

Nuage Networks Virtualized Cloud Services for the Microsoft-Enabled Cloud

One Policy-based SDN Platform for all Environments

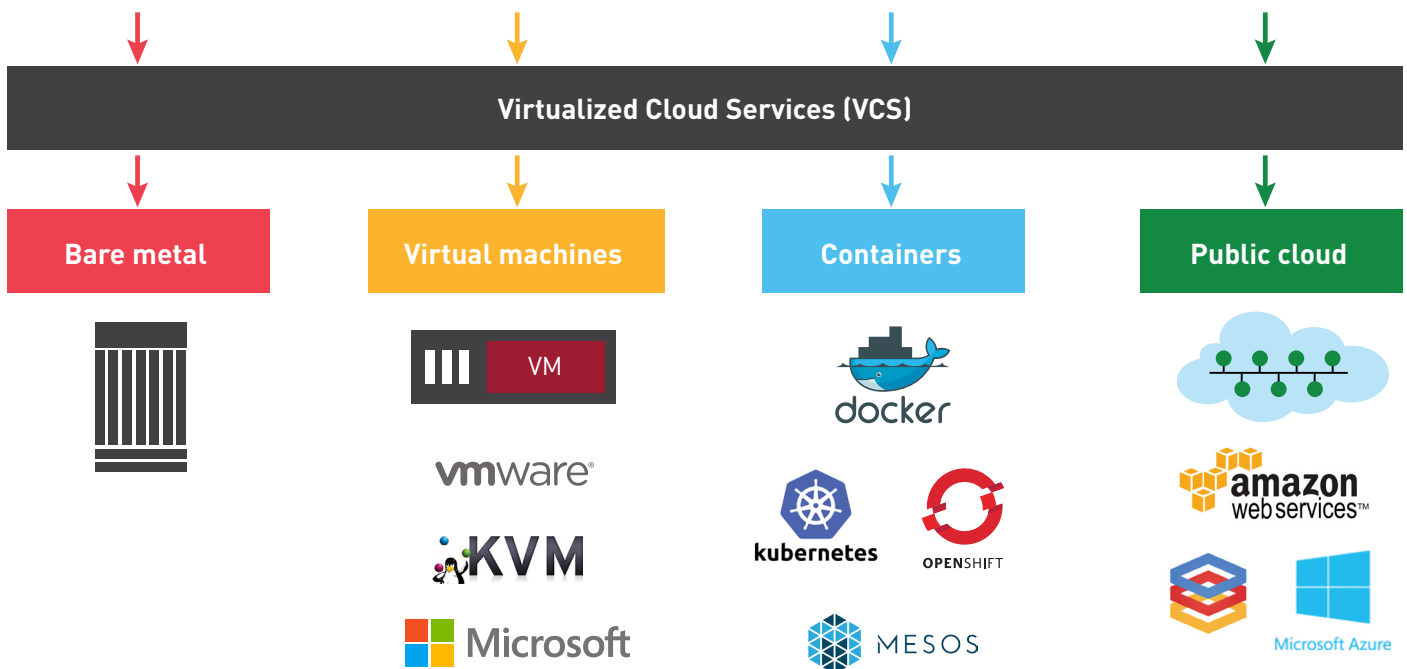
Cloud deployments are opening up new possibilities in IT organizations as they improve overall business processes for use cases ranging from DevOps, to Big Data analytics to the Internet of Things (IoT). At the heart of an on-demand, agile cloud architecture is a network infrastructure that can be provisioned, managed, and tuned through policy-based software, allowing virtual networks to respond in real-time to user requirements and business conditions.

The foundation of this cloud network, as it evolves from traditional data center designs, is a software-defined infrastructure. This infrastructure enables the automation of complex IT tasks, accelerating key IT processes from weeks to minutes. As Software Defined Networking (SDN) becomes more mainstream, we increasingly see a need for an open, multi-vendor platform that can automate networking and

security policies across all types of application workloads — physical servers, VMs and containers.

Organizations are looking to automate networking and security policies across Linux, Docker containers, and Microsoft Windows servers, as well as rely on a range of cloud management platforms.

