ETSI GS NFV-REL 004 V1.1.1 (2016-04)

Network Functions Virtualisation (NFV); Assurance; Report on Active Monitoring and Failure Detection

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
DGS/NFV-REL004

Keywords
assurance, 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

Copyright Notification

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

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**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 develops a report detailing methods for active monitoring of VNFs, NFVI and E2E network services and detection of failures. It addresses the following two aspects of active monitoring:

1) Periodic testing of VNFs and service chains in a live environment to ensure proper functionality and performance adherence to SLAs.

2) Failure prevention and detection - Active monitoring methods for failure prevention (proactive) or timely detection and recovery from failures. Failures include loss or degradation of network connectivity, loss or degradation of session capacity, loss of services, VM failures, VM stalls, etc.

The present document proposes that the monitoring agents be on boarded into the NFV environment, just like other VNFs.

2 References

2.1 Normative 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.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

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 necessary for the application of the present document.

Not applicable.

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] IETF RFC 5357: "A two-way active measurement protocol".

[i.2] Recommendation ITU-T Y.1564: "Ethernet Service Activation Test Methodologies".

[i.3] IETF RFC 2544: "Benchmarking Methodology for Network Interconnect Devices".

[i.4] IETF RFC 2681: "A Round-trip Delay Metric for IPPM".

[i.5] ETSI GS NFV-SEC 003: "Network Functions Virtualisation (NFV); NFV Security; Security and Trust Guidance".

[i.6] IETF RFC 7594: "A Framework for Large-Scale Measurement of Broadband Performance (LMAP)".

[i.7] IETF RFC 7536: "Large-Scale Broadband Measurement Use Cases".

[i.8] IETF draft-ietf-lmap-information-model-06: "Information Model for Large-Scale Measurement Platforms (LMAP)".

[i.9] Recommendation ITU-T Y.1731: "Internet protocol aspects - Quality of service and network Performance".

[i.10] ISO/IEC/IEEE 24765:2010: "Systems and software engineering - Vocabulary".

[i.11] IETF RFC 6349: "Framework for TCP Throughput Testing".

[i.12] ETSI GS NFV 003 (V1.1.1): "Network Functions Virtualisation (NFV); Terminology for Main Concepts in NFV".

[i.13] ETSI GS NFV-MAN 001: "Network Functions Virtualisation (NFV); Management and Orchestration".

[i.14] ETSI GS NFV-REL 001 (V1.0.0): "Network Functions Virtualisation (NFV); Resiliency Requirements".

[i.15] Saurabh Kumar Garg et al.: "SLA-based virtual machine management for heterogeneous workloads in a cloud datacenter", Journal of Network and Computer Applications, Vol. 45, October 2014, pp. 108-120.

[i.16] Eric Bauer, and Randee Adams: "Service Quality of Cloud-Based Applications, Wiley-IEEE Press, February 2014.

[i.17] TM Forum Cloud SLA Application Note Version 1.2 - GB963.

[i.18] TM Forum TR 178: "E2E Cloud SLA Management".

[i.19] Raimund Schatz, Tobias Hoßfeld, Lucjan Janowski, and Sebastian Egger: "From Packets to People: Quality of Experience as a New Measurement Challenge", in 'Data Traffic Monitoring and Analysis' (E. Biersack, C. Callegari, and M. Matijasevic, Eds.), Springer Lecture Notes in Computer Science, Vol. 7754, 2013.

[i.20] OPNFV Doctor project stable draft.

NOTE: Available at https://wiki.opnfv.org/display/doctor/Doctor+Home.

[i.21] Michael R. Lyu (Ed.): "Handbook of Software Reliability Engineering", IEEE Computer Society Press & McGraw-Hill, 1996.

[i.22] SNAPSHOT Draft: "NFV Quality Management Framework", April 23, 2015.

NOTE: The NFV white paper is posted on the NFV team portal on the QuEST Forum member web site/Executive Board/NFV Strategic Initiative/Files & Documents.

