Automate Your Network and Accelerate New Services

GET STARTED

TABLE OF CONTENTS

INTRODUCTION

For CSPs, speed is of the essence in developing and deploying new services, along with delivering a superior Quality of Experience while increasing operational efficiency. Delivering innovation, differentiation and remaining competitive while becoming more efficient can only be achieved when CSPs evolve their network architectures to a virtualized infrastructure with Network Functions Virtualization (NFV). NFV empowers CSPs to keep pace with the rate of change and capitalize on all categories of the digital opportunity, including delivering services such as VoLTE, VoWiFi, Video, IoT, and RCS and deploying them in a multi-functional, cross cloud environment.

The purpose of this e-book is to guide readers on the key requirements for CSPs adopting an NFV architecture and how VMware vCloud NFV, as an ETSI-compliant platform, can enable CSPs to accelerate service innovation, streamline operations, deploy an agile network and deliver multiple services, including vIMS, vCPE, vEPC, SD-WAN, while evolving network architectures to 5G.

“For Manx Telecom, working with VMware is a story of flexibility and agility”

Kevin Paige
Chief Information and Technology Officer, Manx Telecom

TRANSFORMING NETWORKS TO BE AGILE, FLEXIBLE AND SECURE

CSPs evolving their networks to NFV have to ask themselves how to prepare their core network infrastructure and transform the potential of NFV into actual business results. A key consideration and decision as they move to NFV, is what's required of their NFV infrastructure (NFVI) to achieve success.

Service Provisioning and Delivery

NFV gives CSPs the ability to increase the speed and efficiency of delivering new services and seamlessly scaling services based on real-time customer demand as well as the entire lifecycle management for services. Today, CSPs processes to on-board a new service can take months and are prone to errors due to manual interventions, leading to costly and delayed service roll-outs. To avoid these errors and deploy a successful NFV rollout, CSPs need to ask the following questions:

- **How can the development of service catalogs and deployment of new services be automated?**
- **How can services be provisioned based on pre-defined policies?**
- **How can multiple vendors VNFs be on-boarded while simplifying the creation of new services?**
- **How can the lifecycle management of services including adding, de-commisioning services be automated?**

Service Security

To achieve the full potential of benfits offered with NFV, CSPs will be deploying multiple services in a multitenant environment. If not designed and implemented correctly, deploying multiple VNFs in a multitenant environment can introduce a number of security challenges. Among some of these security challenges are:

- **Providing complete isolation and security of each tenant with each tenant having their own application and networking requirements**
- **Securing VNFs from malicious traffic or other rogue VNFs and tenants**
- **Deploying service-based policies to guarantee SLAs for specific services and tenants**
- **Ensuring safeguards against congestion and performance**

TRANSFORMING NETWORKS TO BE AGILE, FLEXIBLE AND SECURE

Operational Intelligence

It's imperative for CSPs to continuously monitor and mange the overall health of the network and understand the performance and capacity of the deployed services and VNFs. Ensuring service continuity even during unexpected failures, unpredictable spikes in demand or even during routine maintenance operations is critical to the success of the CSP. Following standard Day-2 processes can drive operational excellence and offer a high quality of service. To do this, requires the CSP to ask the following questions:

- **Does the network have a fully integrated operations management solution offering analytics, issue isolation, proactive avoidance and remediation?**
- **Is there complete visibility across all components of the service and its dynamic life-cycle?**
- **Can the operations management solution collect and correlate metrics and provide analysis and recommendations for optimal performance?**
- **How can the network provide automated service optimization with closed loop feedback assuring service integrity and dynamic SLAs?**

Carrier-Grade Infrastructure:

