



HPE NFV Director

OMi and uCMDB for NFVD User Guide

Release 4.2

First Edition



Hewlett Packard
Enterprise

Notices

Legal notice

© Copyright 2017 Hewlett Packard Enterprise Development LP

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

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

Printed in the US

Trademarks

Linux is the registered trademark of Linus Torvalds in the U.S. and other countries.

Oracle and Java are registered trademarks of Oracle and/or its affiliates.

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

Microsoft®, Internet Explorer, Windows®, Windows Server 2007®, Windows XP®, and Windows 7® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Firefox® is a registered trademark of the Mozilla Foundation.

Google Chrome® is a trademark of Google Inc.

EnterpriseDB® is a registered trademark of EnterpriseDB.

Postgres Plus® Advanced Server is a registered U.S. trademark of EnterpriseDB.

UNIX® is a registered trademark of The Open Group.

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

Red Hat® is a registered trademark of the Red Hat Company.

Apache CouchDB, CouchDB, and the project logo are trademarks of The Apache Software Foundation.

Node.js project. Joyent® and Joyent's logo are registered trademarks of Joyent, Inc.

Neo4j is a trademark of Neo Technology.

VMware ESX, VMWare ESXi, VMWare vCenter and VMWare vSphere are either registered trademarks or trademarks of VMware, Inc. in the United States and other jurisdictions

Contents

| | |
|---|-----------|
| Notices | 1 |
| Preface..... | 8 |
| About this guide | 8 |
| Audience | 8 |
| Document history..... | 8 |
| Chapter 1 Introduction | 9 |
| 1.1 Overview of resource discovery..... | 9 |
| 1.1.1 What is CMDB? | 9 |
| 1.1.2 Why integration with uCMDB is necessary for NFV Director? | 9 |
| 1.2 Architecture..... | 10 |
| 1.2.1 NFV Director integration with uCMDB and OMi | 10 |
| 1.2.2 Topology discovery using uCMDB..... | 10 |
| 1.2.3 uCMDB integration components | 11 |
| 1.3 List of NFV Director Resources discovered..... | 11 |
| Chapter 2 Installation and configuration | 12 |
| 2.1 Installation | 12 |
| 2.1.1 Prerequisites..... | 12 |
| 2.1.2 Channel Adapter installation steps..... | 12 |
| 2.1.2.1 Configuration for Channel Adapters..... | 12 |
| 2.1.3 Operations Manager integration with NFV Director..... | 14 |
| 2.1.3.1 OMi integration with NFV Director for discovery..... | 14 |
| 2.1.3.2 BSM-C policy import | 14 |
| 2.1.3.3 Configure UCA for OMi integration | 15 |
| 2.2 Enabling and disabling of discovery process | 15 |
| 2.2.1 Disable discovery even in fresh installation | 15 |
| 2.2.2 Disable discovery temporarily | 15 |
| 2.2.3 Enable Discovery..... | 15 |
| 2.2.4 Manual Discovery trigger..... | 15 |
| 2.2.5 Track Discovery/Reconciliation completion..... | 16 |
| Chapter 3 Post discovery steps | 17 |
| 3.1 Update VIM Authentication details from NFV Director-GUI..... | 17 |
| Chapter 4 DCN integration..... | 18 |
| 4.1 Prerequisites | 18 |
| 4.2 Integrate DCN with NFV Director | 18 |
| 4.2.1 Create the SDN Topology manually | 18 |
| 4.2.2 Upload DCN resource | 20 |
| 4.2.3 Connect Datacenter with DCN resources | 21 |
| 4.2.4 Query discovered Networking Artifacts | 24 |
| 4.2.5 Create relationship between NETWORKING and DCN Artifacts | 25 |
| Chapter 5 Monitoring and alarm management | 27 |
| 5.1 Alarm flow architecture..... | 27 |
| 5.2 NFV Director events integration with OMi | 27 |
| 5.2.1 Configure webservice endpoint in OMi | 27 |

| | |
|---|-----------|
| 5.2.2 Create forwarding rule to forward events from OMi | 32 |
| 5.2.3 Property file change | 35 |
| 5.2.4 Generate new events | 35 |
| 5.2.4.1 Configuration | 35 |
| 5.2.5 Send new events | 39 |
| 5.2.6 Verify event received in OMi-CA log | 40 |
| 5.2.7 Generate events in OMi using sendEvent tool | 40 |
| 5.3 NFV Director integration with BSM-C | 41 |
| 5.3.1 Database Structure | 45 |
| 5.3.2 Database Query Configuration | 46 |
| 5.4 BSM-C integration with OMi | 47 |
| 5.5 OpenStack OMi event payload samples | 47 |
| 5.6 VMWare Event Payload | 48 |
| 5.7 OMi Event Payload | 48 |
| Appendix A NFV Director topology structure | 49 |

List of tables

| | |
|--|----|
| Table 1: Document history | 8 |
| Table 2: Alarms policy: Alarm-to-event attribute mapping..... | 43 |
| Table 3: Updates policy: Updates-to-event attribute mapping..... | 43 |
| Table 4: Alarm database schema..... | 45 |
| Table 5: Alarm database schema..... | 46 |
| Table 6: Session Variables | 46 |

List of figures

| | |
|--|----|
| Figure 1: NFV Director integration with uCMDB and OMi..... | 10 |
| Figure 2: Topology discovery using uCMDB..... | 10 |
| Figure 3: uCMDB integration components..... | 11 |
| Figure 4: Discovered resources..... | 11 |
| Figure 5: Setting header and data for BSM-C policy..... | 14 |
| Figure 6: NFV Director: Edit VIM authentication details..... | 17 |
| Figure 7: DCN topology pictorial representation..... | 20 |
| Figure 8: Uploading DCN topology into fulfillment..... | 21 |
| Figure 9: Query ID of Datacenter..... | 22 |
| Figure 10: Response for Datacenter Query..... | 22 |
| Figure 11: Query ID of SHARED_NETRESOURCE:DCN..... | 23 |
| Figure 12: Response for SDN_CONTROLLER:DCN Query..... | 23 |
| Figure 13: Create Relationship..... | 24 |
| Figure 14: Query NETWORKING:OPENSTACK associated with Region..... | 25 |
| Figure 15: Query Response for NETWORKING:OPENSTACK associated with Region..... | 25 |
| Figure 16: REST operation to create relationship between NETWORKING and DCN..... | 26 |
| Figure 17: Alarm flow architecture..... | 27 |
| Figure 18: Configure webservice endpoint in OMi..... | 28 |
| Figure 19: Configure new server..... | 28 |
| Figure 20: Enter webservice endpoint name..... | 29 |
| Figure 21: Enter FQDN..... | 29 |
| Figure 22: Enter URL for webservice server..... | 30 |
| Figure 23: Secure HTTP..... | 30 |
| Figure 24: Enter FQDN..... | 31 |
| Figure 25: Incoming connection setting..... | 31 |
| Figure 26: Choose Event Forwarding option in OMi..... | 32 |
| Figure 27: Create new forwarding rule..... | 32 |

| | |
|--|----|
| Figure 28: Create new event forwarding rule..... | 33 |
| Figure 29: Create new simple filter | 34 |
| Figure 30: Create additional event property | 35 |
| Figure 31: OMi console policy templates..... | 35 |
| Figure 32: Create new test folder..... | 36 |
| Figure 33: Add new template group..... | 36 |
| Figure 34: add new policy template..... | 36 |
| Figure 35: Choose type of policy template..... | 37 |
| Figure 36: Name the policy template..... | 37 |
| Figure 37: Create new rule | 37 |
| Figure 38: Select condition for events | 38 |
| Figure 39: Assign and deploy policy template..... | 38 |
| Figure 40: Send test event | 39 |
| Figure 41: OMi operations console..... | 40 |
| Figure 42: Set DB source..... | 41 |
| Figure 43: BSMC database query..... | 42 |
| Figure 44: Verify BSMC database query | 42 |
| Figure 45: Set data mapping | 42 |
| Figure 46: Fill event attributes..... | 43 |
| Figure 47: Alarm policy..... | 44 |
| Figure 48: Updates policy..... | 44 |
| Figure 49: Create filtering role | 45 |
| Figure 50: Activate policy..... | 45 |
| Figure 51: Relationship between OpenStack and DCN modules..... | 49 |
| Figure 52: DC to SHARED_RESOURCE:DCN relationship..... | 50 |
| Figure 53: Manually create shared resources | 51 |
| Figure 54: Manually create L3Domain..... | 51 |
| Figure 55: Manually create L3Domain..... | 52 |

Figure 56: Management tenant matching L3Domain.....53

Preface

About this guide

This document explains the procedure to install and configure the uCMDB Discovery and OMi events. This document also gives an overview of resource discovery, architectural view, enabling/disabling of discovery process, and list of objects discovered.

By following the procedures in this document, Helion CG resources can be discovered using uCMDB.

Audience

This document is any stakeholder requiring to perform resource discovery using the NFV Director. Pre requisite is to have knowledge of NFV Director concepts, OMi concepts, and an understanding of the NFV Director resource model.

Document history

Table 1: Document history

| Edition | Date | Description |
|---------|-------------------|----------------|
| 1.0 | February 15, 2017 | First edition. |

Chapter 1 Introduction

The aim of this document is to provide

- Purpose and Overview of Resource Discovery from uCMDB.
- Architectural view.
- Installation and configuration of Discovery Process.
- Enabling and Disabling of Discovery Process.
- The list of resources discovered.
- Architecture of OMi event flow.
- Event payload

1.1 Overview of resource discovery

NFV Director is responsible for managing the lifecycle of VNF and it's important for NFVD to know the complete topology of the underlying VIM Resources,

The complete list of VIM resource topology is described below.

The Discovery process described in this document helps in automatic discovery of the VIM Resources and their inter-relationship from CMDB.

1.1.1 What is CMDB?

- A configuration management database (CMDB) is a database that contains all relevant information about the components of the information system used in an organization's IT services and the relationships between those components.
- A CMDB provides an organized view of data and a means of examining that data from any desired perspective.
- Within this context, components of an information system are referred to as configuration items (CI).
- A CI can be any conceivable IT component, including software, hardware, documentation, and personnel, as well as any combination of them.

HPE provides its own configuration management database known as uCMDB.

1.1.2 Why integration with uCMDB is necessary for NFV Director?

Typically in IT organization, uCMDB acts as data warehouse that holds IT assets and relationship between these IT assets. NFV Director is responsible for laying out Virtual topology (VNFs) on top of these Physical Topology judiciously, which is not possible without NFV Director being aware of the underlying Physical Topology

