TECHNICAL WHITE PAPER – **JANUARY 2017**

VMWARE VCLOUD NFV PLATFORM FOR VIRTUALIZED EVOLVED PACKET CORE

vmware®

Table of Contents

1. Executive Summary

As 5G Core technology hurtles towards critical mass in today's mobile telecommunications landscape, network functions virtualization is the only foundation on which new, 5G-related, business- and consumer-oriented services can be constructed and delivered. By virtualizing the evolved packet core (EPC), mobile carriers will be strategically positioned to meet the growing and rapidly evolving requirements of a broader spectrum of voice, video, gaming, virtualized desktop & application, Internet of Things, and machine-to-machine data transmissions as these communications increase and quickly outpace current mobile data demand.

Carriers looking to transition to virtualized evolved packet core (vEPC) should consider the VMware vCloud NFV platform as the foundation for vEPC and all other virtualized networks functions (VNFs). The VMware vCloud NFV platform offers service providers faster deployment and agility with advanced networking and security; a carrier-grade platform with high-performance capabilities to meet or exceed carrier-grade requirements; and automation and orchestration of network infrastructure to accelerate and simplify network provisioning and launch new services to market faster.

Bundling vEPC with vCloud NFV offers mobile carriers service agility in the mobile core, network-sliced elasticity, distributed mobile core-edge, and network monitoring and operations.

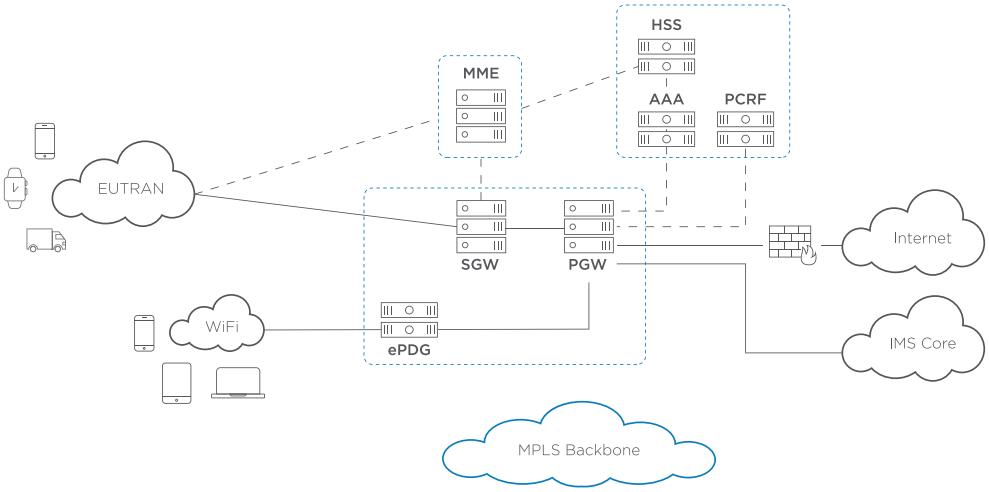
2. Limitations in Traditional vEPC Architectures

Traditional distributed mobile packet core networks were built using physical appliances stitched in a spoke-hub approach with geo-redundant availability zones. As such, the architecture is fairly monolithic, static and inflexible. Operating models have been stretched end to end, but even so, service agility and innovation are gated by handset advancements, mobile and network infrastructure, Network Equipment Providers (NEPs) and physical appliances, cost, competing roadmaps, and closed and proprietary vendor interfaces, among other challenges.

The resources and effort required for common activities like onboarding a new service or adding capacity (i.e. adding additional capacity to a Packet Gateway (PGW), ranging from a line card in the gateway to inserting a new chassis into the EPC core switch LAG) are significant, involving meticulous cross-service validation and impact assessment, not to mention careful coordination and maintenance windows for deployment.

