VMware 2V0-41.23

VMWARE VCP-NV 2024 CERTIFICATION QUESTIONS & ANSWERS

Exam Summary – Syllabus – Questions

2V0-41.23

[VMware Certified Professional - Network Virtualization 2024 (VCP-NV 2024)]

70 Questions Exam – 300 / 500 Cut Score – Duration of 135 minutes

www.VMExam.com

Table of Contents

Know Your 2V0-41.23 Certification Well:

The 2V0-41.23 is best suitable for candidates who want to gain knowledge in the VMware Network Virtualization. Before you start your 2V0-41.23 preparation you may struggle to get all the crucial Network Virtualization 2024 materials like 2V0-41.23 syllabus, sample questions, study guide.

But don't worry the 2V0-41.23 PDF is here to help you prepare in a stress free manner.

The PDF is a combination of all your queries like-

- What is in the 2V0-41.23 syllabus?
- How many questions are there in the 2V0-41.23 exam?
- Which Practice test would help me to pass the 2V0-41.23 exam at the first attempt?

Passing the 2V0-41.23 exam makes you VMware Certified Professional - Network Virtualization 2024 (VCP-NV 2024). Having the Network Virtualization 2024 certification opens multiple opportunities for you. You can grab a new job, get a higher salary or simply get recognition within your current organization.

VMware 2V0-41.23 Network Virtualization 2024 Certification Details:

Exam Name	VMware NSX 4.x Professional (VCP-NV 2024)
Exam Code	2V0-41.23
Exam Price	$250 USD
Duration	135 minutes
Number of Questions	70
Passing Score	300 / 500
Recommended Training / Books	**VMware NSX: Install, Configure, Manage [4.0]**
Schedule Exam	**PEARSON VUE**
Sample Questions	**VMware 2V0-41.23 Sample Questions**
Recommended Practice	**VMware Certified Professional - Network Virtualization 2024 (VCP-NV 2024) Practice Test**

2V0-41.23 Syllabus:

Section	**Objectives**
IT Architectures, Technologies, Standards	
VMware Solution	- Demonstrate knowledge of VMware Virtual Cloud Network and NSX • Describe the purpose of VMware Virtual Cloud Network and its framework • Identify the benefits and recognize the use cases for NSX • Describe how NSX fits into the NSX product portfolio • Recognize features and the main elements in the NSX Data Center architecture • Describe NSX policy and centralized policy management • Describe the NSX management cluster and the management plane • Identify the functions of control plane components, data plane components, and communication channels - Demonstrate knowledge of NSX Management Cluster • Explain the deployment workflows for the NSX infrastructure - Demonstrate knowledge of the NSX UI • Distinguish between the Policy and the Manager UI - Demonstrate knowledge of the data plane • Describe the functions of transport zones, transport nodes, VDS, and N-VDS • Explain the relationships among transport nodes, transport zones, VDS, and N-VDS • Describe NSX Data Center on VDS • Describe uplink profiles - Demonstrate knowledge of logical switching • Describe the functions of NSX Data Center segments • Recognize different types of segments • Explain tunneling and the Geneve encapsulation protocol • Describe the interaction between components in logical switching • Describe the function of kernel modules and NSX agents installed on ESXi

Section	Objectives
	• Describe the function of the management plane in logical switching • Describe the function of the control plane in logical switching - Demonstrate knowledge of logical switching packet forwarding • Describe the functions of each table used in packet forwarding • Describe how BUM traffic is managed in switching • Explain how ARP suppression is achieved - Demonstrate knowledge of segments and segment profiles • Define what a segment is • Describe the purpose of segment profiles • Identify the functions of the segment profiles in NSX - Demonstrate knowledge of logical routing • Explain the function and features of logical routing • Describe the architecture of NSX two-tier routing • Differentiate between north-south and east-west routing • Describe the gateway components • Recognize the various types of gateway interfaces - Demonstrate knowledge of NSX Edge and Edge Clusters • Explain the main functions and features of the NSX Edge node • Describe the functions of the NSX Edge cluster • Identify the NSX Edge node form factors and sizing options • Describe the different NSX Edge node deployment methods - Demonstrate knowledge of Tier-0 and Tier-1 Gateways • Describe how to configure a Tier-1 gateway • Explain how to configure a Tier-0 gateway • Explain Active/Active Tier-0 and Tier-1 configurations • Explain multi-tenancy use in a Tier-0 gateway - Demonstrate knowledge of static and dynamic routing • Distinguish between static and dynamic routing - Demonstrate knowledge of ECMP and high availability

