VMware NSX and vRealize Automation

DELIVERING SECURE, SCALABLE AND HIGH PERFORMING APPLICATIONS ON DEMAND

Applications need much more than appropriately sized virtual machines. They also need accurately configured network connectivity, security, availability, scale, and performance. In order to deliver these capabilities to your applications you will need to automate more than just assigning IP address, DNS entries and vLANs to the virtual machines that host your applications.

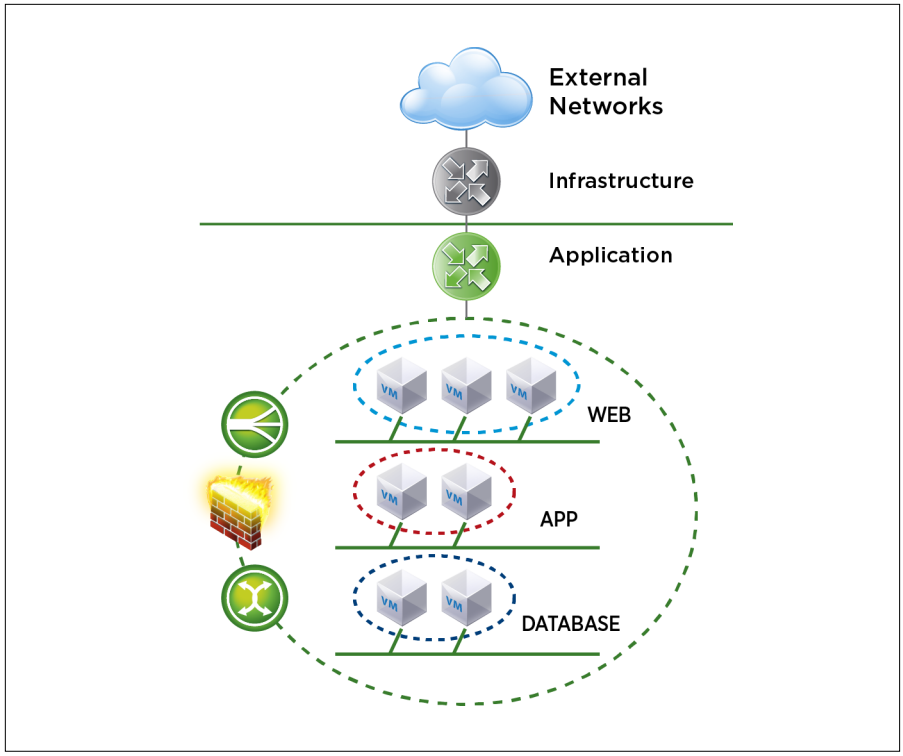
As part of deploying a multi-tiered application you will need to provision connectivity through deployment of logical switches and routers. In addition it is important to securely deploy the application through intelligent placement of workloads in security groups, protected by firewall rules. Finally application availability and performance through the use of load balancers ensures that application users will always have access to a highly responsive application. VMware vRealize™ Automation™ automates all of these processes for VMware NSX™.

Delivering Application-Centric Network and Security Services

vRealize Automation provisions, updates and decommissions network and security services in lockstep with your virtualized applications. Network and security services are deployed as part of the automated delivery of the application, consistent with its connectivity, security, and performance requirements.

Automation creates a standardized repeatable process that helps accelerate delivery, reducing the time needed to perform the task. At the same time automation also improves the consistency and reliability of the final configuration by elimination of manual errors. Finally automation reduces operational costs by eliminating many manual tasks, and improves development productivity by delivering application environments to engineers faster.

vRealize Automation, used in conjunction with NSX, automates an application's network connectivity, security, performance, and availability.



Configuring application-centric NSX networking and security.

Connectivity: Proper network connectivity is fundamental to any business service. Various groups and different applications can have unique requirements. vRealize Automation's resource reservations, service blueprints and network profiles assure that each application receives the right level of network connectivity, with the appropriate service level. For example, each business group can be provided with reserved network connectivity between the virtual and physical world, or specific mission critical

applications can be configured with dedicated virtual switches and routers depending on their performance and reliability needs. In addition, virtual machines can be moved with a tool like VMware vSphere® vMotion® live migration without changes to the virtual machine networking configuration. This allows for the optimal placement of workloads on the compute infrastructure, ultimately leading to reduced capital expenditure.

Security: Ensuring appropriate security policies are applied is one of the most critical steps to delivering and managing your applications and data. Now with vRealize Automation and NSX, applications can be deployed ondemand with network security at the application level or between application tiers to ensure that firewall rules are placed as close to the virtual machine as possible. This leads to a true defense-in-depth solution that cannot be achieved by other solutions. The IT administrator can define vRealize Automation application blueprints that specify NSX security policies which contain firewall rules, intrusion detection integration, and agentless anti-virus scanning at each application tier to allow application and per-tier security.