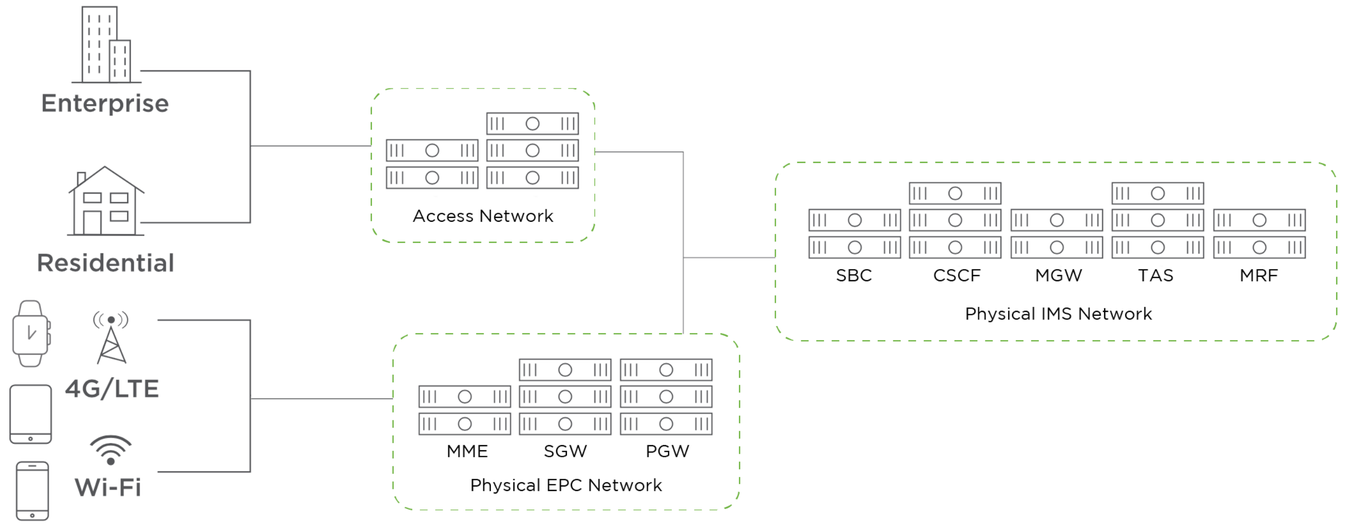
The transformation to virtualized networks will still require CSPs to deliver a highly-available network providing service continuity, guaranteed performance and rigid SLAs. To deliver a carrier-grade network, CSPs need to ask:

- **Does the NFV infrastructure offer high availability?**
- **How does the platform employ proactive optimization strategies?**
- **What is the process to upgrade a live environment with zero to minimal downtime?**
- **What is the process to on-board new vendors / VNF's that are NFV certified?**
- **How can the platform scale on-demand based on real-time network traffic as well as proactive forecasting?**
- **Can the platform be deployed across disaggregated network topologies? And is the cloud orchestration and operations management centralized across the network topologies?**

NFV USE CASE: AUTOMATE & ACCELERATE SERVICE DELIVERY OF VIRTUAL IMS

CSPs are experiencing significant demand to deliver consumer services, such as media-rich applications, including audio and video streaming, along with enterprise demand for rich communications services (RCS), collaboration and IP-PBX services. In addition, competition from OTT providers are pushing CSPs to expand their catalog of service offerings quickly and efficiently. For CSPs, services such as virtualized IMS (vIMS) can be a true differentiator for mobile carriers looking to offer their consumer and enterprise customers converged mobile and fixed services.

While traditional IMS architectures represented an architecture with separation of control and data planes, the initial single-tenant network design with purpose-built hardware and vendor lock-in presented CSPs with challenges especially as they wanted to become a more viable service provider for end-users. To be competitive, CSPs need an architecture where they can add new services, provision for a dynamic architecture to scale up and down and do so in a multi-tenant environment.