1.2 Architecture

1.2.1 NFV Director integration with uCMDB and OMi

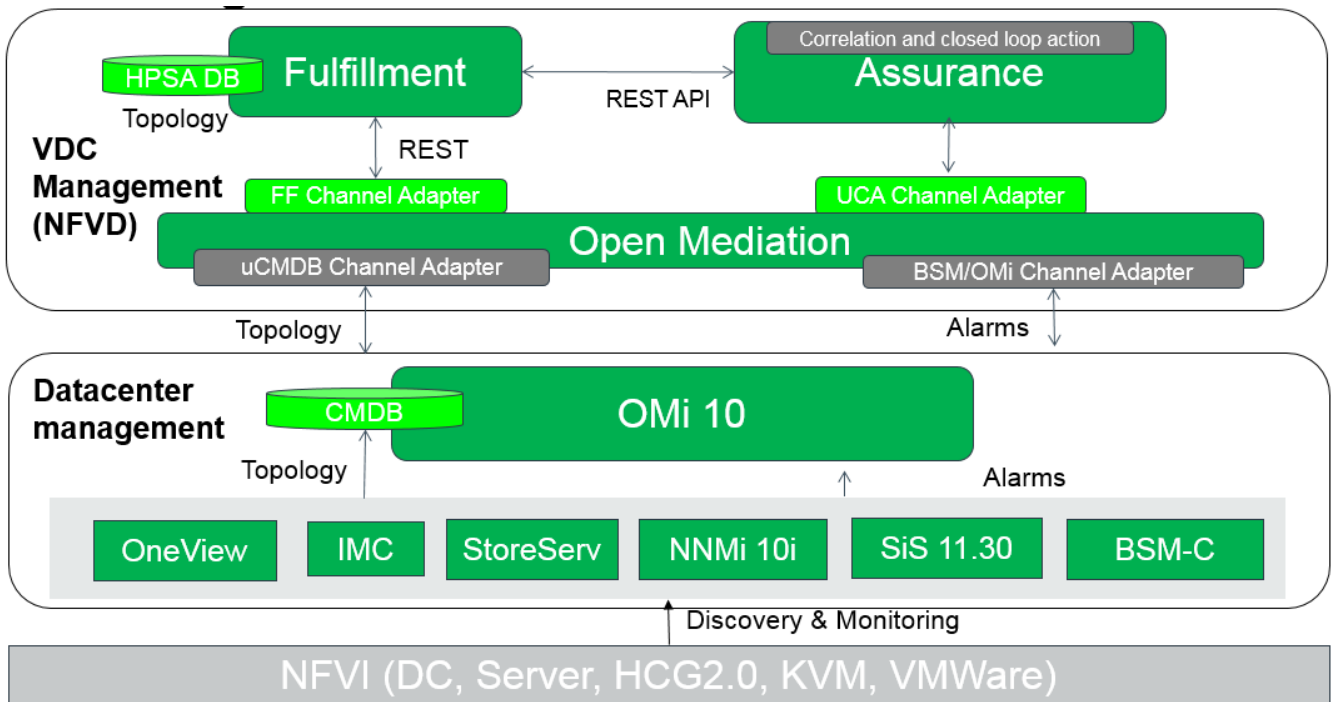


Figure 1: NFV Director integration with uCMDB and OMi

1.2.2 Topology discovery using uCMDB

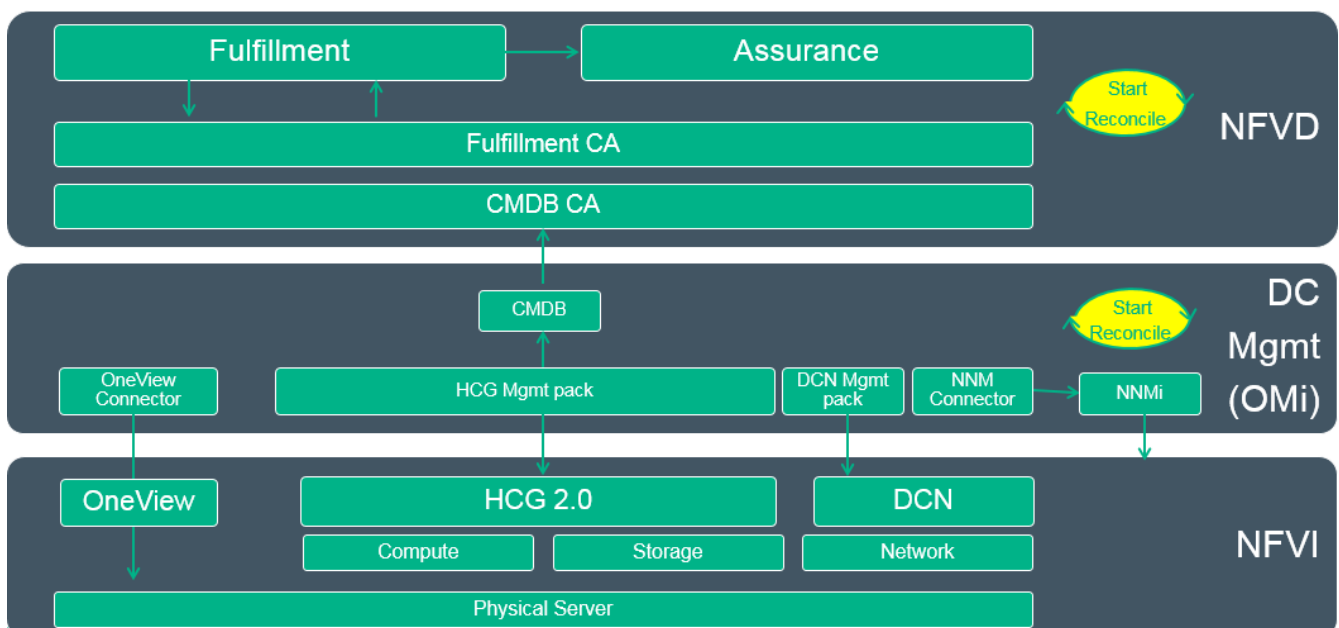


Figure 2: Topology discovery using uCMDB

1.2.3 uCMDB integration components

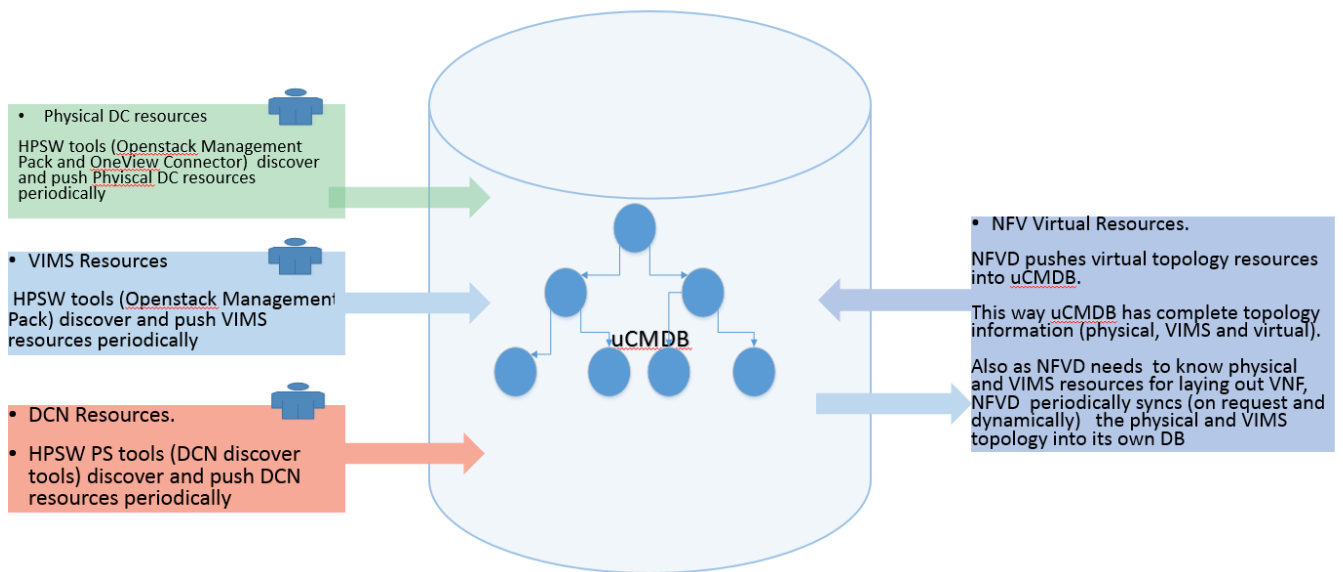


Figure 3: uCMDB integration components

1.3 List of NFV Director Resources discovered

- ✓ Servers
 - CPU, Memory, Disk
 - Port, Interface
 - Total, used and available capacity
- ✓ Regions
- ✓ Tenant
- ✓ OpenStack Services
- ✓ Hypervisors
 - ESX, KVM, Bare metal
- ✓ Availability Zones
- ✓ Host Aggregates
- ✓ Networks
- ✓ Subnetworks
 - IPAddress
- ✓ Virtual Machines
 - vCPU, vMemory, vDisk
 - vPort
- ✓ LUN/vLUN
- ✓ Images
- ✓ Flavor
- ✓ Carrier Grade
 - NUMA, Huge pages
 - PCI-PT
 - SR-IOV
- ✓ DCN
- ✓ TOR Switch
- ✓ Server-TOR Switch connection
- ✓ MicroDC
- ✓ Data center
 - Rack
 - Enclosure

Figure 4: Discovered resources

Chapter 2 Installation and configuration

2.1 Installation

2.1.1 Prerequisites



NOTE: Two servers are required, one for OMi and another for BSM Connector. They cannot collocate. They must be installed on Linux Operating System and are accessible with the recommended configuration.



NOTE: Install and configure the manage packs, following the HPSw documents.

1. OMi 10.00/01 and BSM Connector 10.00.
2. cmdb-ca-1.0.0.zip (part of nfvd-discovery-common-04.00.001-1.el6.noarch.rpm)
 - a. NFVD.zip
3. fulfillment-ca -1.0.0.zip (part of nfvd-discovery-common-04.00.001-1.el6.noarch.rpm)
4. omi-ca-1.0.0.zip (part of nfvd-discovery-cmdb-04.00.001-1.el6.noarch.rpm)
 - a. BSMC-Policy.zip
5. Helion CG Management Pack
6. One View Management Pack

2.1.2 Channel Adapter installation steps

1. Install the omi and discovery RPMs in the <AA_HOST>, where we have the Open Mediation installed.

```
rpm -ivh nfvd-discovery-common-04.00.001-1.el6.noarch.rpm
rpm -ivh nfvd-discovery-cmdb-04.00.001-1.el6.noarch.rpm
rpm -ivh nfvd-alarms-omi-04.00.001-1.el6.noarch.rpm
```

2. Install omi-ca, cmdb-ca and fulfillment-ca

```
unzip -d /opt/openmediation-70/ips/ /opt/HPE/nfvd/discovery/omi/omi-ca-1.0.0.zip
nom_admin --install-ip omi-ca-10
nom_admin --install-ip-in-container 0 omi-ca-10

unzip -d /opt/openmediation-70/ips/ /opt/HP/nfvd/discovery/common/cmdb-ca-1.0.0.zip
nom_admin --install-ip cmdb-ca-10
nom_admin --install-ip-in-container 0 cmdb-ca-10

unzip -d /opt/openmediation-70/ips/ /opt/HP/nfvd/discovery/common/fulfillment-ca -1.0.0.zip
nom_admin --install-ip fulfillment-ca-10
nom_admin --install-ip-in-container 0 fulfillment-ca-10
```

2.1.2.1 Configuration for Channel Adapters

1. Edit the below file for configurations in fulfillment-ca, and provide <FF_HOST_IP> and <HPSA_PORT>

```
/var/opt/openmediation-70/containers/instance-0/ips/fulfillment-ca-10/etc/config/
reconciliation-endpoints.properties
```

```
#Fulfillment rest endpoint protocol http/https
rest.protocol=http

#Fulfillment rest endpoint ipaddress/hostname
```

```
rest.endpoint=<FF_HOST_IP>

#Fulfillment rest endpoint port
rest.port=<FF_PORT>

#Reconciliation CA rest endpoint for sending trigger message, port has to be changed each
container deployment.
recon.rest.endpoint=http://0.0.0.0:18989

#Reconciliation data log folder for artifact-relationship instances.
log.file.folder=/var/tmp

#Reconciliation interval
rest.endpoint.polling.interval=36000s

#REST/LOG OPTION to be triggered for Reconciliation
REST_CALL=TRUE
LOG_ENTRY=FALSE
```

2. Edit the below file for configurations in cmdb-ca, and provide <OMi IP Address>, <Port>, <username> and <password>

```
/var/opt/openmediation-70/containers/instance-0/ips/cmdb-ca-10/etc/endpoints-
config.properties
```

```
#OMi Ip address
omi.host=<IPAddress of OMi>
omi.port=<port>
omi.username=<username>
omi.password=<password>
```

3. Edit the below file to reflect Open Mediation Host/IP address.

```
/var/opt/openmediation-70/containers/instance-0/ips/omi-ca-10/etc/omi-nfvd.properties
```

```
omi.rest.endpoint=http://<OM_HOSTNAME_OR_IP>:17870
```

4. Deploy cmdb-ca, omi-ca and fulfillment-ca.

```
nom_admin --deploy-ip-in-container 0 cmdb-ca-10
nom_admin --deploy-ip-in-container 0 fulfillment-ca-10
nom_admin --deploy-ip-in-container 0 omi-ca-10
```



NOTE: After performing any property changes, the channel adapters have to be un-deployed and redeployed



IMPORTANT: Deploying the fulfillment-ca will trigger discovery.

```
/opt/open-mediation/bin/nom_admin --undeploy-ip-in-container 0 cmdb-ca-10
/opt/open-mediation/bin/nom_admin --undeploy-ip-in-container 0 fulfillment-ca-10
```

2.1.3 Operations Manager integration with NFV Director

2.1.3.1 OMi integration with NFV Director for discovery



NOTE: Copy the NFVD.zip file present in '/opt/HPE/nfvd/discovery/cmd/db/integration' directory to the local workstation from where the OMi GUI is accessed. You can get NFVD.zip on installing the nfvd-discovery-common-04.00.001-1.el6.noarch.rpm

To install NFVD.zip file, follow the below steps -

1. Login to OMi
2. Navigate to Administration >> RTSM Administration >> Package Manager [Under Administration heading]
3. Click the icon -
4. Click on the add button in the 'Deploy Packages to Server' pop-up
5. Browse for the NFVD.zip package in the local directory and click on Open
6. Select/ Click on the NFVD.zip package name
7. Click on the button - to select all resources
8. Click on the button - Deploy
9. Verify that the Package is displayed present in the OMi GUI

2.1.3.2 BSM-C policy import

1. Login to the target BSM Connector.
2. In the BSM Connector user interface, click in the toolbar. A file selection dialog box opens.
3. Unzip the file present in /opt/HPE/nfvd/discovery/omi/integration
4. Navigate to the policy files and, for each policy, select both the header (*_header.xml) and the data (*_data) files.

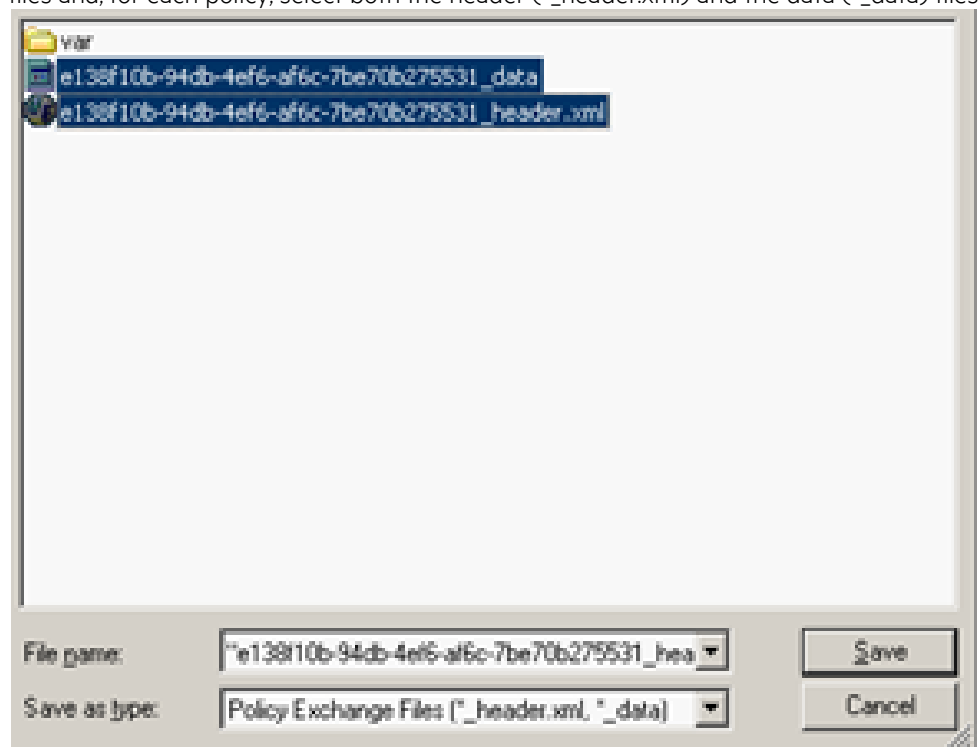


Figure 5: Setting header and data for BSM-C policy

5. Click Open to start the import process.
6. If the policies with the same policy ID already exist in BSM Connector, you are asked whether you would like to replace them with the newly imported policies.
7. The imported policies appear in the list of policies in the BSM Connector user interface. They are by default deactivated.
8. If necessary, edit the imported policies and adapt their contents to the new BSM Connector server.
9. Optional: Activate the policies.

2.1.3.3 Configure UCA for OMi integration

Edit the following file, and add the below content within the <ActionRegistryXML> tag.

```
/var/opt/UCA-EBC/instances/default/conf/ActionRegistry.xml
```

```
<MediationValuePack MvpName="omi_source" MvpVersion="1.0"
url="http://localhost:18192/uca/mediation/action/ActionService?WSDL"
  brokerURL="failover://tcp://localhost:10000">
  <Action actionReference="OMi_Action_localhost">
    <ServiceName>alertService</ServiceName>
    <NmsName>localhost</NmsName>
  </Action>
</MediationValuePack>
```

2.2 Enabling and disabling of discovery process

By default discovery is enabled, when NFV Director discovery components are installed.

2.2.1 Disable discovery even in fresh installation

Execute the below script when you install the fulfillment-ca, before deploying it.

```
cd /opt/HPE/nfvd/discovery/scripts/
sh disable_discovery.sh
```

2.2.2 Disable discovery temporarily

Execute the below script. Once disabled subsequent Discovery runs will not be triggered. Disabling while discovery in progress will not impact the current run.

```
cd /opt/HPE/nfvd/discovery/scripts/
sh disable_discovery.sh
```

2.2.3 Enable Discovery

Execute the below script.

```
cd /opt/HPE/nfvd/discovery/scripts/
sh enable_discovery.sh
```

2.2.4 Manual Discovery trigger

Execute the below script. Manual discovery can be triggered any time. It will not get triggered when another instance of Discovery is already running.

```
cd /opt/HPE/nfvd/discovery/scripts/
./trigger_reconciliation.sh
```




NOTE: If you want to make some changes in properties files of FF-CA, you must

1. disable discovery
2. undeploy the CA
3. make changes to properties
4. deploy CA
5. enable discovery

2.2.5 Track Discovery/Reconciliation completion

Open Mediation log file will have a status message of Discovery:

```
/var/opt/openmediation-70/containers/instance/data/log/service-mix-info.log
```

```
***** Discovery/Reconciliation Service has been completed successfully, Quota Calculation  
is in Progress *****
```

Chapter 3 Post discovery steps

3.1 Update VIM Authentication details from NFV Director-GUI

- Go to Instance view as domain user
- Select Other as Authentication
- Select the VIM, you want to edit
- From ACTION menu, select EDIT
- Enter the VIM's credentials and click Update

The screenshot displays the 'Edit attributes: authentication-Helion_DC1' dialog box in the NFV Director GUI. The dialog is divided into several tabs: GENERAL, CREDENTIALS, STATUS, CAPACITY, ROLES, TEMPLATE, and INTEGRATION. The CREDENTIALS tab is currently selected. The fields within this tab are as follows:

- Uri: http://172.19.248.14:5000/v2.0/tokens
- Login: admin
- Password: (empty)
- TenantName: admin
- UserId: 03b51c670ff7403cb0778482884ed708
- IdentityVersion: V2

At the bottom right of the dialog, there are two buttons: 'Update' and 'Cancel'.