Increasingly users are moving to a multi-hypervisor environment and want one virtual networking solution for all hypervisors. These users can be using single vendor stacks, such as Microsoft (System Center and Hyper-V) and VMware (vRealize and ESXi), or using OpenStack® to manage KVM, Hyper-V and ESXi hypervisors. Our philosophy at Nuage Networks™ has always been built on open, interoperable, multi-vendor systems that avoid vendor lock-in. As a result, in recent product releases of Virtualized Cloud Services (VCS), our SDN platform for data center, we have included support for Microsoft-enabled clouds.



With Nuage Networks Virtualized Cloud Services, users can now use a single network virtualization platform for VMs (running on ESXi, KVM and Hyper-V), Containers (running on Docker, Apache Mesos, Kubernetes) and bare metal servers. Network operation teams benefit from being able to automate all their environments in a single platform rather than having to invest in operationalizing different network virtualization technologies. In addition to supporting multiple hypervisors and application platforms, Nuage Networks extends the cloud management systems it supports, from OpenStack, CloudStack and VMware vRealize Automation, to Microsoft System Center, and eventually to Microsoft Azure public cloud environments.

One Hypervisor, multiple Cloud Management Systems

Most users prefer to manage Hyper-V 2012 using Microsoft's System Center Virtual Machine Manager (SCVMM) — its management solution for managing virtualized host, networking, and storage resources. SCVMM console add-ins allow partners to extend the SCVMM console by adding new actions for SCVMM objects. Through a user-friendly interface, the Nuage Networks SCVMM Add-in allows users to associate Nuage Networks & security policies with VMs on Hyper-V that are managed by SCVMM.

OpenStack is a great option for users who want one system to manage multiple hypervisors. OpenStack has support for all the leading hypervisors — KVM, Hyper-V and ESXi.

Nuage Networks is an enthusiastic supporter of open systems, and our open source Neutron plug-in for OpenStack works with Hyper-V 2012 R2 as well. Some of the largest OpenStack deployments are using Nuage Networks as a scalable SDN and security automation platform in place of native Neutron support.

Why use VCS in Hyper-V deployments

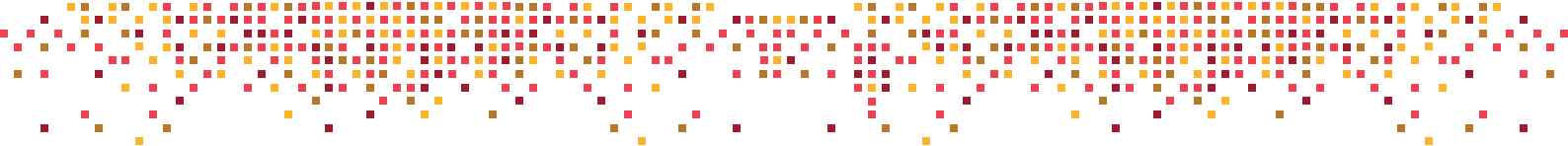
When introducing a new solution, users need to evaluate the benefits of introducing a new solution in their technology stack. The examples below show how VCS can help IT operations by providing cost savings (both CAPEX and OPEX), better control, and greater visibility.

- **Operational Efficiency** – By using widely-deployed and standard technologies, such as VXLAN and OVS, VSP and VCS for Hyper-V, operational efficiencies are achieved.
- **Better Control** – VCS policy groups allow users to easily deploy micro-segmentation for Hyper-V workloads. This gives users more control over their network.
- **Greater Visibility** – ACL counters, flow logs and policy-based mirroring give users more visibility into their network. This is useful for troubleshooting as well as for security audits for critical networks.

More importantly business operations improvements like these provide a springboard to develop innovative solutions for the overall business.