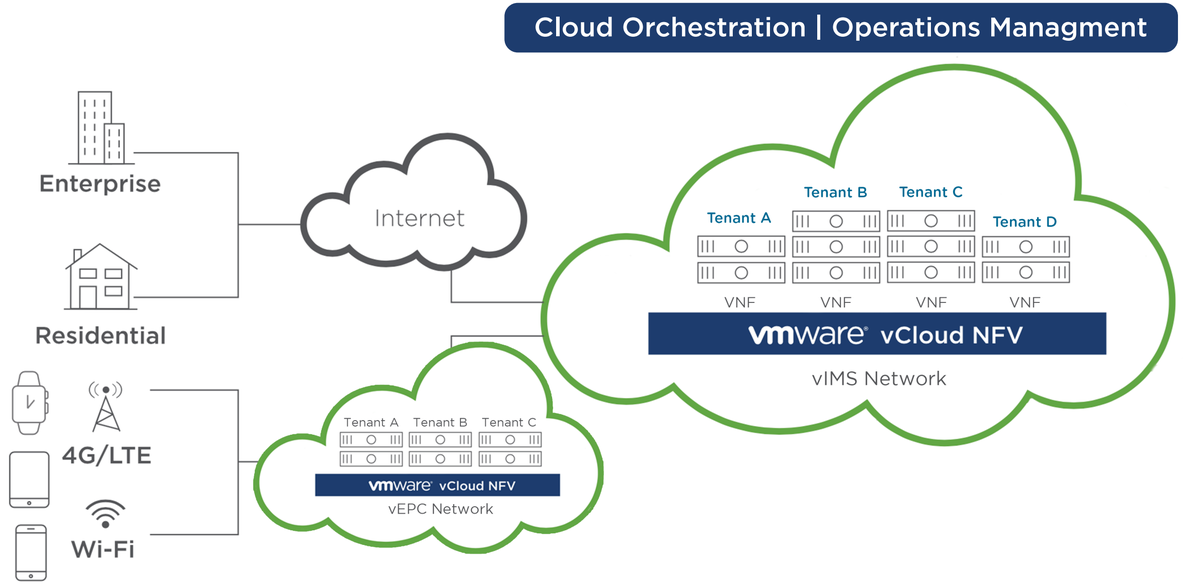


Traditional IMS Architecture

- Single tenant network design
- Rigid architecture
- Expensive capacity expansion
- Limited service innovation
- Complex and expensive operations management

NFV USE CASE: AUTOMATE & ACCELERATE SERVICE DELIVERY OF VIRTUAL IMS

Delivering rich multimedia telephony and communications services, offering on-demand services, network elasticity and deploying multi-tenancy network environments, will require CSPs to adopt NFV, ultimately driving service agility, innovation along with cost and operations efficiency.



vIMS Architecture

- Multitenant tenant network design
- Flexible architecture
- Elastic capacity expansion
- Unlimited service innovation

> **VMware helps us deliver new revenue-generating services, and transforms our infrastructure and operations through the adoption of NFV**

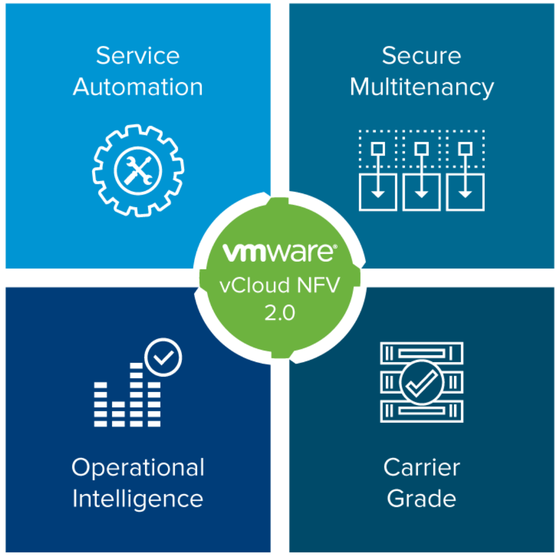
Ed Fox
VP. Network Solutions, MelTel

VMWARE vCLOUD NFV: EMPOWERING MODERNIZARTION OF NETWORKS

VMware vCloud NFV delivers a fully integrated, modular, multi-tenancy ETSI-compliant NFV platform. The standardized architecture of VMware vCloud NFV smooths the transition from proof-of-concept (POC) to service deployment and supports multi-vendor VNF deployments- while reducing total capital expenditures for telco-grade infrastructure.

With its advanced automation capabilities, CSPs can accelerate service creation, VNF on-boarding processes, and infrastructure management. VMware vCloud NFV offers carrier-grade availability, performance, and service continuity. It provides native multi-tenanted network services achieving complete service isolation in a secure multi-tenant environment across NFVI resources. VMware vCloud NFV also features advanced and unique operations management with 360-degree visibility and proactive and predictive analytics offering fast remediation capabilities that deliver operational excellence.

The result is a NFVI platform that is truly capable of transforming network and service delivery. The following sections provide additional detail about specific categories of capabilities.



