ETSI GR NFV-TST 005 V3.1.1 (2017-03)

Network Functions Virtualisation (NFV); Continuous Development and Integration; Report on use cases and recommendations for VNF Snapshot

Disclaimer

The present document has been produced and approved by the Network Functions Virtualisation (NFV) ETSI Industry Specification Group (ISG) and represents the views of those members who participated in this ISG.
It does not necessarily represent the views of the entire ETSI membership.

Reference

DGR/NFV-TST005

Keywords

management, NFV, testing

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Group Report (GR) has been produced by ETSI Industry Specification Group (ISG) Network Functions Virtualisation (NFV).

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

1 Scope

The present document reports on use cases, recommendations and potential solutions for VNF snapshotting, with the following objectives:

a) Describing use cases that would benefit from VNF Snapshot functionality.

b) Identifying gaps by studying the conditions for capturing VNF/VNFC Snapshots and VNF data.

c) Describing end-to-end orchestration procedures and overall framework supporting the capture of VNF data and VNF/VNFC Snapshots.

d) Analysing recommendations for the support of VNF/VNFC Snapshots.

The present document considers analysing and leveraging available related techniques from Open Source and others.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI GS NFV 003: "Network Functions Virtualisation (NFV); Terminology for Main Concepts in NFV".

[i.2] ETSI GS NFV-IFA 005: "Network Functions Virtualisation (NFV); Management and Orchestration; Or-Vi reference point - Interface and Information Model Specification".

[i.3] ETSI GS NFV-IFA 006: "Network Functions Virtualisation (NFV); Management and Orchestration; Vi-Vnfm reference point - Interface and Information Model Specification".

[i.4] ETSI GS NFV-IFA 007: "Network Functions Virtualisation (NFV); Management and Orchestration; Or-Vnfm reference point - Interface and Information Model Specification".

[i.5] ETSI GS NFV-IFA 008: "Network Functions Virtualisation (NFV); Management and Orchestration; Ve-Vnfm reference point - Interface and Information Model Specification".

[i.6] ETSI GS NFV-IFA 011: "Network Functions Virtualisation (NFV); Management and Orchestration; VNF Packaging Specification".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in ETSI GS NFV 003 [i.1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in ETSI GS NFV 003 [i.1].

service consumer: person, device or company consuming a service provided by a Service Provider

VNF provider: person or company providing the VNF

NOTE: This includes, but is not limited to vendor, integrator or in-house developer.

VNF Snapshot: replication of a VNF instance at a specific point in time, containing a consistent set of VNFC Snapshots of all VNFC instances associated to the VNF instance, the VNF Descriptor and the VnfInfo (including state and settings of Virtual Links and Connection Points associated to this VNF)

VNF Snapshot Package: collection of files representing a VNF Snapshot which can be physically stored and transferred

NOTE: A more detailed description of VNF/VNFC Snapshots and their packages is provided in clause 6.1.

VNFC Snapshot: replication of a VNFC instance at a specific point in time, capturing its full or partial state (such as state and content of the disks, memory and devices attached to the VNFC instance plus the infrastructure configuration of the VNFC instance)

VNFC Snapshot Package: collection of files representing a VNFC Snapshot which can be physically stored and transferred

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI GS NFV 003 [i.1] apply.

4 Use cases

4.1 Use cases related to testing

4.1.1 VNF Snapshot during online testing

4.1.1.1 Introduction

Service Providers which use NFV technology verify their virtualised network system (i.e. network service) that they developed by testing from various viewpoints, and once all the system behaviours that will happen during operation in the production environment are thoroughly tested in the testing environment, the Service Providers begin to provide the service using the network system on the production environment. However, the virtualised network systems have been getting complicated due to multi-vendor environment, adoption of variety of open source software, etc., hence it has been getting difficult to verify all the system behaviours thoroughly in the testing environment. If a service is provided under such a situation, it is considered that the possibility of service outage would increase because of the underlying bugs in the production system.

