VMware

Exam Questions 2V0-41.23

VMware NSX 4.x Professional

NEW QUESTION 1
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

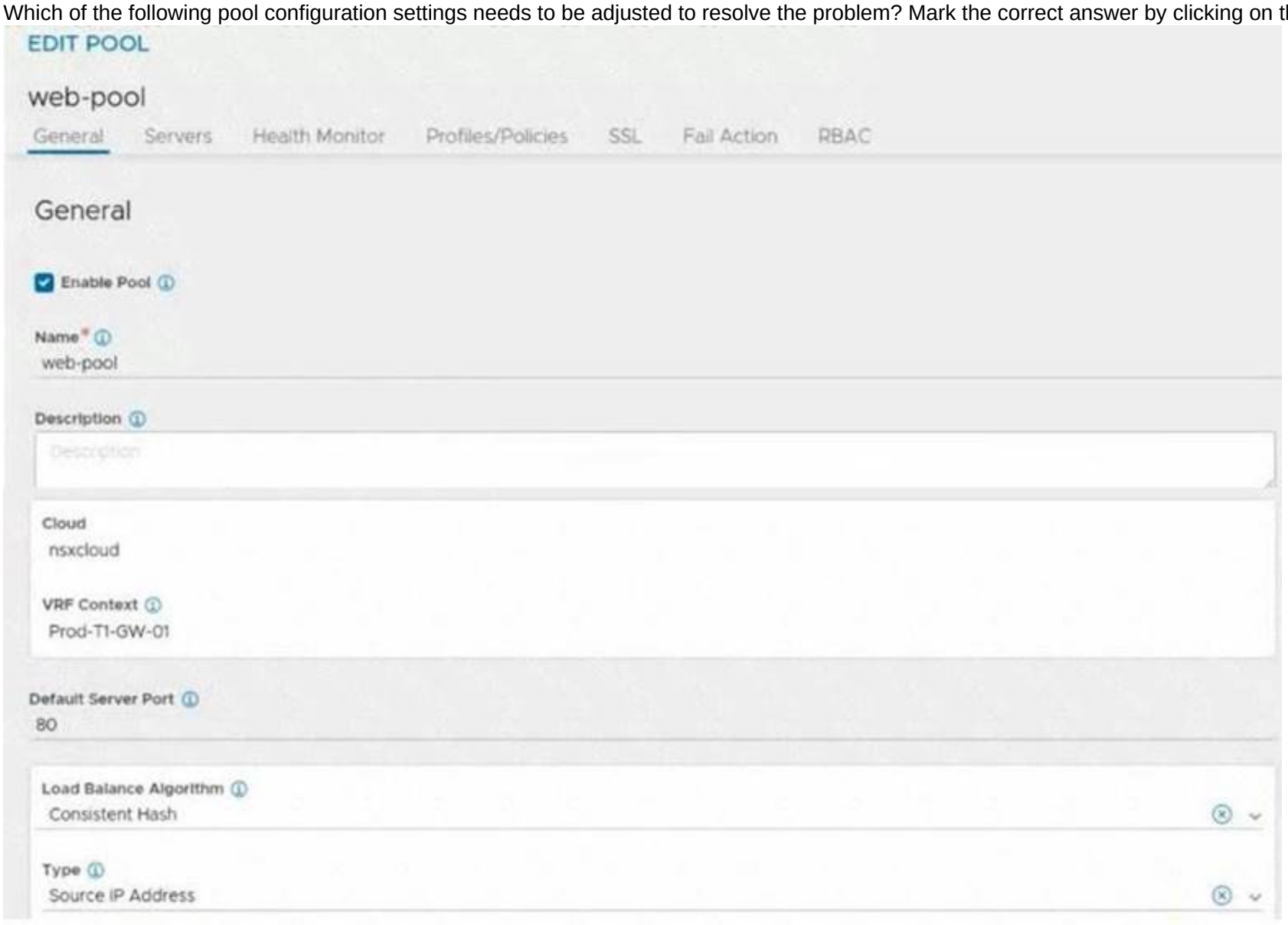
Answer: BC

Explanation:
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.

NEW QUESTION 2
Refer to the exhibit.
An administrator configured NSX Advanced Load Balancer to redistribute the traffic between the web servers. However, requests are sent to only one server
Which of the following pool configuration settings needs to be adjusted to resolve the problem? Mark the correct answer by clicking on the image.



