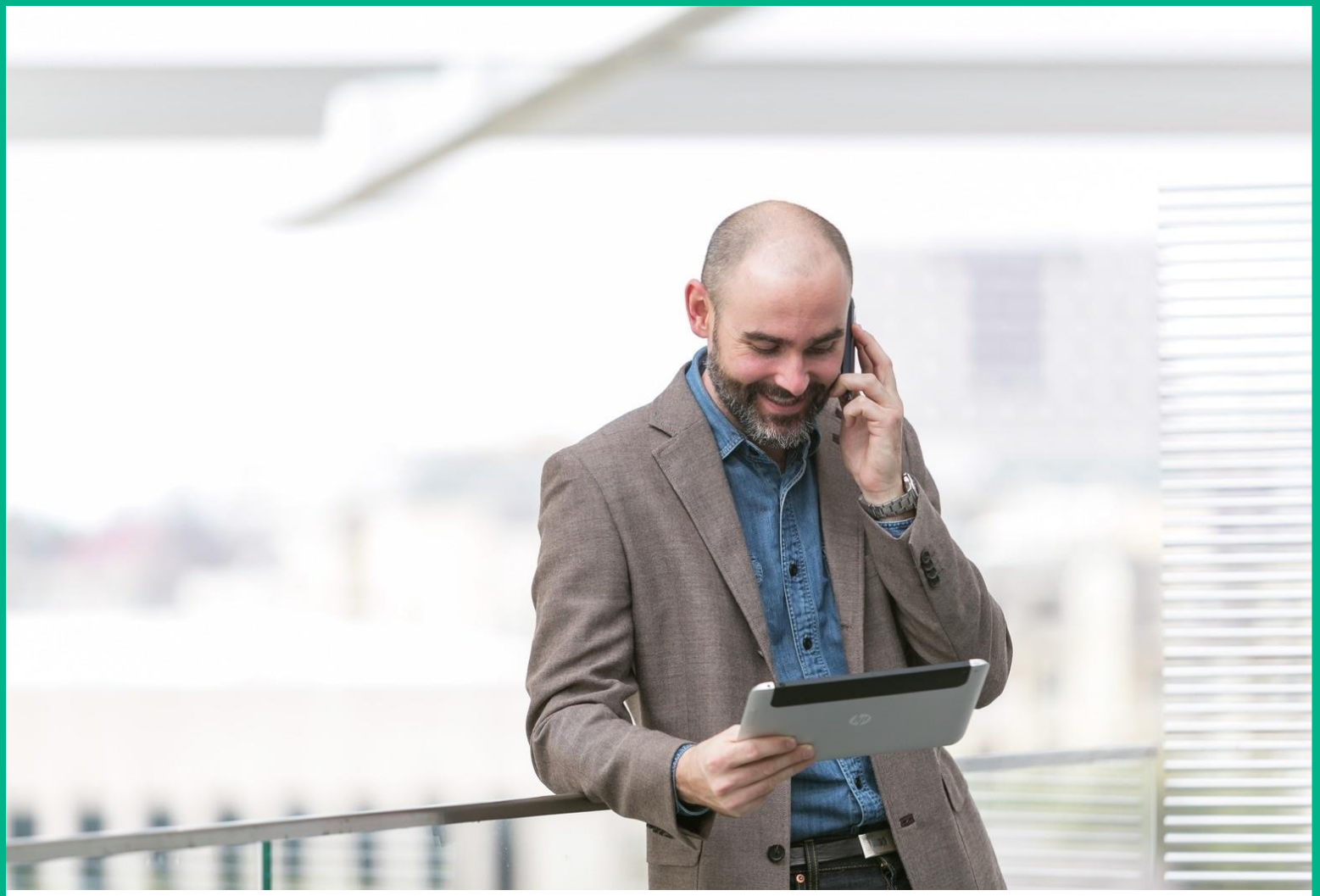


HPE NFV Director

VIM Integration Guide

Release 4.2
First Edition

Notices

Legal notice

Printed in the US

Trademarks

Contents

List of tables

List of figures

Preface

About this guide

This document describes the procedure to integrate VIM with NFV Director, that includes prerequisites to integrate VIM with NFV Director, procedure to import VIM certificate into NFV Director, integrating DCN with NFV Director, and discovery utilities.

- Chapter 1: Introduction
- Chapter 2: Discovery using GUI
- Chapter 3: Discovery using command line utility
- Chapter 4: NFV Director discovered resources
- Chapter 5: Discovery utilities
- Chapter 6: Multi VIM duplicate compute hostname scenario
- Chapter 7: VIM Certificates
- Chapter 8: DCN Integration

By following the procedures in this document, Helion CG and OpenStack Kilo resources can be discovered and integrated with NFV Director.

Audience

This document is any stakeholder requiring to perform resource discovery using the NFV Director, and to create VNFs using the discovered VIM. Pre requisite is to have knowledge of NFV Director Concepts, and an understanding of the NFV Director resource model.

Document history

Table 1: Document history

Edition	Date	Description
1.0	28 Feb 2017	First edition.

Chapter 1
Introduction

VIM integration Guide explains the various aspects of integrating VIM with NFV Director. First step to integrating VIM is to discover the resources managed by VIM into NFV Director. Once discovered, NFV Director should be able to create and monitor the VNFs using the VIM.

This document explains the process to discover a VIM, steps to import VIM certificates into NFV Director to enable monitor deployment of the VNFs that are created using those VIMs, and explains the process to integrate DCN topology with the discovered Datacenter.

Here is an overview of steps involved in integrating VIM with NFV Director:

1. Pre requisites to be met before VIM discovery can be performed.
2. Discover the VIM resources into NFV Director.
3. If there are compute nodes with same name, resolve the ambiguity.
4. Integrate external DCN network with the discovered DataCenter, if required.
5. Import the VIM certificates into HP SiteScope before deploying VNFs using the discovered VIM.

1.1 Pre requisites

1.1.1 NFV Director installation and configuration

NFV Director must be successfully installed and configured. Refer to NFV Director Installation and Configuration Guide for detailed instructions.

1.1.2 VIM patches

Ensure to install the latest patches of the VIM based on the recommendations from the VIM vendor.

1.1.3 Create Cinder volume types in VIM

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

Make sure to configure the CINDER volume types with the following predefined names:

- Vmware-Quality-A
- Kvm-Baremetal-Quality-A
- Vmware-Quality-B
- Kvm-Baremetal-Quality-B
- All-vsa-Quality-A

1.2 Overview of resource discovery

NFV Director is responsible for managing the lifecycle of VNF and it's important for NFV Director to know the complete topology of the OpenStack resources.

The complete list of OpenStack resource topology is described below.

The Discovery process described in this document helps in automatic discovery of OpenStack resources and their inter-relationship.

It is an optional component in the NFV Director.

1.2.1 Architectural View

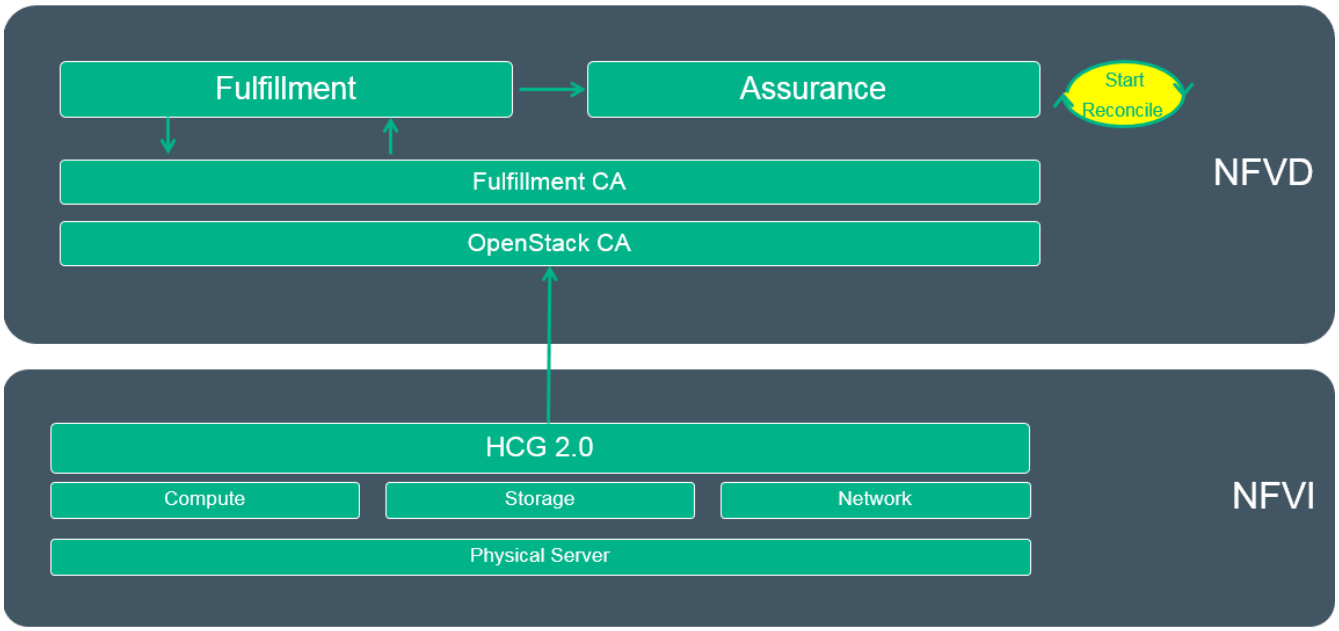


Figure 1: OpenStack Discovery Architecture

Discovery process consists of two modules:

Discovery Module: Interacts with VIM and queries for resource information, and stores the data into NFV Director in artifact-relationship model.

Reconciliation Module: Reconciliation module builds delta information to reconcile. The final data will be prepared and persisted to NFV Director via REST API's.

Below is the pictorial diagram that explains the design approach of NFV Director Discovery.

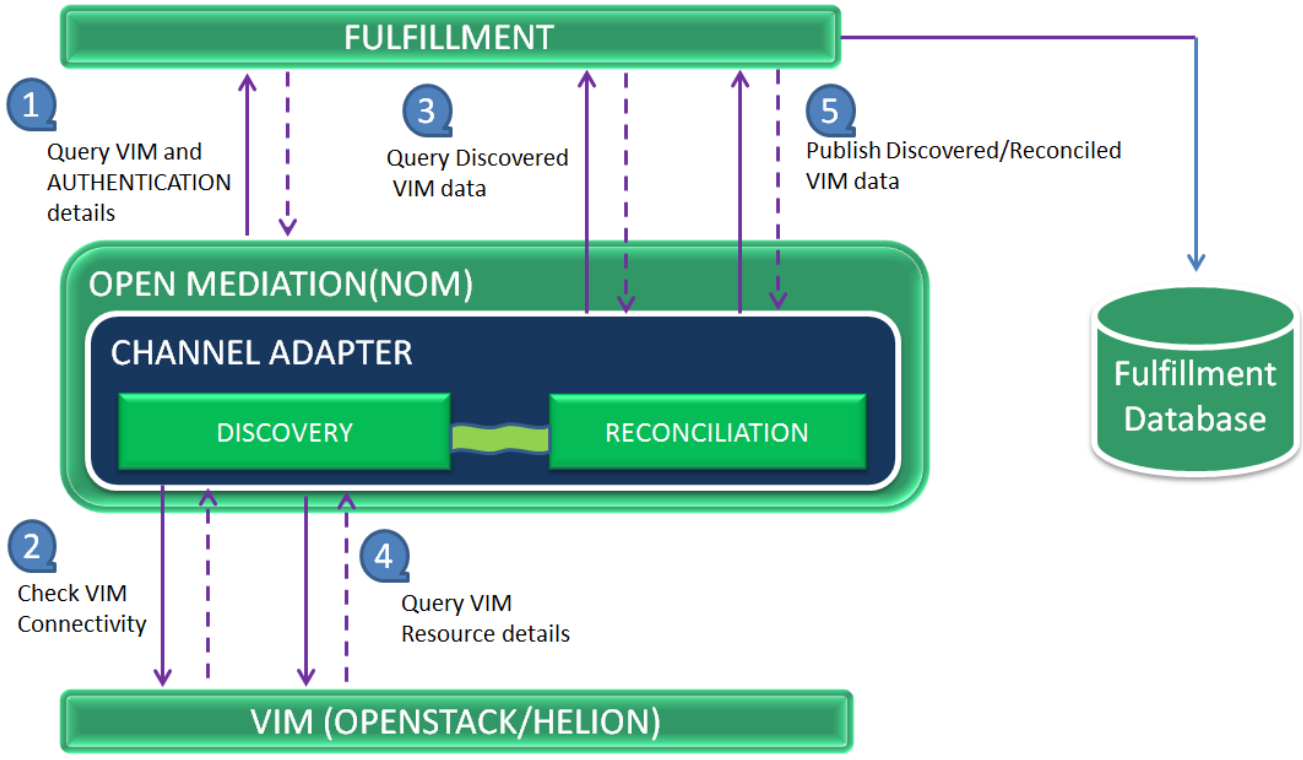


Figure 2: OpenStack Discovery NFV Director components

1.3 Verifying VIM endpoints

Follow the steps below to verify that NFVD can access VIM services before actually proceeding with the discovery.

