

Fortinet

Exam Questions NSE5_FAZ-7.0

Fortinet NSE 5 - FortiAnalyzer 7.0



NEW QUESTION 1

What is the best approach to handle a hard disk failure on a FortiAnalyzer that supports hardware RAID?

- A. Hot swap the disk.
- B. There is no need to do anything because the disk will self-recover.
- C. Run execute format disk to format and restart the FortiAnalyzer device.
- D. Shut down FortiAnalyzer and replace the disk

Answer: D

Explanation:

<https://kb.fortinet.com/kb/documentLink.do?externalID=FD46446#:~:text=On%20FortiAnalyzer%2FFortiMana> 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.

NEW QUESTION 2

Consider the CLI command:

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

What is the purpose of the command?

- A. To add a unique tag to each log to prove that it came from this FortiAnalyzer
- B. To add the MD5 hash value and authentication code
- C. To add a log file checksum
- D. To encrypt log communications

Answer: C

Explanation:

<https://docs.fortinet.com/document/fortianalyzer/6.2.5/cli-reference/849211/global>

NEW QUESTION 3

Which two of the following must you configure on FortiAnalyzer to email a FortiAnalyzer report externally? (Choose two.)

- A. Mail server
- B. Output profile
- C. SFTP server
- D. Report scheduling

Answer: AB

NEW QUESTION 4

What does the disk status Degraded mean for RAID management?

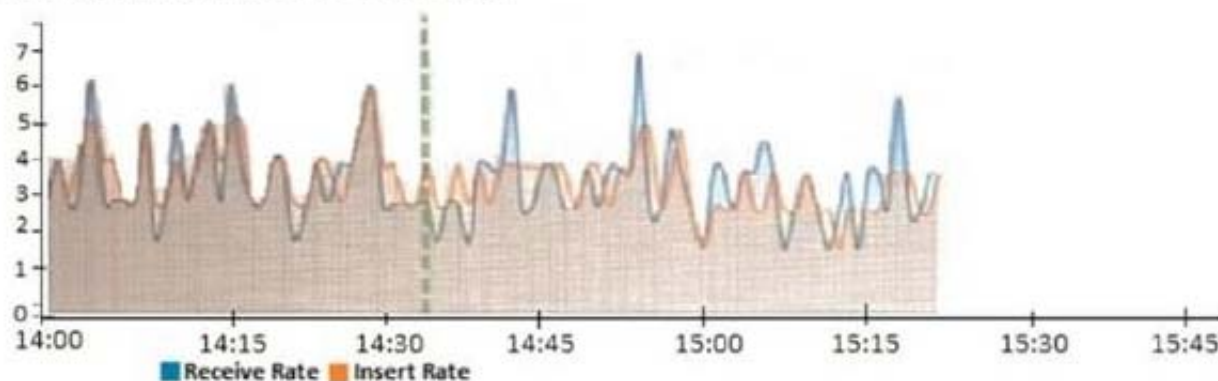
- A. One or more drives are missing from the FortiAnalyzer uni
- B. The drive is no longer available to the operating system.
- C. The FortiAnalyzer device is writing to all the hard drives on the device in order to make the array fault tolerant.
- D. The FortiAnalyzer device is writing data to a newly added hard drive in order to restore the hard drive to an optimal state.
- E. The hard drive is no longer being used by the RAID controller

Answer: D

NEW QUESTION 5

View the exhibit.

Insert Rate vs Receive Rate - Last 1 hour



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.

Answer: B

Explanation:

<https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/47690/insert-rate-vs-receive-rate-wi>

NEW QUESTION 6

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)

Answer: AC

NEW QUESTION 7

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

- A. When in collector mode, FortiAnalyzer collects logs from multiple devices and forwards these logs in the original binary format.
- B. Collector mode is the default operating mode.
- C. When in collector mod
- D. FortiAnalyzer supports event management and reporting features.
- E. 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

Answer: AD

NEW QUESTION 8

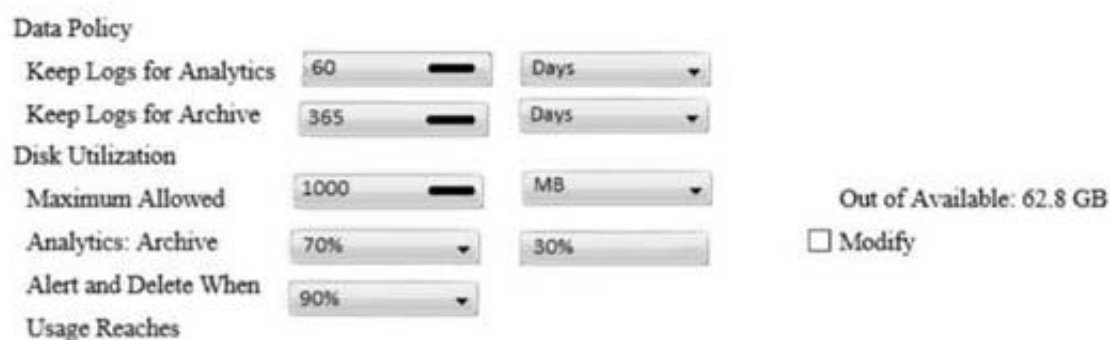
Which SQL query is in the correct order to query the database in the FortiAnslyzer?