VCS brings SDN to Hyper-V 2012R2

Policy and analytics engine	<input checked="" type="checkbox"/> Policy abstraction <input checked="" type="checkbox"/> Statistics & analytics <input checked="" type="checkbox"/> Export capabilities <input checked="" type="checkbox"/> Flow visibility	Hybrid cloud support (AWS, Azure)
Security	<input checked="" type="checkbox"/> Micro-segmentation <input checked="" type="checkbox"/> Security monitoring <input checked="" type="checkbox"/> ACL flow logging <input checked="" type="checkbox"/> Policy-based mirroring <input checked="" type="checkbox"/> Automated quarantine <input checked="" type="checkbox"/> L4-7 security insertion	Broad ecosystem of technology partners
Advanced networking	<input checked="" type="checkbox"/> Datacenter federation <input checked="" type="checkbox"/> Service chaining <input checked="" type="checkbox"/> SW & HW VTEP <input checked="" type="checkbox"/> DC GW integration <input checked="" type="checkbox"/> NAT/PAT <input checked="" type="checkbox"/> Shared domains	Underlay/overlay correlation



VCS adds value to the Microsoft-Enabled Cloud

Network Virtualization based on VXLAN and Open vSwitch (OVS)

Hyper-V 2012R2's native network virtualization uses NVGRE encapsulation to provide overlay networking. VCS, however, uses the more standard and widely-used VXLAN encapsulation to provide network virtualization. This ensures compatibility with more network and security infrastructure for heterogeneous environments.

VCS uses OVS, a leading open source virtual switch, to integrate with the Hyper-V hypervisor. By standardizing on the use of OVS across all environments, VCS users benefit from having to learn to operate only one virtual switch.

Network Policy Abstraction

Using VCS's policy abstraction capabilities, users can easily deploy secure micro-segmentation in their environments. VCS policy groups allow workloads to be easily grouped, according to application type and security requirements, enabling automated network provisioning. Policies can be updated on the fly without having to reconfigure the applications themselves. Moreover, applications can be deployed with minimal to no manual operational overhead. The required security policies are expressed in access control lists (ACLs) that are enforced using VCS's distributed stateful Layer 4 firewall or other third-party security appliances.

ACL Counters and Flow Logs

These extremely powerful tools provide easy troubleshooting and security auditing capabilities to network operators. ACL counters allow users to identify which entries in user-defined ACLs are being hit. These counters are available at a granular level (per-VM), as well as at a summary level (network).

Flow logging can also be selectively enabled to capture flows hitting a particular ACL entry. The relevant packet header information is then sent using syslog messages.

Policy-based Mirroring

Policy-based mirroring enables mirroring of select traffic to an intrusion detection (ID) system or traffic analyzers for threat detection, analytics, and troubleshooting. Being able to do this selectively means that only traffic of interest is mirrored for analysis.

Service Insertion

VCS makes it easy to insert virtual and physical network or security appliances between VMs running different applications. This makes it easy to spin up new applications because firewalls and load balancers can be easily inserted, according to the requirements of the application. VCS completely automates the task of routing application traffic to wherever the workloads and supporting appliances are running.

Moving Beyond Private Cloud

Enterprises increasingly need hybrid cloud. Some application infrastructure is always going to be more cost-effective to run on-premises. Certain types of workloads, such as big data analytics, will remain on-premises because they can't be virtualized and need low-latency access to local storage. Users from highly-regulated industries may also choose to run some of their workload on-premises because proving compliance could be a challenge. On the other hand, public cloud offers these users stand-up resources quickly without having to go through a long procurement and infrastructure deployment cycle.

SDN can help with the automation of both private and public cloud environments as well as connecting the private cloud to public cloud across a seamless overlay network.

Nuage Networks users can connect their Hyper-V environments to the Microsoft Azure cloud or another public cloud, such as AWS. Nuage Networks has a Network Services Gateway (NSG) Amazon Machine Image (AMI) for AWS that allows users to seamlessly connect their DC to the AWS virtual private cloud (VPC) over a secure connection. The NSG AMI can be used to create VPC-to-VPC connections, something that is not natively supported by AWS cloud gateways. Nuage Networks provides virtual and hardware NSGs to be installed on premises for these secure connections. Using NSGs, users can build a full mesh of secure connections, allowing for direct point-to-point communication within multiple cloud locations.