1. Get the Token using the below curl: Replace angled brackets '<...>' with appropriate values

```
curl -k -X POST -H "Content-Type: application/json" --data "{\"auth\": {\"tenantName\": \"<os-tenant-name>\", \"passwordCredentials\": {\"username\": \"<os-user-name>\", \"password\": \"<os-password>\"}}}" <os-keystoneV2-complete-url>
```

Where

<os-tenantName> is the VIM tenant name,

<os-user-name> is the user name having access to the above tenant,

<os-password> is the password for the above user,

<os-keystoneV2-complete-url> is *https://<IP>:5000/v2.0/tokens*

We get the following response snippet:

```
"access": {
   "token": {
     "issued_at": "2015-04-06T05:02:01.202679",
     "expires": "2015-04-06T06:02:01Z",
     "id": "f6e7727541d44d6bb5f1be808e8d6ad5",
     "tenant": {
       "description": null,
       "enabled": true,
       "id": "4836f3ca53e549679dfcf629ff2511ee",
       "name": "admin"
     },
     "audit_ids": ["9icBYv0qT6yhS4Tr9ubRRw"]
   },
            .....
            .....
            .....
            "serviceCatalog": [
    {
      "endpoints": [
        {
          "adminURL": "http://<compute-ip>:8774/v2/4836f3ca53e549679dfcf629ff2511eeError! Hyperlink reference not valid.",
          "region": "RegionOne",
          "internalURL": "http://<compute-ip>:8774/v2/4836f3ca53e549679dfcf629ff2511eeError! Hyperlink reference not valid.",
          "id": "e2417d8b267649498ea03f4bafca8be2",
          "publicURL": "http://<compute-ip>:8774/v2/4836f3ca53e549679dfcf629ff2511ee"
        },
        {
          "adminURL": "http://<compute-ip>:8774/v2/4836f3ca53e549679dfcf629ff2511ee",
          "region": "Regiontwo",
          "internalURL": "http://<compute-ip>:8774/v2/4836f3ca53e549679dfcf629ff2511eeError! Hyperlink reference not valid.",
          "id": "e2417d8b267649498ea03f4bafca8be2",
          "publicURL": "http://<compute-ip>:8774/v2/4836f3ca53e549679dfcf629ff2511eeError! Hyperlink reference not valid."
        }
      ],
      "endpoints_links": [],
      "type": "compute",
      "name": "nova"
    },
……..
```

Note: The above response snippet is illustrating the compute node end-point. Response data will also contain details for all other node end-points, like, network, glance, cinder etc.

2. Using the access.token.id from the above response for each node end-point, verify the following end points (for all regions if there are many):
    a. Nova
    b. Neutron
    c. Glance
    d. Cinder
    e. System Inventory (HCG only)

```
curl -k -X GET -H "Accept: application/json" -H "X-Auth-Token:<token-taken-from-keystone-curl" https://<service-endpoint-ip>:<service-endpoint-port>
```

Where

<token-taken-from-keystone-curl> is the access.token.id from above response.

<service-endpoint-ip> and port is the ip address of the node.

Response will list the API versions hosted for this VIM service. If we get the response for the above query, it confirms that the node end-point is accessible.

Sample response snippet is as follows:


```
      {
  "versions":[
    {
      "status":"SUPPORTED",
      "updated":"2011-01-21T11:33:21Z",
      "links":[
        {
          "href":"http://15.154.112.35:8774/v2/",
          "rel":"self"
        }
      ],
      "min_version":"",
      "version":"",
      "id":"v2.0"
    },
    {
      "status":"CURRENT",
      "updated":"2013-07-23T11:33:21Z",
      "links":[
        {
          "href":"http://15.154.112.35:8774/v2.1/",
          "rel":"self"
        }
      ],
      "min_version":"2.1",
      "version":"2.3",
      "id":"v2.1"
    }
  ]
}
```

1.4 MWFW authentication

It’s needed to verify that first parameters of file: /etc/opt/OV/ServiceActivator/config/OpenStack.properties “mwfwUser” and “mwfwPassword” match with the credentials to authenticate NFV-D in MWFW (HPSA) context. By default:

```
mwfwUser=admin
mwfwPassword=admin123
authenticationJsonV2={ \"auth\":{\"passwordCredentials\":{\"username\":\"${USER}\", \"password\":\"${PASSWORD}\"
},\"tenantName\":\"${TENANT}\" } }
authenticationJson={ \"auth\": { \"identity\": { \"methods\": [ \"password\" ], \"password\": { \"user\": { \"domain\": { \"name\":
\"${DOMAIN}\" }, \"name\": \"${USER}\", \"password\": \"${PASSWORD}\"} }}}}
openstack.url=
```

If HPSA credentials change it’s mandatory to update this file parameters properly. In other case Openstack plugin will fail.

1.5 Usage of VIM's public endpoints

By default, NFV-D uses adminURL endpoints for every interaction with all the Openstack services. It is a pre-requisite you can reach those endpoints from your VM where you are running NFV-D Fulfillment.

If you cannot access the adminURL endpoints but you can access the publicURL endpoints, NFV-D can use those publicURLs endpoints for all the request.

To do that, you have to modify the following file: /etc/opt/OV/ServiceActivator/config/OpenStack.properties

By default, the typical content for this file is:

```
mwfwUser=admin
mwfwPassword=admin
authenticationJsonV2={ \"auth\":{\"passwordCredentials\":{\"username\":\"${USER}\", \"password\":\"${PASSWORD}\"
},\"tenantName\":\"${TENANT}\" } }
authenticationJson={ \"auth\": { \"identity\": { \"methods\": [ \"password\" ], \"password\": { \"user\": { \"domain\": { \"name\":
\"${DOMAIN}\" }, \"name\": \"${USER}\", \"password\": \"${PASSWORD}\"} }}}}
openstack.url=
```

Only allowed values for the *openstack.url=* property are: **[<empty>|public]**. Any other content will be ignored and it will assume it's an <empty> value.

Public endpoints can also be set at VIM level too. For this you have to modify the attribute *CREDENTIALS.OpenstackEndpoint* of the AUTHENTICATION:OPENSTACK artifact. Allowed values are **[<empty>|public|admin]** and it will take preference over the Openstack.properties value, but not the value specified in a particular operation.

If a specific operation (for example, CREATE_SERVER operation) needs to be done with the user admin role, set (on the template file for that operation located under /etc/opt/OV/ServiceActivator/config/NFVTemplates/ folder) the openstack.url attribute.

```
[root@testing-vm3-41 ~]# ll /etc/opt/OV/ServiceActivator/config/NFVTemplates/CREATE_SERVER
total 16
-rw-r--r--. 1 root root   74 Jan 27 03:24 CREATE_SERVER_HP_NOVA_HELIONCG_v1.1.properties
-rw-r--r--. 1 root root 3908 Jan 27 03:24 CREATE_SERVER_HP_NOVA_HELIONCG_v1.1.template
-rw-r--r--. 1 root root   74 Jan 27 03:24 CREATE_SERVER.properties
-rw-r--r--. 1 root root 2855 Jan 27 03:24 CREATE_SERVER.template
```

Default content is:

```
[root@testing-vm3-41 ~]# cat
/etc/opt/OV/ServiceActivator/config/NFVTemplates/CREATE_SERVER/CREATE_SERVER.properties
http.operation=POST
http.url.sufix=/servers
openstack.endpointtype=compute
```

If you need user admin role to execute that operation, you have to update the content to:

```
[root@testing-vm3-41 ~]# cat
/etc/opt/OV/ServiceActivator/config/NFVTemplates/CREATE_SERVER/CREATE_SERVER.properties
http.operation=POST
http.url.sufix=/servers
openstack.endpointtype=compute
openstack.url=public
```

By default that value does not exist and needs to be added when needed.

The openstack.url for each property file can have two values:

- public:
    - when the public endpoint wants to be used for a specific operation
    - and the value for the openstack.url is empty inside the Openstack.properties
- admin
    - when the admin endpoint wants to be used for a specific operation
    - and the value for the openstack.url is public inside the Openstack.properties

It is important to remember that some operations like the tenant or flavor activation cannot be done with the public endpoints.

Given an example of the four main cases:

- The OpenStack.properties has the openstack.url with no value, all the operations will use the admin endpoint.
- The OpenStack.properties has the openstack.url with public, all the operations will use the public endpoint.
- The OpenStack.properties has the openstack.url with no value and in the CREATE_SERVER.properties has the value public. The result will be that all the operations will used the admin endpoint except from the create server operation which will use the public endpoint.
- The OpenStack.properties has the openstack.url with public and in the CREATE_SERVER.properties has the value admin. The result will be that all the operations will used the public endpoint except from the create server operation which will use the admin endpoint.

1.6 Authentication properties

In the previous chapter Openstack.properties file has been cited. In this properties file there will be two parameters needed to do the authentication previous to every activation in Openstack. This parameters are *authenticationJsonV2* and *authenticationJson* and usually their values will be as shown below:

```
mwfwUser=admin
mwfwPassword=admin
authenticationJsonV2={ \"auth\":{\"passwordCredentials\":{\"username\":\"${USER}\", \"password\":\"${PASSWORD}\"
},\"tenantName\":\"${TENANT}\" } }
authenticationJson={ \"auth\": { \"identity\": { \"methods\": [ \"password\" ], \"password\": { \"user\": { \"domain\": { \"name\":
\"${DOMAIN}\" }, \"name\": \"${USER}\", \"password\": \"${PASSWORD}\"} }}}}
```

This values refer to the templates used to get the Token in version 2 and 3 respectively. Values between the '${}' will be replaced by NFVD.

Where

${TENANT} is the VIM tenant name,

${USER} is the user name having access to the above tenant,

${PASSWORD} is the password for the above user,

${DOMAIN} is the VIM domain name

1.7 VIM integration

Once the discovery process is completed, following situations could arise, and may require attention:

1. Handling situations where compute hostnames are duplicate. See Chapter 6 for details.
2. If VIM services are https enabled, it is mandatory to import the VIM certificate into SiteScope before VNF deployment. Else, it would result in monitor deployment failure. See Chapter 7 for details.
3. In case external networking needs to be integrated with NFV Director, it has to be done once discovery is complete. At present, Nuage Networks DCN is supported. See Chapter 8 for details.

Chapter 2 Discovery using GUI

2.1 Discovery APIs

2.1.1 Load Self-Management instances to Fulfillment.

NOTE:

- Auto installer will load this section with default values, In case of any modification required please refer the below section, otherwise ignore the section.
- GUI will invoke Discovery API to perform discovery operations, it's mandatory to load VNF_COMPONENT:OPEN_MEDIATION self-management instances in FF with the appropriate values as given in the below section "Load Self-Management instances to Fulfillment".
- FF-AA sync has to be configured.
- Discovery APIs are invoked through Assurance Gateway, AGW default REST endpoint port is 18080

Required Parameters in VNF_COMPONENT:OPEN_MEDIATION for Discovery API

NFV Director resource attribute	Required value	Remarks
VNF_COMPONENT:OPEN_MEDIATION.CONNECTION.HOST	Hostname	Host name of NOM installed machine (only hostname expected). IP address is not supported
VNF_COMPONENT:OPEN_MEDIATION.CONNECTION.PORT	https: 18999 (default) http: 18989	Discovery API endpoint port
VNF_COMPONENT:OPEN_MEDIATION.CONNECTION.NOMInstanceNumber	0(default)	Nom instance number, depends on which nom is configured. Instance number will be for e.g. 0, 1, 2 …
VNF_COMPONENT:OPEN_MEDIATION.CONNECTION.useSSL	true/false	True: https False: http
VNF_COMPONENT:OPEN_MEDIATION.GENERAL.IS_PRIMARY	true/false	To indicate Nom instance is primary or not, If its primary discovery will find the Datacenters which does not have the association with VNFC and consider the DC as default DC and discovers the same

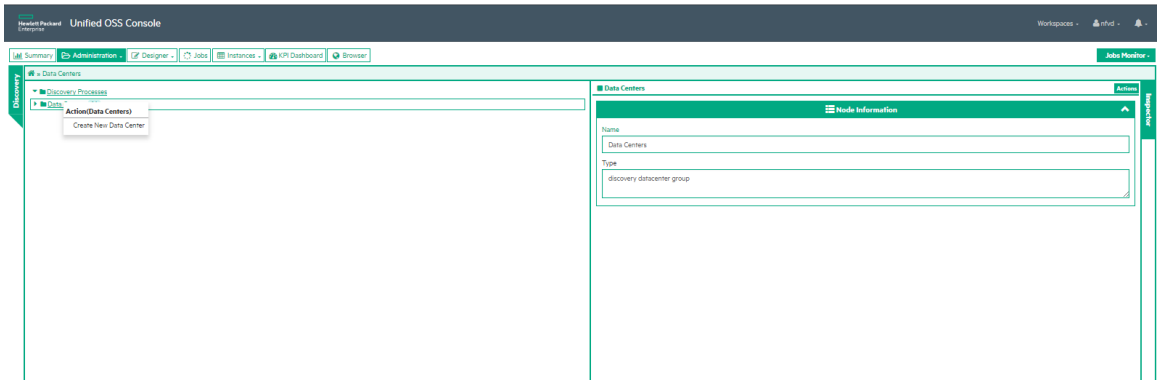
2.2 Steps to discover Datacenter using GUI

1. Create a new Datacenter in GUI

a. Login as domain user

b. Go to “Administration -> Discovery Management” tab.

