VMware Network Virtualization Deployment and Application Security Adoption Service

At a glance

The primary objective of this service is a rapid installation, configuration, and high-level validation (deployment) of a reference design for virtualized networking infrastructure using VMware NSX-T Data Center followed by an extensive knowledge transfer focused on application security. The installation and configuration are conducted jointly with your team members to enhance the learning experience during the deployment.

Key benefits

- Learn the fundamentals of a network virtualization solution

- Deploy a best practice-based, foundational VMware NSX-T implementation

- Improve operational efficiency and network provisioning time

- Expand security protections and capabilities within the virtual data center

SKU

CON-NSX-MSS-DPY

Service overview

The VMware Network Virtualization Deployment and Application Security Service entails a rapid installation, configuration, and high-level deployment validation of a reference design for virtualized networking infrastructure using VMware NSX-T™ Data Center and VMware Aria Operations for Logs.

This two-part service rapidly deploys a virtual network foundation according to a proven best practice design and then focuses in on ensuring that the customer:

- Understands how to identify opportunities for leveraging NSX security

- Becomes proficient at analyzing network communications between application components

- Knows how to build security policies to protect those applications

- Has the confidence to implement and enforce those policies

These skills are developed using actual customer example workloads to ensure a real-world experience.

At the end of the engagement, the customer will have the ability to analyze applications from a communication perspective and subsequently develop security groups and security profiles to protect the respective virtual machines.

This service is ideal for organizations who are just starting out with VMware NSX-T Data Center and have limited exposure to implementing and managing micro-segmentation.

Project scope

Deploy a Network Virtualization Foundation

Deployment of a network virtualization solution based on NSX-T Data Center according to a VMware standard architecture that is implemented and verified in the Customer environment. The service includes technical verification of platform prerequisites, the deployment of network virtualization using NSX-T Data Center, functional testing and a knowledge transfer session for the Customer.

vmware®

Specification	Parameters	Description
NSX-T Foundation		
Data Center Location(s)	Up to one (1)	Data center deployment of NSX-T components
NSX manager Cluster	Up to one (1)	Management cluster of three (3) NSX Managers providing high availability of the user interface, API services, and central control plane function
Hypervisor Hosts Configured as Transport Nodes	Up to ten (10)	Hypervisor hosts (ESXi or KVM) with NSX-T modules installed, registerd to the NSX-T management plane and configured as transport nodes
Logging and monitoring		Direct logging output to a pre-installed end customer-designated syslog target such as VMware Aria Operations for Logs
Role-Based Access Control		Integration of NSX-T to VMware Identity Manager and role-based access control (RBAC) configuration for suers that vIDM manages
Network Virtualization		
NSX Edge VMs Deployed and Configured	Up to two (2)	NSX Edge VMs deployed and configured as a transport node
NSX-T Tier-0 Gateway(s)	Up to one (1)	Tier-0 gateway to process traffic between the logical and physical networks using static or dynamic routing (BGP) peering
NSX-T Tier 1 Gateway(s)	Up to one (1)	Tier-1 gateway configured to connect to one Tier-0 gateway for northbound connectivity and one or more overlay networks for southbound connectivity; a Tier-1 gateway can be an active-standby cluster that provides stateful services
NSX Segments	Up to four (4)	Segments configured to provide virtual Layer 2 switching for VM and gateway interfaces; a segment is also known as a logical switch

vmware®

Deploy a Network Virtualization and Security Operations Visibility Foundation

Deployment of VMware Aria Operations for Networks according to a VMware standard architecture that is implemented and verified in the Customer environment.

Specification	Parameters	Description
Foundational Use Cases		All of the following foundational use cases are included in the engagement as guidelines for product and knowledge transfer discussions
Network visibility		Map application connectivity if allowed in the environment deployed; optimize network performance with 360 visibility; discover VMware vCenter Server and VMware NSX constructions (folders, clusters, VLANs, and security tags)
Micro-segmentation		Plan micro-segmentation deployment and confirm compliance; recommended security policies / firewall rules (zero-trust model)
Operations		Confirm health and availability of NSX deployments

Get Started with Application Security and Isolation

Establish foundational tasks and activities to provide Customer with a repeatable methodology for securing applications within the virtual infrastructure. This is achieved using a recommended practice security policy framework with the VMware NSX-T Data Center Distributed Firewall. The initial workshops establish the principles and build the knowledge for securing applications firewall rules. These workshops then feed into the demonstration of requirements gathering through application or technical-lead interviews, data analysis and policy creation for an initial nominated application.

