



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.geekcert.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 three NSX Edge components are used for North-South Malware Prevention? (Choose three.)

- A. Thin Agent
- B. RAPID
- C. Security Hub
- D. IDS/IPS
- E. Security Analyzer
- F. Reputation Service

Correct Answer: BCD

[https://docs.vmware.com/en/VMware-NSX/4.1/administration/GUID-69DF70C2-1769-4858-97E7B757CAED08F0.html#:~:text=On%20the%20north%2Dsouth%20traffic,Guest%20Introspection%20\(GI\)%20platform.](https://docs.vmware.com/en/VMware-NSX/4.1/administration/GUID-69DF70C2-1769-4858-97E7B757CAED08F0.html#:~:text=On%20the%20north%2Dsouth%20traffic,Guest%20Introspection%20(GI)%20platform.)

The main components on the edge node for north-south malware prevention perform the following functions:

?IDS/IPS engine: Extracts files and relays events and data to the security hub North-south malware prevention uses the file extraction features of the IDS/IPS engine that runs on NSX Edge for north-south traffic. ?Security hub: Collects file events, obtains verdicts for known files, sends files for local and cloud-based analysis, and sends information to the security analyzer ?RAPID: Provides local analysis of the file ?ASDS Cache: Caches reputation and verdicts of known files

QUESTION 2

What must be configured on Transport Nodes for encapsulation and decapsulation of Geneve protocol?

- A. VXIAN
- B. UDP
- C. STT
- D. TEP

Correct Answer: D

According to the VMware NSX Documentation, TEP stands for Tunnel End Point and is a logical interface that must be configured on transport nodes for encapsulation and decapsulation of Geneve protocol. Geneve is a tunneling protocol that encapsulates the original packet with an outer header that contains metadata such as the virtual network identifier (VNI) and the transport node IP address. TEPs are responsible for adding and removing the Geneve header as the packet traverses the overlay network.

QUESTION 3



Which two of the following will be used for Ingress traffic on the Edge node supporting a Single Tier topology? (Choose two.)

- A. Inter-Tier interface on the Tier-0 gateway
- B. Tier-0 Uplink interface
- C. Downlink Interface for the Tier-0 DR
- D. Tier-1 SR Router Port
- E. Downlink Interface for the Tier-1 DR

Correct Answer: BC

The two interfaces that will be used for ingress traffic on the Edge node supporting a Single Tier topology are:

B. Tier-0 Uplink interface

C. Downlink Interface for the Tier-0 DR The Tier-0 Uplink interface is the interface that connects the Tier-0 gateway to the external network. It is used to receive traffic from the physical router or switch that is the next hop for the Tier-0 gateway. The Tier-0 Uplink interface can be configured with a static IP address or use BGP to exchange routes with the external network. The Downlink Interface for the Tier-0 DR is the interface that connects the Tier-0 gateway to the workload segments. It is used to receive traffic from the VMs or containers that are attached to the segments. The Downlink Interface for the Tier-0 DR is a logical interface (LIF) that is distributed across all transport nodes that host the segments. The Downlink Interface for the Tier-0 DR has an IP address that acts as the default gateway for the VMs or containers on the segments.

QUESTION 4

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>



QUESTION 5

An architect receives a request to apply distributed firewall in a customer environment without making changes to the network and vSphere environment. The architect decides to use Distributed Firewall on VDS.

Which two of the following requirements must be met in the environment? (Choose two.)

- A. vCenter 8.0 and later
- B. NSX version must be 3.2 and later
- C. NSX version must be 3.0 and later
- D. VDS version 6.6.0 and later

Correct Answer: BD

Distributed Firewall on VDS is a feature of NSX-T Data Center that allows users to install Distributed Security for vSphere Distributed Switch (VDS) without the need to deploy an NSX Virtual Distributed Switch (N-VDS). This feature provides

NSX security capabilities such as Distributed Firewall (DFW), Distributed IDS/IPS, Identity Firewall, L7 App ID, FQDN Filtering, NSX Intelligence, and NSX Malware Prevention. To enable this feature, the following requirements must be met in

the environment:

The NSX version must be 3.2 and later¹. This is the minimum version that supports Distributed Security for VDS.

The VDS version must be 6.6.0 and later¹. This is the minimum version that supports the NSX host preparation operation that activates the DFW with the default rule set to allow.

References:

Overview of NSX IDS/IPS and NSX Malware Prevention

[Latest 2V0-41.23 Dumps](#)

[2V0-41.23 Practice Test](#)

[2V0-41.23 Exam Questions](#)