[i.23] D. Cotroneo, L. De Simone, A. Ken Iannillo, A. Lanzaro, and R. Natella: "Dependability Evaluation and Benchmarking of Network Function Virtualization Infrastructures", IEEE Conference on Network Softwarization, London, UK, April 2015.

[i.24] CSMIC defined measures.

NOTE: Available at http://csmic.org.

[i.25] "NIST Cloud Computing Cloud Services Description", Rev. 2.3d9.

[i.26] R. Ghosh, F. Longo, V.K. Naik, and K.S. Trivedi: "Quantifying Resiliency of IaaS Cloud", 29th IEEE International Symposium on Reliable Distributed Systems, New Delhi, Punjab, India, October-November 2010.

[i.27] J.P.G. Sterbenz, E.K. Çetinkaya, M.A. Hameed, A. Jabbar, S. Qian, J.P. Rohrer: "Evaluation of network resilience, survivability, and disruption tolerance: analysis, topology generation, simulation, and experimentation", Telecommunication Systems, Vol. 52, Issue 2, February 2013, pp. 705-736.

[i.28] ETSI GS NFV-REL 002 (V1.0.0): "Network Functions Virtualisation (NFV); Reliability; Report on Scalable Architectures for Reliability Management".

[i.29] ETSI GS NFV-REL 003: "Network Functions Virtualisation (NFV); Reliability; Report on Models and Features for E2E Reliability".

[i.30] ETSI GS NFV-SEC 008: "Security Management and Monitoring for NFV".

[i.31] ETSI GS NFV-REL 005 (V1.1.1): "Network Functions Virtualisation (NFV); Accountability; Report on Quality Accountability Framework".

[i.32] IETF draft-browne-sfc-nsh-timestamp-00: "Network Service Header Timestamping".

NOTE: Available at https://tools.ietf.org/html/draft-browne-sfc-nsh-timestamp-00.

[i.33] IETF draft-irtf-nfvrg-resource-management-service-chain-02: "Resource Management in Service Chaining".

NOTE: Available at https://tools.ietf.org/html/draft-irtf-nfvrg-resource-management-service-chain-02.

[i.34] Mark Sylor: "Testing the Cloud," EXFO White Paper 023, 2012.

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in ETSI GS NFV-REL 001 [i.14], ETSI GS NFV 003 [i.12] and the following apply:

failure: termination of the ability of a product to perform a required function or its inability to perform within previously specified limits or an event in which a system or system component does not perform a required function within specified limits

NOTE: As defined in ISO/IEC/IEEE 24765:2010 [i.10].

FaultLoad: set of faults to inject in the NFVI for resiliency evaluation

NOTE: As defined in **[**i.23**]**.

frame loss ratio: ratio, expressed as a percentage, of the number of service frames not delivered divided by the total number of service frames during a time interval T, where the number of service frames not delivered is the difference between the number of service frames arriving at the ingress ETH flow point and the number of service frames delivered at the egress ETH flow point in a point-to-point ETH connection

NOTE: As defined in Recommendation ITU-T Y.1731 [i.9].

frame delay: round-trip delay for a frame, where frame delay is defined as the time elapsed since the start of transmission of the first bit of the frame by a source node until the reception of the last bit of the loop backed frame by the same source node, when the loopback is performed at the frame's destination node

NOTE: As defined in Recommendation ITU-T Y.1731 [i.9].

frame delay variation: measure of the variations in the frame delay between a pair of service frames, where the service frames belong to the same CoS instance on a point-to-point ETH connection

NOTE: As defined in Recommendation ITU-T Y.1731 [i.9].

Test Controller: management module responsible for management of the test agents/probes

NOTE 1: Provides test instructions to the test probes.

NOTE 2: Co-ordinates the test scheduling when multiple tests with large number of test probes are executed.

NOTE 3: Retrieves results from the results analysis engine to provide actionable information to the network operator via NFVO. In this case result reporting to OSS/BSS via NFVO has been used as a deployment option to keep a single interface for communication between Test Controller and MANO. This keeps the changes required to interfaces of the MANO components to minimum and minimizes the effort for Active monitoring System integration with NFV framework.

