vmware EDUCATION SERVICES

VMware Certified Professional – Network Virtualization

Exam Preparation Guide

Exam code: 2V0-642
Exam Preparation Guide Version 2.3
13 December 2019

Disclaimer:
This preparation guide is intended to provide information about the objectives covered by this exam, as well as related resources. The material contained within this guide is not intended to guarantee that a passing score will be achieved on the exam. VMware recommends that a candidate thoroughly understands the objectives indicated in this guide and utilizes the resources recommended in this guide where needed to gain that understanding.

Contributors:

William Grismore
John Hays
Paul Mancuso
Chris McCain
Michael Moore
Victor Sandoval
Elver Sena
Andrew Voltmer
Jon C. Hall
Jeff Hall
Andrew Sturniolo
Jordan Roth

Table of Contents

1. The Exam

1.1 Purpose of Exam

The VMware Certified Professional 6 – Network Virtualization Exam (2V0-642) tests candidates on their skills and abilities installing, configuring and administering a VMware NSX 6.2 environment. Successful candidates demonstrate mastery of these skills and abilities.

1.2 Intended Audience

A candidate for the VCP-NV certification has approximately six months' experience working with NSX implementations. They are typically infrastructure personnel for networking, datacenter and cloud Administrators, as well as virtualization specialists who have a strong understanding of the relationship between physical and virtual network infrastructures and is capable of installing, configuring, managing, and troubleshooting VMware NSX. The successful candidate will most likely have one or more industry recognized networking certifications or equivalent experience (typically 2-3 years) and a familiarity with datacenter virtualization.

2. Objectives covered in the VCP6-NV Exam (2V0-642):

2.1 Introduction

It is recommended that candidates have the knowledge and skills necessary to install, configure and administer an NSX environment before taking the VCP6-NV Exam. It is also recommended that the candidate complete the course requirement prior to attempting the exam. It is not required that the course is completed prior to the exam, but the course requirement must be completed in order to obtain the VCP-NV certification.

2.2 Objectives

Prior to taking this exam, candidates should understand each of the following objectives. Each objective is listed below; along with related tools the candidate should have experience with, and related documentation that contains information relevant to the objective. All objectives may also be referenced in other product documentation not specifically highlighted below. The candidate should be familiar with all relevant product documentation or have an equivalent skillset.

Section 1 – Understand VMware NSX Technology and Architecture

Objective 1.1 – Compare and Contrast the Benefits of a VMware NSX Implementation

- Determine challenges with physical network implementations
- Understand common VMware NSX terms

- Differentiate NSX network and security functions and services
- Differentiate common use cases for VMware NSX

Objective 1.2 – Understand VMware NSX Architecture

- Differentiate component functionality of NSX stack infrastructure components
- Compare and contrast with advantages/disadvantages of topologies (star, ring, etc.) as well as scaling limitations
- Compare and contrast VMware NSX data center deployment models
- Prepare a vSphere implementation for NSX

Objective 1.3 – Differentiate Physical and Virtual Network Technologies

- Differentiate logical and physical topologies, components and services
- Differentiate logical and physical security constructs
  - Endpoint Security
  - Data Security
  - Flow Monitoring
  - Activity Monitoring
  - Distributed Firewall
  - Perimeter Firewall

Objective 1.4 – Understand VMware NSX Integration with Third-Party Products and Services

- Understand integration with third-party partner tools and systems using NSX REST APIs
- Determine integration with third-party services
  - Network services
  - Security services
  - Load Balancing
  - Anti-malware
  - IDS/IPS
- Determine integration with third-party hardware
  - Network Interface Cards (NICs)
  - Terminating overlay networks
  - HW VTEP
  - VXLAN offload
  - RSS
- Install/register a third-party service with NSX

Objective 1.5 – Understand VMware NSX Integration with vRealize Automation (vRA)

- Understand integration with vRealize Automation
- Demonstrate NSX deployment capabilities built into vRealize Automation
- Compare and contrast Network Profiles available in vRealize Automation
- Understand NSX preparation tasks for attaching a network profile to a blueprint

- Discern vRealize Automation preparation tasks for deploying a machine with on-demand network services

