TECHNICAL WHITE PAPER – **JANUARY 2017**

VMWARE VCLOUD NFV PLATFORM FOR VIRTUALIZED CUSTOMER PREMISE EQUIPMENT

vmware®

Table of Contents

1. Executive Summary

Physical (non-virtualized) customer premise equipment (CPE) incorporates a number of unavoidable costs for the communications service provider (CSP), many of which – from deployment to configuration to servicing – require a truck roll. Nearly all of these costs are eliminated with virtualized CPE (vCPE), which also simplifies and accelerates the delivery of services, upgrades and reconfiguration.

Further, vCPE aligns CSPs with the rising trend of home-based IoT devices. In the 2H16 Telecom Software Mediated Networks (NFV/SDN) Customer Adoption Study by Technology Business Research Inc., telco respondents identified 5G and the IoT as the primary drivers of NFV and SDN adoption, followed by digital service creation.

The TBRI study found that most Tier 1 telecom providers worldwide plan to adopt NFV and SDN technologies within one to two years, buoyed by positive business results from extant large-scale commercial deployments. CSPs transitioning to vCPE find themselves in the vanguard of industry movement toward cloud-based, virtual-first services that are becoming the norm for enterprise customers.

Virtualizing CPE simplifies network connectivity and value-added services across CSPs' enterprise and residential customers, while also abstracting the multi-tenant operations and service management complexities into the service provider clouds. Whether deploying vCPE in a thin on-premises model, a heavy on-premises model, or a hybrid of the two, vCPE accelerates networking and communications, allowing CSPs to be much more responsive to customer needs.

VMware vCloud NFV is the ideal platform for virtualizing network functions like CPE, delivering carrier-grade infrastructure with a robust operation and management toolkit. With optimized resource management and prioritization of resources based on service provider workloads, vCloud NFV ensures top performance, scalability, and high resiliency for critical communications network services. The platform allows CSPs to rapidly enable new revenue opportunities and grow beyond high-touch networking services, such as traditional, non-virtualized CPE. With features including on-demand capacity elasticity, dynamic service insertion, and configuration change management, the platform accelerates service deployment – be it for production scale-out or incubation trials.

2. CSP Needs for Virtual CPE

Customer premise equipment provides functionality for networking, optimization, and custom value-added services in the enterprise and residential domains. Sites are typically equipped with physical appliances to deliver routing, NAT, DHCP, FW, tunneling, and WAN optimization, and they are augmented with value-added services such as DPI, security, malware detection, media cache, telephony, and STB, to name a few.

Traditional approaches suffer from operational management complexities and agility challenges. Onboarding CPE typically requires elongated sales, deployment, and verification cycles, and operational costs are high. Physical installation of proprietary equipment and complex integrations across a chain of different CPE vendors – compounded by ongoing high-cost truck rolls – have proved to be operationally unsustainable.

Technology advancements with reliable fixed and 5G mobile broadband Internet initiatives are bolstering the hybrid WAN business case for service innovation and enablement. At the same time, the rapid growth of higher bandwidth applications, largely fueled by the explosion of connected IoT devices and business user needs like mobility initiatives, is straining capital spend and expanding operations management costs.

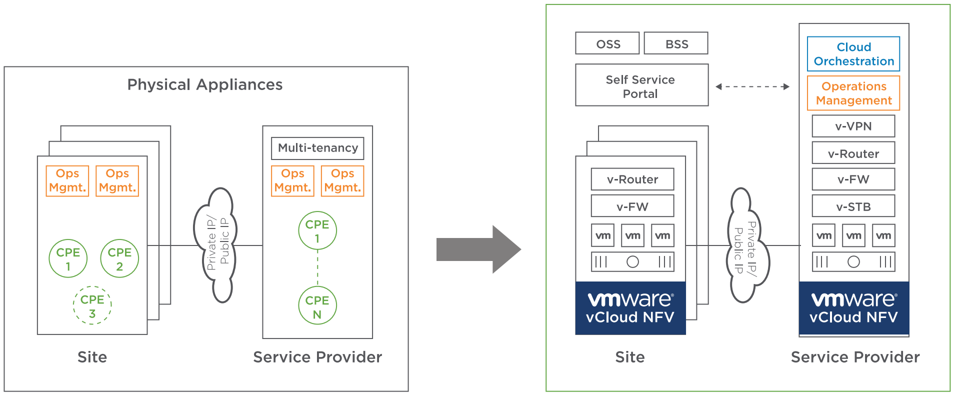
In response to these mounting pressures, CSPs are looking to enable a flexible foundation with software-defined CPE to lower operating costs and introduce innovative new revenue offers. Virtual CPE enables a range of capabilities deemed indispensable to both CSPs and their customers:

- Accelerate new revenues across their enterprise and residential customer base, from networking and security to advanced value-added services.
- Deliver rapid placement and turn-up of new services with multi-vendor VNFs across multi-tenant customers and topologies.
- Dynamically adjust service reliability and availability with auto-scaling and auto-healing.
- Move, add, change, or delete service in a time-efficient manner without errors.
- Accelerate service innovation and delivery for low-cost market entry trials, while scaling up or failing fast.
- Offer enterprise customers a self-service portal to choose and deploy services from a catalog, with pay-as-you-go models and tiered SLA pricing.
- Attain a consolidated, centralized management domain with flexibility for day 1 and day 2 operations, including:
    - Simplified VNF onboarding for application composition and configuration management;
    - Continuous monitoring for service and transport optimization to ensure high QoS;
    - Integrated operations management for timely issue isolation and remediation;
    - Minimal downtime and lower risk for software management.

- Provide networking and connectivity flexibility, not just across physical sites and WAN, but also to secure extensibility for remote users and BYOD end points.
- Open north-bound APIs for service and resource workflow integrations, from BSS/ OSS and network management to fast tracking digital services and omni-channel experiences.

3. Optimizing with Virtualized CPE

CSPs are moving beyond physical CPE to virtualized transformations across their customer base. When thinking of this transformation, the question that comes to mind is whether to virtualize the existing design, implement cloud-based migration with lean remote sites, or consider a mix of the two. With vCloud NFV, the service provider has flexibility to deploy to any topology to optimize and re-balance virtual functions.



vEPC on VMware vCloud NFV

Components of vCloud NFV include a proven NFVI layer with integrated compute, storage, and networking, operations management, analytics, and continuous optimization. vCloud NFV offers:

- Rapid deployment of services with automated VNF onboarding, configuration, and management;
- Advanced overlay networking and service management automation across virtual and physical;
- Centralized and distributed edge aggregation and multi-tenant cloud datacenter topologies for virtual environment orchestration;
- Integrated centralized operations management with built-in 360° single-pane monitoring, analytics, alerts, recommendations, and proactive remediation;
- Open, flexible north- and southbound APIs across a choice of dual VIMs (native vCloud Director and OpenStack) for workflow integrations, service and resource orchestration, and extensible operations management;
- Extensible operational intelligence with fully featured APIs and tools to integrate customized alerts and reporting on system health, and integration of legacy and new monitoring and management applications;
- Multi-vendor VNFs certified by the *Ready for VMware* program.

4. Accelerating Traditional Networking and Communications

Virtual CPE has been the early proof point for service providers looking to transform their business and networks to software-defined and NFV platforms. The goal is to simplify the network connectivity and services across their enterprise and residential customers, and abstract the multi-tenant operations and service management complexities into the service provider clouds. The service provider benefits from both a lowered OpEx and an expanded opportunity to upsell future value-based services with rapid TTM turn-around.

An NFV platform like vCloud NFV with SDN control functions in the cloud is able to orchestrate network functions across the premises, access, service provider, and IT datacenter topologies. Service compositions across the network functions can be distributed across the broader topology or localized within the customer site or centralized datacenter. As such, the following implementation models are attractive use cases for virtual CPE.

Thin On-Premises

This topology minimizes the amount of customer premise equipment installed at the customer edge site while moving all the network functions into the service provider cloud. This scenario is relevant for residential, small business, and remote branch installations that do not require localized traffic and policy control and can withstand higher network latencies with a cloud-backed multi-tenant services infrastructure. A small L2/L3 device at the customer edge is all that is needed to provide basic network connectivity and encryption to the service provider cloud. Network services such as routing, NAT, FW, and DHCP can be moved to the cloud.

