Delivering High Availability in Carrier Grade NFV Infrastructures

VMware vCloud NFV

TECHNICAL WHITE PAPER

vmware®

Table of Contents

Section 1: Introduction

Communication service providers (CSPs) are under pressure from the burden of ever increasing traffic volumes and a need to remain competitive in the face of Over The Top (OTT) providers. As a result there is a need to radically transform network infrastructures in order to reduce operating costs, improve service delivery times and monetize new services. Virtualization of the network infrastructure through Network Functions Virtualization (NFV) and the adoption of cloud-based delivery models are key enablers of this transformation to a more agile and cost effective service infrastructure.

A key requirement throughout this transformation is that services remain 'carrier grade'. Carrier grade can be considered the total ability of the CSP to meet and exceed customer expectations in order to establish customer loyalty and win new business. In the telecommunications industry, if a service is 'carrier grade' it is extremely reliable, well tested and has proven capabilities. By maintaining carrier grade levels of service the CSP brand is protected and enhanced while customer relationships become more profitable through longer and deeper relationships.

Customer expectations and the service specific commitments a CSP is able to provide are typically documented in an end user service level agreement (SLA). These SLA agreements traditionally contain very specific quantifiable metrics for measuring whether or not a service is 'available' at a certain 'quality' to a customer. Failure to maintain the service levels outlined in the SLA agreement results in poor customer experience, low customer satisfaction and in specific cases, a loss of revenue for the CSP through penalties. The accepted industry standard for carrier grade service availability is 99.999%, or 'five 9s' uptime. Since the SLA sets customer expectations, it is also the embodiment of 'carrier grade.' Honoring the SLA therefore becomes the technical challenge that must be solved.

In order to understand how to build carrier grade services in a virtualized environment, it is first important to understand the fundamental principles of virtualized vs. traditional architectures. VMware is the industry leader in assisting customers through this exact transformation – from a rigid system of service-specific silos to flexible, robust and general-purpose infrastructure.

Until recently, mass-market CSP solution strategies were designed to support many customers, and customer types, utilizing a single service infrastructure. This puts great focus on individual physical components since they had to be provisioned to the highest common denominator such as peak load or minimum tolerance of the target customer. This was achieved through highly engineered and expensive proprietary systems that only scaled vertically, and not horizontally.

Virtualization grants the ability to move away from those large proprietary systems, and leverage any number of hardware options. Using Common Off the Shelf (COTS) hardware, in conjunction with software driven processes and an extensive automation capabilities, alleviates the CSP from the need to use proprietary hardware systems while still maintaining the quality of the service. This approach turns the physical platforms used to deliver services into pools of compute, network and storage resources ready to support any service. Automation and resource sharing inevitably changes the methodology of delivering key 'carrier grade' attributes such as exceptional service availability, performance, security and manageability.

Regardless of the platform used to deliver services, customer expectations put on the CSP, be it mobile, fixed or hybrid, remain the same. The service must be 'carrier grade'. As the leading virtualization vendor, with 18 years of practical experience, VMware is often asked by CSP customers "can a five 9's end-to-end service availability be met using virtualized infrastructure?" In this white paper we explain why we always answer this question with a definite yes. We also share our experience that when implemented correctly, service resiliency will not only enable a CSP to maintain and improve SLAs, it will also support OpEx reduction and regulatory compliance.

Section 2: Principles to Achieve High Availability in NFV

In a complex NFV cloud environment, individual system components, such as network interface cards or storage adapters, do fail. In a virtualized infrastructure, ensuring that every such component delivers five 9s of availability is cost prohibitive and unnecessary. Ultimately it is the end-to-end availability of the service from the customer perspective that is most critical and linked to service guarantees. Failure of an intermediate component or process can be tolerated provided the impact on the end user service is within the 5 nines of SLA. By driving the appropriate level of availability at each layer within the architecture, the cost benefits of virtualization are maximized without compromising the five 9s overall service availability requirement.