Section 2 – Understand VMware NSX Physical Infrastructure Requirements

Objective 2.1 – Compare and Contrast the Benefits of Running VMware NSX on Physical Network Fabrics

- Differentiate physical network topologies
  - Differentiate physical network trends
  - Understand the purpose of a Spine node
  - Understand the purpose of a Leaf node
- Differentiate virtual network topologies
  - Enterprise
  - Service Provider Multi-Tenant
  - Multi-Tenant Scalable
- Given a specific physical topology, determine what challenges could be addressed by a VMware NSX implementation.
- Differentiate physical/virtual QoS implementation
- Differentiate single/multiple vSphere Distributed Switch (vDS)/Distributed Logical Router implementations
- Differentiate NSX Edge High Availability (HA)/Scale-out implementations
- Differentiate Separate/Collapsed vSphere Cluster topologies
- Differentiate Layer 3 and Converged cluster infrastructures

Objective 2.2 – Determine Physical Infrastructure Requirements for a VMware NSX Implementation

- Discern management and edge cluster requirements
- Differentiate minimum/optimal physical infrastructure requirements for a VMware NSX implementation
- Determine how traffic types are handled in a physical infrastructure
- Determine use cases for available virtual architectures
- Describe ESXi host vmnic requirements
- Differentiate virtual to physical switch connection methods
- Compare and contrast VMkernel networking scenarios

Section 3 – Configure and Manage vSphere Networking

Objective 3.1 – Configure and Manage vSphere Distributed Switches (vDS)

- Compare and contrast vDS capabilities
- Create/Delete a vDS
- Add/Remove ESXi hosts from a vDS
- Edit general vSphere vDS settings
- Add/Configure/Remove dvPortgroups

- Configure dvPort settings
- Add/Remove uplink adapters to dvUplinkgroups
- Create/Configure/Remove virtual adapters
- Migrate virtual machines to/from a vDS
- Monitor dvPort state
- Determine use cases for a vDS

Objective 3.2 – Configure and Manage vDS Policies

- Compare and contrast common vDS policies
- Configure dvPortgroup blocking policies
- Explain benefits of Multi-Instance TCP/IP stack
- Configure load balancing and failover policies
- Configure VLAN settings
- Configure traffic shaping policies
- Enable TCP Segmentation Offload (TOE) support for a virtual machine
- Enable Jumbo Frame support on appropriate components
- Determine appropriate VLAN configuration for a vSphere implementation
- Understand how DSCP is handled in a VXLAN frame

Section 4 – Install and Upgrade VMware NSX

Objective 4.1 – Configure Environment for Network Virtualization

- Comprehend physical infrastructure configuration for NSX Compute, Edge and Management clusters (MTU, Dynamic Routing for Edge, etc.)
- Prepare a Greenfield vSphere Infrastructure for NSX Deployment
  - Configure Quality of Service (QoS)
  - Configure Link Aggregation Control Protocol (LACP)
- Configure a Brownfield vSphere Infrastructure for NSX
- Determine how IP address assignments work in VMware NSX
- Determine minimum permissions required to perform an NSX deployment task in a vSphere implementation

Objective 4.2 – Deploy VMware NSX Components

- Install/Register NSX Manager
- Prepare ESXi hosts
- Deploy NSX Controllers
- Understand assignment of Segment ID Pool and appropriate need for Multicast addresses
- Install Guest Introspection
- Create an IP pool
- Understand when to use IP Pools versus DHCP for VTEP configuration

Objective 4.3 – Upgrade Existing vCNS/NSX Implementation

- Based on a given upgrade scenario, identify requisite steps and components for upgrading to NSX 6.x
- Upgrade vCNS 5.5 to NSX 6.x
- Upgrade vCNS Virtual Wires to NSX Logical Switches
- Upgrade to NSX Components
  - Upgrade to NSX Firewall
  - Upgrade to NSX Edge
  - Upgrade vShield Endpoint from 5.5 to 6.x
  - Upgrade to NSX Data Security
- Upgrade NSX Manager from 6.0 to 6.x
- Update vSphere Clusters after NSX upgrade
- Understand the impact of availability to the aspects of NSX during an upgrade