Solution:
Load Balancing Algorithm

Does this meet the goal?

A. Yes
B. No

Answer: A

NEW QUESTION 3
Which two choices are solutions offered by the VMware NSX portfolio? (Choose two.)

A. VMware Tanzu Kubernetes Grid
B. VMware Tanzu Kubernetes Cluster
C. VMware NSX Advanced Load Balancer

D. VMware NSX Distributed IDS/IPS
E. VMware Aria Automation

Answer: CD

Explanation:
VMware NSX is a portfolio of networking and security solutions that enables consistent policy, operations, and automation across multiple cloud environments1
The VMware NSX portfolio includes the following solutions:

- VMware NSX Data Center: A platform for data center network virtualization and security that delivers a complete L2-L7 networking stack and overlay services for any workload1
- VMware NSX Cloud: A service that extends consistent networking and security to public clouds such as AWS and Azure1
- VMware NSX Advanced Load Balancer: A solution that provides load balancing, web application firewall, analytics, and monitoring for applications across any cloud12
- VMware NSX Distributed IDS/IPS: A feature that provides distributed intrusion detection and prevention for workloads across any cloud12
- VMware NSX Intelligence: A service that provides planning, observability, and intelligence for network and micro-segmentation1
- VMware NSX Federation: A capability that enables multi-site networking and security management with consistent policy and operational state synchronization1
- VMware NSX Service Mesh: A service that connects, secures, and monitors microservices across multiple clusters and clouds1
- VMware NSX for Horizon: A solution that delivers secure desktops and applications across any device, location, or network1
- VMware NSX for vSphere: A solution that provides network agility and security for vSphere environments with a built-in console in vCenter1
- VMware NSX-T Data Center: A platform for cloud-native applications that supports containers, Kubernetes, bare metal hosts, and multi-hypervisor environments1

VMware Tanzu Kubernetes Grid and VMware Tanzu Kubernetes Cluster are not part of the VMware NSX portfolio. They are solutions for running Kubernetes clusters on any cloud3
VMware Aria Automation is not a real product name. It is a fictional name that does not exist in the VMware portfolio.
https://blogs.vmware.com/networkvirtualization/2020/01/nsx-hero.html/

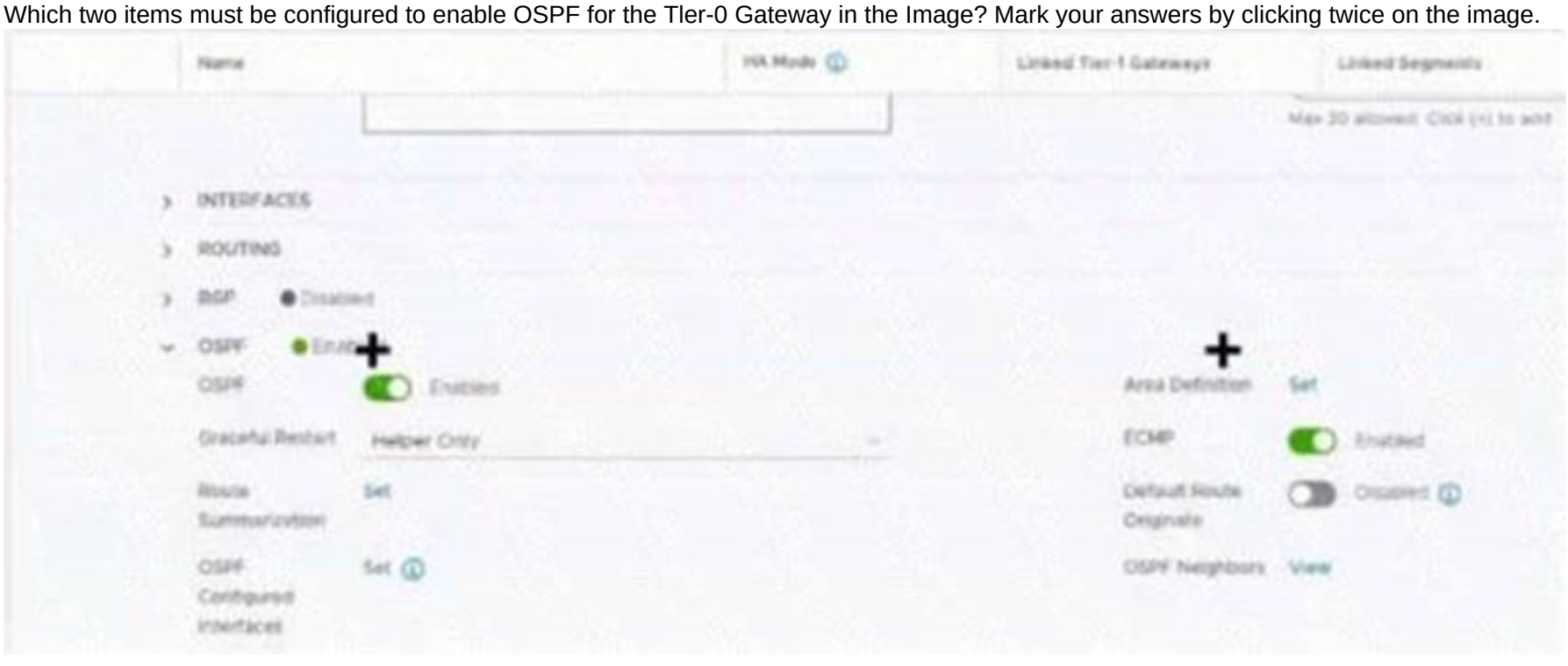
NEW QUESTION 4
Which two statements are true about IDS Signatures? (Choose two.)

