Top considerations in transitioning to NFV

Description

Network Functions Virtualization (Nfv) Is A Network Architecture That Implements Virtualization Of Network Functions To Deliver Communication Services Efficiently. It Offers The Potential For Enhancing Service Delivery And Reducing Capital Expenditure For Service Providers Offering Business, Residential And Mobile Services. Some Of Other Benefits That Drive Networking Stakeholders To Adopt Nfv Include – Significant Reduction In Operational Costs And Time To Market, Elimination Of Vendor Lock-In, Ability To Offer Flexible And Competitive Service Delivery.
Nfv Derives These Benefits By Utilizing Virtualization And Cloud Computing Capabilities In Order To Accommodate Network Appliance In Software. Thus, While The Aforementioned Benefits Of Nfv Are Alluring, The Following Challenges That Co-Exist Must Be Considered Before Adoption.

Performance

While The Software-Based Network Paves A Range Of Opportunities To Innovative Services, It Could Hamper Performance. In Several Scenarios, The Performance Levels Of Dedicated Hardware Cannot Be Achieved By A Single Virtual Network Function (Vnf). Hence The Number Of Instances Of Vnf, Need To Be Scaled-Up To Achieve The Same. During Dynamic Provisioning, This Introduces A Management Overhead, When The Load Of Each Vnf Has To Be Determined. This In Turn Deteriorates The Performance Levels Delivered By Nfv.

Furthermore, As Network Functions Are Moved From Dedicated Hardware To Cloud Infrastructure, Additional Performance Impact Is Introduced In Network Services. Besides This, Service Providers Need To Verify That The Level Of Impact Of Their Sla Metrics Due To Nfv Transition.

Security

While Embracing An Evolving Architecture One Cannot Ignore The Associated Security Challenges. Newer Capabilities And Components In The Network Also Mean Fresh And Unexpected Prospects For Security Attacks. Further Distribution Of Vnfs Across Datacenters And Frequent Migration For Resource Optimization Introduces Practical Difficulties Of Defining And Enforcing The Security Policies.

Reliability

Service Providers Typically Have Demanded Five-Nines Reliability. While The Proprietary Hardware Based Legacy Networks Have The Ability To Adhere To This Standard, A Hybrid Environment Which Encompasses Cots Hardware Capabilities (Both Virtualized And Non-Virtualized) Adhering To The Five-Nines Is A Challenge. The Dependencies On Multiple Components And Utilization Of Commodity Hardware Introduce Complexities Expecting Resiliencies To Be Built Into The Software Component Than The Hardware.

Interoperability / Compatibility

An Nfv Deployment Involves Hypervisor, Hardware And Software Solutions From Various Vendors, Which Could Introduce Compatibility Issues. When A Migration Of Vnfs From Such An Environment Is Attempted This Could Yet Again Lead To Compatibility Challenges. As A Result Consistent Performance Cannot Be Assured.

Troubleshooting

Troubleshooting In A Next Generation Network Involves Correlation Of Information Across Various Cloud Resources. This Increases Operational Costs And Makes It Challenging For The Administrator To Correlate Information Across Heterogeneous Entities And Determine The Root Cause. For Instance, In An Nfv Deployment While Determining The End To End Latency Could Be Feasible, The Root Cause Could Be The Vnf, The Platform Hosting The Vnf Or Any Other Component Across The Network. To Narrow Down And Determine The Actual Root Cause Of Latency In Such An Environment Could Be A Challenge.

Service Provisioning

Traditional Service Provisioning Was Restricted To The Network Elements. However In The Current Scenario Service Provisioning Also Extends To Vnfs In The Cloud. With The Different Functionalities Being Spread Across Both Hardware And Cloud, Service Provisioning Management System Has Becomes Complex And Requires To Be Overcome With Intelligent Systems.

Nfv Provides Flexibility In Migration Of Vnf Components And This In Turn Increases The Need For Service Re-Provisioning. This Is Induced Not Due To Changes In Service Parameters But Due To Increase In Migration Across Cloud Services.

The Aforementioned Factors Mandate Specialized Monitoring And Diagnostics Of Networks Which Support Nfv Capabilities. The Diagnostics Capabilities Should Be Enabled On-Demand During Both Validation And Live Deployment. Further, Gaining Visibility Into The Network And Awareness Of The Performance Levels Is Of Paramount Importance. These Capabilities Ensure That The Rising

Expectations Of Varied Nfv Stakeholders Are Met In A Consistent Manner. Therefore A Solution That Is Able To Monitor And Diagnose Network Service Performance Across The Service Lifecycle Could Be Key In Facilitating Quicker Adoption Of Nfv-Based Infrastructure.

Veryx's Solution

Veryx Samtest Enables Service Providers To Measure Various Performance Metrics, Utilizing A Combination Of Physical And Virtual Probes, Diagnose / Troubleshoot Network Issues And Provide In-Depth Visibility Into Network.

Learn More About Veryx Samtest.

About Author

Charanya Balasubramanian Is The Product Manager At Veryx Technologies. Charanya Handles Product Management Efforts For Sdn And Emerging Technologies At Veryx. She Has Over Five Years Of Experience In The Information And Communication Technologies (Ict) Industry Spanning Across Several Technologies Including Virtualization And Cloud Computing. She Holds A Master's Degree In Strategy And Marketing From Xlri, Jamshedpur, India And Bachelor's Degree In Computer Science And Engineering From Anna University, Chennai, India. Charanya Can Be Reached At Charanya.balasubramanian@Veryxtech.com.