Third-Party NFV Ecosystem Certification Test Plan

Version 1.6 July 2018

Contents

List of Figures and Tables

Document Control

This is version 1.6 published June 2018. Address any questions to nfv-ecosystem@cisco.com

1 Introduction

1.1 Preface

This document addresses the testing requirements forming part of Cisco's open third-party NFV ecosystem. It should be read in conjunction with material describing the ecosystem program found here: https://developer.cisco.com/site/nfv/

This guide will be updated as the needs of our customers evolve, see the document control section preceding this text for revision details.

Conformance testing is done to determine whether a system meets a specified standard. These test specifications are designed to concentrate on areas critical to interoperability between the Cisco solution and the third-party VNF (Virtual Network Function). Testing includes investigating the VNF's reaction to erroneous behaviour.

1.2 Scope

Ecosystem interoperability focuses on certifying a single third-party VNF's basic functionality and interoperability with Cisco's NFVIS, CSP and NFVI platforms. The vendor and Cisco will discuss and agree which Cisco platforms are applicable for testing, according to the likely deployments desired by mutual customers.

Virtual Network Functions Service chaining and inter-VNF interoperability, full orchestration, services data modelling, and services life cycle are concepts outside the scope of ecosystem certification. Likewise, network performance characterization, and VNF *feature* verification are outside the scope of certification testing.

Some customers require a VNF or service chain be tested against these items even though they are outside the scope of the ecosystem testing. In this case, Cisco Advanced Services should be engaged to perform that testing on a bespoke basis. Figure 1 shows the scope of testing Cisco Advanced Services can carry out. Certification testing may be considered a useful first step in more complete, bespoke testing.

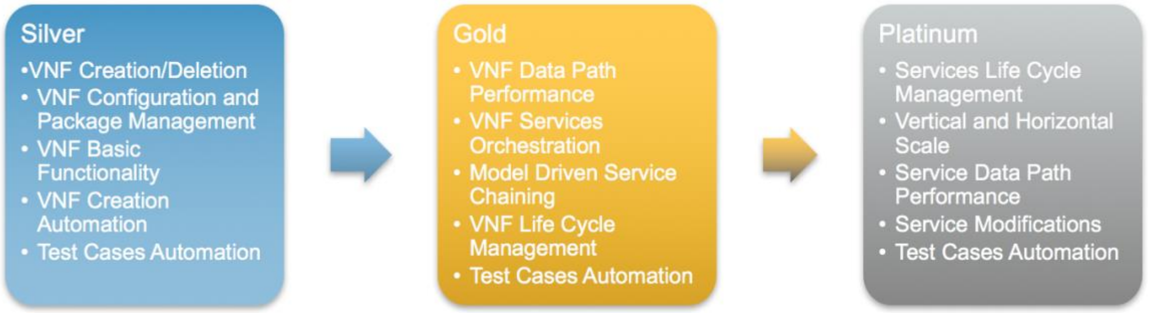
Silver
•VNF Creation/Deletion
• VNF Configuration and Package Management
• VNF Basic Functionality
• VNF Creation Automation
• Test Cases Automation
Gold
• VNF Data Path Performance
• VNF Services Orchestration
• Model Driven Service Chaining
• VNF Life Cycle Management
• Test Cases Automation
Platinum
• Services Life Cycle Management
• Vertical and Horizontal Scale
• Service Data Path Performance
• Service Modifications
• Test Cases Automation

Figure 1: Cisco Advanced Services NFV testing offers

Note: successful customer-driven Advanced Services testing does not afford certification under this program; it does not allow the third-party vendor the benefits of this program.

1.3 Related Documents

- ETSI: Network Functions Virtualisation (NFV); Testing Methodology; Report on NFV Interoperability Testing Methodology
- ETSI: Network Functions Virtualisation (NFV); NFV Security; Security and Trust Guidance

2 Cisco's NFV Solution Components

Cisco offers three solutions in the NFV space designed to cover different use cases. The following building blocks comprise Cisco's NFV solutions:

2.1 Host and Host Operating System

The host platform provides the hardware resources needed, compute, memory and storage. Cisco x86 platforms are supported: Cisco UCS, Cisco ISR routers with UCSe, and purpose-built NFV platforms, the CSP platforms and ENCS 5400 platforms.

These platforms run one of the following environments:

- Cisco's NFVIS operating system: optimized for the virtualized enterprise branch (SD-Branch); a KVM based Linux environment offering Plug-and-Play functionality, a local GUI, and lifecycle management capability. NFVIS is hosted on ENCS or UCS hardware.
- Cisco's NFVIS operating system is also an enabler for the Cisco CloudDock solution. In this role NFVIS is hosted on Cisco's CSP platforms.
- Cisco's CSP operating system: primarily targeted at enterprise DC or Carrier Neutral Facility (CNF) it is the enabler for Cisco's Secure Agile Exchange solution (SAE). CSP is a KVM based Linux environment offering a local GUI, CLI, and lifecycle management capability. The CSP2100, 5200 & 5400 are currently offered as the hardware host.
- Cisco's NFVI: OpenStack environment primarily targeted at service provider customers. In addition to the compute host, this solution also includes storage and switching components.

  For deeper technical information on these solutions please see 'NFVIS & CSP-2100 VNF Spec' and 'NFVI Spec' documents posted in the same place as this collateral.