Test Results Analysis Module (TRAM): integral part of the active monitoring framework that collects or receives test results from the VTAs, NFVI resource statistics and alarms from VIM and analyses test results and presents it to Test Controller, NFVO or other management entities in an actionable format

throughput: maximum rate at which no frame is dropped. This is typically measured under test conditions

NOTE: As defined in IETF RFC 2544 [i.3].

Virtual Test Agent (VTA): VNF for active monitoring probe capable of sending and analysing control plane and data plane testing

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI GS NFV 003 [i.12] and the following apply:

BSS	Business Support Systems
CBS	Constant Bit Rate
CCDF	Complementary Cumulative Distribution Function
CiGoodput	Cloud infrastructure Goodput
CiQoE	Cloud infrastructure Quality of Experience
CiR	Cloud infrastructure Reliability
CoS	Class of Service
DPI	Deep Packet Inspection
DUT	Device Under Test
EBS	Excess Burst Size
EIR	Excess Information Rate
IETF	Internet Engineering Task Force
IPPM	IP Performance Metrics
LMAP	Large scale Measurement of Broadband Performance
NFF	No Fault Found
OSS	Operations Support Systems
PoP	Point of Presence
PPB	Parts Per Billion
PTP	Precision Time Protocol
NTP	Network Time Protocol
NSR	Network Service Record
QoE	Quality of Experience
QoS	Quality of Service
SLA	Service Level Agreement
SPC	Statistical Process Control
TCO	Total Cost of Ownership
TRAM	Test Results Analysis Module
VLR	Virtual Link Record
VNFR	Virtual Network Function Record
VTA	Virtual Test Agent

4 Active Monitoring in traditional networks

In general the 3 stages of service lifecycle are addressed in the present document:

1) Service activation - whereby a service or VNF is deployed and verified that the service is running as expected.

2) Service monitoring - where the resource usage by a service is monitored and management components are alerted upon KPI violation.

3) Service debug - where troubleshooting probes and tools to ascertain the root cause of a service failure are used.

Live testing typically involves end-to-end testing of services versus single node testing where the testing can be performed at the pre-activation, or post-activation, of services. Three key components of a test system in live networks are:

1) Test Controller;

2) results analysis module; and

3) test agent.

In non-NFV network deployments, the testing agents are typically deployed in the long-term as long as the testing or monitoring PoP does not change. Test Controller and results analysis module can be part of the OSS/BSS system or can be a standalone application in the same administration domain as the OSS/BSS system. Figure 1 illustrates a generic active monitoring deployment scenario.

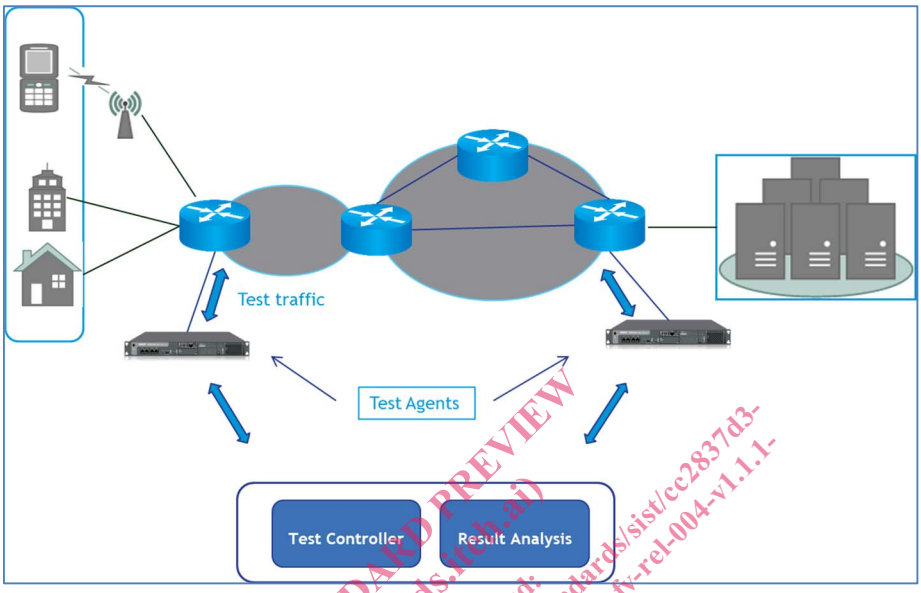

Figure 1: Live network testing in non-NFV networks

Network monitoring methods can be categorized into active, passive or hybrid modes.