Carrier grade services require the infrastructure they run on to be highly available. In order for an infrastructure to have optimal, predictable and sustainable uptime, this system must be able to survive a component failure, be proactive in knowing which and when a failure is likely to occur, as well as be able to balance workloads across the entire infrastructure to reduce any hot-spots or bottlenecks. These capabilities can be summarized as:

- **Redundancy**: Eliminate any single point of failure with the optimal amount of redundant capacity
- **Intelligent Placement**: Optimize the placement of workloads to avoid the over-utilization of resources or to enforce anti-affinity or affinity policy (ensuring workloads are physically separated or co-located as required by the Virtual Network Function (VNF))
- **Predictive Analytics**: Identify the potential failure conditions before they cause disruption so that (automated) preventative action can be taken

If a failure has occurred, it is vital to recover the service to an active state and to reach a state of redundancy for the new configuration in the shortest time feasible. Mitigating failures quickly ensures that SLAs are maintained and analysis of the issue is provided in order to satisfy reporting regulations and improve the system:

- **Detection:** A failure must be detected rapidly at every level of the system including application, virtual infrastructure, and hardware.
- **Event correlation:** It is likely that any given failure will generate multiple errors, just as in a physical architecture. The system must be able to identify the root cause of any failure and filter out unwanted noise effectively.
- **Remediation:** Policy-based automated processes must be capable of recovering the system to a state of availability with limited or no human intervention. This reduces the time to recover and mitigates the risk of human error.

When creating highly available NFV services using VMware technology, the 6 pillars described above will ensure that SLAs are maintained, while operational expenditures (OpEX) are kept to minimum. The following sections dive into these VMware specific features and functions in details.

Section 3: Achieve High Availability with VMware vCloud NFV

As the leading virtualization platform in the world, it was natural for VMware to create a solution to address the requirements so clearly specified by CSPs in the European telecommunications Standards institute (ETSI) NFV Industry Specification group (ISG). The solution, called VMware vCloud® NFV, is a horizontal, multi-tenancy NFV infrastructure (NFVi) which includes an entire virtualization stack, Virtualized Infrastructure Manager (VIM) and a robust set of CSP-oriented operations and management elements. Figure 1 depicts vCloud NFV components within the ETSI reference model.

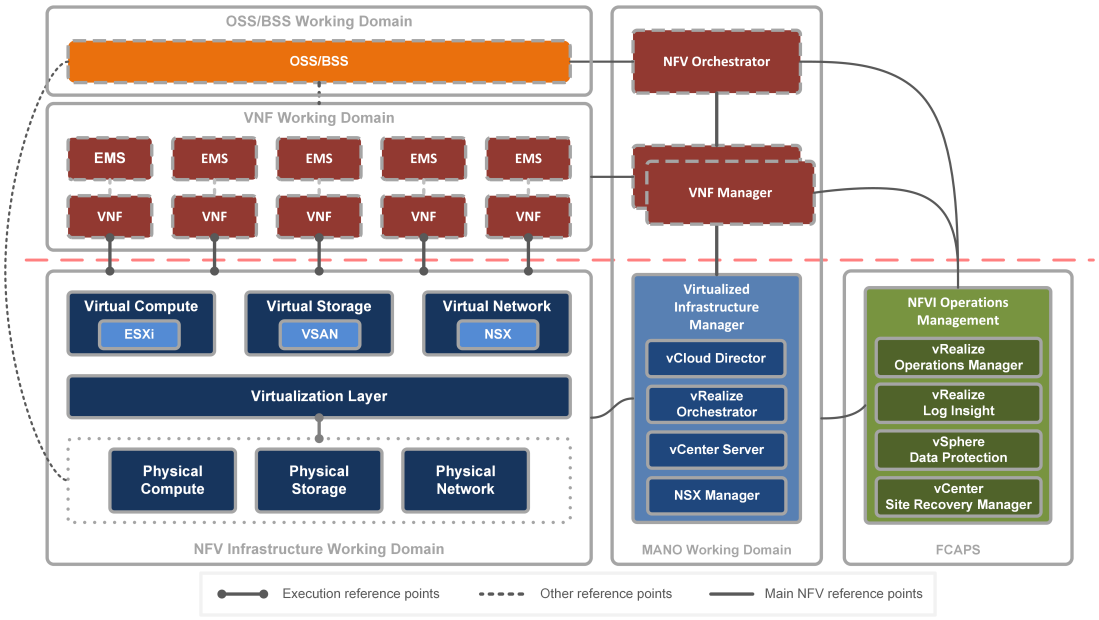

Figure 1: vCloud NFV and its place in the ETSI NFV Architecture Framework

VMware has worked with many customers in areas such as finance, military, government, aviation, and mission critical business services for whom high availability is business-critical. By leveraging the inherent capabilities of a virtualized infrastructure, as well as building on the operational experience gained from deploying the components that make up vCloud NFV, VMware has developed a set of capabilities designed to ensure exceptional service availability detection, redundancy, predictive analysis, intelligent placement, event correlation and remediation. Using these capabilities the CSP is able to maintain longer mean time to failure and shorten the mean time to repair, therefore, providing exceptional availability to its customers.