A typical traditional mobile core network topology could comprise:

- A regionalized site with a cluster of MME's with control plane mobility management;
- Distributed sites with integrated S/PGW control and user plane functions;
- A site with shared functions such as AAA, HSS, PCRF, DRA, DHCP, etc.;
- Another set of sites with shared IMS cores



Typical Traditional Mobile Core Network Topology

This foundation has been instrumental in delivering to stringent quality requirements as well as providing new service discovery and differentiation, all while protecting the customer experience. With an all-IP converged network of voice and data services, the footprint is delivering and optimizing VoLTE/ViLTE communications. And beyond VoLTE and ViLTE, the evolved mobile core is expanding into other business models, as well:

- Machine-to-Machine (M2M) to enable communication for smart meters, auto telematics, asset tracking and logistics, to name a few;
- Mobile Private Network (MPN) to offer enterprises cellular packet data services (with slicing achieved through APN or VRF segmentation);
- Mobile Virtual Network Operator (MVNO) to provide wholesale EPC services and break out to their data centers;
- WiFi Interoperability to complement the macro network to offload capacity, improve QoE in high subscriber dense areas and expand in-building coverage.

VoWiFi, VoLTE and ViLTE are still undergoing tremendous growth, while mobile packet core architectures remain hindered by scale, cost, and operational management. VoWiFi has taken several years to smooth out WiFi-to-Cellular hand-off and continuity, and IPSec tunneling continues to challenge scale for the untrusted access stratum.

Meanwhile, the legacy mobile packet core networks employ a static network design and a topology that is pre-configured end to end and sized to anticipated maximum load targets. Most of the evolved packet core network elements aggregate control and data plane functionality into a single appliance, with prescriptive operating capacities limited by subscribers, message transactions, sessions, throughput, and so on.

Soon, demand will completely outstrip traditional architecture's ability to deliver scalable and secure services, as these architectural and technology innovations are already massively straining networks and demanding their immediate diversification. The only way to achieve the network transformation needed for the service agility and service availability to address today's emerging business opportunities is through disaggregation of the mobile core network and adoption of SDN and NFV, essentially conceptualizing EPC-as-a-service. It is neither feasible nor possible to expand the infrastructure to keep up with the growing demand by leveraging only traditional architectures, and this demand will only accelerate in the future.

Today's mobile telecommunications 5G Core advancements are positioned to meet the demands of both business and the consumer for highly increased throughput, machine-type communications, low latency, high reliability, and real-time service characteristics. 5G technology has enabled services such as video, virtual desktops, gaming, remote monitoring, connected cars, smart-everything, the Internet of Things, etc. to become new business models for the carrier. Network and service transformation within their packet cores is critical to mobile carriers staying competitive and on the cutting-edge. As such, in order to lead service innovation and agility, operators need to:

- Employ software-defined modular network functions combined with programmable networking for advanced service composition;
- Expand beyond the traditional NEPs and into the growing ecosystem of VNF providers;
- Implement flexible service enablement and deployment across geographies and network functions;
- Streamline operations with integrated analytics for improved service operations and reduced costs.

Operators are embracing digital transformation initiatives to improve customer experience, reduce operating costs, and explore new revenue opportunities. This transformation requires the flexible, automated, and open environment for on-demand service composition, delivery and lifecycle management that the VMware vCloud NFV platform can deliver.

3. The Mobile Core Transformation: vEPC on vCloud NFV

Deploying virtualized EPC solutions on the vCloud NFV platform is elegantly simple. Since the deployments are centrally managed, it affords the flexibility to easily deploy those services that make sense closer to the edge, (i.e. MME) outward, while managing, monitoring and automatically scaling the heavier workloads. In conjunction with the micro-segmentation capabilities of NSX, the vCloud NFV architecture opens the door for a truly segmented environment with network slices, a hard requirement for maintaining multi-tenant, multi-service security and service quality in a virtualized environment..