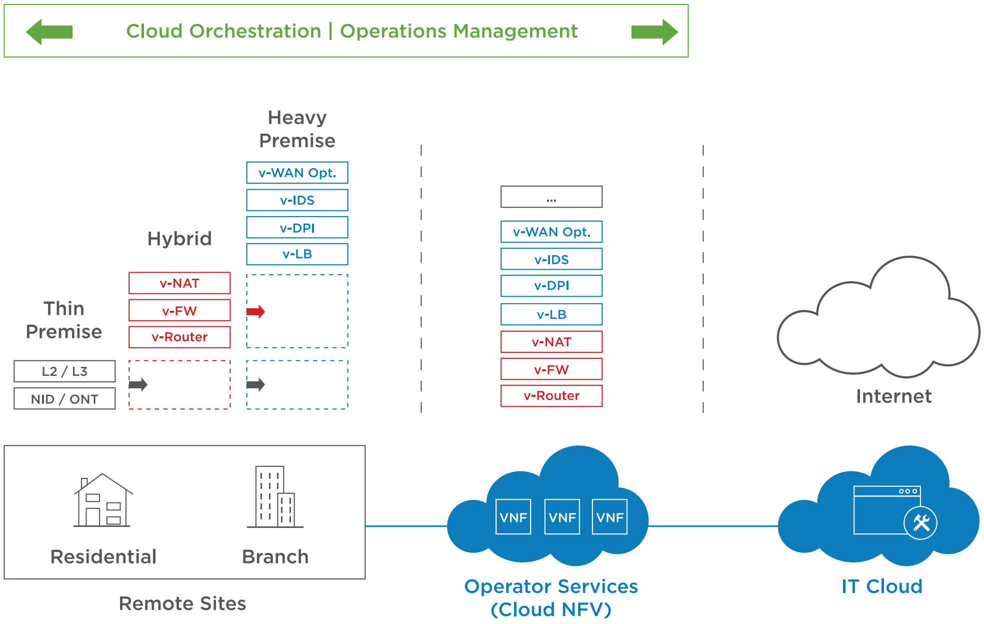
Heavy On-Premises

Larger branch offices that require fully localized traffic and policy control can benefit from this model with service management and operations centralized in the operator cloud. SDN/NFV accelerates VNF provisioning, re-configuration, and service chaining. Onboarding a new offer such as IDS, malware detection, WAN optimization, DPI, or IP telephony can be inserted into the service chain with a self-service construct.

Hybrid

A hybrid of the above two options may be suitable for SMB customers that require basic network and policy control such as routing, FW, NAT, VPN, and DHCP at the branch edge, while other network functions and value-added services can reside in the operator cloud.

The deployment schematic below illustrates flexibility to grow from thin to thick (or vice versa) on-premises model to adapt to the customer needs. In the case of an enterprise branch office, flexible onboarding agility can move or add VNFs to grow with number of users and distributed value-added service needs, such as perimeter security, remote access/VPN, URL filtering, traffic steering, and more.



Flexible deployment architecture across clouds

vCloud NFV makes it possible to deploy flexible topologies with integrated cloud service management, VNF onboarding, security policies, and operations management. The vCloud NFV platform operates over a shared infrastructure and provides the modularity, open APIs, scale, performance, and availability to meet the needs of the service provider multi-tenant ecosystem. With overlay networking, site-to-site and site-to-service-provider networking can be implemented in stretched VXLAN tunnels while perimeter transport security is implemented with edge gateway IPSec and SSL VPNs.

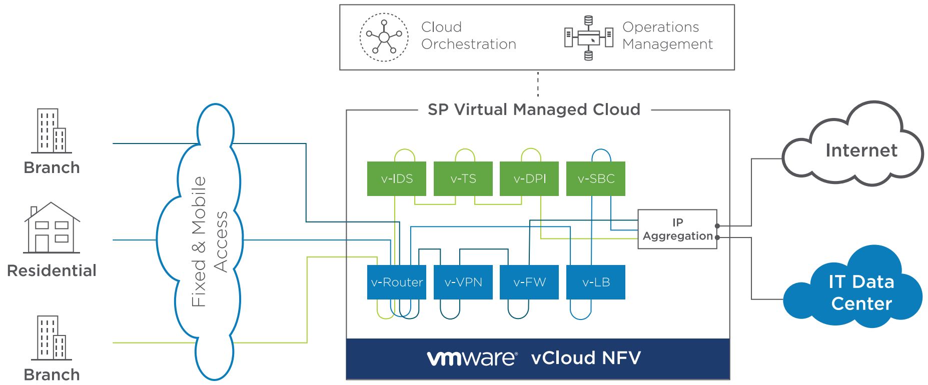
5. Cloud-based Managed Services Potential for CSPs

Virtual managed services offer an excellent opportunity for service providers to accelerate new revenue opportunities to meet the network management and communications needs of their customers. The managed services model also frees up enterprise customer IT and networking resources to focus on business-critical operations and service innovation. The virtualized managed implementation can be deployed either as distributed multi-tenant micro datacenters, potentially employing existing operator's PoP sites, or as a centralized shared datacenter. With the vCloud NFV platform, the cloud-centric operations management and service automation provides flexibility not only to the service provider, but also the enterprise customer to control and implement configurations and policies tailored to their needs.