- Active may operate in two modes:
  - Test mode involves sending test traffic (based on an OAM protocol such as Recommendation ITU-T Y.1731 [i.9] or alternative) into the network to validate the services and applications performance, SLAs and to perform fault isolation.
  - Subscriber mode involves marking subscriber traffic user plane headers in a way such that QoE for subscribers may be derived accurately as flows traverse the network.
- Passive mode testing involves observing the user traffic, providing an analysis based on this untampered traffic and raising alarms if pre-set thresholds are crossed.
- Hybrid mode approach, as the name suggests, uses the information obtained from both active and passive approaches.

5 Impact of NFV on active monitoring

NFV increases the variability in the network topology imposing additional requirements on the active monitoring framework. The active monitoring solution should be able to deal with NFV aspects such as VNF migration, auto-scaling and multi-tenancy of VNFs in order to be effective in a NFV environment.

Note that there has been extensive work done which defines a similar framework as defined in the present document for performance measurement in a traditional broadband network. The IETF Large-scale Measurement has defined a framework for communication between LMAP Controller functions, LMAP Measurement Agents, and LMAP Collector functions in IETF RFC 7594 [i.6]. The LMAP Measurement Agent is similar to the VTA in role and function, but leaving the specifics of active measurement to other protocols and functions (e.g. the IETF IPPM working group supplies these metrics and protocols). Once the functions and agents are deployed, the LMAP specifications will provide a standard Information model, a YANG Data model, and a RESTCONF communications protocol.

Multi-tenancy of VNFs on the same host introduces network visibility challenges when using traditional physical probes for monitoring within VNF service chains. Additionally, VNF migration may result in modification of point of presence for active monitoring. This presents a challenge of how to maintain the POP without changing the physical connections for the probes.

In the case where VNFs are so critical that they are protected in a 1+1 scenario and affinity rules specify that the active and standby VNFs are placed in different NFVI-PoPs, there is also an implication during VNF 1+1 protection switches. In such scenarios Test Controller should be notified of the VNF protection switch and the protection switch should take into account the NFVI resources required for the VTA on the protection path. Figure 2 shows such a scenario where EPC site 1 and EPC site 2 represents a 1+1 protection scenario.