AUTOMATION

For CSPs to deploy multiple services and applications to take on OTT competition, they require the agility and flexibility to bundle and scale new service offerings and continue to expand their catalog of service offerings quickly and efficiently.

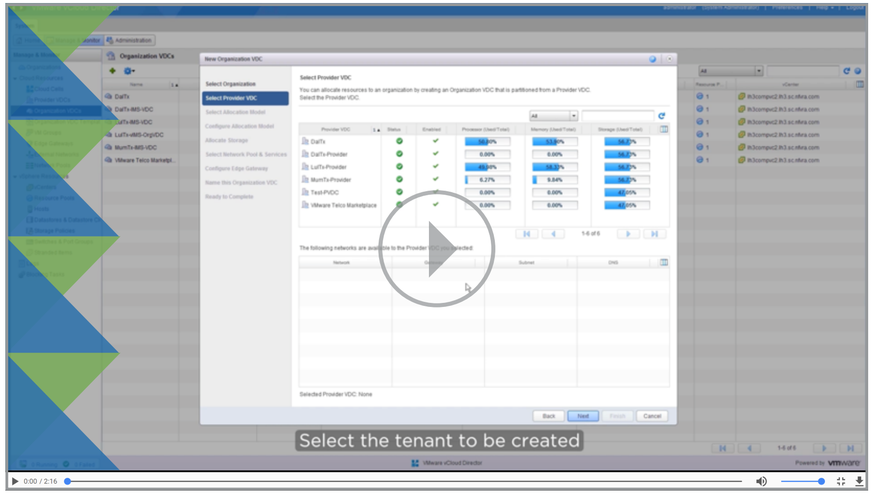
CSPs virtualizing IP Multimedia Subsystems (vIMS), for example, provides the foundational element to a future-proof network architecture that will enable a range of new services including VoLTE, VoWiFi and Rich Communication Services (RCS) for wholesale, enterprise and consumer customers across mobile and fixed line. Offering rich multimedia services from a common NFV infrastructure platform will give CSPs the agility to instantiate new differentiated services, continue to remain cost competitive and increase customer experience.

To maximize the benefits of vIMS while transforming their networks to NFV, CSPs need the ability to automatically and programmatically deploy VNFs rapidly. They need to automatically and intelligently allocate the appropriate resources to each virtual workload, where and when needed. And they need to seamlessly automate the on-boarding of VNFs from multiple vIMS vendors that have been pre-certified and are part of the VMware Ready for NFV partner ecosystem that brings together the largest technology partner marketplace to deliver these services.

Accelerating Service Creation: VMware vCloud NFV supports two integrated virtualized infrastructure managers (VIMs): native VMware vCloud Director or VMware Integrated OpenStack, a full OpenStack implementation that is completely tested and integrated. Both VIMs support templated service descriptions as well as multitenancy and robust networking, enabling the automation of on-boarding VNFs with the acceleration of configuring and allocating compute, storage and networking resources.

AUTOMATION

The vCloud NFV platform supports third-party service orchestration components leveraging TOSCA blueprints as well as configuration standards for service onboarding, policy, and service function chaining. In addition, VMware vCloud NFV offers northbound APIs providing capabilities to integrate with OSS/BSS systems and manage the NFV infrastructure deployment lifecycle.



BENEFITS

- **Policy-based on-demand service creation and resource allocation**
- **Streamlined VNF on-boarding**
- **Ease of deployment with predictable resource consumption**
- **Scalable infrastructure management and automation**
- **Automated capacity optimization**
- **Proactive high availability through intelligent real-time system performance analytics**

Create & Deploy vIMS Service

Virtual IMS service catalogs are imported into the VIM with enhanced policy-driven VMware vSphere vApp templates which automatically associate abstract resource requirements to appropriate resources in the target virtual data center and automates VNF importing. CSPs can deploy this into any multitenant service chain to deploy video calling, voice services, collaboration, and other rich communications services.