2.2 Virtualized Network Functions and Applications

The hosted functions can be categorized into network functions such as routing, firewall, Load Balancer, etc.; also, WAN functions such as WAN optimization, caching, route selection, etc.; and applications such as print servers, directory services, DHCP, etc.

Key to the solution is support for non-Cisco functions and applications.

2.3 Service Chaining

Virtualization enables network functionality to be more easily broken smaller atomic functions. These functions can then be chained together to act on a packet flow in an arbitrary order (a service chain), achieving more granular and unique packet handling than was previously practical.

2.4 Orchestration & Management

NFV Solutions require orchestration and management of the VNF components, and service chains. Without strong management capability, the advantages of NFV in terms of platform reduction and improved agility would be easily eroded.

2.4.1 NFVIS

NFVIS offers a built-in management portal, providing GUI access, that enables the administrator to configure the system and hosted VNFs without needing CLI access (though this is also available) on a per device basis.

Primarily aimed at enterprise environments, Cisco's DNA-C provides orchestration and management of NFVIS devices in larger deployments.

In Service Provider Environments NSO or NSO+VMS may be used to manage NFVIS based CPE. Network Services Orchestrator (NSO) is Cisco's network orchestration and automation product (from Tail-f Systems) for both physical and virtual network functions. NSO can be used with or without Cisco Virtual Managed Services (VMS), a tool enabling Service Providers to offer, manage, and deliver virtualized network and security services via the cloud to their enterprise customers.

An important component of NSO-based orchestration is the Core Function Pack (CFP), which brings use-case specific smarts to an NSO or NSO/VMS deployment. For NFVIS, the vBranch CFP enables Service Providers to define customized catalogues of CPE profiles and VNF deployments. Service creation is simplified: elements, such as CPE, Network, Image/Flavor and VNF, can be created in a single commit. The CFP uses knowledge of the inter-dependencies among these entities to correctly stagger service creation or deletion. The vBranch CFP can instantiate unmanaged VNFs that are subsequently configured and managed by an external NMS or VNFs managed by NSO via a vendor specific NED. [1]

NFVIS on CSP hardware also forms the basis for the Cisco CloudDock solution that is an extension of Enterprise WAN network services to a colocation facility. CloudDock orchestrates Cisco and third-party VNF service chains using Cisco vManage in a prescriptive and easy to use pod-like infrastructure design. This solution is focused on the enterprise and mid-market customer segments.[2]

NFVIS also provides REST and NetConf API access for use by other management platforms.

[1] It is **not** expected or required that the vendor perform NSO related testing pre-submission since SP interest in NSO support for a particular VNF will vary and instantiating an NSO environment requires specialist knowledge. Cisco's NSO team will support vendors wanting to perform this pre-testing on request.

[2] It is **not** expected or required that the vendor perform vManage related testing pre-submission since this testing requires access to a vManage instance and supporting functions (vBond, vSmart etc.)

2.4.2 CSP

CSP platforms offer built-in management via a GUI or CLI, they may also be orchestrated and managed by Cisco NSO as described above.

In addition to CloudDock, CSP platforms also form the basis the Cisco SAE solution. SAE can be thought of as a centralized virtual DMZ most likely physically hosted in a colo facility that securely connects the enterprise, it’s branches and partner sites to multiple cloud providers. SAE supports Cisco and third-party VNF service chains orchestrated using an NSO-based core function pack.

REST and NetConf APIs are also offered.

2.4.3 NFVI

NFVI uses Cisco UCS Director together with OpenStack management and Cisco NSO components.

3 Lab Setup, & Test Pre-Requisites

Testing follows the well-proven testing workflow defined in ISO/IEC 9146 and ETSI validation approach. This standard, which covers the entire testing process, provides the basis of this test plan.

Section 4 describes the test cases. It provides an informal, easy-to-read description of each test, concentrating on the meaning of the test rather than detailing how it may be achieved. As described in the ecosystem collateral items (cs.co/3nfv) the goal of testing is to ensure interoperability between the VNF under test, and Cisco's NFV platform. Testing of performance or particular VNF features is outside the scope of the ecosystem certification.

3.1 Equipment

The VNF test lab requires only a minimal set of equipment. Figure 2 depicts a logical view of the test lab topology.

