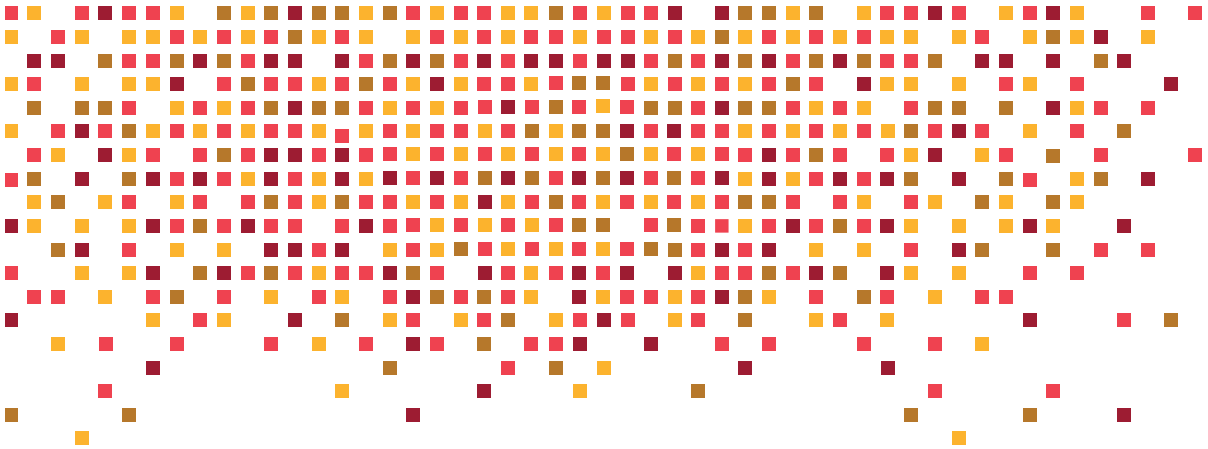
STRATEGIC WHITE PAPER

The next step in server virtualization: How containers are changing the cloud and application landscape

nuagenetworks
From Nokia

Abstract

Container-based server virtualization is gaining in popularity, due to its inherent suitability for cloud environments — the environment businesses are counting on to deliver their myriad applications quickly and efficiently. However, to take full advantage of containers, the networking environment must be optimized to connect container-based applications. Nuage Networks™ Virtualized Services Platform, a Software-Defined Networking solution, has been field-tested to integrate fully with Docker, a leading container technology. By choosing Nuage Networks as the virtual networking solution for Docker containers, businesses can ensure that they have a solid foundation for their applications.



CONTENTS

Containers come of age

Server virtualization has revolutionized the datacenter and paved the way for cloud architectures, more efficient hardware utilization and vastly greater degrees of IT automation. While virtual machine (VM) technology has matured greatly over the last decade, a new form of server virtualization, called "containers" is rapidly increasing in popularity. Containers promise to accelerate application deployment cycles and increase cloud agility in fundamental ways. One technology vendor, Docker, has taken the lead on improving earlier container virtualization formats to the point that now "Docker" and "containers" are virtually synonymous.

Containers allow applications to be isolated from each other using operating system-level virtualization features such as Linux control groups (resource control) and namespaces (resource isolation). Since containers run atop the same operating system they require fewer resources than VMs. For example, containers require fewer CPU cycles and less memory. Container images are also much smaller in comparison to VM images. As a result of these differences and the fact that they don't require an operating system to boot up, containers can be launched very quickly. The smaller footprint of containers means many more application instances can be run on a host compared to VMs.

While the container technology itself is not new, there are three key factors that have made containers popular again for cloud deployments.

1. Containers enable developers to write applications with the architecture required for cloud applications

Containers provide the right foundational building block for the growing number of applications being developed for the cloud (both private and public). Instead of writing monolithic apps that scale vertically, cloud applications are being implemented using micro-services. This modular architecture allows the application components to be maintained independently. Micro-services can be upgraded independently of each other rather than requiring the entire application to be upgraded. Since containers can be quickly spun up/down based on scaling demand, they are ideal for micro-services. The use of containers also facilitates upgrades.

