NSE5_FAZ-7.0^Q&As^

Fortinet NSE 5 - FortiAnalyzer 7.0

QUESTION 1

What is the purpose of output variables?

A. To store playbook execution statistics

B. To use the output of the previous task as the input of the current task

C. To display details of the connectors used by a playbook

D. To save all the task settings when a playbook is exported

Correct Answer: A

QUESTION 2

You crested a playbook on FortiAnalyzer that uses a FortiOS connector

When configuring the FortiGate side, which type of trigger must be used so that the actions in an automation stitch are available in the FortiOS connector?

A. FortiAnalyzer Event Handler

B. Incoming webhook

C. FortiOS Event Log

D. Fabric Connector event

Correct Answer: B

"One possible scenario is shown on the slide:

1.

Traffic flows through the FortiGate

2.

FortiGate sends logs to FortiAnalyzer

3.

FortiAnalyzer detects some suspicious traffic and generates an event

4.

The event triggers the execution of a playbook in FortiAnalyzer, which sends a webhook call to FortiGate so that it runs an automation stitch

5.

FortiGate runs the automation stitch with the corrective or preventive actions"

QUESTION 3

What remote authentication servers can you configure to validate your FortiAnalyzer administrator logons? (Choose three)

A. RADIUS

B. Local

C. LDAP

D. PKI

E. TACACS+

Correct Answer: ACE

QUESTION 4

What statements are true regarding the "store and upload" log transfer option between FortiAnalyzer and FortiGate? (Choose three.)

A. All FortiGates can send logs to FortiAnalyzer using the store and upload option.

B. Only FortiGate models with hard disks can send logs to FortiAnalyzer using the store and upload option.

C. Both secure communications methods (SSL and IPsec) allow the store and upload option.

D. Disk logging is enabled on the FortiGate through the CLI only.

E. Disk logging is enabled by default on the FortiGate.

Correct Answer: BCD

QUESTION 5

Which daemon is responsible for enforcing the log file size?

A. sqlplugind

B. logfiled

C. miglogd

D. ofrpd

Correct Answer: B

Disk quota enforcement is performed by different processes:

The logfiled process enforces the log file size and is also responsible for disk quota enforcement by monitoring the other processes.

FortiAnalyzer_7.0_Study_Guide-Online pag. 121

QUESTION 6

You have recently grouped multiple FortiGate devices into a single ADOM. System Settings > Storage Info shows the quota used. What does the disk quota refer to?

A. The maximum disk utilization for each device in the ADOM

B. The maximum disk utilization for the FortiAnalyzer model

C. The maximum disk utilization for the ADOM type

D. The maximum disk utilization for all devices in the ADOM

Correct Answer: D

page 66 FortiAnalyzer_6.4_Study_Guide

QUESTION 7

FortiAnalyzer centralizes which functions? (Choose three)

A. Network analysis

B. Graphical reporting

C. Content archiving / data mining

D. Vulnerability assessment

E. Security log analysis / forensics

Correct Answer: BCE

QUESTION 8

What must you configure on FortiAnalyzer to upload a FortiAnalyzer report to a supported external server? (Choose two.)

A. SFTP, FTP, or SCP server

B. Mail server

C. Output profile

D. Report scheduling

Correct Answer: BC

From study guide

In order to use any of these external storage mothods, you must set up the back end. This includes configuring a mail service and an output profile.

QUESTION 9

Which two statements express the advantages of grouping similar reports? (Choose two.)