Figure 6: NFV Director: Edit VIM authentication details

Chapter 4 DCN integration

4.1 Prerequisites

If integration with external DCN (Alcatel Lucent Nuage) is considered, we would need the following

1. DCN (Nuage) v3.2.1.1, if external DCN is used.
2. OMi Management Pack for DCN (Nuage).
3. **DCN_Topology.xml → SDN Topology manually created.**



DCN Integration with NFV Director is an optional step. This would be required in case an external DCN has to be used for Networking. In current release DCN (Nuage) is supported.

DCN Topology has to be attached manually once Discovery has been completed. .

Below section explains the procedure to be followed to integrate DCN with NFV Director.

4.2 Integrate DCN with NFV Director

4.2.1 Create the SDN Topology manually

Attachment file 'DCN_Topology.xml' contains the default SDN topology

In the DCN_Topology.xml, edit the following attributes:



NOTE: You can use the NFVD Resource Modeler to edit the DCN_Topology.

- AUTHENTICATION > CREDENTIALS > Url

| Value | Example |
|--|---|
| https://<nuage_ip>:<port>/nuage/api/v3_2 | https://172.19.244.225:8443/nuage/api/v3_2 |

- AUTHENTICATION > CREDENTIALS > Login
- AUTHENTICATION > CREDENTIALS > Password
- AUTHENTICATION > CREDENTIALS > Admin_enterprise
- L3DOMAIN > DOMAIN > RouteDistinguisher

| Value | Example |
|----------|-------------|
| RD Value | 65534:12538 |

- L3DOMAIN > DOMAIN > RouteTarget

| Value | Example |
|----------|-------------|
| RD Value | 65534:56825 |

- L3DOMAIN > DOMAIN > BackHaulRouteDistinguisher

| Value | Example |
|----------|-------------|
| RD Value | 65534:62251 |

- L3DOMAIN > DOMAIN > BackHaulRouteTarget
- L3DOMAIN > DOMAIN > ExportRouteTarget
- L3DOMAIN > DOMAIN > ImportRouteTarget

| Value | Example |
|----------|---------------|
| RT Value | 65534 : 32060 |

- L3DOMAIN > DOMAIN > BackHaulVNID

| Value | Example |
|--------|---------|
| VPN ID | 314849 |

- L3DOMAIN > DOMAIN > BackHaulVNID

| Value | Example |
|--------|---------|
| VPN ID | 314849 |

- L3DOMAIN > DOMAIN > TunnelType

| Value | Example |
|------------|---------|
| TunnelType | VXLAN |

- MACRONET > MACRONET > address
- MACRONET > MACRONET > netmask
- SHARED_NETRESOURCE > RESOURCE > Address
- SHARED_NETRESOURCE > RESOURCE > Netmask
- SHARED_NETRESOURCE > RESOURCE > DomainRouteDistinguisher
- SHARED_NETRESOURCE > RESOURCE > DomainRouteTarget
- SHARED_NETRESOURCE > RESOURCE > Gateway

Below is the pictorial representation of DCN Topology

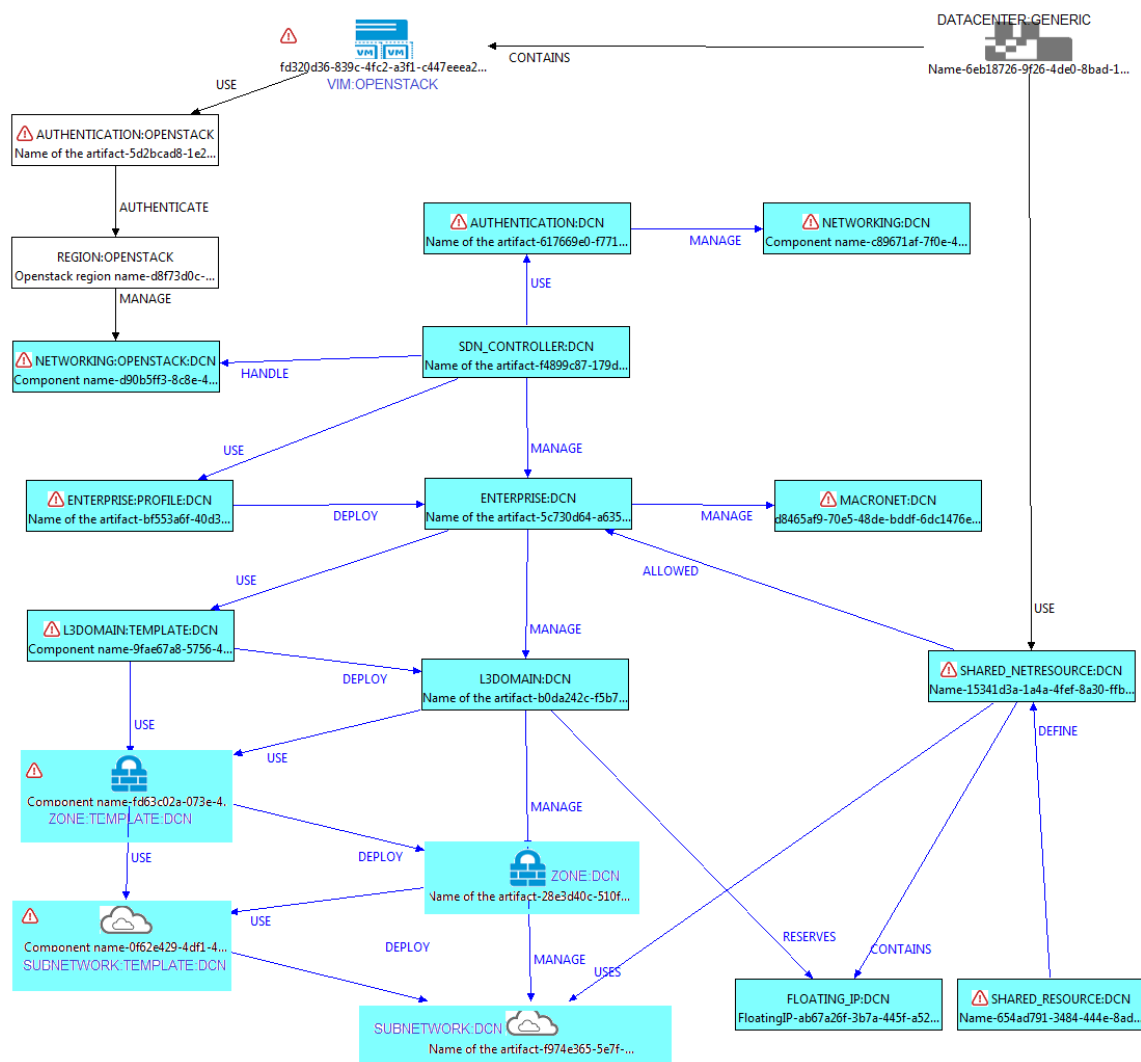


Figure 7: DCN topology pictorial representation

4.2.2 Upload DCN resource

- 1 Open REST Client.
- 2 Provide FF_HOST_IP and FF_PORT details in the REST URL. Select POST HTTP Operation.
- 3 Copy the content of file DCN_Topology.xml inside payload section.



IMPORTANT: For all Rest operations add the below headers:

Content-Type: application/xml

X-Auth-Token: 3778fe88-e71d-4004-86bc-3188f7fd450b.

Request

Host
http://<FF_HOST_IP>:<FF_PORT>

Path
/nfvd/instance/upload

Query parameters

Hash

GET POST PUT DELETE Other methods application/xml

Raw headers Headers form Headers sets

HTTP headers

| | | |
|--------------|--------------------------------------|----------------------------------|
| X-Auth-Token | 3778fe88-e71d-4004-86bc-3188f7fd450b | <input type="button" value="X"/> |
| Content-Type | application/xml | <input type="button" value="X"/> |

Raw payload Data form Files (0)

```
<?xml version="1.0" encoding="utf-8"?>
<instances xmlns="http://www.hp.com/nfvd">
  <instance-trees>
    <instance>
      <id>07559026-75ae-4c2e-99a1-ab44201e5eb6</id>
      <name>DCN</name>
      <type>sdn_controller</type>
      <description>DCN</description>
      <artifact-instances>
        <artifact-instance>
          <id>f5612797-8983-460a-a494-0e974fa463f6</id>
        </artifact-instance>
      </artifact-instances>
      .....
      <relationship-instances>
        <relationship-instance>
          .....
        </relationship-instance>
      </relationship-instances>
    </instance>
  </instance-trees>
  <elements>
    .....
  </elements>
</instances>
```

Figure 8: Uploading DCN topology into fulfillment

4.2.3 Connect Datacenter with DCN resources



CAUTION: Execute it per DC.

- Query Datacenter ID
 - Provide FF_HOST_IP and FF_PORT details in the REST URL. Select GET HTTP Operation.
 - Enter the Path and Query parameters and Headers as shown in sample below.
 - GENERAL.Name attribute filter is used to filter by Datacenter Name DC1 or DC2 (Name of your Datacenter)

Request

Host
http://<FF_HOST_IP>:<FF_PORT>

Path
/nfvd/instance/artifact/query/parameters

Query parameters

| | | |
|-----------------|--------------------|---|
| definition | DATACENTER:GENERIC | × |
| attributeFilter | GENERAL.Name=DC1 | × |
| exactMatching | false | × |

ADD

Hash

GET POST PUT DELETE Other methods

Raw headers Headers form

HTTP headers

| | | |
|--------------|--------------------------------------|-----|
| X-Auth-Token | 3778fe88-e71d-4004-86bc-3188f7fd450b | × |
| Content-Type | application/xml | ✎ × |

ADD

SEND

Figure 9: Query ID of Datacenter

Status: 200: OK ? Loading time: 200 ms

Response headers (4) Request headers (2) Redirects (0) Timings

Server: Apache-Coyote/1.1
Content-Type: application/xml
Transfer-Encoding: chunked
Date: Thu, 28 Apr 2016 13:51:08 GMT

Raw XML

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<artifact-instances xmlns="http://www.hp.com/nfvd">
  <artifact-instance internal-id="8f2e6b76-a367-4fa2-8444-637aab6ff73f" uri="/nfvd/instance/artifact/8f2e6b76-a367-4fa2-8444-637aab6ff73f">
    <artifact-definition>
      <category>GENERIC</category>
      <family>DATACENTER</family>
    </artifact-definition>
    <status><enabled>true</enabled>
    <label>ENABLED</label>
    <visible-label>ENABLED</visible-label>
  </status>
  <categories>
    <category>
```

Figure 10: Response for Datacenter Query

- 2 Query SHARED_NETRESOURCE:DCN ID
 - a. Provide FF_HOST_IP and FF_PORT details in the REST URL. Select GET HTTP Operation.
 - b. Enter the Path and Query parameters and Headers as shown in sample below.
 - c. INFO.DC.Name attribute filter is used to filter by Datacenter Name

Request

Host
http://<FF_HOST_IP>:<FF_PORT>

Path
/nfvd/instance/artifact/query/parameters

Query parameters

| | | |
|-----------------|------------------------|---|
| definition | SHARED_NETRESOURCE:DCN | × |
| attributeFilter | INFO.DCName=DC1 | × |
| exactMatching | false | × |

ADD

Hash

GET POST PUT DELETE Other methods

Raw headers Headers form

HTTP headers

| | | |
|--------------|--------------------------------------|-----|
| X-Auth-Token | 3778fe88-e71d-4004-86bc-3188f7fd450b | × |
| Content-Type | application/xml | ✎ × |

ADD

SEND

Figure 11: Query ID of SHARED_NETRESOURCE:DCN

Status: 200: OK ? Loading time: 200 ms

Response headers (2) Request headers (4) Redirects (0) Timings

Server: Apache-Coyote/1.1
Content-Type: application/xml
Transfer-Encoding: chunked
Date: Thu, 28 Apr 2016 13:51:08 GMT

Raw XML

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<artifact-instances xmlns="http://www.hp.com/nfvd">
  <artifact-instance internal-id="a2d4aee3-25a4-4e3c-a353-a9679046f7a9" uri="/nfvd/instance/artifact/a2d4aee3-25a4-4e3c-a353-a9679046f7a9">
    <artifact-definition>
      <category>DCN</category>
      <family>SHARED_NETRESOURCE</family>
    </artifact-definition>
  </artifact-instance>
  <artifact-instance internal-id="bea8c469-299b-446d-bd72-8cf2c5c0af60" uri="/nfvd/instance/artifact/bea8c469-299b-446d-bd72-8cf2c5c0af60">
    <artifact-definition>
      <category>DCN</category>
      <family>SHARED_NETRESOURCE</family>
    </artifact-definition>
  </artifact-instance>
</artifact-instances>
```

Figure 12: Response for SDN_CONTROLLER:DCN Query

- 3 Create Relationship between DATACENTER and each SHARED_NETRESOURCE retrieved from response above. Relationship sample is shown below:
 - a. parent-artifact-id: DC ID returned from "Query Datacenter ID" step
 - b. child-artifact-id: Shared_NetResource ID returned from "Query SHARED_NETRESOURCE:DCN ID" step

For the above example,

```
<relationship-instances xmlns="http://www.hp.com/nfvd">
```



```

<relationship-instance>
  <categories/>
  <parent-artifact-id>8f2e6b76-a367-4fa2-8444-637aab6ff73f</parent-artifact-id>
  <child-artifact-id>a2d4aee3-25a4-4e3c-a353-a9679046f7a9</child-artifact-id>
  <status>
    <enabled>>true</enabled>
    <label>ENABLED</label>
    <visible-label>ENABLED</visible-label>
  </status>
  <relationship-type>USE</relationship-type>
</relationship-instance>
</relationship-instances>

```

Use the above block as payload section in the Rest client, as shown below.

The screenshot shows a REST client interface with the following configuration:

- Host:** `http://<FF_HOST_IP>:<FF_PORT>`
- Path:** `/nfvd/instance/relationship`
- Method:** **POST** (selected)
- Content-Type:** `application/xml`
- HTTP headers:**
 - `X-Auth-Token: 3778fe88-e71d-4004-86bc-3188f7fd450b`
 - `Content-Type: application/xml`
- Raw payload:**

```

?xml version="1.0" encoding="utf-8"?>
<relationship-instances xmlns="http://www.hp.com/nfvd">
  <relationship-instance>
    <categories/>
    <parent-artifact-id>8f2e6b76-a367-4fa2-8444-637aab6ff73f</parent-artifact-id>
    <child-artifact-id>a2d4aee3-25a4-4e3c-a353-a9679046f7a9</child-artifact-id>
    <status>
      <enabled>true</enabled>
      <label>ENABLED</label>
      <visible-label>ENABLED</visible-label>
    </status>
    <relationship-type>USE</relationship-type>
  </relationship-instance>
</relationship-instances>

```
- SEND** button is highlighted in blue.

Figure 13: Create Relationship

4.2.4 Query discovered Networking Artifacts

1. Query NETWORKING:OPENSTACK associated with each Region of the Datacenter



IMPORTANT: Execute the below steps for each region, **sacramento** region is used as an example.

