NSE5_FAZ-6.4 Q&As

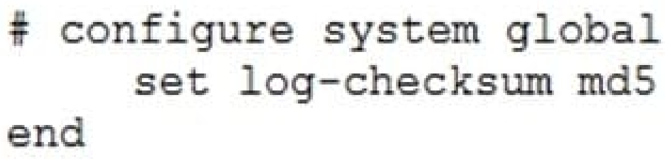
Fortinet NSE 5 - FortiAnalyzer 6.4

Pass Fortinet NSE5_FAZ-6.4 Exam with 100% Guarantee

Following Questions and Answers are all new published by Fortinet Official Exam Center

QUESTION 1

What is the purpose of the following CLI command?



```
# configure system global
      set log-checksum md5
end
```

A. To add a log file checksum

B. To add the MD\\'s hash value and authentication code

C. To add a unique tag to each log to prove that it came from this FortiAnalyzer

D. To encrypt log communications

Correct Answer: A

https://docs2.fortinet.com/document/fortianalyzer/6.0.3/cli-reference/849211/global

QUESTION 2

Which tabs do not appear when FortiAnalyzer is operating in Collector mode?

A. FortiView

B. Event Management

C. Device Manger

D. Reporting

Correct Answer: B

QUESTION 3

Which FortiAnalyzer feature allows you to retrieve the archived logs matching a specific timeframe from another FortiAnalyzer device?

A. Log upload

B. Indicators of Compromise

C. Log forwarding an aggregation mode

D. Log fetching

Correct Answer: D

https://docs.fortinet.com/document/fortianalyzer/6.2.0/administration-guide/651442/fetcher-management

QUESTION 4

If you upgrade the FortiAnalyzer firmware, which report element can be affected?

A. Custom datasets

B. Report scheduling

C. Report settings

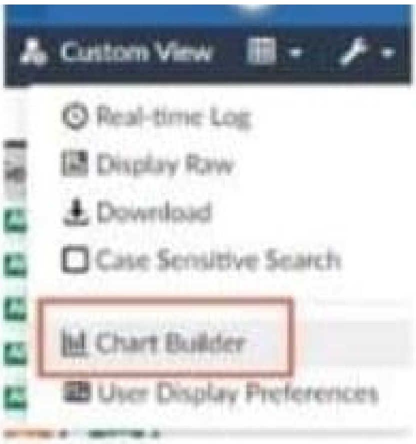
D. Output profiles

Correct Answer: A

https://docs.fortinet.com/document/fortianalyzer/6.2.5/upgrade-guide/669300/checking-reports

QUESTION 5

Refer to the exhibit.



What is the purpose of using the Chart Builder feature on FortiAnalyzer?

A. In Log View, this feature allows you to build a dataset and chart automatically, based on the filtered search results.

B. In Log View, this feature allows you to build a chart and chart automatically, on the top 100 log entries.

C. This feature allows you to build a chart under FortiView.

D. You can add charts to generated reports using this feature.

Correct Answer: A

QUESTION 6

For which two purposes would you use the command set log checksum? (Choose two.)

A. To help protect against man-in-the-middle attacks during log upload from FortiAnalyzer to an SFTP server

B. To prevent log modification or tampering

C. To encrypt log communications

D. To send an identical set of logs to a second logging server

Correct Answer: AB

QUESTION 7

How are logs forwarded when FortiAnalyzer is using aggregation mode?

A. Logs are forwarded as they are received and content files are uploaded at a scheduled time.

B. Logs and content files are stored and uploaded at a scheduled time.

C. Logs are forwarded as they are received.

D. Logs and content files are forwarded as they are received.

Correct Answer: B

https://www.fortinetguru.com/2020/07/log-forwarding-fortianalyzer-fortios-6-2-3/
https://docs.fortinet.com/document/fortianalyzer/6.2.0/administration-guide/420493/modes https://docs.fortinet.com/document/fortianalyzer/6.2.0/cookbook/63238/what-is-the-difference-between-logforward-and-log-aggregation-modes

QUESTION 8

An administrator has configured the following settings:

config system global set log-checksum md5-auth end

What is the significance of executing this command?

A. This command records the log file MD5 hash value.

B. This command records passwords in log files and encrypts them.

C. This command encrypts log transfer between FortiAnalyzer and other devices.

D. This command records the log file MD5 hash value and authentication code.

Correct Answer: D

Reference: https://docs.fortinet.com/document/fortianalyzer/6.4.6/administration-guide/410387/appendix-blog-integrity-and-secure-log-transfer

QUESTION 9

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

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

QUESTION 10

Which statement is true regarding Macros on FortiAnalyzer?

