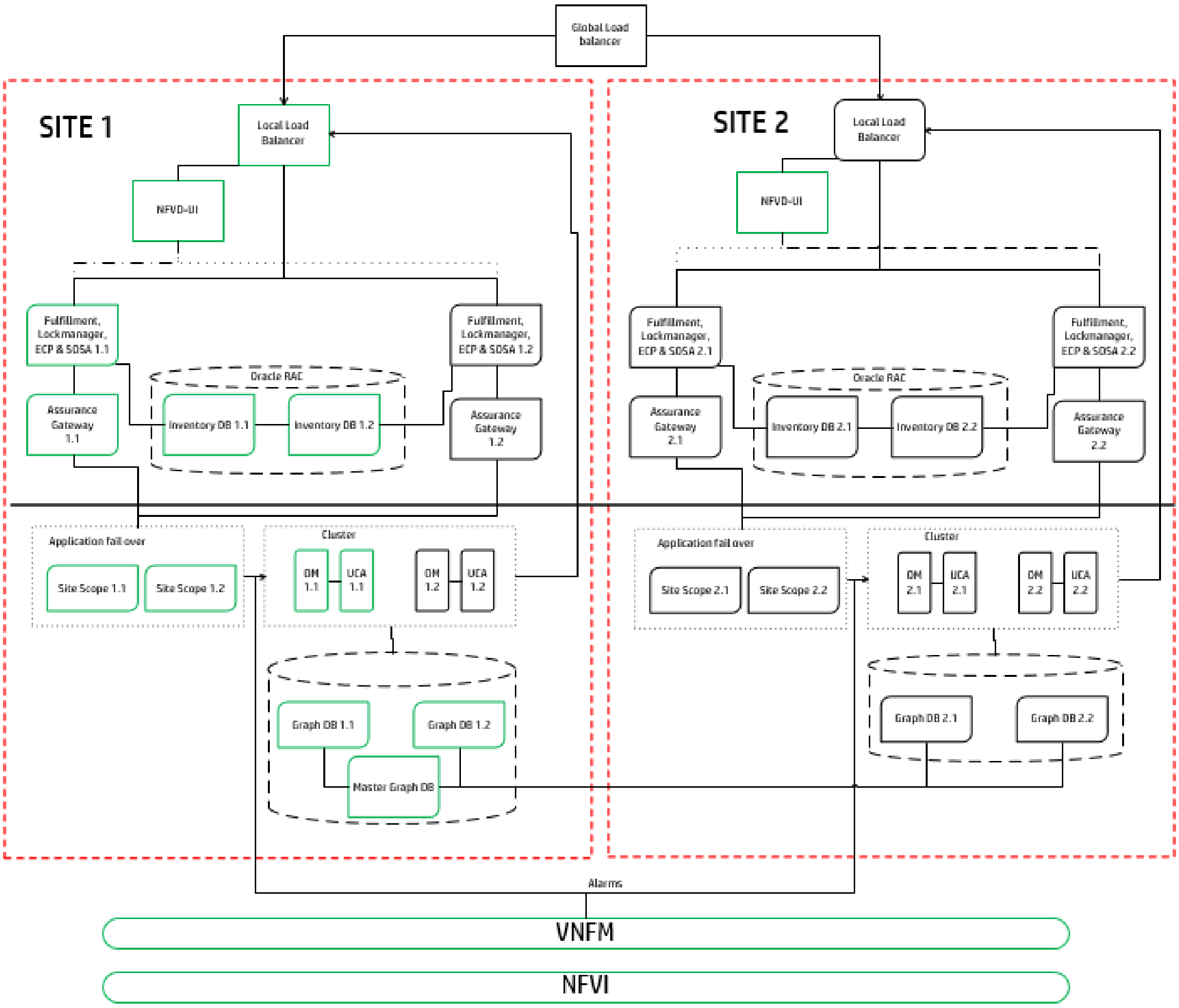


Figure 1 NFVD High Available Deployment Architecture

Table 3 shows the HA mode supported by various NFVD components.

NFVD Component	HA mode supported
HPSA	Active, Active Cluster formation with N nodes
HPSA Extension Packs	Active, Passive Cluster formation with N nodes
SiteScope	Active, Hot Standby Cluster formation with 2 nodes only
UCA-EBC + Open Mediation	Active, Passive Cluster formation with N nodes
Oracle RAC	Active, Active Custer formation with N nodes
Neo4j Graph database	Active, Active with N nodes
Assurance Gateway	Active, Active with one instance per HPSA node

Table 3 NFVD Components – supported HA mode

Chapter 2

Preparing to Install

Refer to the Chapter 3 – Preparing to Install of NFV Director Installation and Configuration Guide for hardware and software requirements for various NFV Director components.

Chapter 3

Installation

This chapter provides quick installation instructions to setup various NFVD components in Highly Available mode – HP Service Activator and HP Service Activator Extension Pack, UCA for EBC Server, UCA for EBC Topology Extension, UCA Automation, SiteScope, OM, and associated Channel Adapters.

Note

For detailed instructions and other installation options, refer to respective product documentation.

3.1 HPSA Cluster setup

3.1.1 HPSA setup on primary node

For instructions on how to install the HPSA, refer to the "Section 4.1 Installing HP Service Activator" in the HP NFV Director Installation and Configuration Guide".

Note

In this release, NFV Director HA setup has been validated on the Oracle database.

3.1.2 HPSA patch setup on primary node

After the installation of HPSA base product, install the HPSA patch by following the instructions in the section 4.1.4 Installing HP Service Activator Patch in the HP NFV Director Installation and Configuration Guide.

3.1.3 HPSA setup on other nodes

Repeat the instructions as provided in Installation of HPSA setup on primary node. However, follow the instruction in the Note below before proceeding with the installation.

Note

Uncheck the "Create database tables" checkbox while running the ActivatorConfig tool.

3.1.4 HPSA patch setup on other nodes

After the installation of HPSA base product, install the HPSA patch by following the instructions in the section 4.1.4 Installing HP Service Activator Patch in the HP NFV Director Installation and Configuration Guide. However, read the Note below before installing the patch.

Note

During installation of HPSA patch on the other nodes, type No when prompted to install the database.
Do you wish to install the database? [Yes/No] No

3.2 Installing the HPSA Extension Pack

3.2.1 Installing the HPSA Extension Pack on primary node

For instructions on how to install the HPSA Extension Pack, refer to the “Section 4.2 Installing HP Service Activator Extension Pack” in the HP NFV Director Installation and Configuration Guide”.

3.2.2 Installing the HPSA Extension Pack patch on primary node

For instructions on how to install the HPSA Extension Pack, refer to the “Section 4.2.1 Installing HP Service Activator Extension Pack patch” in the HP NFV Director Installation and Configuration Guide”.

3.2.3 Installing the HPSA Extension Pack on other nodes

Repeat the instructions as provided in Installing the HPSA Extension Pack on primary node. However, read the Notes below before proceeding with the installation.

Note

During installation of Extension Pack, type No when prompted to install the database.
Do you wish to install the database? [Yes/No] No

3.2.4 Installing the HPSA Extension patch Pack on other nodes

Repeat the instructions as provided in installing the HPSA Extension Pack patch on primary node. However, read the Notes below before proceeding with the installation.

Note

During installation of Extension Pack patch, type No when prompted to migrate the system database.
Do you wish to migrate your system database? [Yes/No] No

3.3 Installing the NFVD Fulfillment Solution on primary node

For instructions on how to install the NFVD Fulfillment solution, refer to the “Section 5.1 Installing the NFVD Fulfillment Solution” in the HP NFV Director Installation and Configuration Guide”.

Note

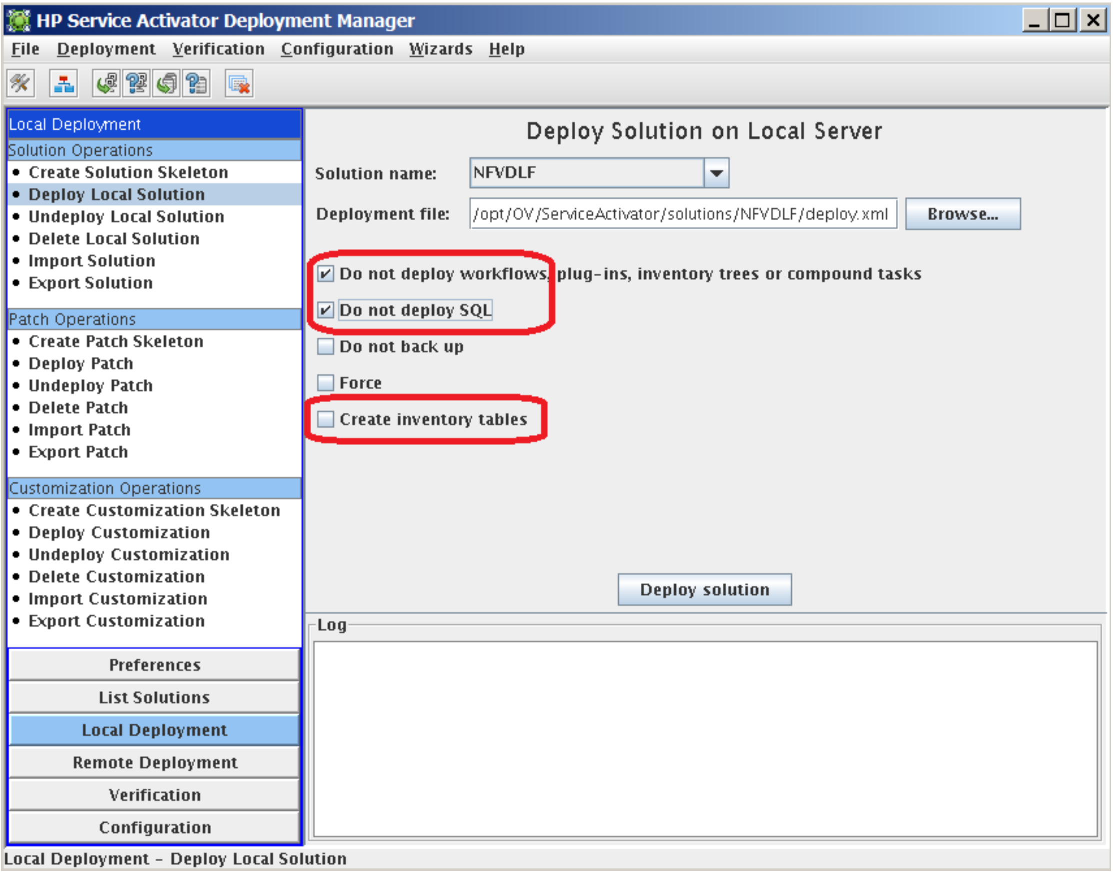
During deployment of Solution packs in the **primary node** using Deployment Manager, make sure to follow the instructions in the Section 5.1 Installing the NFVD Fulfillment Solution in the HP NFV Director Installation and Configuration Guide exactly as instructed.

3.4 Installing the NFVD Fulfillment Solution on other nodes

Repeat the instructions as provided in Installing the NFVD Fulfillment Solution on primary node. However, read the Notes below before proceeding with the installation.

Note

During deployment of Solution packs in the **other nodes** using Deployment Manager, make sure the checkboxes shown in below screen are always checked and others unchecked. A sample deployment window on other nodes is depicted below.



Deploy Solution on Local Server

Solution name: NFVDLF

Deployment file: /opt/OV/ServiceActivator/solutions/NFVDLF/deploy.xml

☑ Do not deploy workflows, plug-ins, inventory trees or compound tasks

☑ Do not deploy SQL

☐ Do not back up

☐ Force

☐ Create inventory tables

3.5 Installation and configuration of Load Balancer for HPSA

1) Perform installation of a LoadBalancer on a system. This procedure is illustrated using Haproxy LoadBalancer as an example.
2) Once installation is successful, edit the /etc/haproxy/haproxy.cfg file as shown below.

```
#---------------------------------------------------------------------
# Example configuration for a possible web application.  See the
# full configuration options online.
#
#   http://haproxy.1wt.eu/download/1.4/doc/configuration.txt
#
```

```
#---------------------------------------------------------------------
#---------------------------------------------------------------------
# Global settings
#---------------------------------------------------------------------
global
    # to have these messages end up in /var/log/haproxy.log you will
    # need to:
    #
    # 1) configure syslog to accept network log events.  This is done
    #    by adding the '-r' option to the SYSLOGD_OPTIONS in
    #    /etc/sysconfig/syslog
    #
    # 2) configure local2 events to go to the /var/log/haproxy.log
    #   file. A line like the following can be added to
    #   /etc/sysconfig/syslog
    #
    #    local2.*                       /var/log/haproxy.log
    #
    log         127.0.0.1 local2
    #chroot      /var/lib/haproxy
    #pidfile     /var/run/haproxy.pid
    maxconn     4000
    daemon
    #user        haproxy
    #group       haproxy

    # turn on stats unix socket
   #stats socket /var/lib/haproxy/stats
#---------------------------------------------------------------------
# common defaults that all the 'listen' and 'backend' sections will
# use if not designated in their block
#---------------------------------------------------------------------
defaults
    mode                    http
    log                     global
    option                  httplog
    option                  dontlognull
    option http-server-close
    option forwardfor       except 127.0.0.0/8
    option                  redispatch
    retries                 3
    timeout http-request    10s
    timeout queue           1m
    timeout connect         10s
    timeout client          1m
    timeout server          1m
    timeout http-keep-alive 10s
    timeout check           10s
    #maxconn                3000
#---------------------------------------------------------------------
#---------------------------------------------------------------------
# main frontend which proxys to the backends
#---------------------------------------------------------------------
#frontend  main *:5000
    #acl url_static       path_beg       -i /static /images /javascript /stylesheets
    #acl url_static       path_end       -i .jpg .gif .png .css .js
    #use_backend static          if url_static
    #default_backend             app
frontend  http-in
    bind *:< any free port >
    default_backend             app
#---------------------------------------------------------------------
# static backend for serving up images, stylesheets and such
```

```
#---------------------------------------------------------------------
#backend static
    #balance     roundrobin
    #server      static 127.0.0.1:4331 check
#---------------------------------------------------------------------
# round robin balancing between the various backends
#---------------------------------------------------------------------
backend app
    #balance     roundrobin
    server  app1 <Node1 IP>:<HPSA port> maxconn 32 check
    server  app2 <Node2 IP>:<HPSA port> maxconn 32 check
```

Launch HP Service Activator UI at http://<Node IP/ Load Balancer IP>:< Load Balancer port>/activator

Note

Make sure you use the configured Load Balancer (HaProxy) IP and port in the configuration files of NFVD.

3.6 SiteScope High Availability setup

This involves the following steps in general:

1. Install SiteScope on a node to act as primary SiteScope
2. Install SiteScope Patch on the primary node.
3. Install SiteScope (same version as in step 1) as Failover SiteScope on another node identified for this purpose.
4. Install SiteScope patch (same version as in step 2) on the failover node.

3.6.1 Installing SiteScope on primary node

For instructions on how to install SiteScope as Primary node, refer to the “Section 4.8 Installing SiteScope” in the HP NFV Director Installation and Configuration Guide”.

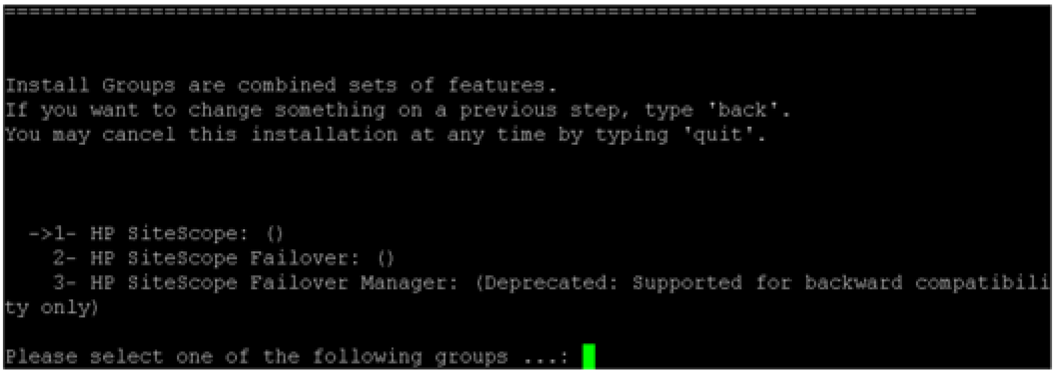
3.6.2 Installing SiteScope on failover node

Repeat the instructions as provided in Installing SiteScope on primary node. However, read the Notes below before proceeding with the installation.

.

Note

Be careful to choose the right options here for failover server setup.
Enter 2 to select HP SiteScope Failover: () to install SiteScope on Failover server, and press Enter. Below screen shows the configuration window sample.



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

Install Groups are combined sets of features.
If you want to change something on a previous step, type 'back'.
You may cancel this installation at any time by typing 'quit'.