4. Service Agility in the Mobile Core

Vendors are moving towards software-defined tiered architectures, modularizing virtualized network function components (VNFCs) across control plane, user plane, exposed interfaces, configuration and management, and platform services (database, DHCP, session management, etc.). Coupled with SDN and NFV advantages, this modularity achieves

a. **Horizontal scalability and load-balancing separated by control and data plane functions:** Provide integrated load-balancing across VNFs with vCloud NFV to manage an exploding number of connected devices (especially in the case of M2M low-bandwidth communications, where control plane resources will exhaust faster than data plane);
b. **Dynamic scaling:** Scale VNFs up/down and in/out dynamically and with enhanced platform awareness (EPA), ensuring optimal performance through vCloud NFV;
c. **Native acceleration:** Take advantage of vCloud NFV native accelerations for data plane processing components– DPDK switch, optimized contention-less resource utilization, reservations, NUMA affinity, and more;
d. **Flexible service chaining:** Apply differentiated policy, shared packet gateway deployment, chained value-add services (content filtering, media transcoding) on the SGi, traffic management (VPN termination, DPI), etc.;
e. **Alignment with emerging RAN innovations:** Include cloud RAN and separation in radio and baseband processing functions;
f. **Gradual and controlled transformation:** Correlate across virtual and physical services;
g. **Declarative SLAs:** Employ declarative SLA and optimization constructs defined in NSD/VNFD blueprints which vCloud NFV can monitor and apply proactive adjustments.
h. **Intelligent topology:** Centralize the compute-intensive services and push the latency-sensitive services closer to the edge.

The disaggregation of the network functions, along with SDN and NFV, also accelerates the disaggregation of mobile network static topologies. For example:

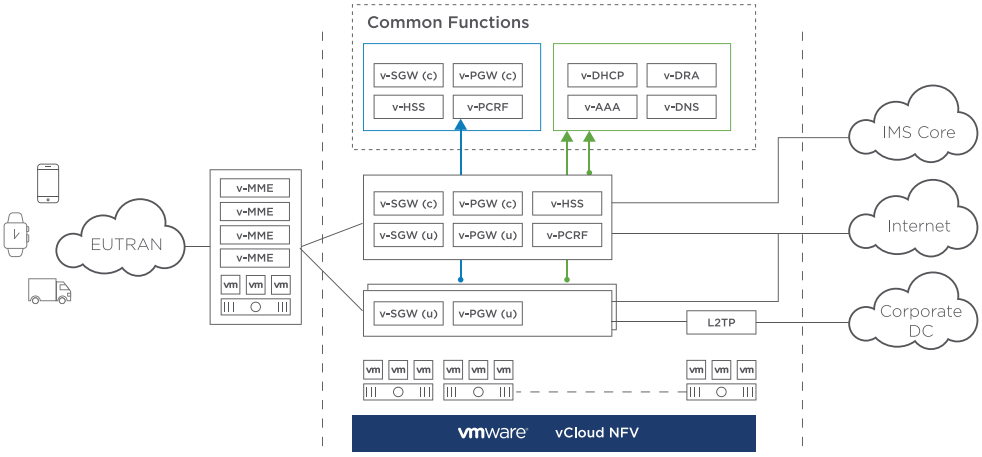
- Mobile edge to serve the end-device proximity use case, say for a smart city or healthcare use case; for low-latency, high reliability communications; for content caching and avoiding long-haul transports to the central DC;
- Non-mobility configurations for stationary connectionless IoT communications.

5. Network-Sliced Elasticity

With vCloud NFV, the decomposed control and data plane functionality of the mobile virtual network functions can now be scaled and distributed into slices to service applications and customers with varying traffic profiles. Each decomposed function, realized as a VM, can be deployed in a shared architecture or orthogonal to other mobile core slices.

Moving away from a single monolithic mobile core designed to serve any service and any customer not only deters agility for the business but also carries a large operational risk. Sliced mobile packet cores can be monitored individually and dynamically scaled, upgraded and chained with other VNF value-adds, for example, without impacting other customers and services.

Service innovation and feasibility analysis can be accelerated significantly with this approach. A trial network slice can spin up VNFs for the mobile core, on-board the new service and integrations, tested and tried before introducing to the market. For that matter, a smaller market trial can be incubated to measure success and fail fast.



