# VMware NSX 4.x Professional

## Exam Details (Last Updated: 5/26/2023)

The VMware NSX 4.x Professional exam (2V0-41.23) which leads to VMware Certified Professional - Network Virtualization 2024 (VCP-NV 2024) certification is a 70-item exam, with a passing score of 300 using a scaled method. Candidates are given an appointment time of 135 minutes, which includes adequate time to complete the exam for non-native English speakers. This exam may contain a variety of item types including multiple-choice, multiple-selection multiple-choice, build-list, matching, drag-and-drop, point-and-click and hot-area. Additional item types may be used but will appear less frequently than those previously mentioned.

## Exam Delivery

This is a proctored exam delivered through Pearson VUE. For more information, visit the Pearson VUE website.

## Certification Information

For details and a complete list of requirements and recommendations for attainment, please reference the VMware Learning Services – Certification website.

## Minimally Qualified Candidate

The candidate can install, configure, manage, and troubleshoot NSX solutions, but occasionally needs to research topics. The candidate should have 6 months or more of experience working with VMware NSX solutions. The candidate should have 2 years of experience working in IT. The candidate is knowledgeable of the features, functions, and architectures of NSX but occasionally needs to research topics. The candidate has experience working in IT and with VMware vSphere and its command line but occasionally needs to research topics. The candidate may require assistance or supervision with some tasks. The candidate may need to research some network virtualization related topics. The candidate possesses most of the knowledge shown in the exam sections (blueprint).

## Exam Sections

VMware exam blueprint sections are now standardized to the five sections below, some of which may NOT be included in the final exam blueprint depending on the exam objectives.

Section 1 – IT Architectures, Technologies, Standards

Section 2 – VMware Solution

Section 3 – Plan and Design the VMware Solution

Section 4 – Install, Configure, Administrate the VMware Solution

Section 5 – Troubleshoot and Optimize the VMware Solution

If a section does not have testable objectives in this version of the exam, it will be noted below, accordingly. The objective numbering may be referenced in your score report at the end of your testing event for further preparation should a retake of the exam be necessary.

## Sections Included in this Exam

### Section 1 – IT Architectures, Technologies, Standards

Not Applicable

### Section 2 – VMware Solution

Objective 2.1 - Demonstrate knowledge of VMware Virtual Cloud Network and NSX

- Objective 2.1.1 Describe the purpose of VMware Virtual Cloud Network and its framework
- Objective 2.1.2 Identify the benefits and recognize the use cases for NSX
- Objective 2.1.3 Describe how NSX fits into the NSX product portfolio
- Objective 2.1.4 Recognize features and the main elements in the NSX Data Center architecture
- Objective 2.1.5 Describe NSX policy and centralized policy management
- Objective 2.1.6 Describe the NSX management cluster and the management plane
- Objective 2.1.7 Identify the functions of control plane components, data plane components, and communication channels

Objective 2.2 Demonstrate knowledge of NSX Management Cluster

- Objective 2.2.1 Explain the deployment workflows for the NSX infrastructure

Objective 2.3 Demonstrate knowledge of the NSX UI

- Objective 2.3.1 Distinguish between the Policy and the Manager UI

Objective 2.4 Demonstrate knowledge of the data plane

- Objective 2.4.1 Describe the functions of transport zones, transport nodes, VDS, and N-VDS
- Objective 2.4.2 Explain the relationships among transport nodes, transport zones, VDS, and N-VDS
- Objective 2.4.3 Describe NSX Data Center on VDS
- Objective 2.4.4 Describe uplink profiles

Objective 2.5 Demonstrate knowledge of logical switching

- Objective 2.5.1 Describe the functions of NSX Data Center segments
- Objective 2.5.2 Recognize different types of segments
- Objective 2.5.3 Explain tunneling and the Geneve encapsulation protocol
- Objective 2.5.4 Describe the interaction between components in logical switching
- Objective 2.5.5 Describe the function of kernel modules and NSX agents installed on ESXi
- Objective 2.5.6 Describe the function of the management plane in logical switching
- Objective 2.5.7 Describe the function of the control plane in logical switching