Section 3.1: Redundancy

Redundancy is at the cornerstone of the vCloud NFV platform. Deploying redundancy in components ensures that the system is able to maintain operations in the event of a failure or component fault. Once a highly redundant system has been established it can be further enhanced using predictive analytics and intelligent placement of resources.

In figure 2 below, we see the infrastructure stack divided between three distinct planes. The vCloud NFV architecture realizes these planes as three unique clusters: The management cluster for the VIM components and operations management components; the edge cluster to contain the virtual network components; and finally the resource cluster to host the tenant VNFs. Redundancy is built at all layers of the architecture.

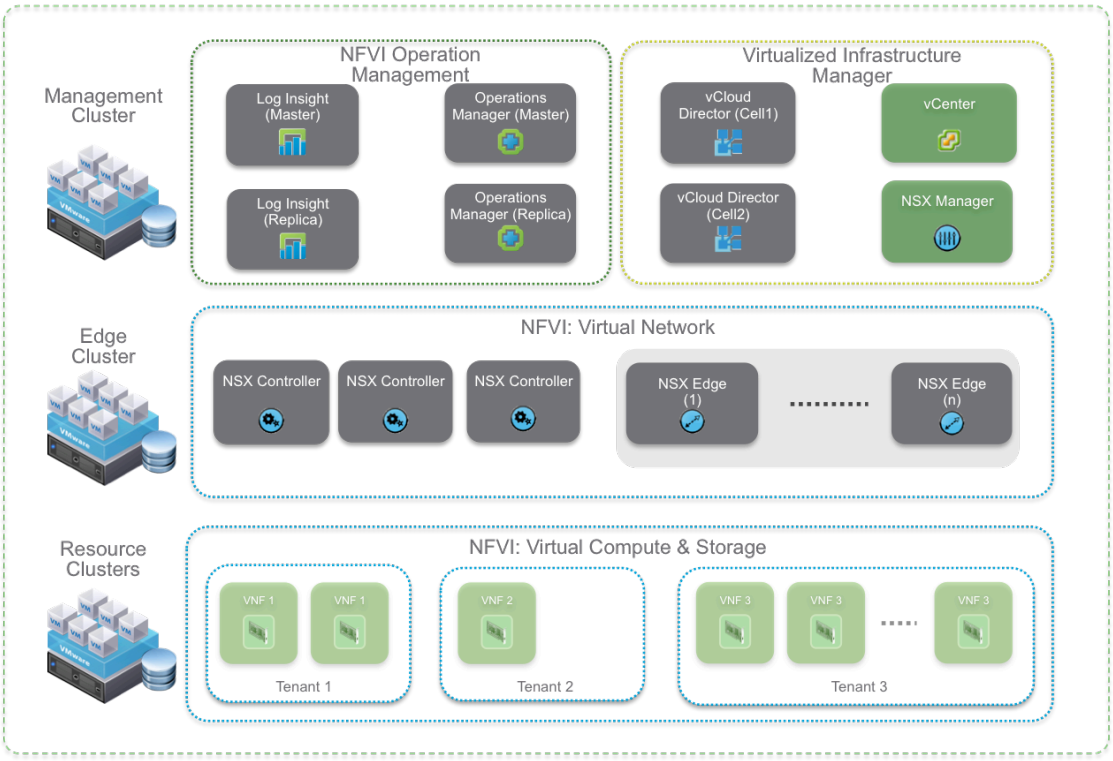

Figure 2: vCloud NFV Architecture

Compute Resources

Starting from the most fundamental element in the stack, vCloud NFV architecture guidelines dictate redundant hypervisor deployment. This enables Virtual Machines (VMs), the elements that run the VNF applications, to be always on. Architecting for redundancy means that if a VMware ESXi™ Server host fails, neighboring hypervisors configured in the same VMware vSphere® cluster (a group of hosts) are able to continue offering the virtualized layer without adversely impacting the VNFs. The physical hardware becomes a highly available resource pool managed by the cluster.