2. Docker images are a big step forward for DevOps

Applications are critical to businesses and, in some cases, the applications are the businesses themselves. Being able to roll out new applications and upgrade them in an agile fashion is a challenge that businesses have been struggling with. In a DevOps environment, the Development and Operations teams come together to achieve those business goals.

The Docker image format is a big step forward. Docker images are the basis of Docker containers and the image captures all the application dependencies in the image itself. Docker-based apps run exactly the same on a laptop as they do in production, making the handoffs between Dev and Ops much easier. The small size of Docker images allows for much more rapid deployment of applications than if they were packaged in a VM image. The combination of instant-start and small footprint enables a development process called "continuous integration", meaning small incremental changes to applications can be rolled out very quickly to meet immediate business requirements.

3. Docker registries enable faster collaboration between developers

Docker registries make collaboration among developers much easier than it is when they must rely on open source software. Docker Hub, a public registry maintained by Docker, has over 100,000 public repositories. These reusable building blocks make it easy to get started. Developers can leverage community best practices by stitching together other developers' containers. Docker images are composed of multiple layers. So instead of creating images from scratch every time, developers can pull base images and add layers they need. This ultimately means that innovation can happen at a faster pace and applications can be created quickly.

In summary, containers are popular because they are a perfect fit for cloud applications and Docker makes using containers easy.

Networking requirements for deploying containers in production

While some may argue that containers are something that only application developers need to worry about, the truth is that deploying them in production requires a networking infrastructure that can successfully connect container-based applications. The networking requirements for deploying Docker-based applications are described below.

- **Can isolate applications:** The most basic requirement for cloud architectures is the ability to isolate applications from each other, and tenants from each other. This is something that needs to be designed for from the beginning. Trying to retrofit this can be challenging and may require a completely new network design. Overlay networks are a way to provide this isolation, since the network extends to the container host.
- **Provides a granular security policy framework:** Traditional application deployments involved multiple tiers with security policies in place to control the traffic between those tiers. Using containers to create applications may change the way the applications are architected, but the security requirements still hold. Containerized applications shouldn't be forced to work around these. In fact, since containers share the underlying operating system kernel the attack surface can be larger than that of a VM. Having a strong security framework for containers is extremely important.
- **Integrates with DevOps workflows:** Introducing an advanced networking solution should not impose unnecessary changes in the developer workflows and tools. The solution should adapt itself to the containerized environment rather than the other way round.
- **Interconnects containers, VMs and physical servers:** While applications are written to run in containerized environments it doesn't mean they won't need to access services running in VMs or on bare metal servers. The overlay networking solution chosen for containers must be able to provide this connectivity without sacrificing security.
- **Scales to meet cloud requirements and greater workload densities:** Containers will impose scaling requirements one to two orders of magnitude greater than VMs. Peak container activation/deactivation events will cause a churn in updating networking and security policies, thereby stressing the network control plane. A high performance data plane is equally important to avoid adding unnecessary latency to the application traffic. The networking control and management plane must be capable of supporting these requirements.

Docker integration with Nuage Networks Virtualized Services Platform

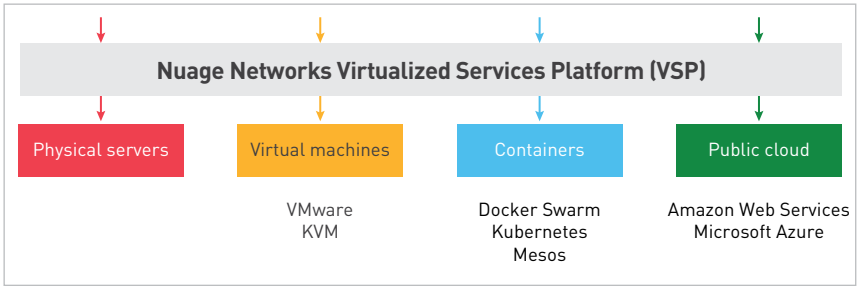
Nuage Networks Virtualized Services Platform (VSP) provides a policy-driven approach to creating VXLAN-based overlay networks. Nuage Networks VSP integrates with Docker by treating Docker containers as first-class citizens — along with VMs and bare metal hosts. This means that all the advanced networking capabilities that are available when using Nuage Networks VSP can be leveraged for Docker deployments. Docker deployments get multi-tenancy, security and performance from the underlying Nuage Networks VSP.

