2V0-41.23Q&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 two tools are used for centralized logging in VMware NSX? (Choose two.)

A. VMware Aria Operations

B. Syslog Server

C. VMware Aria Automation

D. VMware Aria Operations for Logs

E. VMware Aria Operations for Networks

Correct Answer: BD

Two tools that are used for centralized logging in VMware NSX are Syslog Server and VMware Aria Operations for Logs. Syslog Server is a standard protocol for sending log messages from various network devices to a centralized server1. VMware NSX supports syslog for long term retention of logs and all NSX components can send syslog messages to a configured syslog server2. VMware Aria Operations for Logs is a VMware product that provides intelligent log analytics for NSX3. It provides monitoring and troubleshooting capabilities and customizable dashboards for network virtualization, flow analysis, and alerts3. The other options are incorrect because they are not tools for centralized logging in VMware NSX. VMware Aria Operations is a VMware product that provides operations management and automation for NSX4, but it is not the same as VMware Aria Operations for Logs. VMware Aria Automation is a VMware product that provides automation and orchestration for NSX5, but it is not related to logging. VMware Aria Operations for Networks is not a valid product name. References: Syslog, NSX Logging and System Events, VMware vRealize Log Insight for NSX, VMware vRealize Operations Management Pack for NSX, VMware vRealize Automation

QUESTION 2

When collecting support bundles through NSX Manager, which files should be excluded for potentially containing sensitive information?

A. Controller Files

B. Management Files

C. Core Files

D. Audit Files

Correct Answer: C

According to the VMware NSX Documentation1, core files and audit logs can contain sensitive information and should be excluded from the support bundle unless requested by VMware technical support. Controller files and management files are not mentioned as containing sensitive information. Reference: 1: Support Bundle Collection Tool-VMware Docs

Core files and Audit logs might contain sensitive information such as passwords or encryption keys.
https://docs.vmware.com/en/VMware-NSX/4.1/administration/GUID-73D9AF0D-4000-4EF2-AC66-6572AD1A0B30.html

QUESTION 3

As part of an organization\\'s IT security compliance requirement, NSX Manager must be configured for 2FA (two-factor authentication).

What should an NSX administrator have ready before the integration can be configured? O

A. Active Directory LDAP integration with OAuth Client added

B. VMware Identity Manager with an OAuth Client added

C. Active Directory LDAP integration with ADFS

D. VMware Identity Manager with NSX added as a Web Application

Correct Answer: B

To configure NSX Manager for two-factor authentication (2FA), an NSX administrator must have VMware Identity Manager (vIDM) with an OAuth Client added. vIDM provides identity management services and supports various 2FA methods, such as VMware Verify, RSA SecurID, and RADIUS. An OAuth Client is a configuration entity in vIDM that represents an application that can use vIDM for authentication and authorization. NSX Manager must be registered as an OAuth Client in vIDM before it can use 2FA. References: : VMware NSX-T Data Center Installation Guide, page 19. : VMware NSX-T Data Center Administration Guide, page 102. : VMware Blogs: Two-Factor Authentication with VMware NSX-T

QUESTION 4

An administrator has deployed 10 Edge Transport Nodes in their NSX Environment, but has forgotten to specify an NTP server during the deployment.

What is the efficient way to add an NTP server to all 10 Edge Transport Nodes?

A. Use Transport Node Profile

B. Use the CU on each Edge Node

C. Use a Node Profile

D. Use a PowerCU script

Correct Answer: C

A node profile is a configuration template that can be applied to multiple NSX Edge nodes or transport nodes at once. A node profile can include settings such as NTP server, DNS server, syslog server, and so on1. By using a node profile, an administrator can efficiently configure or update the network settings of multiple NSX Edge nodes or transport nodes in a single operation2. The other options are incorrect because they are either not efficient or not supported. Using the CLI on each Edge node would require manual and repetitive commands for each node, which is not efficient. Using a Transport Node Profile would not work, because a Transport Node Profile is used to configure the NSX-T Data Center components on a transport node, such as the transport zone, the N-VDS, and the uplink profiles3. Using a PowerCLI script might work, but it would require writing and testing a custom script, which is not as efficient as using a built-in feature like a node profile.

QUESTION 5

Which two of the following are used to configure Distributed Firewall on VDS? (Choose two.)

A. vSphere API

B. NSX API

C. NSX CU

D. vCenter API

E. NSX UI

Correct Answer: BE

According to the VMware NSX Documentation, these are two of the ways that you can use to configure Distributed Firewall on VDS:

NSX API: This is a RESTful API that allows you to programmatically configure and manage Distributed Firewall on VDS using HTTP methods and JSON payloads. You can use tools such as Postman or curl to send API requests to the NSX

Manager node.

NSX UI: This is a graphical user interface that allows you to configure and manage Distributed Firewall on VDS using menus, tabs, buttons, and forms. You can access the NSX UI by logging in to the NSX Manager node using a web browser.

https://docs.vmware.com/en/VMware-NSX/4.1/administration/GUID-0DEF9F18-608D-4B5C-9175-5514750E901B.html