  ->1- HP SiteScope: ()
    2- HP SiteScope Failover: ()
    3- HP SiteScope Failover Manager: (Deprecated: Supported for backward compatibili
ty only)

Please select one of the following groups ...:
```

3.6.3 Configuring SiteScope Failover node

3.6.3.1 Configure Lightweight Single Sign-on (LWSSO) for Authentication as follows:

Access the primary SiteScope user interface.

Select Preferences > General Preferences > LW SSO Settings.

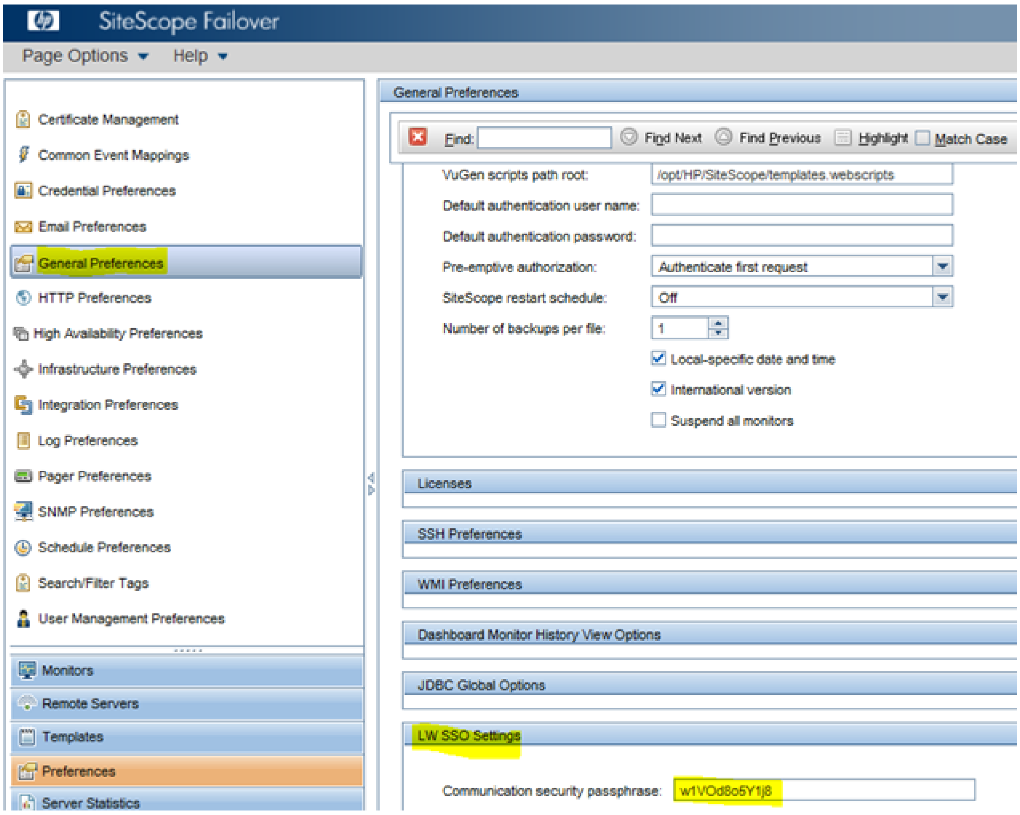
Copy the text from the Communication security passphrase field.

Access the SiteScope Failover user interface.

Navigate to Preferences > General Preferences > LW SSO Settings.

Paste the communication security passphrase, and then click Save.

Restart SiteScope Failover.



VuGen scripts path root: /opt/HP/SiteScope/templates.webscripts

Default authentication user name:

Default authentication password:

Pre-emptive authorization: Authenticate first request

SiteScope restart schedule: Off

Number of backups per file: 1

☑ Local-specific date and time

☑ International version

☐ Suspend all monitors

Communication security passphrase: w1VOd8o5Y1j8

Figure 2 SiteScope Failover LW-SSO Setting

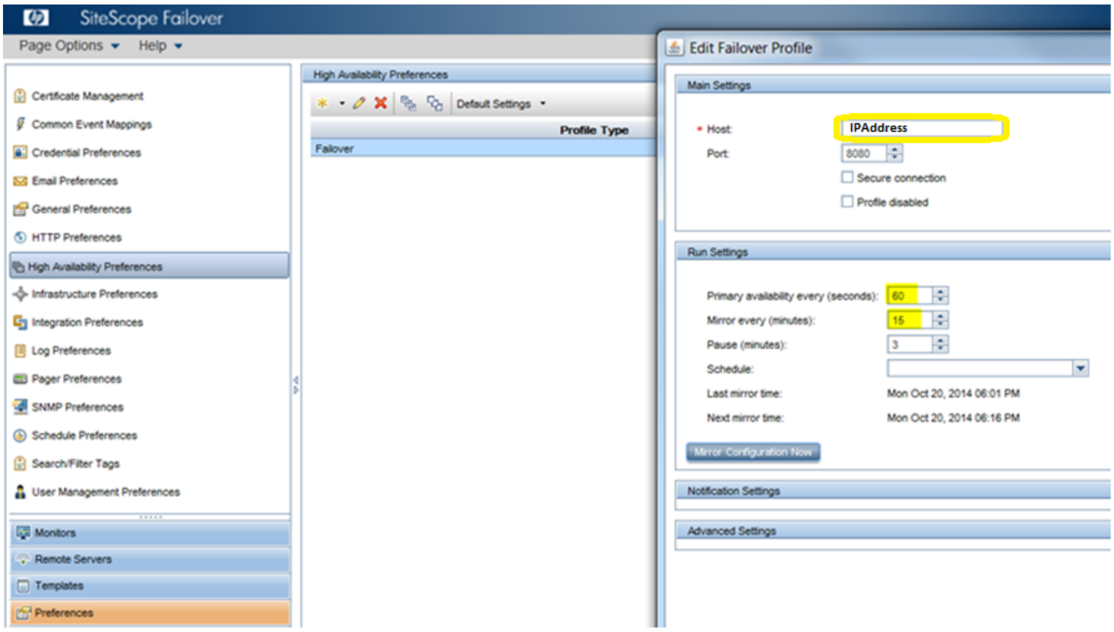
3.6.3.2 Create a new Failover Profile

a) In the Failover node UI, go to Preferences > High Availability Preferences.

b) In the right panel, click New Profile to open the New Failover Profile dialog.

c) Specify the settings as required[sample in screenshot below], and then click OK,

d) The value “Host” is the IP address of the Primary SiteScope.



Profile Type
Failover

* Host: IPAddress

Port: 8080

□ Secure connection

□ Profile disabled

Primary availability every (seconds): 60

Mirror every (minutes): 15

Pause (minutes): 3

Schedule:

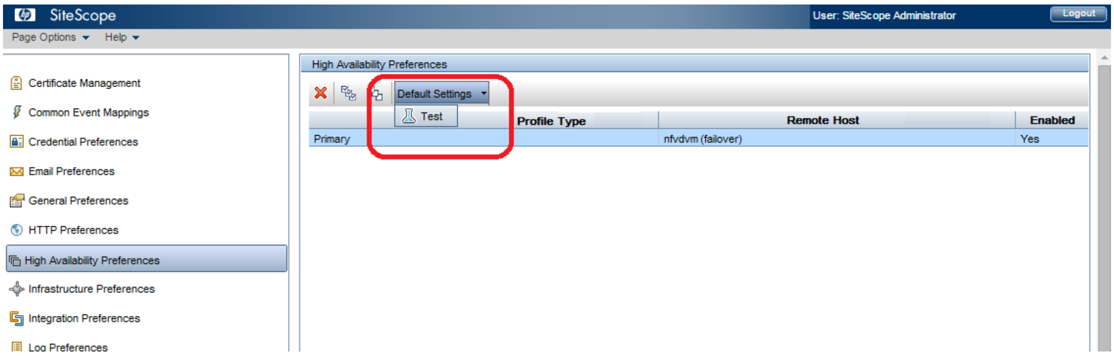
Last mirror time: Mon Oct 20, 2014 06:01 PM

Next mirror time: Mon Oct 20, 2014 06:16 PM

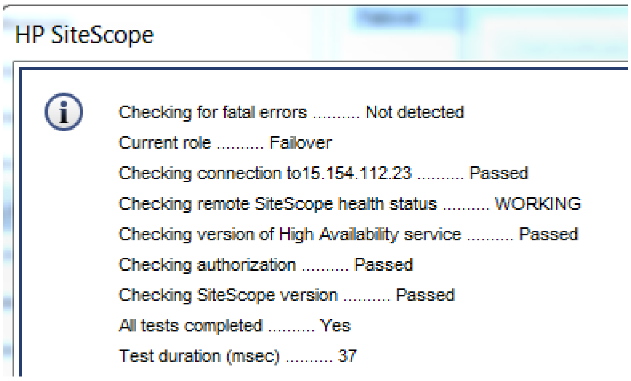
Figure 3 SiteScope Failover Profile Preferences

3.6.3.3 Verify Failover node settings

Login to SiteScope UI using Primary node IP. Go to Preferences > High Availability Preferences. Select Default Settings > Test.



Profile Type	Remote Host	Enabled
Primary	nfvdvm (failover)	Yes



HP SiteScope

```
Checking for fatal errors .......... Not detected
Current role .......... Failover
Checking connection to15.154.112.23 .......... Passed
Checking remote SiteScope health status .......... WORKING
Checking version of High Availability service .......... Passed
Checking authorization .......... Passed
Checking SiteScope version .......... Passed
All tests completed .......... Yes
Test duration (msec) .......... 37
```

Figure 4 SiteScope Failover setup verification

3.7 Installing NFVD SiteScope monitors

For instructions on how to install NFVD SiteScope monitors, refer to the “Section 5.5.5 Installing NFVD SiteScope monitors” in the HP NFV Director Installation and Configuration Guide”. However, read the Notes below before proceeding with the installation.

Note

Follow the instructions as specified in “Section 5.5.1 Installing assurance gateway scripts” in the HP NFV Director Installation and Configuration Guide before performing installation of NFVD SiteScope monitors.

Also perform the installation first on Primary node followed by Failover node

3.8 Import SiteScope templates and configurations

For instructions on how to Import SiteScope templates and configurations, refer to the “Section 5.5.6 Import SiteScope templates and configurations” in the HP NFV Director Installation and Configuration Guide”.

Note

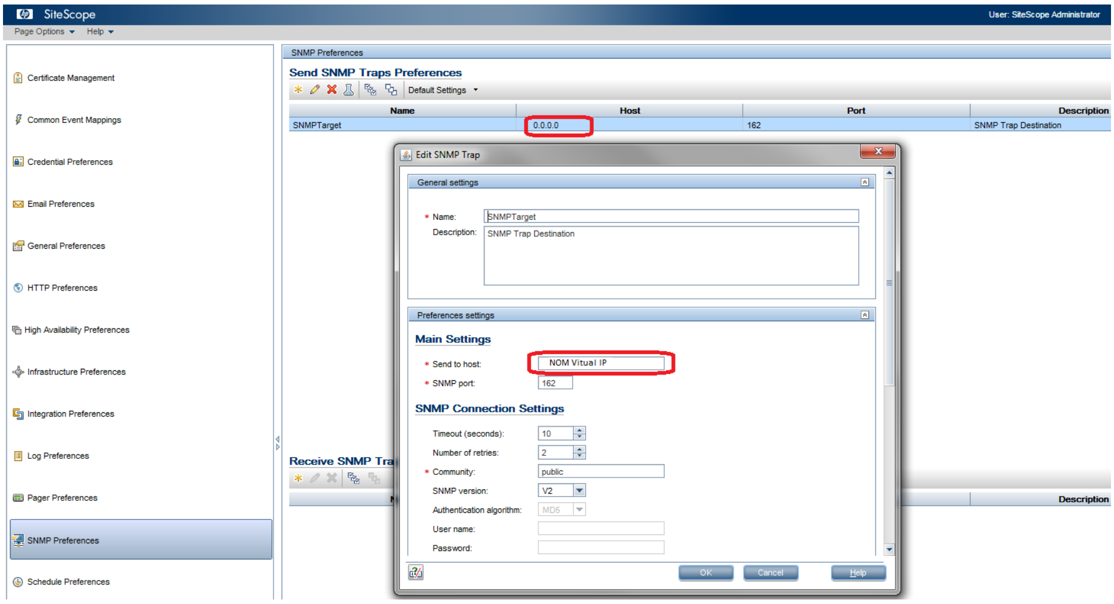
Perform the import operation first on Primary node followed by Failover node

3.9 Configure OM Endpoint in SiteScope

Login to SiteScope UI using Primary node IP. Go to Preferences > SNMP Preferences.

Edit the SNMPTarget entry and provide the Virtual IP configured for OM and click OK button.

Perform the same steps on the Failover node also.



Name	Host	Port	Description
SNMPTarget	0.0.0.0	162	SNMP Trap Destination

* Name: SNMPTarget

Description: SNMP Trap Destination

* Send to host: NOM Vitual IP

* SNMP port: 162

Timeout (seconds): 10

Number of retries: 2

* Community: public

SNMP version: V2

Authentication algorithm: MD5

User name:

Password:

3.10 OM High Availability setup

Note

In NFVD HA setup there is one OM and Channel Adapters per UCA Automation.

3.10.1 Installing OM on Primary node

For instructions on how to install OM on Primary node, refer to the “Section 4.3 Installing OM” in the HP NFV Director Installation and Configuration Guide”.

3.10.2 Installing OM on Failover node

For instructions on how to install OM on Failover node, refer to the “Section 4.3 Installing OM” in the HP NFV Director Installation and Configuration Guide”.

Note

Configurations related to OM HA setup are explained as part of UCA-EBC HA setup in below sections.

3.11 UCA-EBC High Availability setup

Note

In NFVD HA setup, OM and Channel Adapters, UCA-EBC and UCA Automation reside together in both nodes.

3.11.1 Installing UCA for EBC on Primary node

For instructions on how to install UCA for EBC on Primary node, refer to the “Section 4.4.2 Installing UCA for EBC” in the HP NFV Director Installation and Configuration Guide”.

3.11.2 Installing UCA for EBC Server patch on Primary node

For instructions on how to install UCA for EBC Server patch on Primary node, refer to the “Section 4.4.3 Installing UCA for EBC Server patch” in the HP NFV Director Installation and Configuration Guide”.

3.11.3 Installing UCA for EBC Topology Extension on Primary node

For instructions on how to install UCA for EBC Topology Extension on Primary node, refer to the “Section 4.5 Installing UCA for EBC Topology Extension” in the HP NFV Director Installation and Configuration Guide”.

Note

For HA setup, external topology server is used.

3.11.4 Installing UCA for EBC Topology Extension Patch on Primary node

For instructions on how to install UCA for EBC Topology Extension Patch on Primary node, refer to the “Section 4.52 Installing UCA for EBC Topology Extension Patch” in the HP NFV Director Installation and Configuration Guide”.

Note

For HA setup, external topology server is used.

3.11.5 Installing UCA for EBC on Failover node

For instructions on how to install UCA for EBC on Failover node, refer to the “Section 4.4.2 Installing UCA for EBC” in the HP NFV Director Installation and Configuration Guide”.

3.11.6 Installing UCA for EBC Server patch on Failover node

For instructions on how to install UCA for EBC Server patch on Failover node, refer to the “Section 4.4.3 Installing UCA for EBC Server patch” in the HP NFV Director Installation and Configuration Guide”.

3.11.7 Installing UCA for EBC Topology Extension on Failover node

For instructions on how to install UCA for EBC Topology Extension on Failover node, refer to the “Section 4.5 Installing UCA for EBC Topology Extension” in the HP NFV Director Installation and Configuration Guide”.

Note

HA setup is validated with external Graph DB.

3.11.8 Installing UCA for EBC Topology Extension Patch on Failover node

For instructions on how to install UCA for EBC Topology Extension Patch on Failover node, refer to the “Section 4.5 Installing UCA for EBC Topology Extension” in the HP NFV Director Installation and Configuration Guide”.

Note

HA setup is validated with external Graph DB.

3.12 Neo4J High Availability setup (External DB)

UCA for EBC Topology Extension is designed to work with Neo4J 1.9 Graph Database as topology server. For external topology server configuration, the installation and configuration of this product is a prerequisite.

3.12.1 Download and Install Neo4j

a) Download Neo4J 1.9 Enterprise Edition from http://www.neo4j.com

b) Transfer the archive to a location where you want to install Neo4J, and extract.

```
# cp neo4j-enterprise-1.9.9-unix.tar.gz /home/neo4j
# tar -zxvf neo4j-enterprise-1.9.9-unix.tar.gz
```

3.12.2 Configure Neo4j properties

a) Edit /home/neo4j/neo4j-enterprise-1.9.9/conf/neo4j-server.properties

```
Uncomment the line #org.neo4j.server.webserver.address=0.0.0.0
Set org.neo4j.server.database.mode=HA
```

b) Edit /home/neo4j/neo4j-enterprise-1.9.9/conf/neo4j.properties

```
# ha.server_id is the number of each instance in the HA cluster.
# It should be an integer (e.g. 1), and should be unique for each cluster instance

For the first node in the HA cluster that has Neo4J, set
ha.server_id=<number>, where <number> is 1 for first node, 2 for second node, and so on.

# ha.initial_hosts is a comma-separated list (without spaces) of the host:port
# where the ha.cluster_server of all instances will be listening. Typically
# this will be the same for all cluster instances.
ha.initial_hosts=<IP address of other host 1 in the cluster>:5001, <IP address of other host 2 in the cluster>:5001
```

3.12.3 Configure UCA-EBC properties

Edit the following properties in /var/opt/UCA-EBC/instances/default/conf/uca-ebc.properties file to point to this external Neo4j.