Objective 2.6 Demonstrate knowledge of logical switching packet forwarding

- Objective 2.6.1 Describe the functions of each table used in packet forwarding
- Objective 2.6.2 Describe how BUM traffic is managed in switching
- Objective 2.6.3 Explain how ARP suppression is achieved

Objective 2.7 Demonstrate knowledge of segments and segment profiles

- Objective 2.7.1 Define what a segment is
- Objective 2.7.2 Describe the purpose of segment profiles
- Objective 2.7.3 Identify the functions of the segment profiles in NSX

Objective 2.8 Demonstrate knowledge of logical routing

- Objective 2.8.1 Explain the function and features of logical routing
- Objective 2.8.2 Describe the architecture of NSX two-tier routing
- Objective 2.8.3 Differentiate between north-south and east-west routing
- Objective 2.8.4 Describe the gateway components
- Objective 2.8.5 Recognize the various types of gateway interfaces

Objective 2.9 Demonstrate knowledge of NSX Edge and Edge Clusters

- Objective 2.9.1 Explain the main functions and features of the NSX Edge node
- Objective 2.9.2 Describe the functions of the NSX Edge cluster
- Objective 2.9.3 Identify the NSX Edge node form factors and sizing options
- Objective 2.9.4. Describe the different NSX Edge node deployment methods

Objective 2.10 Demonstrate knowledge of Tier-0 and Tier-1 Gateways

- Objective 2.10.1 Describe how to configure a Tier-1 gateway
- Objective 2.10.2 Explain how to configure a Tier-0 gateway
- Objective 2.10.3 Explain Active/Active Tier-0 and Tier-1 configurations
- Objective 2.10.4 Explain multi-tenancy use in a Tier-0 gateway

Objective 2.11 Demonstrate knowledge of static and dynamic routing

- Objective 2.11.1 Distinguish between static and dynamic routing

Objective 2.12 Demonstrate knowledge of ECMP and high availability

- Objective 2.12.1 Explain the purpose of ECMP routing
- Objective 2.12.2 Identify the active-active and active-standby modes for high availability
- Objective 2.12.3 Recognize failure conditions and explain the failover process

Objective 2.13 Demonstrate knowledge of logical routing packet walk

- Objective 2.13.1 Describe the datapath of single-tier routing
- Objective 2.13.2 Explain the datapath of multitier routing

Objective 2.14 Demonstrate knowledge of VRF Lite

- Objective 2.14.1 Describe VRF Lite

- Objective 2.14.2 Explain the benefits of VRF Lite

Objective 2.15 Demonstrate knowledge of logical bridging

- Objective 2.15.1 Describe the purpose and function of logical bridging
- Objective 2.15.2 Distinguish between routing and bridging

Objective 2.16 Demonstrate knowledge of NSX segmentation

- Objective 2.16.1 Define NSX segmentation
- Objective 2.16.2 Recognize use cases for NSX segmentation
- Objective 2.16.3 Identify steps to enforce Zero-Trust with NSX segmentation

Objective 2.17 Demonstrate knowledge of distributed firewall

- Objective 2.17.1 Identify types of firewalls in NSX
- Objective 2.17.2 Describe features of distributed firewalls
- Objective 2.17.3 Describe the distributed firewall architecture

Objective 2.18 Demonstrate knowledge of security in distributed firewall on VDS

- Objective 2.18.1 List the distributed firewall on VDS requirements

Objective 2.19 Demonstrate knowledge of NSX Gateway Firewall

- Objective 2.19.1 Describe the functions of the gateway firewall
- Objective 2.19.2 Explain the purpose of a gateway policy
- Objective 2.19.3 Describe the gateway firewall architecture

Objective 2.20 Demonstrate knowledge of Intrusion Detection and Prevention

- Objective 2.20.1 Explain NSX IDS/IPS and its use cases
- Objective 2.20.2 Define the NSX IDS/IPS Detection terminology
- Objective 2.20.3 Describe the NSX IDS/IPS architecture