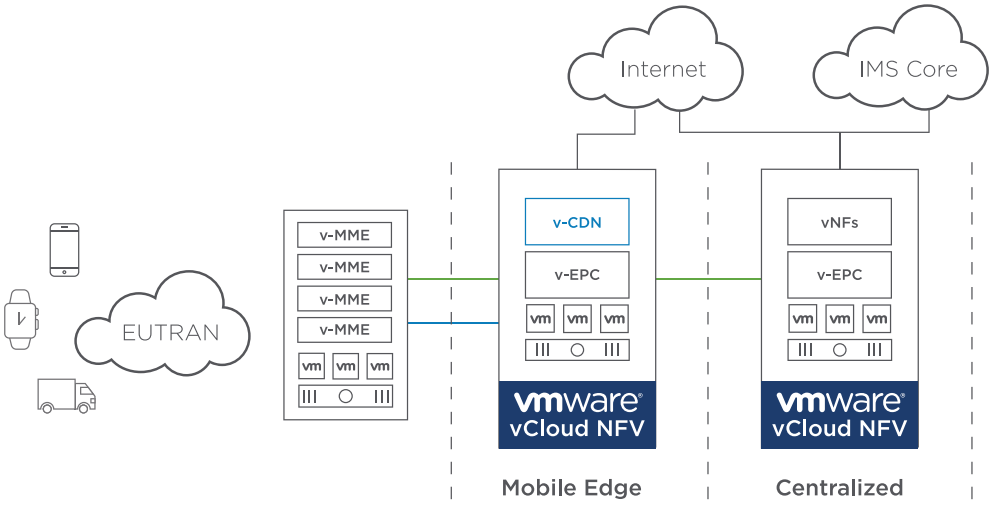
vEPC on VMware vCloud NFV

Service and service-chains can be defined in templates (TOSCA, for example), and virtual network functions can be rapidly instantiated and configured to enable a new mobile packet core slice for a service or enterprise customer. Control plane functions implementing S1-AP, GTP-C, or Diameter protocols from data plane functions implementing GTP-u offer flexible options for clustered or shared deployment to meet different SLAs, connection concurrency, device density, and bandwidth.

Each network slice can be instantiated to serve different business drivers such as MPN, MVNO, M2M, IoT, while WiFi augment can be applied to bandwidth-heavy applications. Each slice can have a dedicated policy and charging virtual function instance as well.

6. Distributed Mobile Core Edge

Extending beyond the regionalized and centralized mobile core deployment topologies, distributed virtual mobile edge packet cores can complement operational and customer experience advantages. For use cases like localized enterprise/branch customers; virtual CDN caching; virtual desktops; machine type communications for smart city, medical care centers and sensory networks; and broadband internet access for high subscriber density areas, mobile cores at the edge benefit where user proximity and service localization are possible. Such segmented deployments afford lower latency, thereby improving QoE for users and lower operating costs for the operator, including issue isolation. Local Internet loops can be employed rather than backhauling traffic over expensive transport providers and operator MPLS backbones.



Distributed Virtual Mobile Edge Packet Cores on VMware vCloud NFV

The mobile core at the edges augments the centralized packet cores to balance across low-latency needs, operations-cost offload, and service anchoring.

7. Network Monitoring and Operations

Ensuring availability and reliability of services and infrastructure across a heterogeneous ecosystem of diverse platform and vendors, network O&M continues to be one of the top priorities for an operator. Network and IT operations have more tools in their environment ranging from device, radio, transport, engineering, traffic instrumentation, and application for analysis and optimization.

Monitoring across this diverse environment requires information collection and correlation aggregated across EMS platform from those vendors. With vCloud NFV, operational intelligence for service operations is baked into the horizontal platform:

- Continuous monitoring of resources and service allows for auto-scaling and auto-healing of VNFs proactively, ensuring optimal service operations;
- On-demand enablement of DPI VNFs can provide deeper issue isolation and RCA;
- Operational intelligence can track service and customer SLAs within a network slice or mobile edge.

