Run CNFs on Virtual Machines To Optimize Your 5G Networks

The Synergy of Combining Containers and VMs Delivers Security, Management, and Automation

"Although containers are sometimes thought of as the next phase of virtualization, surpassing hardware virtualization, the reality for most organizations is less about revolution than evolution. Containers and hardware virtualization not only can, but very frequently do, coexist well and actually enhance each other's capabilities. VMs provide many benefits, such as strong isolation, OS automation, and a wide and deep ecosystem of solutions. Organizations do not need to make a choice between containers and VMs. Instead, organizations can continue to use VMs to deploy, partition, and manage their hardware, while using containers to package their apps and utilize each VM more efficiently."

APPLICATION CONTAINER SECURITY GUIDE, NIST SPECIAL PUBLICATION 800-190

Satisfying Telco Requirements for CNFs and 5G Services

CSPs are turning to containers to streamline and scale the deployment of network functions and 5G services. A container wraps a network function in a consistent, portable package that can be independently distributed and modified with little effort and few or no dependencies. Containers then run on a host operating system and share its kernel. The host operating system resides on either a virtual machine (VM) or a physical server.

Containers and a microservices architecture make it easier to independently deploy, modify, and maintain network functions. A container orchestration system—typically Kubernetes—automates the deployment and management of containerized functions and services at scale.

Cost-effectively putting containerized network functions (CNFs) into production hinges on your ability to secure, manage, and automate them at scale in an efficient and integral way. Running containers on VMs by using VMware Telco Cloud Platform establishes the perfect catalyst for efficiently and securely operating CNFs at scale.

Combining containers and VMs produces a powerful synergy that taps the benefits of both technologies. Virtual machines solve infrastructure-related problems by better utilizing servers, improving infrastructure management at scale, streamlining IT operations, and isolating resources for security. These are some of the reasons why the major public cloud providers use hypervisors and VMs to run containers.

Containers solve application-related problems by, among other things, streamlining DevOps, fostering a microservices architecture, improving portability, and further improving resource utilization.

Virtual machines let you securely and efficiently run containerized functions and 5G services on software-defined infrastructure that you can easily manage, monitor, scale, automate, and optimize. Bare metal servers, in contrast, can root existing monolithic stacks in place and, in a multi-vendor environment, create silos, making management, automation, and maintenance difficult. Adding CNFs and a container orchestrator like Kubernetes to a multi-vendor bare metal environment can compound complexity and further complicate management.

Hardware virtualization was originally developed to address the pain of working with physical hardware, pain that ranges from time-consuming management problems and cash-consuming underutilization to the difficulty of scaling hardware for an elastic workload. By optimizing utilization and simplifying management, virtualization reduces physical hardware costs while improving scalability.

THE SYNERGY OF CONTAINERS AND VIRTUAL MACHINES

VMs solve infrastructure-related problems by better utilizing servers, improving infrastructure management, and streamlining IT operations.

Containers solve application-related problems by streamlining DevOps, fostering a microservices architecture, improving portability, and further improving resource utilization.

Running containers on VMs produces a synergy that helps CSPs transition from 4G to 5G networks with ease.

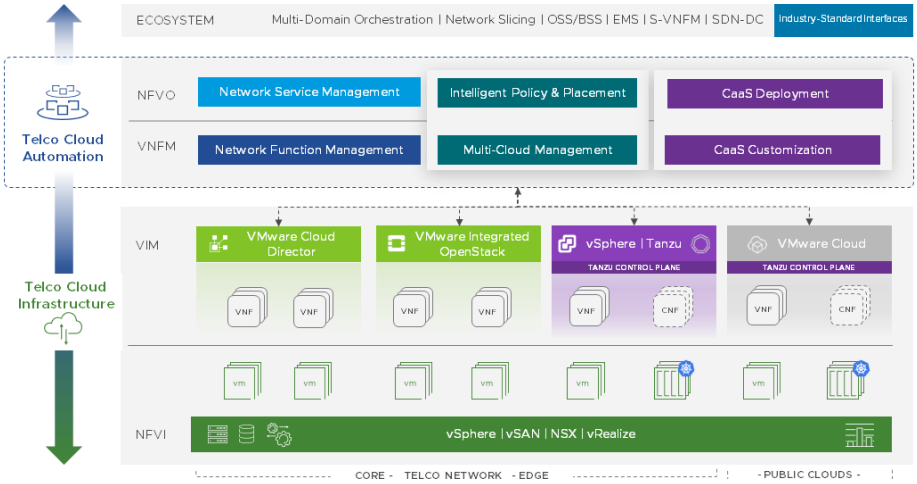

FIGURE 1: VMware Telco Cloud Platform includes VMware Telco Cloud Automation and VMware Telco Cloud Infrastructure. These products work together to run and manage CNFs and containerized 5G applications on consistent horizontal infrastructure.