c. Select and right click on “Data Centers” and click on Create new datacenter



d. Fill-in Datacenter Name

e. Datacenter Description

f. Select the appropriate Datacenter Template

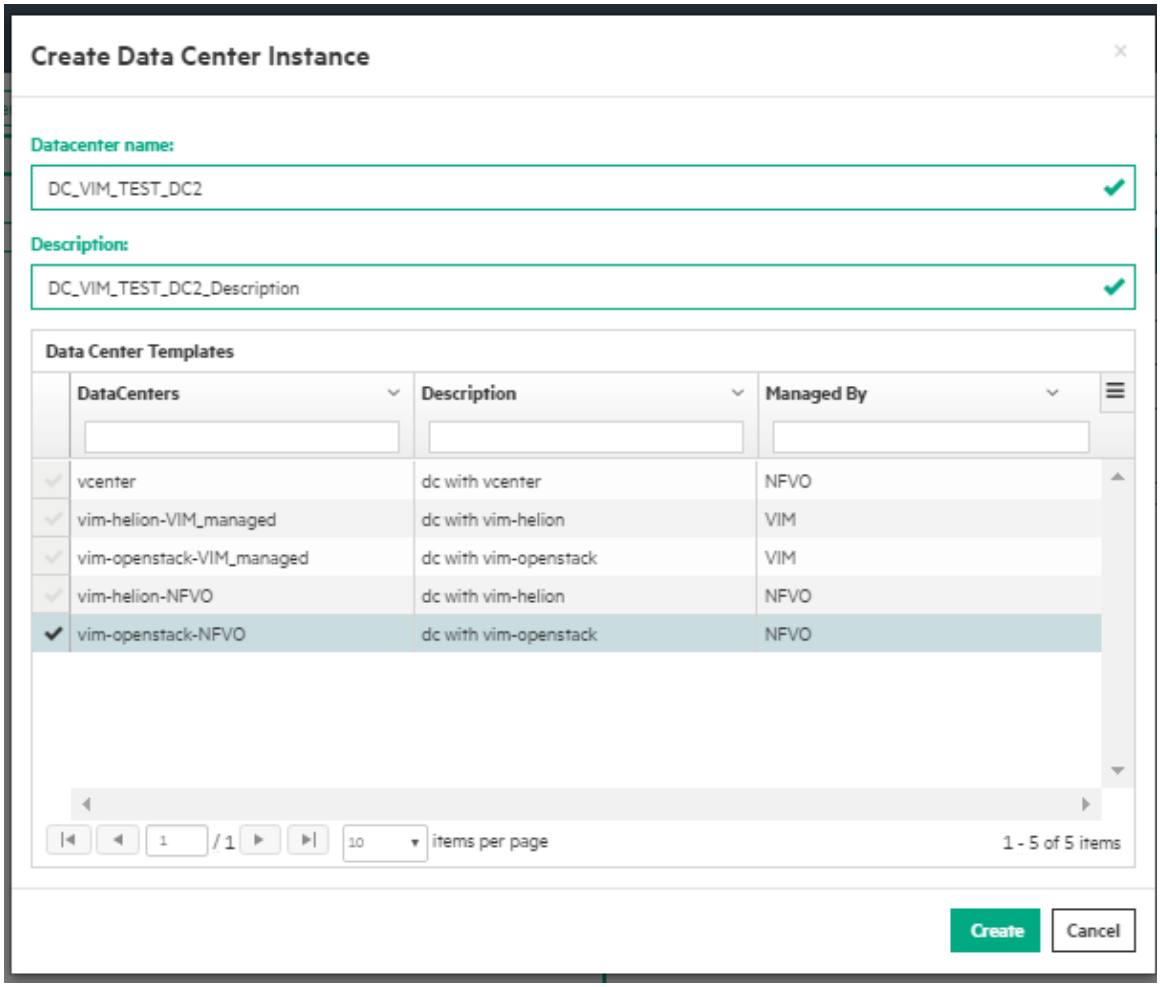
i. vim-helion-VIM_managed: HCG VIM in VIM MANAGED Mode(Bottom up approach)

ii. vim-openstack-VIM_managed: Openstack VIM in VIM Managed mode (Bottom up approach)

iii. vim-helion-NFVO: HCG VIM in NFVO mode (Top down approach)

iv. vim-openstack-NFVO: Openstack VIM in NFVO (Top down approach)

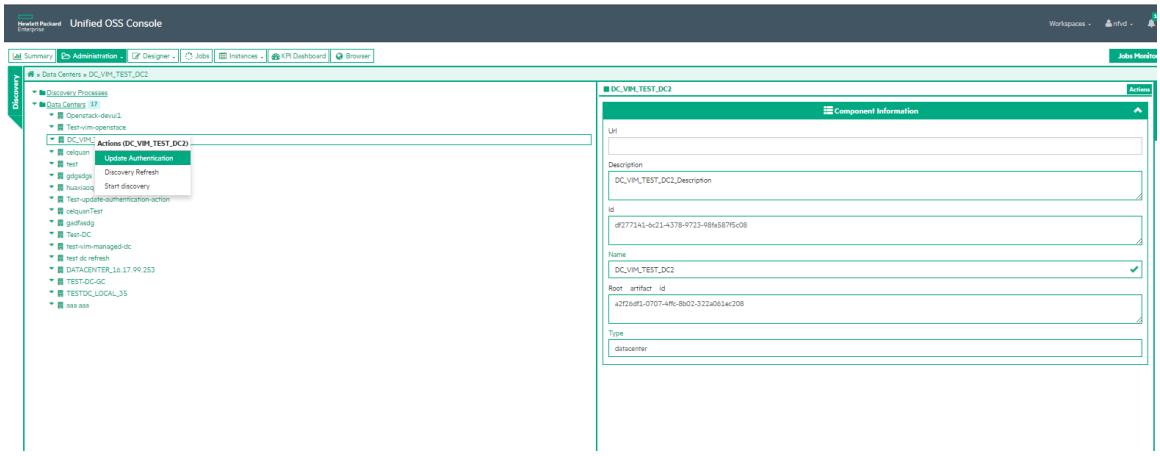
g. Click on create



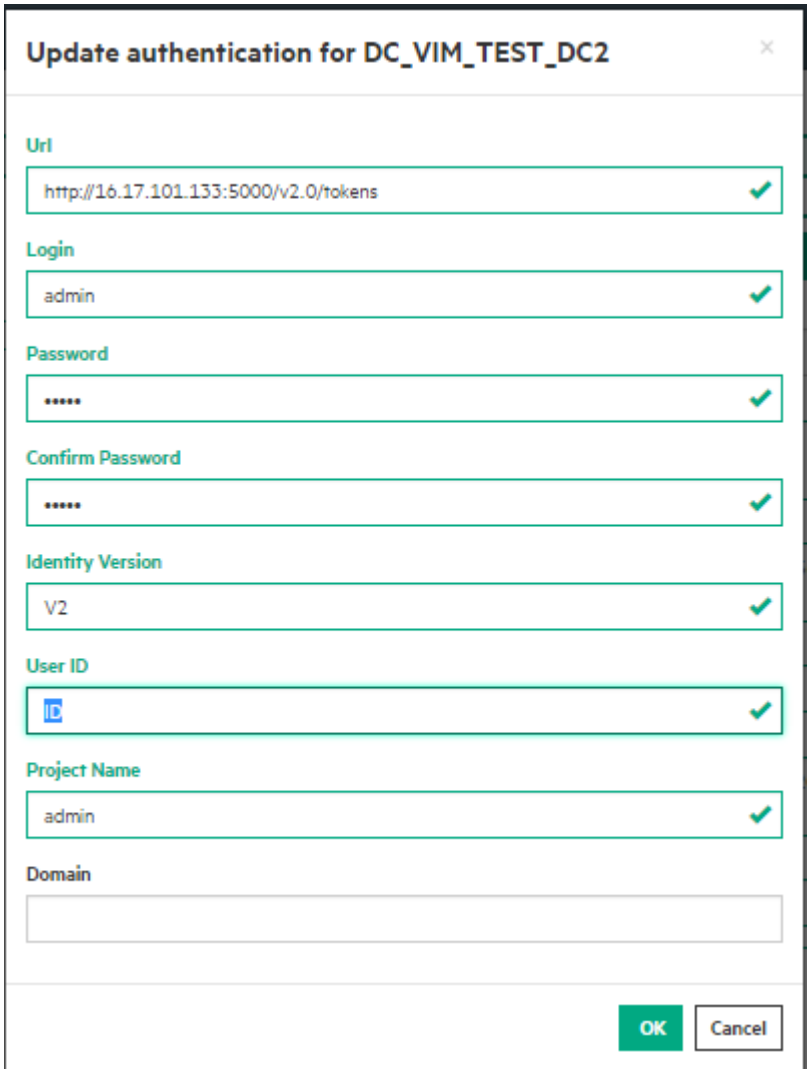
2. Change the authentication attributes for the datacenter

a. Double click the “Data Centers” node to load the new created data center instance.

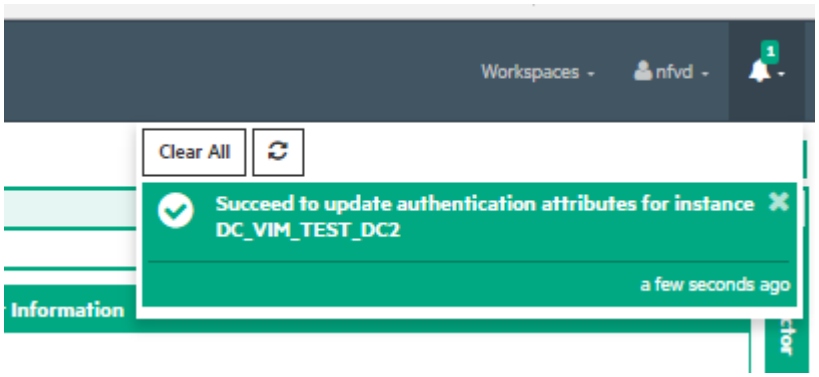
b. Select the new created data center instance node and right click on it to load the context menu.



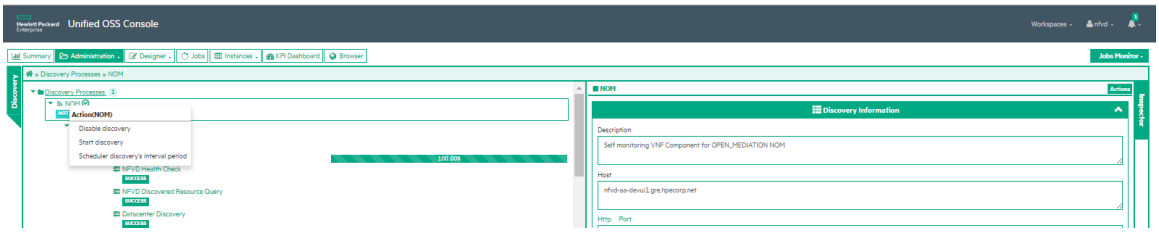
c. Click the “Update Authentication” menu item and filled the attributes.



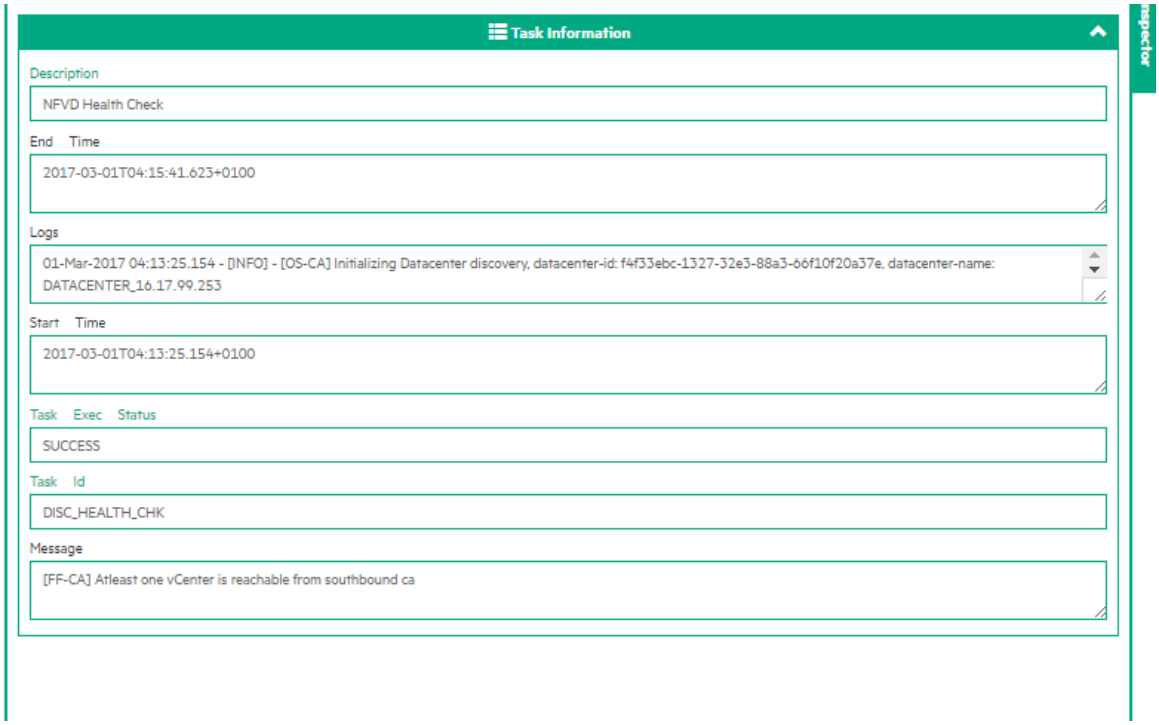
d. Click the “OK” button and the authentication attributes for the data center instance will be updated.



3. Perform Discovery actions for the newly created VIM artifact.
   Login as domain user
   b. Go to “Administration -> Discovery Management” tab.
   c. Click on Discovery Processes
   d. Discovery processes list the Nom instances attached.
   e. To trigger discovery on one nom instance, Right click on the nom instance and click “Start Discovery”

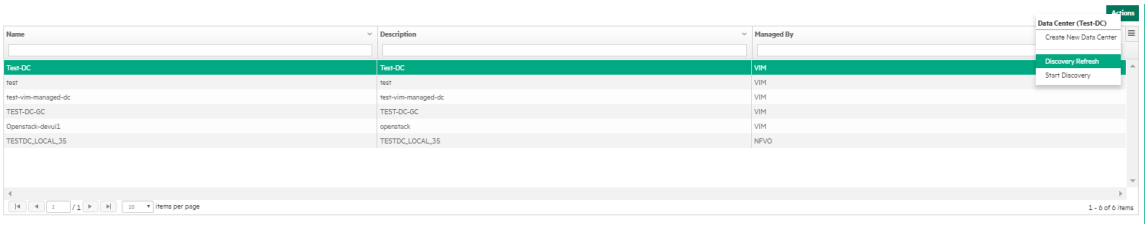


f. Track the tasks status by clicking on the Tasks menu.
i. Click on the specific task and refer to the task information on the right side pane.
i. Logs – will tell about steps executed in discovery and any ERROR occurred.
ii. Task Exec status: Status on the task.