8. Advantages of vEPC on vCloud NFV

VMware vCloud NFV, an ETSI NFV-compliant platform, delivers carrier-grade infrastructure integrated with a robust operation and management toolkit. The platform is open to any VNF by offering a horizontal, multi-tenancy, multi-domain environment. VMware vCloud NFV features

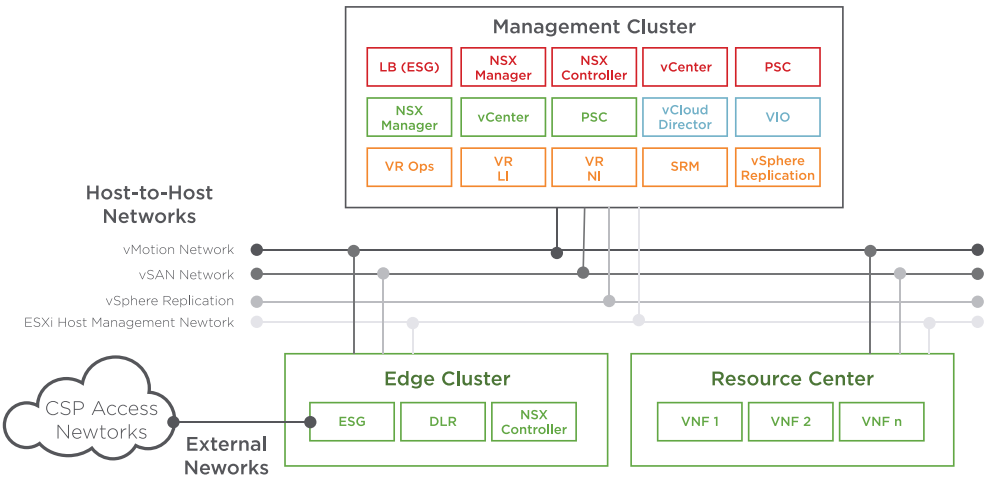
- **Integrated Dynamic Platform:** The VMware vCloud NFV solution is a modular, horizontal, common NFV Infrastructure platform based on ETSI standards. It is built on proven virtualization technologies for compute, storage and networking along with integrated dual multi-tenant Virtual Infrastructure Managers. It enables cloud centralized operations and management across the deployed topologies.
- **Software Defined Networking:** NSX for vSphere provides overlay networking technology for workloads, with integrated logical switches, routers, firewall, load-balancers, and VPN delivering connectivity, performance, and security in any carrier deployment. Logical overlay tunnels make VNFs completely agnostic to the underlying infrastructure. As a result, multi-VNFs with multi-services can seamlessly share the same infrastructure yet have complete isolation from each other. With VMware NSX, service providers can deploy security policies within the VNFs and the NFVI with fine-grained traffic segmentation that can be enforced at the perimeter, across workloads or VMs. Security profiles are bound to the VNFs, and thus migrate seamlessly across resource clusters.
- **Software Defined Storage:** While vSAN is an optional component of the vCloud NFV offering, it adds a number of advantages to the deployment. Virtual SAN pools together local DAS storage into a common sharable datastore, offering a much lower-cost solution across the platform. Through automated and centralized policy controls, storage can be attached and scaled as needed by application demand. The solution is fully integrated into features like vMotion, High Availability (HA), Distributed Resource Scheduler (DRS), and more.
- **Services Management Automation:** vCloud NFV provides flexible, automated VNF onboarding and full-service lifecycle management through multi-VIM capabilities, greatly accelerating new service onboarding and expanding customers with TTM. With VMware native vCloud Director (VCD) or VMware Integrated OpenStack (VIO) – a full OpenStack implementation – service providers can automate the process of deploying VNFs and NFVI resources including the configuration and provisioning of compute, storage, and networking resources. With policy-based provisioning, vCloud NFV simplifies the resource allocation for VNFs. This gives service providers a multi-tenant, robust VIM that automates and accelerates service deployment.
- **Carrier-Grade Performance and Availability:** The platform provides proven carrier-class performance, extending control and data-plane separated cluster design. Workloads can take advantage of the high performance fabric with built-in dynamic high availability and scalability to meet application demands. SLA guarantees are met through resource isolation, reservations, and dynamic workload placements with DRS and vMotion technologies. The platform can be scaled from a branch office virtual PoP to a large centralized datacenter, to achieve micro-datacenter and multi-tenant network sliced designs.