Objective 2.21 Demonstrate knowledge of NSX Application Platform

- Objective 2.21.1 Describe NSX Application Platform and its use cases
- Objective 2.21.2 Explain the NSX Application Platform architecture and services

Objective 2.22 Demonstrate knowledge of malware prevention

- Objective 2.22.1 Identify use cases for malware prevention
- Objective 2.22.2 Identify the components in the malware prevention architecture
- Objective 2.22.3 Describe the malware prevention packet flows for known and unknown files

Objective 2.23 Demonstrate knowledge of NSX Intelligence

- Objective 2.23.1 Describe NSX Intelligence and its use cases
- Objective 2.23.2 Explain NSX Intelligence system requirements
- Objective 2.23.3 Explain NSX Intelligence visualization, recommendation, and network traffic analysis capabilities

Objective 2.24 Demonstrate NSX Network Detection and Response

- Objective 2.24.1 Describe NSX Network Detection and Response and its use cases
- Objective 2.24.2 Explain the architecture of NSX Network Detection and Response in NSX
- Objective 2.24.3 Describe the visualization capabilities of NSX Network Detection and Response

Objective 2.25 Demonstrate knowledge of NAT and how it is used with NSX

- Objective 2.25.1 Explain the role of network address translation (NAT)
- Objective 2.25.2 Distinguish between source and destination NAT
- Objective 2.25.3 Describe how Reflexive NAT works
- Objective 2.25.4 Explain how NAT64 facilitates communication between IPv6 and IPv4 networks
- Objective 2.25.5 Describe stateful active-active NAT operation

Objective 2.26 Demonstrate knowledge of DHCP and DNS

- Objective 2.26.1 Explain how DHCP and DHCP Relay are used for IP address allocation
- Objective 2.26.2 Configure DHCP services in NSX
- Objective 2.26.3 Describe how to use a DNS forwarder service

Objective 2.27 Demonstrate knowledge of NSX Advanced Load Balancer

- Objective 2.27.1 Describe NSX Advanced Load Balancer and its use cases
- Objective 2.27.2 Explain the NSX Advanced Load Balancer architecture
- Objective 2.27.3 Explain the NSX Advanced Load Balancer components and how they manage traffic

Objective 2.28 Demonstrate knowledge of IPSec VPN

- Objective 2.28.1 Explain how IPSec-based technologies are used to establish VPNs
- Objective 2.28.2 Compare policy-based and route-based IPSec VPN
- Objective 2.28.3 Describe IPSec VPN requirements in NSX

Objective 2.29 Demonstrate knowledge of L2 VPN

- Objective 2.29.1 Describe L2 VPN technologies in an NSX
- Objective 2.29.2 Identify various supported L2 VPN endpoints

Objective 2.30 Demonstrate knowledge of integrating NSX with VMware Identity Manager

- Objective 2.30.1 Describe the purpose of VMware Identity Manager
- Objective 2.30.2 Identify the benefits of integrating NSX with VMware Identity Manager

Objective 2.31 Demonstrate knowledge of integrating NSX with LDAP

- Objective 2.31.1 Identify the benefits of integrating NSX with LDAP
- Objective 2.31.2 Describe the LDAP authentication architecture

Objective 2.32 Demonstrate knowledge of managing users and configuring RBAC

- Objective 2.32.1 Identify the different types of users in NSX
- Objective 2.32.2 Recognize permissions and roles available in NSX

Objective 2.33 Demonstrate knowledge of Federation Architecture, needed prerequisites, Federation Networking, and Federation Security

Objective 2.33.1 Describe Federation and its use cases

Objective 2.33.2 Describe the requirements and limitations of Federation

Objective 2.33.3 Describe the Federation configuration workflow

Objective 2.33.4 Describe the prerequisites for Federation

Objective 2.33.5 Describe the onboarding of Local Manager configurations and workloads

