TECHNICAL WHITE PAPER – **JANUARY 2017**

VMWARE VCLOUD NFV PLATFORM FOR SOFTWARE-DEFINED WIDE AREA NETWORK

vmware®

Table of Contents

1. Executive Summary

The software-defined wide area network (SD-WAN) is poised to significantly reduce enterprise WAN investment as well as simplify operations. Gartner estimates that by the end of 2019, 30 percent of enterprises will have deployed SD-WAN technology in their branches. Driven by the cost and complexity of existing enterprise WANs and changes in application and cloud usage, multiple sources predict the SD-WAN market will reach $7.5 billion in the next five years. [Arcluster, Rayno Report]

To capture the shift to SD-WAN, CSPs can leverage network function virtualization (NFV), with its inherent agility, service flexibility and elastic scalability, to offer SD-WAN services to their enterprise customers. As a result, enterprises will benefit from simplified and cost-effective wide area networks. CSPs can offer value-added services on top of the SD-WAN connectivity, to increase their service revenue and address enterprise needs as they evolve. By adopting an NFV-based approach to SD-WAN, CSPs have the opportunity to differentiate their SD-WAN offerings to enterprises, providing requisite highly resilient network and security WAN services as configurable hosted or managed service offerings, and service chaining additional value-added services in to the SD-WAN topology.

CSPs face several questions as they assess the SD-WAN opportunity:

- What advantages would SD-WAN solutions built on NFV have to enterprise customers over other types of SD-WAN solutions in the market?
- How difficult will it be to deploy and operate an agile and scalable SD-WAN offering?
- To what extent is SD-WAN service customization and differentiation possible when built on the VMware vCloud NFV platform?

We explore these questions in this paper and provide a technical overview of the SD-WAN service capabilities powered by VMware's vCloud NFV platform. VMware's agile vCloud NFV platform, together with a broad ecosystem of SD-WAN and NFV certified partners, offers additional functionality that allows CSPs to extend their own differentiated, best-in-class solutions to a wide range of enterprises. Furthermore, VMware's support for industry-accepted standards, such as ETSI's NFV framework and VMware's Integrated OpenStack (VIO) distribution, means that CSPs adopting this solution can quickly leverage other industry-accepted NFV building blocks and best practices.

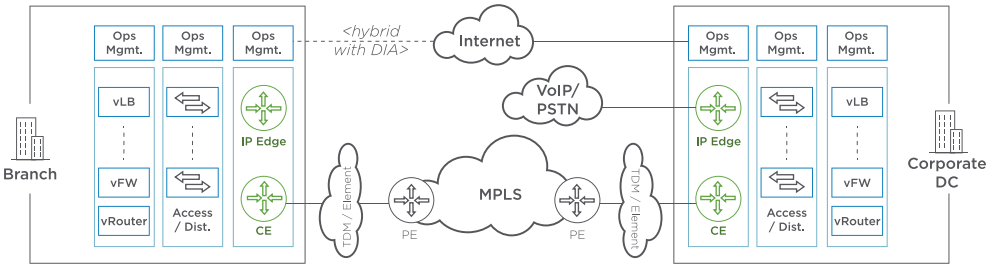
PRESSURE TOWARDS SD-WAN

We are in an age where enterprises are increasingly relying upon applications delivered via SaaS models, including productivity tools like Microsoft Office 365, communication and collaboration applications like Slack, sales products like Salesforce and countless others. Desktop and application virtualization have increased. An enterprise using such tools can not afford to lose its network connectivity, yet it is still pressured to maintain low OpEx.

2. Business Objectives for SD-WAN on NFV

In order to provide a fully meshed network connectivity design, WAN architectures were built on a spoke-hub architecture with compute, security and interconnect functions mostly localized in the central corporate datacenter (DC).

To ensure security, reliability and quality of service (QoS), enterprises have had to rely on costly, inflexible MPLS VPN infrastructure to link branch offices, corporate headquarters and data centers. Meanwhile, IT departments are stretched increasingly thin and have less time to focus on strategic initiatives. Deployment and maintenance of central and branch office network assets has also proven to be labor-intensive.