- **Integrated Operations Management:** This fully integrated single-pane cloud solution ensures and restores service levels using near real-time operation monitoring, analytics, automation and remediation. The solution provides an overall integrated and correlated view across service, access, network, virtual and physical tiers, with issue isolation and recommendations for RCA. Northbound triggering closes the loop with service and resource orchestration remediation and NMS/OSS notifications. The solution can be extended with custom data feeds and third-party domain and technology expert analytics systems.
- **Ready for NFV Partner Ecosystem:** *VMware Ready for NFV* is a certification program that ensures interoperability between VNFs and the vCloud NFV platform. The interoperability tests, performed by VMware engineers, assist partners in understanding and preparing for cloud operations over vCloud NFV.

An Integrated Dynamic Platform

The VMware vCloud NFV solution is an open platform implementation of the ETSI NFV ISG reference architecture (defined in GS NFV 002). The reference architecture paper can be found here. The rich set of capabilities in VMware vCloud NFV is designed with strict functional separation ensuring optimal resource usage, service management, and security. Distributing resources efficiently and achieving functional separation are achieved using a cluster construct:

- **Management cluster:** All management control-plane functions are in this cluster, as well as the operations and management components, themselves.
- **Edge cluster:** This cluster isolates and secures the VNFs from the wide-area network and transitions network traffic between the physical and the virtual domains, and vice versa.
- **Resource cluster:** Multi-tenant VNFs are hosted in this cluster with provided non-contended resource isolation and demand-driven elasticity for optimal performance and scale.



▶ A distributed deployment of the vEPC solution can benefit from a management cluster for control plane operational management and cloud orchestration in a centralized data center. Mobile edge core components comprise the resource and edge cluster distributed across a geography to meet low latency and proximity objectives.

Secured Virtualized Networking with VMware NSX

Virtualizing network functions offers numerous benefits, and one major advantage is the ability to programmatically and automatically deploy new services or extend and scale existing services. VMware NSX for vSphere is the virtualized networking tool underpinning all communication in VMware's vCloud NFV. Using a separation between control and data plane paradigms, demanding network workloads enjoy unhindered resources while control plane components remain unaffected by rogue VNFs.

NSX for vSphere has all the components needed to create a carrier-grade elastic service:

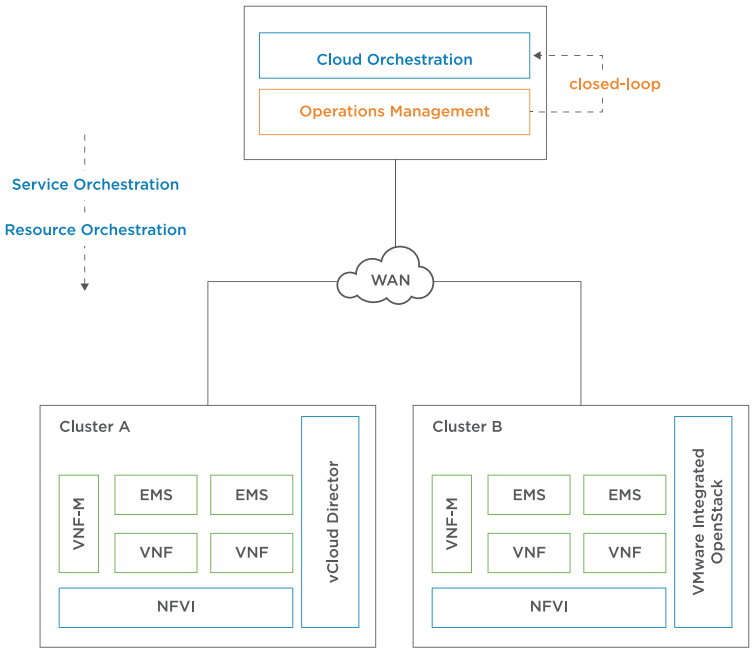
- NSX provides in overlay, the network and service isolation with carrier class service levels and fine-grained security and control.
- Service providers can extend data centers across locations while maintaining the same IP addressing and security policies and extending fault tolerance.
- By using standard protocols such as BGP and OSPF, the virtualized networking components are easy to integrate with the existing service provider networks.
- Built-in distributed logical routing can achieve low-latency network communications across VNFs and their components (VNF-C), minimizing the need to upgrade physical network components.
- NSX management and monitoring is integrated with the management systems such that monitoring VNF health covers a complete stack – from physical to virtual to application.