When the application is provisioned, dynamic security groups are configured with the defined policies to safeguard the service from day one. These services can also be tagged with a security label, for example DB servers, PCI, HIPPA that enforces policies dynamically based on the tags (e.g. type of application) throughout their lifecycle. Finally, application isolation for these business services can also be defined to fence the service from the rest of the network entirely or to deny all traffic to the service except for what is defined in the applied security policies. This granular level of isolation keeps traffic to specific group environments (e.g., development, test, production) or even isolated at the individual application or application tier level.

Performance: vRealize Automation's governance policies and automated delivery can be used to meet the specific network performance needs of each application being deployed. vRealize Automation can also configure NSX to minimize traffic through the oversubscribed core. Traffic between virtual machines on the same host will remain in the host while still getting the distributed routing, switching, load-balancing, firewalling, and security services that are required by modern applications.

Availability: vRealize Automation improves application availability through the dynamic configuration of network load balancers in the context of deploying or updating application configurations. NSX load balancer can be used in all phases of the application lifecycle (development, staging, production) without requiring expensive physical hardware or manual configuration of legacy load-balancing components. Depending on vRealize Automation's application blueprints and network profiles, applications can be added to an existing load balancer pool or configured with their own dedicated load balancer. This integration provides organizations with application centric availability management.

Accelerating Application Delivery with vRealize Automation and NSX

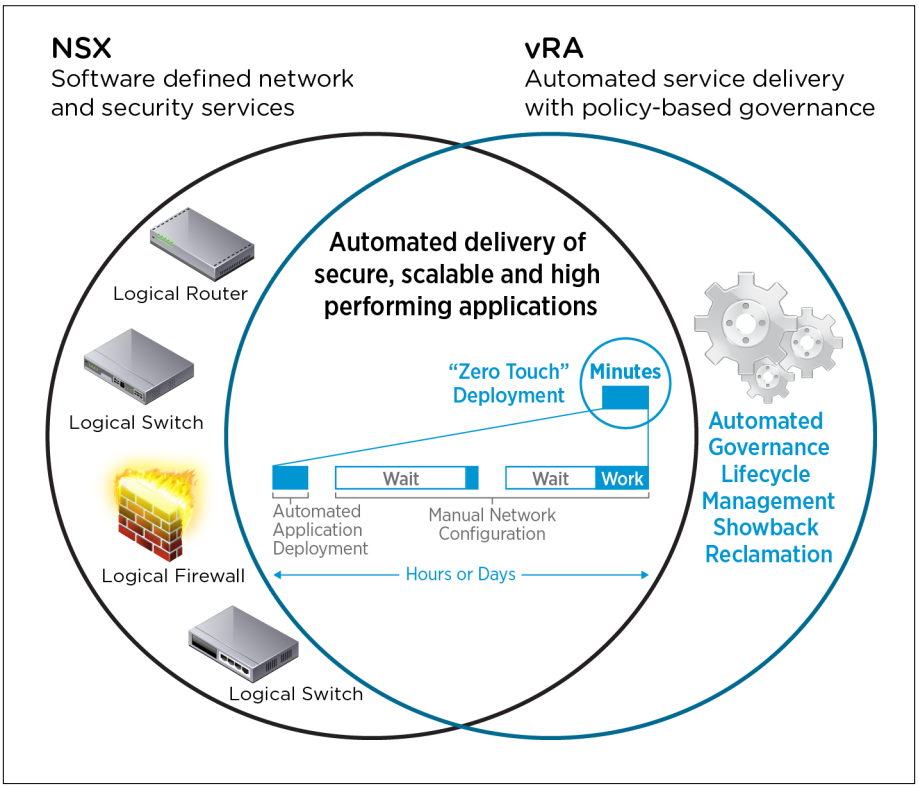
Working together, vRealize Automation and NSX accelerate the delivery of network and security services customized to the specific needs of modern applications. vRealize Automation dynamically configures network and security services within the context of the infrastructure or applications that are being deployed.

Using vRealize Automation, organizations can enable self-service requests for application or infrastructure resources. This joint solution reduces provisioning processes that used to take days or weeks down to a matter of minutes – with the exact same configuration.

vRealize Automation's network configuration policies ensure that resources reserved for one tenant or business group cannot be seen or accessed by others. This provides isolation in a shared private cloud environments.

vRealize Automation service blueprint policies specified by administrators control how these services are provisioned, so resource consumers don't have to be networking and security experts. Automation and standardization not only accelerate IT services delivery, but provide repeatable processes that eliminate delays caused by manual errors.

The combined capabilities of these products empower IT to fully automate the delivery of secure, scalable and high performing multi-tier applications.



Better together: vRealize Automation and NSX.

Learn More

To learn more about how vRealize Automation and NSX can be used to deploy and maintain your micro-segmentation security see the following resources:

- Whitepaper: Data Center Micro-Segmentation
  A Software Defined Data Center Approach for a "Zero Trust" Security Strategy.
- Tech Note: vRealize Automation and NSX Micro-Segmentation
  How to configure vRealize Automation policies for Micro Segmentation.

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