A. Macros are ADOM specific and each ADOM will have unique macros relevant to that ADOM.

B. Macros are supported only on the FortiGate ADOM.

C. Macros are useful in generating excel log files automatically based on the reports settings.

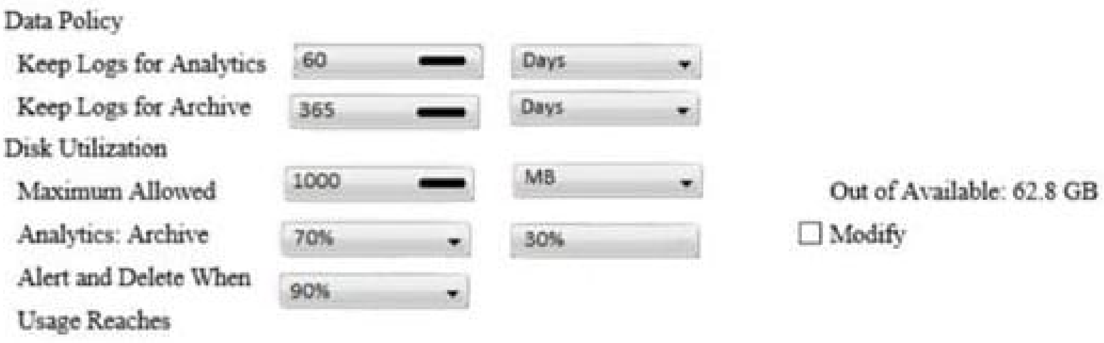
D. Macros are predefined templates for reports and cannot be customized.

Correct Answer: A

Reference: https://docs2.fortinet.com/document/fortianalyzer/6.2.3/administration-guide/617380/creatingmacros

QUESTION 11

View the exhibit:



Data Policy

Keep Logs for Analytics 60 Days

Keep Logs for Archive 365 Days

Disk Utilization

Maximum Allowed 1000 MB Out of Available: 62.8 GB

Analytics: Archive 70% 30% □ Modify

Alert and Delete When Usage Reaches 90%

What does the 1000MB maximum for disk utilization refer to?

A. The disk quota for the FortiAnalyzer model

B. The disk quota for all devices in the ADOM

C. The disk quota for each device in the ADOM

D. The disk quota for the ADOM type

Correct Answer: B

https://docs.fortinet.com/document/fortianalyzer/6.2.0/administration- guide/743670/configuring-logstorage-policy

QUESTION 12

What purposes does the auto-cache setting on reports serve? (Choose two.)

A. To reduce report generation time

B. To automatically update the hcache when new logs arrive

C. To reduce the log insert lag rate

D. To provide diagnostics on report generation time

Correct Answer: AB

Reference: https://docs.fortinet.com/document/fortianalyzer/6.0.0/administration-guide/282280/enablingautocache

QUESTION 13

What are two advantages of setting up fabric ADOM? (Choose two.)

A. It can be used for fast data processing and log correlation

B. It can be used to facilitate communication between devices in same Security Fabric

C. It can include all Fortinet devices that are part of the same Security Fabric

D. It can include only FortiGate devices that are part of the same Security Fabric

Correct Answer: AC

https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/448471/creating-a-securityfabric-adom

QUESTION 14

Which clause is considered mandatory in SELECT statements used by the FortiAnalyzer to generate reports?

A. FROM

B. LIMIT

C. WHERE

D. ORDER BY

Correct Answer: A

https://kb.fortinet.com/kb/documentLink.do?externalID=FD48500

QUESTION 15

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?

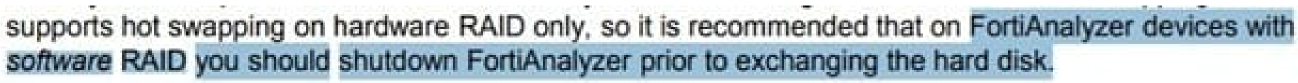
A. Shut down FortiAnalyzer and then replace the disk

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%20know n%20as%20hot%20swapping

[Latest NSE5_FAZ-6.4 Dumps](#) [NSE5_FAZ-6.4 VCE Dumps](#) [NSE5_FAZ-6.4 Exam Questions](#)