Assistance and mentoring are provided, while the Customer uses the education provided to undertake the assessment, analysis and policy creation for the remaining two (2) applications. VMware NSX-T policy creation also accounts for the infrastructure services, and a high-level policy related to the nominated applications. At the end of the engagement, the customer will have the ability to analyze applications from a communication perspective and subsequently develop security groups and security profiles to protect the respective virtual machines.

Specification	Parameters	Description
Number of Infrastructure Service Policies	Up to five (5)	Security rules that contain mutually agreed upon widely used core and foundation services (e.g. NTP, Active Directory, DNS, etc.)
Number of High-Level Policies	Up to one (1)	Security policy that segments between broadly defined object groups (e.g. tenants, business units, environments)
Number of Applications to be Secured	Up to three (3)	Target applications identified for micro-segmentation, with each application comprised of ten (10) or less virtual machines
NSX Manager Cluster	Up to one (1)	Target application virtual machines exist within a single NSX Manager Cluster

Estimated Schedule

VMware estimates that the duration of this project will not exceed six (6) weeks. VMware consulting services will be performed according to a schedule agreed to by both parties. Typically, consulting services are performed during normal business hours and workdays (weekdays and non-holidays).

Project Activities

The activities for this engagement are organized in phases as shown in the following table.

Activities / Week	1	2	3	4	5	6
Phase 1: Initiate	▓					
Phase 2: Plan	▓					
Phase 3.1: Execute: Implement	▓	▓	▓	▓		
Phase 3.2: Execute: Knowledge Transfer				▓	▓	▓
Phase 4: Close						▓

The VMware Project Manager hosts one (1) project initiation call with key Customer and VMware stakeholders. Topics to be discussed include the following:

- Project business drivers, scope, and objectives

- Project deadlines, estimated timelines, scheduling, and logistics

- Identification of key Customer team members with whom VMware will work to perform the task defined in this SOW

- Participating team members are confirmed, and contact details are exchanged to schedule the project kickoff meeting

Deliverables

- One (1) project initiation call

Phase 2: Plan

VMware leads one (1) project kickoff meeting with Customer project sponsors and stakeholders to review expectations about the purpose of the engagement, the delivery approach, and estimated timelines. The following are the objectives of the meeting.

- Introducing the VMware team, roles, and responsibilities

- Describing the project goals, phases, and key dates

- Agreeing on communication and reporting process and creating a communications plan

- Validating the project expectations and clarifying roles and responsibilities

- Confirming the prerequisites are met as detailed in the solution checklist for specified solutions

- Presenting the solution overview for specified solutions including expected project results and deliverables

- The VMware Project manager and the Customer Project Manager collaborate to develop the project plan

Deliverables

- Communication plan

- One (1) project kickoff meeting

- Project plan

- Solution checklist

- Solution overview presentation

Phase 3: Execute

The key activities for this phase are organized in the following sub-phases.

- Implement

- Transfer

Phase 3.1: Implement

VMware implements the solution according to the VMware solution specification. VMware does the following:

- Implements the specified solutions as detailed in the specification workbooks

- Verifies the implementation and documents results in the verification workbooks for the specified solutions

Deliverables

- Solution specification workbook

- Solution versification workbook

Phase 3.2: Knowledge Transfer

VMware conducts knowledge transfer sessions covering the design, implementation, and operational considerations relating to the scope of this project. VMware does the following.

- Conducts up to forty-eight (48) hours of knowledge transfer sessions for appropriate Customer representatives

- Provides an adoption guide document(s) containing operational guidelines for the specified solutions

Note: For clarification, the Knowledge Transfers herein do not comprise VMware product training or certification courses as offered by the VMware Education unit (http://mylearn.vmware.com/mgrreg/index.cfm).