- a. Provide FF_HOST_IP, FF_PORT details in REST URL.
- b. Select GET HTTP operation.
- c. Provide headers, path and query parameters as shown in below sample.

id: DC ID returned from “Query Datacenter ID” step

expression:

DATACENTER>VIM>AUTHENTICATION>REGION#GENERAL.Name=sacramento>NETWORKING

Request

Host
http://<FF_HOST_IP>:<FF_PORT>

Path
/nfvd/instance/artifact/query/path

Query parameters

| | | |
|------------|---|---|
| id | 8f2e6b76-a367-4fa2-8444-637aab6ff73f | X |
| expression | DATACENTER>VIM>AUTHENTICATION>REGION#GENERAL.Name=sacramento>NETWORKING | X |

ADD

Hash

GET POST PUT DELETE Other methods

Raw headers Headers form Headers sets

X-Auth-Token: 3778fe88-e71d-4004-86bc-3188f7fd450b
Content-Type: application/xml

SEND

Figure 14: Query NETWORKING:OPENSTACK associated with Region

Below is the response received.

Status: 200 OK Loading time: 206 ms

Response headers (4) Request headers (2) Redirects (0) Timings

Server: Apache-Coyote/1.1
Content-Type: application/xml
Content-Length: 3921
Date: Fri, 29 Apr 2016 07:06:43 GMT

Raw XML

```
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
<artifact-instances xmlns="http://www.hp.com/nfvd">
  <artifact-instance internal-id="a7fc5aa9-e10d-3380-a3be-da9ed6f213c3" uri="/nfvd/instance/artifact/a7fc5aa9-e10d-3380-a3be-da9ed6f213c3">
    <artifact-version>1</artifact-version>
    <artifact-definition>
      <category>OPENSTACK</category>
      <family>NETWORKING</family>
    </artifact-definition>
  </artifact-instance>
</artifact-instances>
```

Figure 15: Query Response for NETWORKING:OPENSTACK associated with Region

4.2.5 Create relationship between NETWORKING and DCN Artifacts



IMPORTANT: Execute the below steps for each region.

- 1 Create Relationship between NETWORKING_OPENSTACK:DCN and SDN_CONTROLLER:DCN. Relationship sample is shown below:

- parent-artifact-id: Id of SDN_CONTROLLER:DCN Artifact. If you use the DCN_Template.xml, the value MUST be 94c80294-2175-4011-bdf2-78db5c689158
- child-artifact-id: NETWORKING:OPENSTACK Id's returned from "Query NETWORKING:OPENSTACK associated with each Region of the Datacenter" step.

For our example:

```
<relationship-instances xmlns="http://www.hp.com/nfvd">
  <relationship-instance>
    <categories/>
    <parent-artifact-id>94c80294-2175-4011-bdf2-78db5c689158</parent-artifact-id>
    <child-artifact-id>a7fc5aa9-e10d-3380-a3be-da9ed6f213c3</child-artifact-id>
    <status>
      <enabled>>true</enabled>
      <label>ENABLED</label>
      <visible-label>ENABLED</visible-label>
    </status>
    <relationship-type>HANDLE</relationship-type>
  </relationship-instance>
</relationship-instances>
```

Paste the above content in the payload section of the REST client.

The screenshot shows a REST client interface with the following configuration:

- Request:** Host: `http://<FF_HOST_IP>:<FF_PORT>`, Path: `/nfvd/instance/relationship`
- Method:** POST
- Raw headers:**
 - X-Auth-Token: `3778fe88-e71d-4004-86bc-3188f7fd450b`
 - Content-Type: `application/xml`
- Raw payload:**

