OSC Partnership VNF Compatibility Test Plan

# Revision History

| ***Revision*** | ***Release Date*** | ***Description of Change*** | ***Author*** |
| --- | --- | --- | --- |
| 1.0 |  | Initial test plan | Albert Lin |
|  |  |  |  |

# Reviewers

|  |  |  |
| --- | --- | --- |
| **Department** | **Name and Title** | **Acceptance Date** |
| ***Engineering Development*** |  |  |
| ***Eng. Integration Test*** |  |  |
| ***Quality Assurance*** |  |  |
| ***Marketing*** |  |  |
| ***Technical Support*** |  |  |
| ***Operations*** |  |  |

Table of Contents

[1 Purpose 3](#_Toc456880498)

[2 Features/Functionalities to Be Tested 4](#_Toc456880499)

[2.1 Openstack Environment 4](#_Toc456880500)

[2.2 VMware NSX Environment 4](#_Toc456880501)

[3 Requirements and Test-Bed 5](#_Toc456880502)

[3.1 Hardware Requirements 5](#_Toc456880503)

[3.2 Software Requirements 5](#_Toc456880504)

[3.3 Test Topology 5](#_Toc456880505)

[4 Test Cases Identification 6](#_Toc456880506)

[4.1 VNF Openstack Test Cases 6](#_Toc456880507)

[4.2 VNF VMware vCenter NSX Test Cases 8](#_Toc456880508)

# Purpose

Open Security Controller (OSC version 2.5) partners with other vendor Cloud Security Virtualized Network Function (VNF) products. NFV (Network Function Virtualization) Infrastructure (NFVI) between vendors’ products needs to be tested. We tested two environments, Openstack (here tested with Redhat 7.1 Kilo) and VMware NSX (6.2) with vCenter (5.5). Other versions will be tested e.g. Openstack Liberty, vCenter 6.0 and so on.

# Features/Functionalities to Be Tested

This document describes the QA Test Plan for testing VNF. **Details in the test cases section**.

## Openstack Environment

We are using Redhat 7.1 OS, Openstack – Kilo.

Test setup includes at least 3 nodes:

* One controller node and one compute node, and one network node

## VMware NSX Environment

The VMware environment should be at minimum vSphere 5.5 with NSX 6.1.4 or higher vSphere and NSX versions

# Requirements and Test-Bed

## Hardware Requirements

Whatever required in order to install the Software Requirements.

## Software Requirements

Minimum for VMware: ESXi 5.5 or higher, vCenter 5.5 or higher NSX version 6.1 or higher.

Minimum for Openstack: Kilo or newer.

Also need to use OSC, SECURITY VNF and VNF Manager.

## Test Topology

End to end applications and data traffic redirects to Security VNF through SDN.

Have Openstack environment or VMware environment.

For Openstack the Network topology should have: Inspection Net, Mgmt Net, Public Net and their subnets.

For Openstack environment you suppose to have one controller one compute node and one network node.

Also SDN Controller installed for traffic redirection.

VNF manager is installed.

Also have Victim, and Attacker VMs for end to end test.

Having a VNF image which can be imported to OSC.

# Test Cases Identification

All these test cases should pass, OSC has Status Jobs passed, for the Security VNF to work with OSC.

Some tests may be more OSC related than VNF, but they are relevant for the workflow to test 3rd party VNF product Compatibility with OSC.

## VNF Openstack Test Cases

#### From OSC Manage => Plugins => Manager Plugins uploads VNF Manager plugin and see it’s in the UI.

#### From OSC Manage => Plugins => Manager Plugins, verify you can delete the plugin in UI.

#### From OSC Setup => Virtualization Connectors Add a VC, type OPENSTACK, verify that VC was added to OSC UI with accurate parameters.

#### From OSC Setup => Manager Connectors Add a Security VNF Manager with host IP login credentials & Job Status passed.

#### From OSC Setup => Manager Connectors Edit a Security VNF Manager with host IP login credentials & Job Status passed.

#### From OSC Setup => Manager Connectors Sync a Security VNF Manager with host IP login credentials & Job Status passed. After a sync new information from VNF Manager should be passed to the appliances and new information about VNFs should be passed to the VNF Manager.

#### From OSC Setup => Manager Connectors Delete a Security VNF Manager with host IP login credentials & Job Status passed.

* If not in use the manager connector will be deleted
* If there are VNF instances or there are distributed appliances the delete will fail, need to delete other connection first

#### From OSC Setup => Service Function Catalog Auto Import a Security VNF Model/Image, show up in OSC Service Function Catalog pane as passed.

#### From OSC Setup => Distributed Appliance Add a SECURITY VNF image DA, show up in OSC DA pane with Last Job Status passed.

#### From OSC Setup => Distributed Appliance Edit a SECURITY VNF image DA, see update in OSC DA pane with Last Job Status passed.