For CSPs, performance, security, and management are key factors.

- Studies show that optimizations in the vSphere CPU scheduler for NUMA architectures quash the belief that running containers on VMs comes with a performance tax.
- Noisy neighbor situations can cause interference for co-located containers on physical hardware, and cross-container interference can result from containers sharing the same kernel resources or components.
- Kubernetes on bare metal is unlikely to outperform Kubernetes on VMware vSphere, which uses advanced scheduling algorithms to optimize all workloads. A recent test of vSphere 7 with Kubernetes shows better performance compared with a bare-metal Kubernetes node because the VMware hypervisor does a better job at scheduling pods on the right CPUs, thereby reducing random memory accesses.
- Containers alone are inadequate security boundaries; containers do not establish security boundaries and strong isolation as VMs do.
- Running CNFs on bare metal would create a complex patchwork of bolted-on security controls and tools. In contrast, running CNFs on VMs lets you impose security by using built-in mechanisms that can be managed at scale without silos.
- Running containers on physical hardware would resurrect difficult infrastructure management and operational problems that virtualization solved years ago.
- Operating containers in production requires lifecycle management, high availability, resource management, data persistence, networking, and automation.

Using VMware Telco Cloud Platform to run and automate CNFs on virtual machines instead bare metal satisfies the complete set of operational, management, and security requirements for deploying CNFs in production.

Performance

Many of the studies that compare the performance of containers on VMs and bare metal overlook the integral requirements of securing and managing containers in a real-world environment. Studies that consider performance in a real-world context take into account such integral requirements as security and lifecycle management.

The CPU scheduler of VMware ESXi™ enables the hypervisor to provide equivalent or better overall workload performance for containers than multi-purpose Linux operating systems running on physical hardware.

"Applications can benefit from the security and performance isolation provided by the VM, and still take advantage of the provisioning and deployment aspects of containers. This approach is quite popular, and is used to run containers in public clouds where isolation and security are important concerns."

CONTAINERS AND VIRTUAL MACHINES AT SCALE: A COMPARATIVE STUDY

"While network virtualization presents risk, it also allows advanced and flexible network protections. For this reason, a well-built virtualised network can be more secure and resilient than an equivalent network built on dedicated hardware."

SECURITY ANALYSIS FOR THE UK TELECOM SECTOR: SUMMARY OF FINDINGS, NATIONAL CYBER SECURITY CENTRE, JANUARY 2020

A *comparative study by VMware* shows that an enterprise web application can run in Docker containers on vSphere 6.5 with better performance than Docker containers on bare metal, largely because of optimizations in the vSphere CPU scheduler for nonuniform memory access (NUMA) architectures, quashing the belief that running containers on VMs comes with a performance tax.

A *recent test of vSphere 7 with Kubernetes* shows better performance compared with a bare-metal Linux Kubernetes node. vSphere native pods, isolated by the hypervisor, can achieve up to 8 percent better performance than pods on a bare-metal Linux Kubernetes node.

By using virtual machines, you can easily select the container host operating system that works best for the performance demands of your CNF. On vSphere, one example is Photon OS, a security-hardened minimalist operating system for containers. Its Linux kernel is optimized for performance on vSphere, and it supports new devices such as ARM64 (Raspberry Pi 3) to, for instance, help enable IoT apps at edge sites.

