NSE5_FAZ-6.4 Q&As

Fortinet NSE 5 - FortiAnalyzer 6.4

Pass Fortinet NSE5_FAZ-6.4 Exam with 100% Guarantee

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

https://www.pass2lead.com/nse5_faz-6-4.html

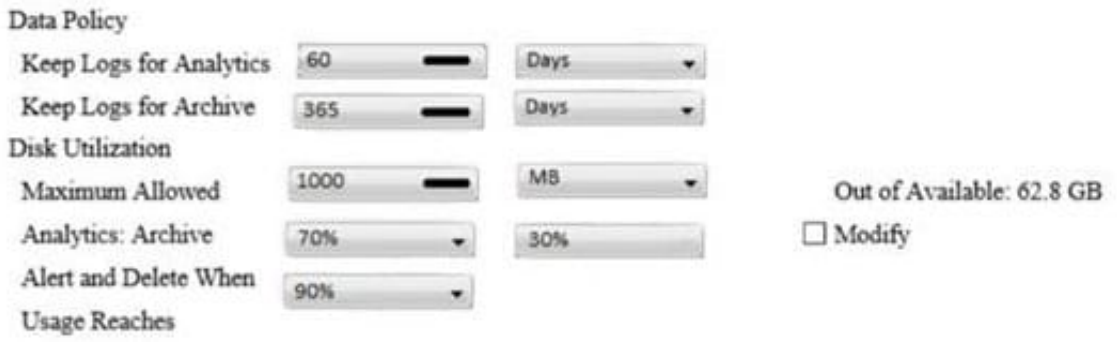
100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

View the exhibit:



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 2

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 3

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 4

What is the recommended method of expanding disk space on a FortiAnalyzer VM?

A. From the VM host manager, add an additional virtual disk and use the #execute lvm extend command to expand the storage

B. From the VM host manager, expand the size of the existing virtual disk

C. From the VM host manager, expand the size of the existing virtual disk and use the # execute format disk command to reformat the disk

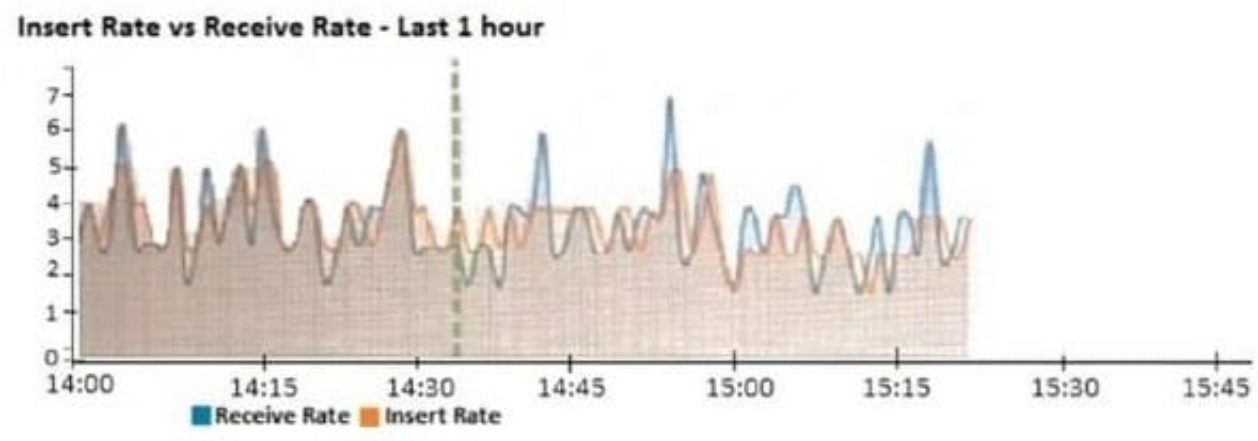
D. From the VM host manager, add an additional virtual disk and rebuild your RAID array

Correct Answer: A

https://kb.fortinet.com/kb/documentLink.do?externalID=FD40848

QUESTION 5

View the exhibit.



What does the data point at 14:35 tell you?

A. FortiAnalyzer is dropping logs.

B. FortiAnalyzer is indexing logs faster than logs are being received.

C. FortiAnalyzer has temporarily stopped receiving logs so older logs\\' can be indexed.

D. The sqlplugind daemon is ahead in indexing by one log.

Correct Answer: B

https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/47690/insert-rate-vs-receiverate-widget

QUESTION 6

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 7

What is the main purpose of using an NTP server on FortiAnalyzer and all of its registered devices?

A. Log correlation

B. Host name resolution

C. Log collection

D. Real-time forwarding

Correct Answer: A

QUESTION 8

What happens when a log file saved on FortiAnalyzer disks reaches the size specified in the device log settings?

A. The log file is stored as a raw log and is available for analytic support.

B. The log file rolls over and is archived.

C. The log file is purged from the database.

D. The log file is overwritten.

Correct Answer: B

Reference: https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/6d9f8fb5-6cf4-11e9-81a400505692583a/FortiAnalyzer-6.0.5-Administration-Guide.pdf https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/355632/log-browse

QUESTION 9

What is the purpose of a dataset query in FortiAnalyzer?