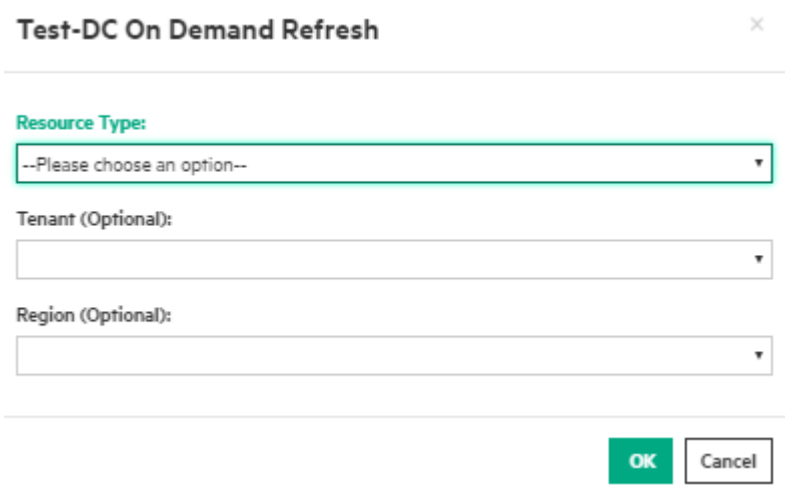
2.3 Discovery Refresh for a datacenter

Select a datacenter instance, and click the “Actions” button, it will show the “Discovery Refresh” menu item.



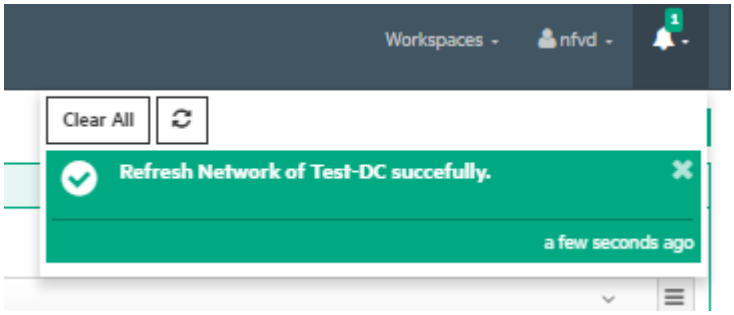
Tips: you can also right click the instance you selected to show the context action menu.

Click this menu item, a dialog will be opened.



Choose the resource type, tenant (optional) and region (optional), then click the “OK” button.

Then a discovery refresh operation for this datacenter instance will be triggered.



Chapter 3 Discovery using command line utility

Triggering the discovery involves two steps:

- Uploading DC, VIM and AUTHENTICATION artifacts and relationship instances to NFV Director
- Triggering discovery

3.1 Upload DC, VIM and AUTHENTICATION instances

On: <AA_HOST>

Login: root

DC, VIM and AUTHENTICATION details of the OpenStack must be populated into NFV Director. By doing this, NFV Director becomes aware of the OpenStack URL, credentials and tenant details.

Run the following script to populate the DC, VIM and AUTHENTICATION details

```
/opt/HPE/nfvd/discovery/scripts/nfvd_createVIM.sh
```

Usage: nfvd_createVIM.sh

```
Usage: ./nfvd_createVIM.sh [-host <host>] [-port <port>] [-vimname <vimname>] [-url <url>] [-username <username>] [-password <password>] [-tenantname <tenantname>] [-discovertenant <discovertenant>] [-vimcategory <vimcategory>] [-vimtype <vimtype>][-authversion <authversion>] [-nomartifactid <nomartifactid>] [-managedby <managedby>]
```

Example:

```
./nfvd_createVIM.sh -host 10.206.254.14 -port 8080 -vimname FC33 -url https://10.207.114.100:5000/v2.0/tokens -username admin -password 4b1ec8122bf0c5b1c19bac886e4b4f01c95d53318506c67dce5c29ef5a318ed81 -tenantname admin -vimcategory HELION -vimtype HCG -nomartifactid 1fb88d77-a1ad-4ce2-b39c-938756a5deaf -managedby NFVO
```

NOTE: Password provided to 'nfvd_createVIM.sh' has to be encrypted.
Password encryption can be done using the below script that is present on <FF_HOST>:
cd /opt/HPE/nfvd/fulfillment/scripts/
./ encryption.sh -o encrypt -p <password>

Where:

MANDATORY:

-host	Hostname or IPAddress of Fulfillment, <FF_HOST>.
-port	Fulfillment Port (eg: 8080)
-vimname	VIM Name eg. vim-helion
-url	VIM Authentication URL(Keystone V2/V3 URL) Note: In case of V2 keystone, you need to append /tokens at the end of keytone URL Ex: *https://<VIM IP>:5000/v2.0/tokens* In case V3, you need to append "/auth/tokens" Ex: *https://<VIM IP>:5000/v3/auth/tokens*
-username	VIM user with administrator privileges on the tenants to be discovered
-password	VIM password for the user
-tenantname	Tenant on which the user has administrative privileges
-vimcategory	VIM category , values are either OPENSTACK/HELION

OPTIONAL:

-discovertenant Comma separated list of specific tenants that needs to be discovered (default:blank), if not provided all tenants will be discovered

-vimtype General type of the VIM (default:OPENSTACK for vimcategory OPENSTACK, HCG for HELION)

-authversion VIM Authentication keystone version (default:V2)

-**nomartifactid** NOM Artifact Id (default:blank) if not provided, discovery will be triggered on a default nom

-**managedby** Managed by VIM or NFVO (default:NFVO)

NOTE: If there are multiple OpenStack instances to be discovered, their respective VIM and AUTHENTICATION instances must be uploaded.

3.2 Triggering discovery

Run the script trigger_reconciliation.sh on <AA_HOST> to trigger discovery of the VIM instances uploaded in the previous step.

For usage details of the script, refer to Manual Discovery trigger

NOTE: For various command line discovery utilities, refer to the “Discovery Utilities” chapter.

Chapter 4 NFV Director discovered resources

4.1 Discovered resources

Following resources are auto discovered from OpenStack or HCG

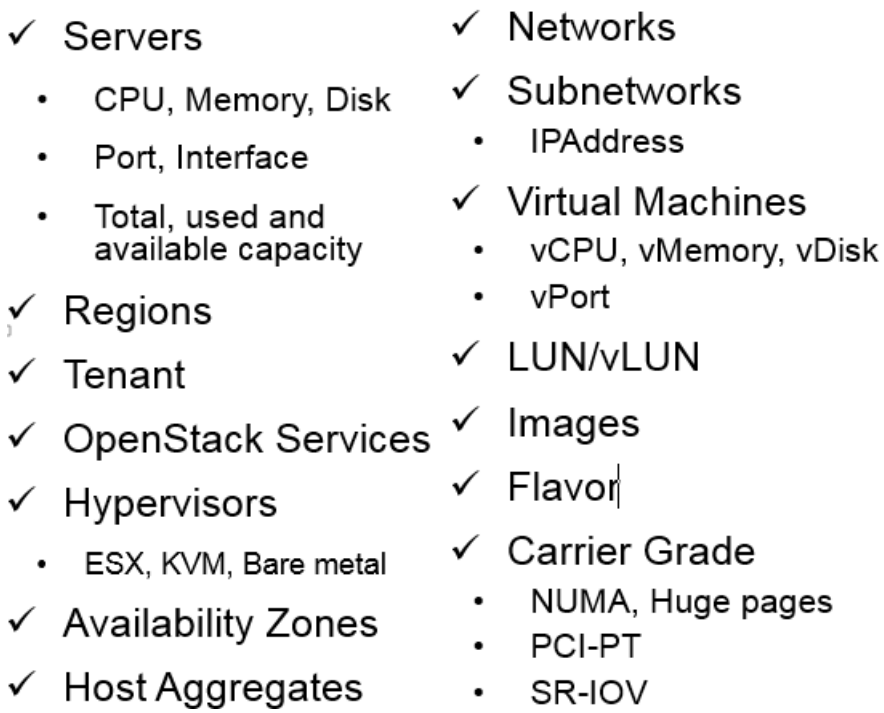


Figure 3: Discovered resources

For the discovery of resources from VIM, VIM and its AUTHENTICATION details must be already present in the NFV Director system.

Thus, VIM and AUTHENTICATION are manually provided as input.

4.2 Resources with default value

NOTE: This section is only applicable, when NFVD wants to deploy VNF on Storage.

Once discovery operation is complete, some resources are stored in NFVD with default value. Following are the resources and their default values:

NFV Director resource attribute	Default value	Remarks
Policy.OVER_SUBSCRIPTION.OVER_SUBSCRIPTION.Rate	1	
LUN.Info.Amount	0	In GB
Server.General.Class	Class_A	Class_A or Class_B
Server.General.usage_mode	shared	shared or dedicated
CPU.General.usage_mode	shared	shared or dedicated
Datacenter.General.Name	datacenter-<VIM Name>	
Rack.General.Name, Rack.General.Type, Rack.General.Descrption	Static data	
Enclosure.General.Name, Enclosure.General.Type, Enclosure.General.Description	Static data	

Card.General.Name, Card.General.Type, Card.General.Description	Static data	

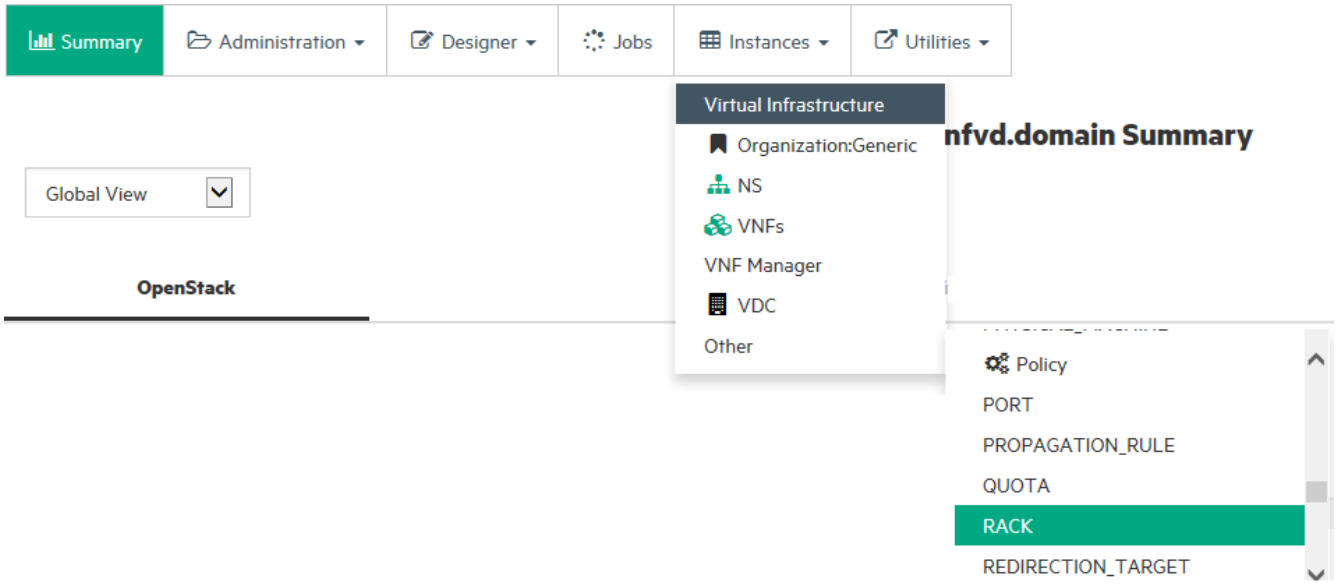
4.3 Updating the resources with default value