Security

In contrast to using bare metal, running containers on VMs improves your ability to secure them and manage their security at scale. Security for CNFs involves container images, the containers themselves, their orchestration system, and their interfaces with the network and other services. Three governmental bodies have produced or are preparing security standards for containers or 5G services and functions:

1. National Institute of Standards and Technology (NIST)
2. National Cyber Security Centre (NCSC) of the U.K.
3. European Commission

In September 2017, the National Institute of Standards and Technology (NIST) published its *Application Container Security Guide*, also known as NIST Special Publication 800-190. It exposes several fundamental areas of concern with containers:

- Degree of isolation
- Operating system management and configuration
- Orchestration systems without adequate protection
- Containers alone are inadequate security boundaries

Containers are not miniature VMs, and containers do not establish security boundaries as VMs do. An important implication of the Application Container Security Guide is to run containerized functions on virtual machines: Containers, the guide says, "do not offer as clear and concrete of a security boundary as a VM. Because containers share the same kernel and can be run with varying capabilities and privileges on a host, the degree of segmentation between them is far less than that provided to VMs by a hypervisor."

To run containers that properly isolate tenants on physical Linux hosts, you would need to run different tenants on separate physical machines. The likely outcome is either low resource utilization stemming from fragmentation or overly high utilization leading to long wait times for using new hardware. The major cloud providers, such as Google and Amazon Web Services (AWS), typically isolate the container workloads of tenants by using separate VMs.

Containers or the operating system of a physical host can easily be misconfigured, increasing the attack surface and the level of risk. "Carelessly configured environments can result in containers having the ability to interact with each other and the host far more easily and directly than multiple VMs on the same host," the NIST Application Container Security Guide says.

INTRINSIC SECURITY

With the VMware Telco Cloud, security is intrinsic—integrated with the software and built into the infrastructure so that security is programmable, automated, adaptive, and context-aware. Intrinsic security improves visibility, reduces complexity, and focuses your defenses by enabling you to apply and automate adaptive security measures like micro-segmentation in the right place.

VMWARE TELCO CLOUD PLATFORM AT A GLANCE

VMware Telco Cloud Platform™ enables CSPs to rapidly deploy and efficiently operate multi-vendor CNFs and VNFs with agility and scalability across 5G networks. The platform includes VMware Telco Cloud Infrastructure™ and VMware Telco Cloud Automation™.

VMware Telco Cloud Infrastructure supplies infrastructure as a service (IaaS) and containers as a service (CaaS) with VMware vSphere® and VMware NSX-T™ Data Center.

VMware Telco Cloud Automation centralizes the provisioning and management of Kubernetes clusters and other resources. VMware Tanzu Standard for Telco provides a carrier-grade Kubernetes distribution with telco extensions to manage and orchestrate CNFs at scale.

KEY BENEFITS

- Deploy virtual network functions (VNFs) and CNFs on consistent horizontal infrastructure
- Quickly provision and optimize Kubernetes clusters on demand
- Manage CNFs at scale
- Optimize the placement of xNFs
- Automate lifecycle management of Kubernetes clusters, network functions, and services
- Follow a reference architecture from VMware to implement a solution that works best for your requirements
- Add optional components, including VMware vRealize® Suite, VMware vSAN™, VMware Telco Cloud Operations, and a VIM — either VMware Cloud Director or VMware® Integrated OpenStack

LEARN MORE

For more information about VMware Telco Cloud Platform, call 1-877-VMWARE (outside North America, dial +1-650-427-5000) or visit *https://telco.vmware.com/*

In contrast, the abstraction, automation, and isolation of an operating system running on a VM in a hypervisor reduces the attack surface and decreases the risk of a breach.

Mitigating security risks in a complex multi-cloud environment that mixes 4G and 5G as well as VNFs and CNFs requires security to be built into the networking fabric, the stack, and the management systems. Otherwise, managing security will spiral out of control with too much complexity, too many silos, and too many security tools.

Security that is built into the software and infrastructure improves visibility, reduces complexity, and focuses your defenses by enabling you to apply and automate adaptive security measures like micro-segmentation in the right place.

Running CNFs on bare metal would create a complex web of bolted-on security controls and tools. In contrast, running CNFs on virtual machines lets you impose security by using built-in, proven mechanisms that can be managed en masse, at scale, and without silos.

For more information on protecting telecommunications infrastructure with *build-in security measures*, see *Intrinsic Security for Telco Clouds at the Dawn of 5G*.

