



# Fortinet

## Exam Questions NSE5\_FAZ-7.2

Fortinet NSE 5 - FortiAnalyzer 7.2

## About ExamBible

*[Your Partner of IT Exam](#)*

## Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

## Our Advances

### \* 99.9% Uptime

All examinations will be up to date.

### \* 24/7 Quality Support

We will provide service round the clock.

### \* 100% Pass Rate

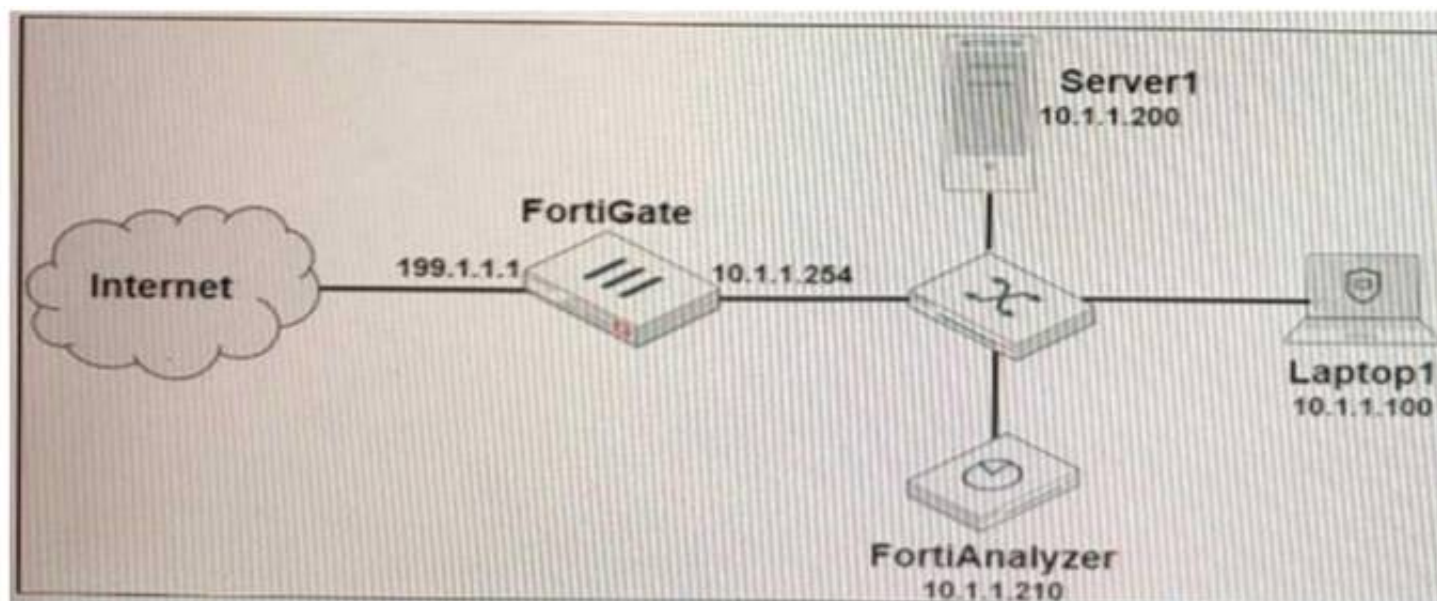
Our guarantee that you will pass the exam.

### \* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

### NEW QUESTION 1

Refer to the exhibit.



Laptop1 is used by several administrators to manage FortiAnalyzer. You want to configure a generic text filter that matches all login attempts to the web interface generated by any user other than "admin" and coming from Laptop1:  
 Which filter will achieve the desired result?

- A. operation-login & performed\_on=="GUI(10.1.1.100)" & user!=admin
- B. operation-login & srcip==10.1.1.100 & dstip==10.1.1.210 & user==admin
- C. operation-login & dstip==10.1.1.210 & user!=admin
- D. operation-login & performed\_on=="GUI(10.1.1.210)" & user!=admin

**Answer: A**

#### Explanation:

On there the task was to create a filter for failed logins from any other location but the local computer: "Add the text performed\_on!~10.0.1.10. This includes any attempts coming from devices with an IP address that is not the one configured on the Local-Client computer."

### NEW QUESTION 2

A rogue administrator was accessing FortiAnalyzer without permission, and you are tasked to see what activity was performed by that rogue administrator on FortiAnalyzer.

What can you do on FortiAnalyzer to accomplish this?

- A. Click FortiView and generate a report for that administrator.
- B. Click Task Monitor and view the tasks performed by that administrator.
- C. Click Log View and generate a report for that administrator.
- D. View the tasks performed by the rogue administrator in Fabric View.

**Answer: B**

### NEW QUESTION 3

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 4

What are two benefits of using fabric connectors? (Choose two.)

- A. They allow FortiAnalyzer to send logs in real-time to public cloud accounts.
- B. You do not need an additional license to send logs to the cloud platform.
- C. Fabric connectors allow you to improve redundancy.
- D. Using fabric connectors is more efficient than using third-party polling with API.

**Answer: AC**

### NEW QUESTION 5

What must you consider when using log fetching? (Choose two.)