Objective 4.4 – Expand Transport Zone to Include New Cluster(s)

- Understand the function of a Transport Zone
- Understand proper addition of a Transport Zone
- Understand necessity to expand or contract a Transport Zone
- Edit a Transport Zone
- Understand appropriate use of Control Plane mode modification of a Transport zone

Section 5 – Configure VMware NSX Virtual Networks

Objective 5.1 – Create and Administer Logical Switches

- Given a scenario, demonstrate the proper way to add/remove a Logical Switch
- Determine use case for and contrast the three Control Plane Modes
  - Multi-cast
  - Hybrid
  - Unicast
  - Determine use case for connecting a Logical Switch to an NSX Edge gateway
- Deploy services to a Logical Switch
- Demonstrate multiple ways of adding or removing virtual machines from a Logical Switch
- Test Logical Switch connectivity

Objective 5.2 – Configure VXLAN

- Determine areas where VXLANs should be configured
- Understand physical network requirements for virtual topologies with VXLANs
- Understand how to prepare a vSphere cluster for VXLAN
- Determine the appropriate teaming policy for a given implementation
- Understand how to configure and modify the options of a Transport Zone
- Understand how prepare VXLAN Tunnel End Points (VTEPs) on vSphere clusters

Objective 5.3 – Configure and Manage Layer 2 Bridging

- Given a scenario, determine an appropriate High Availability configuration for Layer 2 Bridging
- Understand how to add a Layer 2 Bridge to an NSX Edge device
- Determine when Layer 2 Bridging would be required for a given NSX implementation
- Determine use cases for multiple Layer 2 Bridges
- Compare and contrast software and hardware bridging

Objective 5.4 – Configure and Manage Logical Routers

- Install NSX Edge
- Understand how to connect/disconnect a Logical Switch from a logical router
- Understand and describe the different types of router interfaces
- Determine NSX components needed to build out topologies with logical routers
- Understand how to add and configure a new logical router
- Determine use case for and configure a management interface
- Determine use case for and configure High Availability for a logical router
- Configure routing protocols
  - Static
  - OSPF
  - BGP
  - IS-IS
- Configure default gateway
- Determine if cross-protocol route sharing is needed for a given NSX implementation
- Understand how to configure administrative distances for routing
- Understand configuration differences between iBGP and eBGP
- Understand and configure route redistribution

Section 6 – Configure and Manage NSX Network Services

Objective 6.1 – Configure and Manage Logical Load Balancing

- Differentiate when to use the two topologies for load balancing
- Understand how to configure load balancing
- Configure and understand service monitors
- Understand how to Add/Edit/Delete a server pool
- Understand how to Add/Edit/Delete an application profile
- Understand how to Add/Edit/Delete virtual servers
- Determine appropriate NSX Edge instance size based on load balancing requirements

Objective 6.2 – Configure and Manage Logical Virtual Private Networks (VPN)

- Understand how to configure IPSec VPN
  - Configure IPSec VPN parameters
  - Enable logging
- Understand how to configure Layer 2 VPN

- Add Layer 2 VPN Client/Server
- View Layer 2 VPN Statistics
- Configure Network Access/Web Access SSL VPN-Plus
- Edit Client Configurations
- Edit General Settings
- Edit Web Portal Designs
- Add/Edit/Delete IP Pools
- Add/Edit/Delete Private Networks
- Add/Edit/Delete Installation Packages
- Add/Edit/Delete Users
- Add/Edit/Delete Login/Logoff script
- Determine appropriate VPN service type for a given NSX implementation

Objective 6.3 – Configure and Manage DHCP/DNS/NAT

- Understand proper use and addition of a DHCP IP Pool
- Enable a DHCP IP pool
- Determine use and proper implementation of DNS services
- Determine when and how to configure Source NAT
- Determine when and how to configure Destination NAT
- Given a scenario, compare and contrast proper DHCP uses