A. Improve report completion time.

B. Conserve disk space on FortiAnalyzer by grouping multiple similar reports.

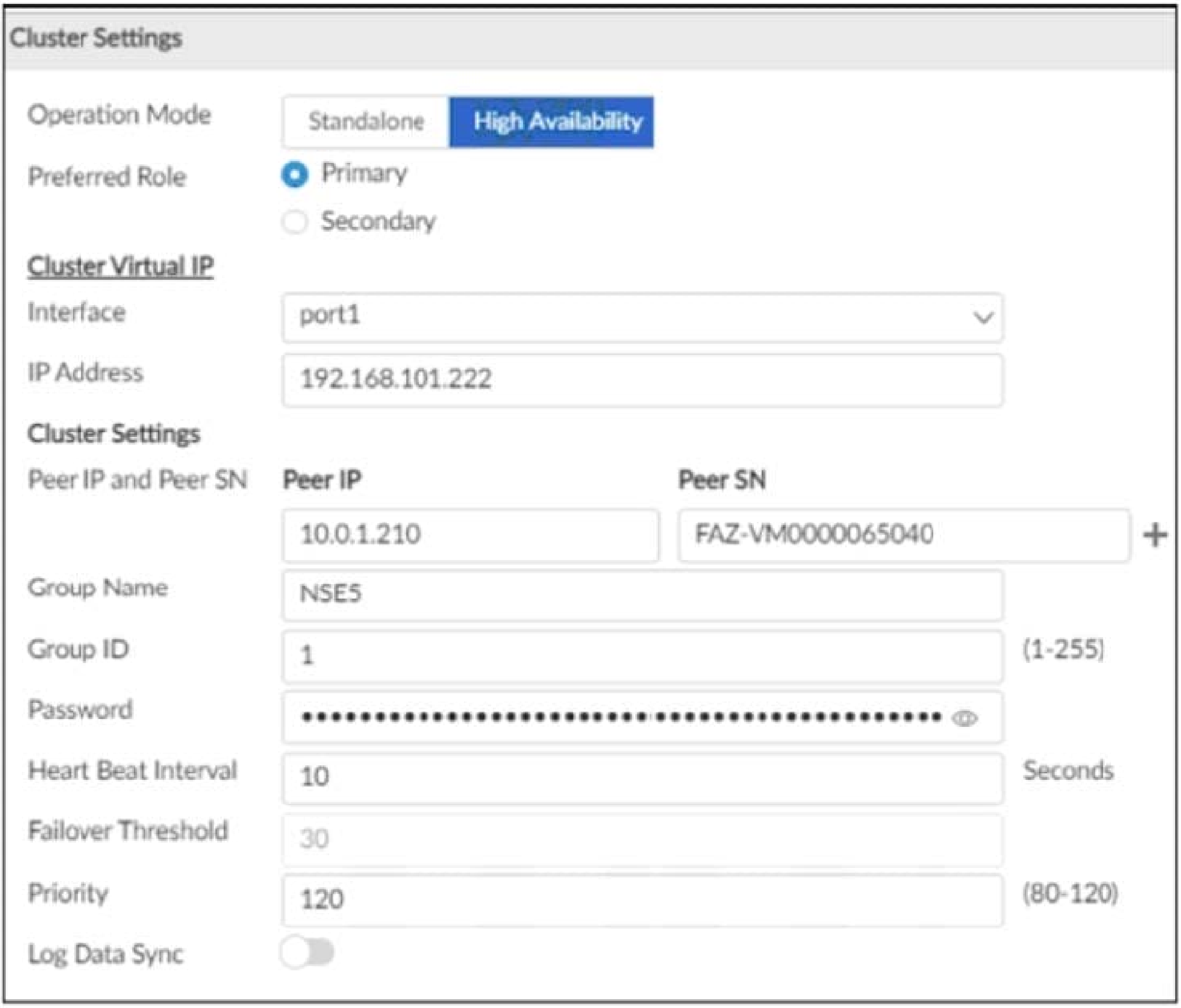
C. Reduce the number of hcache tables and improve auto-hcache completion time.

D. Provides a better summary of reports.

Correct Answer: AC

QUESTION 10

Refer to the exhibit.



Cluster Settings

Operation Mode	Standalone / **High Availability**
Preferred Role	● Primary ○ Secondary

Cluster Virtual IP

Interface	port1
IP Address	192.168.101.222

Cluster Settings

Peer IP and Peer SN	Peer IP	Peer SN	
	10.0.1.210	FAZ-VM0000065040	+
Group Name	NSE5		
Group ID	1	(1-255)	
Password	••		
Heart Beat Interval	10	Seconds	
Failover Threshold	30		
Priority	120	(80-120)	
Log Data Sync	○		

The image displays the configuration of a FortiAnalyzer the administrator wants to join to an existing HA cluster. What can you conclude from the configuration displayed?