#### From OSC Setup => Distributed Appliance Sync a SECURITY VNF image DA, see update in OSC DA pane with Last Job Status passed.

For last three test cases – at the end of having DA of security VNF – you might (depend on manger implementation) need to have in the manager to show this Virtual Security System (VSS, e.g. IPS’ VNF Manager)

#### From OSC Setup => Distributed Appliance Delete a SECURITY VNF image DA, see DA deleted in OSC DA pane as passed.

* If not DAI in use – delete pass
* If DAI but not used for inspection – delete pass
* If DAI used for inspection – delete fail

#### From OSC Setup => Add (In Deployments Spec) the DA to the Openstack Compute, Openstack Project Instances see this DAI (DA Instance) - Last Job Status should show passed. And the instance should be launched in Openstack.

#### From OSC Setup => Distributed Appliance Edit (In Deployments Spec) the DA to the Openstack Compute, Openstack Project Instances sees this DAI (DA Instance) updated - Last Job Status should show passed. The VNF should be updated in Openstack.

#### From OSC Setup => Distributed Appliance Sync (In Deployments Spec) the DA to the Openstack Compute, Openstack Project Instances sees this DAI (DA Instance) updated. Last Job Status should show passed. The VNF should be updated if it wasn’t previously in Openstack.

#### From Openstack UI, terminate the VNF Instance – it should be automatically redeployed by OSC and job launching it and the VNF instance will show up in Openstack UI.

#### From OSC Setup => Distributed Appliance Delete (In Deployments Spec) the DA to the Openstack Compute, Last Job Status should show passed. If used the VNF won’t be removed from Openstack. If the VNF doesn’t currently protect any port, the VNF should be automatically deleted from Openstack.

#### From OSC Setup => Virtualization Connectors Add a Security Group with VM type and selected Items to have this Victim VM, show up in OSC Virtualization Connectors’ Security Group pane as passed.

#### From OSC Setup => Virtualization Connectors Edit a Security Group with VM type and selected Items to have this Victim VM, show up in OSC Virtualization Connectors’ Security Group pane as passed.

#### From OSC Setup => Virtualization Connectors Sync a Security Group with VM type and selected Items to have this Victim VM as passed.

#### From OSC Setup => Virtualization Connectors Delete a Security Group with VM type and selected Items to have this Victim VM as passed.

#### From OSC Setup => Virtualization Connectors Security Group Bind a DA with specific Policy to this Security Group, next test case end to end will happen as passed.

#### From Attacker, launch an Attack on the Victim VM that supposed to be treated by the VNF that used in the DA, bound to the security group of the Victim VM – the attack should be treated according to the policy that it bound.

#### From OSC Setup => Virtualization Connectors Security Group, Unbind Policy from this Security Group and it has a result the Victim should not be protected anymore.

## VNF VMware vCenter NSX Test Cases

All tests are the same as Openstack except:

* Security grouping and binding policies done from NSX and not from OSC.

#### From OSC Setup => Virtualization Connectors Add a VC with type VMWARE, verify that the VC was appears in OSC as expected.

#### From OSC Setup => Service Function Catalog Auto Import a Security VNF Model/Image, show up in OSC Service Function Catalog pane as passed.

#### From OSC Setup => Distributed Appliance Add a SECURITY VNF image DA. Last Job Status in OSC should show passed. Related Service Definition should be added to NSX. It should also be reflected in the VNF Manager UI.

#### From OSC Setup => Distributed Appliance Edit a SECURITY VNF image DA. Last Job Status in OSC should show passed. Related Service Definition should be updated on NSX. It should also be reflected in the VNF Manager UI.

#### From OSC Setup => Distributed Appliance Sync a SECURITY VNF image DA. Last Job Status in OSC should show passed. Related Service Definition should be updated on NSX. It should also be reflected in the VNF Manager UI.

#### From OSC Setup => Distributed Appliance Delete a SECURITY VNF image DA,. If there is NO VNF deployed that protects VMs in Security group for this DA. This DA should be successfully deleted and the related Service Definition and reflection in VNF Manager should be removed.

### NOTE: Following test cases are in vCenter web client to test it works with OSC:

#### From Installation->Service Deployments add this DA (Service Definition) and install. Installation should be successful and ESX agents should be created on related ESXs. VNF manager should show these devices too, OSC after a while will show those appliance instances as Discovered and Inspection Ready.

#### From NSX Service Composer->Security Groups, Add Victim VM to security group. From NSX Service Composer->Security Policies add a security VNF policy. Apply the new Policy to the Victim VM Security Group.

### From Attacker, launch an Attack on the Victim VM that supposed to be treated by the VNF that used in the DA, bound to the security group of the Victim VM – the attack should be treated according to the policy that it bound.