```
uca.ebc.topology=external
uca.ebc.topology.serverhost= < external topology  server host name >
uca.ebc.topology.webPort=7474
```

Manually copy the following files to the Neo4J topology server `plugins` directory:

- `/opt/UCA-EBC/lib/opencsv-2.3.jar`
- `/opt/UCA-EBC/lib/scalalogging-slf4j_2.10-1.0.1.jar`
- `/opt/UCA-EBC/lib/uca-ebc-topology-dataload-3.1.jar`
- `/opt/UCA-EBC/lib/config-0.5.2.jar`

The following commands will start/stop/check status of Neo4J respectively.

- `/home/neo4j/neo4j-enterprise-1.9.9/bin/neo4j start`

- `/home/neo4j/neo4j-enterprise-1.9.9/bin/neo4j stop`
- `/home/neo4j/neo4j-enterprise-1.9.9/bin/neo4j status`

3.12.4 Start/Stop Neo4j

Start Neo4J on one VM after the other

Run `/home/neo4j/bin/neo4j start` on each node in the cluster

Run /home/neo4j/bin/neo4j status to check status

Starting Neo4j Server...HA instance started in process [1296]. Will be operational once connected to peers. See /var/tmp/neo4j215/neo4j-enterprise-2.1.5/data/log/console.log for current status

```
./neo4j start
WARNING: Max 1024 open files allowed, minimum of 40 000 recommended. See the Neo4j manual.
Using additional JVM arguments:  -server -XX:+DisableExplicitGC -Dorg.neo4j.server.properties=conf/neo4j-
server.properties -Djava.util.logging.config.file=conf/logging.properties -
Dlog4j.configuration=file:conf/log4j.properties -XX:+UseConcMarkSweepGC -XX:+CMSClassUnloadingEnabled
```

Note

On the master node in the cluster, the log content will be:

```
2014-10-24 15:05:32.908+0000 INFO  [Cluster] Instance 2 is available as slave at
ha://15.154.112.29:6001?serverId=2 with StoreId{creationTime=1414160150852,
randomId=8313842770032418635, storeVersion=14406081294923270,
upgradeTime=1414160150852, upgradeId=8313842770032418635}
```

Note

On the slave node in the cluster, the log content will be:

```
2014-10-24 15:05:31.026+0000 INFO  [Cluster] Attempting to join cluster of [15.154.112.28:5001,
15.154.112.29:5001]
2014-10-24 15:05:35.104+0000 INFO  [Cluster] Joined cluster:Name:neo4j.ha
Nodes:{1=cluster://15.154.112.28:5001, 2=cluster://15.154.112.29:5001} Roles:{coordinator=1}
2014-10-24 15:05:35.109+0000 INFO  [Cluster] Instance 2 (this server)  joined the cluster
2014-10-24 15:05:35.143+0000 INFO  [Cluster] Instance 1 was elected as coordinator
2014-10-24 15:05:35.153+0000 INFO  [Cluster] Instance 1 is available as master at
ha://15.154.112.28:6001?serverId=1 with StoreId{creationTime=1414160150852,
randomId=8313842770032418635, storeVersion=14406081294923270,
upgradeTime=1414160150852, upgradeId=8313842770032418635}
2014-10-24 15:05:35.165+0000 INFO  [Cluster] ServerId 2, moving to slave for master
ha://15.154.112.28:6001?serverId=1
```

Note

Once Neo4j is started, the client can be launched at http://<Neo4J Node IP>:7474

Verify the status of each host in the cluster, on the link:

http://<Ip address of the server>:7474/webadmin/#/info/org.neo4j/High%20Availability/

Note

Verify the setup by adding a node to the master DB and confirm if the slave DB(s) also get updated with the same node.

3.13 Installation and Configuration of LOAD Balancer for Neo4J

Note

This section explains the steps involved in installation and configuration of a load balancer using HA Proxy as an example.

Perform installation of haproxy on a system. Once installation is successful, edit the /etc/haproxy/haproxy.cfg file as shown below.

```
#---------------------------------------------------------------------
# Example configuration for a possible web application.  See the
# full configuration options online.
#
#   http://haproxy.1wt.eu/download/1.4/doc/configuration.txt
#
#---------------------------------------------------------------------
#---------------------------------------------------------------------
# Global settings
#---------------------------------------------------------------------
global
    # to have these messages end up in /var/log/haproxy.log you will
    # need to:
    #
    # 1) configure syslog to accept network log events.  This is done
    #    by adding the '-r' option to the SYSLOGD_OPTIONS in
    #    /etc/sysconfig/syslog
    #
    # 2) configure local2 events to go to the /var/log/haproxy.log
    #   file. A line like the following can be added to
    #   /etc/sysconfig/syslog
    #
    #    local2.*                       /var/log/haproxy.log
    #
    log         127.0.0.1 local2
    #chroot      /var/lib/haproxy
    #pidfile     /var/run/haproxy.pid
    maxconn     4000
    daemon
    #user        haproxy
    #group       haproxy

    # turn on stats unix socket
   #stats socket /var/lib/haproxy/stats
#---------------------------------------------------------------------
# common defaults that all the 'listen' and 'backend' sections will
# use if not designated in their block
#---------------------------------------------------------------------
defaults
    mode                    http
    log                     global
    option                  httplog
    option                  dontlognull
    option http-server-close
    option forwardfor       except 127.0.0.0/8
    option                  redispatch
    retries                 3
    timeout http-request    10s
    timeout queue           1m
    timeout connect         10s
    timeout client          1m
    timeout server          1m
    timeout http-keep-alive 10s
    timeout check           10s
    #maxconn                3000
#---------------------------------------------------------------------
#---------------------------------------------------------------------
# main frontend which proxys to the backends
#---------------------------------------------------------------------
#frontend  main *:5000
    #acl url_static       path_beg       -i /static /images /javascript /stylesheets
    #acl url_static       path_end       -i .jpg .gif .png .css .js
    #use_backend static          if url_static
    #default_backend             app
frontend  http-in
    bind *:< any free port >
    default_backend             app
#---------------------------------------------------------------------
# static backend for serving up images, stylesheets and such
#---------------------------------------------------------------------
#backend static
    #balance     roundrobin
    #server      static 127.0.0.1:4331 check
#---------------------------------------------------------------------
# round robin balancing between the various backends
#---------------------------------------------------------------------
backend app
    #balance     roundrobin
    option httpchk GET /db/manage/server/ha/available
    server  app1 <Node1 IP>:<Neo4j port> maxconn 32 check
    server  app2 <Node2 IP>:< Neo4j port> maxconn 32 check
```

Note

Once HAProxy is started, the client can be launched at http://<HA Proxy IP>:<proxy port>

3.14 Installation and Configuration of RHEL High-Availability Add-On

Note

Installation of Clustering software is illustrated using Redhat Clustering software.
'yum' tool is used for installation in this example. Ensure that yum has access to "High Availability" and "Resilient Storage" rpms

3.14.1 Installation of RHEL High-Availability Add-On

Configure local yum repository and run the below 2 commands on all the nodes in the cluster

```
# yum -y groupinstall "High Availability"
# yum -y groupinstall "Resilient Storage"
```

Install the 'luci' component on the management node in the cluster.

Note

Execute the below command to install the luci component only on the node chosen to become the management node of the cluster.

```
# yum -y install luci ccs
```

Ensure that the following RPMs are installed.

```
# rpm -qa | grep ccs
ccs-0.16.2-63.el6.x86_64

# rpm –qa | grep cman
cman-3.0.12.1-49.el6.x86_64

# rpm -qa | grep omping
omping-0.0.4-1.el6.x86_64

# rpm -qa | grep rgmanager
rgmanager-3.0.12.1-17.el6.x86_64
```

On the management node,

```
# rpm -qa | grep luci
luci-0.26.0-37.el6.x86_64
```

3.14.2 Configuration of RHEL High-Availability Add-On

Execute following commands: replace 255.255.248.0/24 with the appropriate subnet mask and CIDR

```
# iptables -I INPUT -m state --state NEW -m multiport -p udp -s 255.255.248.0/24 -d 255.255.248.0/24 --dports
5404,5405 -j ACCEPT

# iptables -I INPUT -m addrtype --dst-type MULTICAST -m state --state NEW -m multiport -p udp -s
255.255.248.0/24 --dports 5404,5405 -j ACCEPT

# iptables -I INPUT -m state --state NEW -p tcp -s 255.255.248.0/24 -d 255.255.248.0/24 --dport 21064 -j
ACCEPT

# iptables -I INPUT -m state --state NEW -p tcp -s 255.255.248.0/24 -d 255.255.248.0/24 --dport 11111 -j
ACCEPT

# iptables -I INPUT -m state --state NEW -p tcp -s 255.255.248.0/24 -d 255.255.248.0/24 --dport 16851 -j
ACCEPT

# iptables -I INPUT -m state --state NEW -p tcp -s 255.255.248.0/24 -d 255.255.248.0/24 --dport 8084 -j ACCEPT

# iptables -I INPUT -p igmp -j ACCEPT

# service iptables save ; service iptables restart
iptables: Saving firewall rules to /etc/sysconfig/iptables:[  OK  ]
iptables: Flushing firewall rules:                         [  OK  ]
iptables: Setting chains to policy ACCEPT: filter          [  OK  ]
iptables: Unloading modules:                               [  OK  ]
iptables: Applying firewall rules:                         [  OK  ]
```

Set password for 'ricci' user on all the nodes in the cluster as follows.

Note

This password must be provided while creating the cluster in Step 7.

```
# passwd ricci
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
```

3.14.3 Starting RHEL High-Availability Add-On services

Start ricci by using ‘service ricci start’ and enable it to start at boot time via chkconfig

```
# service ricci start
Starting oddjobd:                                    [  OK  ]
generating SSL certificates...  done
Generating NSS database...  done
Starting ricci:                                      [  OK  ]

# chkconfig ricci on
```

Start luci as follows only on the node chosen to be management node (or enable it to start at boot time via chkconfig)

Note

Management Node is the node chosen in Step 2 above.

```
# service luci start
Adding following auto-detected host IDs (IP addresses/domain names), corresponding to `nfvdvm46.ind.hp.com'
address, to the configuration of self-managed certificate `/var/lib/luci/etc/cacert.config' (you can change them by
editing `/var/lib/luci/etc/cacert.config', removing the generated certificate `/var/lib/luci/certs/host.pem' and
restarting luci):
        (none suitable found, you can still do it manually as mentioned above)

Generating a 2048 bit RSA private key
writing new private key to '/var/lib/luci/certs/host.pem'
Start luci...                                        [  OK  ]
Point your web browser to https://nfvdvm46.ind.hp.com:8084 (or equivalent) to access luci
```

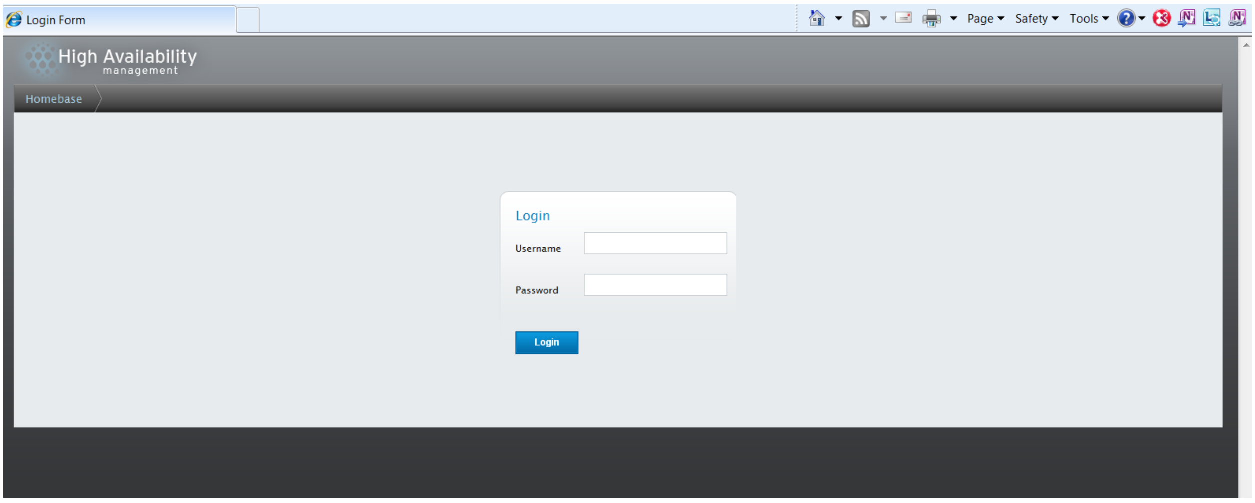
3.14.4 Access Luci Management console

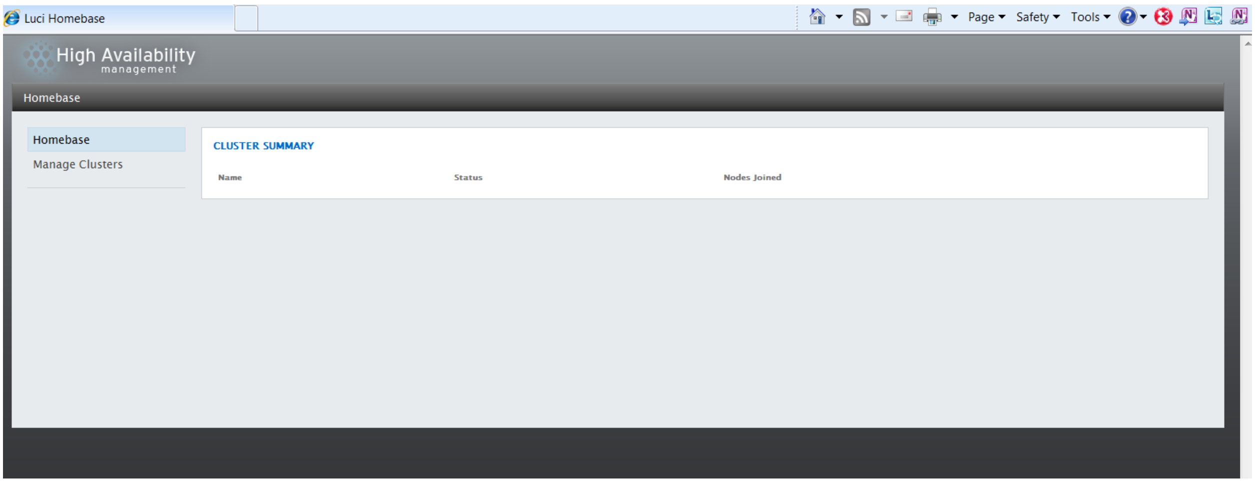
Luci Management Console UI can be accessed at

https://<IP_address_of_server_where_luci_is_installed>:8084

Note

Login credentials are the same as the root credentials for the server on which luci is installed.



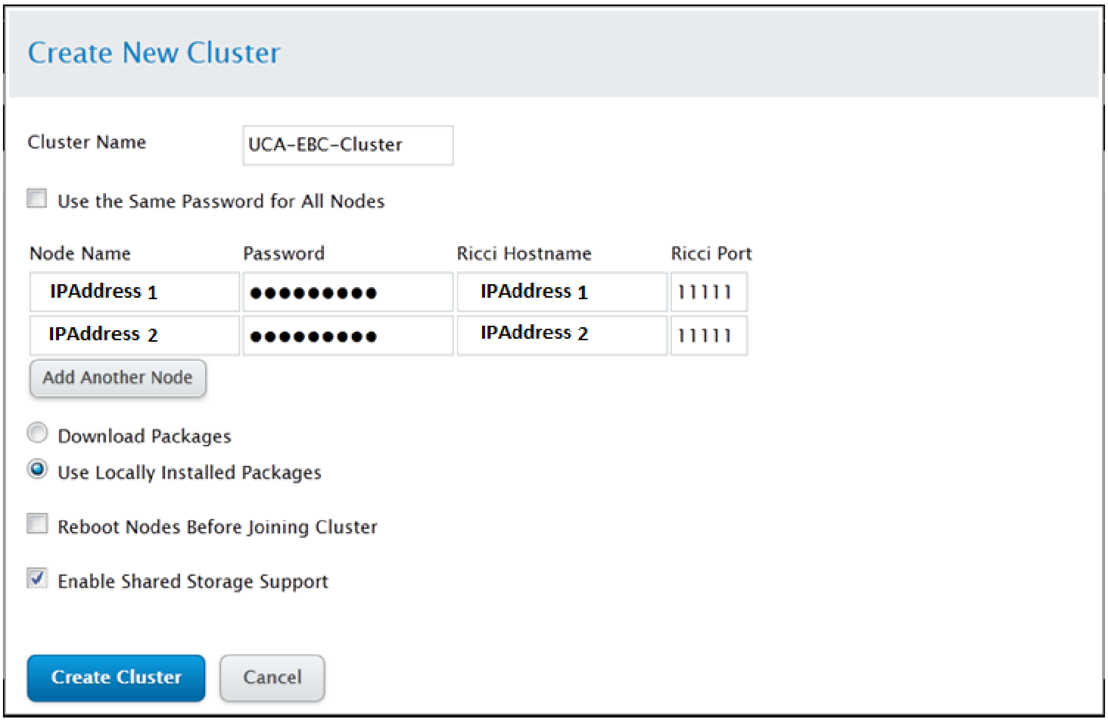


3.14.5 Cluster configurations

Click on Manage Clusters-> Create

Note

The ricci password is the password created in Step 5; use "Add Another Node" button to add details of subsequent nodes in the cluster. Hit "Create Cluster" button when details of all the nodes in the cluster have been added.



Create New Cluster

Cluster Name: UCA-EBC-Cluster

□ Use the Same Password for All Nodes

Node Name	Password	Ricci Hostname	Ricci Port
IPAddress 1	●●●●●●●●●	IPAddress 1	11111
IPAddress 2	●●●●●●●●●	IPAddress 2	11111

○ Download Packages

● Use Locally Installed Packages

□ Reboot Nodes Before Joining Cluster

☑ Enable Shared Storage Support

Stop NetworkManager before starting Cluster Manager [cman]

```
# service NetworkManager stop
# chkconfig NetworkManager off
# /etc/init.d/cman start
Starting cluster:
   Checking if cluster has been disabled at boot...        [  OK  ]
   Checking Network Manager...                        [  OK  ]
   Global setup...                                [  OK  ]
   Loading kernel modules...                          [  OK  ]
   Mounting configfs...                            [  OK  ]
   Starting cman...                               [  OK  ]
   Waiting for quorum...                            [  OK  ]
   Starting fenced...                              [  OK  ]
   Starting dlm_controld...                          [  OK  ]
   Tuning DLM kernel config...                         [  OK  ]
   Starting gfs_controld...                          [  OK  ]
   Unfencing self...                               [  OK  ]
   Joining fence domain...                           [  OK  ]
```

Note

Start cman on other node(s) in the cluster

Start CLVMD service:

```
# /etc/init.d/clvmd start
Starting clvmd:
Activating VG(s):   2 logical volume(s) in volume group "vg_nfvdvm" now active
  clvmd not running on node <IP Address2>     … this suggests that this clvmd service should be started on the
other node(s) in the cluster
                                                   [  OK  ]
```

Upon starting clvmd on other node, the output is as follows:

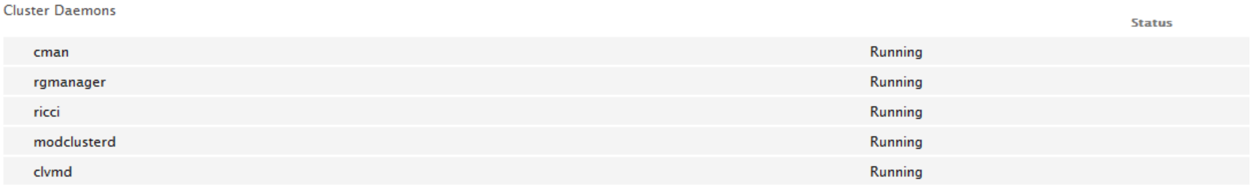
```
# /etc/init.d/clvmd start
Starting clvmd:
```

```
Activating VG(s):   2 logical volume(s) in volume group "vg_nfvdvm" now active