In order for a service to be fault tolerant, the VNF applications deployed in this shared resource pool must also be built with application level redundancy. In support of this, the vCloud NFV platform leverages the production-proven VMware vSphere® High Availability mechanism to restore redundancy. As show in Figure 3 below, in the event of a physical server failure, the VM running on the affected server is impacted, but the

other VM instance in the application redundant pair continues to function. Since only 1 VM instance is running at this point, the overall system is no longer redundant. vSphere HA automatically detects this failure and restarts the affected VM on one of the remaining servers within the cluster that has spare capacity. This minimizes the window of time during which the VNF application availability is degraded and restores redundancy, thus protecting the system from further failure. The vSphere HA Admission Control policy is used to ensure that sufficient resources are available in a cluster to provide failover protection, eliminating the need for human manual intervention. The platform can also detect operating system failures and be configured to restart a VM in the event of an internal VNF failure. vCloud NFV platform also comes with a full suite of API interfaces that VNF providers leverage to trigger events like standby-activation, new VM instantiation and more.

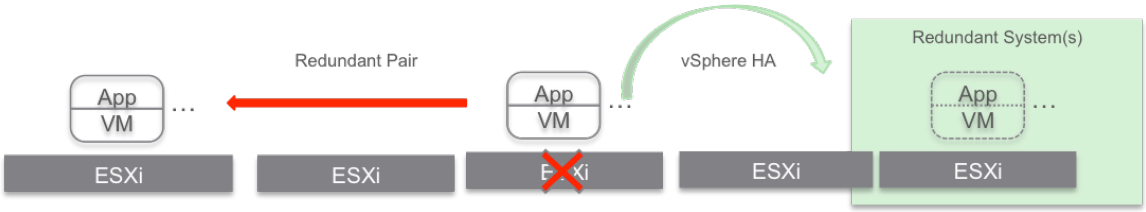

Figure 3: Application Fault Tolerant with vSphere HA

Where it is applicable and compatible, a VNF could be deployed with higher levels of availability than offered by vSphere HA by utilizing VMware vSphere® Fault Tolerance. vSphere FT provides availability by creating and maintaining an identical copy of a VM that is ready to replace it in the event of a failure. The protected VM, is referred to as the primary VM, and the duplicate, the secondary VM is created on a separate ESXi Server host, such that in the case of a physical server failure, the secondary VM is immediately activated to replace the primary VM. Following failover a new secondary VM is automatically created to reestablish vSphere FT redundancy. vSphere FT is performed without the knowledge of the operating system running in the VM and without breaking any of the network connections.

Networking

For connectivity, redundant network connections are established from each hypervisor (in VMware terminology, Network Interface Card (NIC) Teaming), such that if the underlying physical network experiences issues, connectivity is still maintained. NIC teaming can use both link status failure or specialized beacon probes to detect conditions in which the link still remains in an 'up' state. When an interface in a NIC team recovers, failback policies are automatically applied. These allow the operator the flexibility to decide if recovery should result in a revertive mode and if certain links should only be used as standby.

The network layer in the vCloud NFV platform is virtualized using VMware NSX® for vSphere®. All aspects of the data center and site networking are protected and are made highly available. The VMware NSX® Controller™ is always deployed in clusters of three (or higher) to maintain control plane redundancy. NSX for vSphere supports several standardized protocols, such as Equal-Cost Multipath (ECMP), Graceful Restart, and Multi-Chassis Link Aggregation Group (MC-LAG) among others to provide highly redundant connectivity. Furthermore, the data plane traffic is architecturally separated from the control plane traffic. Any failure occurring in one plane does not impact the other plane. Network traffic is also prioritized to avoid service failures in peak scenarios where the network may become congested..