Traditional WAN and CPE topology example

SD-WAN offers a new approach for addressing these issues by providing improved network performance, reliability, maintainability, scalability and security over traditional WAN architectures.

As CSPs and enterprise customers are looking to derive benefits from the SD-WAN solution, some of the transformation drivers include

1. Freedom from costly, proprietary, and physical appliance vendor lock-in deployments at the branches and corporate DC for connectivity, as well as the on-going maintenance service contract or extensions related to them (i.e. WAN optimization solutions, security and encryption solutions, compression, etc.)

2. Flexible connections from the branches or regionalized NFV-PoPs to optimize cost and balance services across pools of broadband Internet, satellite, cellular and MPLS connections:

   a. Improving network availability and QoS for inter-branch, internet, and UC without incurring MPLS-cost over long-haul connections;

   b. Meeting the needs for capacity demands extending beyond traditional TDM circuits for voice and data;

   c. Flexible mixing and matching of service offers from cloud SaaS providers with those hosted and managed by enterprise IT;

   d. Reducing risk in managing and operating a common centralized traditional core, its configuration, class of services, network optimization, management and troubleshooting;

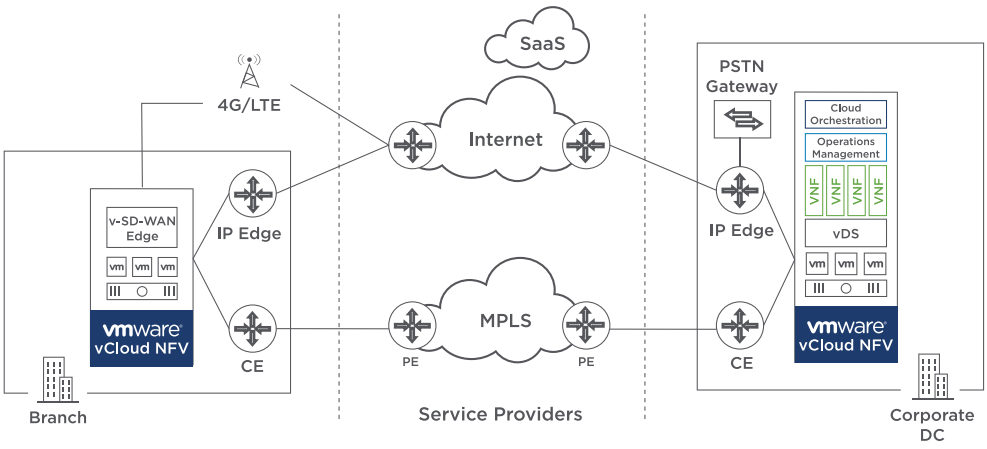
3. Adaptive, software controlled QoS in a fully-meshed architecture without having to build for over-subscription, anticipated peak capacity, highly-available network in a single core, complex traffic engineering, complex configuration management and design, to name a few;
4. Deployment of new services and chains that span the branch edge and corporate data center in an agile manner with flexible disaster recovery options;
5. Flexibility to reallocate IT resources to focus on strategic initiatives through centralized, automatic, dynamic WAN configuration and management;
6. Real-time network monitoring to allow enterprises to improve operational efficiencies in usage-based WAN optimization, issue isolation, remediation, incident reduction, proactive analytics for preventative maintenance, and more;
7. Tightly integrated and centrally controlled security from network edge to application-level granularity, the advantages of which include:
    a. Umbrella security model at the corporate DC, coupled with transport security across edges of the hub-spoke architecture;
    b. Localized security implementation and policies at the branch;
    c. Virtual edge security much similar to the centralized security model, but distributed regionally at the aggregation sites;
    d. Cloud security services offered by SaaS providers, wrapping internet access and policies in the cloud.
8. Ease and speed when onboarding new branches with consistent policy, control and security profiles via centralized cloud orchestration;
9. Agile deployment of new services and compositions at the branch edge or corporate datacenter;
10. Layer 7 traffic shaping capabilities based on dynamic policies based on user, usage, business priority, etc.