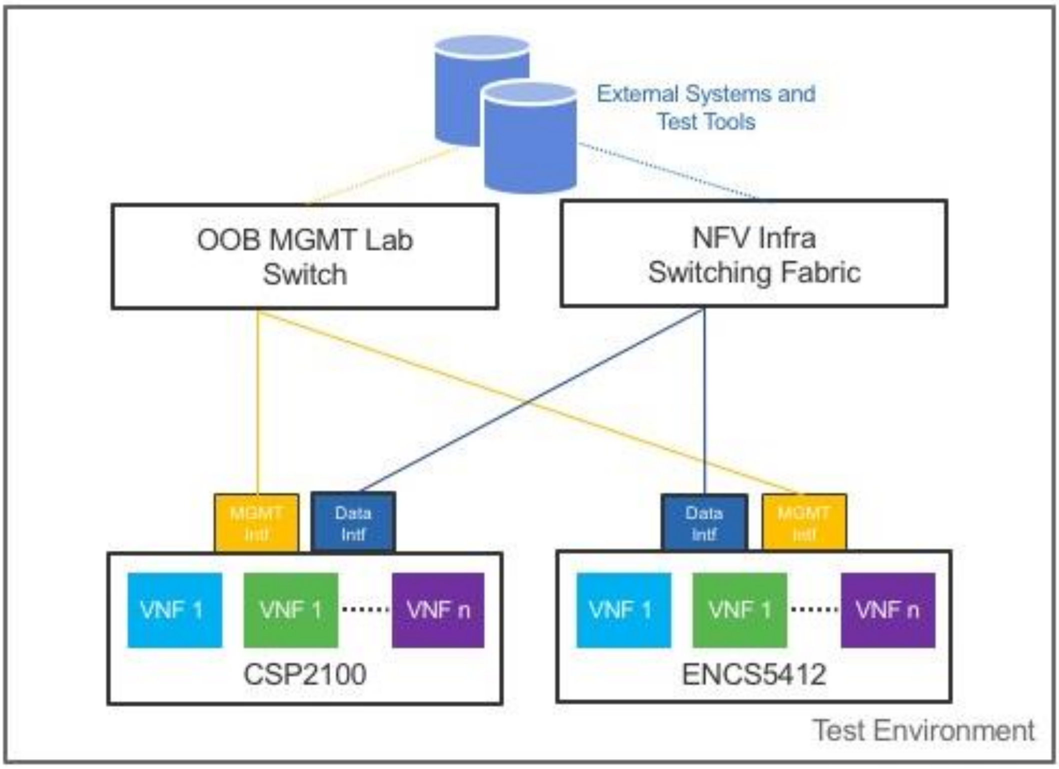

Figure 2: Phase I Lab Topology

ENCS is a host for NFVIS, Cisco's UCS series of x86 servers can also host NFVIS as described in section 2.1 of this document. ENCS and UCS should be considered interchangeable. There is no specific need to test on both.

NFVI infrastructure is not explicitly shown, it is simply an alternative NFV environment to the two shown.

3.2 Software

~~At the time of writing CSP, NFVIS & NFVI are different systems, with specific hypervisors. CSP and NFVIS will merge at some point in the future. In the meantime, a given VNF may be tested on one or more of the three options, depending on the anticipated customer use case.~~

Broadly, Cisco will make available pertinent software to facilitate vendor pre-testing. Hardware can be made available on loan, depending on availability, or via a discounted purchase in others, on a case by case basis. Note,

- NFVIS – can be hosted on ENCS or UCS. In the case a vendor already has UCS hardware, the simplest option is to use that, and receive NFVIS via a software download. UCS C series or UCSe may be used.
- CSP – the software element and hardware are inseparable. To carry out testing therefore, the vendor will require a CSP appliance.
- NFVI – supported on UCS hardware and generic x86. In the case a vendor already has suitable hardware, the simplest option is to use that, and receive NFVI via a software download.

Cisco will perform certification testing on the current GA code, as posted on the software download site of cisco.com, in all cases, noting the version(s) used. For pre-submission testing, consult with the ecosystem team to determine the best option for a particular VNF.

3.3 Configuration Information

Before certification testing begins, Cisco requires certain VNF parameters to be supplied as part of the VNF submission. The document ‘Submission Procedure’ posted on cs.co/3nfv details these. Also posted is an excerpt of the questionnaire section for easier submission.

The requested information should be assembled by the vendor at the time of pre-submission testing.

4 Test Plan

The test plan comprises the individual tests listed in the tables that follow.

‘Test applicability’ defines when the particular individual test will be applied.

- Initial Certification: When a VNF is first on boarded into the ecosystem program
- Vendor re-certification: A re-test following a significant revision made by the vendor to the VNF.
- Cisco re-certification: A re-test at Cisco’s discretion following a significant revision to the underlying Cisco NFV infrastructure.

‘Priority’ defines whether a test is mandatory, or the level of importance attached to the test case.

4.1 Single VNF Instantiation with NSO Core Function Pack (CFP)

The purpose of this test is to discover if the VNF can be orchestrated by NSO (and hence, by extension, VMS). Please note footnote to section **Error! Reference source not found.**

Test Case Objective	Instantiation of a single newly-defined VNF by NSO
Test applicability	☒ Initial certification ☒ Vendor re-certification ☒ Cisco re-certification ☒ NFVIS ☐ CSP
Priority	Highly recommended [especially if VNF vendor targets SP customers]
Prerequisites	1. NSO and vBranch CFP are installed and connected with ENCS/NFVIS 2. ENCS are accessible over management IP address with admin account privileges 3. VNF specs: vCPU, Memory, Storage, Bridge type (Linux, OVS, SR-IOV) and Networks 4. VNF vendor should specify which interfaces should be utilized (i.e. for OOB management, data, etc.) 5. VNF image format: tar.gz, qcow2, img, or iso 6. Any VNF license required 7. VNF vendor should provide file path of day0 file on the mounted configuration drive upon deployment
Test Procedure	1. Login into NSO with SSH 2. Define VNF Descriptor based on VNF package, and create vnfd.xml for VNF and load merge it in NSO 3. Define VNF catalog, and create catalog-deployment.xml for VNF and load merge it in NSO 4. Create register-vnfd.xml for VNF and load merge it in NSO 5. Create vnf.xml for VNF and load merge it in NSO
Test Validation	1. Validate that VNF deployed successfully, and it complies with VNF specifications and requirements 2. Access VNF over console or SSH 3. Verify VNF license is installed if it is defined in the VNFD. 4. Check whether VNF consumes day0 configuration
Pass/Failure Criteria	VNF should be up and accessible over console or SSH
References	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/csp_2100/command_ref/Cisco_CSP_2100_Command_Ref.html http://www.cisco.com/c/en/us/td/docs/switches/datacenter/csp_2100/rest_api/Cisco_CSP_2100_REST_API_Guide.pdf http://www.cisco.com/c/en/us/products/routers/enterprise-nfv-infrastructure-software/index.html Validating 3rd Party VNFs with Cisco's vBranch Core Function Pack & NFVIS