Therefore, it is necessary to reveal and remove the underlying bugs from the network system by continually verifying the network system which is already providing the service on the production environment. This clause calls this kind of testing online testing. If the Service Providers verify the systems which are in operation by online testing, they can conduct various tests under the real complex system states which are created by real users. It is expected that the systems are tested under more realistic conditions and that the underlying bugs in the system will be easier to be found and removed compared with the testing environment.

The online testing includes fault injection testing (e.g. by stop a VM at random), load injection testing (e.g. by adding large amount of traffic), etc. to verify reliability/availability of the system. By practicing this kind of tests continually "in a controlled manner", the service provider can discover and fix potential bugs which could not be found in the testing environment, build up more robust system, and prevent the system from major service outages.

The online testing should be done in a controlled manner, as this testing may affect the running system especially when the test fails, which means an underlying bug is revealed by the test. To conduct online tests in a controlled manner, one thing is to reinforce monitoring around tested area and then the Service Provider can react a test failure immediately if it happens. Another is to capture data of the VNF instances which are potentially affected by the test prior to the test. This can be done by taking VNF Snapshots. In case the test fails and the VNF instance cannot recover after restart, the capture data/VNF Snapshots will be used to recover the (failed) VNF instances to a previous normal running status without consuming time to inject any configuration data (If those VNF instances are deleted and re-instantiated without using snapshots, it will take time to make the VNF instances be ready to start the services because no configuration data exist in the VNF instances after instantiation of them. Also, this requires to store the exact data somehow at the time before the test was started.). In this way, the online testing can be done in a controlled and safe manner.

This present use case shows the VNF Snapshot as part of an online testing by injecting failure(s) (e.g. VM stall, network disruption, etc.) to verify the system's reliability. The online testing is supposed to be performed by the Service Provider manually, or an online testing function which may be part of the NFV-MANO or outside of it (e.g. the OSS/BSS) automatically, depending on architectural options. Once VNF Snapshot(s) are created for restore purpose, an actual test scenario is executed. In case the test results in failure, the system is restored using the capture data by hand or automatically.

4.1.1.2 Actors

For this use case, the following actors are involved:

1) Service Provider is informed about the availability of captured data.

2) VNF Provider is informed about the availability of captured data.

4.1.1.3 Pre-conditions

1) A network service which is intended to be tested, is in operation on the production environment, and is providing a service to the Service Consumers.

2) The network service is composed of one or more VNF instances, which are composed of one or more VNFC instances. A VNFC instance is running on a virtualised container (e.g. virtual machine, system/application container).

3) The VNF instances have a high availability mechanism and they have auto recovery functionality for possible failures.

4) The expected recovery time from failures are defined by the network service.

5) For the network service to be tested, the execution of the online testing to verify failure recovery is triggered by the Service Provider.

4.1.1.4 Description

The following steps are executed:

1) The Service Provider determines the place to be tested and test scenario (e.g. VM shutdown for the simulation of VM stall) for the network service.

2) The Service Provider gets the necessary criteria information for the test result judgement (e.g. expected service quality or service traffic volume after the test is finished) by collecting the monitoring information around the area to be tested.

3) The Service Provider requests the NFV MANO to create and store the VNF Snapshots including the virtualised containers around the area to be tested. These snapshots are used to restore the network service if the test results fail. The VNF Snapshots may include memory image in some cases (e.g. expected recovery time is less than order of seconds) or in some types of VNFs. If memory level Snapshot is taken for a VNF, it can skip its system's booting process as well as its application's setup process as the result of the process is already in the memory. Also, it may be helpful to restore the states from the memory Snapshot especially when a number of those are stored in the memory.

NOTE 1: The VNF Snapshots include VNFD (including VL) ETSI GS NFV-IFA 011 [i.6] and VnfInfo ETSI GS NFV-IFA 007 [i.4], in addition to the snapshots of virtualised containers.

4) The Service Provider executes the test scenario (e.g. performing VM shutdown) determined in the step 1.

5) The network service reacts to the test scenario (e.g. the system detect the failure and recover from the situation by invoking the auto recovery functionality).

6) To know the test result, once the expected recovery time from the failure elapses, the service provider again gets the same information as step 2 (e.g. actual service quality at this time).