Section	Objectives
	- Explain the purpose of ECMP routing - Identify the active-active and active-standby modes for high availability - Recognize failure conditions and explain the failover process - Demonstrate knowledge of logical routing packet walk - Describe the datapath of single-tier routing - Explain the datapath of multitier routing - Demonstrate knowledge of VRF Lite - Describe VRF Lite - Explain the benefits of VRF Lite - Demonstrate knowledge of logical bridging - Describe the purpose and function of logical bridging - Distinguish between routing and bridging - Demonstrate knowledge of NSX segmentation - Define NSX segmentation - Recognize use cases for NSX segmentation - Identify steps to enforce Zero-Trust with NSX segmentation - Demonstrate knowledge of distributed firewall - Identify types of firewalls in NSX - Describe features of distributed firewalls - Describe the distributed firewall architecture - Demonstrate knowledge of security in distributed firewall on VDS - List the distributed firewall on VDS requirements - Demonstrate knowledge of NSX Gateway Firewall - Describe the functions of the gateway firewall - Explain the purpose of a gateway policy - Describe the gateway firewall architecture - Demonstrate knowledge of Intrusion Detection and Prevention - Explain NSX IDS/IPS and its use cases - Define the NSX IDS/IPS Detection terminology - Describe the NSX IDS/IPS architecture

Section	Objectives
	- Demonstrate knowledge of NSX Application Platform • Describe NSX Application Platform and its use cases • Explain the NSX Application Platform architecture and services - Demonstrate knowledge of malware prevention • Identify use cases for malware prevention • Identify the components in the malware prevention architecture • Describe the malware prevention packet flows for known and unknown files - Demonstrate knowledge of NSX Intelligence • Describe NSX Intelligence and its use cases • Explain NSX Intelligence system requirements • Explain NSX Intelligence visualization, recommendation, and network traffic analysis capabilities - Demonstrate NSX Network Detection and Response • Describe NSX Network Detection and Response and its use cases • Explain the architecture of NSX Network Detection and Response in NSX • Describe the visualization capabilities of NSX Network Detection and Response - Demonstrate knowledge of NAT and how it is used with NSX • Explain the role of network address translation (NAT) • Distinguish between source and destination NAT • Describe how Reflexive NAT works • Explain how NAT64 facilitates communication between IPv6 and IPv4 networks • Describe stateful active-active NAT operation - Demonstrate knowledge of DHCP and DNS • Explain how DHCP and DHCP Relay are used for IP address allocation • Configure DHCP services in NSX • Describe how to use a DNS forwarder service - Demonstrate knowledge of NSX Advanced Load Balancer • Describe NSX Advanced Load Balancer and its use cases

Section	Objectives
	• Explain the NSX Advanced Load Balancer architecture • Explain the NSX Advanced Load Balancer components and how they manage traffic - Demonstrate knowledge of IPSec VPN • Explain how IPSec-based technologies are used to establish VPNs • Compare policy-based and route-based IPSec VPN • Describe IPSec VPN requirements in NSX - Demonstrate knowledge of L2 VPN • Describe L2 VPN technologies in an NSX • Identify various supported L2 VPN endpoints - Demonstrate knowledge of integrating NSX with VMware Identity Manager • Describe the purpose of VMware Identity Manager • Identify the benefits of integrating NSX with VMware Identity Manager - Demonstrate knowledge of integrating NSX with LDAP • Identify the benefits of integrating NSX with LDAP • Describe the LDAP authentication architecture - Demonstrate knowledge of managing users and configuring RBAC • Identify the different types of users in NSX • Recognize permissions and roles available in NSX - Demonstrate knowledge of Federation Architecture, needed prerequisites, Federation Networking, and Federation Security • Describe Federation and its use cases • Describe the requirements and limitations of Federation • Describe the Federation configuration workflow • Describe the prerequisites for Federation • Describe the onboarding of Local Manager configurations and workloads • Describe the stretched networking concepts in Federation • Explain the supported Tier-0 and Tier-1 stretched topologies • Explain Layer 2 concepts related to NSX Federation • Explain the Federation security use cases • Describe the Federation security components