Deliverables

- Adoption guide document

- Knowledge transfer workshop presentation

- Up to forty-eight (48) hours of knowledge transfer sessions

Phase 4: Close

The VMware Project Manager conducts one (1) closure meeting with Customer covering project status, next steps, and how to engage further with VMware.

Deliverables

- Engagement summary presentation

- One (1) closure meeting

Out of Scope

The following are out of scope for this project.

General

- Installation and configuration of custom or third-party applications and operating systems on deployed virtual machines

- Operating system administration including the operating system itself or any operating system features or components

- Management of change to virtual machines, operating systems, custom or third-party applications, databases, and administration of general network changes within Customer control

- Remediation work associated with any problems resulting from the content, completeness, accuracy, and consistency of any data, materials, or information supplied by Customer

- Installation or configuration of VMware products not included in the scope of this document

- Installation and configuration of third-party software or other technical services that are not applicable to VMware components

- Installation and configuration of Customer-signed certificates

- Configuration of VMware products used for the service other than those implemented for the mutually agreed to use cases

- Customer solution training other than the defined knowledge transfer session

Deploy a network virtualization foundation

- Stateful services attached to a Tier-0 or Tier-1 logical router (such as NAT, load balancing, edge firewall, or DHCP services)

Deploy a network virtualization and security operations visibility foundation

- Capturing physical endpoint network flows

Get started with application security and isolation

- Applications hosted on physical workloads or containers

Appendix – Service Checklist

Customer is responsible for executing all items discussed in the Service Checklist prior to arrival of VMware consultants on site.

The participation of the following Customer stakeholders is required for the Service to be performed.

- Network Architecture team leads

- Network Operations team leads

- Infrastructure Architect

- Security policy team leads

- Firewall/DMZ team leads

- VMware operations team leads

- Enterprise Architect

- Security Manager

- Application Operations Leads

- Service Owner

- Infrastructure manager

- IT Operations manager

- Chief Technology Officer

The following prerequisites are required to enable VMware to perform this Service:

Deploy a network virtualization foundation

- Software Requirements: Customer will have the required software installed and configured as required and communicated in the Service Checklist

- MTU Size required. Defined minimum: 1700 (9000 recommended)

- Number of IP subnets required. Defined minimum: 1

- Minimum number of hosts required of. Defined minimum: 4

- Virtualized CPU Capacity (GHz). Defined minimum: Enough CPU capacity must be available to deploy three (3) NSX Manager nodes and two (2) NSX Edge VMs

- Virtualized RAM Capacity (GB). Defined minimum: Enough memory capacity must be available to deploy three (3) NSX Manager nodes and two (2) NSX Edge VMs

- Shared Storage must be provisioned. Defined minimum: Enough storage capacity must be available to deploy three (3) NSX Manager nodes and two (2) NSX Edge VMs

- Shared storage maximum disk access latency. Maximum: 10ms

- Network latency between NSX Managers in a Manager Cluster. Maximum: 10ms

Learn more

Visit vmware.com/services.

- Network latency between NSX Managers and Transport Nodes. Maximum: 150ms

- NTP must be setup and time verified to be correct

- DNS must be configured and tested for forward, reverse, short and long name resolution

- FIPS compliant SFTP server to store NSX-T backups

Deploy a network virtualization and security operations visibility foundation

- Virtualized RAM capacity (GB). Defined minimum: 42 GB

- Virtualized storage capacity (GB). Defined minimum: 900 GB

- vSphere Distributed Switches Required. Defined minimum: 1

- Storage IOPs required. Defined minimum: 25-

- Service account with permissions in vCenter.

Get started with application security and isolation

- Syslog events must be sent ot a log centralization system (ideally VMware Aria Operations for Logs)

- NTP must be set up and time verified to be correct

- Relevant hypervisors or bare-metal hosts prepared, registered to the NSX-T management plane and configured as transport nodes

- VMware Aria Operations for Networks deployed or planned for deployment and configuration

- VMware Aria Operations for Networks collecting IPFIX data for 2 weeks prior to engagement start

- VMware NSX-T management plane and control plane deployed and configured with VMware recommended practices

This service must be delivered and accepted within the first 12 months of purchase, or the service will be forfeited. Pricing for this service excludes travel and other expenses. For detailed pricing, contact your local VMware representative.