The Nuage Networks VSP policy component, called the Virtualized Services Directory (VSD), allows users to define and manage network policies for applications. Application network endpoints are then placed in Zones or Policy Groups on-the-fly, and the network policies are automatically pushed from the VSD to distributed virtual switches connected to containers. A Zone is a logical construct in Nuage Networks VSP consisting of one or more subnets. A Policy Group is a collection of virtual ports (vPorts) that are grouped together for the creation of security policies.

Since containers are similar to VMs from a networking perspective, they get the same treatment. Docker containers may also be connected to VMs and bare metal servers that are managed by the Nuage Networks VSP.

Docker deployments in the public cloud are becoming increasingly common. Nuage Networks VSP can be easily deployed on cloud VMs (like AWS Amazon Machine Images) to manage containers as well. This approach shows the value of implementing Software-Defined Networking (SDN) in software; some SDN solutions actually require proprietary hardware.

FIGURE 1. Nuage Networks VSP: policy-driven networking for all environments



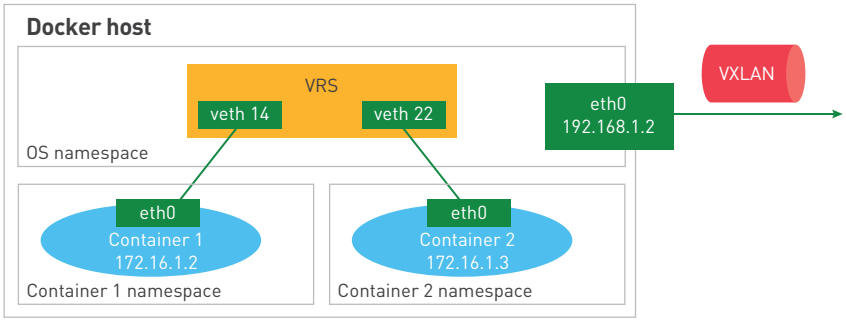
Docker integration details

Nuage Networks has created a plug-in for Docker networking. The Nuage Networks VSP plug-in runs on every Docker host. Each Docker host, whether bare metal or virtual, also has the Nuage Networks VSP's Virtual Routing and Switching (VRS) component installed on it. The VRS is a software agent that is responsible for forwarding traffic from the containers, performing the VXLAN encapsulation of traffic and enforcing security policies. While creating a Docker container the user can specify what Zone or Policy Group it belongs to. All endpoints in a given zone adhere to the same set of security policies.

The Nuage Networks VSP plug-in first creates a virtual Ethernet (*veth*) interface pair to connect the Docker container to the VRS, which is the distributed routing component that runs on each host. The Nuage Networks VSP plug-in then passes the Zone or Policy Group information to the VRS, which uses it to resolve the IP address of the container. The Platform plug-in configures the resolved IP addresses in the container's namespace. This means that every container gets its own IP address. With some other approaches containers are given an address from a subnet that is local to the host and therefore require the use of NAT to reach the container.

The VRS also downloads the security policies based on the container's Zone or Policy Group from the VSD. The container can only exchange information with other containers/VMs that are authorized by the configured policies.

FIGURE 2. Nuage Networks VSP architecture with Docker



Conclusion

Docker containers are gaining rapid adoption for the next generation of cloud applications. By choosing Nuage Networks as the networking solution for Docker containers, businesses can ensure that they have a solid foundation for their applications. The Docker integration for Nuage Networks VSP has been available since July 2015. Integrations with other Docker orchestration platforms like Kubernetes and Mesos are also on the Nuage Networks VSP roadmap.