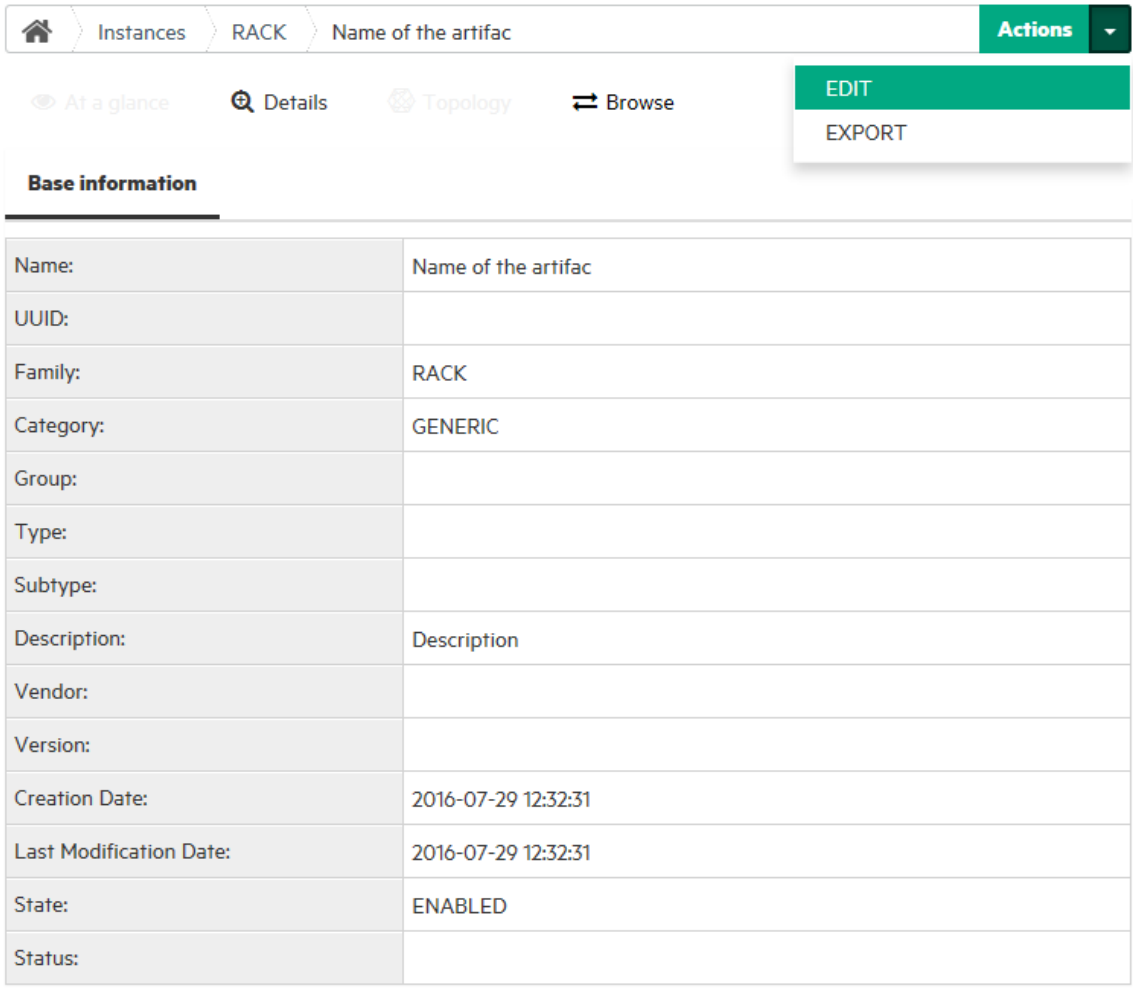
4.3.1 Updating non-significant resources

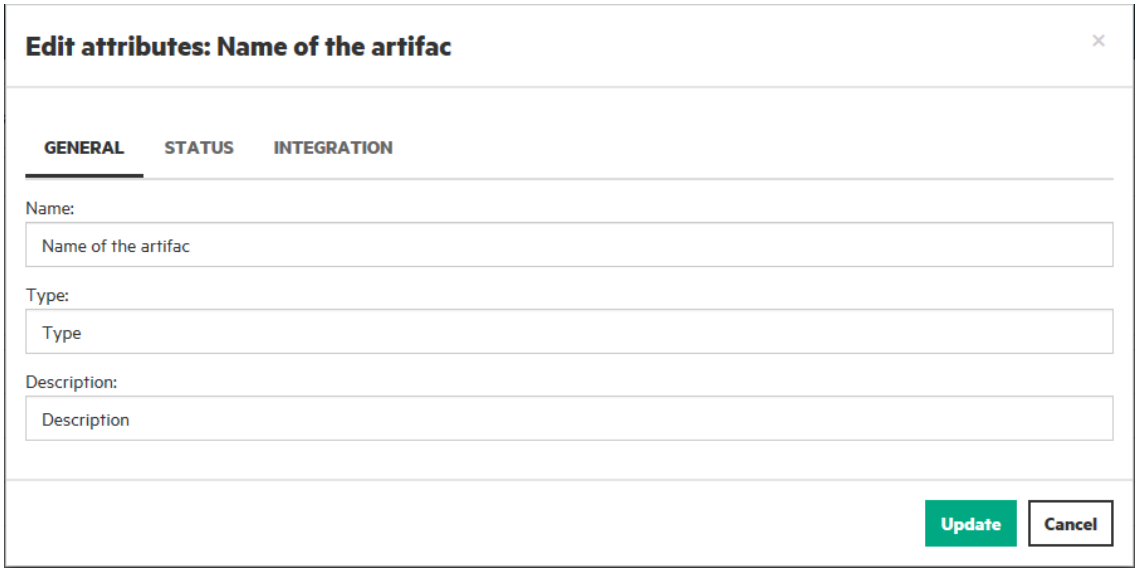
For the following NFV Director resources, updating the attributes will not have any impact on the behavior of the solution.

- Policy.OVER_SUBSCRIPTION.OVER_SUBSCRIPTION.Rate
- Datacenter.General.Name
- Rack.General.<Attribute>
- Enclosure.General.<Attribute>
- Card.General.<Attribute>

As an example, in order to update Rack.General.<Attribute>, in the NFV Director GUI, select Instances > Other > RACK, choose the appropriate Rack from the list, choose the Edit Action, edit the attribute, and click on Update button.







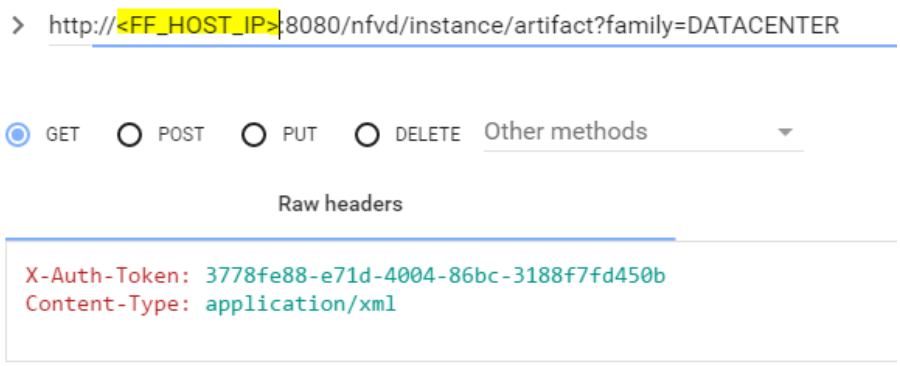
4.3.2 Updating resources that require DC quota recalculation

When the following NFV Director resource attributes are updated, datacenter quota must be recalculated.

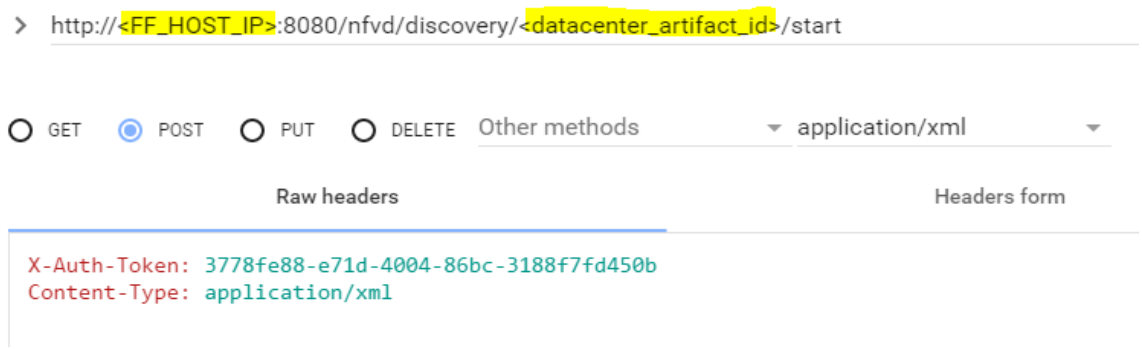
- LUN.Info.Amount
- Server.General.Class
- Server.General.usage_mode
- CPU.General.usage_mode

Follow the below steps:

1. Query the DATACENTER artifact ID from fulfillment server using REST client.

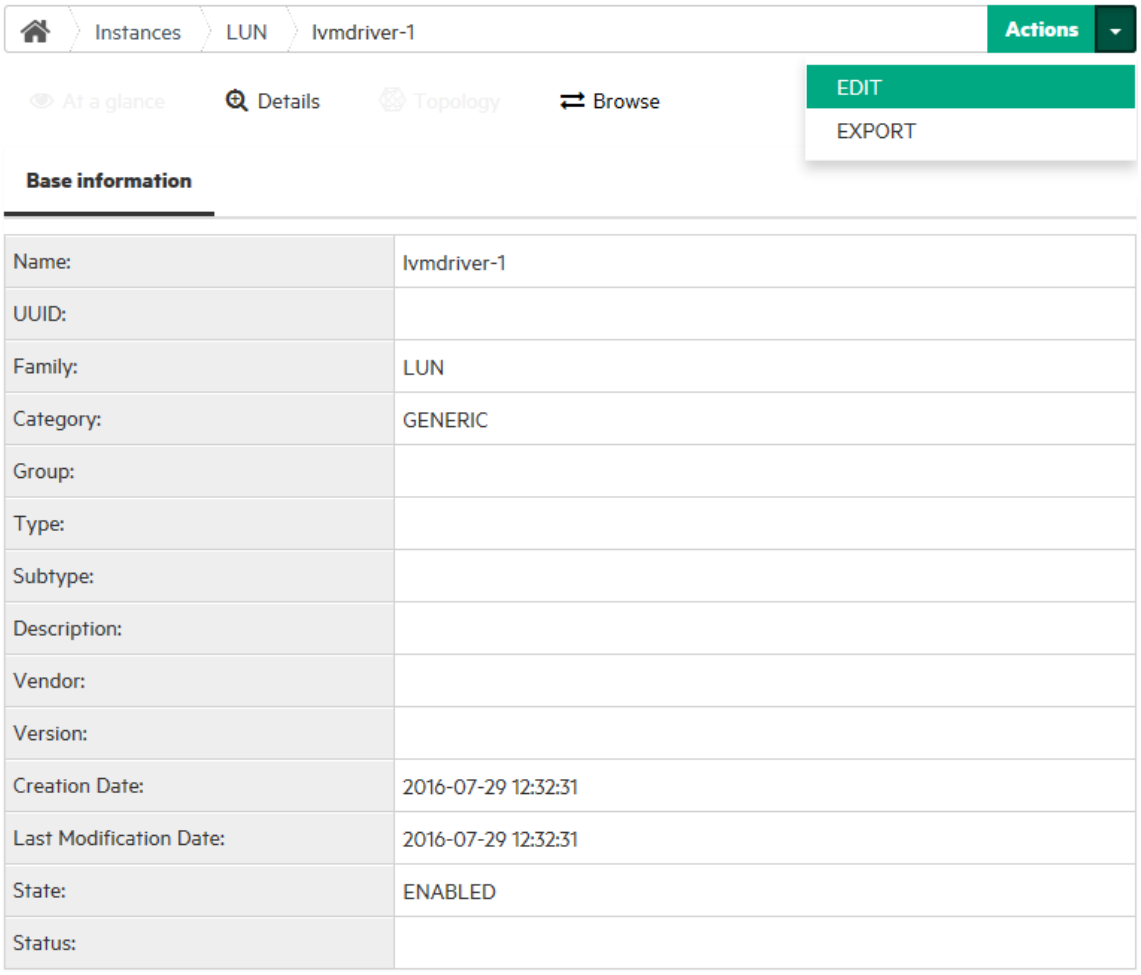


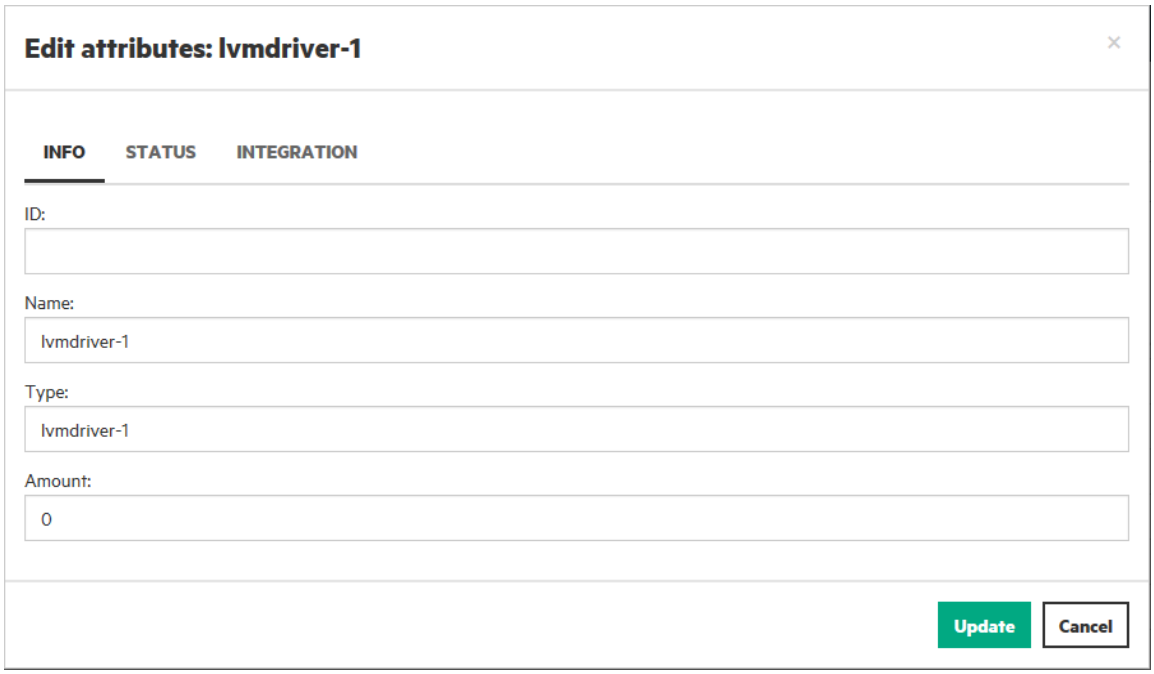
2. Pick the DATACENTER artifact ID from the response body, for which you want to modify the resource.
3. Perform a start of data load by executing the REST request "**/nfvd/discovery/<datacenter_artifact_id>/start**".