Infrastructure and Lifecycle Management

Running containers on physical hardware would resurrect difficult infrastructure management and operational problems. Kubernetes can manage containerized functions and services, not the underlying infrastructure on which they are running. If you use physical hardware as the underlying infrastructure, you must address numerous requirements while avoiding the creation of difficult-to-manage silos:

- Infrastructure deployment and configuration
- Patching, updating, and upgrading
- Backup and disaster recovery
- Logging and monitoring

Multiple infrastructure silos can duplicate teams, tooling, and processes. Rather than driving focused innovation on a single platform, IT ends up repeatedly performing the same tasks. By running containers on physical hosts, many of the old problems that virtualization solved would come back to plague IT.

A VMware software-defined data center (SDDC) with VMware Telco Cloud Platform solves these problems with a comprehensive, flexible solution that uses the power of automation to deploy and manage multiple Kubernetes clusters as well as to patch and upgrade the container host operating system. The platform's multi-layer lifecycle management automates the provisioning and management of all the layers of the telco cloud, including virtual machines, to reduce costs.

Scalability

Hypervisors were originally developed to address the pain of working with physical hardware, pain that ranges from time-consuming management problems and cash-consuming underutilization to the difficulty of scaling hardware for a developer environment or an application's expanding workload. By optimizing utilization, virtualization lets you reduce physical hardware costs while improving scalability.

If IT operations deploys a bare-metal server with a container runtime to which developers can push their containers, scaling the system is difficult and time consuming: You would have to add another bare-metal server, install a container runtime on it, manually hook the server up to the network, and connect the runtime to a container orchestration engine.

In contrast, with a hypervisor, you can quickly connect a new bare-metal server to the

TELCO-GRADE KUBERNETES

The CaaS functionality of VMware Telco Cloud Platform simplifies the operation of Kubernetes for multi-cloud deployments, centralizing management and governance for clusters. The platform provides telco-grade CaaS enhancements, such as the following:

- Multus to attach multiple container networking interfaces to Kubernetes pods through its plugins
- Topology Manager to optimally allocate CPU memory and device resources on the same NUMA node to support performance-sensitive applications
- Kubernetes cluster automation to simplify deployments and management of Kubernetes master and worker nodes.

With these enhancements, CSPs can take advantage of a telco-grade Kubernetes platform to address emerging 5G use cases.

container domain. The ease of scalability that comes with virtualization is one of the reasons major public cloud providers use hypervisors to run their container services.

Resource Management

Kubernetes provides powerful quality-of-service (QoS) mechanisms to share a cluster between teams running different workloads. Running Kubernetes clusters on vSphere complements the QoS mechanisms of Kubernetes, especially when the workloads require strong workload isolation. The advanced scheduling and dynamic resource management of vSphere help reclaim and share unused resources. The resource management capabilities of vSphere include dynamic rebalancing, resource pools, shares, reservations, limits, and safe overcommitment. All these capabilities empower you to run traditional and containerized workloads on common infrastructure while ensuring optimal performance and preventing interference.

VMware Telco Cloud Platform extends resource management to telco-specific networks through powerful intent-based placement and dynamic resource allocation with late binding to optimize a Kubernetes cluster for a given CNF.

Storage and Data Persistence

Although many containerized applications are stateless, the drive to port network functions to containers is generating requirements to furnish containerized stateful apps with host-local, shared-nothing storage for data persistence across hosts.

Managing physical storage devices, however, is a painful, manual process often worsened by service-specific workflows. Adding new SSDs to expand capacity is inefficient. Different technologies and processes across infrastructure silos can complicate the situation, and dedicating physical hardware to an app is uneconomical.

A single software-driven model that works for network functions and services, whether containerized or not, radically simplifies storage management, operations, troubleshooting, capacity expansion, and storage operations like backup and disaster recovery. By providing a distributed, shared-nothing storage abstraction, VMware vSAN simplifies storage operations and consolidates workloads on the same storage infrastructure. For both virtual machines and containers, virtualized storage not only hides the complexity of adding storage capacity but also makes the task much easier.

Container Networking for Kubernetes Clusters

NSX-T Data Center supplies Kubernetes clusters with advanced container networking, security policies, and micro-segmentation. It also furnishes networking between CNFs and VNFs. You can quickly deploy networks on demand with micro-segmentation and virtualized load balancing and ingress services. Multus lets you establish multiple network interfaces for Kubernetes pods to address 5G telco use cases with containers. VMware Telco Cloud Platform extends the following performance features to CNFs:

- Data Plane Development Kit, or DPDK, accelerates data-intensive workloads.
- NSX managed Virtual Distributed Switch in Enhanced Data Path mode (N-VDS (E)) that leverages DPDK techniques to provide fast virtual switching fabric on vSphere.
- N-VDS to offload data plane traffic onto a physical NIC to further improve the Enhanced Data Path performance of NSX-T. This capability increases throughput, reduces latency, and scales performance.
- Improved performance through multi-tiered routing and huge pages with the increased access efficiency of translation lookaside buffers.
- A bare-metal NSX Edge cluster acts as an edge router that connects to a physical router to improves performance, increases throughput, and speeds up failover.