▶ With NSX for vSphere, micro data centers can extend networking across sites or create tenant-specific network isolation in a network-sliced environment, maintaining existing IP addressing schemes. Secure IPSec and SSL tunneling can enabled across sites or cloud services.

Service Management Automation

The vCloud NFV platform provides and exposes flexible VNF onboarding, from resource orchestration to service lifecycle management through multi-VIM capabilities.

Both VCD and VIO VIMs support templated service descriptions as well as multi-tenancy and robust networking, automating and accelerating service deployment and lifecycle management with closed-loop operations management.



Being fully compliant with the ETSI NFV architecture framework, the vCloud NFV platform also supports open APIs to third-party service orchestration components (NFV-O and VNF-M) leveraging TOSCA blueprints and YANG/NETCONF data modeling specifications. This also allows for customization and automation of the orchestrator to suit any deployment.

▶ Multi-site, disaggregated control and data plane functions across the CSP topology can benefit from centralized orchestration and management functions. Operations experts can leverage a flexible northbound standardized API, integrated into OSS/BSS and service creation automation, as needed.

Service Availability

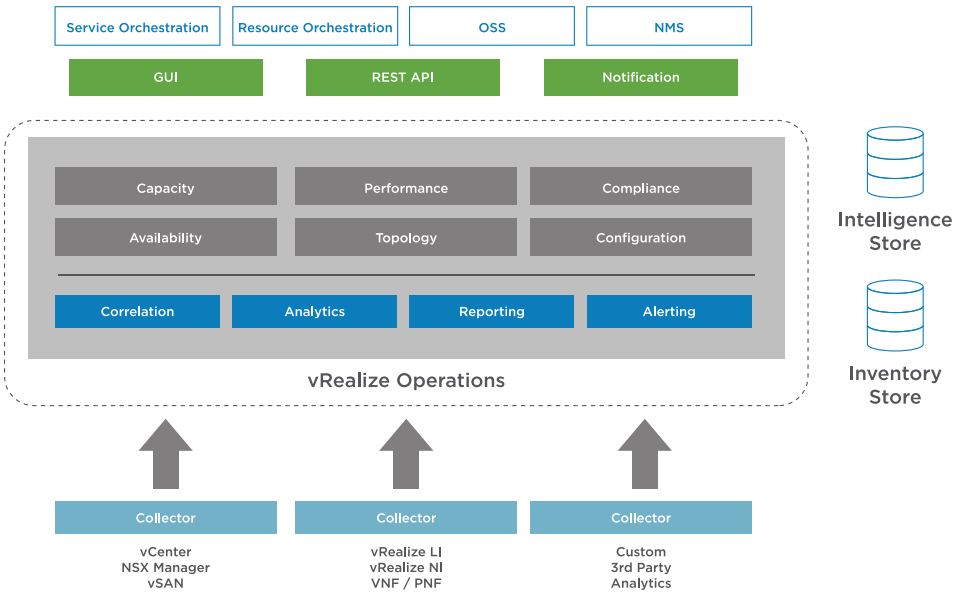
The vCloud NFV platform not only employs a well-thought-out redundancy design using active-active, active-standby, and N+1 architecture principles, it also integrates monitoring for proactive, automated, and semi-supervised service availability safeguards. If all proactive issue-avoidance mechanisms fail, components of a VNF are configured to automatically return to life using VMware's High Availability (HA) mechanism.