VMWARE VCLOUD NFV DELIVERS:

- **Reliability:** Tested, optimized and proven NFVi in more than 70 NFV implementations worldwide.
- **Interoperability:** More than 100 Telecom Technology Alliance Partners and more than 26 Certified NFV Partners through VMware Ready for NFV program.
- **Extensibility:** Ability to extend and unify automation and control in a cross-cloud environment: IT, NFV, public and managed clouds.
- **Operations:** End-to-end operational intelligence and management from physical layer to applications and virtual network functions (VNF)s.
- **Support:** VMware-first Carrier Grade Support for NFV.

3. Accelerate and Automate with SD-WAN

With VMware vCloud NFV, CSPs can quickly customize and deploy a broad range of new services and offerings, allowing their enterprise customers to easily adopt, utilize and benefit from SD-WAN. The service also opens up new revenue streams for CSPs due to the rapid development and deployment of new, value-added services across the network while at the same time increases the "stickiness" of the customers.



Software-Defined WAN transformation

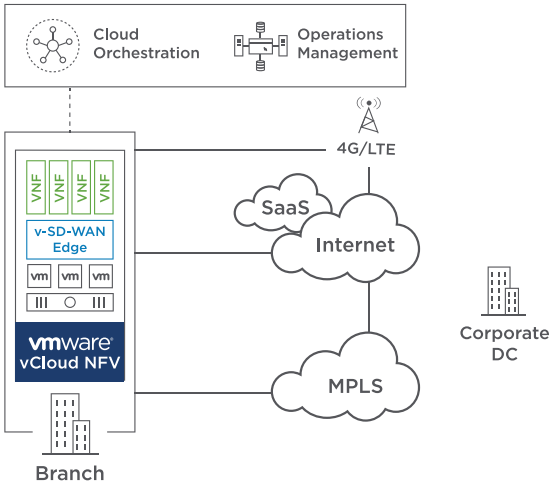
SD-WAN architectures simplify integrating branch and central office networks. Such software-defined hybrid WAN architecture offers an overall cheaper and more scalable model with direct access broadband links to the internet and cloud services, while still maintaining core services that require MPLS or dedicated network transport.

4. SD-WAN Solution Components

There are numerous SD-WAN solutions on the market with a steady increase in new offerings constantly joining the market. Still, most solutions share a common set of components or functions that are fundamental to the successful operations of an SD-WAN service.

Branch Edge

SD-WAN deployment requires an end-point at the branch locations. To keep the cost of the end-point device low, as well as maintaining control over operational costs (e.g. electricity), low-powered servers are used in the enterprise branch. The branch termination point must deliver enough performance to realize the benefits of SD-WAN – intelligent traffic differentiation, security policy enforcement and the ability to add applications or functions to the ones already deployed as part of the service. Branch edge connectivity could be as diverse as DSL lines, direct fiber or even 4G, all of which are supported by vCloud NFV virtualized compute platform of choice.



This design would be suitable for basic edge connectivity or for SME branches with a moderate number of users. With local broadband loops and MPLS connectivity to the corporate DC, the solution provides the flexibility to support applications hosted locally, in the public cloud, and in the corporate DC, all in accordance with criticality, privacy and security needs.

VMware ESXi, the virtualized compute platform in vCloud NFV, supports a range of low-powered CPUs such as Intel ATOM.