Section	**Objectives**
	• Explain the security configuration workflows - Demonstrate knowledge of DPU-based acceleration for NSX
Plan and Design the VMware Solution	
Install, Configure, Administrate the VMware Solution	- Prepare an NSX infrastructure for deployment • Create Transport Zones • Create IP Pools • Prepare ESXi Hosts - Configure segments • Create segments • Attach VMs to segments • Use network topology to validate the logical switching configuration - Deploy and configure NSX Edge Nodes • Deploy NSX Edge Nodes • Configure an Edge Cluster - Configure the Tier-1 gateway • Create a Tier-1 gateway • Connect segments to the Tier-1 gateway • Use network topology to validate the Tier-1 gateway configuration - Create and configure a Tier-0 gateway with OSPF • Create uplink segments • Create a Tier-0 gateway • Connect the Tier-0 and Tier-1 gateways • Use network topology to validate the Tier-0 gateway configuration - Configure the Tier-0 gateway with BGP • Create uplink segments • Create a Tier-0 gateway • Connect the Tier-0 and Tier-1 gateways • Use network topology to validate the Tier-0 gateway configuration - Configure VRF Lite • Create the uplink trunk segment • Deploy and configure the VRF gateways • Deploy and connect the Tier-1 gateways to the VRF

Section	Objectives
	gateways • Create and connect segments to the Tier-1 gateways • Attach VMs to segments on each VRF • Review the routing tables in each VRF - Configure the NSX Distributed Firewall • Create security group • Create Distributed Firewall rules - Configure the NSX Gateway Firewall • Configure a gateway firewall rule to block external SSH requests - Configure Intrusion Detection • Enable Distributed Intrusion Detection and Prevention • Download the Intrusion Detection and Prevention signatures • Create an Intrusion Detection and Prevention profile • Configure Intrusion Detection rules • Configure North-South IDS/IPS • Create a segment and attach a VM • Analyze Intrusion Detection events • Modify the IDS/IPS settings to prevent malicious traffic • Analyze Intrusion Prevention events - Deploy NSX Application Platform - Configure malware prevention for East-West and North-South Traffic - Use NSX Network Detection and Response to detect threats - Configure Network Address Translation • Create a Tier-1 gateway for Network Address Translation • Create a segment • Attach a VM to NAT segment • Configure NAT • Configure NAT route redistribution - Configure NSX Advanced Load Balancer • Create segments for the NSX Advanced Load Balancer • Deploy the NSX Advanced Load Balancer controller • Access the NSX Advanced Load Balancer UI • Create a Cloud Connector for NSX • Configure Service Engine Networks and Routing • Create a virtual service

Section	Objectives
	• Configure route advertisement and route redistribution for a virtual IP - Deploy Virtual Private Networks • Deploy a new NSX Edge Node to support a VPN deployment • Configure a new Edge Cluster • Deploy and configure a new Tier-0 gateway and segments for VPN support • Create an IPSec VPN service • Create an L2 VPN server and session • Configure a pre-deployed autonomous Edge as an L2 VPN client - Manage users and roles • Add an Active Directory Domain as an identity source • Assign NSX roles to domain users and validate permissions • Modify an existing role and validate the role permissions - Perform operations tasks in a VMware NSX environment (syslog, backup/restore etc.) - Monitor a VMware NSX implementation
Troubleshoot and Optimize the VMware Solution	- Use log files to troubleshoot issues • Identify the default log file locations of NSX components • Generate Log Bundles • Use log files to help identify NSX issues - Identify Tools Available for Troubleshooting Issues - Troubleshoot Common NSX Issues • Troubleshoot Common NSX Installation/Configuration Issues • Troubleshoot Common NSX Component Issues • Troubleshoot Common Connectivity Issues • Troubleshoot Common physical infrastructure Issues

VMware 2V0-41.23 Sample Questions:

Question: 1

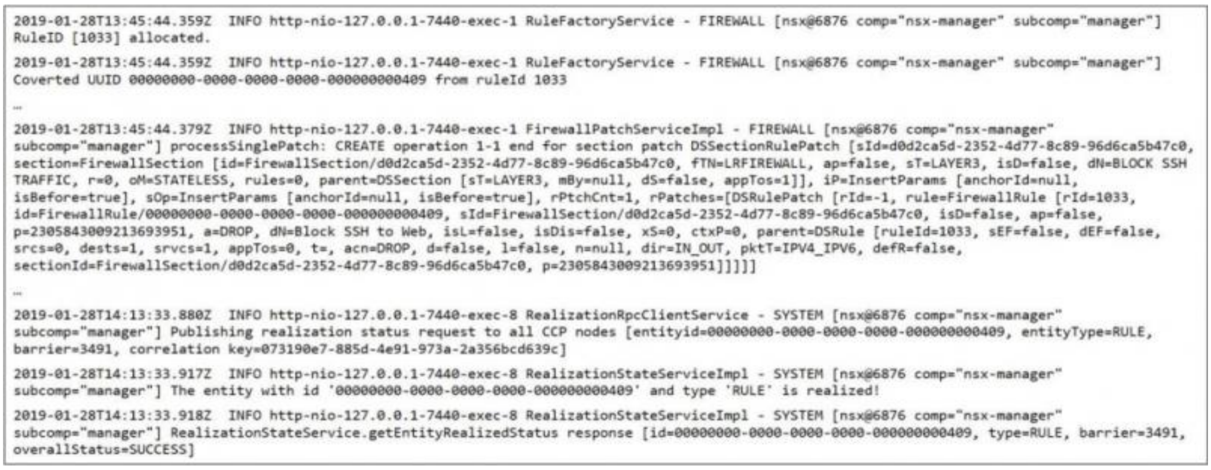
Which command is used to set the NSX Manager's logging-level to debug mode for troubleshooting?

a) set service manager log-level debug
b) set service nsx-manager logging-level debug
c) set service manager logging-level debug
d) set service nsx-manager log-level debug

Answer: c

Question: 2

Refer to the exhibit.



```
2019-01-28T13:45:44.359Z  INFO http-nio-127.0.0.1-7440-exec-1 RuleFactoryService - FIREWALL [nsx@6876 comp="nsx-manager" subcomp="manager"]
RuleID [1033] allocated.

2019-01-28T13:45:44.359Z  INFO http-nio-127.0.0.1-7440-exec-1 RuleFactoryService - FIREWALL [nsx@6876 comp="nsx-manager" subcomp="manager"]
Coverted UUID 00000000-0000-0000-0000-000000000409 from ruleId 1033

…

2019-01-28T13:45:44.379Z  INFO http-nio-127.0.0.1-7440-exec-1 FirewallPatchServiceImpl - FIREWALL [nsx@6876 comp="nsx-manager"
subcomp="manager"] processSinglePatch: CREATE operation 1-1 end for section patch DSSectionRulePatch [sId=d0d2ca5d-2352-4d77-8c89-96d6ca5b47c0,
section=FirewallSection [id=FirewallSection/d0d2ca5d-2352-4d77-8c89-96d6ca5b47c0, fTN=LRFIREWALL, ap=false, sT=LAYER3, isD=false, dN=BLOCK SSH
TRAFFIC, r=0, oM=STATELESS, rules=0, parent=DSSection [sT=LAYER3, mBy=null, dS=false, appTos=1]], iP=InsertParams [anchorId=null,
isBefore=true], sOp=InsertParams [anchorId=null, isBefore=true], rPtchCnt=1, rPatches=[DSRulePatch [rId=-1, rule=FirewallRule [rId=1033,
id=FirewallRule/00000000-0000-0000-0000-000000000409, sId=FirewallSection/d0d2ca5d-2352-4d77-8c89-96d6ca5b47c0, isD=false, ap=false,
p=2305843009213693951, a=DROP, dN=Block SSH to Web, isL=false, isDis=false, xS=0, ctxP=0, parent=DSRule [ruleId=1033, sEF=false, dEF=false,
srcs=0, dests=1, srvcs=1, appTos=0, t=, acn=DROP, d=false, l=false, n=null, dir=IN_OUT, pktT=IPV4_IPV6, defR=false,
sectionId=FirewallSection/d0d2ca5d-2352-4d77-8c89-96d6ca5b47c0, p=2305843009213693951]]]]]

…

2019-01-28T14:13:33.880Z  INFO http-nio-127.0.0.1-7440-exec-8 RealizationRpcClientService - SYSTEM [nsx@6876 comp="nsx-manager"
subcomp="manager"] Publishing realization status request to all CCP nodes [entityid=00000000-0000-0000-0000-000000000409, entityType=RULE,
barrier=3491, correlation key=073190e7-885d-4e91-973a-2a356bcd639c]

2019-01-28T14:13:33.917Z  INFO http-nio-127.0.0.1-7440-exec-8 RealizationStateServiceImpl - SYSTEM [nsx@6876 comp="nsx-manager"
subcomp="manager"] The entity with id '00000000-0000-0000-0000-000000000409' and type 'RULE' is realized!

2019-01-28T14:13:33.918Z  INFO http-nio-127.0.0.1-7440-exec-8 RealizationStateServiceImpl - SYSTEM [nsx@6876 comp="nsx-manager"
subcomp="manager"] RealizationStateService.getEntityRealizedStatus response [id=00000000-0000-0000-0000-000000000409, type=RULE, barrier=3491,
overallStatus=SUCCESS]
```