Table 1: VNF Instantiation

4.2 Single VNF Instantiation with vManage

The purpose of this test is to discover if the VNF can be orchestrated by vManage. Please note second footnote to section **Error! Reference source not found.**

Test Case Objective	**Instantiation of a single newly-defined VNF by NSO**
Test applicability	☒ Initial certification ☒ Vendor re-certification ☒ Cisco re-certification ☒ NFVIS ☐ CSP
Priority	Highly recommended [especially if VNF vendor targets Enterprise/SP customers]
Prerequisites	1. vManage is installed and connected with CSP/NFVIS 2. CSP is accessible over management IP address with admin account privileges 3. VNF specs: vCPU, Memory, Storage, Bridge type (Linux, OVS, SR-IOV) and Networks 4. VNF vendor should specify which interfaces should be utilized (i.e. for OOB management, data, etc.) 5. VNF image format: tar.gz, qcow2, img, or iso 6. Any VNF license required 7. VNF vendor should provide file path of day0 file on the mounted configuration drive upon deployment
Test Procedure	1. Login into vManage GUI 2. Create a service chain using multiple VNFs with day0 files 3. Deploy the service chain in CSP
Test Validation	1. Validate that VNF deployed successfully, and it complies with VNF specifications and requirements 2. Access VNF over console or SSH 3. Verify VNF license is installed if it is defined in the VNFD. 4. Check whether VNF consumes day0 configuration
Pass/Failure Criteria	VNF should be up and accessible over console or SSH
References	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/csp_2100/command_ref/Cisco_CSP_2100_Command_Ref.html http://www.cisco.com/c/en/us/td/docs/switches/datacenter/csp_2100/rest_api/Cisco_CSP_2100_REST_API_Guide.pdf http://www.cisco.com/c/en/us/products/routers/enterprise-nfv-infrastructure-software/index.html Validating 3rd Party VNFs with Cisco's vBranch Core Function Pack & NFVIS

Table 2: VNF Instantiation – Solutions Test

4.3 Single VNF Termination with NSO CFP

Test Case Objective	**Termination of a single newly-defined VNF by NSO**
Test applicability	☒ Initial certification ☒ Vendor re-certification ☒ Cisco re-certification ☒ NFVIS □ CSP
Priority	Mandatory **if** test 4.1 is executed.
Prerequisites	1. NSO CFP is installed and connected with ENCS/NFVIS 2. ENCS are accessible over management IP address with admin privileges 3. Single VNF instance should be active and accessible over console port
Test Procedure	1. Login into to NSO with SSH CLI 2. Delete VNF instance with CLI
Test Validation	1. Validate that VNF was deleted successfully and all reserved compute resources have been released. 2. Verify VNF license has been revoked and returned to free licenses pool if applicable.
Pass/Failure Criteria	VNF should be removed from ENCS/NFVI, compute resources, and license has been released
References	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/csp_2100/command_ref/Cisco_CSP_2100_Command_Ref.html http://www.cisco.com/c/en/us/td/docs/switches/datacenter/csp_2100/rest_api/Cisco_CSP_2100_REST_API_Guide.pdf http://www.cisco.com/c/en/us/products/routers/enterprise-nfv-infrastructure-software/index.html Validating 3rd Party VNFs with Cisco's vBranch Core Function Pack & NFVIS

Table 3: Single VNF Termination

4.4 Single VNF Instantiation

Test Case Objective	**Instantiation of a single newly-defined VNF hosted by CSP2100 and ENCS platforms**
Test applicability	☒ Initial certification ☒ Vendor re-certification ☒ Cisco re-certification ☒ NFVIS ☒ CSP
Priority	Mandatory
Prerequisites	8. CSP2100 and ENCS are accessible over management IP address with admin account privileges 9. VNF specs: vCPU, Memory, Storage, Bridge type (Linux, OVS, SR-IOV) and Networks 10. VNF vendor should specify which interfaces should be utilized (i.e. for OOB management, data, etc.) 11. VNF image format tar.gz, qcow2, img, or iso 12. VNF license 13. VNF vendor should provide file path of day0 file on the mounted configuration drive upon deployment 14. Uploading Day0 configuration options (CDROM, or virtual mounted disk) 15. Uploading day1/2 VNF configuration (Optional)
Test Procedure	4. Login into CSP2100 and ENCS/NFVIS WebUI or SSH CLI 5. Upload VNF image into CSP2100 and ENCS/NFVIS inventory 6. Check the syntax of the day0 configuration in order to be consumed properly by the VNF 7. Instantiate the VNF instance using CSP2100 and ENCS/NFVIS CLI, WebUI utilities, or REST APIs
Test Validation	5. Validate that VNF deployed successfully and it complies with VNF specifications and requirements 6. Access VNF over console or SSH 7. Verify VNF license installation 8. Check whether VNF consumes day0 configuration
Pass/Failure Criteria	VNF should be up and accessible over console or SSH
References	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/csp_2100/command_ref/Cisco_CSP_2100_Command_Ref.html http://www.cisco.com/c/en/us/td/docs/switches/datacenter/csp_2100/rest_api/Cisco_CSP_2100_REST_API_Guide.pdf http://www.cisco.com/c/en/us/products/routers/enterprise-nfv-infrastructure-software/index.html

