2V0-41.23 Q&As

VMware NSX 4.x Professional

Pass VMware 2V0-41.23 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/2v0-41-23.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by VMware Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Which of the two following characteristics about NAT64 are true? (Choose two.)

A. NAT64 is stateless and requires gateways to be deployed in active-standby mode.

B. NAT64 is supported on Tier-1 gateways only.

C. NAT64 is supported on Tier-0 and Tier-1 gateways.

D. NAT64 requires the Tier-1 gateway to be configured in active-standby mode.

E. NAT64 requires the Tier-1 gateway to be configured in active-active mode.

Correct Answer: CD

https://docs.vmware.com/en/VMware-NSX/4.1/administration/GUID-69604E49-BC8B-4777-BFD8-B98F8D1FF064.html

QUESTION 2

When configuring OSPF on a Tler-0 Gateway, which three of the following must match in order to establish a neighbor relationship with an upstream router? (Choose three.)

A. Naming convention

B. MTU of the Uplink

C. Subnet mask

D. Address of the neighbor

E. Protocol and Port

F. Area ID

Correct Answer: BCF

according to the VMware NSX Documentation, these are the three parameters that must match in order to establish an OSPF neighbor relationship with an upstream router on a tier-0 gateway: MTU of the Uplink: The maximum transmission unit (MTU) of the uplink interface must match the MTU of the upstream router interface. Otherwise, OSPF packets may be fragmented or dropped, causing neighbor adjacency issues. Subnet mask: The subnet mask of the uplink interface must match the subnet mask of the upstream router interface. Otherwise, OSPF packets may not reach the correct destination or be rejected by the upstream router. Area ID: The area ID of the uplink interface must match the area ID of the upstream router interface. Otherwise, OSPF packets may be ignored or discarded by the upstream router. https://www.computernetworkingnotes.com/ccna-study-guide/ospf-neighborship-condition-and-requirement.html

QUESTION 3

An NSX administrator is using ping to check connectivity between VM1 running on ESXi1 to VM2 running on ESXi2. The ping tests fails. The administrator knows the maximum transmission unit size on the physical switch is 1600.

Which command does the administrator use to check the VMware kernel ports for tunnel end point communication?

A. esxcli network diag ping-I vmk0O-H

B. vmkping ++netstack=geneve-d-s 1572

C. esxcli network diag ping-H

D. vmkping ++netstack=vxlan-d-s 1572

Correct Answer: B

The command vmkping ++netstack=geneve-d-s 1572 is used to check the VMware kernel ports for tunnel end point communication. This command uses the geneve netstack, which is the default netstack for NSX-T. The-d option sets the DF (Don\\'t Fragment) bit in the IP header, which prevents the packet from being fragmented by intermediate routers. The-s 1572 option sets the packet size to 1572 bytes, which is the maximum payload size for a geneve encapsulated packet with an MTU of 1600 bytes. The is the IP address of the remote ESXi host or VM. References: : VMware NSX-T Data Center Installation Guide, page 19. : VMware Knowledge Base: Testing MTU with the vmkping command (1003728). : VMware NSX-T Data Center Administration Guide, page 102.

QUESTION 4

Which two statements are true about IDS Signatures? (Choose two.)

A. Users can upload their own IDS signature definitions.

B. An IDS signature contains data used to identify known exploits and vulnerabilities.

C. An IDS signature contains data used to identify the creator of known exploits and vulnerabilities.

D. IDS signatures can be High Risk, Suspicious, Low Risk and Trustworthy.

E. An IDS signature contains a set of instructions that determine which traffic is analyzed.

Correct Answer: BE

According to the Network Bachelor article1, an IDS signature contains data used to identify an attacker\\'s attempt to exploit a known vulnerability in both the operating system and applications. This implies that statement B is true. According to the VMware NSX Documentation2, IDS/IPS Profiles are used to group signatures, which can then be applied to select applications and traffic. This implies that statement E is true. Statement A is false because users cannot upload their own IDS signature definitions, they have to use the ones provided by VMware or Trustwave3. Statement C is false because an IDS signature does not contain data used to identify the creator of known exploits and vulnerabilities, only the exploits and vulnerabilities themselves. Statement D is false because IDS signatures are classified into one of the following severity categories: Critical, High, Medium, Low, or Informational1. Reference: 3: Distributed IDS/IPS Settings and Signatures-VMware Docs 2: Distributed IDS/IPS-VMware Docs 1: NSX-T: Exploring Distributed IDS-Network Bachelor

QUESTION 5

Which two of the following features are supported for the Standard NSX Application Platform Deployment? (Choose two.)

A. NSX Intrusion Detection and Prevention

B. NSX Intelligence

C. NSX Network Detection and Response

D. NSX Malware Prevention Metrics

E. NSX Intrinsic Security

Correct Answer: CD

The NSX Application Platform Deployment features are divided into three form factors: Evaluation, Standard, and Advanced. Each form factor determines which NSX features can be activated or installed on the platform1. The Evaluation form factor supports only NSX Intelligence, which provides network visibility and analytics for NSX-T environments2. The Standard form factor supports both NSX Intelligence and NSX Network Detection and Response, which provides network threat detection and response capabilities for NSX-T environments3. The Advanced form factor supports all four features: NSX Intelligence, NSX Network Detection and Response, NSX Malware Prevention, and NSX Metrics1. https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.2/nsx-application-platform/GUID-85CD2728-8081-45CE-9A4A-D72F49779D6A.html