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<relationship-instances xmlns="http://www.hp.com/nfvd">
  <relationship-instance>
    <categories/>
    <parent-artifact-id>94c80294-2175-4011-bdf2-78db5c689158</parent-artifact-id>
    <child-artifact-id>a7fc5aa9-e10d-3380-a3be-da9ed6f213c3</child-artifact-id>
    <status>
      <enabled>true</enabled>
      <label>ENABLED</label>
      <visible-label>ENABLED</visible-label>
    </status>
    <relationship-type>HANDLE</relationship-type>
  </relationship-instance>
</relationship-instances>
```

A **SEND** button is located at the bottom right of the interface.

Figure 16: REST operation to create relationship between NETWORKING and DCN

Chapter 5 Monitoring and alarm management

5.1 Alarm flow architecture

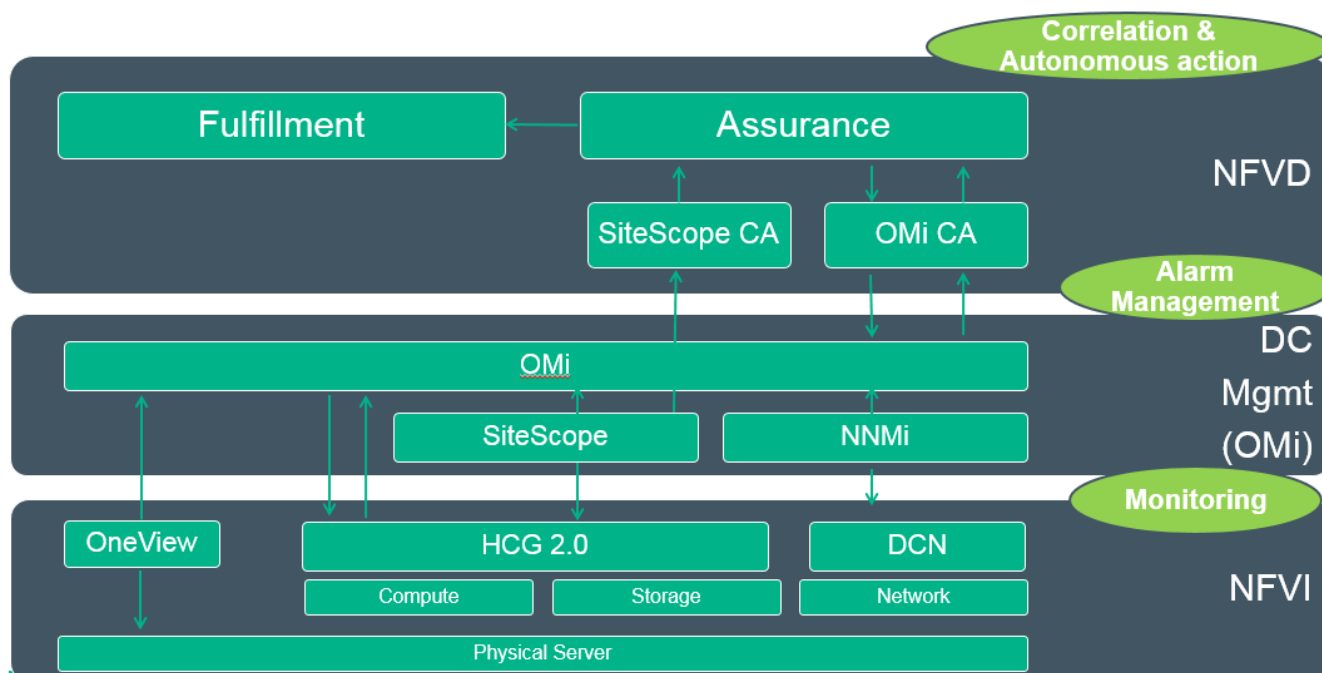


Figure 17: Alarm flow architecture

5.2 NFV Director events integration with OMi



CAUTION: OMi server has a known issue with supporting hostname with characters - hyphen "-", underscore "_". Configure VM hostname in OMi server /etc/hosts file without these characters. [in case of DNS registrations not in place].

5.2.1 Configure webservice endpoint in OMi

To manually forward events to external webservice, webservice endpoint should be configured in OMi GUI. To configure this, go to Administration > Setup and Maintenance > Connected Servers:

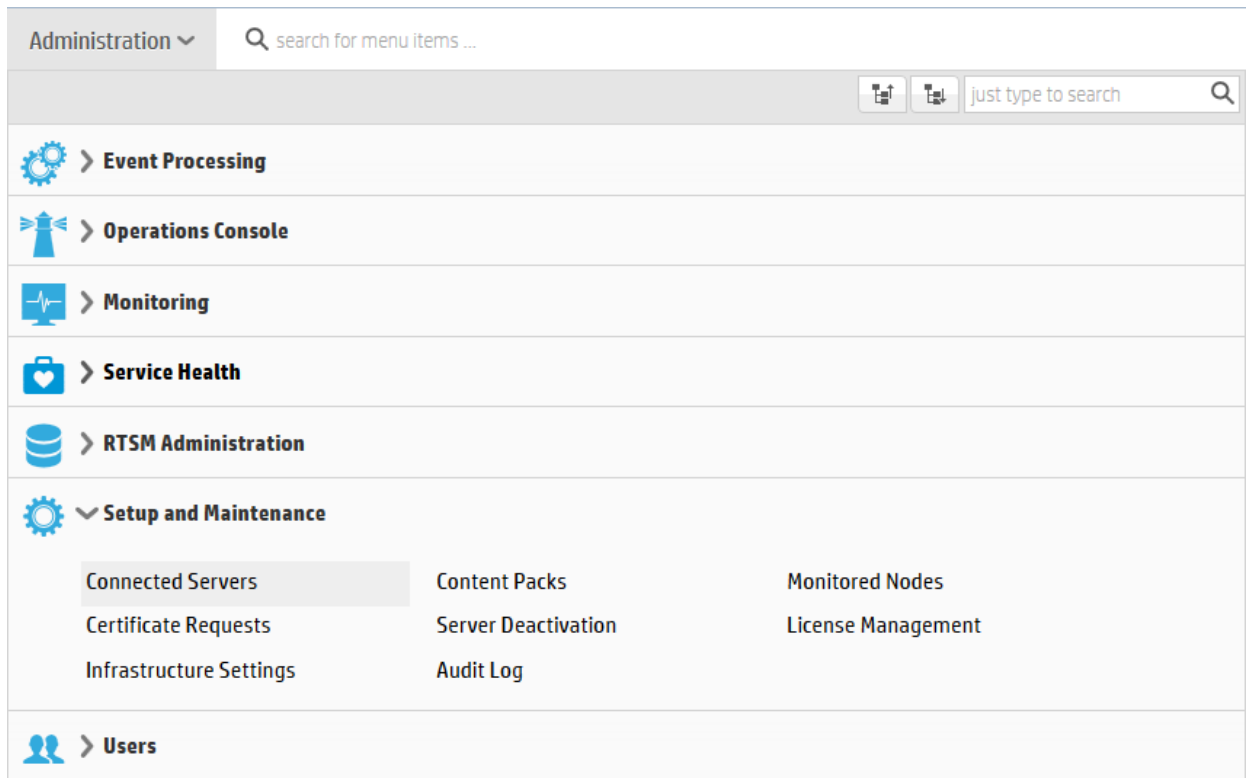


Figure 18: Configure webservice endpoint in OMI

In the right pane, under Connected Servers, configure new server selecting 'External Event Processing' using star button:

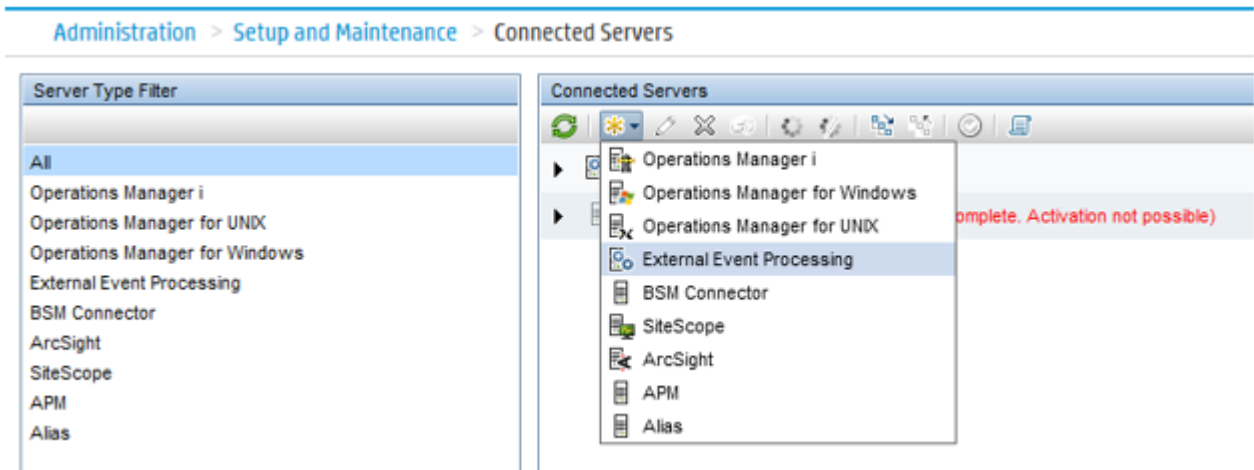


Figure 19: Configure new server

This will open new window as below. Enter name for webservice endpoint in Display Name field. Name field is auto filled. Enter valid description in Description field.

Create New Server Connection - External Event Processing

General

* Display Name:
 * Name:
 Description:

(+) Required field

Active: Activate External Event Processing Server after creation

< Back Next > Finish Cancel Help

Figure 20: Enter webservice endpoint name

Click Next.

In Server Properties tab, Enter fully qualified DNS Name of the machine having webservice running. Select CI Type as 'Management System' (Default).

Create New Server Connection - External Event Processing

Server Properties

Operations Manager i → External Event Processing

Target Server

* Fully Qualified DNS Name:
 * CIType:

Advanced Delivery Options

(+) Required field

< Back Next > Finish Cancel Help

Figure 21: Enter FQDN

Click Next.

In Integration Type tab, select Call External Event Web Service. Enter URL path for the webservice server endpoint. Select 'Support Bulk Transfer' for bulk transfer of events from OMi to webservice endpoint.

Create New Server Connection - External Event Processing

- ✓ General
- ✓ Server Properties
- ▶ Integration Type
 - Outgoing Connection
 - Event Drilldown
 - Incoming Connection

Integration Type

Operations Manager i ↔ External Event Processing

Integration Type

Call Script Adapter

Script Name:

[Manage Scripts](#)

Call External Event Web Service

URL Path:

Supports Bulk Transfer:

Timeout

* Maximum Transaction Time: Seconds

(* Required field)

Figure 22: Enter URL for webservice server

Click Next.

In Outgoing Connection, Enter the port configured for rest webservice. By default, Use Secure HTTP will be selected, unselect this check.

Create New Server Connection - External Event Processing

- ✓ General
- ✓ Server Properties
- ✓ Integration Type
- ▶ Outgoing Connection
 - Event Drilldown
 - Incoming Connection

Outgoing Connection

Operations Manager i → External Event Processing

Event Forwarding & Change Notification

User Name:

Password:

Verify Password:

Port: [Set default port](#)

Use Secure HTTP:

Certificate not specified. [Retrieve from Server](#) (nfvdvm22.ind.hp.com:17870) or [Import from File](#)

Enable Synchronize and Transfer Control:

(* Required field)

Figure 23: Secure HTTP

Click Next.

In Event Drilldown, Enter Fully Qualified DNS name of the server running webservice. By default, Use Secure HTTP will be selected, unselect this check. Enter port of the webservice configured and the User Name, password & Verify Password fields.

Figure 24: Enter FQDN

Click Next.

In Incoming Connection, Please leave the fields blank.

Figure 25: Incoming connection setting

Click Finish.

5.2.2 Create forwarding rule to forward events from OMi

New rule should be created using OMi console to forward events from OMi to external webservice URL configured in Connected Server. This rule will filter events and will forward relevant events to each server configured.

To create new forwarding rule, go to Administration > Event Processing > Event Forwarding.

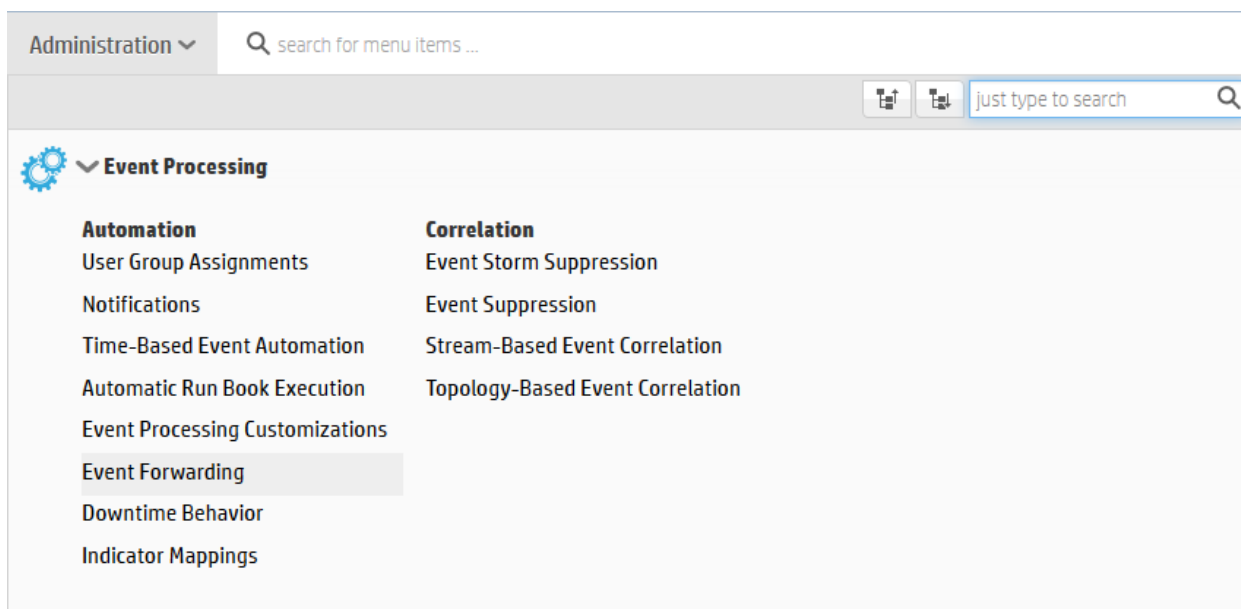


Figure 26: Choose Event Forwarding option in OMi

In the left pane, under Event Forwarding Rules, create new forwarding rule using star button.

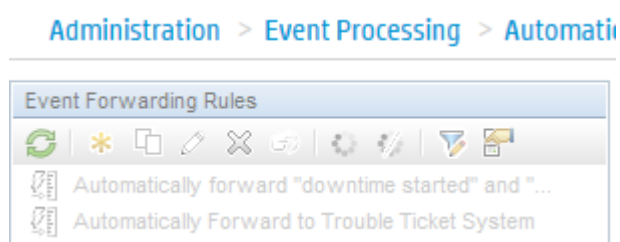


Figure 27: Create new forwarding rule

Enter valid name in Display Name, Enter description (optional).

TestForward - Create New Event Forwarding Rule

▼ **General**

* Display Name:

Description:

Condition

* Event Filter:

Target Servers

*

Figure 28: Create new event forwarding rule

Click browse button next to Event Filter field. Select an Event filter dialog box will open. Click on star button to create New Simple Filter.

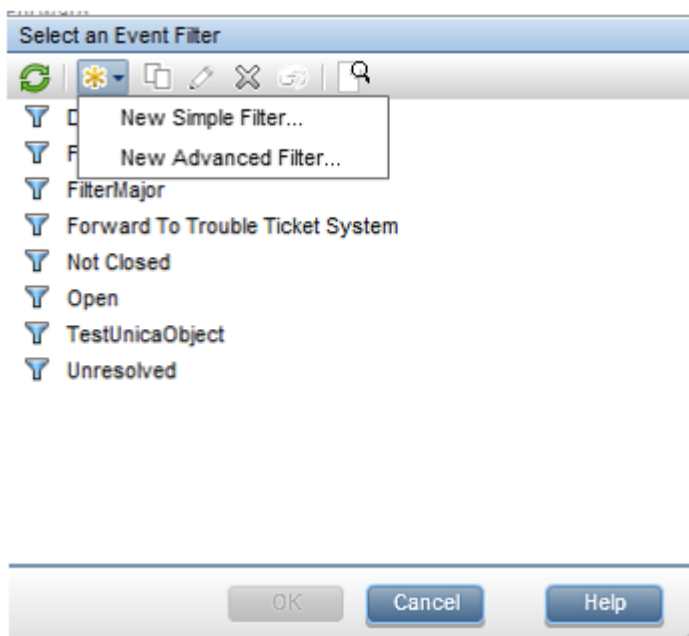


Figure 29: Create new simple filter

In the filter Display Name field, enter name of the filter. Click on Additional Event Properties, Select 'Object'. Enter value as 'HPE' (This can be changed).

Create New Event Filter

* Display Name:

Description:

General
Dates
Additional Event Properties

| | | |
|---|--|--|
| <input type="checkbox"/> Application | equals | <input type="text"/> |
| <input checked="" type="checkbox"/> Object | equals | <input type="text"/> |
| <input type="checkbox"/> Key | equals | <input type="text"/> |
| <input type="checkbox"/> Original Data | equals | <input type="text"/> |
| <input type="checkbox"/> CI Type | equals | <input type="text" value="Select a CI Type"/> <input type="button" value="..."/> |
| <input type="checkbox"/> Subcomponent ID | equals | <input type="text"/> |
| <input type="checkbox"/> Solution | equals | <input type="text"/> |
| <input type="checkbox"/> Custom Attribute | <input type="text"/> equals | <input type="text"/> |
| <input type="checkbox"/> Event Type Indicator | <input type="text" value="<Select an indicator>"/> <input type="button" value="..."/> | |
| | <input checked="" type="radio"/> Any Value <input type="radio"/> Specific Value <input type="text"/> <input type="button" value="..."/> | |

(*) Required field

Figure 30: Create additional event property

Click OK.

Select Target Server as configured webservice endpoint and add it.

5.2.3 Property file change

Got to `/var/opt/openmediation-70/containers/instance-0/ips/omi-ca-10/etc/` directory on the VM where OMi-CA is installed.

Edit `omi-nfvd.properties`

Edit `omi.rest.endpoint` key to the actual URL where webservice endpoint is running.



NOTE: After performing the property changes, the channel adapter have to be un-deployed and redeployed

5.2.4 Generate new events

5.2.4.1 Configuration

In order to manually create events in OMi 10 a policy should be created and deploy to the server.

In OMi console, go to Administration > Monitoring > Policy Templates:

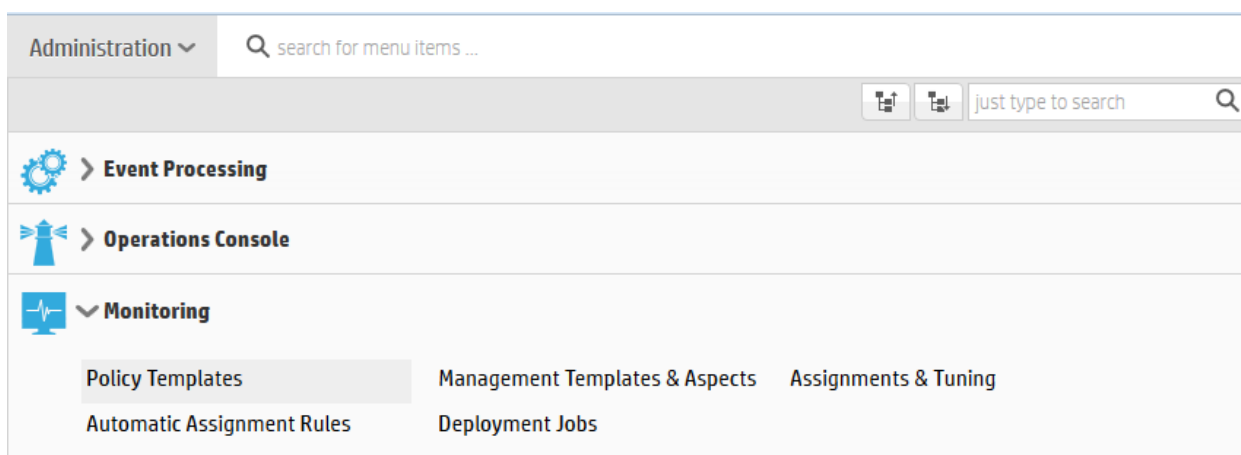


Figure 31: OMi console policy templates

In the left pane, under Policy template Groups, Policy Management > Template Groups, create a new test folder using the star button:

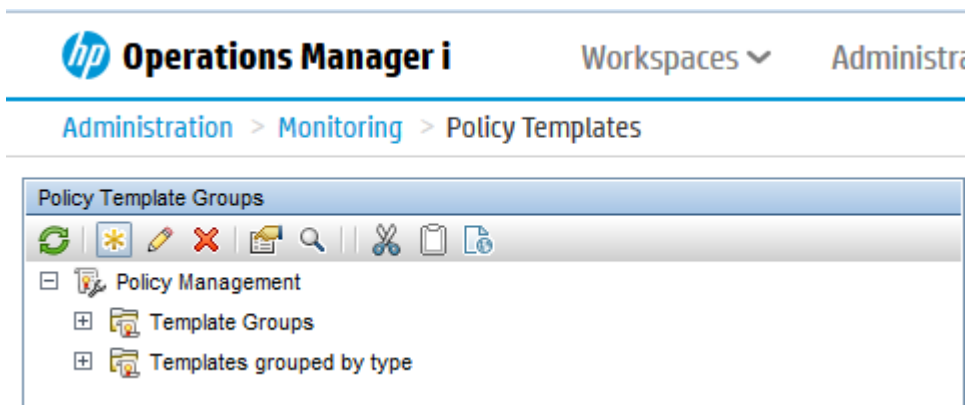


Figure 32: Create new test folder

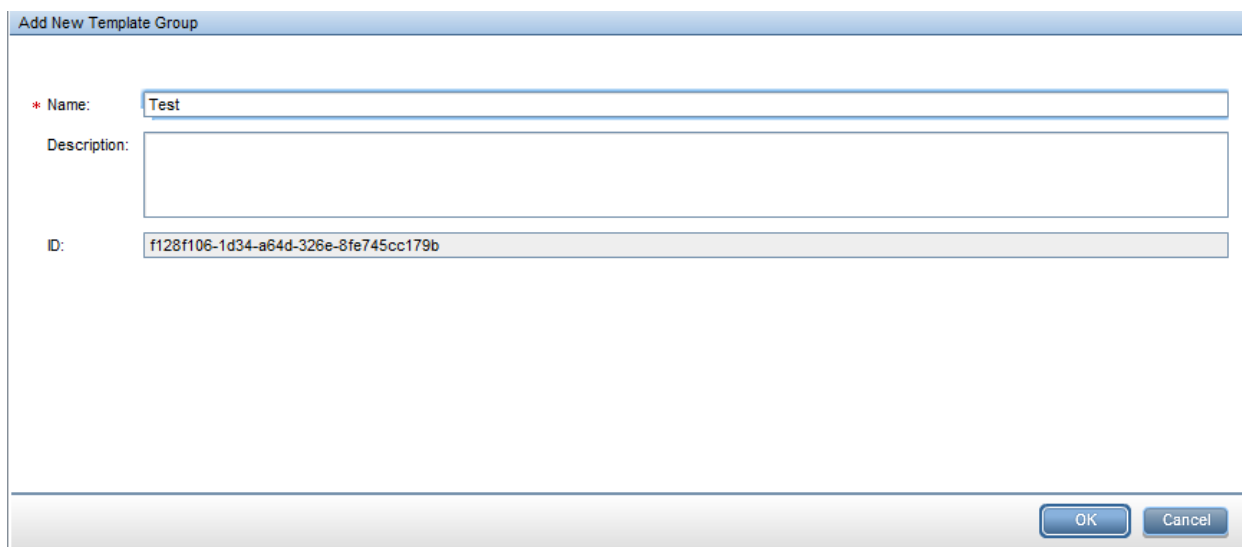


Figure 33: Add new template group

Select this new group, and in the middle pane, use the star to create a New Policy Template

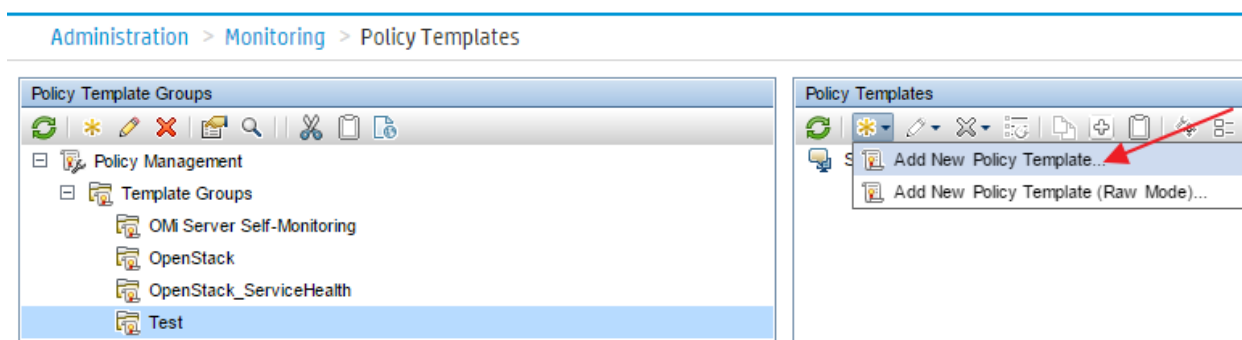


Figure 34: add new policy template

In Type, select 'Open Message Interface':

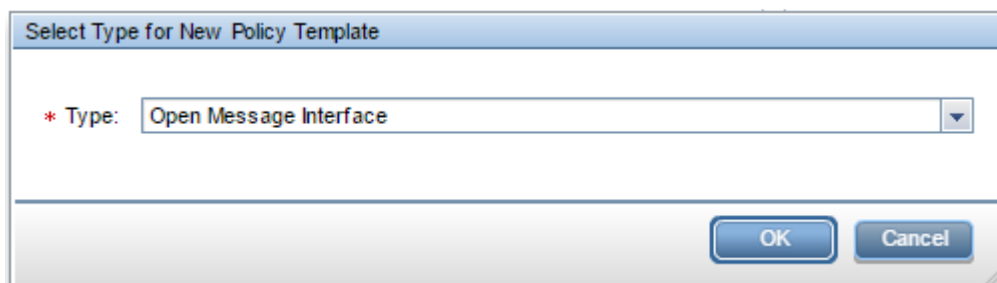


Figure 35: Choose type of policy template

In Properties tab enter a valid name, e.g. 'Send test events':

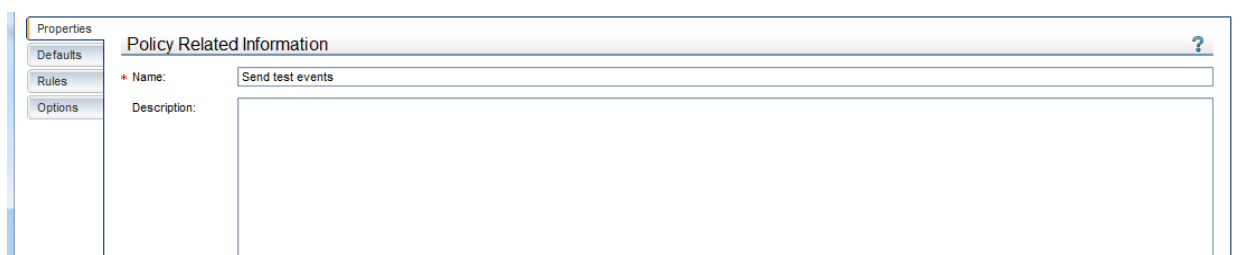


Figure 36: Name the policy template

Leave Defaults tab predefined.

In Rules tab, create a new rule:

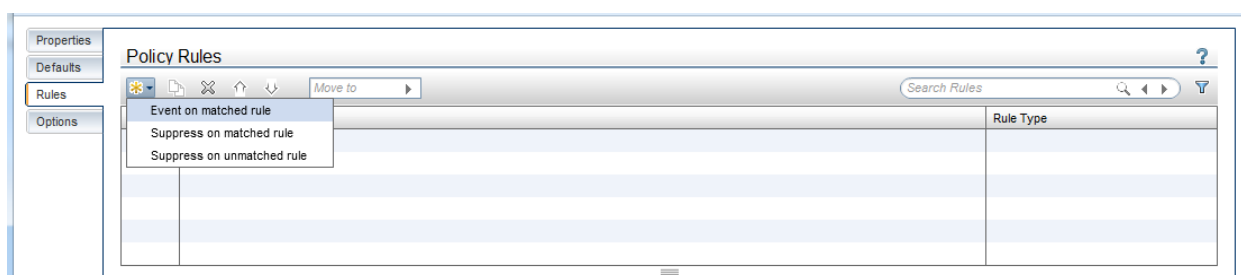


Figure 37: Create new rule

Enter a name for the rule (e.g. 'Test') and select condition for events

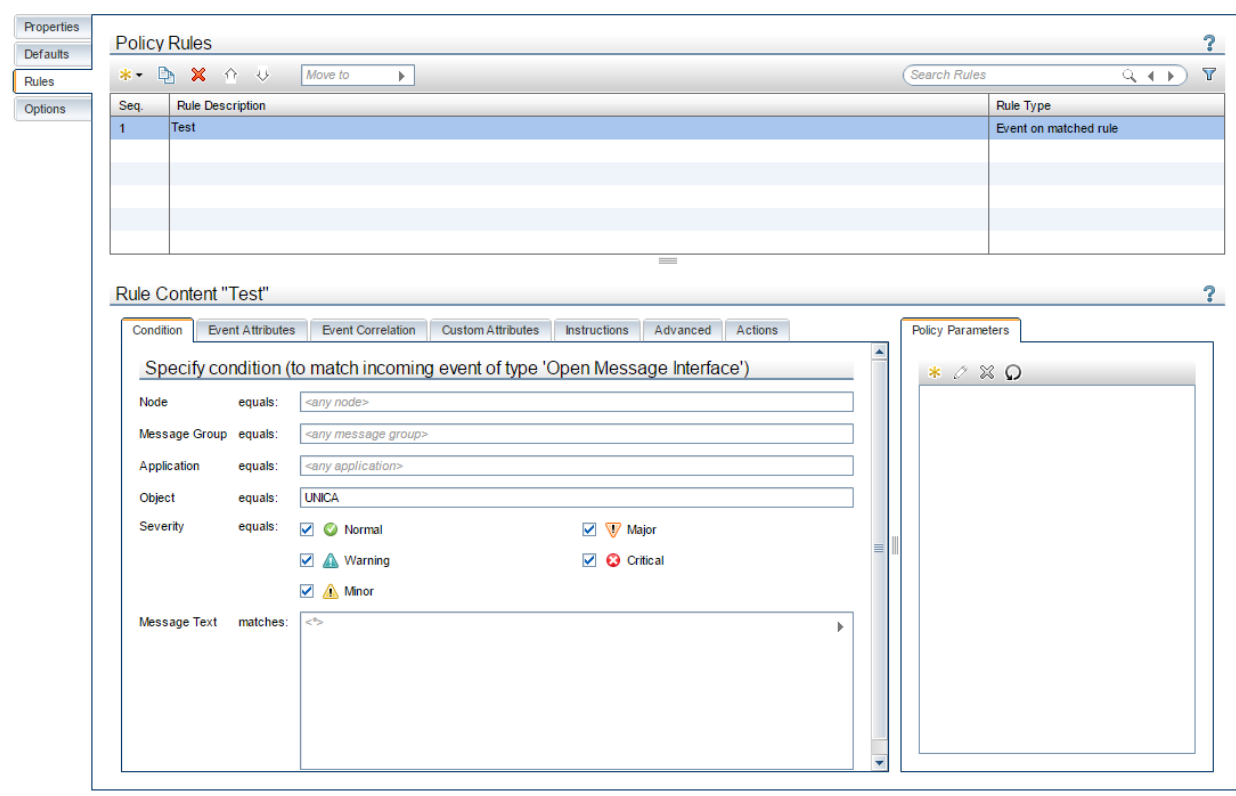


Figure 38: Select condition for events

Save and close.

In Policy Templates screen, select this new 'Send Test Events Policy' and press the assignment button:

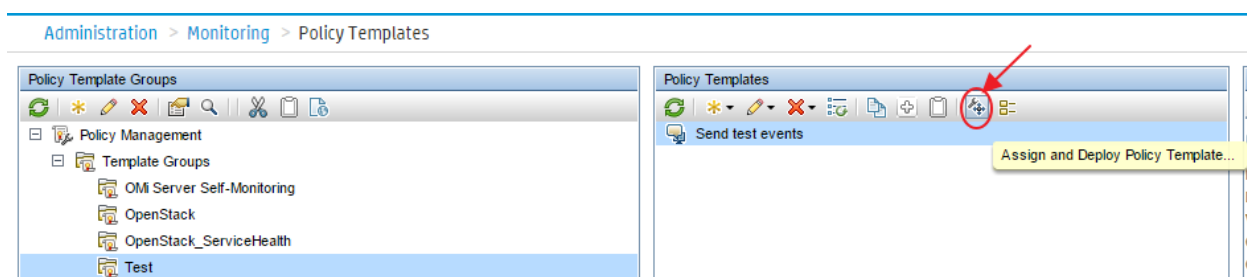


Figure 39: Assign and deploy policy template

And select OMi10 server from the list that appears (e.g., localhost is selected):

Click Next

Click Finish

Note: The below is optional and is only for troubleshooting purposes

Policy will be the automatically deployed to the OMi server. You can check it by running 'ovpolicy -list' on OMi server and see these 'Send Test Event' appears:

```

root@omigw ~]# ovpolicy -list
* List installed policies for host 'localhost'.

-----
Version          Status
-----
le               "OMi Bus Logfile"          enabled  0001.0000
le               "OMi Event Receiver Logfile" enabled  0001.0000
le               "OMi Nanny Logfile"        enabled  0001.0000
letmpl           "OMi Bus Logfile"          enabled  0001.0000
letmpl           "OMi Event Receiver Logfile" enabled  0001.0000
letmpl           "OMi Nanny Logfile"        enabled  0001.0000
monitor          "OMi Server Processes (Linux)" enabled  0001.0000
monitor          "Sys_FileSystemUtilizationMonitor" enabled  0001.0000
monitor          "Sys_PerDiskAvgServiceTime-AT" enabled  0001.0000
monitor          "Sys_PerDiskUtilization-AT" enabled  0001.0000
monitortmpl      "OMi Server Processes (Linux)" enabled  0001.0000
monitortmpl      "Sys_FileSystemUtilizationMonitor" enabled  0001.0000
monitortmpl      "Sys_PerDiskAvgServiceTime-AT" enabled  0001.0000
monitortmpl      "Sys_PerDiskUtilization-AT" enabled  0001.0000
msgi             "Send test events"         enabled  0001.0000
sched            "Health Check - Heart Beat Policy" enabled  0001.0000
schedtmpl        "Health Check - Heart Beat Policy" enabled  0001.0000

root@omigw ~]#

```

Figure 40: Send test event

5.2.5 Send new events

Enter OMi 10 server and generate new messages using command 'opcmsg' and object HPE

For example:

```
opcmsg a=a o=HPE msg_t=TESTAA
```

To view the above sent message in OMi, login to OMi and navigate to Workspaces >> Operations Console >> Event Perspective and select the infrastructure endpoint created for the same.

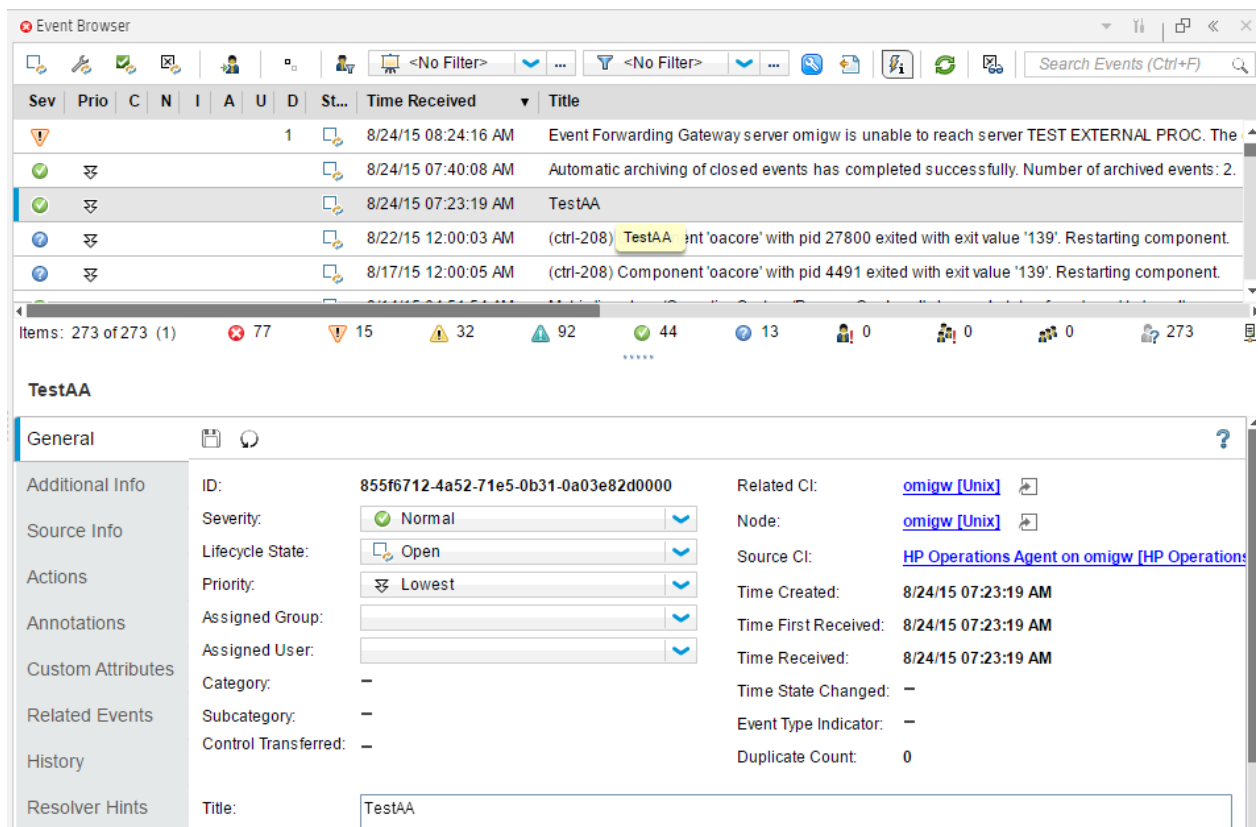


Figure 41: OMi operations console

Opcmsg requires object (o=<*>), application (a=<*>) and message text (msg_t=<*>) to work, but you can also set:

Severity (severity=critical|major|minor|warning|normal)

CI (node=<*>)

5.2.6 Verify event received in OMi-CA log

Go to directory `/var/opt/openmediation-70/containers/instance-0/data/log`

Open `servicemix-info.log` log file.

Events submitted by OMi should be present in `servicemix-info.log` log file.

Response should be send to OMi. This can be verified also if OMi doesn't send event again

5.2.7 Generate events in OMi using `sendEvent` tool

1. Navigate to directory `/opt/HP/BSM/opr/support/`
2. Execute below command to see all available options :

```
./sendEvent.sh -help
```

1. The options to be passed to the below scripts can be added as required.

As an example please find below command:

```
# ./send_event.sh -s critical -t "Instance is live migrated." -a NNMi -o HPE
```

5.3 NFV Director integration with BSM-C



NOTE:

- Oracle JDBC driver needs to be downloaded from the manufacturers site [NFVDv4.0 supports Oracle database 11gR2]; After download, rename it to oracle_jdbc.jar and it has to be placed in /opt/HPE/nfvd/tpp/jboss/standalone/deployments directory.
- Alternately this file can be copied from the Assurance VM [/opt/HPE/nfvd/tpp/jboss/standalone/deployments/oracle_jdbc.jar] or FulFillment VM from /opt/HP/jboss/modules/com/hp/ov/activator/edb/main/oracle_jdbc.jar to /opt/HPE/nfvd/tpp/jboss/standalone/deployments directory
- Rename the file as required to say ojdbc7.jar based on the JDK built version

1. Login into or access the BSM Connector UI
2. Access Event >> Database.
3. In the 'Connection' tab (inside the 'Source' tab), specify the connection settings:
 - o Classpath: path of the .jar file of the JDBC driver in the BSMC server.
 - o The suggested path is: /usr/lib/java/ojdbc7.jar
 - o JDBC Driver Class: name of the class.
 - For Oracle: 'oracle.jdbc.driver.OracleDriver'
 - o Connect string: with the following format:
 - Oracle: 'jdbc:oracle:thin:@<db_host_IP>:1521:xe'
 - o User and password of the database.
 - o Polling interval: interval to execute the query of the policy (by default 5 minutes).

The screenshot shows the 'Database Source' configuration window with the 'Connection' tab active. The fields are as follows:

- Classpath:** /usr/lib/java/ojdbc7.jar
- JDBC Driver Class:** oracle.jdbc.driver.OracleDriver
- Connect string:** jdbc:oracle:thin:@15.154.112.77:1521:xe
- Username:** nfvAlarm
- Password:** [masked]
- Polling Interval:** 0 d, 0 h, 5 m, 0 s

Figure 42: Set DB source

4. In the 'Collection' tab (inside the 'Source' tab), write the query that BSMC will execute. Session variables can be configured, as well as an initial statement. In BSMC the query can be as complex and specific as desired, there are no limits while it is a valid query in the database installed. The queries for the NFV Database can be found in the [Database Query Configuration Section](#).



NOTE:

- The query for Alarms Policy and the query for Updates Policy are different.
- The below are sample queries to check connectivity and data collection. The can be obtained from the link – '[Database Query Configuration Section](#)'

* SQL statement:

