NSE5_FAZ-6.2^{Q&As}

Fortinet NSE 5 - FortiAnalyzer 6.2

Pass Fortinet NSE5_FAZ-6.2 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/nse5_faz-6-2.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Which two constraints can impact the amount of reserved disk space required by FortiAnalyzer? (Choose two.)

A. License type

B. Disk size

C. Total quota

D. RAID level

Correct Answer: BD

Reference: https://docs.fortinet.com/document/fortianalyzer/6.0.5/administration-guide/929977/diskspaceallocation

QUESTION 2

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: B

QUESTION 3

What is the purpose of employing RAID with FortiAnalyzer?

A. To introduce redundancy to your log data

B. To provide data separation between ADOMs

C. To separate analytical and archive data

D. To back up your logs

Correct Answer: A

QUESTION 4

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 5

Logs are being deleted from one of the ADOMs earlier than the configured setting for archiving in the data policy.

What is the most likely problem?

A. CPU resources are too high

B. Logs in that ADOM are being forwarded, in real-time, to another FortiAnalyzer device

C. The total disk space is insufficient and you need to add other disk

D. The ADOM disk quota is set too low, based on log rates

Correct Answer: D

Reference: https://help.fortinet.com/fmgr/50hlp/56/5-6-1/FMG-FAZ/1100_Storage/0017_Deleted%20device
%20logs.htm

QUESTION 6

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 7

FortiAnalyzer reports are dropping analytical data from 15 days ago, even though the data policy setting for

analytics logs is 60 days.

What is the most likely problem?

A. Quota enforcement is acting on analytical data before a report is complete

B. Logs are rolling before the report is run

C. CPU resources are too high

D. Disk utilization for archive logs is set for 15 days

Correct Answer: A

Reference: https://forum.fortinet.com/tm.aspx?m=138806

QUESTION 8

In FortiAnalyzer\\'s FormView, source and destination IP addresses from FortiGate devices are not resolving to a hostname. How can you resolve the source and destination IPs, without introducing any additional performance impact to FortiAnalyzer?

A. Configure local DNS servers on FortiAnalyzer

B. Resolve IPs on FortiGate

C. Configure # set resolve-ip enable in the system FortiView settings

D. Resolve IPs on a per-ADOM basis to reduce delay on FortiView while IPs resolve

Correct Answer: B

QUESTION 9

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

To prevent the log in the store from being modified, you can add a log checksum by using the config system global command. When the log is split, archived, and the log is uploaded (if the feature is enabled), you can configure the FortiAnalyzer to log the log file hash value, timestamp, and authentication code. This can help defend against man-in-

the-middle attacks when uploading log transmission data from the FortiAnalyzer to the SFTP server.

QUESTION 10

You\'ve moved a registered logging device out of one ADOM and into a new ADOM. What happens when you rebuild the new ADOM database?

A. FortiAnalyzer resets the disk quota of the new ADOM to default.

B. FortiAnalyzer migrates archive logs to the new ADOM.

C. FortiAnalyzer migrates analytics logs to the new ADOM.

D. FortiAnalyzer removes logs from the old ADOM.

Correct Answer: C

QUESTION 11

In the FortiAnalyzer FortiView, source and destination IP addresses from FortiGate devices are not resolving to a hostname.

How can you resolve the source and destination IP addresses, without introducing any additional performance impact to FortiAnalyzer?

A. Resolve IP addresses on a per-ADOM basis to reduce delay on FortiView while IPs resolve

B. Configure # set resolve-ip enable in the system FortiView settings

C. Configure local DNS servers on FortiAnalyzer

D. Resolve IP addresses on FortiGate

Correct Answer: B

Reference: https://forum.fortinet.com/tm.aspx?m=156950

QUESTION 12

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

QUESTION 13

For which two SAML roles can the FortiAnalyzer be configured? (Choose two.)

A. Principal

B. Service provider

C. Identity collector

D. Identity provider

Correct Answer: BD

Reference: https://docs.fortinet.com/document/fortianalyzer/6.2.0/new-features/957811/samladminauthentication#:~:text=for%20the%20administrator.-,FortiAnalyzer%20can%20play%20the%20role%20of%20the%20identity%20provider%20(IdP,external%20identity%20provider%20is%20available

QUESTION 14

By default, what happens when a log file reaches its maximum file size?

A. FortiAnalyzer overwrites the log files.

B. FortiAnalyzer stops logging.

C. FortiAnalyzer rolls the active log by renaming the file.

D. FortiAnalyzer forwards logs to syslog.

Correct Answer: C

QUESTION 15

What is the purpose of a predefined template on the FortiAnalyzer?

A. It can be edited and modified as required

B. It specifies the report layout which contains predefined texts, charts, and macros

C. It specifies report settings which contains time period, device selection, and schedule

D. It contains predefined data to generate mock reports

Correct Answer: B

Reference: https://help.fortinet.com/fa/faz50hlp/56/5-6-2/FMGFAZ/2300_Reports/0010_Predefined_reports.htm#:~:text=FortiAnalyzer%20includes%20a%

20number%20of,create%20and%2For%20build%20reports.andtext=A%20template%20populates%20the %20Layout,that%20is%20to%20be%20created.