A. Users can upload their own IDS signature definitions.
B. An IDS signature contains data used to identify known exploits and vulnerabilities.
C. An IDS signature contains data used to identify the creator of known exploits and vulnerabilities.
D. IDS signatures can be High Risk, Suspicious, Low Risk and Trustworthy.
E. An IDS signature contains a set of instructions that determine which traffic is analyzed.

Answer: BE

Explanation:
According to the Network Bachelor article1, an IDS signature contains data used to identify an attacker's attempt to exploit a known vulnerability in both the operating system and applications. This implies that statement B is true. According to the VMware NSX Documentation2, IDS/IPS Profiles are used to group signatures, which can then be applied to select applications and traffic. This implies that statement E is true. Statement A is false because users cannot upload their own IDS signature definitions, they have to use the ones provided by VMware or Trustwave3. Statement C is false because an IDS signature does not contain data used to identify the creator of known exploits and vulnerabilities, only the exploits and vulnerabilities themselves. Statement D is false because IDS signatures are classified into one of the following severity categories: Critical, High, Medium, Low, or Informational1.

NEW QUESTION 5
Refer to the exhibit.
Which two items must be configured to enable OSPF for the Tler-0 Gateway in the Image? Mark your answers by clicking twice on the image.



Solution:
The correct answer is to enable the OSPF toggle and to add an Area Definition for the Tier-0 gateway in image. These two items are required to configure OSPF on the Tier-0 gateway, as explained in the web search results123.
To mark your answers by clicking twice on the image, you can double-click on the toggle switch next to OSPF to turn it on. The switch should change from gray to blue, indicating that the option is enabled. The you can double-click on the Set button next to Area

Definition to add an area definition. A pop-up windo should appear where you can specify the area ID and type.
* 1. Click the OSPF toggle to enable OSPF 2. In the Area Definition field, click Set to add an area definition https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.2/administration/GUID-5BEC626C-5312-467D-B

Does this meet the goal?

A. Yes
B. No

Answer: A

NEW QUESTION 6
Which table on an ESXi host is used to determine the location of a particular workload for a frame-forwarding decision?

A. TEP Table
B. MAC Table
C. ARP Table
D. Routing Table

Answer: B

Explanation:
The MAC table on an ESXi host is used to determine the location of a particular workload for a
frame-forwarding decision. The MAC table maps the MAC addresses of the workloads to their corresponding tunnel endpoint (TEP) IP addresses. The TEP IP address identifies the ESXi host where the workload resides. The MAC table is populated by learning the source MAC addresses of the incoming frames from the workloads. The MAC table is also synchronized with other ESXi hosts in the same transport zone by using the NSX Controller.
https://nsx.techzone.vmware.com/resource/nsx-reference-design-guide

NEW QUESTION 7
Which CLI command shows syslog on NSX Manager?