7) The Service Provider compares the information (test result) gotten at step 6 with the information (expected test result) at step 2, and if the result is as expected (e.g. the service quality was same as before), the test is terminated. Otherwise, the Service Provider requests the NFV MANO to start the new virtualised containers using the snapshots stored at step 3 and switch the (failed) virtualised containers around tested area to the new virtualised containers by the snapshots, so that the network service is restored from the failure situation, and then the test is terminated.

8) If the test results fail, the Service Provider requests the NFV-MANO to create and store the snapshots of the (failed) virtualised containers. These snapshots are used for the root cause analysis by the Service Provider and the VNF Provider(s) so to help fixing the network service.

NOTE 2: The Service Provider's behaviours described above can be programed as online testing functions which may be part of the NFV-MANO or outside of it (e.g. the OSS/BSS), depending on architectural options.

4.1.1.5 Post-conditions

If the test results in successful, the network service provides the service as per normal.

If the test results in fail, the tested area gets back to the running state before the test scenario is executed. That is, the network service is restored to its former state, and it provides the service as per normal. The snapshots of the (failed) virtualised containers are stored in the NFV MANO. These snapshots are used for the root cause analysis by the Service Provider and the VNF Provider(s) so to help fixing the network service. By continuing to test and fix the network service, the Service Provider can remove the underlying bugs from the network service, and hence they can avoid potential major service outages.

4.2 Use cases related to troubleshooting

4.2.1 VNF Snapshot for root cause analysis

4.2.1.1 Introduction

In a virtualised environment, the decoupling of software from hardware makes it difficult to collect sufficient evidence to correlate faults. During a failure situation, the Service Provider with the help of the VNF Provider can perform a root-cause-analysis, e.g. determining whether the failure was internal to the VNF or the source of the failure was external to the VNF (e.g. hypervisor or hardware) and in some cases may request a VNF/VNFC Snapshot. Activation of capturing data may depend on certain policies, e.g. it may only be triggered when the VIM has reported NFVI faults to the VNFM and VNF performance degradation has been observed.

4.2.1.2 Actors

For this use case, the following actors are involved:

1) Service Provider is informed about the availability of captured data.

4.2.1.3 Pre-conditions

1) VNF instance subject to be executed the VNF Snapshot is running.

4.2.1.4 Description

The use case begins when VNF Snapshot creation has been determined by the VNFM (either automatically or triggered by the EM) to be performed.

The following steps are executed:

1) The VNFM requests the VIM to create snapshot(s) of the VM images for a selected list of VNFC instances.
2) The snapshot(s) are created by the VIM and images of the snapshots are stored.
3) The VIM sends back to the VNFM information to identify and locate the stored snapshots.
4) The VNFM extends the VNF Snapshot(s) with information about the VNF including all necessary information for root cause analysis, e.g. VNFM logs, operational information related to that VNF instance.
5) The VNFM informs the EM about the completion of the VNF Snapshot(s) procedure including information to identify and locate the stored snapshots. If the create VNF Snapshot procedure is not successful, the VNFM informs about the failure to the EM. The EM then forwards the information about the VNF Snapshot result to the Service Provider.

4.2.1.5 Post-conditions

If the VNF Snapshot creation was successful, the Service Provider has received all data related to the VNF Snapshot (e.g. location of the VNF Snapshot and VNF). If the VNF Snapshot creation failed, the Service Provider is notified with a corresponding error message including additional information about the failure.

4.3 Use cases related to agile lifecycle management of VNF

4.3.1 VNF Snapshot during VNF lifecycle procedure

4.3.1.1 Introduction

NFV enables greater levels of automation in terms of lifecycle management of network entities, now VNF instances. To help minimizing the impact of lifecycle procedures on the service availability, mechanisms to capture data during the lifecycle procedure are needed. For instance, capturing data previous to initiating the actual VNF lifecycle procedure will help recover the VNF instance to a previous known running status in case the procedure fails. Activation of capturing data may also depend on operator policies, resource consumption, etc.; e.g. it may only be triggered by specific lifecycle procedures and critical VNFs.

