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

The security administrator turns on logging for a firewall rule.

Where is the log stored on an ESXi transport node?

A. /var/log/vmware/nsx/firewall.log

B. /var/log/messages.log

C. /var/log/dfwpktlogs.log

D. /var/log/fw.log

Correct Answer: C

The log for a firewall rule on an ESXi transport node is stored in the /var/log/dfwpktlogs.log file. This file contains information about the packets that match or do not match the firewall rules, such as the source and destination IP addresses, ports, protocols, actions, and rule IDs. The log file can be viewed using the esxcli network firewall get command or the vSphere Client. https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.2/administration/GUID-D57429A1-A0A9-42BE-A299-0C3C3546ABF3.html

QUESTION 2

How does the Traceflow tool identify issues in a network?

A. Compares the management plane configuration states containing control plane traffic and error reporting from transport node agents.

B. Compares intended network state in the control plane with Tunnel End Point (TEP) keepalives in the data plane.

C. Injects ICMP traffic into the data plane and observes the results in the control plane.

D. Injects synthetic traffic into the data plane and observes the results in the control plane.

Correct Answer: D

The Traceflow tool identifies issues in a network by injecting synthetic traffic into the data plane and observing the results in the control plane. This allows the tool to identify any issues in the network and provide a detailed report on the problem. You can use the Traceflow tool to test connectivity between any two endpoints in your NSX-T Data Center environment.

QUESTION 3

Which CLI command is used for packet capture on the ESXi Node?

A. tcpdump

B. debug

C. pktcap-uw

D. set capture

Correct Answer: C

According to the VMware Knowledge Base, this CLI command is used for packet capture on the ESXi node. pktcap-uw stands for Packet Capture User World and is a tool that allows you to capture packets from various points in the network

stack of an ESXi host. You can use this tool to troubleshoot network issues or analyze traffic flows. The other options are either incorrect or not available for this task. tcpdump is not a valid CLI command for packet capture on the ESXi node,

as it is a tool that runs on Linux systems, not on ESXi hosts. debug is not a valid CLI command for packet capture on the ESXi node, as it is a generic term that describes the process of finding and fixing errors, not a specific tool or command.

set capture is not a valid CLI command for packet capture on the ESXi node, as it does not exist in the ESXi CLI.

https://kb.vmware.com/s/article/2051814

QUESTION 4

Which command is used to display the network configuration of the Tunnel Endpoint (TEP) IP on a bare metal transport node?

A. tepconfig

B. ifconfig

C. tcpdump

D. debug

Correct Answer: B

The command ifconfig is used to display the network configuration of the Tunnel Endpoint (TEP) IP on a bare metal transport node2. The TEP IP is assigned to a network interface on the bare metal server that is used for overlay traffic. The ifconfig command can show the IP address, netmask, broadcast address, and other information of the network interface. For example, the following command shows the network configuration of the TEP IP on a bare metal transport node with interface name ens192: ifconfig ens192 The output of the command would look something like this: ens192: flags=4163 mtu 1500 inet 10.10.10.10 netmask 255.255.255.0 broadcast 10.10.10.255 inet6 fe80::250:56ff:fe9a:1b8c prefixlen 64 scopeid 0x20 ether 00:50:56:9a:1b:8c txqueuelen 1000 (Ethernet) RX packets 123456 bytes 123456789 (123.4 MB) RX errors 0 dropped 0 overruns 0 frame 0 TX packets 234567 bytes 234567890 (234.5 MB) TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

The TEP IP in this example is 10.10.10.10.

References:

IBM Cloud Docs

QUESTION 5

Where is the insertion point for East-West network introspection?

A. Tier-0 router

B. Partner SVM

C. Guest VM vNIC

D. Host Physical NIC

Correct Answer: C

The insertion point for East-West network introspection is the Guest VM vNIC. Network introspection is a service insertion feature that allows third-party network services to be integrated with NSX. Network introspection enables traffic redirection from the Guest VM vNIC to a service virtual machine (SVM) that runs the partner service. The SVM can then inspect, monitor, or modify the traffic before sending it back to the original destination1. The other options are incorrect because they are not the insertion points for East-West network introspection. The Tier-0 router is used for North-South routing and network services. The partner SVM is the service virtual machine that runs the partner service, not the insertion point. The host physical NIC is not involved in network introspection. References: Network Introspection Settings