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.pass4itsure.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

After you have moved a registered logging device out of one ADOM and into a new ADOM, what is the purpose of running the following CLI command?

execute sql-local rebuild-adom

A. To reset the disk quota enforcement to default

B. To remove the analytics logs of the device from the old database

C. To migrate the archive logs to the new ADOM

D. To populate the new ADOM with analytical logs for the moved device, so you can run reports

Correct Answer: D

QUESTION 2

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 3

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 4

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 5

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 6

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 7

FortiAnalyzer uses the Optimized Fabric Transfer Protocok (OFTP) over SSL for what purpose?

A. To upload logs to an SFTP server

B. To prevent log modification during backup

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

D. To encrypt log communication between devices

Correct Answer: D

QUESTION 8

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.

https://help.fortinet.com/fa/faz50hlp/56/5-6-2/FMG- FAZ/2300_Reports/0010_Predefined_reports.htm

https://docs2.fortinet.com/document/fortianalyzer/6.0.8/administration- guide/618245/predefined-reportstemplates-charts-and-macros

QUESTION 9

Which statements are true regarding securing communications between FortiAnalyzer and FortiGate with SSL? (Choose two.)

A. SSL is the default setting.

B. SSL communications are auto-negotiated between the two devices.

C. SSL can send logs in real-time only.

D. SSL encryption levels are globally set on FortiAnalyzer.

E. FortiAnalyzer encryption level must be equal to, or higher than, FortiGate.

Correct Answer: AD

QUESTION 10

Which two statements about log forwarding are true? (Choose two.)

A. Forwarded logs cannot be filtered to match specific criteria.

B. Logs are forwarded in real-time only.

C. The client retains a local copy of the logs after forwarding.

D. You can use aggregation mode only with another FortiAnalyzer.

Correct Answer: CD

https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/420493/modes
https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/621804/log-forwarding

QUESTION 11

If a hard disk fails on a FortiAnalyzer that supports software RAID, what should you do to bring the

FortiAnalyzer back to functioning normally, without losing data?

A. Hot swap the disk

B. Replace the disk and rebuild the RAID manually

C. Take no action if the RAID level supports a failed disk

D. Shut down FortiAnalyzer and replace the disk

Correct Answer: D

https://kb.fortinet.com/kb/documentLink.do?externalID=FD46446#:~:text=On%20FortiAnalyzer%2FFortiManager%20devices%20that,to%20exchanging%20the%20hard%20disk.

If a hard disk on a FortiAnalyzer unit fails, it must be replaced. On FortiAnalyzer devices that support hardware RAID, the hard disk can be replaced while the unit is still running ?known as hot swapping. On FortiAnalyzer units with software RAID, the device must be shutdown prior to exchanging the hard disk.

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

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

What are offline logs on FortiAnalyzer?

A. Compressed logs, which are also known as archive logs, are considered to be offline logs.

B. When you restart FortiAnalyzer. all stored logs are considered to be offline logs.

C. Logs that are indexed and stored in the SQL database.

D. Logs that are collected from offline devices after they boot up.

Correct Answer: A

Reference: https://help.fortinet.com/fa/faz50hlp/56/5-6-6/Content/
FortiAnalyzer_Admin_Guide/0300_Key_concepts/0600_Log_Storage/0400_Arch ive_analytics_logs.htm

QUESTION 14

On FortiAnalyzer, what is a wildcard administrator account?

A. An account that permits access to members of an LDAP group

B. An account that allows guest access with read-only privileges

C. An account that requires two-factor authentication

D. An account that validates against any user account on a FortiAuthenticator

Correct Answer: A

https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/747268/configuring-wildcard-admin-accounts

QUESTION 15

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