This present use case shows the VNF Snapshot as part of a VNF lifecycle procedure, wherein information to the Service Provider is provided about the availability of capture data (e.g. VNF Snapshot).

4.3.1.2 Actors

For this use case, the following actors are involved:

1) Service Provider is informed about the availability of captured data.

4.3.1.3 Pre-conditions

1) VNF instance subject to be executed the VNF Snapshot is running.

4.3.1.4 Description

The use case begins when VNF Snapshot creation has been determined by the VNFM to be performed.

The following steps are executed:

1) The VNFM requests the VIM to create snapshot(s) of the VM images for a selected list of VNFC instances.
2) The snapshot(s) are created by the VIM and images of the snapshots are stored.
3) The VIM sends back to the VNFM information to identify and locate the stored snapshots.
4) The VNFM extends the VNF Snapshot(s) with information about the VNF including operational information related to that VNF instance that is necessary to fall back to a previous running status.
5) The VNFM informs lifecycle management consumers (i.e. NFVO and/or EM) about the completion of the VNF Snapshot(s) procedure including information to identify and locate the stored snapshots. If the create VNF Snapshot procedure is not successful, the VNFM informs about the failure to the consumers. Those consumers then forward the information about the VNF Snapshot result to the Service Provider.

4.3.1.5 Post-conditions

If the VNF Snapshot creation was successful, the Service Provider has received all data related to the VNF Snapshot (e.g. location of the VNF Snapshot and VNF). If the VNF Snapshot creation failed, the Service Provider is notified with a corresponding error message including additional information about the failure.

4.3.2 VNF Snapshot for quick VNF recovery

4.3.2.1 Introduction

This present use case shows how to restore a VNF instance to a previous running status using a previously captured VNF Snapshot.

4.3.2.2 Actors

For this use case, the following actors are involved:

1) Service Provider requests to revert the VNF using a previously captured VNF Snapshot.

4.3.2.3 Pre-conditions

1) VNF Snapshot is available, i.e. the VNFM or NFVO can retrieve VNF Snapshot Package information.

4.3.2.4 Description

The use case begins when the Service Provider determines to revert the VNF to a previous VNF Snapshot.

The following steps are executed:

1) The Service Provider requests the VNFM or NFVO to use the VNF Snapshot on the VNF instance. In the latter case, the NFVO identifies the VNFM that manages the VNF instance and forwards the request to this VNFM.

2) The VNFM retrieves information on how to use the VNF Snapshot on the VNF instance, this involves determining the individual VNFC Snapshots which are part of the VNF Snapshot, as well as operational information related to that VNF instance (minimally VNF instance runtime information, e.g. vnfdId, onboardedVnfPkgInfoId, vnfState and vnfConfigurableProperty ETSI GS NFV-IFA 007 [i.4]) that is necessary to revert to the VNF Snapshot.

3) The VNFM requests the VIM to execute revert to Snapshot operation on the VM(s) using the individual VNFC Snapshot(s).

4) The VIM executes revert to Snapshot operation(s) on the VM(s).

5) The VIM sends back to the VNFM information about the success of the operation(s).

6) The VNFM informs lifecycle management consumers (i.e. NFVO and/or EM) about the completion of the operation(s).

4.3.2.5 Post-conditions

If the operation was successful, the VNF instance uses the VNF Snapshot (i.e. the VNF instance has reverted its state to the one that was available at the time the VNF Snapshot was created) and the Service Provider has been notified about the successful operation.

If the operation has failed, the Service Provider is notified with a corresponding error message including additional information about the failure.

5 Gap analysis

5.1 Current supporting solutions

5.1.1 Overview

This clause aims at documenting current solutions that can support the execution of VNF/VNFC Snapshots. The analysis leverages available techniques, capabilities of implementations of virtualisation technologies (e.g. KVM/QEMU, LXC/LXD), hypervisors abstraction layers (e.g. libvirt) and virtualisation management solutions (e.g. OpenStack) that can be found in current implementations. The selection of implementations is not exclusive and should be considered as examples sufficient for analysing the current state of the supporting solutions. The analysis is based on the current available versions of the solutions (see annex A).