- A. SELECT devid FROM Slog GROOP BY devid WHERE * user' =* USERI'
- B. SELECT devid WHERE 'u3er'='USERI' FROM \$ log GROUP BY devid
- C. SELECT devid FROM Slog- WHERE *user' = ' USERI' GROUP BY devid
- D. FROM Slog WHERE 'user* =' USERI' SELECT devid GROUP BY devid

Answer: C

NEW QUESTION 9

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

Answer: B

Explanation:

<https://docs.fortinet.com/document/fortianalyzer/6.2.0/administration-guide/743670/configuring-log-storage-pol>

NEW QUESTION 10

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 <new-ADOM-name>

- 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

Answer: D

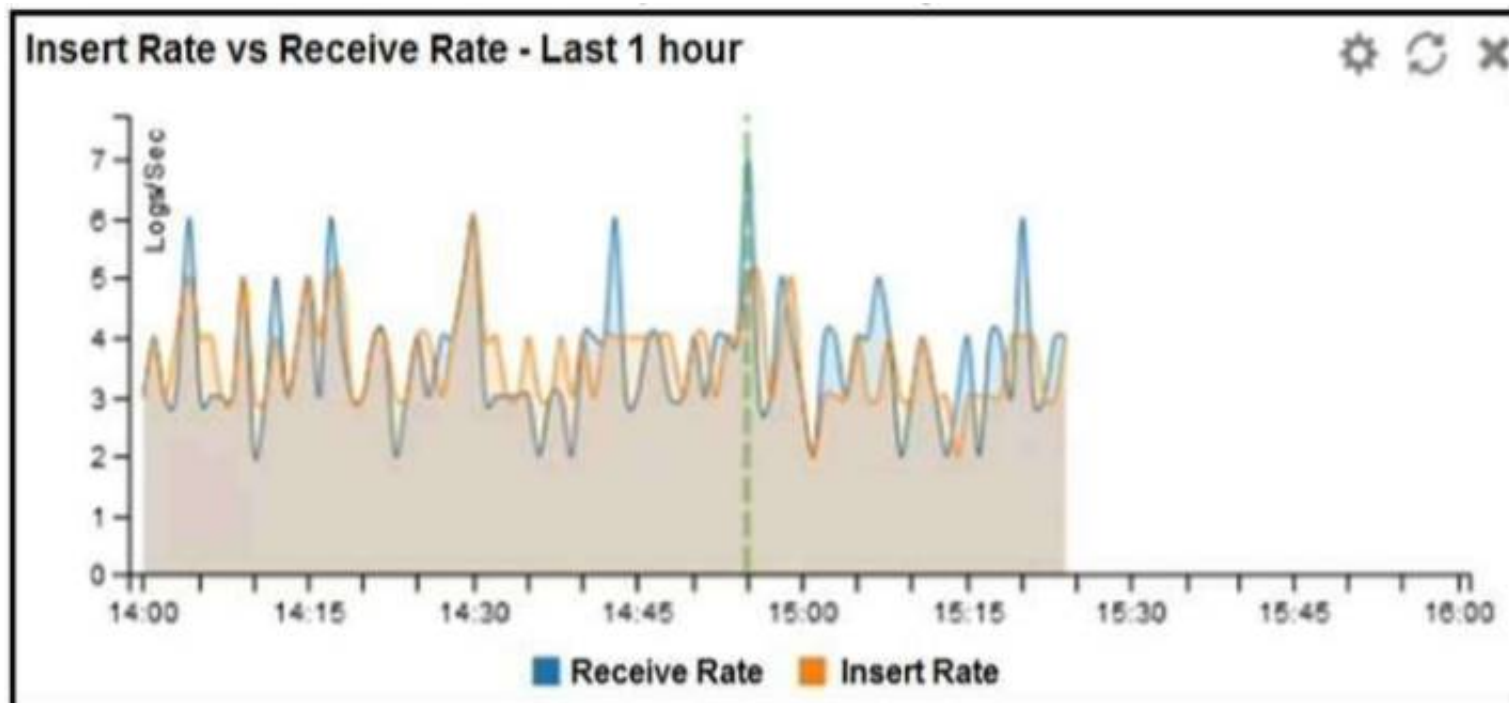
Explanation:

- Are the device's analytics logs required for reports in the *new* ADOM? If so, rebuild the new ADOM database:

```
# exe sql-local rebuild-adom <new-ADOM-name>
```

NEW QUESTION 10

Refer to the exhibit.



