MEETING THE SERVICE ASSURANCE CHALLENGE TO NFV (PART 1)

Virtualizing and Automating the Network
NFV Changes the Game for Service Assurance
Service Assurance Today: FCAPS
Components Enabling “Open” Service Assurance
Summary

Where to Get More Information
Intel® Network Builders – NFV Service Assurance

networkbuilders.intel.com/network-technologies/serviceassurance
Network transformation starts today

2+ ZB global data traffic annually by 2020

5G

50B connected devices by 2020

Virtualized software defined cloud enabled

Transforming architecture
Value chain
Service delivery

Agility + scale on IA

VIRTUALIZING AND AUTOMATING THE NETWORK

DRIVING NETWORK SCALE AND AGILITY

Yesterday:
Purpose-Built

Siloed Management Consoles

Management Router
Management VPN
Management Firewall

TRANSFORMING:
ARCHITECTURE
VALUE CHAIN
BUSINESS
PROCESS

Infrastructure Wide Orchestration

SDN: Unified Management and Control

Virtual Router
Virtual VPN
Virtual Firewall

Tomorrow:
Add NFV and SDN
NFV changes the game for service assurance

Virtual systems as peer to traditional physical network infrastructure

**Pre-NFV Service Assurance**
- Traditional equipment hand-crafted into tightly integrated vertical stacks
- Platform, Management and Operations
- Physical equipment, networking software, resiliency solutions, service assurance solutions and management systems delivered as solution

**The Impact of Network Transformation**
- Agility and efficiency through a common playing field for application solution vendors using a common, standardized and open platform
- NFV transforms the traditional vertically integrated stack and SDN adds challenge of dynamically provisioned service chains

**Open NFV Platform and Service Assurance**
- Service assurance components must transform into common open standard components and interfaces
- Must integrate with both traditional management systems and next generation open management systems
SERVICE ASSURANCE CAPABILITY REQUIREMENTS: INDUSTRY FEEDBACK

UK CoSP
“Can we measure the resource utilisation (per VNF type) at various throughputs and configurations to build a model of how real VNFs use CPU resources (or has this already been done)?”

Global Service Assurance ISV
“Service Assurance is critical. Data collection from both physical and virtualised network equipment, directly through SNMP and/or standard APIs”

EMEA TEM
“Automation, network agility and service agility are the corner stones of NFV and SDN. This is one of the key areas where service assurance plays a vital role. Service assurance, network analytics will play a key role by providing proactive and predictive actionable intelligence.”

EMEA/LAR CoSP
“One of the topics that is delaying UNICA final technical acceptance by TEF ………TEF main concern is about making sure that, if VNF has an issue, other VNFs running in the same servers are not compromised.”
# Service Assurance Today: FCAPS

"Service Assurance" = FCAPS

<table>
<thead>
<tr>
<th>Fault</th>
<th>Configuration</th>
<th>Accounting</th>
<th>Performance</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify component or service failures in the network</td>
<td>Setting up or managing the many systems that comprise the network</td>
<td>Monitoring data flows for billing, chargeback</td>
<td>Measuring data flows and usages for trending, management and analysis</td>
<td>Controlling the access and use of network resources</td>
</tr>
</tbody>
</table>

Scores of tools are used to collect, report FCAPS data, for graphing and trending.

- Thresholds, baselines and watermarks are established and used to decide when to actions are required
- Entire system is used for tracking end-end network service levels and conformance to subscribed service levels

---

FCAPS is the operational scope of Service Assurance, Foundation for SLAs
Components enabling “Open” Service Assurance

All layers of the stack must be enabled to instantiate service assurance

Addressing the service assurance barrier in the path to adoption of NFV and virtualized services requires enhancements in:

- NFV Base Platform
- Physical, presentation, collector and monitoring systems (virtual via libvirt)
- Management / Service Assurance / Orchestration layers

Source: Derived from ETSI model
PLATFORM SA HARDWARE FEATURES - OPEN I/F

Monitoring/Analytics Systems

Common / Open APIs

NFVI

E.g. Working/Protect Failover

Vendor SA Middleware

Fast Path Triggers

Monitoring/Analytics Systems

Slow Path

Standard Open APIs

Intel Components

Virtualised Compute

Virtualised Network

Virtualised Storage

Hypervisor

[RT/SA KVM4NFV extensions]

Local Corrective Action

Vendor SA Middleware

Includes NetFlow Collectors

Monitoring/Analytics Systems

Common / Open APIs

NFVI

Slow Path

Standard Open APIs

Intel Components

Virtualised Compute

Virtualised Network

Virtualised Storage

Hypervisor

[RT/SA KVM4NFV extensions]

