IEEE COMMUNICATIONS SOCIETY

STUDY GROUP
FOR
SECURITY, RELIABILITY, AND PERFORMANCE
FOR SOFTWARE DEFINED AND VIRTUALIZED ECOSYSTEMS
(SRPSDVE)

Highlights from the ETSI GS NFV-REL 001 Document and Possible Options/Approaches

December 8, 2014

Spilios Makris , PhD, CBCP
Palindrome Technologies

Outline

- Differentiators between the IT/Virtualized & Network Domains
  1. Level of Service Continuity Required
  2. Level of Resilience
  3. Automated Recovery from Failures
  4. Single Point of Failure (SPOF)
  5. Multi-vendor Environment
- Gaps for Standardization in SDN/NFV Reliability
- Q&A

Differentiators between the IT/Virtualized and the Network Domains - 1

1. Level of Service Continuity Required

- Duration of outages
  - Seconds vs. milliseconds
  - Retries (“re-boot”) vs. automatic recovery
- Customer expectation (e.g., market dynamics) vs. regulatory requirement (e.g., critical services)
- Impact of service outages (e.g., number of users, certain geography)
- Multiple service availability classes (e.g., 911 calls, voice, text/SMS, video)

Possible Options/Approaches

- Clash of the “IT and Net cultures” based on “bottom line” (cost)
- “At least as good as current service offerings…(e.g., QoS, availability, etc.)”
- “Customer-perceived reliability (or Quality of Experience)” vs. “network/service-based metrics”

Differentiators between the IT/Virtualized and the Network Domains - 2

2. Level of Resilience

- Hardware-centric vs. Network Function (i.e., software) driven
  - Network Reference Architectures ("cut through" path) vs. virtualized environment
  - "Design for uptime" vs. "Design for failure"
  - Availability of single nodes for Physical Network Functions (PNF) vs. end-to-end service availability
  - Node resilience (e.g., dual core) vs. hardware redundancy implicitly available on infrastructure level

Possible Options/Approaches

- Standardize software-reliability modeling as it was done for hardware-reliability modeling (e.g., Markov modeling)
- Limit potential failure impacts (e.g., number of parallel users allowed, parallel transactions to be handled, etc.)
- Support capacity limitations per instance as part of the deployment instructions of a Virtualized Network Function (VNF)

Differentiators between the IT/Virtualized and the Network Domains - 3

3. Automated Recovery from Failures

- "Hardware recovery in milliseconds " vs. "Hardware availability is not critical within a VNFI since hardware is always regarded as pool of resources"
- "Hardware recovery via system/component –level redundancy" vs. "Scalable NFVI supporting thousands of VMs with a high degree of process automation"

Possible Options/Approaches

- Hardware repair should be treated as a scheduled maintenance activity rather than a emergency action
- Seamless re-assignment of NFV resources to ensure service continuity in the NFV

Differentiators between the IT/Virtualized and the Network Domains - 4

4. Single Point of Failure (SPOF)

- "Hardware (even with duplicated components within a node) is a potential SPOF in a conventional PNF" vs. "Dynamic allocation of highly standardized resources (processing, storage, connectivity) to remove SPOFs by design"
- Switches (except in dual-homing cases) are considered SPOFs" vs. "NFV framework tools like hypervisors or NFV M&O functions may become SPOFs"

Possible Options/Approaches

- Hierarchical structure of resilience measures (e.g., the risk of failure for a certain type of hypervisor may be mitigated by separating the NFVI into several blocks of resources managed by different types of hypervisors)
- The orchestration software can re-assign virtual machines (VMs) to a different block in case of a hypervisor failure
- Tools required during VNF runtime shall be designed not to become a SPOF

Differentiators between the IT/Virtualized and the Network Domains - 5

5. Multi-vendor Environment

- "Established, global vendor to ensure interoperability" vs. "all resiliency mechanisms shall be provided for a multi-vendor environment, where NFVI, NFV M&O, and VNFs may be supplied by different vendors"