SECURE MULTI-TENANCY

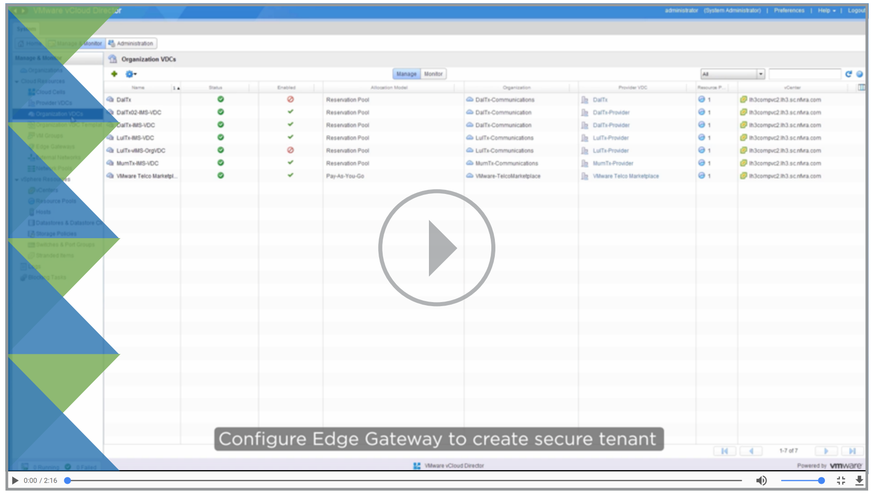
Offering rich multimedia IP communications services as a cloud-hosted service can open up new revenue opportunities for CSPs. Cloud services such as Unified Communications, IP-PBX, and emergency calling services can be offered as a fully managed service that can be offered to MVNOs as well as multiple enterprises and M2M customers serving multiple vertical industries. For example, an MVNO could offer voice telephony services along with roaming and international calling features, while an enterprise would choose multiple services such as IP-PBX and collaboration services.

Deploying multitenancy networks also requires each tenant is fully secure from attacks, breaches, or insecure communications from any other tenant. VMware vCloud NFV delivers complete service separation in a secure multi-tenant environment across NFVI functions and allows the creation of customer-specific services for each offer, ensuring multi-tenant slices of share infrastructure can be carved out to meet the service, security and SLA requirements for each specific customer.

Service and Network Isolation: VMware vCloud NFV delivers native secure network multi-tenancy through native VMware vCloud Director, VMware Integrated OpenStack and VMware NSX integration. CSPs can segment virtual resource pools, networking, security, and services into isolated network slices with well-defined service levels and provides security from the public internet as well as potential rogue VNFs. This allows multi-VNFs with multiple services to seamlessly share the same NFV infrastructure, yet have complete isolation from each other.

SECURE MULTI-TENANCY

VMware vCloud NFVs integration with VMware NSX, provides micro-segmentation with fine-grained access controls for provider and tenant administrators. With VMware NSX, CSPs can deploy security policies within the VNFs and the NFVI that can be enforced at the perimeter, across workloads, or Virtual Machines. This fine-grained security protects the tenant and safeguards control plane traffic such as SIP and Diameter, not only from north-south traffic, but also east-west traffic across shared services. Finally, security groups can be provisioned at the VM level to protect against malicious traffic of message flooding (such as SIP or Diameter) that could impair service availability.



BENEFITS

- **Fully isolated and secured workloads**
- **Guaranteed resource pools providing pre-defined SLAs to each tenant**
- **Single virtualization platform supporting multiple services and tenants**
- **Service-based deployment, isolation, and security**
- **Provider- and tenant-based roles and service policies**

Create Secure Multi-Tenant Environment

For CSPs to deploy a multi-tenant environment, CSPs must ensure that each tenant can be network-sliced and operate with differentiated service levels (e.g. compute, network, QoS, performance) while common services across all enterprises are implemented as a horizontal service with prioritized service levels across tenants.

OPERATIONAL INTELLIGENCE

Deploying NFV services requires CSPs to transform their operational processes. CSPs offering VoLTE services, amongst ma ny others, are required to deliver a highly available and high Quality of Service (QoS) to ensure a high customer Quality of Experience (QoE). In addition, they need to monitor the entire infrastructure for faults and performance issues, and they require the ability to dynamically and programmatically add resources when performance degrades or when a service-impacting disruption that may impact service level agreements (SLA) occurs.