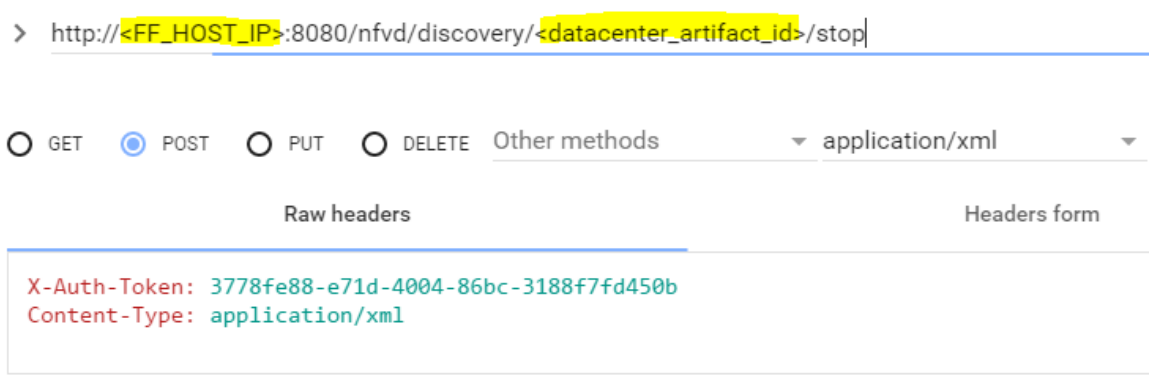
4. Edit the resources using GUI for which default values were populated by Discovery module. Browse to the respective resource from Instance Menu in GUI and select Edit option from Actions.

As an example, in order to update LUN.Info.Amount, in the NFV Director GUI, select Instances > Other > LUN, choose the appropriate LUN from the list, choose the Edit Action, edit the INFO.Amount value, and click on Update button.





5. To recalculate the data center quota, stop the data load by executing the REST request "**/nfvd/discovery/<datacenter_artifact_id>/stop**".



NOTE:
Quota calculation time will vary based on number of DATACENTER resources.

6. Login with an Organization or VDC level user in the GUI, and the changes should reflect in Quota management windows.
7. User can now modify the Organization or VDC level quota , as per the need.

Chapter 5 Discovery utilities

5.1 Enabling and Disabling of discovery process

On: <AA_HOST>

Login: root

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

5.1.1 Disable discovery even in fresh installation

Execute the below script when you install the fulfillment-ca, before deploying it. By default, the script works in https mode. In case http mode is required, use '-m http' option.

```
cd /opt/HPE/nfvd/discovery/scripts/

sh disable_discovery.sh -m http

Usage: disable_discovery.sh [OPTIONS...]
 -h <<Hostname or IPADDRESS of the machine where Discovery needs to be disabled>>
 -m <<https or http>>
```

5.1.2 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. By default, the script works in https mode. In case http mode is required, use '-m http' option.

```
cd /opt/HPE/nfvd/discovery/scripts/
sh disable_discovery.sh -m http

Usage: disable_discovery.sh [OPTIONS...]
 -h <<Hostname or IPADDRESS of the machine where Discovery needs to be disabled>>
 -m <<https or http>>
```

5.1.3 Enable Discovery

Execute the below script. By default, the script works in https mode. In case http mode is required, use '-m http' option.

```
cd /opt/HPE/nfvd/discovery/scripts/
sh enable_discovery.sh -m http

Usage: enable_discovery.sh [OPTIONS...]
 -h <<Hostname or IPADDRESS of the machine where Discovery needs to be enabled>>
 -m <<https or http>>
```

5.1.4 Manual Discovery trigger

NOTE: Discovery logs will be available in Open Mediation Service Mix log.
Default location: /var/opt/openmediation-70/containers/instance-0/data/log

Manual discovery can be triggered any time. It will not get triggered when another instance of Discovery is already running. Run the following script to trigger manual discovery. By default, the script works in https mode. In case http mode is required, use '-m http' option.

```
cd /opt/HPE/nfvd/discovery/scripts/
./trigger_reconciliation.sh -m http

Usage: trigger_reconciliation.sh [OPTIONS...]
 -h <<Hostname or IPADDRESS of the machine where Reconciliation needs to be triggered>>
 -m <<https or http>>
```

5.1.5 Making changes in Channel Adapter properties

Two Channel Adapters are involved in the Helion CG and OpenStack discovery – fulfillment-ca-10 and openstack-ca-10.

Following are the steps, if you want to make changes in channel adapter properties:

1. disable discovery
2. un-deploy the Channel Adapters
3. make changes to properties
4. deploy Channel Adapters
5. enable discovery

NOTE:
See 5.1.2 for instructions to disable discovery
See 5.1.3 for instructions to enable discovery

Channel Adapter properties can be edited to update the Fulfillment endpoint details, if required.

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

Below are the steps to Undeploy and deploy Channel Adapters

```
/opt/open-mediation-70/bin/nom_admin --undeploy-ip-in-container 0 openstack-ca-10

/opt/open-mediation-70/bin/nom_admin --undeploy-ip-in-container 0 fulfillment-ca-10
```

```
/opt/open-mediation-70/bin/nom_admin --deploy-ip-in-container 0 openstack-ca-10

/opt/open-mediation-70/bin/nom_admin --deploy-ip-in-container 0 fulfillment-ca-10
```

5.1.6 Track Initial/Incremental Discovery completion

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

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

****** [FF-CA] Initial/Incremental Discovery Service has been completed successfully, Quota Calculation is in Progress ******
```

5.2 Enabling and disabling discovery of Virtual Machines

On: <AA_HOST>

Login: root

By default discovery of virtual machines is disabled, when NFV Director Discovery components are installed.

5.2.1 Disable discovery of virtual machines

Execute the below steps.

5.2.1.1 Modify “discover.virtual_topology.enabled” property value to false

```
cd /var/opt/openmediation-70/containers/instance-0/ips/openstack-ca-10/etc/

vi nfvd-grm-users.properties

##Enable/Disable discovery of virtual topology
discover.virtual_topology.enabled=false
```

5.2.1.2 Undeploy and redeploy openstack channel adapter

```
/opt/open-mediation-70/bin/nom_admin --undeploy-ip-in-container 0 openstack-ca-10

/opt/open-mediation-70/bin/nom_admin --deploy-ip-in-container 0 openstack-ca-10
```

NOTE: If disable task has been performed after initial discovery run, already discovered Virtual machines will neither be reconciled nor deleted from NFVD database.

5.2.2 Enable discovery of virtual machines

Execute the below steps.

5.2.2.1 Modify “discover.virtual_topology.enabled” property value to true

```
cd /var/opt/openmediation-70/containers/instance-0/ips/openstack-ca-10/etc/

vi nfvd-grm-users.properties

##Enable/Disable discovery of virtual topology
discover.virtual_topology.enabled=true
```

5.2.2.2 Undeploy and redeploy openstack channel adapter

```
/opt/open-mediation-70/bin/nom_admin --undeploy-ip-in-container 0 openstack-ca-10

/opt/open-mediation-70/bin/nom_admin --deploy-ip-in-container 0 openstack-ca-10
```

Chapter 6 Multi VIM duplicate compute hostname scenario

This section addresses the scenario to resolve the discovered topology, where in two VIM's have same compute node names across them.

6.1 Run amend duplicate compute hostnames tool

On: <AA_HOST>

Login: root

The script has to be used only in case the setup matches the below scenario:

1) VIM-1 has been discovered using previous kits and few VNF deployments have been made.
2) New VIM-2 has been added and discovered and one of its compute nodes has the same name as of VIM-1 compute node.

Once the kits have been installed disable discovery by referring to Note below.

Run the following script to amend the topology. By default the script runs in https mode. In case http mode is required, use '-m http' option.

```
cd /opt/HPE/nfvd/discovery/scripts/
./amend_duplicate_compute_topology.sh -m http

Usage: amend_duplicate_compute_topology.sh [OPTIONS...]
 -h <<Hostname or IPADDRESS of the machine where Discovery needs to be enabled>>
 -m <<https or http>>
```

NOTE: Discovery has to be disabled manually using the script as soon as the discovery kits have been installed. Refer to section **Disable discovery temporarily**

6.1.1 Track amend topology script completion

Open Mediation log file will have below messages:

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

[AMEND-DISCOVERY] || Processing amend discovered topology trigger ||

[AMEND-DISCOVERY] || Successfully completed amend topology for duplicate compute nodes ||
```

6.1.2 Enable Discovery

Refer to section 5.1.3 Enable Discovery to enable discovery again.

6.1.3 Rerun Discovery

Refer to section 5.1.4 Manual Discovery trigger for triggering discovery again.

Once discovery has been completed the Topology will have the proper data.

Chapter 7 VIM Certificates

When monitoring a remote server, if the target server uses a self-signed certificate, the certificate must be added to a trusted keystore.

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

When the VIM services are https enabled, the 'Access and Security' > API Access details on the VIM would show all Service endpoints in https mode.

IMPORTANT: To view the **Certificate Management** page, you must be an administrator in SiteScope or a user granted with View certificates list permissions.
Make sure the certificate exported from the target system has a valid CN and SAN. Any issues, for example, improperly configured SAN pointing to a domain and in the SiteScope template if the target host is given as IP address, then monitoring will not happen due to SSL issue as SiteScope adheres to strict SSL and validates the target host.

7.1 Importing VIM certificate to SiteScope

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

1. Go to SiteScope Preferences > Certificate Management
2. Click on "Import Certificates" option.
3. Provide the Host IP where Keystone service is installed and the Port. e.g. for OpenStack, the Keystone port is 5000.
   In case of OpenStack, check keystone URL in "Access and Security" → "API Access" via horizon dashboard
4. Click on the 'Load' button to load the certificate.
5. Now select the loaded certificate and click on 'Import'.

Note: Make sure that VIM certificates valid, i.e. they generated for correct VIM IP addresses

7.2 Importing Ceilometer certificate to SiteScope

1. Go to SiteScope Preferences > Certificate Management
2. Click on "Import Certificates" option.
3. Provide the Host IP where Ceilometer component is installed, and the Port. E.g. for OpenStack, the Ceilometer port is 8777.
   In case of OpenStack, check ceilometer URL in "Access and Security" → "API Access" via horizon dashboard

4. Click on the ‘Load’ button to load the certificate.
5. Now select the loaded certificate and click on ‘Import’.

Note: Make sure that VIM certificates valid, i.e. they generated for correct VIM IP addresses

Chapter 8 DCN Integration

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.

8.1 Prerequisites

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

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

8.2 Integrate DCN with NFV Director

8.2.1 Create the SDN Topology manually

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

In the DCN_Topology.xml, edit the following attributes:

- 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 figure depicts the pictorial representation of DCN topology

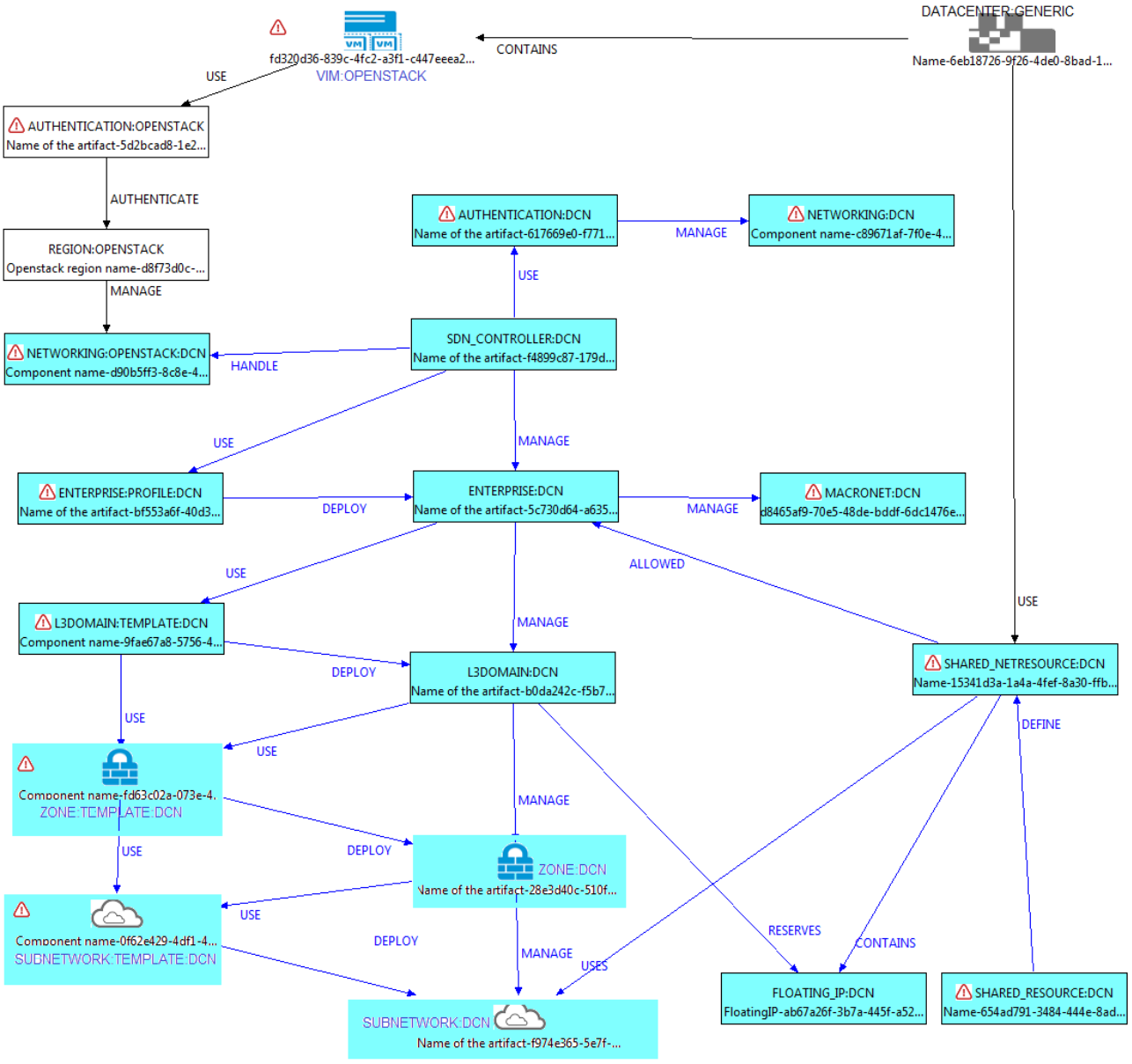


Figure 4: DCN topology pictorial representation

8.2.2 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.