The vCloud NFV platform continuously monitors service performance characteristics as defined by SLAs and uses VMware's Dynamic Resource Scheduler (DRS) and vMotion technologies to balance live workloads with Enhanced Platform Awareness (EPA). vSphere Replication and Data Protection technologies provide VM-level data replication and continuous data backup to recover from an outage.

Integrated Operations Management

Historically, operations management approaches are a tedious aggregation of vertical management components across different vendor devices and OSS/BSS solutions. vCloud NFV is bundled with fully integrated operation monitoring, analytics, proactive avoidance, issue isolation, and remediation.

- **Monitoring and Remediation:** vROps provides complete visibility of all components responsible for the delivery of a service – from topology discovery to cross-tier physical and virtual hierarchies. Data is collected and computed near-real time (centralized or distributed) to provide correlated health, performance, capacity, and availability metrics. Prioritized alert and recommendations drive closed-loop integration into resource and service orchestration workflows for issue avoidance and remediation.



- **Issue Isolation:** The vRealize Log Insight tool captures all unstructured log and event data from the environment, providing log analysis and analytics for issue isolation. Unstructured to structured object models can be filtered for fault/error conditions, and optionally put under observation towards future alerts, presented in the single-pane.
- **Network and Security Troubleshooting:** vRealize Network Insight provides full visibility into virtual and physical networks as well as security engineering analytics. The engine is pre-integrated with the NFVI components, ingesting data ranging from network inventory and configuration metrics to IPFIX records, Security Groups, FW rules, IP Routes (across VXLAN/VLAN), and growing list of physical infrastructure elements metrics. It helps optimize network and security designs, surfacing gaps in network micro-segmentation compliance, security violations, traffic routing and performance, VM traffic analysis, flow monitoring (virtual to physical, E-W and N-S), and more.

▶ vEPC can benefit from centralized network monitoring, optimization, and issue isolation. vCloud NFV components in the management domain allow third party developers to create plug-ins to enhance their understanding of the workloads they are monitoring.

By default, operations management provides coverage for infrastructure, virtualization, and transport tiers, however it can be extended with data adapters, KPI computations, alert profiles, recommendation, and custom dashboards from DPI virtual probes, VNF KPI's, or third-party analytics, for example.

Partner Ecosystem

The vCloud NFV platform is pre-certified with Telco NFV solutions from our extensive partner ecosystem. Service acceleration is key and the VMware Ready™ for NFV partner program brings together the largest Technology Partner Marketplace with VNFs for telco solutions. The Cloud Management Marketplace offers a robust collection of extensibility tools, management packs, and content packs for monitoring and analytics integration into the vRealize Operations Management suite.

7. Conclusion

The VMware vCloud NFV platform allows CSPs to offer vEPC services to their enterprise customers and open up new revenue streams in the process. Because the vCloud NFV platform is modular and extensible, and surrounded by a rich ecosystem of partners, it enables CSPs to build quickly, tailor and deploy offerings that meet the needs of their regional customers.

To learn more about VMware vCloud NFV, please visit http://www.vmware.com/go/nfv.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com
Copyright © 2016 VMware, Inc. and SQLHA, LLC. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents. VMware is a registered trademark or trademark of VMware, Inc. and its subsidiaries in the United States and/or other jurisdictions. SQLHA is a registered trademark of SQLHA, LLC www.sqlha.com. All other marks and names mentioned herein may be trademarks of their respective companies. Item No: VMW-vEPC Technical Whitepaper_v1
11/16