Objective 6.4 – Configure and Manage Edge Services High Availability

- Given a scenario, compare and contrast proper HA uses
- Determine service availability during an Edge High Availability failover
- Differentiate NSX Edge High Availability and vSphere High Availability
- Configure NSX Edge High Availability
  - Configure heartbeat settings
  - Configure management IP addresses
- Modify and existing Edge High Availability deployment
- Determine resource pool requirements for a given Edge High Availability configuration
- Configure Equal-Cost Multi-Path Routing (ECMP)
  - Determine ECMP timers
  - Understand process flows
- Combine ECMP with other stateful services

Section 7 – Configure and Administer Netw Network Security

Objective 7.1 – Configure and Administer Logical Firewall Services

- Add/Edit/Delete an Edge Firewall rule
- Configure Source/Destination/Service/Action rule components
- Compare and contrast between Edge Rule Types (PreRules/Internal/User Rules/Default Rules)
- Change the order of an Edge User Firewall rule

- Demonstrate how to configure an Edge Firewall PreRule
- Understand the limitations of ECMP and Edge Firewall Policy

Objective 7.2 – Configure Distributed Firewall Services

- Understand VM IP Address learning for the purposes of DFW vCenter attribute learning
- Differentiate between Layer 2 and Layer 3 rules
- Differentiate between entity-based and identity-based rules
- Understand firewall rule entities
- Determine rule processing order
- Understand rule segregation
- Demonstrate steps to Add/Delete a Distributed Firewall rule
- Demonstrate configuration of Source/Destination/Service/Action rule components
- Change the order of a Distributed Firewall rule
- Add/Merge/Delete a Distributed Firewall rule section
- Determine publishing requirements for rules in a given NSX implementation
- Demonstrate Import/Export Distributed Firewall Configuration
- Load Distributed Firewall configuration
- Determine need for excluding virtual machines from distributed firewall protection
- Describe SpoofGuard Operation and Default Policy and Actions
- Describe SpoofGuard IP Address Learning
- Determine requirements for a Spoofguard Policy
- Demonstrate how to Create and Edit a SpoofGuard Policy
    - IP Local Addresses
    - Approve IP addresses
    - Edit/Clear IP addresses

Objective 7.3 – Configure and Manage Service Composer

- Understand assets that can be used with a Security Group
- Differentiate services contained in a Security Policy
- Compare and contrast common Service Composer use cases
- Differentiate third party integration and service redirection
- Differentiate Security Groups and Security Policies
- Demonstrate the ability to redirect specific flows (e.g. 80) to network introspection services
- Differentiate between vCenter attribute based Firewall rules (including IP Sets) vs Active Directory identity-based rule
- Create/Edit a Security Group in Service Composer
- Create/Edit/Delete a Security Policy in Service Composer
- Map a Security Policy to a Security Group
- Add/Edit/Delete a Security Tag
- Assign and view a Security Tag

Section 8 – Deploy a Cross-vCenter NSX environment

Objective 8.1 – Differentiate single and Cross-vCenter NSX deployments

- Understand the benefits/use cases for Cross-vCenter NSX
- Contrast single and Cross-vCenter deployment models
- Determine the appropriate NSX topology for a given use case
- Understand options for ingress and egress traffic flows in a multi-site topology
- Describe and differentiate Universal components
    - Universal Firewall rules
    - Universal Network and Security objects
    - Universal Logical Switches
    - Universal Distributed Logical Routers

Objective 8.2 – Determine Cross-vCenter Requirements and Configurations

- Deploy a Cross-vCenter NSX environment
    - Create and configure the Primary NSX Manager
    - Create and configure the Secondary NSX Manager
- Migrate an NSX deployment to Cross-vCenter
- Create and configure Cross-vCenter components
    - Universal Segment ID Pool
    - Universal Transport Zone
    - Universal Logical Switch
    - Universal Distributed Logical Router
- Compare and contrast Local and Universal Firewall Rules

Section 9 – Perform Operations Tasks in a VMware NSX Environment

Objective 9.1 – Configure Roles, Permissions, and Scopes

- Understand default roles
- Understand Single Sign-On (SSO) integration
- Configure SSO
- Assign a role to a vCenter Server user or group
- Compare and contrast the uses for the various NSX Security Roles
- Determine how roles can be applied to a subset of the vCenter infrastructure for multi Tenancy purposes
- Understand how to apply NSX Roles to an AD group
- Assign objects to a user
- Enable/Disable a user account
- Edit/Delete a user account