Figure 5.1.1-1 illustrates the analysed current solutions and their relationship to each other, including the reference points enabling intercommunication with regards to Snapshot operations.

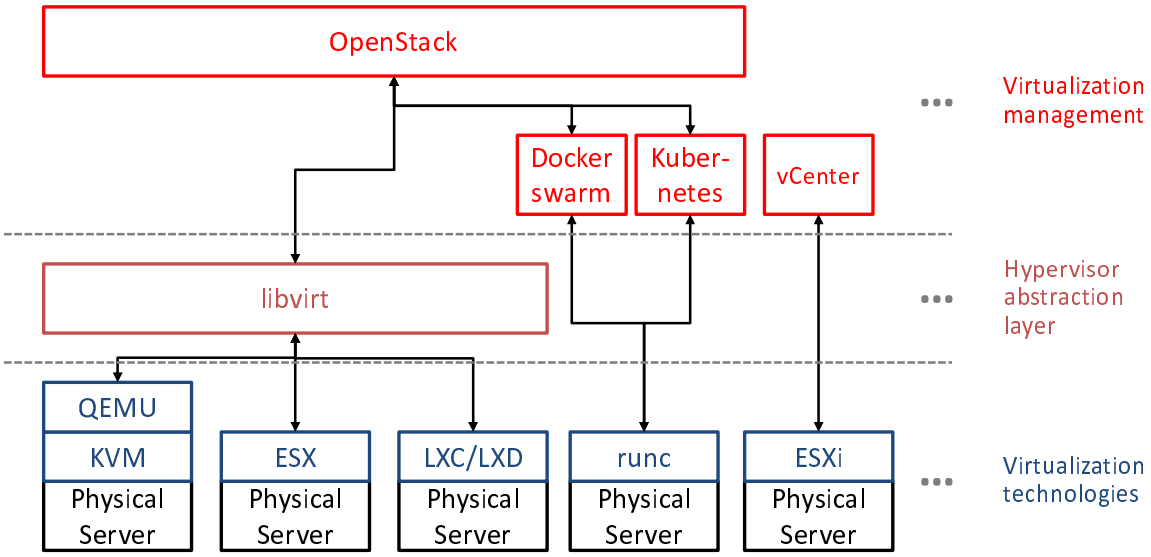

Figure 5.1.1-1: Relations and reference points of exemplary solutions

5.1.2 Snapshot techniques

The current snapshotting solutions of the virtualisation technologies are using different techniques to capture the memory state and the disk state of the instances. Their characteristics can be described as follows:

Memory state

- Internal memory snapshot: The content of the memory of the instance(s) is stored in a file and is placed in the disk image of the instance snapshot. It can only be used in combination with the Snapshot of the disk state of an instance.
- External memory snapshot: The content of the memory of the instance(s) is stored in a dedicated file, external to and independent of the Snapshot of the disk state.

Disk state

- Sequential snapshot: The content of the specified disks of the instance is copied into disk images each time an instance Snapshot is created.
- Incremental snapshot: The first time an instance Snapshot is created, the associated disks of the instance are frozen and represent the baseline Snapshot of the disk state. Additionally delta snapshots for all disks of the instance are created which contain only the changes in the disk state compared to the last snapshot. Creation of consecutive disk state snapshots results in creation of new delta disk snapshots.
- Internal disk snapshot: The same file contains the disk image Snapshot and the changes since the Snapshot creation.
- External disk snapshot: The disk image Snapshot and the changes since the Snapshot creation are stored in different files.

5.1.3 Snapshot capabilities

5.1.3.1 Introduction

The Snapshot capabilities are grouped by operations concerning Snapshot management, such as creating, listing, reverting to or deleting a snapshot. Depending on the underlying virtualisation technology, the instance being snapshotted is different and could be a virtual machine, an OS container or something similar. Each of the snapshotted instances represents a VNFC instance and therefore the resulting Snapshot equals to a VNFC Snapshot.