Possible Options/Approaches

- None of the resilience mechanisms shall make implicit assumptions on the behavior of each other
- The VNF selects the information to be stored and the NFVI provides the bare object store for any kind of state information to be stored

Differentiators between the IT/Virtualized and the Network Domains - 6

5. Hybrid Infrastructure

- "Only physical implementation of a network function (NF)" vs. "Co-existence of VNFs with physical implementations of the same NF"

Possible Options/Approaches

- Geographic redundancy across virtualized and physical implementations
- The combination of VNFs is simply to be regarded as external legacy platform, behaving to the other legacy platforms just as it would have be one of them

ETSI NFV Phase 2
Objectives and Scope

- Objectives and Scope
  - Grow an interoperable NFV Ecosystem
  - Specify reference points and requirements defined in Phase 1
  - Further grow industry engagement to ensure that NFV requirements are satisfied
  - Clarify how NFV intersects with SDN and related standards, industry, and open source initiatives
- Focus of new ETSI NFV Working Group structure
  - Less on requirements and more on adoption

Source: "ETSI Network Function Virtualization enters Phase 2"
http://www.etsi.org/index.php/news-events/news/850-2014-12-news-etsi-network-function-virtualization-enters-phase-2

IEEE COMMUNICATIONS SOCIETY

*Source: Mohammad Asad Chaudhry, SRPSDVE Study Group Vice Chair, Univ. of Toronto

IEEE

ETSI NFV Phase 2

Key Areas that will be Addressed

- Stability, Interoperability, Reliability, Availability, Maintainability
- Intensified collaboration with other bodies
- Testing and validation to encourage interoperability & solidify implementations
- Definition of interfaces
- Establishment of a vibrant NFV ecosystem
- Performance and assurance considerations
- Security

Source: "ETSI Network Function Virtualization enters Phase 2"
http://www.etsi.org/index.php/news-events/news/850-2014-12-news-etsi-network-function-virtualization-enters-phase-2

IEEE COMMUNICATIONS SOCIETY

*Source: Mohammad Asad Chaudhry, SRPSDVE Study Group Vice Chair, Univ. of Toronto

IEEE

ETSI NFV Phase 2

Approved New Working Group Structure

- IFA: Interface and Architecture
- TST: Test
- EVE: Ecosystem
- REL: Reliability
- SEC: Security

Source: "ETSI Network Function Virtualization enters Phase 2"
http://www.etsi.org/index.php/news-events/news/850-2014-12-news-etsi-network-function-virtualization-enters-phase-2

IEEE COMMUNICATIONS SOCIETY

*Source: Mohammad Asad Chaudhry, SRPSDVE Study Group Vice Chair, Univ. of Toronto

IEEE

SDN/NFV: Gaps for Standardization* - 1

Examples of where standardization in SDN/NFV Reliability is required

- Level of Resilience
  - N+1, or N+x
- Five 9's vs. Three 9's
  - Cost vs. Need for Reliability
- Use Cases
  - Data Center vs. Mobile
- Key Performance Indicators (KPIs)
- Hot Swap
  - E.g., Protocol for Hot Swap of two SDN Controllers
- Balance in Provision of Reliability
  - Hardware vs. Software
- Layered vs. Cross-layered

IEEE COMMUNICATIONS SOCIETY

*Source: Mohammad Asad Chaudhry, SRPSDVE Study Group Vice Chair, Univ. of Toronto

IEEE

SDN/NFV: Gaps for Standardization* - 2

Examples of where standardization in SDN/NFV Reliability is required

- User experience ought to remain the same regardless of the type of infrastructure being used to deliver service
- Can the industry implement standard requirements for service reliability attributes?
  - Accessibility
  - Continuity
  - Release
- Promulgate standard reliability models for SDN/NFV architectures
  - Stochastic Petri net models
    - Failovers
    - Timing
- Establish explicit, quantitative links between service reliability attributes and reliability/behavior of SDN/NFV infrastructures

IEEE COMMUNICATIONS SOCIETY

*Source: Mike Tortorella, Rutgers University

IEEE