# chkconfig  clvmd on
```

Start RGMANAGER:

```
# /etc/init.d/rgmanager start
Starting Cluster Service Manager:                          [  OK  ]

# chkconfig rgmanager on
```

Click on each node listed in the cluster and ensure that all components are running as can be seen below:



Cluster Daemons

	Status
cman	Running
rgmanager	Running
ricci	Running
modclusterd	Running
clvmd	Running

Note

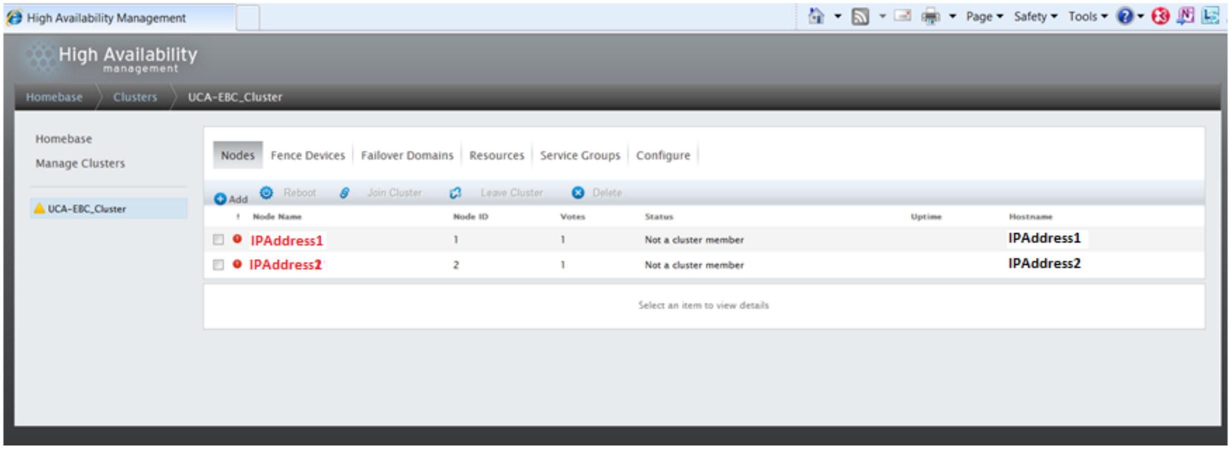
Fencing has not been setup here

Note

If there are issues with opening on the UI, change the browser and check; IE or Mozilla is preferred. Issues seen with Chrome.

Note

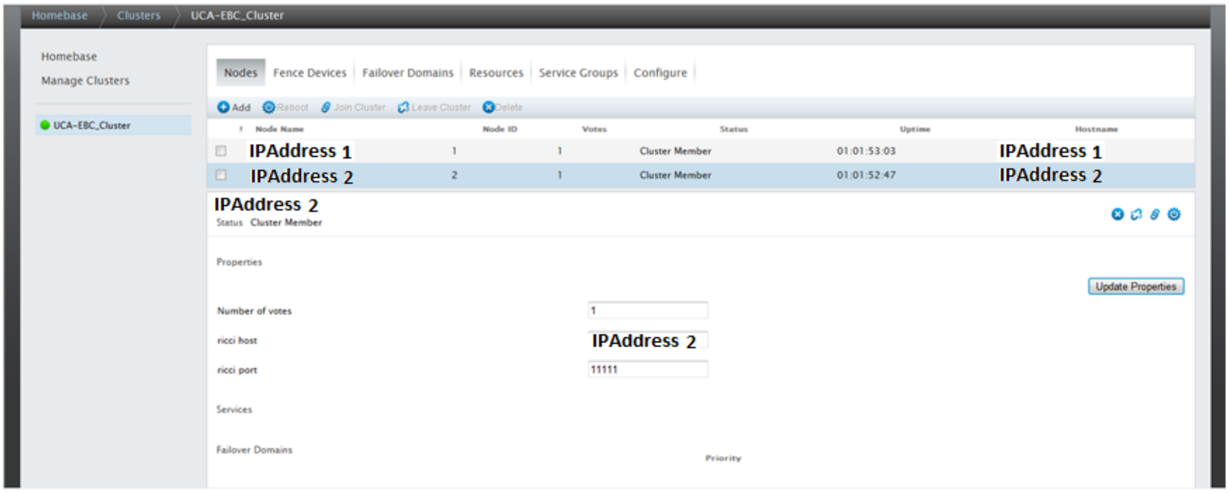
If you get the following screen showing nodes in red, then click on the node to see if any of the above services are 'not running'



	!	Node Name	Node ID	Votes	Status	Uptime	Hostname
□	●	IPAddress1	1	1	Not a cluster member		IPAddress1
□	●	IPAddress2	2	1	Not a cluster member		IPAddress2

Select an item to view details

Screen showing successfully setup cluster:



	Node Name	Node ID	Votes	Status	Uptime	Hostname
□	IPAddress 1	1	1	Cluster Member	01:01:53:03	IPAddress 1
□	IPAddress 2	2	1	Cluster Member	01:01:52:47	IPAddress 2

IPAddress 2

Status Cluster Member

Properties

Number of votes: 1

ricci host: IPAddress 2

ricci port: 11111

Services

Failover Domains

Priority

Note

Always follow the same order for stopping/starting the cluster as shown below:

Stopping Cluster services

On each node: # service rgmanager stop
On each node: # service clvmd stop
On each node: # service cman stop

Starting Cluster services

On each node: # service cman start
On each node: # service clvmd start
On each node: # service rgmanager start

Configuring UCA-EBC as a service:

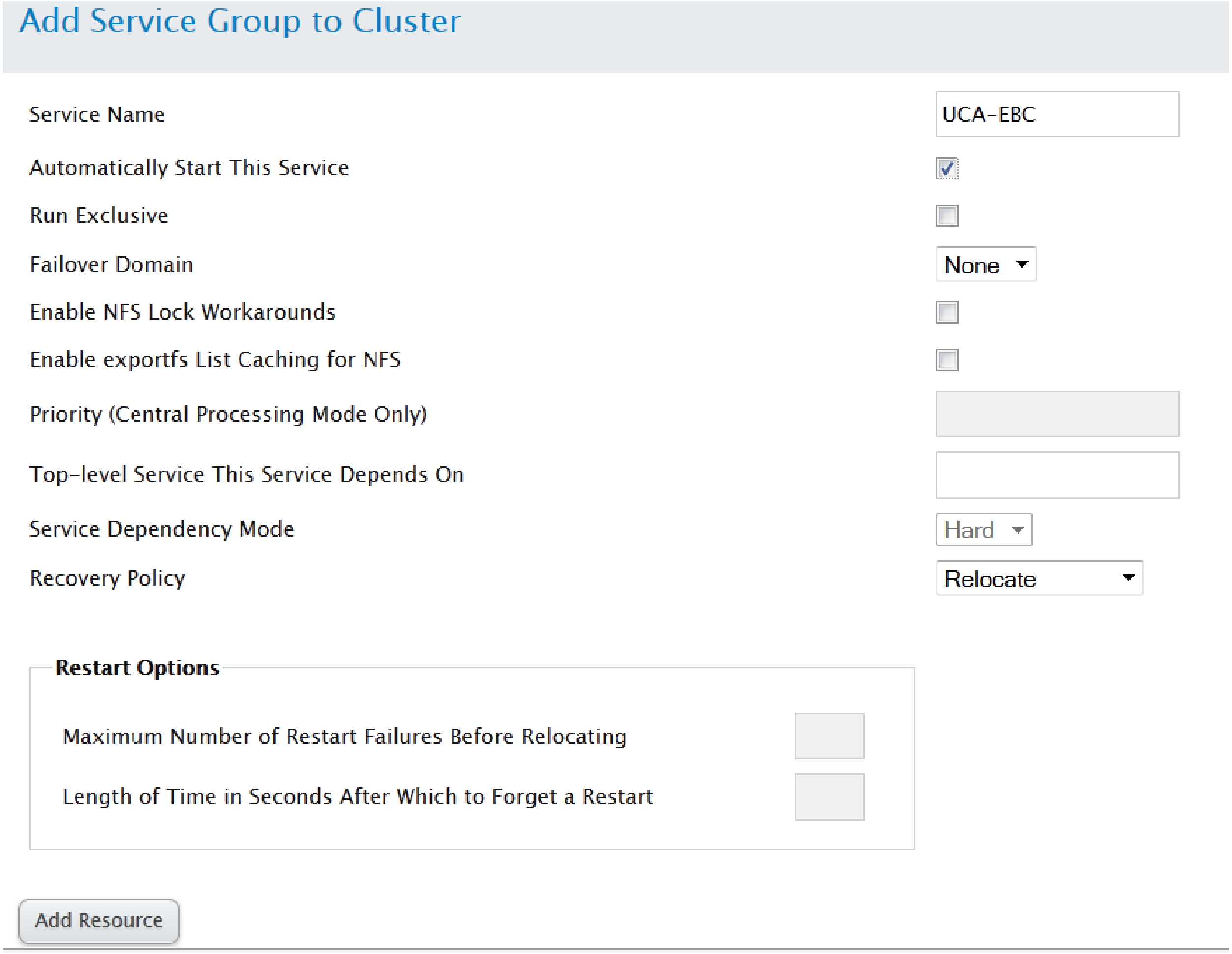
Note

This worked on Mozilla only. https://<IP>:<port>/cluster/UCA-EBC_Cluster/services

Declare UCA for EBC service. It will be created in the cluster as a service group.

From the cluster-specific page, add the UCA-EBC service to that cluster by

- Clicking on "Service Groups" along the top of the cluster display.
- Click Add. This displays the Add Service Group to Cluster dialog box.
- On the Add Service Group to Cluster dialog box, at the Service Name text box, type the name of the UCA for EBC service, e.g. UCA-EBC
- Check the Automatically Start This Service checkbox if you want the UCA-EBC service to start automatically when the cluster is started.
- Use the Recovery Policy drop-down box to select a recovery policy for the service. We recommend to use the option 'Relocate', and ignore the restart options



Add Service Group to Cluster

Service Name	UCA-EBC
Automatically Start This Service	☑
Run Exclusive	□
Failover Domain	None
Enable NFS Lock Workarounds	□
Enable exportfs List Caching for NFS	□
Priority (Central Processing Mode Only)	
Top-level Service This Service Depends On	
Service Dependency Mode	Hard
Recovery Policy	Relocate

Restart Options

Maximum Number of Restart Failures Before Relocating	
Length of Time in Seconds After Which to Forget a Restart	

Adding resources for UCA-EBC HA service:

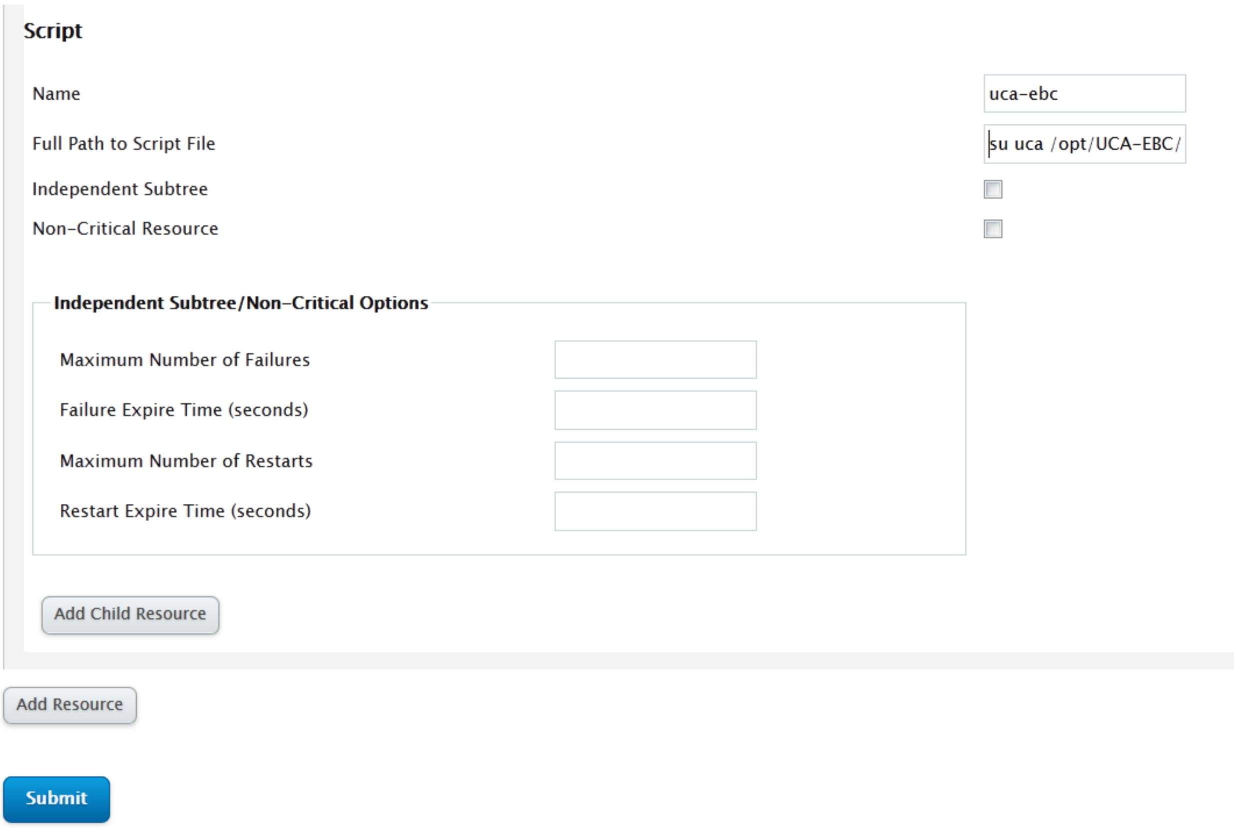
In the Service Groups tab, click on the UCA-EBC service, and then click on the Add Resource button.

Then from the dropdown list choose Script

Mention the details as shown in the screenshot that follows:

In the “Full Path to Script File” mention: su uca /opt/UCA-EBC/bin/uca-ebc-rhelcluster

Hit Submit button after entering all the details.



Script

Name	uca-ebc
Full Path to Script File	su uca /opt/UCA-EBC/
Independent Subtree	□
Non-Critical Resource	□

Independent Subtree/Non-Critical Options

Maximum Number of Failures	
Failure Expire Time (seconds)	
Maximum Number of Restarts	
Restart Expire Time (seconds)	

Adding IP address as a resource

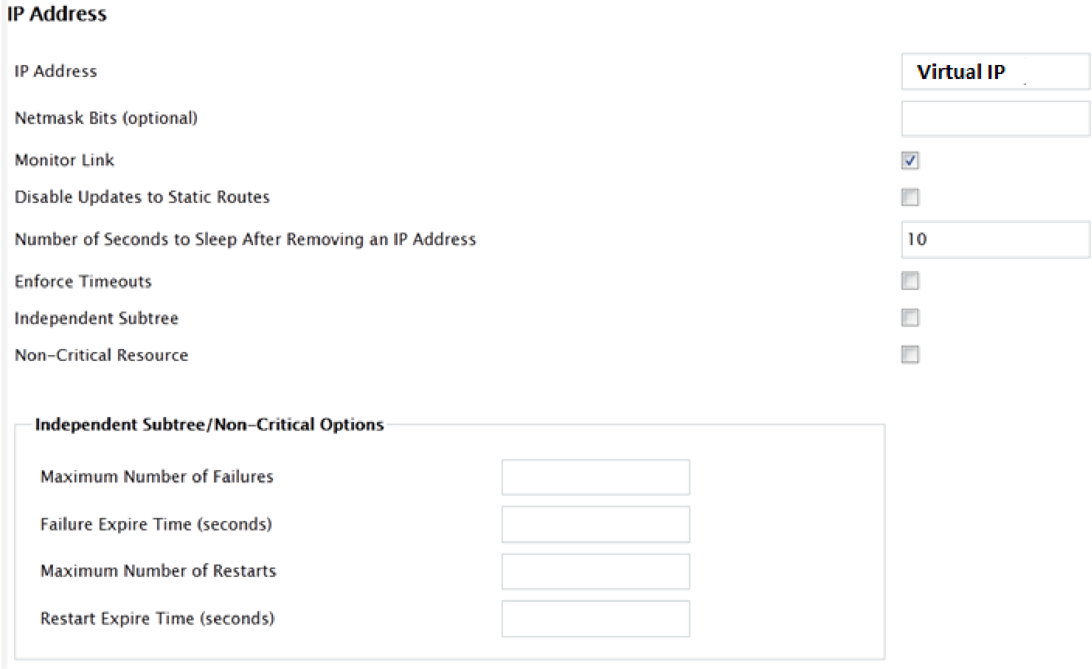
In the Service Groups tab, click on the UCA-EBC service, and then on the Add Resource button.

Then from the dropdown list choose IP Address.

Mention the details as shown in the screenshot that follows:

In the IP Address field, mention the virtual IP that would be used to access all the nodes in this cluster

Hit Submit button after entering all the details.



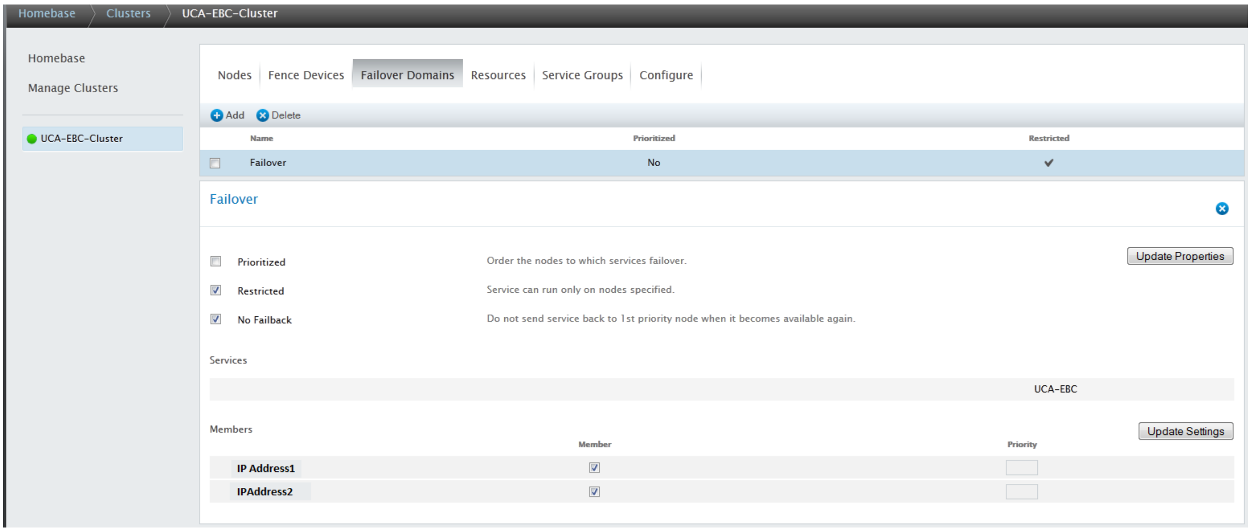
IP Address

IP Address	Virtual IP
Netmask Bits (optional)	
Monitor Link	☑
Disable Updates to Static Routes	□
Number of Seconds to Sleep After Removing an IP Address	10
Enforce Timeouts	□
Independent Subtree	□
Non-Critical Resource	□

Independent Subtree/Non-Critical Options

Maximum Number of Failures	
Failure Expire Time (seconds)	
Maximum Number of Restarts	
Restart Expire Time (seconds)	

Ensure to configure a failover domain as shown below:



Homebase 〉 Clusters 〉 UCA-EBC-Cluster

Homebase

Manage Clusters

● UCA-EBC-Cluster

Nodes | Fence Devices | Failover Domains | Resources | Service Groups | Configure

Add Delete

	Name	Prioritized	Restricted
☐	Failover	No	✓

Failover

☐	Prioritized	Order the nodes to which services failover.
☑	Restricted	Service can run only on nodes specified.
☑	No Failback	Do not send service back to 1st priority node when it becomes available again.

Update Properties

Services

UCA-EBC

Members

Update Settings

	Member	Priority
IP Address1	☑	
IPAddress2	☑	

Note

Useful link describing how to configure Redhat Cluster
http://www.golinuxhub.com/2014/02/configure-red-hat-cluster-using-vmware.html

Note

For shared data directory, configure a shared Disc (NFS was used for validation in this release) and mention the shared directory as a resource at the cluster level. Kindly note, it’s not at the service level. The script and IP address resources are added at service level.

Note

Ensure that mounted shared data directory has write permission from all systems

Note

By default OM listens on port 162 for traps. Please make sure this port is not occupied by any other service if the default port is used.

Note

Edit the /etc/sudoers file in both the systems where UCA-EBC and OM is installed. Comment the below property:

```
#Defaults    requiretty
```

Note

Navigate to / <UCA-EBC HOME>/bin directory, replace the existing uca-ebc-rhelcluster file with below contents and provide the respective UCA-EBC and NOM home directories.