A. get log-file auth.lag
B. /var/log/syslog/syslog.log
C. show log manager follow
D. get log-file syslog

Answer: D

Explanation:
According to the VMware NSX CLI Reference Guide, this CLI command shows the syslog messages on the NSX Manager node. You can use this command to view the system logs for troubleshooting or monitoring purposes.
The other options are either incorrect or not available for this task. get log-file auth.log is a CLI command that shows the authentication logs on the NSX Manager node, not the syslog messages. /var/log/syslog/syslog.log is not a CLI command, but a file path that may contain syslog messages on some Linux systems, but not on the NSX Manager node. show log manager follow is not a valid CLI command, as there is no show log command or manager option in the NSX CLI.
NSX Cli command get log-file <fiilename>
get log-file <filename> follow
Below are commonly used log files, there are many more log files
get log-file <auth.log | controller | controller-error | http.log | kern.log | manager.log | node-mgmt.log | policy.log | syslog> [follow]
use [follow] to continuing monitor Example: get log-file syslog follow get log-file syslog

NEW QUESTION 8
An NSX administrator is creating a Tier-1 Gateway configured In Active-Standby High Availability Mode. In the event of node failure, the failover policy should not allow the original tailed node to become the Active node upon recovery.
Which failover policy meets this requirement?

A. Non-Preemptive
B. Preemptive
C. Enable Preemptive
D. Disable Preemptive

Answer: A

Explanation:
According to the VMware NSX Documentation, a non-preemptive failover policy means that the original failed node will not become the active node upon recovery, unless the current active node fails again. This policy can help avoid unnecessary failovers and ensure stability.
The other options are either incorrect or not available for this configuration. Preemptive is the opposite of non-preemptive, meaning that the original failed node will become the active node upon recovery, if it has a higher priority than the current active node. Enable Preemptive and Disable Preemptive are not valid options for the failover policy, as the failover policy is a drop-down menu that only has two choices: Preemptive and Non-Preemptive.

NEW QUESTION 9
What are three NSX Manager roles? (Choose three.)

A. master
B. cloud
C. zookeepet
D. manager
E. policy
F. controller

Answer: DEF

Explanation:
According to the VMware NSX 4.x Professional documents and tutorials, an NSX Manager is a standalone appliance that hosts the API services, the management plane, control plane, and policy management. The NSX Manager has three built-in roles: policy, manager, and controller2. The policy role handles the declarative configuration of the system and translates it into desired state for the manager role. The manager role receives and validates the configuration from the policy role and stores it in a distributed persistent database. The manager role also publishes the configuration to the central control plane. The controller role implements the central control plane that computes the network state based on the configuration and topology information3. The other roles (master, cloud, and zookeeper) are not valid NSX Manager roles.

NEW QUESTION 10
Which NSX CLI command is used to change the authentication policy for local users?

A. Set cli-timeout
B. Get auth-policy minimum-password-length
C. Set hardening- policy
D. Set auth-policy

Answer: D

Explanation:
According to the VMware NSX Documentation4, the set auth-policy command is used to change the authentication policy settings for local users, such as password length, lockout period, and maximum authentication failures. The other commands are either used to view the authentication policy settings (B), change the CLI session timeout (A), or change the hardening policy settings ©.

NEW QUESTION 11
An NSX administrator would like to export syslog events that capture messages related to NSX host preparation events. Which message ID (msgld) should be used in the syslog export configuration command as a filler?

A. MONISTORING
B. SYSTEM
C. GROUPING
D. FABRIC

Answer: D

Explanation:
According to the VMware NSX Documentation2, the FABRIC message ID (msgld) captures messages related to NSX host preparation events, such as installation, upgrade, or uninstallation of NSX components on ESXi hosts. The syslog export configuration command for NSX host preparation events would look something like this:
set service syslog export FABRIC
The other options are either incorrect or not relevant for NSX host preparation events. MONITORING captures messages related to NSX monitoring features, such as alarms and system events2. SYSTEM captures messages related to NSX system events, such as login, logout, or configuration changes2. GROUPING captures messages related to NSX grouping objects, such as security groups, security tags, or IP sets2.
https://docs.vmware.com/en/VMware-NSX/4.1/administration/GUID-CC18C0E3-D076-41AA-8B8C-133650FD

NEW QUESTION 12
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

2V0-41.23 Practice Exam Features:

* 2V0-41.23 Questions and Answers Updated Frequently

* 2V0-41.23 Practice Questions Verified by Expert Senior Certified Staff

* 2V0-41.23 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* 2V0-41.23 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year