High-touch sales cycles prohibit service and revenue agility. A virtual managed service business case accelerates pay-as-you-go models and self-service delivery. Cloud-centric service automation and operations management ensures continuous performance and reduces ongoing OpEx spend and expensive truck rolls.

A catalog of VNFs can be made available to an enterprise through a self-service portal, giving the customer flexibility to enable such services at a virtualized edge micro-datacenter or at the service provider's central datacenter cloud. The self-service portal simply turns up a new tenant in the CSP's managed service cloud for the additional service (say, a TV package), starting with the fulfillment workflow to instantiating and configuring the v-STB in the cloud with channel selections. The enterprise customer connects over a secure IPSec tunnel with the vCloud NFV Edge gateway to enjoy the TV service. Further, the CSP can upsell IP voice telephony service in the future, onboarding a v-SBC and perhaps a v-IP-PBX VNF in the managed cloud to provide the private branch voice telephony. Security profiles can be configured at the perimeter, workload, and VM edges to isolate and secure the tenant traffic.

Integrated analytics and extensibility with packet inspection VNFs allow the service provider to conduct traffic analysis using the vCloud NFV platform. The platform continuously monitors traffic to ensure SLAs are being met and optimizes workload placement, scaling, and healing with built-in DRS and vMotion technologies. With traffic analysis via the built-in vRealize Network Insight component or third-party integrated packet inspection, VNF service providers can reveal security vulnerabilities, OTT communications, and bandwidth overages, for example, allowing the CSP to upsell edge or cloud security, HD voice, and other value-added services.



A virtualized managed service cloud with multi-tenant service chains

The multi-vendor VNF and multi-tenant flexibilities with the vCloud NFV platform enable service providers to rapidly compose service chains. Automated VNF onboarding can rapidly drive business value with flexible lifecycle management for a production scale out or fast fail.

6. Advantages of vCPE 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:

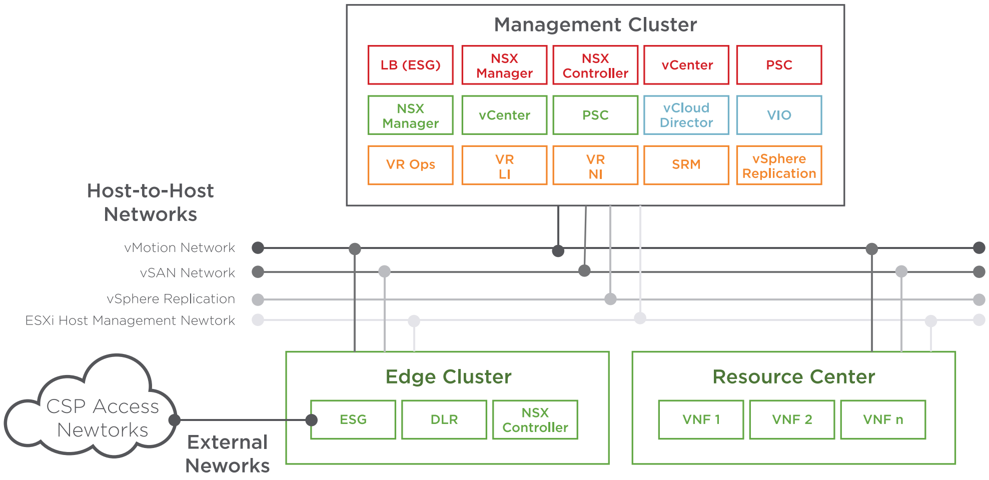
- **Integrated Dynamic Platform:** The VMware vCloud NFV solution is a modular, horizontal, common NFV Infrastructure platform based on ETSI standards. It is built on proven virtualization technologies for compute, storage and networking along with integrated dual multi-tenant Virtual Infrastructure 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 vCPE solution can benefit from resource and edge clusters, deployed at the branch edge and virtualized edge sites, with a centralized management cluster at the corporate datacenter. Service onboarding, configuration, operations, and management can be orchestrated centrally.

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.