```
#!/bin/sh
set -x
#=========================================================================#
#                                                     #
#              ****  COPYRIGHT NOTICE ****                      #
#                                                     #
#                                                     #
#    Copyright (c) Hewlett-Packard Corporation, 2012.                  #
#    All Rights Reserved.  Unpublished rights reserved                  #
#    under the copyright laws of the United States.                     #
#                                                                       #
#    The software contained on this media is proprietary                #
#    to and embodies the confidential technology of                     #
#    Hewlett-Packard Corporation.  Possession, use,                     #
#    duplication or dissemination of the software and                   #
#    media is authorized only pursuant to a valid written               #
#    license from Hewlett-Packard Corporation.                          #
#                                                                       #
#    RESTRICTED RIGHTS LEGEND   Use, duplication, or                    #
#    disclosure by the U.S. Government is subject to                    #
#    restrictions as set forth in Subparagraph (c)(1)(ii)               #
#    of the Rights in Technical Data and Computer Software              #
#    clause at DFARS 252.227-7013 or in FAR 52.227-19, as               #
#    applicable.                                                        #
#                                                                       #
#                                                                       #
#===========================================================================#
#
OSNAME=`uname -s | tr -d '-'`
if [ "$OSNAME" = "HPUX" ]; then
        echo "RHEL cluster not available on HP-UX ";
        exit 1;
fi
SUDO="sudo -i -u uca"
LOG_DIR=/var/tmp/ ; export LOG_DIR
DASH="---------------------"; export DASH
RC=0                    ; export RC        # Service Return Code
#
# Script for UCA-EBC handling through the Red Hat Enterprise Linux 6 High Availability Add-On (Cluster)
# Usage : uca-ebc-rhelcluster command [instance-name]
#
# Configuration of VCS resource for default instance:
#
#        GetStatusOfProgram    global     /opt/UCA-EBC/bin/uca-ebc-rhelcluster status
#        StartProgram          global     /opt/UCA-EBC/bin/uca-ebc-rhelcluster start
#        StopProgram           global     /opt/UCA-EBC/bin/uca-ebc-rhelcluster stop
#
echo "testing..." >> tmp.txt
[ "${UCA_EBC_HOME}" = "" ] && UCA_EBC_HOME="<UCA-EBC Home Directory>"
DEFAULT_INSTANCE=default
[ "${OM_HOME}" = "" ] && OM_HOME="<NOM Home Directory>"
[ "$2" = "" ] && INSTANCE=${DEFAULT_INSTANCE} || INSTANCE=$2
ONLINE=110
ALIVE=105
OFFLINE=100
echo "$1" >> tmp.txt
case "$1" in
start)
echo "inside start"
     echo  "${DASH}" >> ${LOG_DIR}/rhelcluster-uca-service-start.out 2>&1
     echo "starting UCA-EBC"
     ${SUDO} ${UCA_EBC_HOME}/bin/uca-ebc -i ${INSTANCE} start -v &> ${LOG_DIR}/rhelcluster-uca-service-start.out
     ${OM_HOME}/bin/nom_admin --start-container &> ${LOG_DIR}/rhelcluster-uca-service-start.out
     RC=$?
     FPID=`ps -ef |grep -v grep |grep -i "uca" |awk '{ print $2 }'|head -1`
     OMPID=`ps -ef |grep -v grep |grep -i "openmediation" |awk '{ print $2 }'|head -1`
     echo "Service UCA-EBC started - PID=${FPID} RC=$RC">> ${LOG_DIR}/rhelcluster-uca-service-start.out
     echo "Service OpenMediation started - PID=${OMPID} ">> ${LOG_DIR}/rhelcluster-uca-service-start.out
     echo "${DASH}" >> ${LOG_DIR}/rhelcluster-uca-service-start.out 2>&1
     exit 0
     ;;
stop)
echo "inside stop" >> tmp.txt
    echo  "${DASH}" >> ${LOG_DIR}/rhelcluster-uca-service-stop.out 2>&1
    echo "stopping UCA-EBC"
    ${SUDO}  ${UCA_EBC_HOME}/bin/uca-ebc -i ${INSTANCE} stop  | tee ${LOG_DIR}/rhelcluster-uca-service-stop.out
    ${OM_HOME}/bin/nom_admin --shutdown-container  | tee ${LOG_DIR}/rhelcluster-uca-service-stop.out
    exit 0
    ;;
status)
echo "status  param" >> tmp.txt
 ${OM_HOME}/bin/nom_admin --list-container | tee ${LOG_DIR}/rhelcluster-uca-service-status.out && grep "STARTED" ${LOG_DIR}/rhelcluster-uca-service-status.out >/dev/null && ${SUDO} ${UCA_EBC_HOME}/bin/uca-ebc -i ${INSTANCE} show 2>&1 | tee ${LOG_DIR}/rhelcluster-uca-service-status.out && grep "Server is running" ${LOG_DIR}/rhelcluster-uca-service-status.out >/dev/null && exit 0
      # at the end, UCA-EBC is not running
      exit ${OFFLINE}
      ;;
esac
```

3.15 UCA Automation setup

3.15.1 Configuring HP UCA for EBC

For instructions on how to configure HP UCA for EBC, refer to the “Section 4.7.1 Configure HP UCA for EBC” in the HP NFV Director Installation and Configuration Guide”.

Note

Follow the same procedure on both Primary and Failover nodes.

3.15.2 Installing UCA Automation Solution and Patch

For instructions on how to install the UCA Automation Solution, refer to the “Section 4.7.2 Installing UCA Automation Solution” and “Section 4.7.3 Installing UCA Automation Patch” in the HP NFV Director Installation and Configuration Guide”.

Note

Follow the same procedure on both Primary and Failover nodes.

3.15.3 Installing UCA Automation’s HPSA Foundation Solution Pack

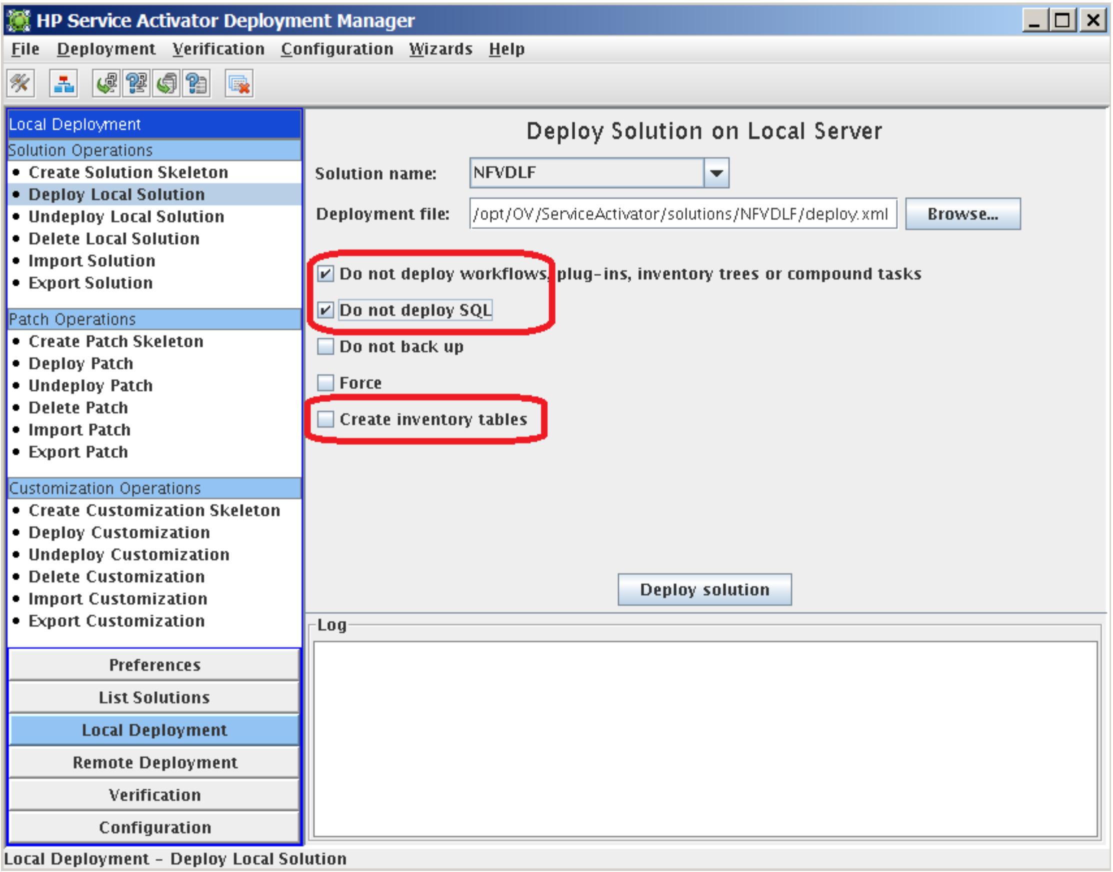
For instructions on how to install the UCA Automation’s HPSA Foundation Solution Pack, refer to the “Section 4.7.6 Installing UCA Automation’s HPSA Foundation Solution Pack” in the HP NFV Director Installation and Configuration Guide”.

Note

Follow the same procedure on both Primary and Failover nodes except the below listed Note.

Note

During deployment of HPSA Foundation Solution pack in the **other nodes** using Deployment Manager, make sure the checkboxes shown in below screen are always checked and others unchecked. A sample deployment window on other nodes is depicted below.



Solution name: NFVDLF

Deployment file: /opt/OV/ServiceActivator/solutions/NFVDLF/deploy.xml

☑ Do not deploy workflows, plug-ins, inventory trees or compound tasks

☑ Do not deploy SQL

☐ Do not back up

☐ Force

☐ Create inventory tables

3.15.4 Installing UCA Automation's UCA for EBC Foundation Value Pack

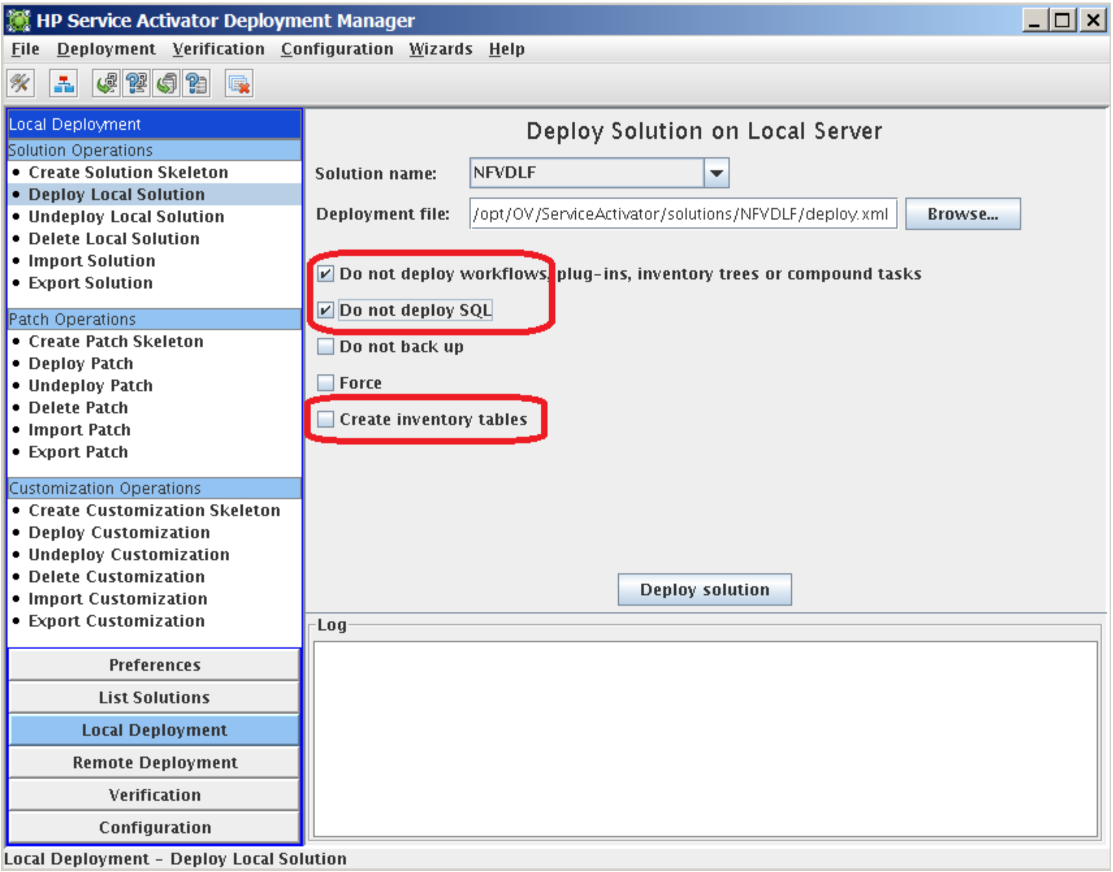
For instructions on how to install the UCA Automation UCA for EBC Foundation Value Pack, refer to the "Section 4.7.7 Installing UCA Automation's UCA for EBC Foundation Value Pack" in the HP NFV Director Installation and Configuration Guide".

Note

Follow the same procedure on both Primary and Failover nodes except the below listed Note.

Note

During deployment of EBC Foundation Value pack in the **other nodes** using Deployment Manager, make sure the checkboxes shown in below screen are always checked and others unchecked. A sample deployment window on other nodes is depicted below.



Solution name: NFVDLF

Deployment file: /opt/OV/ServiceActivator/solutions/NFVDLF/deploy.xml

☑ Do not deploy workflows, plug-ins, inventory trees or compound tasks

☑ Do not deploy SQL

☐ Do not back up

☐ Force

☐ Create inventory tables

3.15.5 Installing UCA automation NFVD packs

For instructions on how to install the UCA automation NFVD packs, refer to the “Section 5.5.4.1 Installing UCA Automation NFVD HPSA SP” in the HP NFV Director Installation and Configuration Guide”. However, read the Notes below before proceeding with the installation.

Note

Follow the instructions as specified in “Section 5.5.1 Installing assurance gateway scripts” in the HP NFV Director Installation and Configuration Guide before performing installation of UCA Automation NFVD Packs.

Also perform the installation first on Primary node followed by Failover node

3.15.6 Installing Channel Adapters on Primary and Failover nodes

For instructions on how to install the UCA EBC CA, refer to the “Section 4.6.1 Installing UCA for EBC CA” in the HP NFV Director Installation and Configuration Guide”.

For instructions on how to install the Generic SNMP CA, refer to the “Section 4.6.2 Installing Generic SNMP CA” in the HP NFV Director Installation and Configuration Guide”.

For instructions on how to install the SiteScope CA, refer to the “Section 4.6.3 Installing SiteScope Customization for Generic SNMP CA” in the HP NFV Director Installation and Configuration Guide”.

For instructions on how to install the VMWARE ESXi CA, refer to the “Section 4.6.4 Installing VMWare ESXi Customization for Generic SNMP CA” in the HP NFV Director Installation and Configuration Guide”.

For instructions on how to install the UCA HPSA CA, refer to the “Section 4.7.4 Installing UCA HPSA CA” in the HP NFV Director Installation and Configuration Guide”.

For instructions on how to install the UCA Automation Console CA, refer to the “Section 4.7.5 Installing UCA Automation Console CA” in the HP NFV Director Installation and Configuration Guide”.

For instructions on how to install the NFVD Capacity Management CAs, refer to the “Section 5.5.8 Installing NFVD Capacity Management Components” in the HP NFV Director Installation and Configuration Guide”.

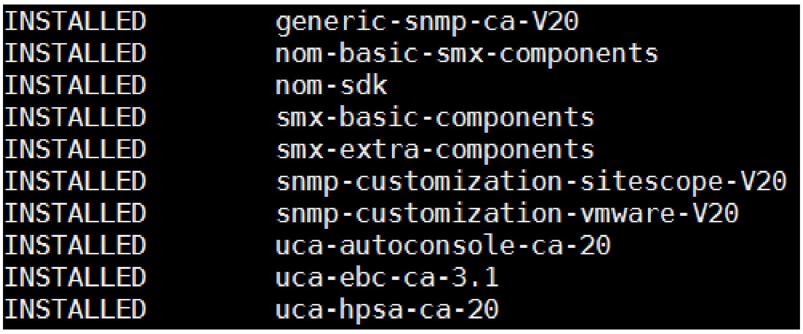
Note

Follow the same procedure on both Primary and Failover nodes.

Note

After successfully installing all Channel Adapters, verify the same by running the command on both primary and failover nodes.

