Dependability of the NFV Orchestrator: State of the Art and Research Challenges

Deeksha Mysore Ramesh

November 9, 2018

Abstract

This is a report of the paper - Dependability of NFV Orchestrator: State of the Art and Research challenges, which briefs about the dependability challenges of the NFVO and also the scope for further research regarding the same.

1 Introduction

Network function virtualisation (NFV) is a model consisting of different network elements which can be programmable, having a centralised control system yielding to a better cost-efficient services and utilisation of resources. The primary component of such an architecture is Network Function Virtualisation Orchestrator (NFVO) which maintains a global view of the logically centralised network and its services. So, it is important to know the dependency factors and effects of such a network during its misoperation. The objective of this paper is to identify the dependability challenges, the state of the art of NFVO, and highlight the issues that needed to be addressed to make NFV dependable[3].

2 NFV-MANO Concepts and Definitions

- **NFV Generic Architecture**: According to the architecture proposed by ETSI, NFV has the hardware resources at their basic end constituting storage, network and computing. The virtualisation layer aggregates these hardware resources to its corresponding virtualised resources, forming a NFV Infrastructure(NFVI) subsystem. The VNF is the software implementation of the network functions that are decoupled from the hardware resources they use[3]. These are in turn locally managed by Element Management System(EMS) and globally by VNF Manager (VNFM).Dynamic management of this network is represented by NFV Management and Orchestration (NFV MANO).

- **MANO Components**: Its main components include NFVO,VNFM and VIM. NFVO manages the lifecycle of the Network Services (NSs). The VNFM coordinates the configuration between Virtualised Infrastructure Manager(VIM) and EMS. The VIM manages the NFVI by assigning the virtual resources needed.

- **Dependability Taxonomy[3]**: The parameters can be classified as below -
  - Based on its attributes : Availability ,Partial availability , Reliability,Survivability and Maintainability
  - Based on threats: Fault,Error and Failure.
  - Based on faults: Physical faults, Transient faults, Intermittent faults , Design faults, operational faults, excessive load, malicious attack.
  - Failure Semantics: Omission failure, value failure, Timing failure, Arbitrary failure.
  - Recovery: Repair and Replacement.

3 NFV Dependability Challenges:

- **Strength and vulnerabilities of NFV**: The network functions presently are vendor-specific implementations with dedicated hardware resources, whereas in virtualised network, the network elements are controlled and managed centrally, which can inturn handle faults effectively without any manual intervention. Also, the VNF can be restarted in another virtual machine with minor delay[3]. In an NFVI system, as it is centralised, it is more vulnerable to errors between software elements, giving way to network outages.

  The architecture's flexibility and adaptivity increases its complexity and also its chances of faulty design, implementation and configuration. This distributed network should have a crash failure semantics.

- **Depends-on relations of the NFV architecture**: The depends-upon graphs[2] are useful means to study relationships between functional elements to understand how failure semantics and fault tolerance may be built into the system while providing end-to -end services[3]. It reveals the structural relations between functions. The objective of such graph is to discuss fault tolerance provisioning. This graph splits the network into two domains - network domain, compute and store domain. It depicts the dependencies of network elements with each other.

4 Monitoring and Failure Recovery:

- **Monitoring**: There are many monitoring factors to be considered for the design of a orchestrator solution. The ways for monitoring can be classified on how different agents request and gather information – i.e., passive or active. In Passive monitoring, the monitoring server collects the unmodified data as it is reported by the agents allocated on the monitored elements[3]. Active monitoring proactively waits to gather information from the monitoring server enabling the fault detection. It also performs autonomous tasks that requires tests for any specific monitoring situation.

The second way of monitoring differs if the system is centralised or distributed. In centralised systems , the monitoring tasks are carried out by a single unit. The advantage of such a method is , the behaviour is coordinated by a single entity which maintains a complete view of the current state of the monitored system[3].In distributed monitoring, the components monitor their own operation.

Finally , monitoring the components below and above the virtualisation layer also differ from each other. The low-level monitoring focuses on availability and performance of the physical components of the entire infrastructure such as servers ,storage arrays, and network equipment[3]. The functionality and resources delivered by physical devices are aggregated and managed on higher levels[3].

- **Failure Recovery**: In NFV , the recovery can be either local recovery or global recovery. Local recovery requires short recovery time and is usually performed by pre-planned mechanisms of EMS. Two common techniques in this are active hot replication –each process is performed at the same time on every replica which is actively running, or passive hot replication – each requests are to be processed on a single replica before the results are transferred[3].

  Whereas , in global recovery – a global entity in charge of the recovery procedures allows centralised coordination for identification of the system-wide optimal solutions , helping in troubleshooting[3].

  Redundancy planning is a methodology for recovery of VNFs. It works on two kinds of scenarios – Active-Standby and Active-Active . Active-Standby redundancy reduces corrected failures and standby and active instances are worked upon. In Active-Active redundancy schemes , the load distribution functions are required to work upon pool of active resources.

5 Impact of NFVO on NS Dependability:

- **Dependancy of NS on the NFVO**: During the downtime of NFVO , the deployed VNFs and NSs are also affected. So it calls for a design where NFVO and the managed targets should be present in two different domains. The failure of NFVO for a longer period , effects the NFV system to not be able to handle the load inturn leading to poor orchestrations and no services[3].

- **Dependability threats and challenges**: The mentioned are the some of the threats that needed to be addressed : Monitoring all components and system layers,Failure Management,Management of stateful NSs and VNFs,Interaction with heterogeneous VIMs,Correctness of Orchestration operations[3].

6 Fault tolerant NFVO

A robust with fault tolerant NFVO has to be planned. One of the solutions for the same is introducing redundant controllers that work incase of failures[1]. These controllers have a dynamic system which affects the performance and consistency of the same[3].

7 Conclusion

The conclusion for this report will be the summary of challenges for dependability on NFV Orchestrator - Lack of research on the dependability of NFV-based services[3], A Well defined fault tolerant and fault management system is required, Dependability on MANO has to be considered as a significant domain along with NFVO.Also, Handling and preventing failures are more focused upon.

References

[1] Fábio Botelho, Alysson Bessani, Fernando Ramos, and Paulo Ferreira. Smartlight: A practical fault-tolerant sdn controller. *arXiv preprint arXiv:1407.6062*, 2014.

[2] Flavin Cristian. Understanding fault-tolerant distributed systems. *Communications of the ACM*, 34(2):56–78, 1991.

[3] Andres J Gonzalez, Gianfranco Nencioni, Andrzej Kamisiński, Bjarne E Helvik, and Poul E Heegaard. Dependability of the nfv orchestrator: State of the art and research challenges. *IEEE Communications Surveys & Tutorials*, 2018.