Table 4: VNF Instantiation

4.5 Multi VNF Creation

Test Case Objective	**Instantiation of multiple instances of newly-defined VNFs hosted by CSP2100 and ENCS platforms**
Test applicability	☒ Initial certification ☒ Vendor re-certification ☒ Cisco re-certification ☒ NFVIS ☒ CSP
Priority	Highly Recommended
Prerequisites	1. CSP2100 and ENCS are accessible over management IP address with admin account privileges 2. VNF specs: vCPU, Memory, Storage, Bridge type (Linux, OVS, SR-IOV) and Networks 3. VNF vendor should specify which interfaces should be utilized (i.e. for OOB management, data, etc.) 4. VNF image format tar.gz, qcow2, img, or iso 5. VNF license 6. VNF vendor should provide file path of day0 file on the mounted configuration drive upon deployment 7. Uploading Day0 configuration options (CDROM, or virtual mounted disk) 8. Uploading day1/2 VNF configuration (Optional)
Test Procedure	1. Login into CSP2100 and ENCS/NFVIS WebUI or SSH CLI 2. Upload VNF image into CSP2100 and ENCS/NFVIS inventory 3. Check the syntax of the day0 configuration in order to ensure proper consumption by the VNF 4. Instantiate multiple (2 or more) VNF instances using CSP2100 and ENCS REST APIs
Test Validation	1. Validate that all VNFs deployed successfully and they comply with VNF specifications and requirements 2. Access VNF over console or SSH 3. Verify VNF license installation 4. Check whether VNF consumes day0 configuration
Pass/Failure Criteria	VNF should be up and accessible over console or SSH
References	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/csp_2100/command_ref/Cisco_CSP_2100_Command_Ref.html http://www.cisco.com/c/en/us/td/docs/switches/datacenter/csp_2100/rest_api/Cisco_CSP_2100_REST_API_Guide.pdf http://www.cisco.com/c/en/us/products/routers/enterprise-nfv-infrastructure-software/index.html

Table 5: Multi VNF creation

4.6 Single VNF Termination

Test Case Objective	**Termination of a single newly-defined VNF hosted by CSP2100 and ENCS platforms**
Test applicability	☒ Initial certification ☒ Vendor re-certification ☒ Cisco re-certification ☒ NFVIS ☒ CSP
Priority	Mandatory
Prerequisites	4. CSP2100 and ENCS are accessible over management IP address with admin privileges 5. Single VNF instance should be active and accessible over console port
Test Procedure	3. Login into CSP2100 and ENCS/NFVIS WebUI or SSH CLI 4. Delete the VNF instance using CSP2100 and ENCS/NFVIS CLI, WebUI utilities, or REST APIs
Test Validation	3. Validate that VNF was deleted successfully and all reserved compute resources have been released. 4. Verify VNF license has been revoked and returned to free licenses pool
Pass/Failure Criteria	VNF should be removed from CSP2100 and ENCS/NFVI, compute resources, and license has been released
References	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/csp_2100/command_ref/Cisco_CSP_2100_Command_Ref.html http://www.cisco.com/c/en/us/td/docs/switches/datacenter/csp_2100/rest_api/Cisco_CSP_2100_REST_API_Guide.pdf http://www.cisco.com/c/en/us/products/routers/enterprise-nfv-infrastructure-software/index.html

Table 6: Single VNF Termination

4.7 Multiple VNF Termination

Test Case Objective	Termination of Multiple VNFs hosted by CSP2100 and ENCS platforms
Test applicability	☒ Initial certification ☐ Vendor re-certification ☐ Cisco re-certification ☒ NFVIS ☒ CSP
Priority	Highly Recommended
Prerequisites	1. CSP2100 and ENCS are accessible over management IP address with admin account privileges 2. Multiple VNF instances should be active and accessible over console port
Test Procedure	1. Login into CSP2100 and ENCS/NFVIS WebUI or SSH CLI 2. Delete all VNF instances using CSP2100 and ENCS/NFVIS REST APIs
Test Validation	5. Validate that VNFs were deleted successfully and all reserved compute resources have been released. 6. Verify VNF license has been revoked and returned to free licenses pool
Pass/Failure Criteria	VNF should be removed from CSP2100 and ENCS/NFVI, compute resources, and license has been released
References	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/csp_2100/command_ref/Cisco_CSP_2100_Command_Ref.html http://www.cisco.com/c/en/us/td/docs/switches/datacenter/csp_2100/rest_api/Cisco_CSP_2100_REST_API_Guide.pdf http://www.cisco.com/c/en/us/products/routers/enterprise-nfv-infrastructure-software/index.html