Storage

VMware has a wide variety of ecosystem partners with storage solutions that work effectively with the vCloud NFV platform, that are capable of supporting highly available carrier-grade architectures. While it is possible to use any of the VMware supported storage vendors, this white paper focuses on the capabilities of VMware Virtual SAN™. Virtual SAN is a Software-Defined Storage (SDS) solution and offers several

benefits over traditional storage solutions. These include, but are not limited to:

- **Simplicity and Efficiency**: SDS, similarly to server virtualization, abstracts underlying storage allowing storage to be managed and adjusted as needed on a per VM, and hence per application, basis.
- **Policy-based Management:** Storage requirements such as performance and availability can be defined as a series of policies that can be applied to VMs, as they are created.
- **Rapid changes:** Leveraging abstraction and policy-based management, admins can dynamically change storage characteristic to match application demand.

Virtual SAN is fully integrated with vSphere. It aggregates local disks from ESXi Server hosts, that are members of a vSphere cluster, in to disk groups to create a distributed shared storage solution. Distribution of storage across multiple ESXi Server hosts, facilitates simplified scaling through an increase in the cluster size and an increase in the number of disk groups.

In order to ensure redundancy Virtual SAN includes a policy called 'Number of Failures to Tolerate', which defines the requirement for how many concurrent host, network or disk failures that can be tolerated within a vSphere cluster while maintaining availability. This policy ensures that 'Number of Failures to Tolerate' +1 replicas of any given object are created. In addition Virtual SAN supports the concept of Fault Domains. Fault Domains provide support for rack or chassis awareness, such that new VMs are deployed with replica objects distributed across fault domains, mitigating the risk of data loss in the event of a localized rack or chassis failure.

The final compelling feature of the Virtual SAN component of the vCloud NFV platform is how tightly it is integrated with the operations management component such as VMware vRealize® Operations Manager™. In the event of a failed VM, a clone can be provisioned and imaged automatically. All of these features combine to add a highly available storage solution to the vCloud NFV platform.

Management Cluster

By design, the management cluster, where the VIM and operations management elements reside, is physically and logically separated from the compute resource and virtual networking clusters. This means that any failure within the management cluster is well contained and does not impact the compute resources where the VNFs reside. In addition to the availability features of vSphere HA and, where appropriate, vSphere FT, management and operations components support additional application-level resiliency.

In order to increase availability and scale, VMware vCloud Director® is deployed as a load-balanced pool of multiple vCD cells. In combination with a load balancer that supports session persistence, it is possible to ensure the smooth continuation of operations should one instance fail or become unresponsive.

VMware vCenter™ Server deployment model includes a watchdog that monitors for any failed services and attempts to automatically restart them if required. Similarly, it is possible to protect against vCenter database failure through the use of technologies such as Microsoft SQL Server AlwaysOn and Database Mirroring.

Both vRealize Operations Manager and VMware vRealize® Log Insight™ are setup in a cluster mode. Both configurations facilitate speedy failover from master node to redundant node. Data is backed up to ensure exact copy is always available.

Section 3.2: Predictive Analytics and Intelligent Placement

Complementing our strong redundancy principles are the two management-level pillars: *predictive analytics*

and *intelligent placement*. Predictive analytics is the proactive examination, monitoring and telemetry data collection, gathered from all elements in infrastructure to make informed decisions to identify potential risks and issues before they become failures. Once the system can predict certain conditions such as utilization and service quality, it can also place workloads in safe areas intelligently.

The two capabilities are tightly coupled enabling the management layer to detect potential issues, based on heuristics as well as machine learning, to migrate VNFs out of harms way before issues occur. From a service operations perspective, the first view into the health, risk and efficiency of the vCloud NFV platform is vRealize Operations Manager – a robust NFVi fault, capacity, audit, performance and security (FCAPS) solution. vRealize Operations Manager constantly collects performance metrics from every element in the system: from low-level metrics such as CPU utilization, disk I/O, network throughput and memory utilization, to availability, communication patterns as well as user-defined metrics. This extensive data collection empowers the carrier to increase the system uptime by preemptively detecting health, risk, abnormalities and efficiency issues. These metrics can also be summarized as custom dashboards so that customers can view only those metrics that are important to their particular implementation.