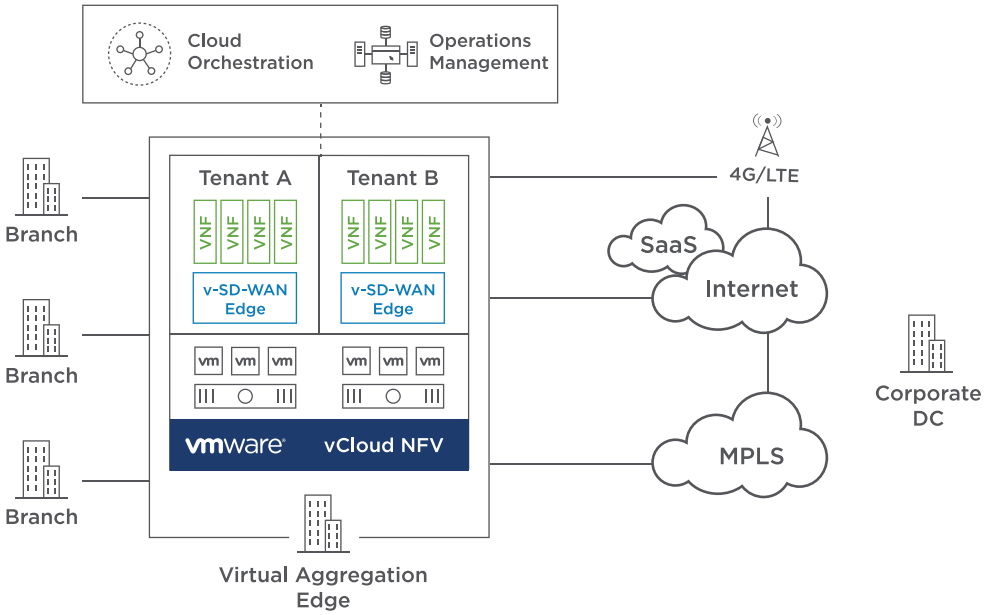
Branch offices must also be managed centrally. In the ideal deployment, a branch will be managed from a regional or central headquarters' IT department, without the need for a network and security administrator at each branch. The branch edge will distribute connectivity based on business policies between direct Internet access connections and the existing MPLS links to the service provider network. For example, corporate applications such as HR and finance could be tunneled through the MPLS VPN circuits or 4G backup loops; cloud applications such as email, web collaboration and sales management connected directly over the internet with user-group security and network isolation; and branch-to-branch video telephony using overlay networking (VXLAN).

The vCloud NFV platform provides the necessary centralized control and resource level management required to deliver this SD-WAN component. Branch edge customizations can be chained with value-added service VNFs such as WAN optimization, content optimization, URL filtering and malware protection. The vCloud NFV platform contains pre-integrated management tools in the vRealize Operations Management suite that grant end-to-end visibility of the VNF deployments, topology and system health.

Aggregation Hub

The aggregation hub could be a regional central location such as the CSP point of presence (PoP) or the enterprise data center. This location serves as the connectivity hub for the branch offices and is likely to already have several IT components running VMware software.

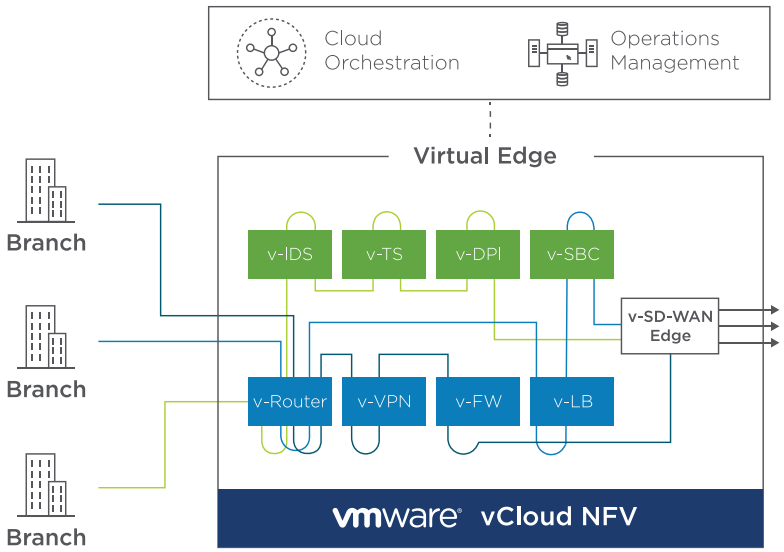
Essential components to the healthy operations of an SD-WAN service, such as an SD-WAN controller and service orchestrator, and, depending on the service, value-added VNFs such as analytics engine, content caching, document management and IP-PBX are likely to be installed here. The aggregation hub approach allows enterprise customers to capitalize on the localized crowding and short-haul low-latency to connected sites.



If the aggregation hub is owned by the CSP, vCloud NFV's multi-tenancy is essential, since several enterprises are likely to connect to this location, enabling branch-to-branch stretched networking, SSL VPN connectivity for remote users, mobile end-points, among other services. Applications such as the SD-WAN controller could be scaled out as more customers are added and protected using the inherent high availability mechanisms in vCloud NFV virtualized compute platform. By leveraging the open APIs in the vCloud NFV suite, it becomes simple to integrate the management and orchestration solution of choice or customize and automate deployments.