Objective 2.33.6 Describe the stretched networking concepts in Federation

Objective 2.33.7 Explain the supported Tier-0 and Tier-1 stretched topologies

Objective 2.33.8 Explain Layer 2 concepts related to NSX Federation

Objective 2.33.9 Explain the Federation security use cases

Objective 2.33.10 Describe the Federation security components

Objective 2.33.11 Explain the security configuration workflows

Objective 2.34 Demonstrate knowledge of DPU-based acceleration for NSX

**Section 3 – Plan and Design the VMware Solution**

Not Applicable

**Section 4 – Install, Configure, Administrate the VMware Solution**

Objective 4.1 - Prepare an NSX infrastructure for deployment

Objective 4.1.1 Create Transport Zones

Objective 4.1.2 Create IP Pools

Objective 4.1.3 Prepare ESXi Hosts

Objective 4.2 Configure segments

Objective 4.2.1 Create segments

Objective 4.2.2 Attach VMs to segments

Objective 4.2.3 Use network topology to validate the logical switching configuration

Objective 4.3 Deploy and configure NSX Edge Nodes

Objective 4.3.1 Deploy NSX Edge Nodes

Objective 4.3.2 Configure an Edge Cluster

Objective 4.4 Configure the Tier-1 gateway

Objective 4.4.1 Create a Tier-1 gateway

Objective 4.4.2 Connect segments to the Tier-1 gateway

Objective 4.4.3 Use network topology to validate the Tier-1 gateway configuration

Objective 4.5 Create and configure a Tier-0 gateway with OSPF

Objective 4.5.1 Create uplink segments

Objective 4.5.2 Create a Tier-0 gateway

- Objective 4.5.3 Connect the Tier-0 and Tier-1 gateways
- Objective 4.5.4 Use network topology to validate the Tier-0 gateway configuration

Objective 4.6 Configure the Tier-0 gateway with BGP

- Objective 4.6.1 Create uplink segments
- Objective 4.6.2 Create a Tier-0 gateway
- Objective 4.6.3 Connect the Tier-0 and Tier-1 gateways
- Objective 4.6.4 Use network topology to validate the Tier-0 gateway configuration

Objective 4.7 Configure VRF Lite

- Objective 4.7.1 Create the uplink trunk segment
- Objective 4.7.2 Deploy and configure the VRF gateways
- Objective 4.7.3 Deploy and connect the Tier-1 gateways to the VRF gateways
- Objective 4.7.4 Create and connect segments to the Tier-1 gateways
- Objective 4.7.5 Attach VMs to segments on each VRF
- Objective 4.7.6 Review the routing tables in each VRF

Objective 4.8 Configure the NSX Distributed Firewall

- Objective 4.8.1 Create security group
- Objective 4.8.2 Create Distributed Firewall rules

Objective 4.9 Configure the NSX Gateway Firewall

- Objective 4.9.1 Configure a gateway firewall rule to block external SSH requests

Objective 4.10 Configure Intrusion Detection

- Objective 4.10.1 Enable Distributed Intrusion Detection and Prevention
- Objective 4.10.2 Download the Intrusion Detection and Prevention signatures
- Objective 4.10.3 Create an Intrusion Detection and Prevention profile
- Objective 4.10.4 Configure Intrusion Detection rules
- Objective 4.10.5 Configure North-South IDS/IPS
- Objective 4.10.6 Create a segment and attach a VM
- Objective 4.10.7 Analyze Intrusion Detection events
- Objective 4.10.8 Modify the IDS/IPS settings to prevent malicious traffic
- Objective 4.10.9 Analyze Intrusion Prevention events

Objective 4.11 Deploy NSX Application Platform

Objective 4.12 Configure malware prevention for East-West and North-South Traffic

Objective 4.13 Use NSX Network Detection and Response to detect threats

Objective 4.14 Configure Network Address Translation

- Objective 4.14.1 Create a Tier-1 gateway for Network Address Translation
- Objective 4.14.2 Create a segment