Table 7: Multi VNF Termination

4.8 VNF Operational State Changes

Test Case Objective	**Validate Operational state changes on operational VNF**
Test applicability	☒ Initial certification ☒ Vendor re-certification ☒ Cisco re-certification ☒ NFVIS ☒ CSP
Priority	Mandatory
Prerequisites	1. CSP2100 and ENCS are accessible over management IP address with admin account privileges 2. Single VNF instance should be active and accessible over console port
Test Procedure	1. Login into CSP2100 and ENCS/NFVIS WebUI or SSH CLI 2. Validate VNF functionality after platform (CSP2100 and ENCS5400) forced reboot over CLI or WebUI 3. Validate the following the following operational states on an active VNF: a. Power-on and power-off b. Reset | Restart (soft reset)
Test Validation	1. Validate that VNF recovers from the operational state change 2. Access VNF over console or SSH
Pass/Failure Criteria	VNF should recover from operational state change
References	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/csp_2100/command_ref/Cisco_CSP_2100_Command_Ref.html http://www.cisco.com/c/en/us/td/docs/switches/datacenter/csp_2100/rest_api/Cisco_CSP_2100_REST_API_Guide.pdf http://www.cisco.com/c/en/us/products/routers/enterprise-nfv-infrastructure-software/index.html

Table 8: VNF State Changes

4.9 VNF Scaling-Up and Scaling-Down (Vertical Scalability)

Test Case Objective	Validate VNF functionality and service continuity after boosting pre-allocated compute resources
Test applicability	☒ Initial certification ☒ Vendor re-certification ☒ Cisco re-certification ☒ NFVIS ☒ CSP
Priority	Mandatory
Prerequisites	1. CSP2100 and ENCS are accessible over management IP address with admin account privileges 2. Single VNF instance should be active and accessible over console port
Test Procedure	1. Login into CSP2100 and ENCS/NFVIS WebUI or SSH CLI 2. Stop VNF 3. Increase pre-allocated VNF resources. The change should be bounded within the platform's available resources a. vCPU b. Memory c. Storage d. vNICs 4. Start VNF
Test Validation	1. Validate VNF functionality after resources boost. 2. Access VNF over console or SSH
Pass/Failure Criteria	1. Check resource availability after scaling-up/down hence to ensure that resources have been properly allocated or released
References	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/csp_2100/command_ref/Cisco_CSP_2100_Command_Ref.html http://www.cisco.com/c/en/us/td/docs/switches/datacenter/csp_2100/rest_api/Cisco_CSP_2100_REST_API_Guide.pdf http://www.cisco.com/c/en/us/products/routers/enterprise-nfv-infrastructure-software/index.html

Table 9: VNF Scale up / Scale down

4.10 VNF Scaling-In and Scaling-Out (Horizontal Scalability)

Test Case Objective	Validate scaling out and scaling VNF instances hosted by CSP2100 and ENCS platforms
Test applicability	☒ Initial certification ☒ Vendor re-certification ☒ Cisco re-certification ☒ NFVIS ☒ CSP
Priority	Optional
Prerequisites	1. CSP2100 and ENCS are accessible over management IP address with admin account privileges 2. VNF specs: vCPU, Memory, Storage, Bridge type (Linux, OVS, SR-IOV) and Networks 3. VNF vendor should specify which interfaces should be utilized (i.e. for OOB management, data, etc.) 4. VNF image format tar.gz, qcow2, img, or iso 5. VNF license 6. VNF vendor should provide file path of day0 file on the mounted configuration drive upon deployment 7. Uploading Day0 configuration options (CDROM, or virtual mounted disk) 8. Uploading day1/2 VNF configuration (Optional)
Test Procedure	1. Login into CSP2100 and ENCS/NFVIS WebUI or SSH CLI 2. Upload VNF image into CSP2100 and ENCS/NFVIS inventory 3. Check the syntax of the day0 configuration to ensure proper consumption by the VNFs 4. Instantiate multiple VNF instances using CSP2100 and ENCS REST APIs 5. Start terminating VNF instances while validating CSP2100 and ENCS resource quota
Test Validation	1. Validate CSP2100 and ENCS resources utilization. Scaling VNF instances should not exceed platform available resources 2. Validate CSP2100 and ENCS resources availability. VNF instances termination should release allocated resources
Pass/Failure Criteria	CSP2100 and ENCS should accommodate VNF instances up to available resources. VNF termination should recover allocated resources.
References	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/csp_2100/command_ref/Cisco_CSP_2100_Command_Ref.html http://www.cisco.com/c/en/us/td/docs/switches/datacenter/csp_2100/rest_api/Cisco_CSP_2100_REST_API_Guide.pdf http://www.cisco.com/c/en/us/products/routers/enterprise-nfv-infrastructure-software/index.html

Table 10: VNF Scale In / Scale Out

4.11 VNF Backup and Recovery

Test Case Objective	Validate VNF backup and restore support
Test applicability	☒ Initial certification ☒ Vendor re-certification ☒ Cisco re-certification ☐ NFVIS ☒ CSP
Priority	Optional
Prerequisites	1. Single VNF instance should be up 2. VNFs have at least admin user account which permits wide privileged access 3. VNF has day0 configuration. All required bridging, pNICs, and vNICs should be up and active
Test Procedure	1. Login into CSP2100 WebUI or SSH CLI 2. Backup/snapshot VNF instance 3. Terminate active VNF instance 4. Load backup VNF instance file from device file inventory 5. Spin a new VNF instance following □test procedure
Test Validation	1. Check VNF backup file store on CSP2100 file inventory 2. VNF restored with day0 configuration
Pass/Failure Criteria	VNF should support backup and restore
References	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/csp_2100/command_ref/Cisco_CSP_2100_Command_Ref.html http://www.cisco.com/c/en/us/td/docs/switches/datacenter/csp_2100/rest_api/Cisco_CSP_2100_REST_API_Guide.pdf http://www.cisco.com/c/en/us/products/routers/enterprise-nfv-infrastructure-software/index.html