THE VMWARE TELCO CLOUD

We help communications service providers build, run, manage, and protect telco cloud infrastructure to transform their networks, accelerate the delivery of modern services, and thrive in a multi-cloud world.

The VMware Telco Cloud puts in place consistent infrastructure for operating all generations of cellular and fixed-line technology while leading the way to 5G adoption with solutions for orchestration, automation, optimization, and intrinsic security.

At the dawn of 5G, the VMware Telco Cloud combines consistent infrastructure and operations with intrinsic security to give CSPs a strong foundation for digital transformation and rapid innovation.

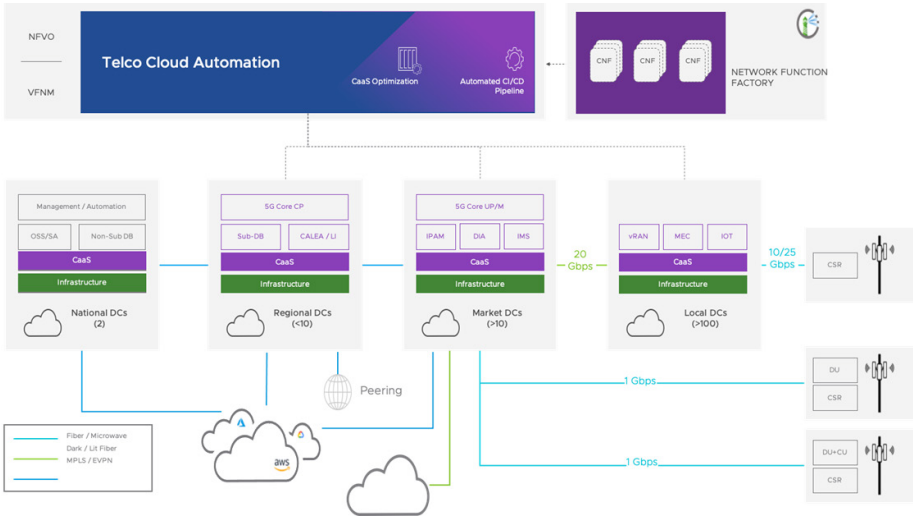

FIGURE 2: VMware Telco Cloud Automation provides CaaS for CNFs.

Automation

VMware Telco Cloud Platform automates the discovery, registration, and creation of Kubernetes clusters while continuously synchronizing between the CaaS layer and VMware Telco Cloud Automation. This synchronization creates Kubernetes cluster resource awareness, centralizes fault and performance monitoring, and optimizes workload placements.

During workload instantiation, the system will optimize a cluster or create a new one to match CNF requirements through late binding. Achieving this kind of automation and dynamic optimization using bare metal is likely to be difficult and expensive.

The platform also enables CSPs to automate the onboarding and upgrading of network functions and infrastructure components with zero-touch provisioning. Full lifecycle management can define and apply policies using a decisioning engine to automate deployments, operations, and maintenance.

As investments in infrastructure continue and 5G proliferates, it is increasingly important for operators to match their resources with their operational needs. If you can effectively use your fast-evolving cloud resources to fulfill your operational requirements, it can reduce complexity. Using bare metal as the basis for a multi-cloud, multi-vendor strategy that puts a premium on the deployment, management, and automation of CNFs is a step in the wrong direction.

Conclusion: Management, Security, and Automation

Running containers on virtual machines fuses the benefits of proven virtualization technology with the emerging benefits of cloud-native technology. The combination produces a sustainable multi-cloud solution with the security, management, scalability, and automation to turn your 5G strategy into a sustainable reality.

LEARN MORE

For more information about VMware Telco Cloud Platform, call 1-877-VMWARE (outside North America, dial +1-650-427-5000) or visit *https://telco.vmware.com/*