```
SELECT ALARM_IDENTIFIER AS ALARM_ID, ALARMRAISEDTIME AS ALARM_TIME, PROBABLECAUSE AS CAUSE, PERCEIVEDSEVERITY AS SEVERITY,
STATE, SOURCEIDENTIFIER AS SOURCE_ID, ADDITIONALINFORMATION AS ADD_INFO, ADDITIONALTEXT AS ADD_TEXT,
SUBSTR(ADDITIONALTEXT, 103, 36) AS RELATED_CI,
TO_CHAR(MAX(ALARMRAISEDTIME), 'DD-MON-RR HH.MI.SS.FF3') AS TIMESTAMP
```

Session variables:

| Result column name | Initial value |
|--------------------|---------------------------|
| TIMESTAMP | 01-JAN-15 12.00.00.000 AM |

Initial value statement:

```
SELECT TO_CHAR((MIN(ALARMRAISEDTIME) - INTERVAL '0.1' SECOND), 'DD-MON-RR HH.MI.SS.FF3 AM') AS TIMESTAMP FROM NFVALARM.ALARM
```

Figure 43: BSMC database query

- To check if the query works and gets the fields, click on the icon just over the query text field, to execute the SQL statement. This is required to map the data in the mapping section later. The same execution can be done for the initial value statement (and the data will appear on 'Initial value sample data').

Initial value sample data

Sample Data

Search Properties

Input Data Properties:

- additional_text
- clearance_timestamp
- correlated_notification_info
- create_timestamp
- custom_field
- event_type
- external_reference_id
- last_update_timestamp
- managed_object
- notification_id
- probable_cause
- severity
- specific_problem
- state

Figure 44: Verify BSMC database query

- In the 'Mappings' tab, data mappings can be set (if necessary). To do so, in the left table, click on New, set a Map Name and in the input Data Property drag and drop one of the input data. Then, with the map selected, in the left table add as many data values to be mapped as needed. Values can be written or dropped from an input data, policy variables or OMi indicators. For NFV Database, the field Severity {'CLEAR', 'CRITICAL'} has to be mapped to recognizable states for the 'Severity' parameter: {'Normal','Critical'}. In the following screenshot shows how it should be set.

Default Value Mapping

| Map Name | Input Data Property | Source Value | Target Value |
|----------|---------------------|--------------|--------------|
| SEVERITY | <SDATA:SEVERITY> | CRITICAL | Critical |
| | | CLEAR | Normal |

Sample Data

Input Data Properties:

- ADD_INFO
- ADD_TEXT
- ALARM_ID
- ALARM_TIME
- CAUSE
- RELATED_CI
- SEVERITY
- SOURCE_ID
- STATE
- TIMESTAMP

Figure 45: Set data mapping

7. In the 'Event Attributes' tab (inside the 'Defaults' tab), fill all the parameters needed. This attributes will be evaluated in OMi console; this is important because they will be the parameters that permit OMi to associate the event to an existing CI. The attributes can be data from the database, mapped data, a string directly written in the text field, operators, OMi indicators, or policy variables.

The screenshot shows the 'Default Event Attributes' configuration interface. The 'Event Attributes' tab is selected, displaying various fields with their corresponding values or templates. The 'Sample Data' tab is also visible, showing a list of input data properties.

Figure 46: Fill event attributes

The following tables contain the fields to fill in the 'Event Attributes' tab for both Alarms and Updates policies, the specific string to copy in the fields and the database data used:

Table 2: Alarms policy: Alarm-to-event attribute mapping

| Event Attributes (OMi) | BSMC String | Data Used (NFV Director) |
|-------------------------|---|--|
| Title | Alarm - ID: <\$DATA:ALARM_ID> (<\$DATA:CAUSE>) | ALARMIDENTIFIER, PROBABLECAUSE |
| Description | <\$DATA:ADD_TEXT> <\$DATA:ADD_INFO> | ADDITIONALINFORMATION, ADDITIONALTEXT |
| Severity | <\$MAP(SEVERITY)> | PERCEIVEDSEVERITY |
| Time Created | <\$DATA:ALARM_TIME> | ALARMRAISEDTIME |
| Related CI | nfvdvm66 | None |
| Source CI | nfvdvm66 | None |
| Source Event ID | <\$DATA:SOURCE_ID> | SOURCEIDENTIFIER |
| Send with closed status | 0 | None |

Table 3: Updates policy: Updates-to-event attribute mapping

| Event Attributes (OMi) | BSMC String | Data Used (NFV Director) |
|------------------------|--|---|
| Title | Alarm update - ID: <\$DATA:UPDATE_ID> (Source alarm ID: <\$DATA:ALARM_ID>) (<\$DATA:CAUSE>) | IDENTIFIER, ALARMIDENTIFIER, PROBABLECAUSE |
| Description | <\$DATA:ADD_TEXT> | ADDITIONALINFORMATION, ADDITIONALTEXT |

| | | |
|-------------------------|---------------------|-------------------|
| | <\$DATA:ADD_INFO> | |
| Severity | <\$MAP(SEVERITY)> | PERCEIVEDSEVERITY |
| Time Created | <\$DATA:ALARM_TIME> | ALARMRAISEDTIME |
| Related CI | nfvdvm66 | None |
| Source CI | nfvdvm66 | None |
| Source Event ID | <\$DATA:SOURCE_ID> | SOURCEIDENTIFIER |
| Send with closed status | 0 | None |

8. In the 'Event Correlation' tab, an event key is assigned for the alarms. This permits to OMi to relate ID's between alarms and updates, and close related events. The data to introduce are the following:

- o For Alarms policy:

Default Event Attributes

Event Attributes | **Event Correlation** | Custom Attributes | Advanced

Event Key: NFVD_ALARM:<\$DATA:ALARM_ID>

Close Events with Key:

Suppress Deduplication on Server

Figure 47: Alarm policy

- o For Updates policy:

Default Event Attributes

Event Attributes | **Event Correlation** | Custom Attributes | Advanced

Event Key: NFVD_ALARM:<\$DATA:UPDATE_ID>

Close Events with Key: NFVD_ALARM:<\$DATA:ALARM_ID>

Suppress Deduplication on Server

Figure 48: Updates policy

9. In the 'Rules' tab, a filtering rule must be created. To avoid looping of events between OMi and NFVD, the rule is set to generate an event for OMi, as long as the 'SOURCE_ID' parameter of the alarm does not have the value 'OMi' (temporary value, to be defined by NFV). To do so, click on 'New > Event on Matched Rule', fill the description if desired and generate a condition in the Condition tab as shown below:

Policy Rules

Event on matched rule

Suppress on matched rule

Suppress on unmatched rule

Events forwarded from OMi to NFV

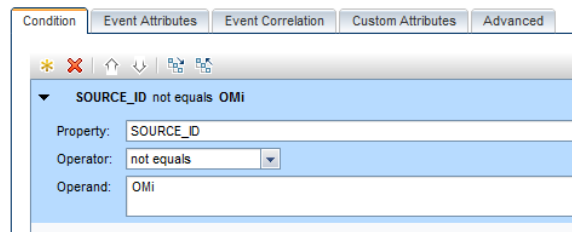


Figure 49: Create filtering role

10. Finally, on the Options tab, specify that **unmatched events are ignored**.
11. When finished configuring, click on 'Save and Close' and the policy can be seen on the main dashboard. The policy is deactivated by default, to activate it select the policy and click on the blue icon on the top, or right click > Activate.

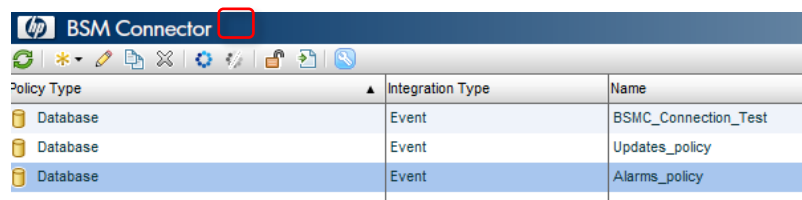


Figure 50: Activate policy

12. For further information regarding the policy creation, check the BSM Connector User Guide available in the [OMi Complete Documentation Set](#).

5.3.1 Database Structure

The tables provided by NFV will have the following fields:

1. Alarms:

Table 4: Alarm database schema

| Column | Type | Comment |
|-----------------------------|-----------|---------------------|
| ALARM_IDENTIFIER | Number | Unique ID |
| ADDITIONALINFORMATION | Text | |
| ADDITIONALTEXT | Text | Contains Related CI |
| ALARMRAISEDTIME | Timestamp | Timestamp for BSMC |
| ALARMTYPE | Text | |
| CLEARANCETIME | Timestamp | |
| CORRELATIONNOTIFICATIONID | Text | |
| EXTERNALREFERENCEIDENTIFIER | Text | |
| LASTUPDATETIME | Timestamp | |
| NOTIFICATIONIDENTIFIER | Text | |
| ORIGINATINGMANAGEDENTITY | Text | |
| PERCEIVEDSEVERITY | Text | {CLEAR, CRITICAL} |
| PROBABLECAUSE | Text | |
| SOURCEIDENTIFIER | Text | |
| SPECIFICPROBLEM | Text | |
| STATE | Text | |

2. Updates:

Table 5: Alarm database schema

| Column | Type | Comment |
|-----------------------------|-----------|-------------------------------|
| IDENTIFIER | Number | Unique ID of the update |
| ADDITIONALINFORMATION | Text | |
| ADDITIONALTEXT | Text | Contains Related CI |
| ALARMRAISEDTIME | Timestamp | Timestamp for BSMC |
| CLEARANCETIME | Timestamp | |
| CORRELATIONNOTIFICATIONID | Text | |
| EXTERNALREFERENCEIDENTIFIER | Text | |
| LASTUPDATETIME | Timestamp | |
| NOTIFICATIONIDENTIFIER | Text | |
| PERCEIVEDSEVERITY | Text | {CLEAR, CRITICAL} |
| PROBABLECAUSE | Text | |
| SOURCEIDENTIFIER | Text | |
| SPECIFICPROBLEM | Text | |
| STATE | Text | |
| ALARM_IDENTIFIER | Number | Unique ID of the source alarm |

5.3.2 Database Query Configuration



NOTE: OMi integrates with Oracle

Collection tab

- Session Variables (Same for Alarms Policy and Updates Policy):

Table 6: Session Variables

| Result Column Name | Initial Value |
|--------------------|---------------------------|
| TIMESTAMP | 01-JAN-15 12.00.00.000 AM |

'TIMESTAMP' variable will act as a pointer who controls the last field read in the table (so that when the query executes periodically, does not read data more than once). The timestamp will be updated every time the query executes.

- Initial Value Statement:
 - Alarms Policy:

```
SELECT TO_CHAR((MIN(ALARMRAISEDTIME) - INTERVAL '0.1' SECOND), 'DD-MON-RR HH.MI.SS.FF3 AM') AS
TIMESTAMP FROM NFVALARM.ALARM
```

- Updates Policy:

```
SELECT TO_CHAR((MIN(ALARMRAISEDTIME) - INTERVAL '0.1' SECOND), 'DD-MON-RR HH.MI.SS.FF3 AM') AS
TIMESTAMP FROM NFVALARM.ALARM_UPDATE
```

This query will be executed when the policy starts. It set the session variable 'TIMESTAMP' to the minimum date value of the table (actually 0.1 seconds earlier, so that the first field is read correctly in the main query).

- SQL Statement:
 - Alarms Policy:

```
SELECT ALARM_IDENTIFIER AS ALARM_ID, ALARMRAISEDTIME AS
ALARM TIME, PROBABLECAUSE AS CAUSE, PERCEIVEDSEVERITY AS
SEVERITY, STATE, SOURCEIDENTIFIER AS SOURCE ID,
ADDITIONALINFORMATION AS ADD INFO, ADDITIONALTEXT AS ADD TEXT,
SUBSTR(ADDITIONALTEXT, 103, 36) AS RELATED_CI,
TO_CHAR(MAX(ALARMRAISEDTIME), 'DD-MON-RR HH.MI.SS.FF3 AM') AS
TIMESTAMP
FROM NFVALARM.ALARM
WHERE ALARMRAISEDTIME > '<$DATA:TIMESTAMP>' AND ROWNUM < 1001
GROUP BY ALARM_IDENTIFIER, ALARMRAISEDTIME, PROBABLECAUSE,
PERCEIVEDSEVERITY, STATE, SOURCEIDENTIFIER,
ADDITIONALINFORMATION, ADDITIONALTEXT
ORDER BY ALARM_TIME ASC
```

- Updates Policy:

```
SELECT IDENTIFIER AS UPDATE_ID, ALARM_IDENTIFIER AS ALARM_ID,
ALARMRAISEDTIME AS ALARM TIME, PROBABLECAUSE AS CAUSE,
PERCEIVEDSEVERITY AS SEVERITY, STATE, SOURCEIDENTIFIER AS
SOURCE_ID, ADDITIONALINFORMATION AS ADD_INFO, ADDITIONALTEXT
AS ADD TEXT, SUBSTR(ADDITIONALTEXT, 103, 36) AS RELATED_CI,
TO_CHAR(MAX(ALARMRAISEDTIME), 'DD-MON-RR HH.MI.SS.FF3 AM') AS
TIMESTAMP
FROM NFVALARM.ALARM UPDATE
WHERE ALARMRAISEDTIME > '<$DATA:TIMESTAMP>' AND ROWNUM < 1001
GROUP BY IDENTIFIER, ALARM_IDENTIFIER, ALARMRAISEDTIME,
PROBABLECAUSE, PERCEIVEDSEVERITY, STATE, SOURCEIDENTIFIER,
ADDITIONALINFORMATION, ADDITIONALTEXT
ORDER BY ALARM_TIME ASC
```

Each query sets the timestamp to the highest value of the result set, gets new alarms/updates since the last timestamp, and orders it by date.

A limit of 1000 events per interval (5 minutes by default) is set. This is in case the connection between NFVD and BSMC is lost and a big number of alarms are to be read from the database when reconnecting. This measure will avoid event storm in OMi and make the data easier to read and control.

5.4 BSM-C integration with OMi

To configure BSM Connector to forward events to OMi after finishing the installation, on the BSMC server, navigate to the following path:

```
cd /var/opt/OV/installation/HPOprBSMC
```


Execute the following instruction:

```
bsmc-conf.sh -srv <hostname> [-cert_srv <hostname>] -admin_user <username> <password>
```




NOTE: The above instruction has some more input parameters available, but this is the basic configuration. The Certificate Server must be introduced in case OMi Gateway and OMi DPS are installed in distributed machines. In that case, the main server should be the gateway and the certificate server should be the DPS


5.5 OpenStack OMi event payload samples

| Event Payload Samples | Example |
|--|---|
| 700.001 Instance Failed |  |
| 700.003 Instance Rebooted | |
| 700.004 Instance Paused | |
| Instance Suspended | |
| Compute Node Down/Up | |
| Live Migration | |
| Cold Migration | |
| Evacuation | |
| Server/Compute node brought down for maintenance | |

5.6 VMWare Event Payload

| Event Payload Samples | Example |
|-----------------------|---|
| VM Power Off/On |  |
| VM Migrating/Migrated | |
| Compute node Up/Down | |

5.7 OMi Event Payload

| Event Payload Samples | Example |
|--|---|
| Compute node Up/Down |  |
| Server/Compute node brought down for maintenance | |

Appendix A NFV Director topology structure

What is needed

Within NFV Director it is needed to have at least 1 Datacenter tree attached to the resource pool of the domain. The Datacenter tree is the representation of the VIM with all its structure including:

- Servers and its OpenStack available resources
- Regions and the OpenStack modules related to them

Some Datacenters may have the Networking module handled by a DCN module so it is needed to have a

RELATIONSHIP between the OpenStack module and the DCN module

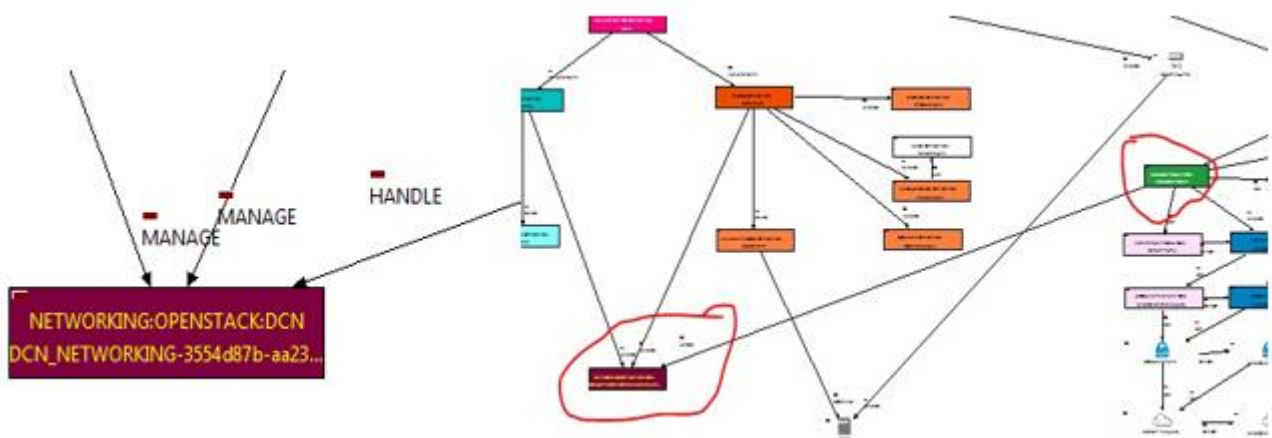


Figure 51: Relationship between OpenStack and DCN modules

Also in order to make use of DCN floating ips, the shared management network the datacenter must have RELATIONSHIP to the corresponding SHARED_RESOURCE:DCN

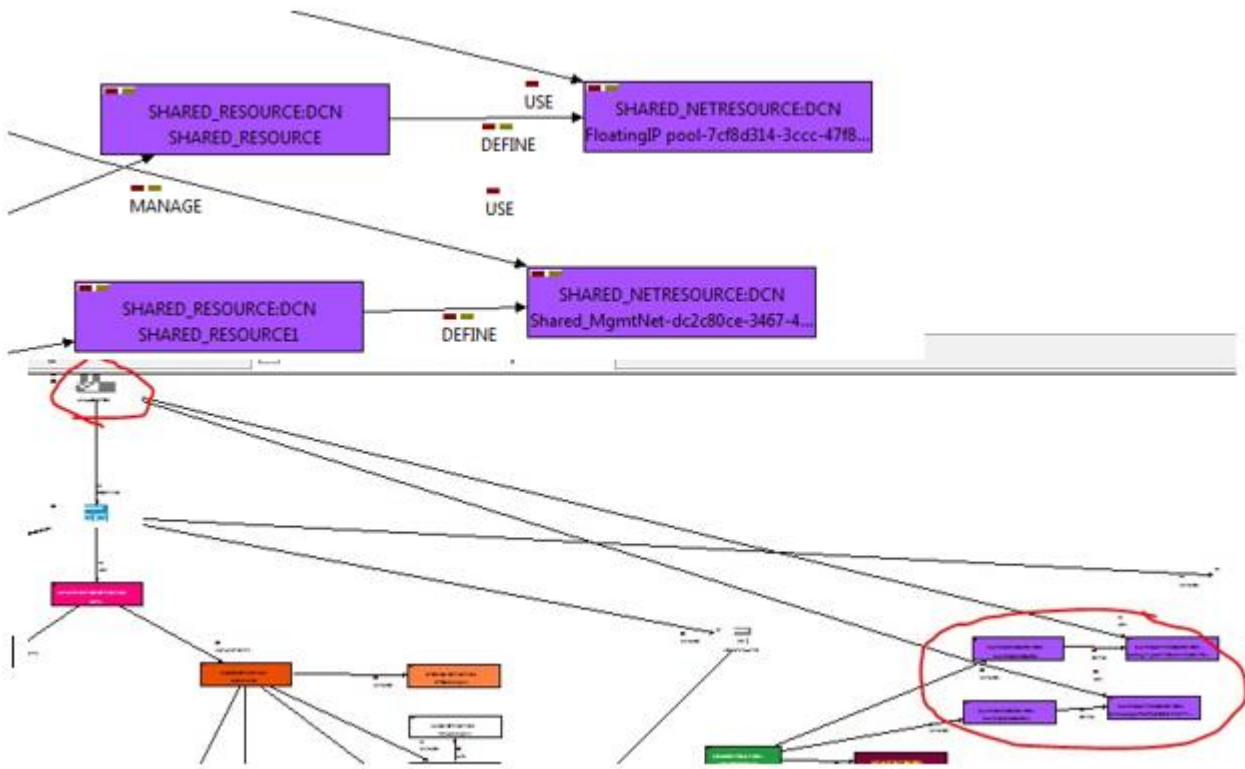


Figure 52: DC to SHARED_RESOURCE:DCN relationship

If the Discovery version installed only discover the Datacenter the DCN side must be manually uploaded.

If the Discovery version installed discover the Datacenter AND the DCN side it is still needed to create the relationships:

- From datacenter to SHARED_RESOURCE:DCN
- From SDN_CONTROLLER:DCN to NETWORKING:OPNESTACK:DCN to

NFV Director SDN work

Important attributes

Authorization

Make sure user password and URL are manually and correctly set into AUTHORIZATION artifact

Shared network artifacts

Make sure those do NOT have allocation pools configured (start / end ip)

Subnetwork of Virtual Link on Tenant_mngt template

Make sure it has blank value on the gateway_ip attribute of the subnetwork

What is needed

As starting point at least 2 shared resources must be MANUALLY created in DCN at platform level (so NOT tied to any organization) AND the corresponding OpenStack side OpenStack

- One management network for the Datacenter
- At least One floating ip pool

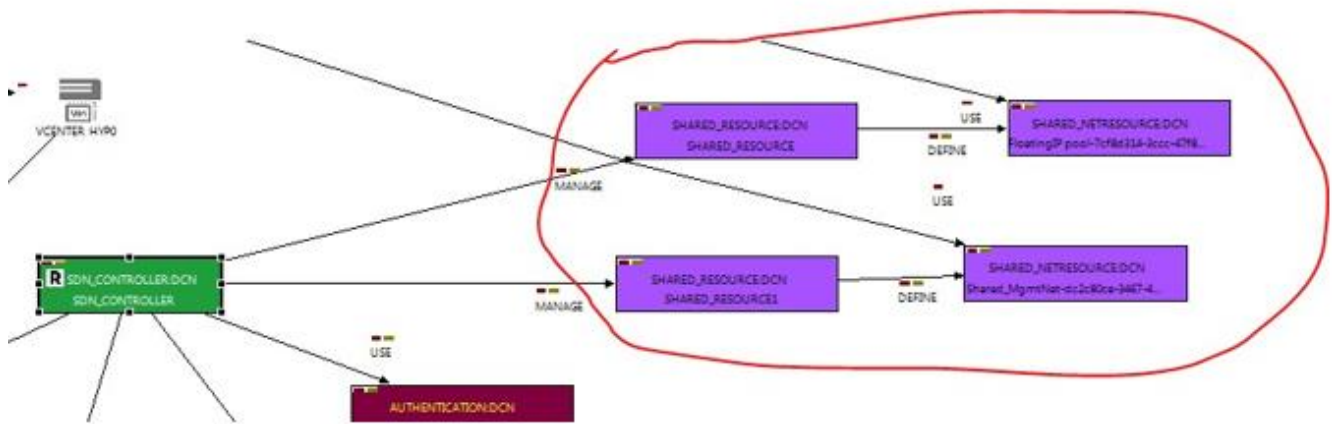


Figure 53: Manually create shared resources

MANAGEMENT organization with a MANAGEMENT L3Domain must be manually created in DCN containing the management network with its macros with its corresponding on the OpenStack side

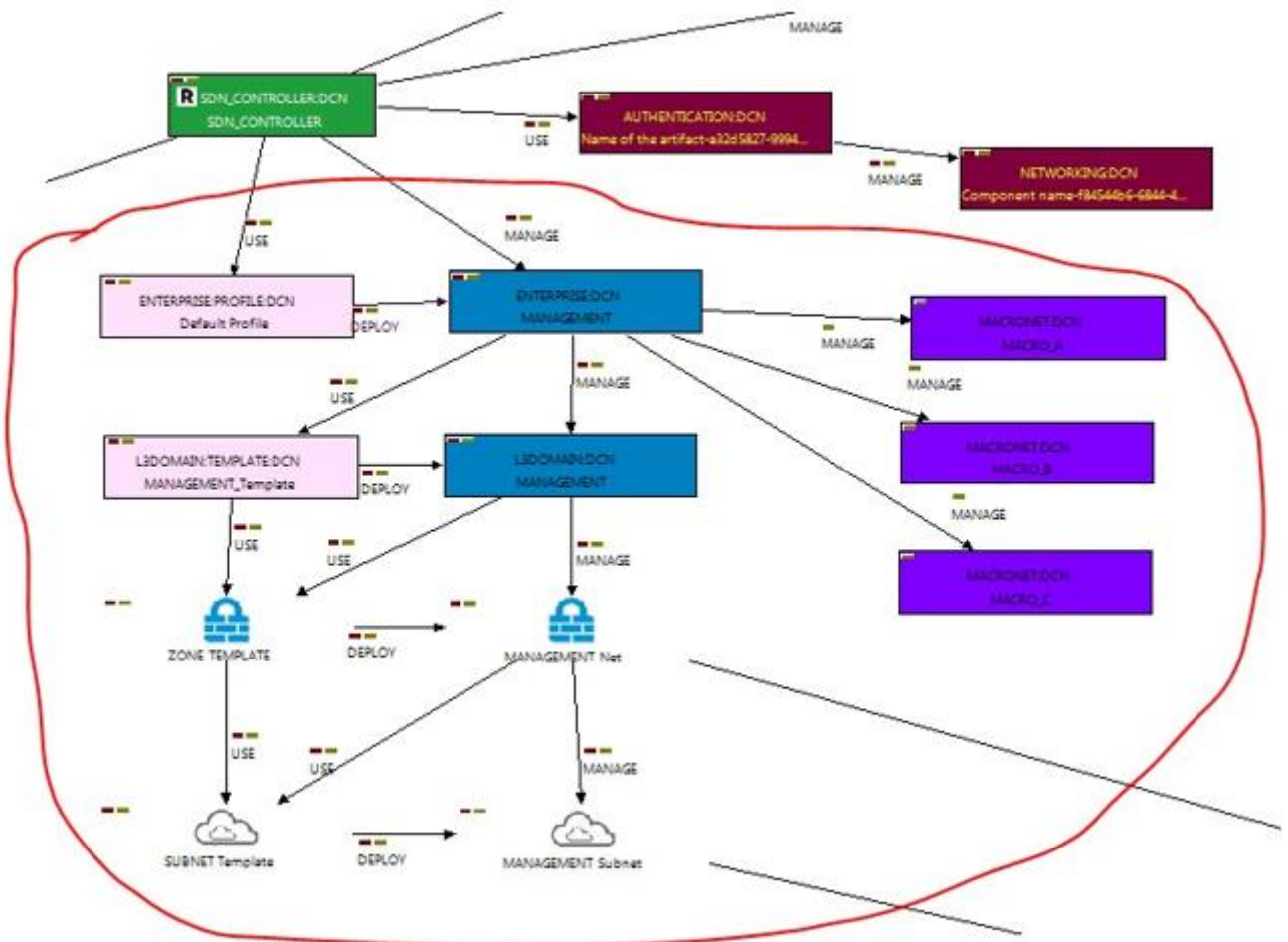


Figure 54: Manually create L3Domain

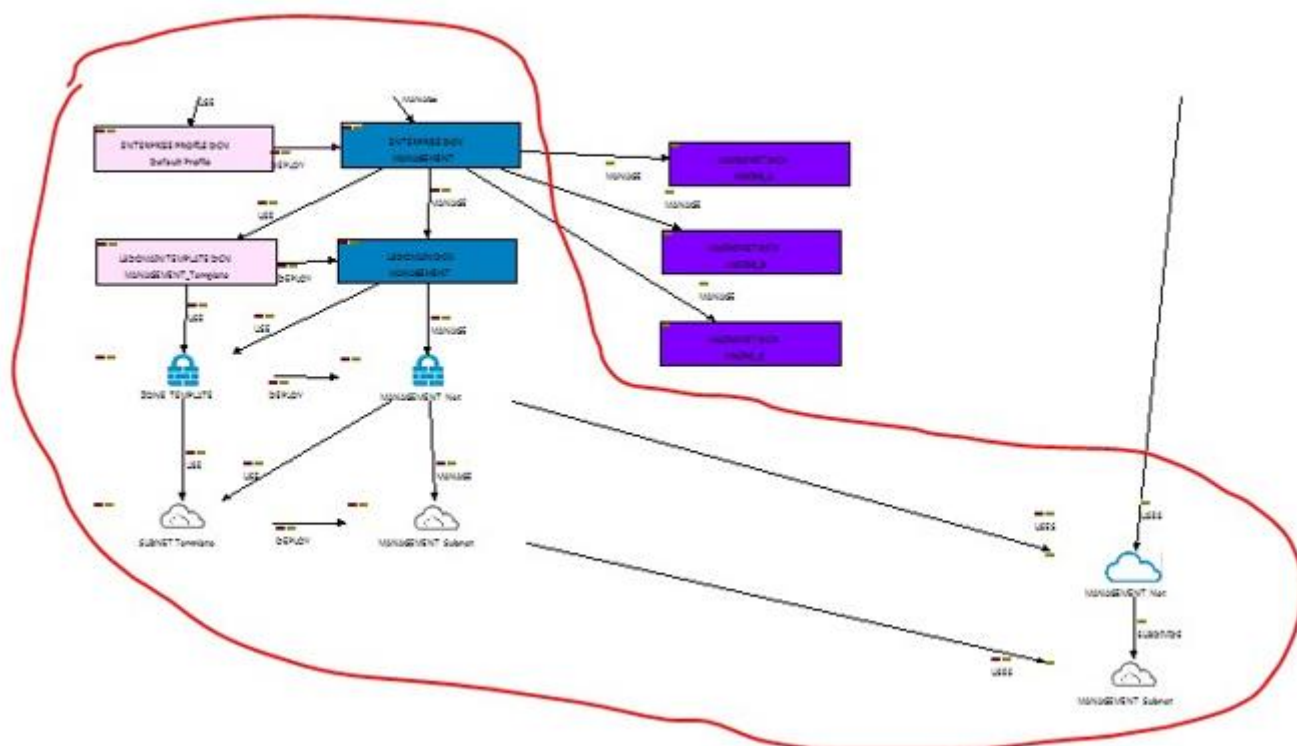


Figure 55: Manually create L3Domain

NFV Director OpenStack work

Important attributes

Authorization

Make sure user password and URL are manually and correctly set into AUTHORIZATION artifact

Server hostnames

Make sure hostnames of server matches (case sensitive) the OpenStack names

Subnetwork of Virtual Link on virtual link template

Make sure it has NO_GATEWAY value on the gateway_ip attribute of the subnetwork

What is needed

Within OpenStack it must exist the management tenant MATCHING the management L3domain containing a management network matching the Management DCN network.