Local Corrective Action

Vendor SA Middleware

Includes NetFlow Collectors

Monitoring/Analytics Systems

Common / Open APIs

NFVI

Slow Path

Standard Open APIs

Intel Components

Virtualised Compute

Virtualised Network

Virtualised Storage

Hypervisor

[RT/SA KVM4NFV extensions]

Local Corrective Action

Vendor SA Middleware

Includes NetFlow Collectors

Monitoring/Analytics Systems

Common / Open APIs

NFVI

Slow Path

Standard Open APIs

Intel Components

Virtualised Compute

Virtualised Network

Virtualised Storage

Hypervisor

[RT/SA KVM4NFV extensions]
Intel server platforms provide a rich and growing set of data and control points that can be used for configuration, reporting, monitoring and managing workloads and data:

If you can't measure and control the underlying platform resources, it is hard to measure, monitor and guarantee services running on that infrastructure.
EXAMPLE: PERFORMANCE MANAGEMENT
TRADITIONAL AND MANO ORIENTED MODELS CAN BENEFIT AND COEXIST

1. Cache Utilization rates for workloads captured by Intel performance monitoring counter (PCM)
   - Intel Infrastructure Management Technology
     - Resilient System Technologies
     - Resilient Memory Technologies
     - Compute
     - Network
     - Storage
     - Standard OS Telemetry
     - Open Virtual Switching
     - Standard Driver Interfaces

2. Utilization data collected through plug-in
   - open telemetry framework
   - sFlow
   - IPFIX
   - REST APIs

3. Utilization data passed to MANO system via Ceilometer (Gnocchi and AODH) and OpenStack
   - Ceilometer (Gnocchi and AODH)

4. MANO policy indicates workload priorities—directs relocation of “noisy Neighbor” workload
   - openstack
   - Ceilometer

Admin decides if actions are required or automated action triggered

Utilization data passed to Network Mgmt system via SNMP
ENGAGING COMMUNITIES AND STANDARDS FOR SERVICE ASSURANCE SOLUTIONS
A BROAD ECOSYSTEM IS ENGAGING TO ADDRESS THE SERVICE ASSURANCE CHALLENGE


NFV Management and Orchestration (MANO)

VNFs

NFVi

KVM | OPEN CONTAINER INITIATIVE | Xen

A BROAD ECOSYSTEM IS ENGAGING TO ADDRESS THE SERVICE ASSURANCE CHALLENGE
MACHINE LEARNING WILL COMPLETE THE EVOLUTION
MOVING FROM AUTOMATION TO SELF-OPTIMIZATION

Watch
Expose Platform and App data through APIs

Decide
Analytics to define correct response

Act
Mechanism for Policy Activation and Enforcement

Learn
Machine Learning for continuous improvement
Service Assurance capabilities are essential for realizing the full benefits of SDN/NFV

Provide SDN and NFV solutions that *fit in and interoperate*

Using Xeon processor platform capabilities and functions we are now able to monitor and manage NFV platforms, workloads and services

Engage with Intel to enable these features to unlock more value with new use models along with integration with MANO and Service Assurance frameworks

GAIN BUSINESS AGILITY BY ADOPTING SDN AND NFV
NOTICE AND DISCLAIMERS

• Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Performance varies depending on system configuration. No computer system can be absolutely secure. Check with your system manufacturer or retailer or learn more at intel.com.

• Tests document performance of components on a particular test, in specific systems. Differences in hardware, software, or configuration will affect actual performance. Consult other sources of information to evaluate performance as you consider your purchase. For more complete information about performance and benchmark results, visit http://www.intel.com/performance.

• Software and workloads used in performance tests may have been optimized for performance only on Intel microprocessors. Performance tests, such as SYSmark and MobileMark, are measured using specific computer systems, components, software, operations and functions. Any change to any of those factors may cause the results to vary. You should consult other information and performance tests to assist you in fully evaluating your contemplated purchases, including the performance of that product when combined with other products. For more complete information visit http://www.intel.com/performance.

• Cost reduction scenarios described are intended as examples of how a given Intel-based product, in the specified circumstances and configurations, may affect future costs and provide cost savings. Circumstances will vary. Intel does not guarantee any costs or cost reduction.

• No license (express or implied, by estoppel or otherwise) to any intellectual property rights is granted by this document.

• Intel does not control or audit third-party benchmark data or the web sites referenced in this document. You should visit the referenced web site and confirm whether referenced data are accurate.

• © 2017 Intel Corporation. Intel, the Intel logo, and Intel Xeon are trademarks of Intel Corporation in the U.S. and/or other countries. *Other names and brands may be claimed as property of others.