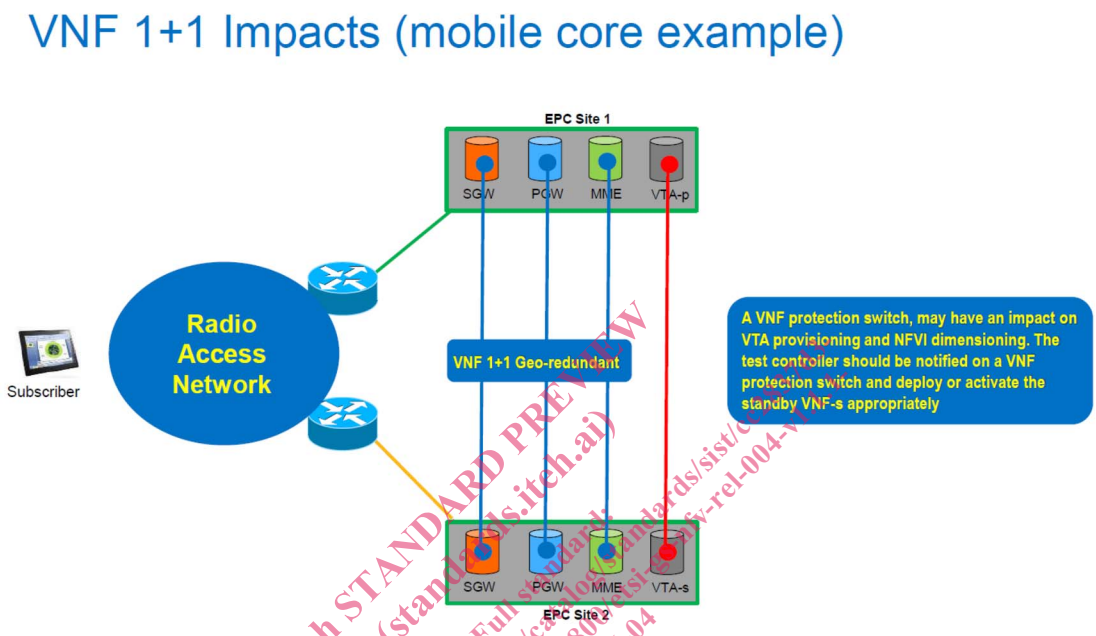

Figure 2: VNF 1+1 impacts

Although LMAP framework provides a comprehensive details for large scale measurement for broadband networks it does not address the challenges applicable to the NFV environment. The present document presents an active monitoring framework to address these challenges. It is the intent of the present document to present the NFV active monitoring framework at a level that is not prescriptive. Although it does not preclude any future normative work to detail the operation of the framework to the level as described in LMAP framework for broadband networks.

6 Proposed Active Monitoring Framework for NFV

6.0 Introduction

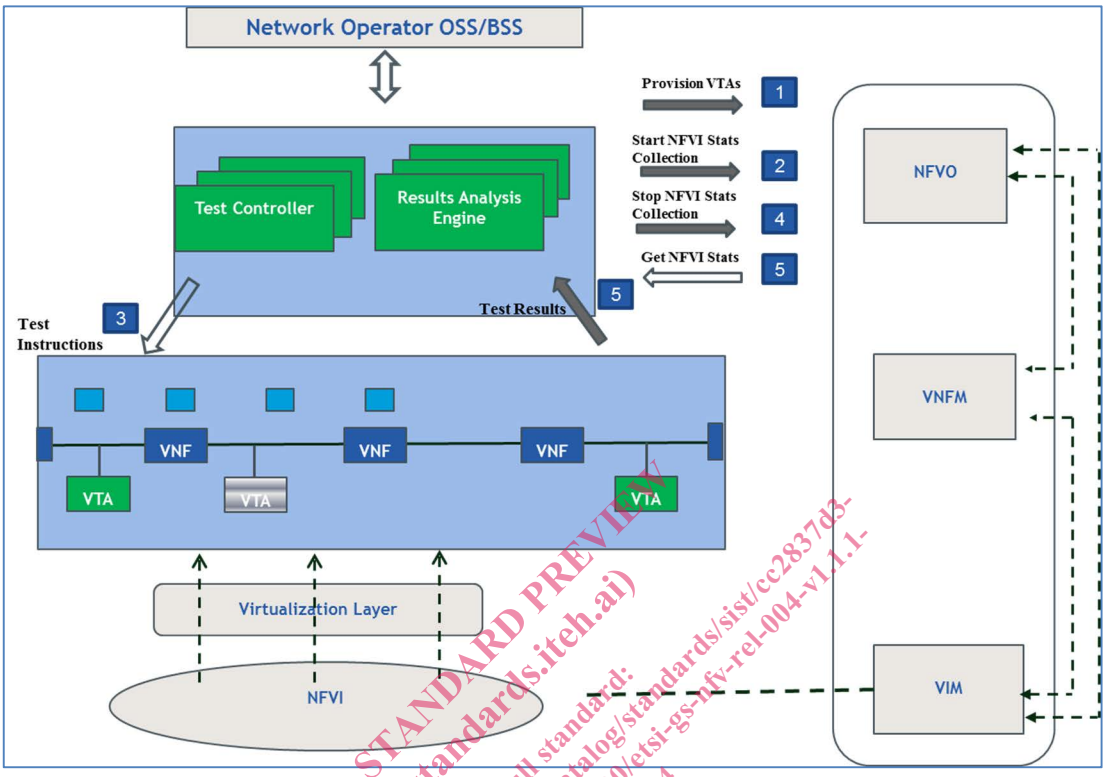

Figure 3: Active Monitoring Framework

The active monitoring framework for NFV networks proposed in the present document as shown in figure 3 consists of three core modules:

- Test Controller.
- Virtual Test Agent (VTA).
- Test Result Analysis Module (TRAM).