Table 11: VNF Backup & Recovery

4.12 VNF Management Connectivity

Test Case Objective	**Validate VNF secure communicate paths outside and within CSP2100 and ENCS/NVIS OS components**
Test applicability	☒ Initial certification ☒ Vendor re-certification ☒ Cisco re-certification ☒ NFVIS ☒ CSP
Priority	Mandatory
Prerequisites	1. CSP2100 and ENCS are accessible over management IP address with admin account privileges 2. Single VNF instance should be active and accessible over console port
Test Procedure	1. From vendor's documentation, determine management interfaces expected on VNF (for example, ssh, SNMP, HTTPS) 2. From vendor's documentation, determine nature of any API present on a management interface(s) (for example, REST, RESTCONF, NetConf etc.)
Test Validation	1. Validate connectivity to expected ports/services in (1) above 2. Validate API(s) identified in (2) above are active 3. Check for unexpected or malicious traffic generated by VNF
Pass/Failure Criteria	VNF should allow management connections to expected management interfaces
References	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/csp_2100/command_ref/Cisco_CSP_2100_Command_Ref.html http://www.cisco.com/c/en/us/td/docs/switches/datacenter/csp_2100/rest_api/Cisco_CSP_2100_REST_API_Guide.pdf http://www.cisco.com/c/en/us/products/routers/enterprise-nfv-infrastructure-software/index.html

Table 12: VNF Management Connectivity

4.13 VNF Integration with External Services

Test Case Objective	**Validate VNF to integrate with external services**
Test applicability	☒ Initial certification ☒ Vendor re-certification ☒ Cisco re-certification ☒ NFVIS ☒ CSP
Priority	Highly Recommended
Prerequisites	1. VNF is up 2. VNF has at least admin user account which permits wide privileged access
Test Procedure	1. Login into CSP2100 and ENCS/NFVIS WebUI or SSH CLI 2. Upload VNF image into CSP2100 and ENCS/NFVIS inventory 3. Edit day0 configuration thus incorporate the following services configuration: a. DNS server(s) b. NTP server(s) c. DHCP Client d. Zero-touch (Plug-n-Play Open client) 4. Check the syntax of the day0 configuration to ensure proper consumption by the VNF 5. Instantiate single VNF instance using CSP2100 and ENCS REST APIs 6. Connect to VNF, and…
Test Validation	Validate VNF accepts external services configuration
Pass/Failure Criteria	VNF should configure and document external services supportability
References	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/csp_2100/command_ref/Cisco_CSP_2100_Command_Ref.html http://www.cisco.com/c/en/us/td/docs/switches/datacenter/csp_2100/rest_api/Cisco_CSP_2100_REST_API_Guide.pdf http://www.cisco.com/c/en/us/products/routers/enterprise-nfv-infrastructure-software/index.html

Table 13: VNF Integration with External Services

4.14 VNF High Availability

Test Case Objective	**Validate VNF high availability support**
Test applicability	☒ Initial certification ☒ Vendor re-certification ☒ Cisco re-certification ☒ NFVIS ☒ CSP
Priority	Optional – applies only if VNF has H.A. capability
Prerequisites	1. VNF must support HA functionality, or test is not applicable. 2. Two VNF instances are up on different CSP2100 or ENCS platforms 3. VNFs have at least admin user account which permits wide privileged access 4. VNF has day0 configuration. All required bridging, pNICs, and vNICs should be up and active
Test Procedure	1. Login into CSP2100 and ENCS/NFVIS WebUI or SSH CLI 2. Connect to VNFs as admin user 3. Configure day1/2 VNF high-availability configuration. VNF peer (virtual cluster) should operate one of the following: a. Active/active; or, b. Active/standby 4. Start a continuous ping from a device external to the NFV platform to the VNF 5. Force reload active VNF
Test Validation	Check VNF, CSP2100, and ENCS interface counters. They all should reporting that IP Ping packets got forwarded properly. Record number of pings lost, and time duration of switchover.
Pass/Failure Criteria	1. HA partner VNF should assume processing of traffic 2. Any packet loss should be in line with vendor guidance
References	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/csp_2100/command_ref/Cisco_CSP_2100_Command_Ref.html http://www.cisco.com/c/en/us/td/docs/switches/datacenter/csp_2100/rest_api/Cisco_CSP_2100_REST_API_Guide.pdf http://www.cisco.com/c/en/us/products/routers/enterprise-nfv-infrastructure-software/index.html

Table 14: VNF High Availability

4.15 Data Path Integrity

Test Case Objective	Validate VNF north-south data path using IPv4 and IPv6 Pings
Test applicability	☒ Initial certification ☒ Vendor re-certification ☒ Cisco re-certification ☒ NFVIS ☒ CSP
Priority	Optional
Prerequisites	1. VNF is up 2. VNF has at least admin user account which permits wide privileged access 3. VNF has day0 configuration. All required bridging, pNICs, and vNICs should be up and active
Test Procedure	1. Login into CSP2100 and ENCS/NFVIS Web UI or SSH CLI 2. Connect to VNF as admin user via console or management interface 3. Configure day1/2 VNF interfaces configuration 4. Starts continuous IPv4 and IPv6 Ping process from VNF to an outside IP address
Test Validation	Check VNF, CSP2100, and ENCS interface counters. They all should reporting that IP ping packets were forwarded properly
Pass/Failure Criteria	VNF, CSP2100, and ENCS should not report any ping loss
References	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/csp_2100/command_ref/Cisco_CSP_2100_Command_Ref.html http://www.cisco.com/c/en/us/td/docs/switches/datacenter/csp_2100/rest_api/Cisco_CSP_2100_REST_API_Guide.pdf http://www.cisco.com/c/en/us/products/routers/enterprise-nfv-infrastructure-software/index.html