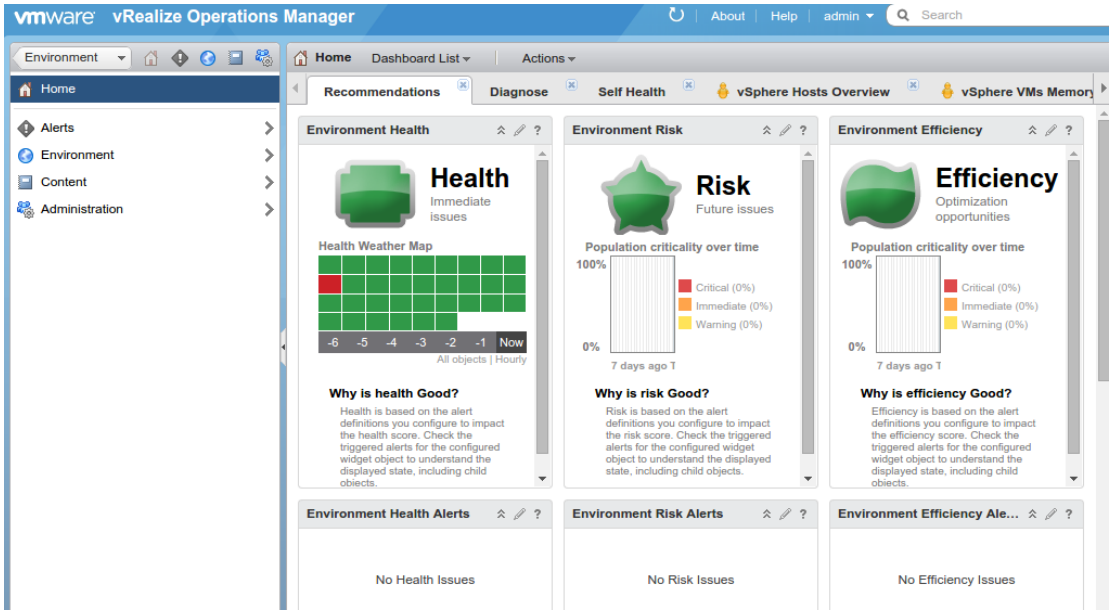

Figure 4: vRealize Operations Manager

Since the system is constantly monitoring the NFVi, as well as the VNFs, it is able to learn and define what the normal operating bands are by analyzing historical data over time. vRealize Operations Manager can then alert the operator to abnormal behavior, be it under utilization or overutilization. This is a fundamental function of a monitoring system that every operator depends on for healthy infrastructure and services management.

vRealize Operations Managers functionality is easily extended and expanded in the case that certain network functions are spread across a collection of VNFs. There are plenty such examples in the ETSI NFV use cases: virtual Evolved Packet Core (vEPC), virtual IP Multimedia Subsystem (vIMS), virtual home environment, and fixed access network functions. Each of these is typically constructed using a collection of VNFs that could be grouped to form “application VNF aware” dashboards. Events and trends impacting the group are then reported and acted upon using vRealize Operations Manager. In this way, the vCloud NFV platform enables powerful and customizable operations’ dashboards to be created for 3rd party applications and services running on the platform. This is an immensely powerful operations tool. The dashboards ability to have a holistic view, reporting health, risk and efficiency state on your virtualized network functions, as opposed to just a collection of virtual machines, allows your operations team to focus on revenue generating

applications, in their networking domains of expertise, and only dive into the underlying layers when and if problems arise.

By monitoring the entire NFVi, vRealize Operations Manager creates a holistic view that enables not only predictive analysis, but also intelligent placement. vRealize Operations Manager not only identifies the stress points in the infrastructure, but also the locations where capacity, CPU, memory, disk and network are ample. The system can then associate VNFs, hypervisors and clusters into one of three categories: underutilized, optimal, over utilized. Workloads can be rebalanced, removing stress from the system and reaching more optimal utilization. This activity can be semi or fully automated depending on the degree of operator intervention desired.

Anti-Affinity is another resource placement capability provided by the vCloud NFV platform. To achieve high availability, VMs inside a VNF application are often configured in redundant pairs. These redundant VMs must be deployed in such a way so that they are not brought down at the same time by a single hardware failure. The vCloud NFV platform supports the configuration of the anti-affinity policies which ensures these VMs never exist on the same physical server. The complementary method is of course, affinity rules. Such rules ensure that VMs that must be placed in specific proximity are indeed kept together. This, for example, could be the case where network traffic between two VMs is high, and both VMs may need to be placed on the same host to minimize the network latency and potential failure points between them.