Monitoring and Remediation: VMware vCloud NFV offers a pre-integrated and extensible operations management solution providing a single-pane-of-glass with complete visibility into all components responsible for the delivery of a service, from the underlying servers, through the hypervisor, networking, virtual machines that make up the VNF, and the service itself. vRealize Operations Manager collects near real-time data to provide correlated health, performance, capacity, and availability metrics along with recommendations. vRealize Operations Manager can be configured to generate prioritized alert notifications for closed-loop integration into resource and service orchestration workflows, providing complete 360-degree monitoring capabilities across service, virtual, and physical tiers.

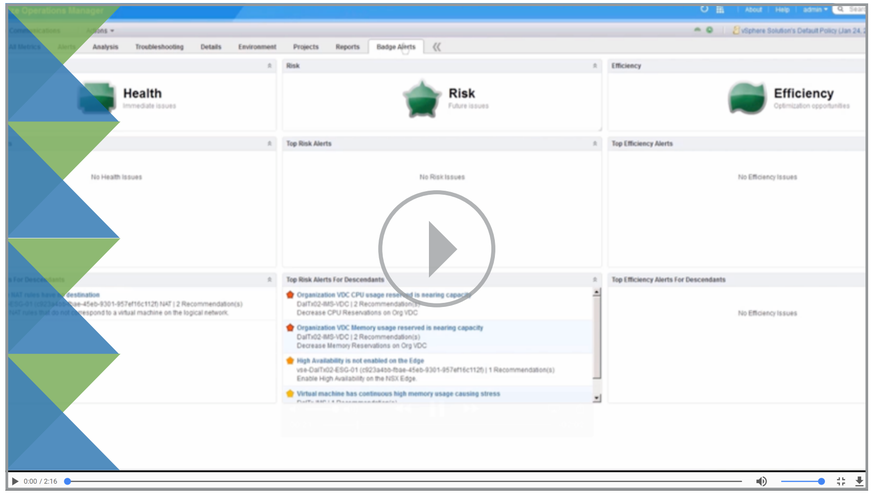
Real-time Network and Security Analytics: CSPs can gather real-time network intelligence with vRealize Network Insight, which provides full visibility into virtual and physical networks and network flow-level analysis that matches VNF workloads. As vRealize Network Insight is pre-integrated with the NFVI components, it unveils any gaps in network micro-segmentation compliance, security violations, traffic routing and performance, providing optimized security policies.

Fine-grained Issue Isolation: VMware vRealize Log Insight captures all unstructured data from the environment, providing log analysis and analytics for issue isolation. Any logs, events, incidents tickets, syslogs can be ingested by the vRealize Log Insight engine, which can be filtered to look for fault / error conditions and optionally put under observation toward future alerts.

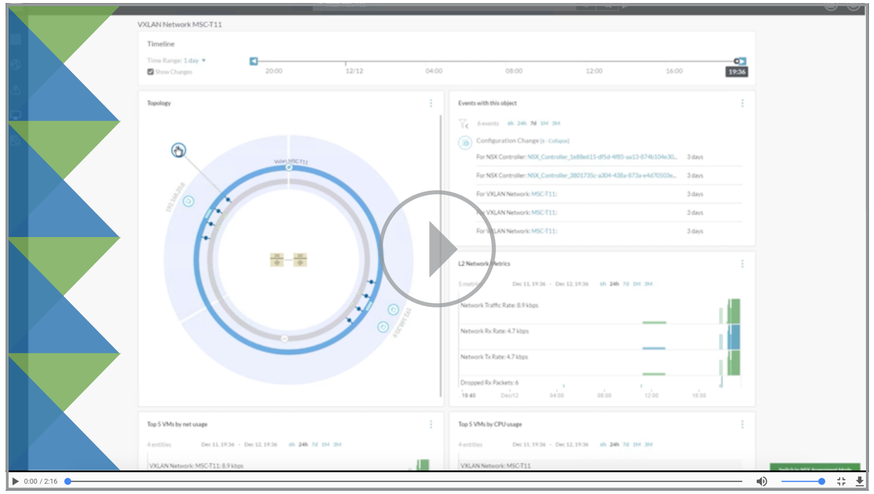
OPERATIONAL INTELLIGENCE

vRealize Operations Manager monitors the health of the vIMS infrastructure and provides visibility at multiple layers in the event of a service impacting interruption. With vRealize Network Insight and vRealize Log Insight, CSPs have complete visibility and can rapidly isolate the issue and provide fast Root Cause Analysis (RCA), along with remediation and validation of the vIMS service returning to normal service.