Objective 4.14.3 Attach a VM to NAT segment

Objective 4.14.4 Configure NAT

Objective 4.14.5 Configure NAT route redistribution

Objective 4.15 Configure NSX Advanced Load Balancer

Objective 4.15.1 Create segments for the NSX Advanced Load Balancer

Objective 4.15.2 Deploy the NSX Advanced Load Balancer controller

Objective 4.15.3 Access the NSX Advanced Load Balancer UI

Objective 4.15.4 Create a Cloud Connector for NSX

Objective 4.15.5 Configure Service Engine Networks and Routing

Objective 4.15.6 Create a virtual service

Objective 4.15.7 Configure route advertisement and route redistribution for a virtual IP

Objective 4.16 Deploy Virtual Private Networks

Objective 4.16.1 Deploy a new NSX Edge Node to support a VPN deployment

Objective 4.16.2 Configure a new Edge Cluster

Objective 4.16.3 Deploy and configure a new Tier-0 gateway and segments for VPN support

Objective 4.16.4 Create an IPSec VPN service

Objective 4.16.5 Create an L2 VPN server and session

Objective 4.16.6 Configure a pre-deployed autonomous Edge as an L2 VPN client

Objective 4.17 Manage users and roles

Objective 4.17.1 Add an Active Directory Domain as an identity source

Objective 4.17.2 Assign NSX roles to domain users and validate permissions

Objective 4.17.3 Modify an existing role and validate the role permissions

Objective 4.18 Perform operations tasks in a VMware NSX environment (syslog, backup/restore etc.)

Objective 4.19 Monitor a VMware NSX implementation

## Section 5 – Troubleshoot and Optimize the VMware Solution

Objective 5.1 – Use log files to troubleshoot issues

Objective 5.1.1 Identify the default log file locations of NSX components

Objective 5.1.2 Generate Log Bundles

Objective 5.1.3 Use log files to help identify NSX issues

Objective 5.2 Identify Tools Available for Troubleshooting Issues

Objective 5.3 Troubleshoot Common NSX Issues

Objective 5.3.1 Troubleshoot Common NSX Installation/Configuration Issues

Objective 5.3.2 Troubleshoot Common NSX Component Issues

Objective 5.3.3 Troubleshoot Common Connectivity Issues

Objective 5.3.4 Troubleshoot Common physical infrastructure Issues

Courses used to develop this exam and strongly recommended to you for exam preparation:

VMware NSX: Install, Configure, Manage [V4.0]

Certification Requirements

VCP-NV 2024

## References

No additional resources.

## Exam Contributors

Ross Wynne
Rick Watson
Jennifer Schmidt
Tim Burkard
Marco van Baggum
Ronak Patel
Karel Novak
Arantxa Duque Barrachina
Jens Hennig
Chand Basha Shaik
Abdullah Abdullah
Iwan Hoogendoorn
Tobias Paschek
Reinhard Partman
Tommy Grot
Christian Parker
Jiri Viktorin
Nicola Marco Decandia

**VMware, Inc.** 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com © 2024 VMware, Inc. All rights reserved. The product or workshop materials is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/download/patents.html. VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies. VMware warrants that it will perform these workshop services in a reasonable manner using generally accepted industry standards and practices. THE EXPRESS WARRANTY SET FORTH IS IN LIEU OF ALL OTHER WARRANTIES, EXPRESS, IMPLIED, STATUTORY OR OTHERWISE INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE WITH RESPECT TO THE SERVICES AND DELIVERABLES PROVIDED BY VMWARE, OR AS TO THE RESULTS WHICH MAY BE OBTAINED THEREFROM. VMWARE WILL NOT BE LIABLE FOR ANY THIRD-PARTY SERVICES OR PRODUCTS IDENTIFIED OR REFERRED TO CUSTOMER. All materials provided in this workshop are copyrighted by VMware ("Workshop Materials"). VMware grants the customer of this workshop a license to use and make reasonable copies of any Workshop Materials strictly for the purpose of facilitating such company's internal understanding, utilization and operation of its licensed VMware product(s). Except as set forth expressly in the sentence above, there is no transfer of any intellectual property rights or any other license granted under the terms of this workshop. If you are located in the United States, the VMware contracting entity for the service will be VMware, Inc., and if outside of the United States, the VMware contracting entity will be VMware International Limited.

REV. 1/24