With all the different elements in the vCloud NFV platform providing mechanisms to quickly recover from failure, achieving carrier grade redundancy is a reality. The five 9s that have been defining 'carrier grade' availability since data networking became a mass market product, are attainable even when some of the underlying components might offer availability of less than five 9s. In the vCloud NFV platform, the end-to-end CSP application availability is maintained using strong redundancy principles in the architecture as well as active-active application level high availability - a capability that is only available in virtualized environments.

Section 3.3: Detection, Correlation and Remediation

Detection of Failures

While every measure could be taken to architect the NFVi, MANO and Operations Management domains for maximum uptime, it is a fact that hardware, data centers, central offices (COs) and components do at times fail. To minimize the impact of failures, designing the system to rapidly detect, contain and recover is key. Detecting, containing and recovering from faults quickly also means that for certain services, no degradation is noticed at all. These design principles are realized through a sophisticated and comprehensive set of alarm, alert, and event reporting capability of the vCloud NFV platform.

In addition to tying in to the vRealize Operations Manager API, VNFs can also use VMware vRealize® Hyperic®, an optional component of the vCloud NFV platform. It is a client-server, multi-vendor, cross platform-monitoring tool for both applications and infrastructure. Using Hyperic Agents to gather performance and availability metrics, enables control functions such as starting and stopping servers, complete run-book deployment automation and more. Agents send the inventory and performance data they collect to a central Hyperic server.

The fundamental NFVi elements in the vCloud NFV platform, storage, compute and network, are constantly monitored. Every virtual object (such as CPU, RAM, vNIC, switch, port, storage link, etc) can be monitored, and alerts and alarms can be defined and raised through SNMP to send traps to an existing monitoring system.

Event correlation

In the event of a failed component, it is typical for multiple errors to be generated. The vCloud NFV platform has the capability of intelligent event correlation to finalize root cause analysis and take action sooner. A

key component in that respect is vRealize Log Insight. This application digests all of the log data across the entire NFVi sorts and correlates all of the relevant logs and displays only that information that is important to the operator. vRealize Log Insights also works in concert with vRealize Operations Manager to make decisions regarding failures and remediation recommendations.

Remediation

By leveraging the capabilities of the vCloud NFV platform, operators gain the capability to have the infrastructure make decisions and take recovery actions with minimal or no intervention. This effectively creates a self-healing infrastructure. While completely automating failure recovery may not be appropriate for every VNF, in the event a failure does occur, the failure origin is clear and in almost all instances, the operator receives a recommendation on how to resolve the issue. Thus, recovery time is minimized, the operations team is able to benefit from the experience and ensures that similar issues will be handled quickly or completely mitigated in the future.

Section 4: Summary

VMware has taken the capabilities of the standard NFV infrastructure and added components and features to create a truly 'carrier grade' solution. vCloud NFV has the ability to deliver the availability that CSP's demand in a stable, tested and integrated platform. Creating an NFVi that is both multi-vendor capable, robust and provides exceptional availability can only be done through extensive operational experience. Supporting mission critical business services that emphasize high availability can only be done well when error detection and redundancy principles are deep-rooted in the system and are complemented by additional capabilities such as intelligent placement, predictive analytics, event correlation and remediation. VMware has created a robust NFVi solution based on over a decade of experience which displays that when implemented correctly, exceptional availability will not only enable a CSP to maintain and improve SLAs, it will also support OpEx reduction as well as regulatory compliance.

References

[1] vCloud NFV Reference Architecture
https://www.vmware.com/resources/techresources/10515

[2] vSphere Availability
http://www.vmware.com/files/pdf/VMware-High-Availability-DS-EN.pdf

[3] VMware NSX for vSphere Design Guide
https://www.vmware.com/files/pdf/products/nsx/vmw-nsx-network-virtualization-design-guide.pdf

[4] VMware API and SDK Documentation
https://www.vmware.com/support/pubs/sdk_pubs.html

[5] VMware Fault Tolerance
http://www.vmware.com/files/pdf/VMware-Fault-Tolerance-FT-DS-EN.pdf

[6] VMware vCenter Server 6.0 Availability Guide
http://www.vmware.com/files/pdf/techpaper/vmware-vcenter-server-availability-guide.pdf

[7] VMware Virtual SAN 6.0 Scalability and Best Practices
http://www.vmware.com/files/pdf/products/vsan/VMware-Virtual-San6-Scalability-Performance-Paper.pdf

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