Operations Management



360 Degree Visibility



BENEFITS

- **360 degree single pane-of-glass visibility into all layers**
- **Greater network control through proactive and predictive analytics and intelligent log analysis**
- **Fast time to resolution with contextual troubleshooting and visual root-cause analysis**
- **Active remediation of workloads and northbound integration with OSS/BSS and third-party solutions**

CARRIER-GRADE

vCloud NFV delivers a carrier-grade NFVI platform with continuous five-nines availability, service continuity, guaranteed performance, and simplified management, enabling CSPs to extend the mean time to failure (MTTF) and shorten the mean time to repair (MTTR) resulting in exceptional availability to customers.

Network Resiliency: The vCloud NFV platform employs typical active-active, active-standby, and N+1 architectural principles to achieve high availability in functional components and service availability. vCloud NFV employs proactive monitoring to ensure dynamic optimization of NFVI resources to avoid failure conditions. If all proactive issue-avoidance mechanisms fail, components of the VNF are configured to automatically return to life using VMware's High Availability (HA) and Fault Tolerance self-healing mechanisms. Resource pools assigned are continuously monitored and expanded or collapsed as needed, defined by advanced policies such as time-of-day, threshold, or capacity targets.

Real-time Network and Security Analytics: For CSPs, enterprises and consumers expect highly available services and stringent SLAs for services such as audio and video streaming, as well as real-time and high priority applications. The vCloud NFV platform continuously and proactively monitors service performance characteristics as defined by SLAs and uses VMware's Distributed Resource Scheduler (DRS) and vMotion technology with Enhanced Platform Awareness (EPA) that greatly increases service availability and extends workload balancing across geo-redundant availability zones.

In addition, vCloud NFV offers advanced tuning parameters for enhanced performance, including native Intel NIC drivers for VMware vSphere and virtual remote direct memory access (vRDMA) for east-west traffic optimization.

BENEFITS

- **Proven high-availability platform**
- **High Service availability and continuity**
- **Improved networking performance for data plane workloads**
- **Increased network efficiency through predictive on-demand policy based scaling of workloads**
- **Simplified infrastructure lifecycle management for upgrades and patches**

vCLOUD NFV: DISTINCT ADVANTAGES

VMware vCloud NFV delivers a unique combination of attributes that set it apart from competitive platforms, including modularity, freedom of choice through open standards and multi-vendor VNF support, mature partner ecosystem, future-ready agility, and carrier-grade support. Additional advantages include:

Flexible deployment and management tools:

vCloud NFV employs a single architecture supporting multiple VIMs, adding flexibility to deployment, dynamic optimization, and management.

Deep visibility and insight:

vCloud NFV provides holistic, 360-degree visibility and insight into all network layers along with smart alerts and recommendations.

NFV ready certification:

VMware has the largest number of certified VNF partners and the most comprehensive testing and certification program with the VMware Ready for NFV program.

Proven in production:

vCloud NFV has been deployed in over 80 product implementations, across 45 operators supporting over 300 million subscribers.

NET RESULT: HIGHER BUSINESS VALUE

By delivering all of the capabilities described above, the VMware vCloud NFV platform is uniquely capable of providing a new level of business value to CSPs through three primary attributes:

Accelerated Service Delivery: CSPs can accelerate delivery and activation of new services and innovations, cut time to revenue (TTR), transform networks from static to adaptive, and employ software-defined economies in service delivery.

Simplified Operations: CSPs can deepen visibility into networks and resources, automate the delivery of services, maintain high availability and uptime for networks, and reduce total cost of ownership (TCO) while delivering a superior customer experience.

Increased Choice: CSPS achieve freedom of choice and additional benefits from multi-vendor agnostic VNF support, a mature NFV ecosystem, a common multi-platform that is open and supports open APIs, an extensible platform, and multiple-VIM support.

GET STARTED TODAY

Learn more at http://www.vmware.com/go/nfv

Join Us Online:

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com