The clauses 6.1 to 6.3 describe the roles and responsibilities of these three modules. Additionally, clause 6.4 describes the workflow definition and message exchange between these modules in detail.

6.1 Roles and responsibilities for a virtual test agent

Network visibility and fault diagnostic capability in an NFV network is limited when using physical active test agents. With physical test agents/probes, it may not be possible to maintain the monitoring PoP. In order to provide increased visibility and better fault diagnostic in an NFV based network, the test agent needs to be a virtual entity. A virtual test agent provides the advantage of ability to reside between the VNFs in a service chain and automatically re-provision to maintain the monitoring PoP in a VNF migration scenario.

For an effective active monitoring solution in a NFV environment following are the requirements for a test agent:

- Test agent should be virtual and should be able to instantiate as a Test VNF using the VNF instantiation workflow recommended in [i.15].
- Test agent should be able to re-provision or move if the monitoring PoP is moved as a result of VNF migration.
- Test agent should be able to re-provision or move if the monitoring PoP is moved as a result of service chain migration.

- Test agent should have minimal impact on the performance of the VNFs that reside on the same server as the test agent. The ideal state of 100 % performance isolation should be the goal when implementation of a virtual test agent. This is particularly applicable for deployment scenario where VTA is residing on the same server/host as other VNFs that are part of the service chain under test. For other deployment scenarios where VTA is deployed out of band on separate server/host performance isolation may not be an issue.

- A repository of test agents with specific test features and performance capabilities may exist. Targeted test agents will make the test agents lightweight and help with achieving higher performance and minimizing the performance impact on other VNFs that reside on the same physical server.

- Test VNFD (see clause A.3.1 for details) may be defined for specifying test capability parameters in addition to the standard VNFD parameters.

- Periodic Keepalive messages between VTA and Test Controller may be implemented for fast failure detection and high availability.

- Test agent may provide failure and logging messages if the measurement task was not run to completion:

  - Although Test Controller tracks the resource utilization of the VTAs, performance isolation issues or changes in the resource provisioning may result in the test agent's inability to run the desired test. In such a scenario VTA, should send a failure or error message to the Test Controller.

  - If VTA is not able to report the results to TRAM, then it should send a failure message to the Test Controller indicating the reason.

  - Logging messages should be provided events such as start of test execution, any exceptions or signposts reached during the test execution and end of test execution results reporting events such as results logged into result database or results sent to specified TRAM or results received by TRAM may be logged as well. Such logging information is useful for debugging purposes.

- A VTA should perform the following pre-checks before it starts sending test traffic:

  - A test would need to send high throughput traffic on the same path as the service under test. In this scenario, VTA should ensure that there is not too much user traffic on the path before it begins transmitting. It is partly the network operator's responsibility to schedule such tests at a time so that end user service experience is not impacted.

  - There should be a mechanism to differentiate between test and end user data such that test traffic does not use the service quota allocated to the user.

  - VTA is able to communicate with TRAM.

- Primary Test Controller failure:

  - Additional Test Controller may be configured as a back up to provide high availability.

  - If a backup Test Controller exists, VTA's VNFR (VNF Record) should contain the backup Test Controller's ID.

  - If the Test Controller timeout timer expires, VTA should establish a session with the backup Test Controller using the backup controller ID in the VNFR.

  - Primary and back up Test Controllers should be synchronized periodically in terms of information on supported VTAs, test instructions for tests under execution and the information on periodically scheduled tests.

  - Once the backup Test Controller takes over, it should also establish communication with the NFVO and any other management entities wishing to avail of the test subsystem.

6.2 Roles and responsibilities for a Test Controller

- Maintain test agent VNFR catalogue.

- Track active tests, resource utilization taking into account the tests that are scheduled to run periodically.