Objective 9.2 – Understand NSX Automation

- Discern common use cases that require the NSX REST API

- Compare and contrast how the NSX REST API works and how it is used with a support browser
- Understand how NSX REST API Calls are sent to the NSX Manager
- Differentiate common NSX REST API verbs
- Determine how to use NSX REST API calls to learn the network topology

Objective 9.3 – Monitor a VMware NSX Implementation

- Compare and contrast available monitoring methods (UI, CLI, API, etc.)
- Monitor infrastructure components
    - Control Cluster Health
    - Manager Health
    - Hypervisor Health
- Perform Inbound/Outbound activity monitoring
- Enable data collection for single/multiple virtual machines
- Perform virtual machine activity monitoring
- Monitor activity between inventory containers (security groups, AD groups)
- Analyze network and security metrics in vRealize Operations
- Monitor logical networks and services
    - Identify available statistics/counters
    - Network/service health
    - Configure and collect data from network

Objective 9.4 – Perform Auditing and Compliance

- Given an auditing scenario, determine where applicable log information can be located
- Differentiate permissions for auditing
- Differentiate common data security regulations supported by NSX Data Security
- Differentiate information available in audit logs
- Use flow monitoring to audit firewall rules
- Audit deleted users
- Audit infrastructure changes
- View NSX Manager audit logs and change data
- Configure NSX Data Security
- Create a Data Security Policy
- Install Data Security
- Run a Data Security scan
- View and download compliance reports
- Create a regular expression
- Configure Guest Introspection (Install vShield Endpoint)

Objective 9.5 – Administer Logging

- Given a scenario, utilize information contained in technical support bundles/logs to assist in troubleshooting
- Explain usage of CLI for logging
- Configure Syslog(s)
- Configure logging for Dynamic Routing information

- Log Distributed Firewall rule processing information
- Log Edge Firewall rule processing information
- Log address translation information
- Log VPN traffic
- Configure basic/advanced Load Balancer logging
- Log DHCP assignments
- Log DNS resolutions
- Log security policy session information
- Download NSX Edge tech support logs
- Generate NSX Manager tech support logs

Objective 9.6 – Backup and Recover Configurations

- Understand how to backup and recover various components
- Schedule backups
- Export/Restore vSphere Distributed Switch configuration
- Import/Export Service Composer profiles
- Perform NSX Manager backup and restore operation

Section 10 – Troubleshoot a VMware Network Virtualization Implementation

Objective 10.1 – Compare and Contrast Tools Available for Troubleshooting

- Capture and trace uplink, vmknic, and physical NIC packets
- Audit NSX infrastructure changes
- Output packet data for use by a protocol analyzer
- Capture and analyze traffic flows
- Mirror network traffic for analysis
- Perform a network health check
- Configure vSphere Distributed Switch alarms

Objective 10.2 – Troubleshoot Common NSX Installation/Configuration Issues

- Troubleshoot lookup service configuration
- Troubleshoot vCenter Server link
- Troubleshoot licensing issues
- Troubleshoot permissions issues
- Troubleshoot host preparation issues
- Troubleshoot IP pool issues

Objective 10.3 – Troubleshoot Common NSX Component Issues

- Differentiate NSX Edge logging and troubleshooting commands
- Verify NSX Controller cluster status and roles
- Verify NSX Controller node connectivity
- Check NSX Controller API service

- Validate VXLAN and Logical Router mapping tables
- List Logical Router instances and statistics
- Verify Logical Router interface and route mapping tables
- Verify active controller connections
- View Bridge instances and learned MAC addresses
- Display Logical Router instances
- Verify NSX Manager services status
- View Logical Interfaces and routing tables
- Analyze NSX Edge statistics

Objective 10.4 – Troubleshoot Common Connectivity Issues

- Review netcpa logs for control plane connectivity issues
- Verify VXLAN, VTEP, MAC, and ARP mapping tables
- List VNI configuration
- View VXLAN connection tables and statistics
- Perform VTEP connectivity tests