5. Extend with Value-Added Services

CSPs can quickly develop, provision and configure new value-added services at any site with seamless, centralized, cloud-based configuration and operations management. For example, CSPs (or their enterprise customers) can rapidly enable such new services either at the branch, aggregation edge or corporate datacenter to meet their business and compliance needs. CSPs can maintain a unique and differentiated SD-WAN offering for each of their customers.



VNF on-boarding and application composition is far simpler and automated to distribute business value as a fast-fail trial or production scale-out. The example illustration shows a virtual aggregation edge site with differentiated service compositions for each branch, ranging in content and traffic management, malware detection, intrusion detection, DPI and SIP trunks.

The vCloud NFV platform's open, modular and extensible architecture circumvents the vendor lock-in and extends service chaining with centralized cloud management. Lifecycle management, performance monitoring, capacity scaling, compliance monitoring, security analysis, issue isolation and recommendations are also built into the platform. When deployed in concert with any number of Ecosystem partners, the door opens to dynamically insert new services without disruption or downtime.

6. Advantages of SD-WAN 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

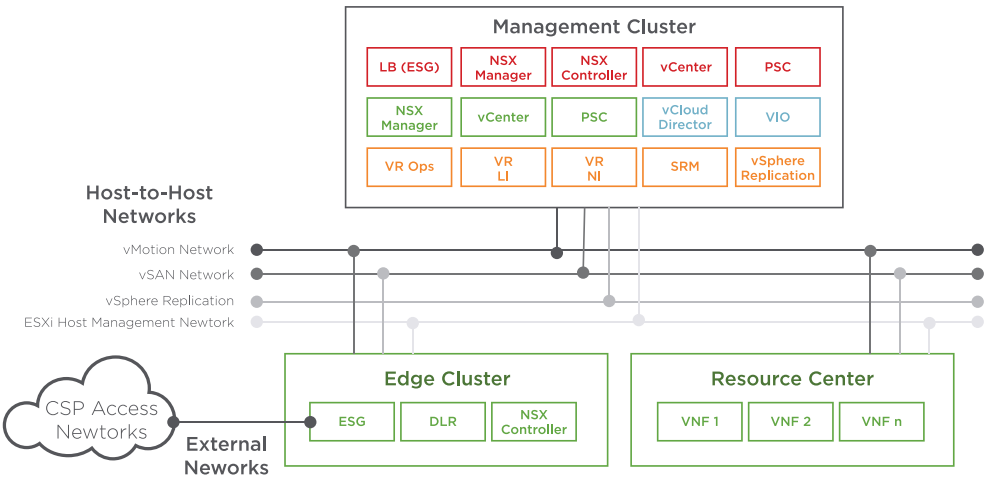
- **Integrated Dynamic Platform**: The VMware vCloud NFV solution is a modular, horizontal, common NFV Infrastructure platform based on ETSI standards. It is built on proven virtualization technologies for compute, storage and networking along with integrated dual multi-tenant Virtual Infrastructure 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.



▶ An SD-WAN solution can benefit from a resource and edge cluster deployed at the aggregation hub, with a centralized management cluster at the corporate DC. Service on-boarding, 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.

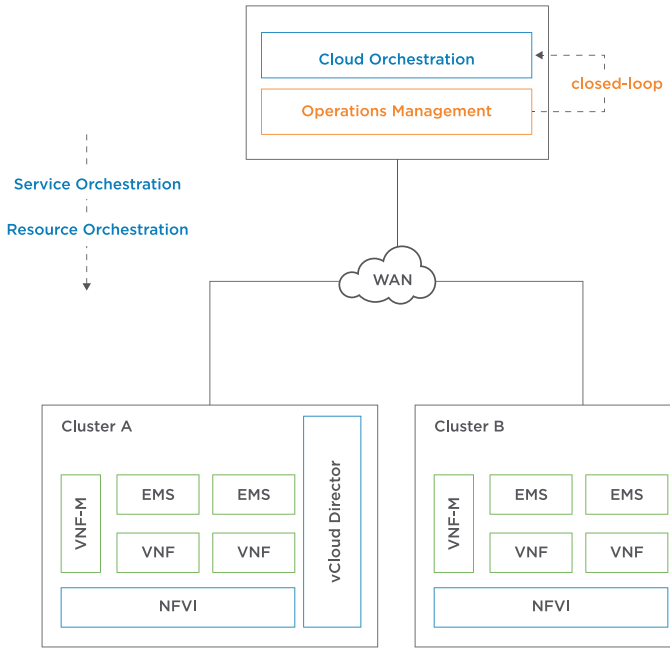
▶ Branch sites can be transformed to an NFV environment. This maintains the existing IP addressing scheme, creates service segments and network isolation, creates stretched networking between branches for inter-site communications, and secures IPSec and SSL tunneling to corporate and cloud services.