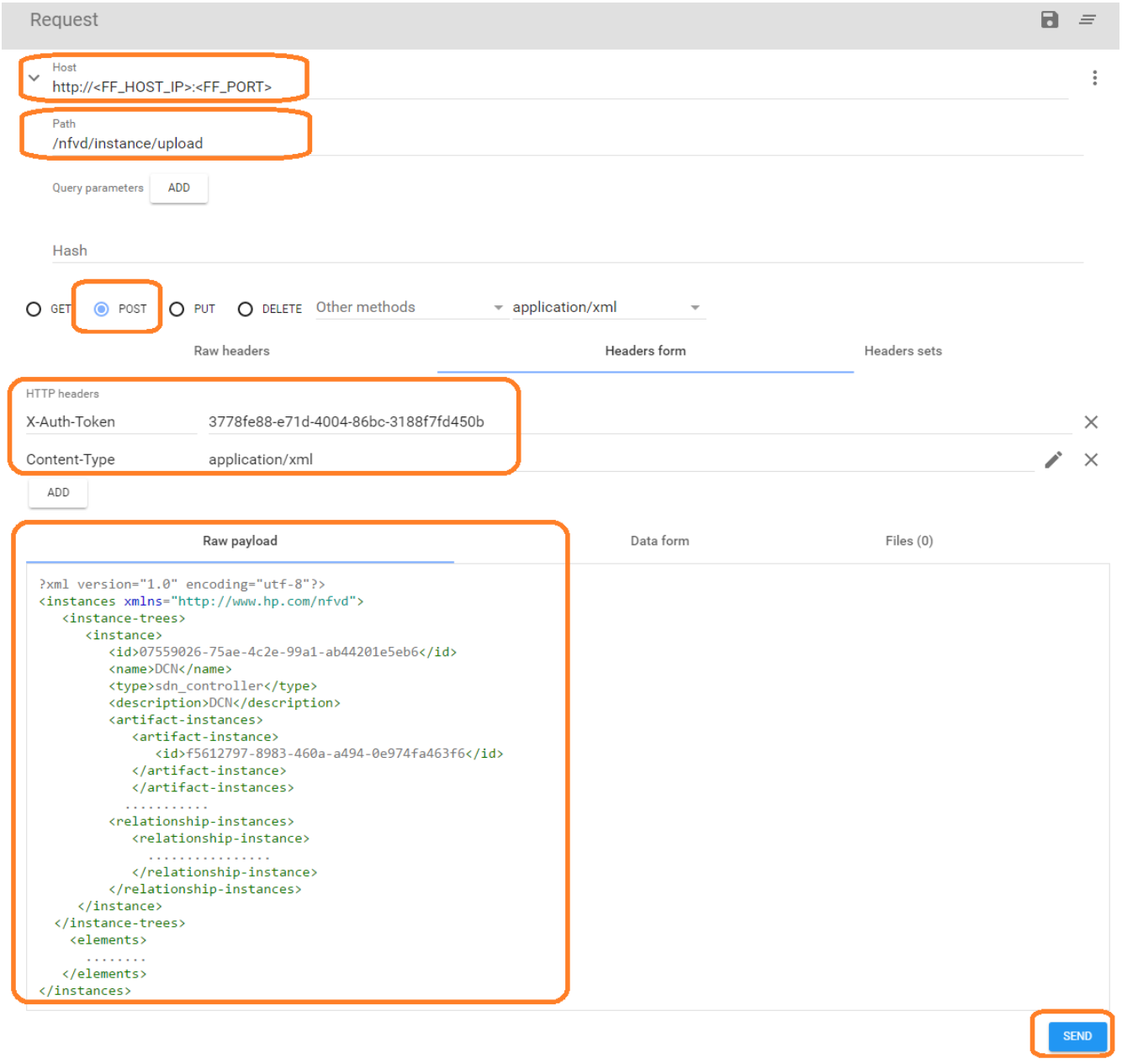


Figure 5: Uploading DCN topology into fulfillment

8.2.3 Connect Datacenter with DCN resources

CAUTION: Execute it per DC.

1 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)

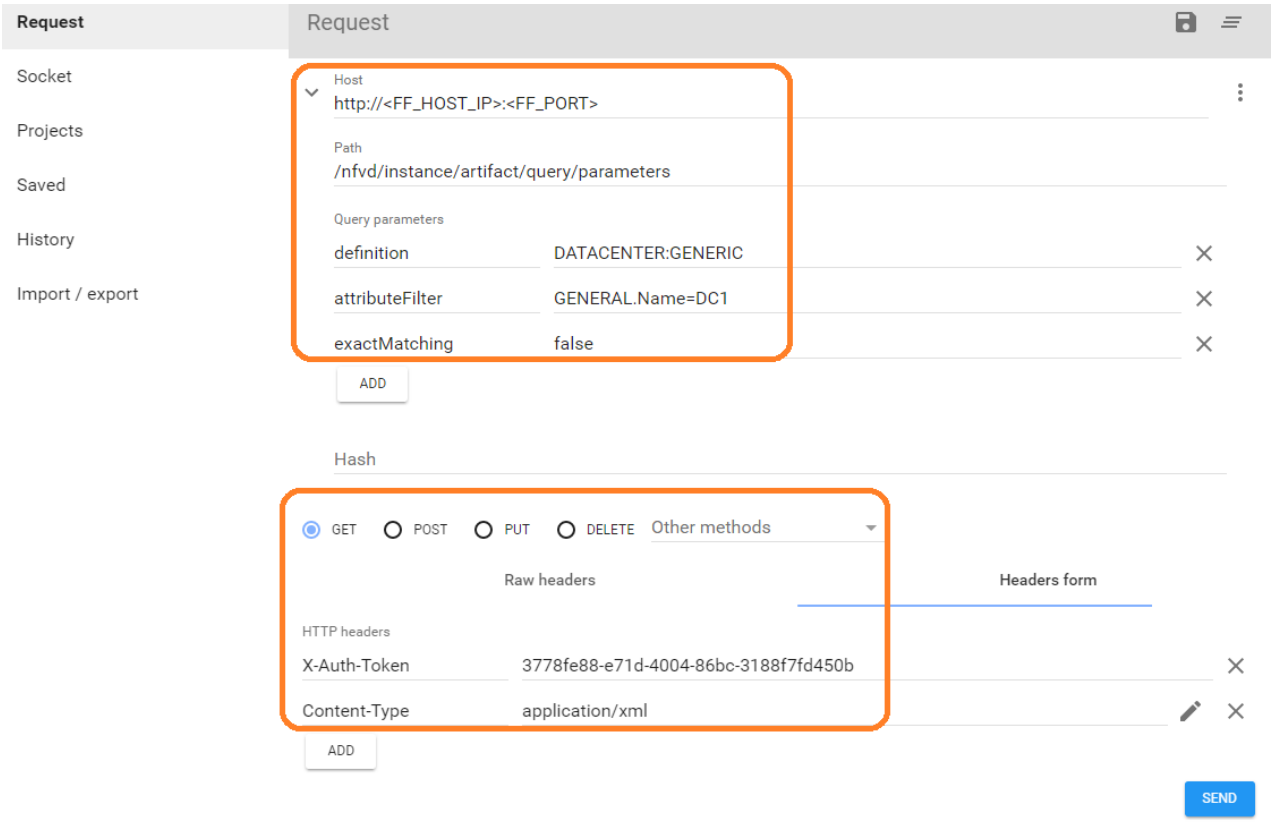


Figure 6: Query ID of Datacenter

Figure 7: 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

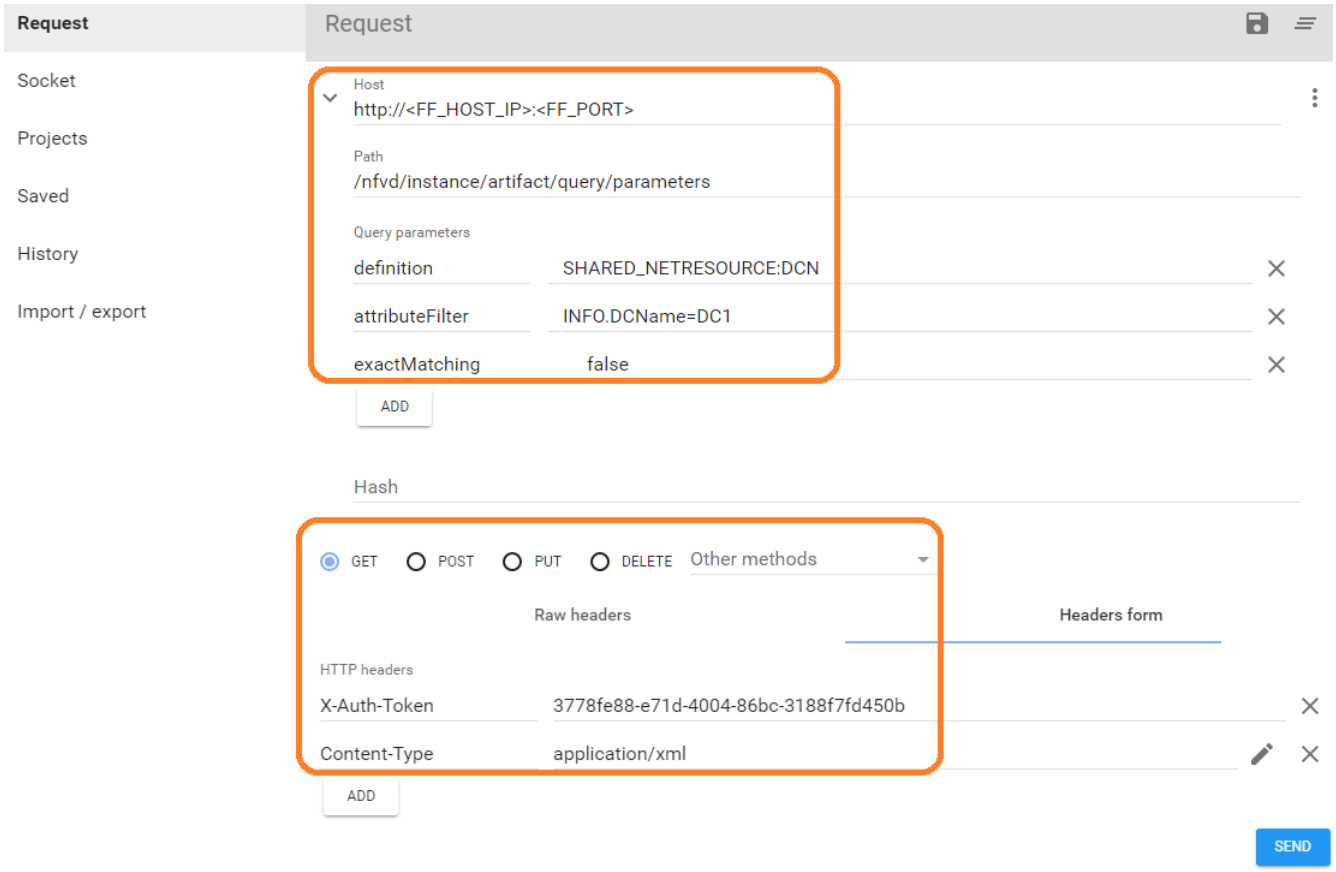


Figure 8: Query ID of SHARED_NETRESOURCE:DCN

Figure 9: 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.