```
# /opt/openmediation-70/bin/nom_admin --list-ip-in-container
```



```
INSTALLED        generic-snmp-ca-V20
INSTALLED        nom-basic-smx-components
INSTALLED        nom-sdk
INSTALLED        smx-basic-components
INSTALLED        smx-extra-components
INSTALLED        snmp-customization-sitescope-V20
INSTALLED        snmp-customization-vmware-V20
INSTALLED        uca-autoconsole-ca-20
INSTALLED        uca-ebc-ca-3.1
INSTALLED        uca-hpsa-ca-20
```

3.16 Assurance Gateway setup

For instructions on how to install Assurance Gateway:

Refer to the “Section 5.5.1 Installing assurance gateway scripts” in the HP NFV Director Installation and Configuration Guide”.

Refer to the “Section 5.5.2 NFVD Assurance third-party products” in the HP NFV Director Installation and Configuration Guide”.

Refer to the “Section 5.5.3 Installing Assurance gateway core” in the HP NFV Director Installation and Configuration Guide”.

Note

Follow the same procedure on both Assurance nodes.

3.17 Installation and Configuration of RHEL High-Availability Add-On

Note

Installation of Clustering software is illustrated using Redhat Clustering

software.
'yum' tool is used for installation in this example. Ensure that yum has access to "High Availability" and "Resilient Storage" rpms

3.17.1 Installation of RHEL High-Availability Add-On

Configure local yum repository and run the below 2 commands on all the nodes in the cluster

```
# yum -y groupinstall "High Availability"
# yum -y groupinstall "Resilient Storage"
```

Install the 'luci' component on the management node in the cluster.

Note

Execute the below command to install the luci component only on the node chosen to become the management node of the cluster.

```
# yum -y install luci ccs
```

Ensure that the following RPMs are installed.

```
# rpm -qa | grep ccs
ccs-0.16.2-63.el6.x86_64

# rpm –qa | grep cman
cman-3.0.12.1-49.el6.x86_64

# rpm -qa | grep omping
omping-0.0.4-1.el6.x86_64

# rpm -qa | grep rgmanager
rgmanager-3.0.12.1-17.el6.x86_64
```

On the management node,

```
# rpm -qa | grep luci
luci-0.26.0-37.el6.x86_64
```

3.17.2 Configuration of RHEL High-Availability Add-On

Execute following commands: replace 255.255.248.0/24 with the appropriate subnet mask and CIDR

```
# iptables -I INPUT -m state --state NEW -m multiport -p udp -s 255.255.248.0/24 -d 255.255.248.0/24 --dports
5404,5405 -j ACCEPT

# iptables -I INPUT -m addrtype --dst-type MULTICAST -m state --state NEW -m multiport -p udp -s
255.255.248.0/24 --dports 5404,5405 -j ACCEPT

# iptables -I INPUT -m state --state NEW -p tcp -s 255.255.248.0/24 -d 255.255.248.0/24 --dport 21064 -j
ACCEPT

# iptables -I INPUT -m state --state NEW -p tcp -s 255.255.248.0/24 -d 255.255.248.0/24 --dport 11111 -j
ACCEPT

# iptables -I INPUT -m state --state NEW -p tcp -s 255.255.248.0/24 -d 255.255.248.0/24 --dport 16851 -j
ACCEPT

# iptables -I INPUT -m state --state NEW -p tcp -s 255.255.248.0/24 -d 255.255.248.0/24 --dport 8084 -j ACCEPT

# iptables -I INPUT -p igmp -j ACCEPT
# service iptables save ; service iptables restart
iptables: Saving firewall rules to /etc/sysconfig/iptables:[  OK  ]
iptables: Flushing firewall rules:                         [  OK  ]
iptables: Setting chains to policy ACCEPT: filter          [  OK  ]
iptables: Unloading modules:                               [  OK  ]
iptables: Applying firewall rules:                         [  OK  ]
```

Set password for 'ricci' user on all the nodes in the cluster as follows.

Note

This password must be provided while creating the cluster in Step 7.

```
# passwd ricci
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
```

3.17.3 Starting RHEL High-Availability Add-On services

Start ricci by using 'service ricci start' and enable it to start at boot time via chkconfig

```
# service ricci start
Starting oddjobd:                                      [  OK  ]
generating SSL certificates...  done
Generating NSS database...  done
Starting ricci:                                        [  OK  ]

# chkconfig ricci on
```

Start luci as follows only on the node chosen to be management node (or enable it to start at boot time via chkconfig)

Note

Management Node is the node chosen in Step 2 above.

```
# service luci start
Adding following auto-detected host IDs (IP addresses/domain names), corresponding to `nfvdvm46.ind.hp.com'
address, to the configuration of self-managed certificate `/var/lib/luci/etc/cacert.config' (you can change them by
editing `/var/lib/luci/etc/cacert.config', removing the generated certificate `/var/lib/luci/certs/host.pem' and
restarting luci):
        (none suitable found, you can still do it manually as mentioned above)

Generating a 2048 bit RSA private key
writing new private key to '/var/lib/luci/certs/host.pem'
Start luci...                                          [  OK  ]
Point your web browser to https://nfvdvm46.ind.hp.com:8084 (or equivalent) to access luci
```

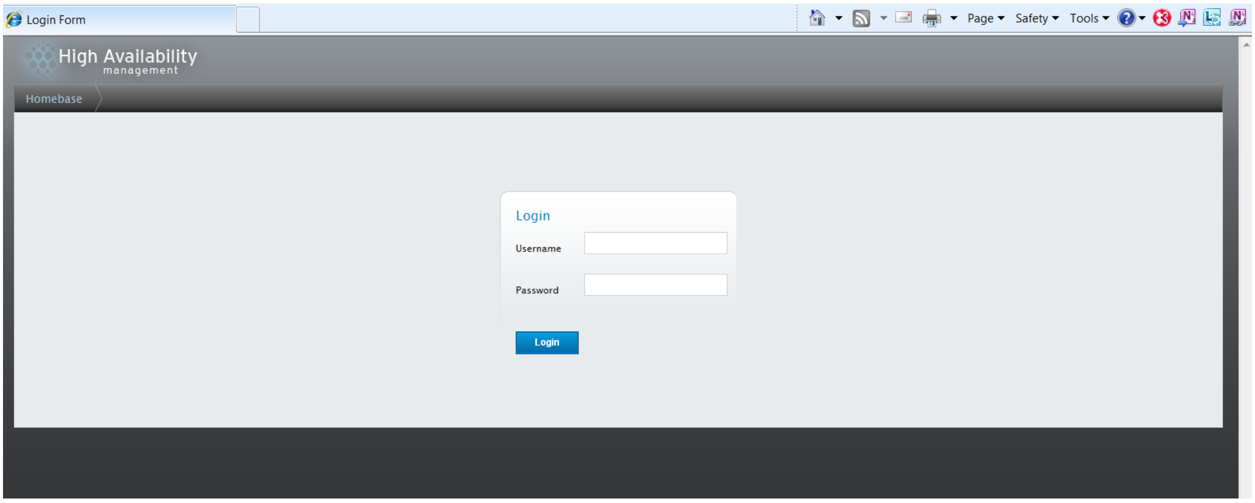
3.17.4 Access Luci Management console

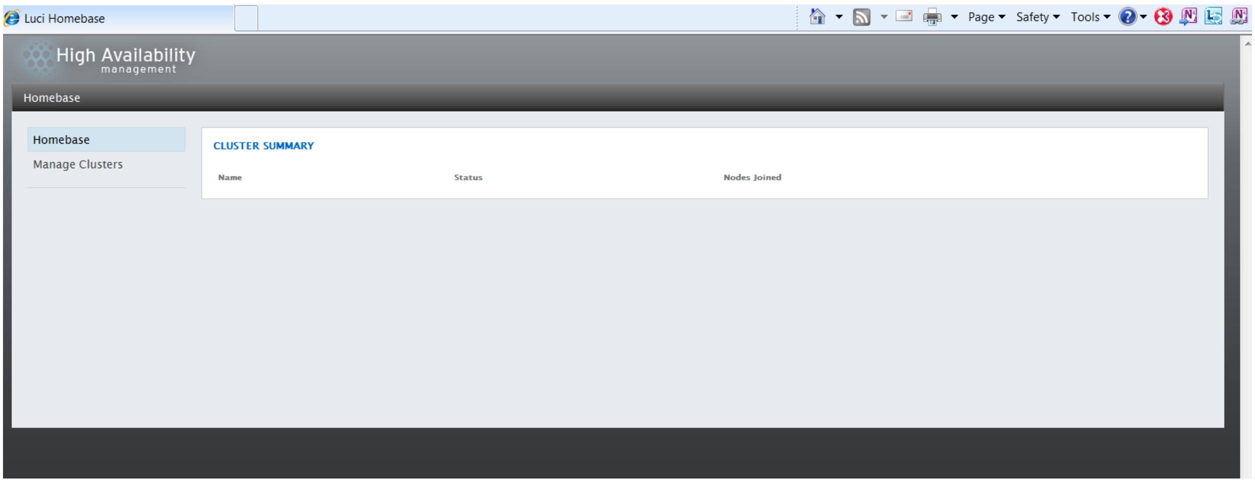
Luci Management Console UI can be accessed at

https://<IP_address_of_server_where_luci_is_installed>:8084

Note

Login credentials are the same as the root credentials for the server on which luci is installed.



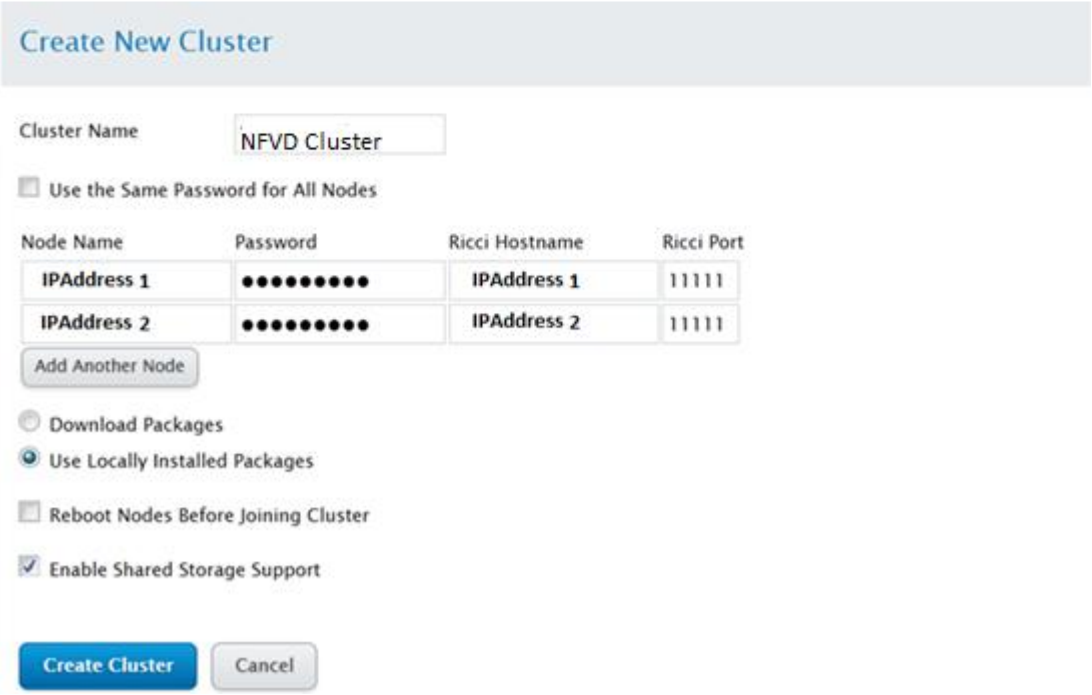


3.17.5 Cluster configurations

Click on Manage Clusters-> Create

Note

The ricci password is the password created in Step 5; use "Add Another Node" button to add details of subsequent nodes in the cluster. Hit "Create Cluster" button when details of all the nodes in the cluster have been added.



Create New Cluster

Cluster Name: NFVD Cluster

□ Use the Same Password for All Nodes

Node Name	Password	Ricci Hostname	Ricci Port
IPAddress 1	●●●●●●●●●	IPAddress 1	11111
IPAddress 2	●●●●●●●●●	IPAddress 2	11111

○ Download Packages

● Use Locally Installed Packages

□ Reboot Nodes Before Joining Cluster

☑ Enable Shared Storage Support

Stop NetworkManager before starting Cluster Manager [cman]

```
# service NetworkManager stop
# chkconfig NetworkManager off
# /etc/init.d/cman start
Starting cluster:
   Checking if cluster has been disabled at boot...        [  OK  ]
   Checking Network Manager...                             [  OK  ]
   Global setup...                                         [  OK  ]
   Loading kernel modules...                               [  OK  ]
   Mounting configfs...                                    [  OK  ]
   Starting cman...                                        [  OK  ]
   Waiting for quorum...                                   [  OK  ]
   Starting fenced...                                      [  OK  ]
   Starting dlm_controld...                                [  OK  ]
   Tuning DLM kernel config...                             [  OK  ]
   Starting gfs_controld...                                [  OK  ]
   Unfencing self...                                       [  OK  ]
   Joining fence domain...                                 [  OK  ]
```

Note

Start cman on other node(s) in the cluster

Start CLVMD service:

```
# /etc/init.d/clvmd start
Starting clvmd:
Activating VG(s):   2 logical volume(s) in volume group "vg_nfvdvm" now active
  clvmd not running on node <IP Address2>     … this suggests that this clvmd service should be started on the other node(s) in the cluster
                                                   [  OK  ]
```

Upon starting clvmd on other node, the output is as follows:

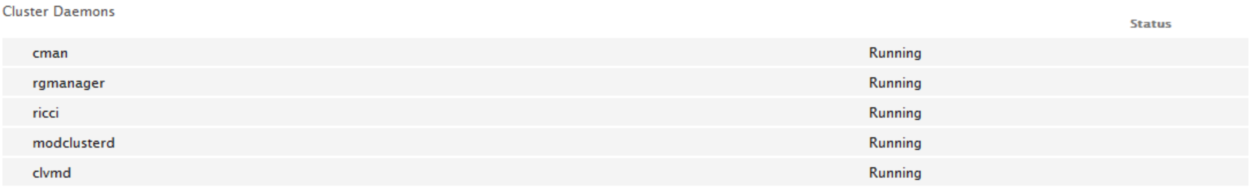
```
# /etc/init.d/clvmd start
Starting clvmd:
Activating VG(s):   2 logical volume(s) in volume group "vg_nfvdvm" now active
```

```
# chkconfig  clvmd on
```

Start RGMANAGER:

```
# /etc/init.d/rgmanager start
Starting Cluster Service Manager:                       [  OK  ]