Virtual aggregation hubs offer low-latency and proximity services that are better suited to be deployed close to the branches, while global centralized services can be stretched between large corporate DCs.

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 API's 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.

▶ SD-WAN orchestration and management benefits from a northbound standardized API with flexible workflow integration into OSS/BSS and service creation automation. Manage edge sites centrally and minimize truck-rolls.

Service Availability

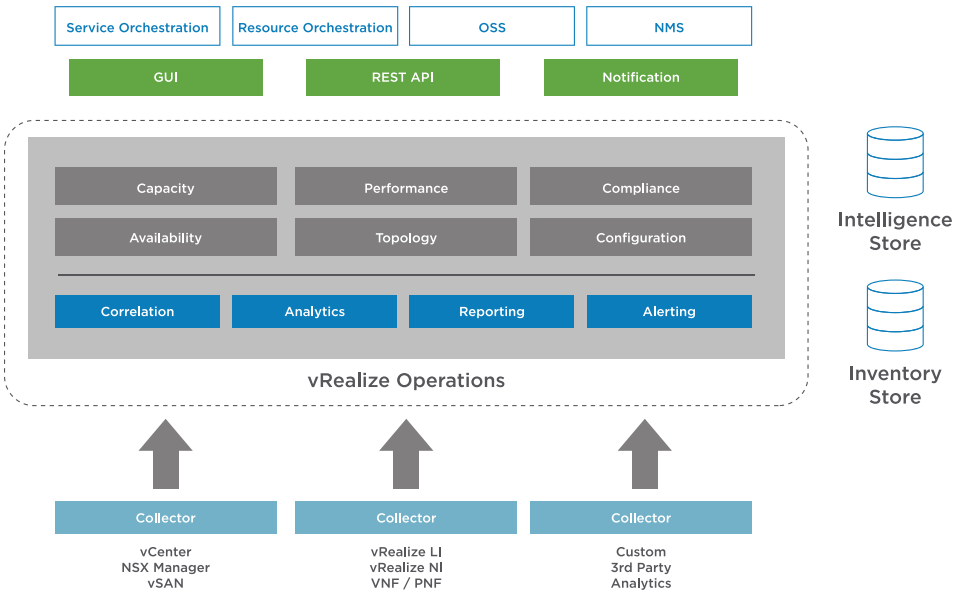
The vCloud NFV platform not only employs a well-thought-out redundancy design using active-active, active-standby, and N+1 architecture principles, it also integrates monitoring for proactive, automated, and semi-supervised service availability safeguards. If all proactive issue-avoidance mechanisms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

▶ SD-WAN 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, recommendation 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

Service localization in the enterprise's core network is now a thing of the past. In order to maximize benefits from the software-defined revolution, the WAN strategy needs to be refreshed. Enterprises have traditionally deployed MPLS-based architectures to meet their needs for connectivity, security, reliability and availability. The needs of the business user have changed – high-speed broadband Internet, cost-effective cloud SaaS application models, user mobility, service innovation, seamless access from any location and so on. SD-WAN is the underpinning to address the needs of this transformation at lower cost and greater flexibility.

The VMware vCloud NFV platform allows CSPs to offer differentiated SD-WAN 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 quickly build, tailor and deploy offerings that meet the needs of their customers. vCloud NFV offers the horizontal platform, with integrated compute, storage, networking and operations management to deliver flexibility, elasticity and agility across the enterprise's dynamic landscape and multi-cloud interoperability.

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