A. It sorts log data into tables

B. It extracts the database schema

C. It retrieves log data from the database

D. It injects log data into the database

Correct Answer: C

Reference: https://docs2.fortinet.com/document/fortianalyzer/6.0.4/administration-guide/148744/creatingdatasets

QUESTION 10

What are two of the key features of FortiAnalyzer? (Choose two.)

A. Centralized log repository

B. Cloud-based management

C. Reports

D. Virtual domains (VDOMs)

Correct Answer: AC

QUESTION 11

What FortiView tool can you use to automatically build a dataset and chart based on a filtered search result?

A. Chart Builder

B. Export to Report Chart

C. Dataset Library

D. Custom View

Correct Answer: A

https://docs.fortinet.com/document/fortianalyzer/6.2.0/cookbook/989203/building-charts-with-chart-builder

QUESTION 12

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

https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/368682/disk-space-allocation

QUESTION 13

An administrator has moved FortiGate A from the root ADOM to ADOM1. Which two statements are true regarding logs? (Choose two.)

A. Analytics logs will be moved to ADOM1 from the root ADOM automatically.

B. Archived logs will be moved to ADOM1 from the root ADOM automatically.

C. Logs will be presented in both ADOMs immediately after the move.

D. Analytics logs will be moved to ADOM1 from the root ADOM after you rebuild the ADOM1 SQL database.

Correct Answer: BD

Reference: https://community.fortinet.com/t5/Fortinet-Forum/FW-Migration-between-ADOMs/m-p/32683? m=158008

QUESTION 14

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

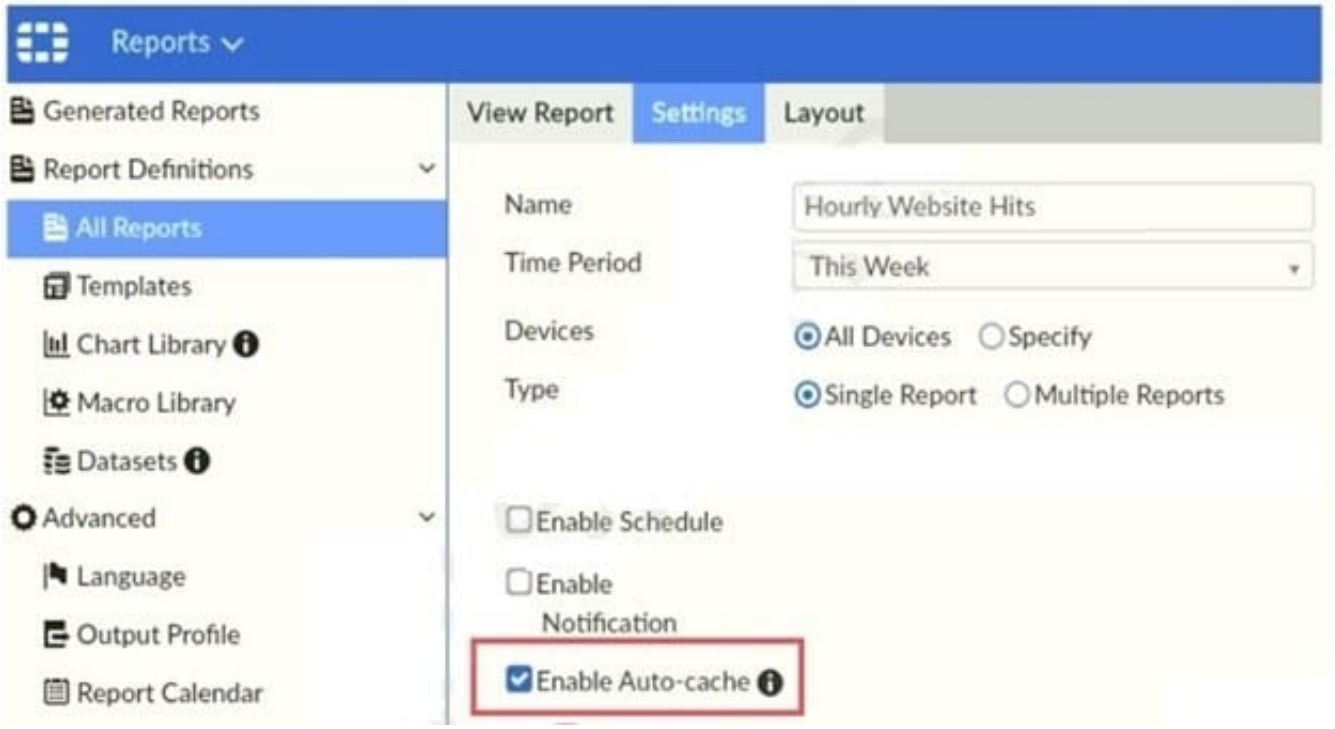
C. The maximum disk utilization for the ADOM type

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

Correct Answer: D

QUESTION 15

Refer to the exhibit.



Which two statements are true regarding enabling auto-cache on FortiAnalyzer? (Choose two.)

A. Report size will be optimized to conserve disk space on FortiAnalyzer.

B. Reports will be cached in the memory.

C. This feature is automatically enabled for scheduled reports.

D. Enabling auto-cache reduces report generation time for reports that require a long time to assemble datasets.

Correct Answer: CD

Reference: https://help.fortinet.com/fa/faz50hlp/56/5-6-2/FMG-FAZ/2300_Reports/0025_Auto-cache.htm