A security administrator has configured a gateway firewall rule to block traffic to all Web servers. What can the administrator infer about the rule publication after reviewing the log extract?

a) The user has no permission to create gateway firewall rules.
b) The rule has been successfully realized in the NSX Manager.
c) The rule has been successfully realized in the data path.
d) There was a communication problem with the Central Control Plane.

Answer: a, b

Question: 3

Which discovery protocol is supported for hypervisor transport nodes?

a) Link Layer Discovery Protocol
b) Cisco Discovery Protocol
c) Neighbor Discovery Protocol
d) Adobe Real-time CDP

Answer: a

Question: 4

Which three protocols could an NSX administrator use to transfer log messages to a remote log server?

(Choose three.)

a) TCP
b) SSL
c) UDP
d) HTTPS
e) TLS
f) SSH

Answer: a, c, e

Question: 5

Which two tools could be used to view NSX Policy logs?

(Choose two.)

a) NSX Manager CLI
b) NSX Manager root privileged mode
c) ESXI host nsxcli
d) KVM host nsxcli
e) Edge CLI

Answer: a, b

Question: 6

Which three networking features could be configured using the NSX Manager Simplified UI?

(Choose three.)

a) NAT Rules
b) containers
c) load balancers
d) logical routers
e) segments
f) logical switches

Answer: a, c, e

Question: 7

An administrator wants to validate the BGP connection status between the Tier-0 Gateway and the upstream physical router.

What sequence of commands could be used to check this status on NSX Edge node?

a) - set vrf <ID>
- show logical-routers- show <LR-D> bgp
b) - show logical-routers- get vrf
- show ip route bgp
c) - enable <LR-D>
- get vrf <ID>
- show bgp neighbor
d) - get logical-routers
- vrf <number>
- get bgp neighbor

Answer: d

Question: 8

A centralized packet analysis tool VM configured to monitor a NSX-T deployment is dropping some of the packets sent to it.

Which three actions could minimize the drops?

(Choose three.)

a) Increase the RX buffer ring size.
b) Assign more CPU resources to the VM.
c) Use DPDK to improve packet processing performance.
d) Ensure the host 10GbE NIC is configured for full duplex.
e) Increase the TX buffer ring size.
f) Increase MTU on the VM to 9000.

Answer: a, b, c

Question: 9

Which two VMware Cloud Management systems are compatible with NSX-T Data Center capabilities?

(Choose two.)

a) VMware Power CLI
b) vRealize Automation
c) vRealize CodeStream
d) VMware Integrated OpenStack
e) VMware vSphere

Answer: b, d

Question: 10

Which CLI command does a NSX administrator use to obtain information about the NSX Manager configuration when troubleshooting a production system?

a) show configuration
b) get managers
c) show interface
d) get configuration

Answer: b

Study Guide to Crack VMware Network Virtualization 2024 2V0-41.23 Exam:

- Getting details of the 2V0-41.23 syllabus, is the first step of a study plan. This pdf is going to be of ultimate help. Completion of the syllabus is must to pass the 2V0-41.23 exam.
- Making a schedule is vital. A structured method of preparation leads to success. A candidate must plan his schedule and follow it rigorously to attain success.
- Joining the VMware provided training for 2V0-41.23 exam could be of much help. If there is specific training for the exam, you can discover it from the link above.
- Read from the 2V0-41.23 sample questions to gain your idea about the actual exam questions. In this PDF useful sample questions are provided to make your exam preparation easy.
- Practicing on 2V0-41.23 practice tests is must. Continuous practice will make you an expert in all syllabus areas.