What does the data point at 14:55 tell you?

- A. The received rate is almost at its maximum for this device
- B. The sqlplugind daemon is behind in log indexing by two logs
- C. Logs are being dropped
- D. Raw logs are reaching FortiAnalyzer faster than they can be indexed

Answer: D

NEW 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

Answer: AB

NEW QUESTION 14

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.

Answer: BCD

NEW QUESTION 17

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

Answer: D

Explanation:

<https://packetplant.com/fortigate-and-fortianalyzer-resolve-source-and-destination-ip/>

"As a best practice, it is recommended to resolve IPs on the FortiGate end. This is because you get both source and destination, and it offloads the work from FortiAnalyzer. On FortiAnalyzer, this IP resolution does destination IPs only"

NEW QUESTION 19

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

Answer: A

Explanation:

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

NEW QUESTION 21

How do you restrict an administrator's access to a subset of your organization's ADOMs?

- A. Set the ADOM mode to Advanced
- B. Assign the ADOMs to the administrator's account
- C. Configure trusted hosts
- D. Assign the default Super_User administrator profile

Answer: B

Explanation:

<https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/717578/assigning-administrators-to>

NEW QUESTION 25

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

Answer: A

Explanation:

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

NEW QUESTION 26

When you perform a system backup, what does the backup configuration contain? (Choose two.)

- A. Generated reports
- B. Device list
- C. Authorized devices logs
- D. System information

Answer: BD

Explanation:

https://help.fortinet.com/fa/cli-olh/5-6-5/Content/Document/1400_execute/backup.htm

NEW QUESTION 29

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

Answer: D

NEW QUESTION 30

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

Answer: AC

Explanation:

<https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/448471/creating-a-security-fabric-a>

NEW QUESTION 32

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.

Answer: AD

NEW QUESTION 34

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

Answer: BC

Explanation:

<https://docs.fortinet.com/document/fortianalyzer/6.0.2/administration-guide/598322/creating-output-profiles>

NEW QUESTION 36

Which two statement are true regardless initial Logs sync and Log Data Sync for Ha on FortiAnalyzer?

- A. By default, Log Data Sync is disabled on all backup device.
- B. Log Data Sync provides real-time log synchronization to all backup devices.
- C. With initial Logs Sync, when you add a unit to an HA cluster, the primary device synchronizes its logs with the backup device.
- D. When Logs Data Sync is turned on, the backup device will reboot and then rebuilt the log database with the synchronized logs.

Answer: CD

NEW QUESTION 40

Refer to the exhibit.

The screenshot shows the 'New Administrator' configuration page in FortiAnalyzer. The 'User Name' is 'remoteadmin'. The 'Admin Type' is 'GROUP'. The 'GROUP' dropdown is set to 'remoteservergroup'. The 'Match all users on remote server' checkbox is checked and highlighted with a red box. The 'Admin Profile' is 'Super_User'. The 'Administrative Domain' is set to 'All ADOMs'. The 'JSON API Access' is 'None'. The 'Trusted Hosts' are set to 'OFF'.

The exhibit shows “remoteservergroup” is an authentication server group with LDAP and RADIUS servers. Which two statements express the significance of enabling “Match all users on remote server” when configuring a new administrator? (Choose two.)

- A. It creates a wildcard administrator using LDAP and RADIUS servers.
- B. Administrator can log in to FortiAnalyzer using their credentials on remote servers LDAP and RADIUS.
- C. Use remoteadmin from LDAP and RADIUS servers will be able to log in to FortiAnalyzer at anytime.
- D. It allows administrators to use two-factor authentication.

Answer: AB

NEW QUESTION 42

An administrator fortinet, is able to view logs and perform device management tasks, such as adding and removing registered devices. However, administrator fortinet is not able to create a mail server that can be used to send email. What could be the problem?

- A. Fortinet is assigned the Standard_ User administrator profile.
- B. A trusted host is configured.
- C. ADOM mode is configured with Advanced mode.
- D. Fortinet is assigned the Restricted_ User administrator profile.

Answer: A

NEW QUESTION 47

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

NSE5_FAZ-7.0 Practice Exam Features:

- * NSE5_FAZ-7.0 Questions and Answers Updated Frequently
- * NSE5_FAZ-7.0 Practice Questions Verified by Expert Senior Certified Staff
- * NSE5_FAZ-7.0 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * NSE5_FAZ-7.0 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The NSE5_FAZ-7.0 Practice Test Here](#)