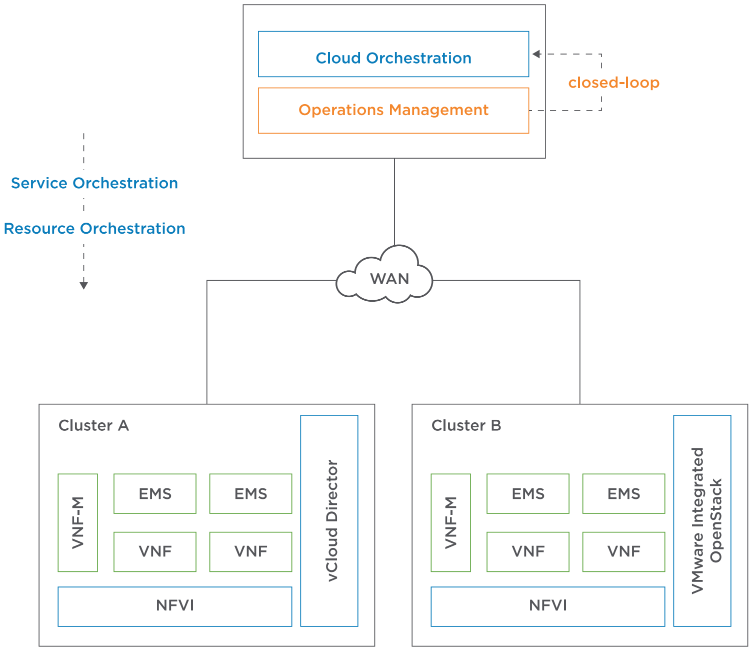
▶ Enterprise branch sites can be transformed to an NFV environment. This maintains the existing IP addressing scheme, creates service segments and network isolation, creates stretched networking between branches for inter-site communications, and secures IPSec and SSL tunneling to corporate and cloud services.

Aggregation sites can benefit from isolated virtual networks to dynamically orchestrate a variety of workloads, performance, and policies across the multi-tenant shared infrastructure environment. Applications, policies, and networking can be bundled in a fully portable package which can likewise be dynamically orchestrated across customers and lifecycle.

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.

▶ vCPE orchestration and management benefits from a northbound standardized API with flexible workflow integration into OSS/BSS, self-service portals, customer NMS, and others.

Service Availability

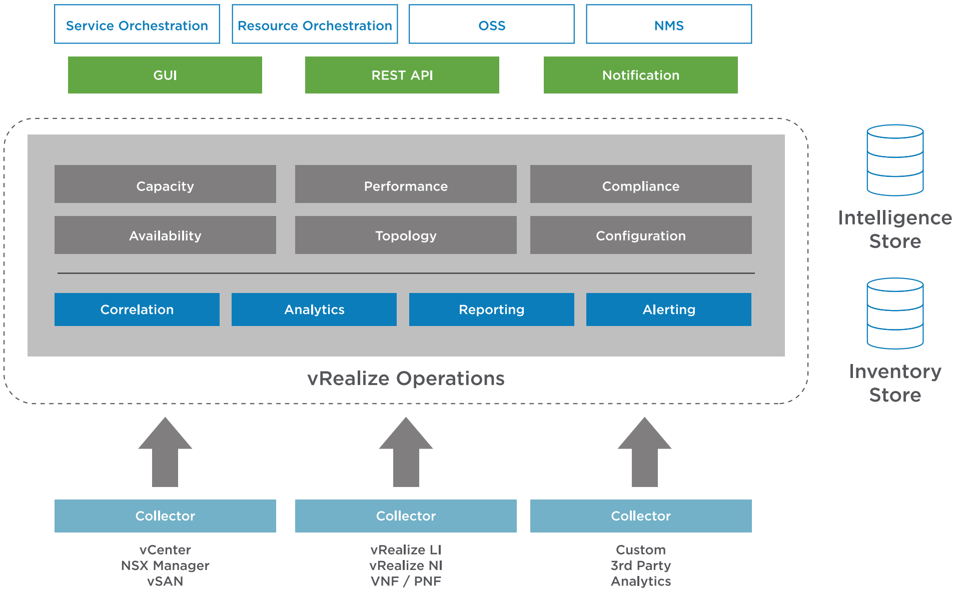
The vCloud NFV platform not only employs a well-thought-out redundancy design using active-active, active-standby, and N+1 architecture principles, it also integrates monitoring for proactive, automated, and semi-supervised service availability safeguards. If all proactive issue-avoidance mechanisms 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.

▶ vCPE and services can benefit from centralized network monitoring, optimization, and issue isolation without costly truck rolls. 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. Enterprises and CSPs benefit from a framework to create new data adapters, KPI computations, alert profiles, recommendations, and custom dashboards, to name a few.

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 vCloud NFV platform allows CSPs to accelerate their vCPE transformation in both residential and enterprise customer deployments, and simultaneously opens up new revenue opportunities through dynamic VNF onboarding service compositions either as pay-as-you-go self-service or fully managed services offers. Because the vCloud NFV platform is modular, extensible, and surrounded by a rich ecosystem of partners, it enables CSPs to quickly enable networking, security, and other value-added service offers with a lower cost of operations through centralized operations management control. Resource elasticity across the infrastructure allows dynamic capacity expansion, without having to over-provision for peak scenarios.

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