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 command Is used to test management connectivity from a transport node to NSX Manager?

A. esxcli network ip connection list | grep 1234

B. esxcli network connection list | grep 1235

C. esxcli network ip connection list | grep 1235

D. esxcli network connection list | grep 1234

Correct Answer: C

The NSX Manager management plane communicates with the transport nodes by using APH Server over NSX-RPC/TCP through port 1234. CCP communicates with the transport nodes by using APH Server over NSX-RPC/TCP through port 1235. Reference: https://docs.vmware.com/en/VMware-NSX/4.1/installation/GUID-FD3140B2-81BD-4FE7-9A23-4EB55B4E3099.html

QUESTION 2

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

QUESTION 3

Where in the NSX UI would an administrator set the time attribute for a time-based Gateway Firewall rule?

A. The option to set time-based rule is a clock Icon in the rule.

B. The option to set time based rule is a field in the rule Itself.

C. There Is no option in the NSX UI. It must be done via command line interface.

D. The option to set time-based rule is a clock Icon in the policy.

Correct Answer: D

According to the VMware documentation1, the clock icon appears on the firewall policy section that you want to have a time window. By clicking the clock icon, you can create or select a time window that applies to all the rules in that policy section. The other options are incorrect because they either do not exist or are not related to the time-based rule feature. There is no option to set a time-based rule in the rule itself, as it is a policy-level setting. There is also an option to set a time-based rule in the NSX UI, so it does not require using the command line interface.
https://docs.vmware.com/en/VMware-NSX/4.1/administration/GUID-8572496E-A60E-48C3-A016-4A081AC80BE7.html

QUESTION 4

NSX improves the security of today\\'s modern workloads by preventing lateral movement, which feature of NSX can be used to achieve this?

A. Network Segmentation

B. Virtual Security Zones

C. Edge Firewalling

D. Dynamic Routing

Correct Answer: A

According to the web search results, network segmentation is a feature of NSX that improves the security of today\\'s modern workloads by preventing lateral movement. Lateral movement is a technique used by attackers to move from one compromised system to another within a network, exploiting vulnerabilities or credentials . Network segmentation prevents lateral movement by dividing a network into smaller segments or zones, each with its own security policies and controls. This way, if one segment is compromised, the attacker cannot access other segments or resources . NSX enables network segmentation by using micro-segmentation, which applies granular firewall rules at the virtual machine level, regardless of the physical network topology .

QUESTION 5

When a stateful service is enabled for the first lime on a Tier-0 Gateway, what happens on the NSX Edge node\\'

A. SR is instantiated and automatically connected with DR.

B. DR Is instantiated and automatically connected with SR.

C. SR and DR Is instantiated but requites manual connection.

D. SR and DR doesn\\'t need to be connected to provide any stateful services.

Correct Answer: A

The answer is A. SR is instantiated and automatically connected with DR. SR stands for Service Router and DR stands for Distributed Router. They are components of the NSX Edge node that provide different functions1 The SR is responsible for providing stateful services such as NAT, firewall, load balancing, VPN, and DHCP. The DR is responsible for providing distributed routing and switching between logical segments and the physical network1 When a stateful service is enabled for the first time on a Tier-0 Gateway, the NSX Edge node automatically creates an SR instance and connects it with the existing DR instance. This allows the stateful service to be applied to the traffic that passes through the SR before reaching the DR2 According to the VMware NSX 4.x Professional uide, understanding the SR and DR components and their functions is one of the exam objectives3 To learn more about the SR and DR components and how they work on the NSX Edge node, you can refer to the following resources: VMware NSX Documentation: NSX Edge Components 1 VMware NSX 4.x Professional: NSX Edge Architecture VMware NSX 4.x Professional: NSX Edge Routing