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

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 2

What are the four types of role-based access control (RBAC) permissions? (Choose four.)

A. Read

B. None

C. Auditor

D. Full access

E. Enterprise Admin

F. Execute

G. Network Admin

Correct Answer: ABDF

The four types of role-based access control (RBAC) permissions are Read, None, Full access, and Execute1. Read permission allows the user to view the configuration and status of the system. None permission denies any access to the system. Full access permission grants all permissions including Create, Read, Update, and Delete (CRUD). Execute permission includes Read and Update permissions1. Auditor, Enterprise Admin, and Network Admin are not types of permissions, but types of roles that have different sets of permissions. References: NSX Features There are four types of permissions. Included in the list are the abbreviations for the permissions that are used in the Roles and Permissions

and Roles and Permissions for Manager Mode tables. Full access (FA)-All permissions including Create, Read, Update, and Delete Execute (E)-Includes Read and Update Read (R) None NSX-T Data Center has the following built-in roles. Role names in the UI can be different in the API. In NSX-T Data Center, if you have permission, you can clone an existing role, add a new role, edit newly created roles, or delete newly created roles. Role-Based Access Control (vmware.com)

QUESTION 3

An NSX administrator would like to create an L2 segment with the following requirements:

L2 domain should not exist on the physical switches.

East/West communication must be maximized as much as possible.

Which type of segment must the administrator choose?

A. VLAN

B. Overlay

C. Bridge

D. Hybrid

Correct Answer: B

An overlay segment is a layer 2 broadcast domain that is implemented as a logical construct in the NSX-T Data Center software. Overlay segments do not require any configuration on the physical switches, and they allow for optimal east/west communication between workloads on different ESXi hosts. Overlay segments use the Geneve protocol to encapsulate and decapsulate traffic between the hosts. Overlay segments are created and managed by the NSX Manager. https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.2/administration/GUID-316E5027-E588-455C-88AD-A7DA930A4F0B.html

QUESTION 4

Which VMware GUI tool is used to identify problems in a physical network?

A. VMware Aria Automation

B. VMware Aria Orchestrator

C. VMware Site Recovery Manager

D. VMware Aria Operations Networks

Correct Answer: D

According to the web search results, VMware Aria Operations Networks (formerly vRealize Network Insight) is a network monitoring tool that can help monitor, discover and analyze networks and applications across clouds1. It can also provide enhanced troubleshooting and visibility for physical and virtual networks2. The other options are either incorrect or not relevant for identifying problems in a physical network. VMware Aria Automation is a cloud automation platform that can help automate the delivery of IT services. VMware Aria Orchestrator is a cloud orchestration tool that can help automate workflows and integrate with other systems. VMware Site Recovery Manager is a disaster recovery

solution that can help protect and recover virtual machines from site failures.

QUESTION 5

A security administrator needs to configure a firewall rule based on the domain name of a specific application.

Which field in a distributed firewall rule does the administrator configure?

A. Profile

B. Service

C. Policy

D. Source

Correct Answer: A

To configure a firewall rule based on the domain name of a specific application, the administrator needs to use the Profile field in a distributed firewall rule. The Profile field allows the administrator to select a context profile that contains one or

more attributes for filtering traffic. One of the attributes that can be used is Domain (FQDN) Name, which specifies the fully qualified domain name of the application. For example, if the administrator wants to filter traffic to *.office365.com,

they can create a context profile with the Domain (FQDN) Name attribute set to *.office365.com and use it in the Profile field of the firewall rule.

References:

Filtering Specific Domains (FQDN/URLs)

FQDN Filtering