Objective 10.5 – Troubleshoot Common vSphere Networking Issues

- Verify network configuration
- Verify a given virtual machine is configured with the correct network resources
- Troubleshoot virtual switch and port group configuration issues
- Troubleshoot physical network adapter configuration issues
- Determine the root cause of a network issue based on troubleshooting information

2.3 Tools and References

The tools and references listed below were used to help write the exam items, and can be used to help prepare for the exam. The tools listed contains information relevant to respective objective. All objectives may also be referenced in other product documentation not specifically highlighted below. The candidate should be familiar with all relevant product documentation or have an equivalent skill set.

Objectives:	1.1	1.2	1.3	1.4	1.5	2.1	2.2	3.1	3.2	4.1	4.2	4.3	4.4	5.1	5.2	5.3	5.4
VMware NSX Network Virtualization Design Guide	✓	✓	✓			✓	✓										
vSphere Networking Guide		✓					✓	✓	✓	✓							
NSX Administration Guide		✓		✓						✓	✓	✓	✓	✓	✓	✓	✓
Physical Networks in the Virtualized Networking World			✓														
Next Generation Security with VMware NSX and Palo Alto Networks VM-Series white paper				✓					✓								
Deploying VMware NSX with Cisco UCS and Nexus 7000				✓													
VMware NSX and vRealize Automation					✓												
IaaS Configuration for Virtual Platforms					✓												
IaaS Configuration for Multi-Machine Services					✓												
Data Center Micro-Segmentation						✓											
NSX Installation Guide							✓			✓	✓	✓	✓	✓	✓	✓	✓
vSphere Installation and Setup Guide								✓	✓								
VMware NSX Brownfield Deployment Guide										✓							
NSX Upgrade Guide												✓					
Cross-vCenter NSX Installation Guide													✓		✓	✓	
NSX Manager																	✓
NSX CLI																	✓

	6.1	6.2	6.3	6.4	7.1	7.2	7.3	8.1	8.2	9.1	9.2	9.3	9.4	9.5	9.6
NSX Installation Guide	✓	✓													

	6.1	6.2	6.3	6.4	7.1	7.2	7.3	8.1	8.2	9.1	9.2	9.3	9.4	9.5	9.6
NSX Administration Guide	✓	✓	✓	✓	✓	✓	✓	✓		✓		✓	✓	✓	✓
HAProxy Configuration Manual	✓														
NSX Command Line Interface Reference			✓									✓		✓	
Securing VMware® NSX					✓										
Microsegmentation using NSX Distributed Firewall: Getting Started						✓									
WhitePaper: NSX Distributed Firewalling Policy Rules Configuration Guide						✓									
VMware NSX Network Virtualization Design Guide						✓									
Cross-vCenter NSX Installation Guide								✓	✓						
NSX vSphere API Guide									✓		✓				
vRealize Operations Manager (vROps)												✓			
NSX Ticket Logger													✓		
Log Insight														✓	

	10.1	10.2	10.3	10.4	10.5
NSX Administration Guide	✓	✓	✓	✓	
vSphere Networking Guide	✓				✓
vSphere Command-Line Interface Concepts and Examples	✓			✓	✓
NSX Installation Guide		✓			
NSX Command Line Interface Reference		✓	✓	✓	
NSX vSphere API Guide			✓		

	10.1	10.2	10.3	10.4	10.5
vSphere Troubleshooting Guide					✓

3. Additional Resources

3.1 VCP Community

VMware provides an online community for VCP candidates. This community contains valuable information from other candidates and senior VCPs, and is moderated by VMware certification staff. The community is located at: http://communities.vmware.com/community/vmtn/certedu/certification/vcp.

3.2 Test Driving a VMware NSX environment

VMware provides a Hands-on Lab for VMware NSX that can be evaluated at no cost. The environment allows you to gain hands-on experience with NSX Logical Switches, Logical Routing, firewalls and network services. The lab environment can be accessed by going here: https://my.vmware.com/web/vmware/evalcenter?p=nsx-hol