# chkconfig rgmanager on
```

Click on each node listed in the cluster and ensure that all components are running as can be seen below:



Cluster Daemons

	Status
cman	Running
rgmanager	Running
ricci	Running
modclusterd	Running
clvmd	Running

Note

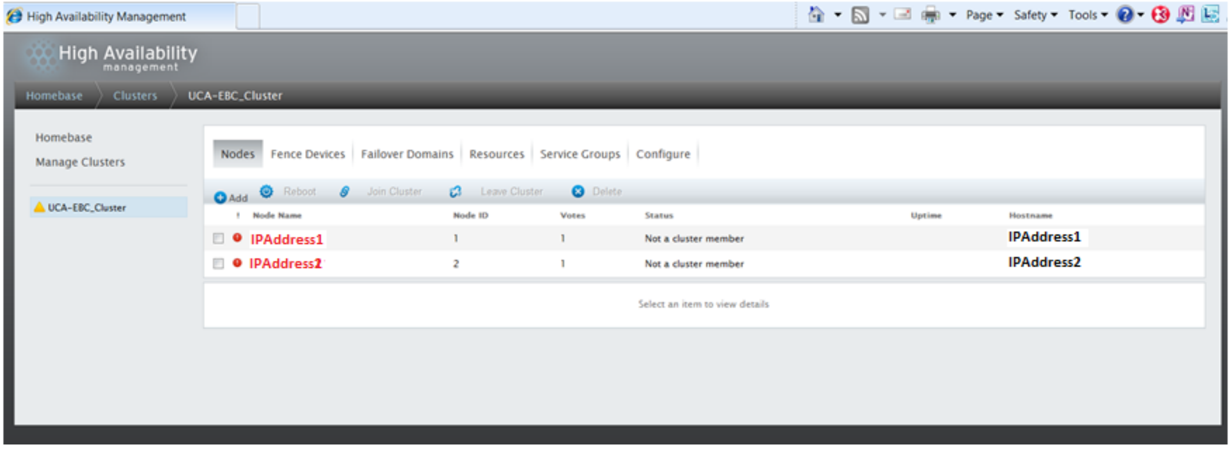
Fencing has not been setup here

Note

If there are issues with opening on the UI, change the browser and check; IE or Mozilla is preferred. Issues seen with Chrome.

Note

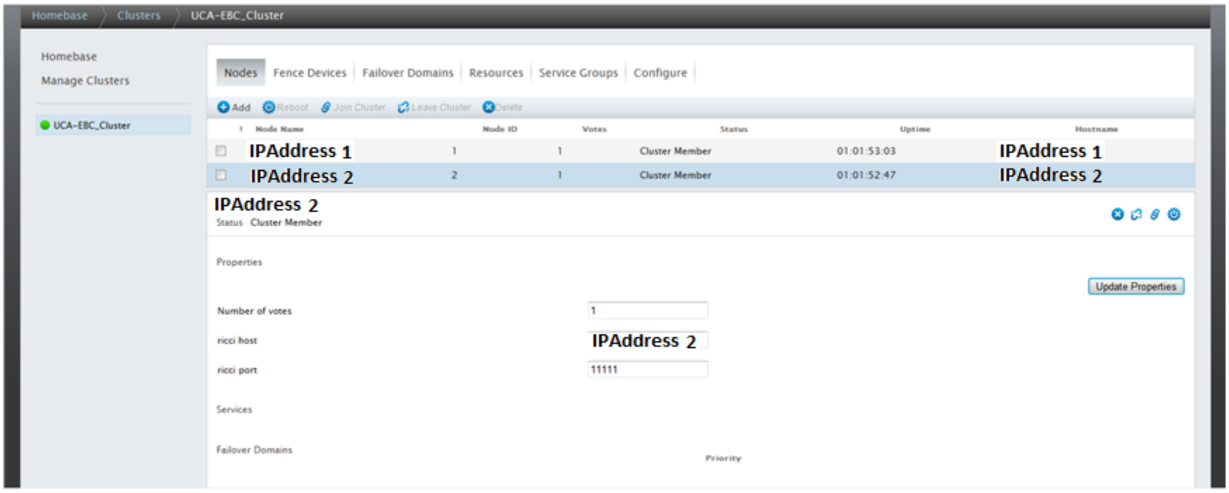
If you get the following screen showing nodes in red, then click on the node to see if any of the above services are 'not running'



!	Node Name	Node ID	Votes	Status	Uptime	Hostname
□ ●	IPAddress1	1	1	Not a cluster member		IPAddress1
□ ●	IPAddress2	2	1	Not a cluster member		IPAddress2

Select an item to view details

Screen showing successfully setup cluster:



	Node Name	Node ID	Votes	Status	Uptime	Hostname
□	IPAddress 1	1	1	Cluster Member	01:01:53:03	IPAddress 1
□	IPAddress 2	2	1	Cluster Member	01:01:52:47	IPAddress 2

IPAddress 2

Status Cluster Member

Properties

Number of votes: 1

ricci host: IPAddress 2

ricci port: 11111

Services

Failover Domains

Priority

Note

Always follow the same order for stopping/starting the cluster as shown below:

Stopping Cluster services

On each node: # service rgmanager stop
On each node: # service clvmd stop
On each node: # service cman stop

Starting Cluster services

On each node: # service cman start
On each node: # service clvmd start
On each node: # service rgmanager start

Configuring Assurance Gateway as a service:

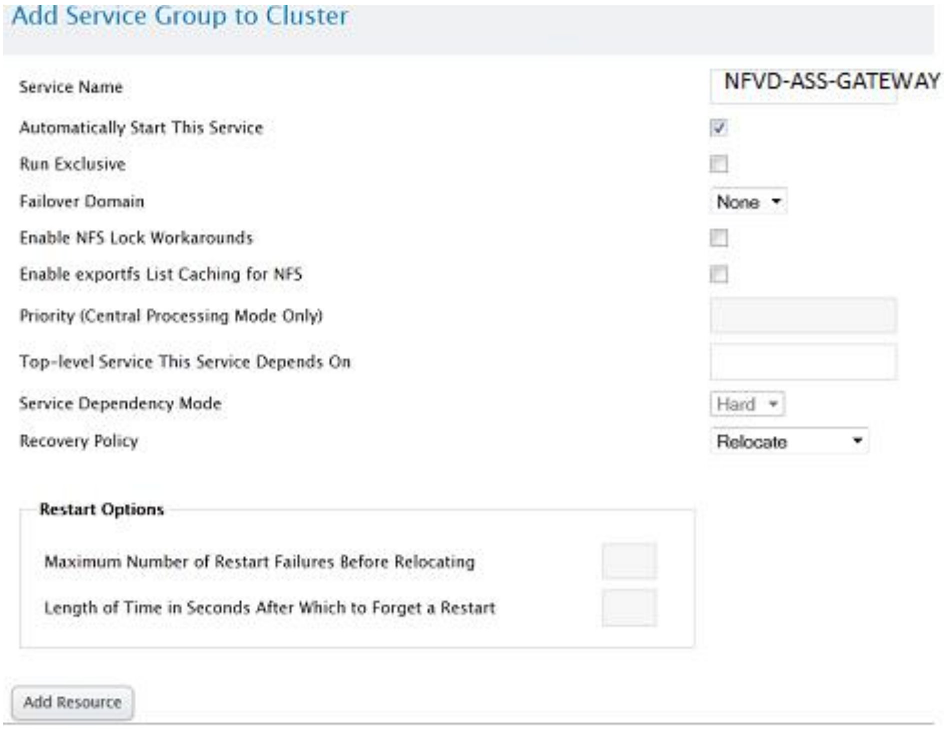
Note

This worked on Mozilla only. https://<IP>:<port>/cluster/UCA-EBC_Cluster/services

Declare Assurance Gateway service. It will be created in the cluster as a service group.

From the cluster-specific page, add the NFVD-ASSURANCE-GATEWAY service to that cluster by

- Clicking on "Service Groups" along the top of the cluster display.
- Click Add. This displays the Add Service Group to Cluster dialog box.
- On the Add Service Group to Cluster dialog box, at the Service Name text box, type the name of the Assurance Gateway service for Assurance Gateway. e.g. NFVD-ASSURANCE-GATEWAY
- Check the Automatically Start This Service checkbox if you want the Assurance Gateway service to start automatically when the cluster is started.
- Use the Recovery Policy drop-down box to select a recovery policy for the service. We recommend to use the option 'Relocate', and ignore the restart options



Add Service Group to Cluster

Service Name	NFVD-ASS-GATEWAY
Automatically Start This Service	☑
Run Exclusive	□
Failover Domain	None ▾
Enable NFS Lock Workarounds	□
Enable exportfs List Caching for NFS	□
Priority (Central Processing Mode Only)	
Top-level Service This Service Depends On	
Service Dependency Mode	Hard ▾
Recovery Policy	Relocate ▾

Restart Options

Maximum Number of Restart Failures Before Relocating	
Length of Time in Seconds After Which to Forget a Restart	

Adding resources for ASSURANCE GATEWAY HA service:

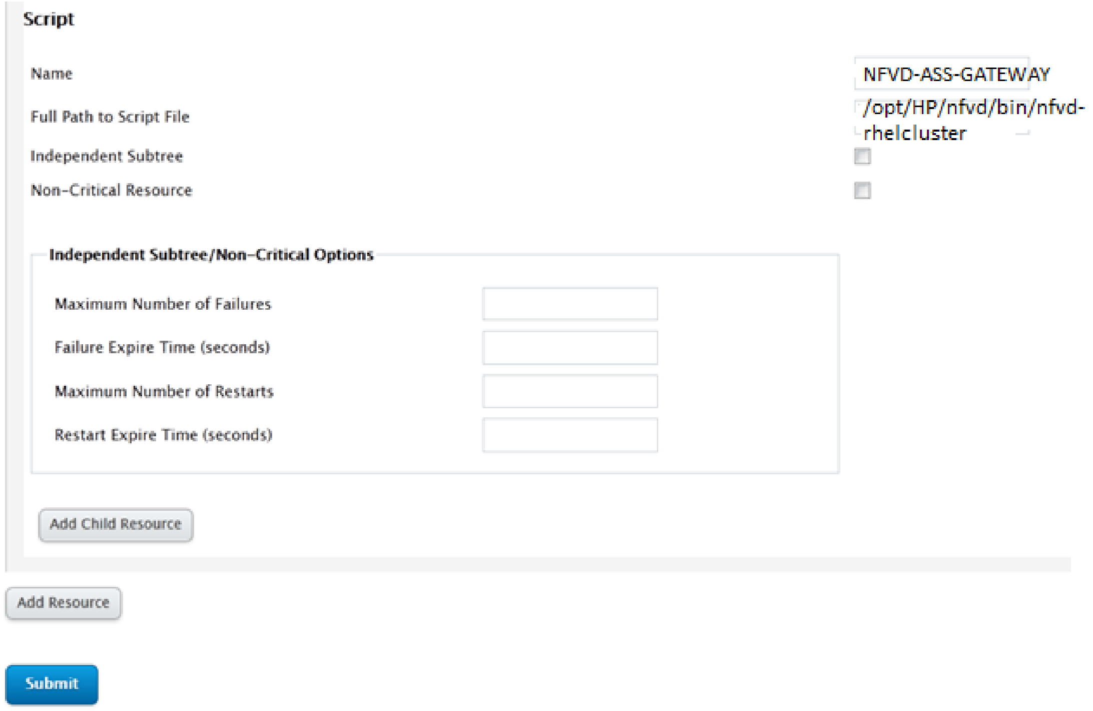
In the Service Groups tab, click on the NFVD CLUSTER service, and then click on the Add Resource button.

Then from the dropdown list choose Script

Mention the details as shown in the screenshot that follows:

In the “Full Path to Script File” mention: su /opt/HP/nfvd/bin/nfvd-rhelcluster

Hit Submit button after entering all the details.



Script

Name	NFVD-ASS-GATEWAY
Full Path to Script File	/opt/HP/nfvd/bin/nfvd-rhelcluster
Independent Subtree	□
Non-Critical Resource	□

Independent Subtree/Non-Critical Options

Maximum Number of Failures	
Failure Expire Time (seconds)	
Maximum Number of Restarts	
Restart Expire Time (seconds)	

Adding IP address as a resource

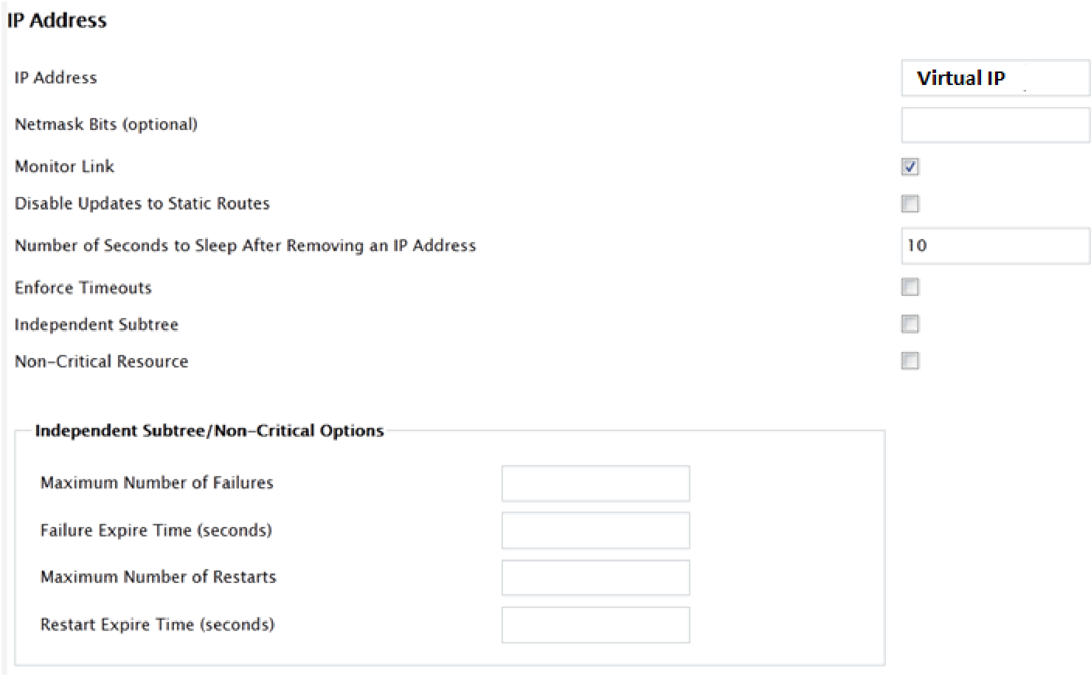
In the Service Groups tab, click on the NFVD-ASS-GATEWAY service, and then on the Add Resource button.

Then from the dropdown list choose IP Address.

Mention the details as shown in the screenshot that follows:

In the IP Address field, mention the virtual IP that would be used to access all the nodes in this cluster

Hit Submit button after entering all the details.



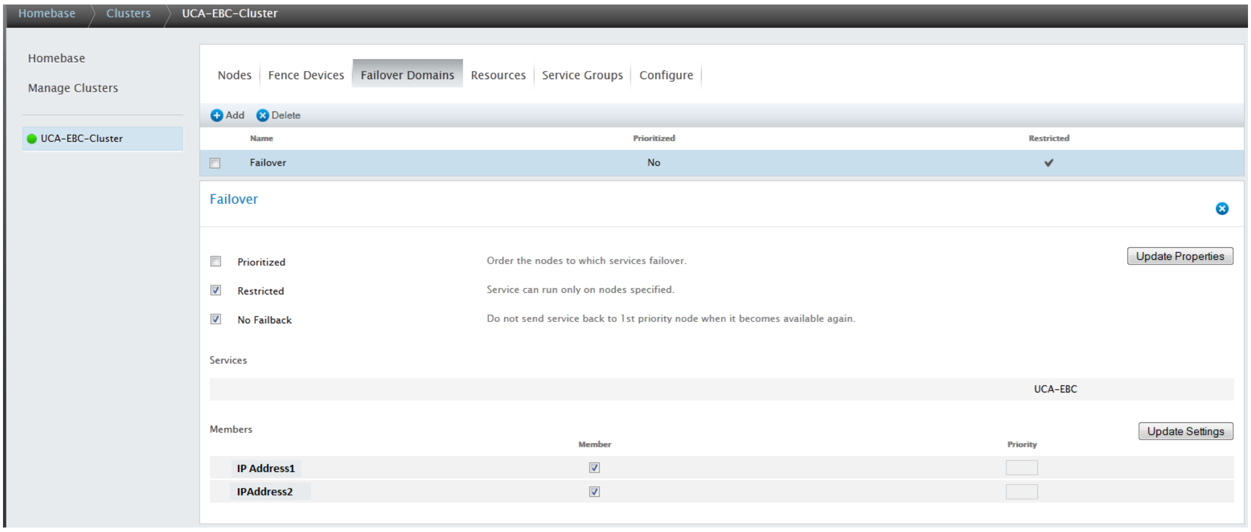
IP Address

IP Address	Virtual IP
Netmask Bits (optional)	
Monitor Link	☑
Disable Updates to Static Routes	□
Number of Seconds to Sleep After Removing an IP Address	10
Enforce Timeouts	□
Independent Subtree	□
Non-Critical Resource	□

Independent Subtree/Non-Critical Options

Maximum Number of Failures	
Failure Expire Time (seconds)	
Maximum Number of Restarts	
Restart Expire Time (seconds)	

Ensure to configure a failover domain as shown below:



Homebase 〉 Clusters 〉 UCA-EBC-Cluster
Homebase
Manage Clusters
● UCA-EBC-Cluster
Nodes | Fence Devices | Failover Domains | Resources | Service Groups | Configure
Add
Delete
Update Properties
Update Settings

	Name	Prioritized	Restricted
□	Failover	No	✓

Failover

□	Prioritized	Order the nodes to which services failover.
☑	Restricted	Service can run only on nodes specified.
☑	No Failback	Do not send service back to 1st priority node when it becomes available again.

Services

UCA-EBC

Members

	Member	Priority
IP Address1	☑	
IPAddress2	☑	

Note

Useful link describing how to configure Redhat Cluster
http://www.golinuxhub.com/2014/02/configure-red-hat-cluster-using-vmware.html

Note

Edit the /etc/sudoers file in both the systems where UCA-EBC and OM is installed. Comment the below property:

```
#Defaults    requiretty
```

Note

Restart the Service Group in NFVD cluster using the below command

```
/usr/sbin/clusvcadm –R  “NFVD-ASS-GATEWAY”
```

Note

Navigate to /opt/HP/nfvd/bin directory, create new file nfvd-rhelcluster,replace the nfvd-rhelcluster file with below contents

```
#!/bin/sh
set -x
#==========================================================================#
#                                                  #
#               ****  COPYRIGHT NOTICE ****                   #
#                                                  #
#                                                  #
#    Copyright (c) Hewlett-Packard Corporation, 2012.              #
#    All Rights Reserved.  Unpublished rights reserved             #
#    under the copyright laws of the United States.              #
#                                                  #
#    The software contained on this media is proprietary           #
#    to and embodies the confidential technology of              #
#    Hewlett-Packard Corporation.  Possession, use,              #
#    duplication or dissemination of the software and            #
#    media is authorized only pursuant to a valid written          #
#    license from Hewlett-Packard Corporation.                 #
#                                                  #
#    RESTRICTED RIGHTS LEGEND   Use, duplication, or                #
#    disclosure by the U.S. Government is subject to             #
#    restrictions as set forth in Subparagraph (c)(1)(ii)        #
#    of the Rights in Technical Data and Computer Software         #
#    clause at DFARS 252.227-7013 or in FAR 52.227-19, as          #
#    applicable.                                          #
#                                                  #
#                                                  #
#==========================================================================#
#

OSNAME=`uname -s | tr -d '-'`

if [ "$OSNAME" = "HPUX" ]; then
        echo "RHEL cluster not available on HP-UX ";
        exit 1;
fi

LOG_DIR=/var/tmp/ ; export LOG_DIR
DASH="---------------------"; export DASH
RC=0                    ; export RC        # Service Return Code
#
# Script for UCA-EBC handling through the Red Hat Enterprise Linux 6 High Availability Add-On (Cluster)
# Usage : uca-ebc-rhelcluster command [instance-name]
#
# Configuration of VCS resource for default instance:
#
#        GetStatusOfProgram    global     /opt/HP/nfvd/bin/nfvd-rhelcluster status
#        StartProgram          global     /opt/HP/nfvd/bin/nfvd-rhelcluster start
#        StopProgram           global     /opt/HP/nfvd/bin/nfvd-rhelcluster stop
#


[ "${NFVD_ASS_GATEWAY}" = "" ] && NFVD_ASS_GATEWAY="/opt/HP/nfvd"