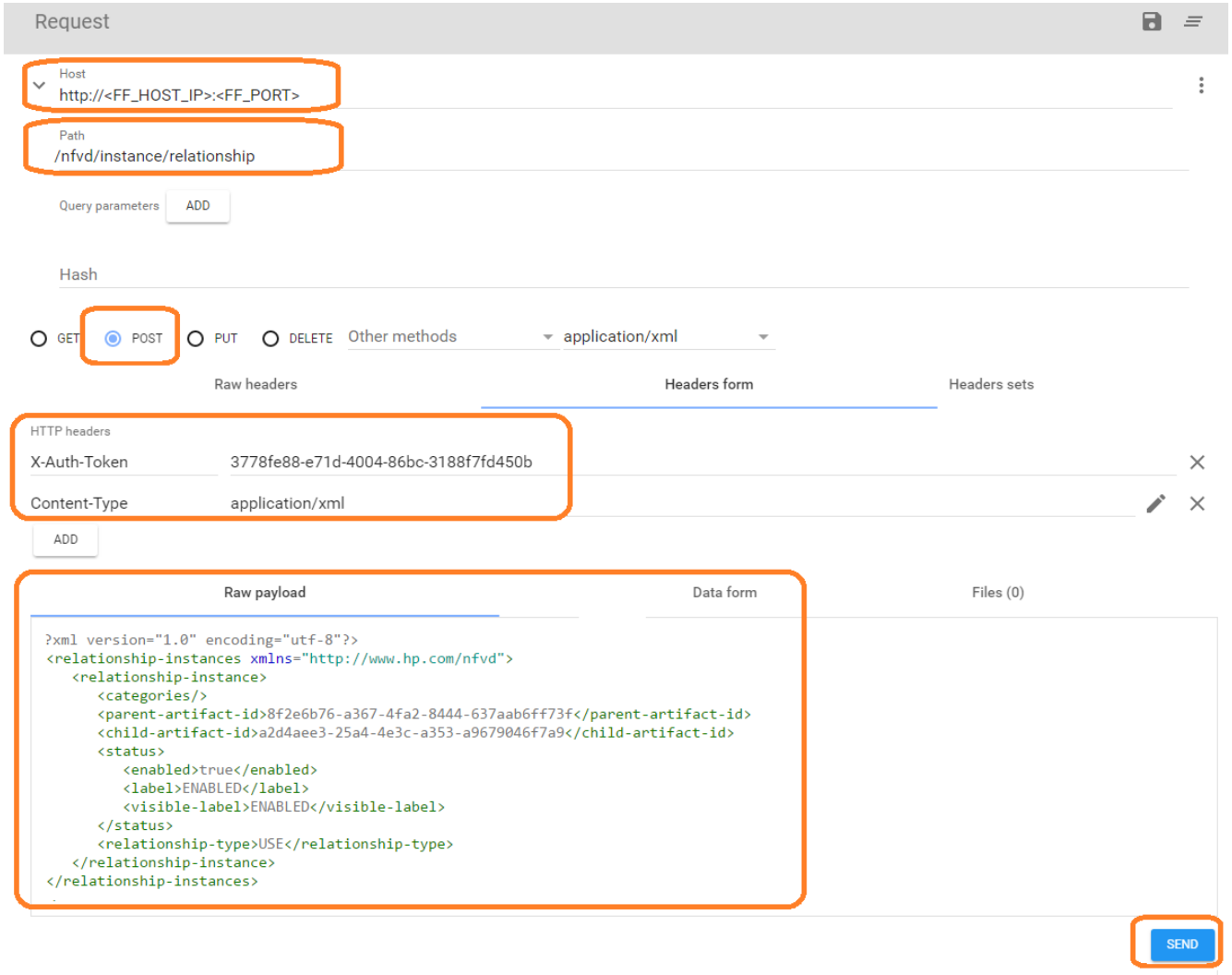


Figure 10: Create Relationship

8.2.4 Replacement of Networking Artifacts

8.2.4.1 Replace NETWORKING:OPENSTACK Artifacts with NETWORKING:OPENSTACK:DCN

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

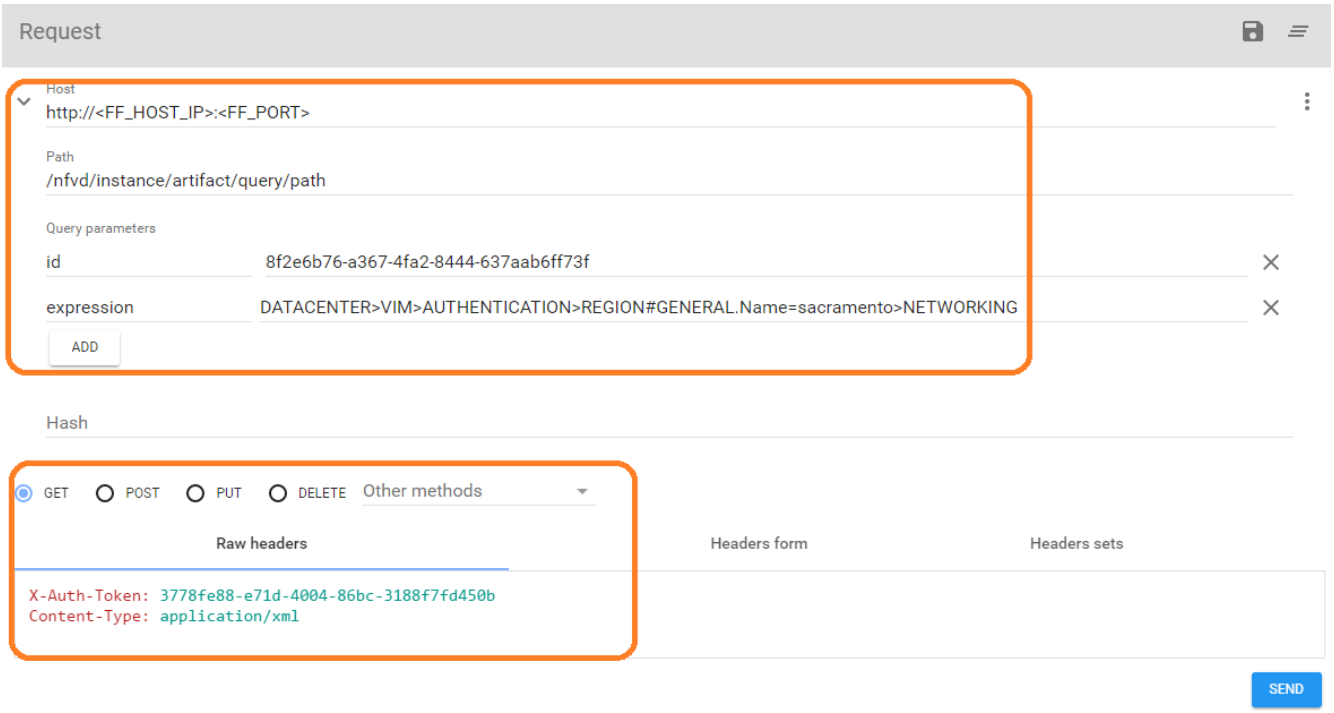


Figure 11: Query NETWORKING:OPENSTACK associated with Region

Below is the response received.

Figure 12: Query Response for NETWORKING:OPENSTACK associated with Region

1. Replace NETWORKING:OPENSTACK with NETWORKING:OPENSTACK:DCN for each Region
   a. Copy the Response received and paste it in Payload section of REST Client.
   b. Provide FF_HOST_IP, FF_PORT in the REST URL. Provide the Headers and Path as shown below.
   c. Change the artifact group to DCN as shown in below sample.
   d. Perform PUT HTTP operation.

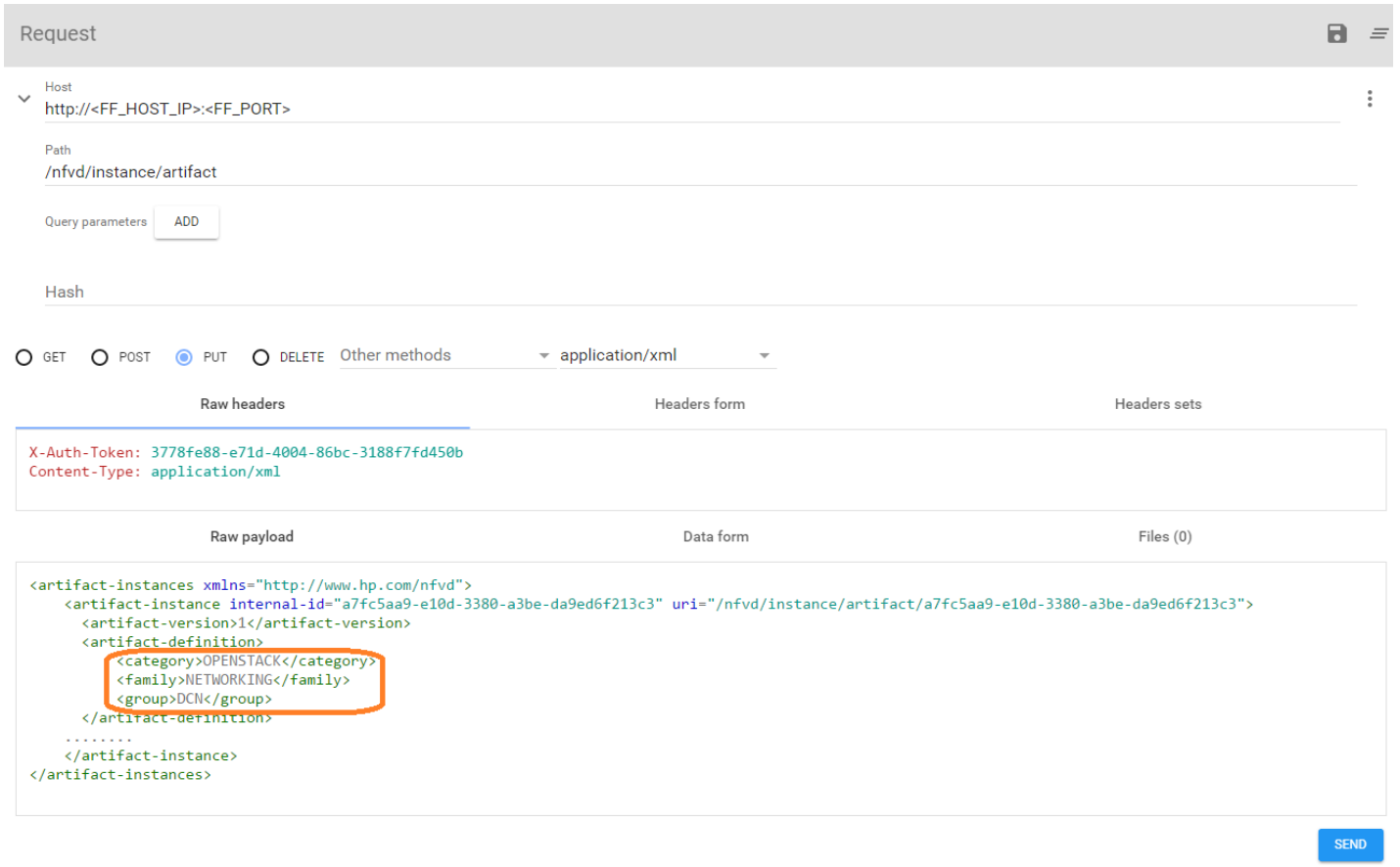


Figure 13: REST operation to update NETWORKING:OPENSTACK

8.2.5 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:

   a. 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

   b. child-artifact-id: NETWROKING:OPENSTACK:DCN Id's returned from "Query NETWORKING:OPENSTACK associated with each Region of the Datacenter" step for each region.

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.

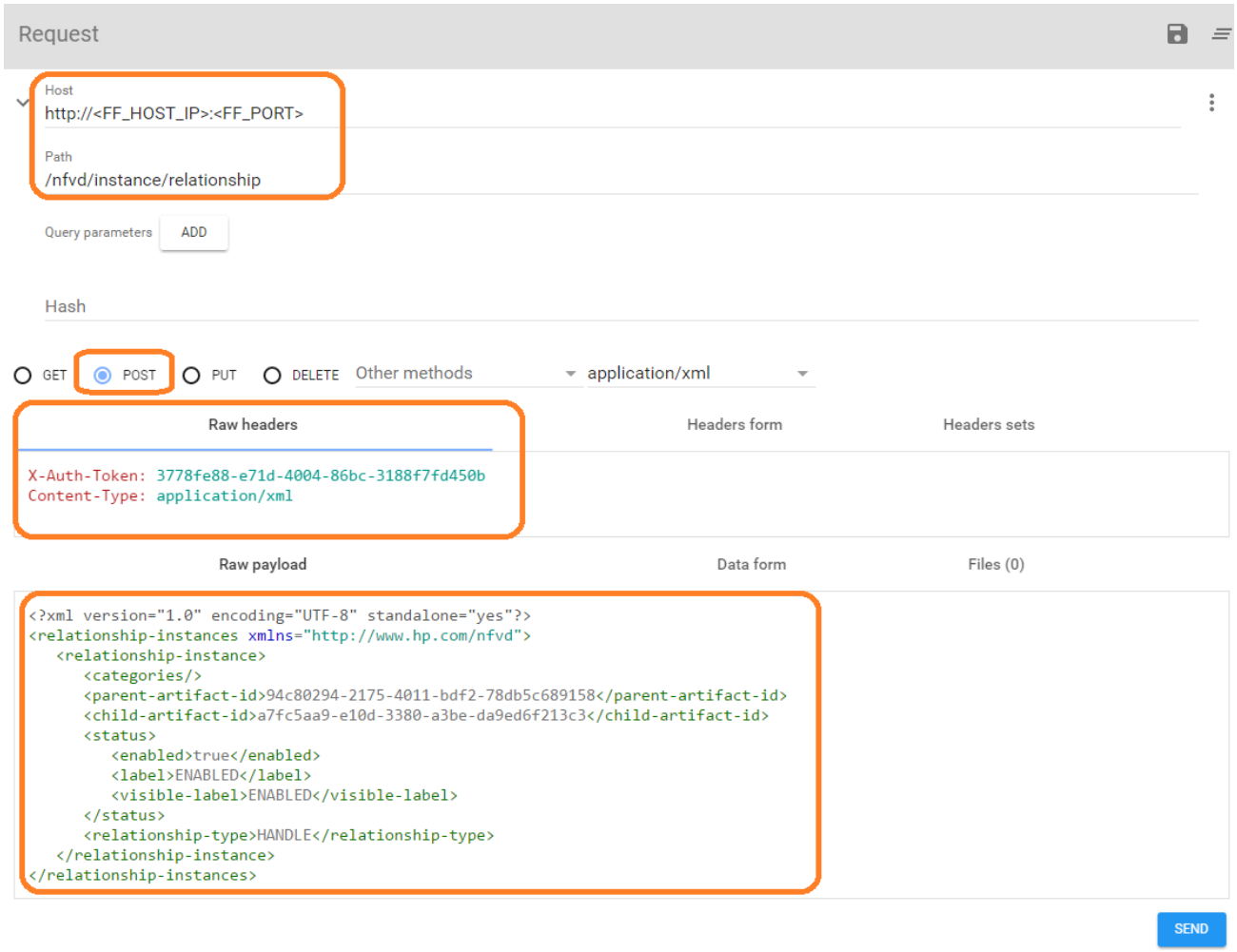


Figure 14: REST operation to create relationship between NETWORKING and DCN