Table 15: VNF Data Path Integrity

4.16 VNF Error Handling

Test Case Objective	**VNF reaction to synthetic error injection**
Test applicability	☒ Initial certification ☒ Vendor re-certification ☒ Cisco re-certification ☒ NFVIS ☒ CSP
Priority	Highly Recommended
Prerequisites	1. NFV platform with multiple VNF instances should be up leaving enough compute resources for additional VNF instance 2. VNF image present on NFV platform's resource storage
Test Procedure	1. Login into CSP2100 and ENCS/NFVIS WebUI or SSH CLI 2. Spin a new VNF instance by requesting proper compute resources from NFV platform 3. Once VNF is running, inject synthetic error: a. Storage space exhaustion. Document how the VNF reacts during operation while allocated storage is near full and exhausted. b. External network connectivity failure. Document how the VNF reacts while one of the data links is failed. c. Internal platform NFV platform connectivity failure (vSwitch issue). Document how the VNF reacts while VIM vSwitch is failed. 4. For each, document VNF behaviour and any error generation.
Test Validation	VNF should generate error when platform resources are unavailable and should recover from the error condition once resolved. VNF vendor should share error logs/traps/notifications and troubleshooting in an operational guide.
Pass/Failure Criteria	VNF should recover from error condition once the cause of failure is removed
References	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/csp_2100/command_ref/Cisco_CSP_2100_Command_Ref.html http://www.cisco.com/c/en/us/td/docs/switches/datacenter/csp_2100/rest_api/Cisco_CSP_2100_REST_API_Guide.pdf http://www.cisco.com/c/en/us/products/routers/enterprise-nfv-infrastructure-software/index.html

Table 16: Test Plan Template

4.17 VNF Configuration and Package Management

Test Case Objective	**Patching software to an active VNF hosted by CSP2100 and ENCS platforms**
Test applicability	☐ Initial certification ☒ Vendor re-certification ☐ Cisco re-certification ☒ NFVIS ☒ CSP
Priority	Mandatory in case where upgrade is via a patch, else not applicable.
Prerequisites	1. CSP2100 and ENCS are accessible over management IP address with admin account privileges 2. Single VNF instance should be active and accessible over console port
Test Procedure	1. Login into CSP2100 and ENCS/NFVIS WebUI or SSH CLI 2. Upload VNF patch software into CSP2100 and ENCS/NFVIS inventory 3. Patch additive software into VNF instance using CSP2100 and ENCS/NFVIS CLI, WebUI utilities, or REST APIs
Test Validation	1. Validate that VNF patch deployed successfully 2. Access VNF over console or SSH 3. Validate that software update process has no functional impact on VNF
Pass/Failure Criteria	VNF should maintain functionality while patching software update
References	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/csp_2100/command_ref/Cisco_CSP_2100_Command_Ref.html http://www.cisco.com/c/en/us/td/docs/switches/datacenter/csp_2100/rest_api/Cisco_CSP_2100_REST_API_Guide.pdf http://www.cisco.com/c/en/us/products/routers/enterprise-nfv-infrastructure-software/index.html

Table 17: VNF Configuration and Package Management

4.18 NFV Infrastructure Upgrade

Test Case Objective	Validate VNF Operation while CSP2100 and ENCS platform upgrade
Test applicability	☐ Initial certification ☐ Vendor re-certification ☒ Cisco re-certification ☒ NFVIS ☒ CSP
Priority	Mandatory
Prerequisites	1. CSP2100 and ENCS are accessible over management IP address with admin account privileges 2. Single VNF instance should be active and accessible over console port
Test Procedure	1. Login into CSP2100 and ENCS/NFVIS WebUI or SSH CLI 2. Mount CSP2100 and ENCS NFVIS OS file into CIMC virtual terminal disk 3. Could reboot from CIMC 4. While CSP2100 and ENCS booting up; Press F6 to access “BIOS boot up sequence” menu 5. Select CIMC DVD mounted image option, then continue booting 6. Validate VNF functionality after platform (CSP2100 and ENCS5400) forced to reboot via CLI or WebUI
Test Validation	3. Validate that VNF recovered after CSP2100 and ENCS finish OS upgrade 4. Access VNF over console or SSH
Pass/Failure Criteria	VNF should recover from infrastructure/platform OS upgrade
References	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/csp_2100/command_ref/Cisco_CSP_2100_Command_Ref.html http://www.cisco.com/c/en/us/td/docs/switches/datacenter/csp_2100/rest_api/Cisco_CSP_2100_REST_API_Guide.pdf http://www.cisco.com/c/en/us/products/routers/enterprise-nfv-infrastructure-software/index.html

Table 18: NFV Infrastructure Upgrade

Trademarks, Disclaimers and Contact Information

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THIRD PARTY SUPPLIERS ARE PROVIDED “AS IS” WITH ALL FAULTS. CISCO AND THIRD PARTY SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Please direct any queries relating to this document, or the third-party ecosystem, to nfv-ecosystem@cisco.com