ONLINE=110
ALIVE=105
OFFLINE=100
case "$1" in
```

```
start)
echo "inside start"
    echo  "${DASH}" >> ${LOG_DIR}/rhelcluster-nfvd-cluster-start.out 2>&1
    echo "starting NFVD ASS GATEWAY"
     ${NFVD_ASS_GATEWAY}/bin/nfv-director.sh -a  start -c nfvd-agw &> ${LOG_DIR}/rhelcluster-nfvd-cluster-start.out
    RC=$?
    FPID=`ps -ef |grep -v grep |grep -i "nfvd" |awk '{ print $2 }'|head -1`
    echo "Service NFVD ASS GATEWAY started - PID=${FPID} RC=$RC">> ${LOG_DIR}/rhelcluster-nfvd-cluster-start.out
    echo "${DASH}" >> ${LOG_DIR}/rhelcluster-nfvd-cluster-start.out 2>&1
exit 0
    ;;


stop)
echo "inside stop" >> tmp.txt
   echo  "${DASH}" >> ${LOG_DIR}/rhelcluster-nfvd-cluster-stop.out 2>&1
   echo "stopping ASSURANCE GATEWAY"
    ${NFVD_ASS_GATEWAY}/bin/nfv-director.sh -a  stop -c nfvd-agw  | tee ${LOG_DIR}/rhelcluster-nfvd-cluster-stop.out
   exit 0
   ;;

status)
echo "status  param" >> tmp.txt
  ${NFVD_ASS_GATEWAY}/bin/nfv-director.sh -a  status -c nfvd-agw  2>&1 | tee ${LOG_DIR}/rhelcluster-nfvd-cluster-status.out && grep "HP Assurance Gateway application server is running" ${LOG_DIR}/rhelcluster-nfvd-cluster-status.out >/dev/null && exit 0

     # at the end,NFVD-ASSURANCE-GATEWAY is not running
     exit ${OFFLINE}
     ;;

esac
```

Note

Configure the property “FULFILLMENT_REST_URL” in /var/opt/HP/nfvd/conf/nfvd.properties to point to HPSA HA proxy ip and port in Assurance Gateway. Refer to the “Section 5.5.3 Installing Assurance gateway core” in the HP NFV Director Installation and Configuration Guide”.

Chapter 4

Auto Instantiation of Self-Monitoring for High Availability

This chapter provides an overview of how Assurance Engine in NFV Director provides self-monitoring capability for all High Availability components with in NFV Director. And provides the configuration to be done to achieve this capability.

4.1 Overview

The High Available Components in NFV Director are UCA-EBC, Open Mediation, NEO4J, HPSA, SiteScope and Assurance Gateway.

In Assurance Engine the High Available Components are related to each other with a relationship type “HA”.

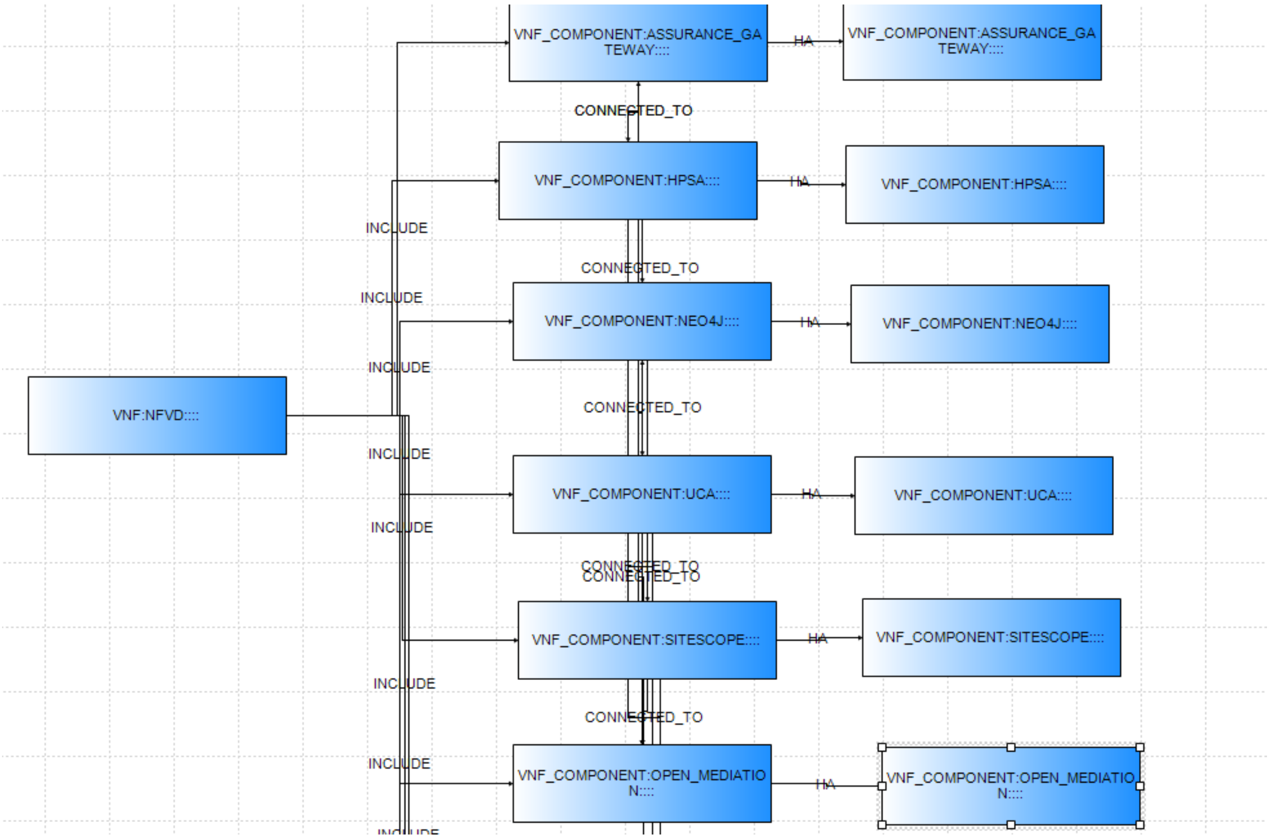
The process and logs of each of these High Available components in NFV Director are

Monitored in Assurance Engine and the monitors are deployed in the configured Sitescope.

4.1.1 Sample Instance to be installed

Below is an example of how the sample instance looks like. This sample instance is provided as part of installation in Assurance Gateway.

This sample instance needs to be loaded in Fulfillment Rest Sever, for the self-monitoring capability to work.



As seen above the High Available Components are related to each other with a relationship type “HA” in Assurance Engine.

4.2 Configuration

Certain configuration needs to be done for self-monitoring support for High Availability to work in Assurance Gateway.

Below is the list of configuration that’s needs to be done.

1. Auto Instantiation of SELF MONITORS is controlled by a flag which is by default true.

   Each of the above components have an attribute ENABLED, under the category MONITOR, Which is part of instances

   As shown below

```
<category>
        <attributes>
<attribute>
          <label>ENABLED</label>
           <description />
           <mandatory>true</mandatory>
           <order>5</order>
        <type>TEXT</type>
<unit>TEXT</unit>
 <value>true</value>
 </attribute>
                  </attributes>
                     <label>MONITOR</label>
  </category>
```

2. The hostUser, hostPassword needs to be provided in order to monitor the process/logs of each of the components mentioned above in point 1, these are part of instances. Its needs to be configured under Category Connection.

A sample of this configuration is shown below

```
<category>
<attributes>
<attribute>
   <label>hostUser</label>
                      <description />
                        <mandatory>true</mandatory
                            <order>3</order>
           <type>TEXT</type>
  <unit>TEXT</unit>
<value >root</value>
</attribute>
                 <attribute>
      <label>hostPassword</label>
              <description />
                        <mandatory>true</mandatory>
 <order>4</order>
                       <type>TEXT</type>
  <unit>TEXT</unit>
  <value>nfvd*help</value>
  </attribute>
 <attributes>
                 <label>CONNECTION</label>
   </category>
```

3. Once all the instances are loaded, the frequency of the SELF MONITORING, is controlled by this property SELF_MONITORS_RUN_FREQUENCY in nfvd. Properties this configuration is in minutes.

4. User need to specify which SiteScope the monitors need to deployed, which is configured in the instances for the VNFC_COMPONENT with artifact category SITESCOPE.

   a) Configure attributes appUser, appPassword under category CONNECTION sample is as shown below

```
<category>
<attributes>
<label>appUser</label>
 <description />
 <mandatory>true</mandatory>
  <order>3</order>
 <type>TEXT</type>
 <unit>TEXT</unit>
 <value >admin</value>
</attribute>
  <attribute> <label>appPassword</label>
         <description />
    <mandatory>true</mandatory>
     <order>4</order
   <type>TEXT</type>
  <unit>TEXT</unit>
  <value>admin</value
  </attribute>
 <attributes>
<label>CONNECTION</label>
        </category>
```

b) Configure the attribute IS_DEFAULT under category GENERAL, with value “true” as shown below

```
<attribute>
    <label>IS_DEFAULT</label>
    <description />
    <mandatory>true</mandatory>
    <order>3</order>
    <type>TEXT</type>
    <unit>TEXT</unit>
    <value>true</value>
   </attribute>
```

5. Once the interval is reached, all the process/log monitors for these components are deployed in the default SiteScope configured.

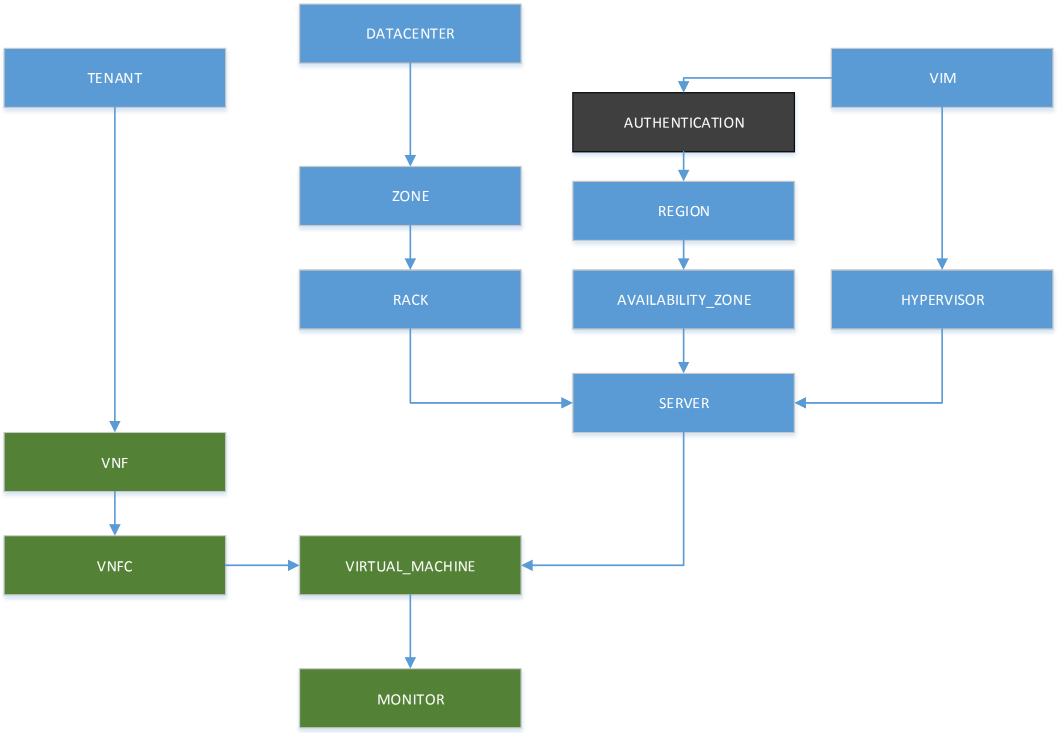
Chapter 5

Multiple SiteScope Instances

This chapter provides an overview of how multiple instances of SiteScopes can be configured to monitor KPIs at various levels, to distribute the load and to isolate the monitoring.

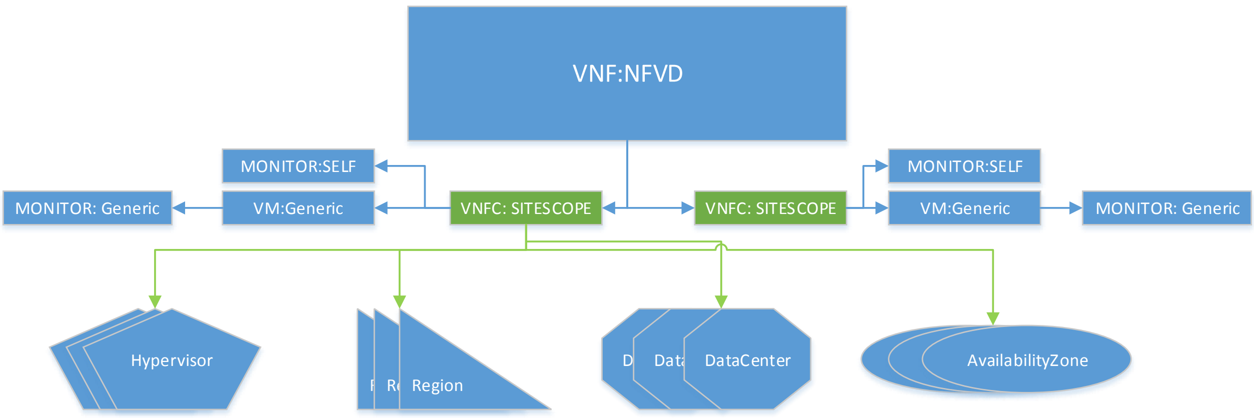
5.1 Overview

Different instances of SiteScope can be configured within a single NFVD setup, to monitor KPIs , based on defined criteria, like VIM , Data Center, Tenant, Zone, Rack, Region, AZ, Server and Hypervisor, as can be seen in blue boxes in the below figure.



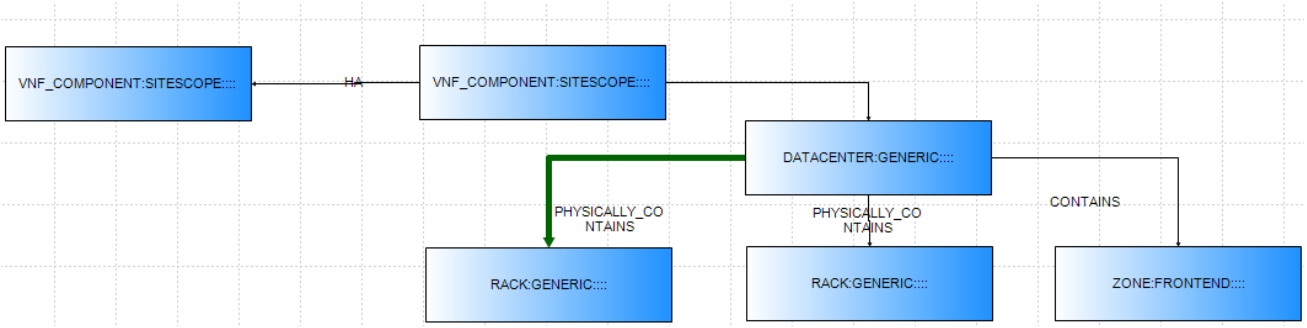
SiteScope artefact can be related to any of the artifacts in blue box as parent. NFVD will pick up the relevant SiteScope for monitor deployment.

If there are multiple SiteScope artifacts in the resource tree, then SiteScope is allocated based on the weightage attribute. For example: If SiS1 is associated at DC level, and SiS2 is associated at Hypervisor level, and a VM is created under the Server that is managed by the above Hypervisor, and is in this DC, both the SiteScope instances are eligible to monitor this VM. The SiteScope is chosen in this situation based on the weightage attribute; SiteScope with higher weightage is chosen. VNFC:SITESCOPE > GENERAL.WEIGHTAGE. See Installation Guide for more details on this attribute.

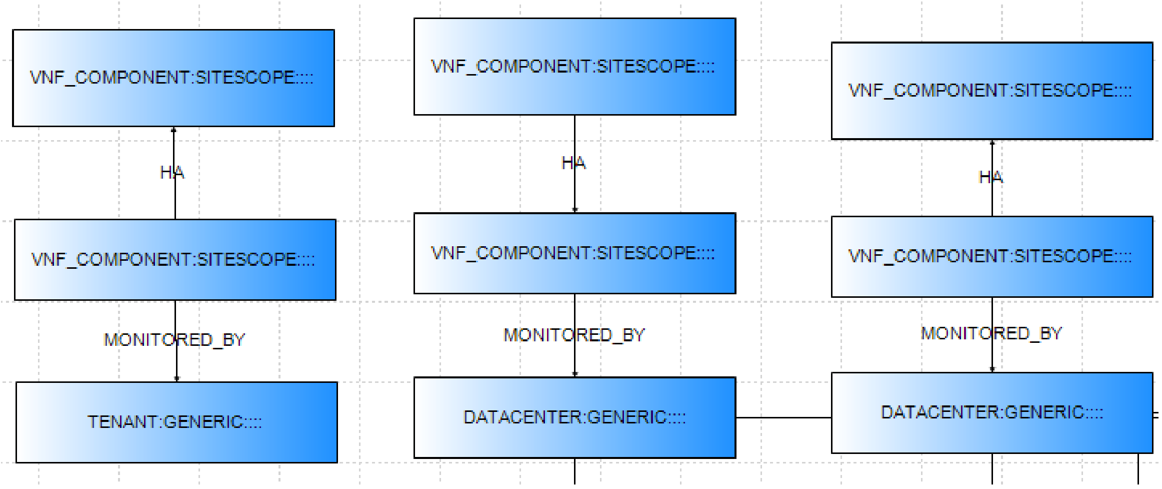


5.2 Multi SiteScope in HA

Snippet data with DC level multi SiS HA is as shown below



Snippet data with 2 Data Center, 1 Tenant multi SiS HA


VNF_COMPONENT:SITESCOPE::::
VNF_COMPONENT:SITESCOPE::::
VNF_COMPONENT:SITESCOPE::::
HA
HA
HA
VNF_COMPONENT:SITESCOPE::::
VNF_COMPONENT:SITESCOPE::::
VNF_COMPONENT:SITESCOPE::::
MONITORED_BY
MONITORED_BY
MONITORED_BY
TENANT:GENERIC::::
DATACENTER:GENERIC::::
DATACENTER:GENERIC::::