A. This FortiAnalyzer will join to the existing HA cluster as the primary.

B. This FortiAnalyzer is configured to receive logs in its port1.

C. This FortiAnalyzer will trigger a failover after losing communication with its peers for 10 seconds.

D. After joining to the cluster, this FortiAnalyzer will keep an updated log database.

Correct Answer: B

If the preferred role is Primary, then this unit becomes the primary unit if it is configured first in a new HA cluster. If there is an existing primary unit, then this unit becomes a secondary unit.

QUESTION 11

What can the CLI command # diagnose test application oftpd 3 help you to determine?

A. What devices and IP addresses are connecting to FortiAnalyzer

B. What logs, if any, are reaching FortiAnalyzer

C. What ADOMs are enabled and configured

D. What devices are registered and unregistered

Correct Answer: A

Device and ADOM Status Check

diagnose test application oftpd 3 # Devices and IPs are connecting to FortiAnalyzer diagnose test application oftpd 8 # Receiving logs in FortiAnalyzre diagnose dvm adom list # ADOMs are enabled and configured diagnose dvm device list # Devices or VDOMs are currently registed and unregistered

https://docs.fortinet.com/document/fortianalyzer/6.2.5/cli- reference/395556/test#test_application

QUESTION 12

Which two statements are true regarding FortiAnalyzer operating modes? (Choose two.)

A. By deploying different FortiAnalyzer devices in both modes, you can improve their overall performance.

B. When in collector mode. FortiAnalyzer collects logs from multiple devices and forwards these logs in the original binary format.

C. When in collector mode. FortiAnalyzer supports event management and reporting features.

D. By deploying different FortiAnalyzer devices with collector and analyzer mode in a network, you can improve the overall performance of log receiving, analysis, and reporting

E. Collector mode is the default operating mode.

Correct Answer: AB

FortiAnalyzer_7.0_Study_Guide-Online pag. 10

QUESTION 13

The admin administrator is failing to register a FortiClient EMS on the FortiAnalyzer device. What can be the reason for this failure?

A. FortiAnalyzer is in an HA cluster.

B. ADOM mode should be set to advanced, in order to register the FortiClient EMS device.

C. ADOMs are not enabled on FortiAnalyzer.

D. A separate license is required on FortiAnalyzer in order to register the FortiClient EMS device.

Correct Answer: C

Reference: https://help.fortinet.com/fa/faz50hlp/56/5-6-2/FMG-FAZ/0800_ADOMs/0015_FortiClient%20and%20ADOMs.htm

QUESTION 14

You are using RAID with a FortiAnalyzer that supports software RAID, and one of the hard disks on FortiAnalyzer has failed. What is the recommended method to replace the disk?

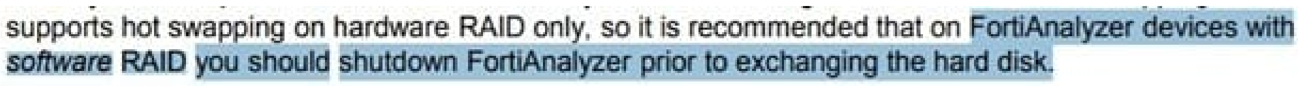
A. Shut down FortiAnalyzer and then replace the disk

B. Downgrade your RAID level, replace the disk, and then upgrade your RAID level

C. Clear all RAID alarms and replace the disk while FortiAnalyzer is still running

D. Perform a hot swap

Correct Answer: A



supports hot swapping on hardware RAID only, so it is recommended that on FortiAnalyzer devices with *software* RAID you should shutdown FortiAnalyzer prior to exchanging the hard disk.

https://community.fortinet.com/t5/FortiAnalyzer/Technical-Note-How-to-swap-Hard-Disk-on- FortiAnalyzer/ta-p/194997?externalID=FD41397#:~:text=If%20a%20hard%20disk%20on,process%20known%20as%20hot%20swapping

QUESTION 15

Which log type does the FortiAnalyzer indicators of compromise feature use to identify infected hosts?

A. Antivirus logs

B. Web filter logs

C. IPS logs

D. Application control logs

Correct Answer: B

Reference: https://help.fortinet.com/fa/faz50hlp/60/6-0-2/Content/FortiAnalyzer_Admin_Guide/3600_FortiView/0200_Using_FortiView/1200_Compromised_ hosts_page.htm?TocPath=FortiView%7CUsing%20FortiView%7C_____6