- A. The fetch client can retrieve logs from devices that are not added to its local Device Manager
- B. You can use filters to include only logs from a single device.
- C. The fetching profile must include a user with the Super\_User profile.
- D. The archive logs retrieved from the server become archive logs in the client.

**Answer: BC**

#### NEW QUESTION 6

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:** AC

#### Explanation:

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

#### NEW QUESTION 7

FortiAnalyzer centralizes which functions? (Choose three)

- A. Network analysis
- B. Graphical reporting
- C. Content archiving / data mining
- D. Vulnerability assessment
- E. Security log analysis / forensics

**Answer:** BCE

#### NEW QUESTION 8

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

**Answer:** AB

#### Explanation:

To prevent logs from being tampered with while in storage, you can add a log checksum using the config system global command. You can configure FortiAnalyzer to record a log file hash value, timestamp, and authentication code when the log is rolled and archived and when the log is uploaded (if that feature is enabled). This can also help against man-in-the-middle only for the transmission from FortiAnalyzer to an SSH File Transfer Protocol (SFTP) server during log upload.  
FortiAnalyzer\_7.0\_Study\_Guide-Online page 149

#### NEW QUESTION 9

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

- A. It automatically updates the hcache when new logs arrive.
- B. It provides diagnostics on report generation time.
- C. It reduces the log insert lag rate.
- D. It reduces report generation time.

**Answer:** AD

#### NEW QUESTION 10

Which statement describes online logs on FortiAnalyzer?

- A. Logs that reached a specific size and were rolled over
- B. Logs that can be used to create reports
- C. Logs that can be viewed using Log Browse
- D. Logs that are saved to disk, compressed, and available in FortiView

**Answer:** C

#### NEW QUESTION 10

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

- A. Both modes, forwarding and aggregation, support encryption of logs between devices.
- B. In aggregation mode, you can forward logs to syslog and CEF servers as well.
- C. Aggregation mode stores logs and content files and uploads them to another FortiAnalyzer device at a scheduled time.
- D. Forwarding mode forwards logs in real time only to other FortiAnalyzer devices.

**Answer:** AC

#### Explanation:

A) FortiAnalyzer\_7.0\_Study\_Guide-Online.pdf page 148: The log communication between devices can be protected by encryption, with the desired encryption level, using the commands shown on the slide. (You need to interpret this. "Real time" and "aggregation" is about the "moment" when Fortigate sends the logs. However, no matter the moment, Fortigate will upload logs encrypted or unencrypted based on previous / different config).  
C) FortiAnalyzer\_7.0\_Study\_Guide-Online.pdf page 147: Aggregation: Logs and content files stored and uploaded at scheduled time.

#### NEW QUESTION 11

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.

**Answer:** B

#### NEW QUESTION 12

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

- A. Principal
- B. Service provider
- C. Identity collector
- D. Identity provider

**Answer:** BD

#### NEW QUESTION 15

You need to upgrade your FortiAnalyzer firmware.

What happens to the logs being sent to FortiAnalyzer from FortiGate during the time FortiAnalyzer is temporarily unavailable?

- A. FortiAnalyzer uses log fetching to retrieve the logs when back online
- B. FortiGate uses the miglogd process to cache the logs
- C. The logfiled process stores logs in offline mode
- D. Logs are dropped

**Answer:** B

#### Explanation:

If FortiAnalyzer becomes unavailable to FortiGate for any reason, FortiGate uses its *miglogd* process to cache the logs. There is a maximum value to the cache size, and the miglogd process will drop cached logs. When the connection between the two devices is restored, the miglogd process begins to send the cached logs to FortiAnalyzer. Therefore, the FortiGate buffer will keep logs long enough to sustain a reboot of your FortiAnalyzer (if you are upgrading the firmware, for example). But it is not intended for a lengthy FortiAnalyzer outage.

#### NEW QUESTION 18

What is Log Insert Lag Time on FortiAnalyzer?

- A. The number of times in the logs where end users experienced slowness while accessing resources.
- B. The amount of lag time that occurs when the administrator is rebuilding the ADOM database.
- C. The amount of time that passes between the time a log was received and when it was indexed on FortiAnalyzer.
- D. The amount of time FortiAnalyzer takes to receive logs from a registered device

**Answer:** C

#### NEW QUESTION 23

Which two statements are true regardless of initial Logs sync and Log Data Sync for HA on FortiAnalyzer?

- A. By default, Log Data Sync is disabled on all backup devices.
- 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 rebuild the log database with the synchronized logs.

**Answer:** CD

#### NEW QUESTION 28

Which two statements are true regarding high availability (HA) on FortiAnalyzer? (Choose two.)

- A. FortiAnalyzer HA can function without VRR
- B. and VRRP is required only if you have more than two FortiAnalyzer devices in a cluster.
- C. FortiAnalyzer HA supports synchronization of logs as well as some system and configuration settings.
- D. All devices in a FortiAnalyzer HA cluster must run in the same operation mode: analyzer or collector.
- E. FortiAnalyzer HA implementation is supported by many public cloud infrastructures such as AWS, Microsoft Azure, and Google Cloud.

**Answer:** BC

#### NEW QUESTION 29

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



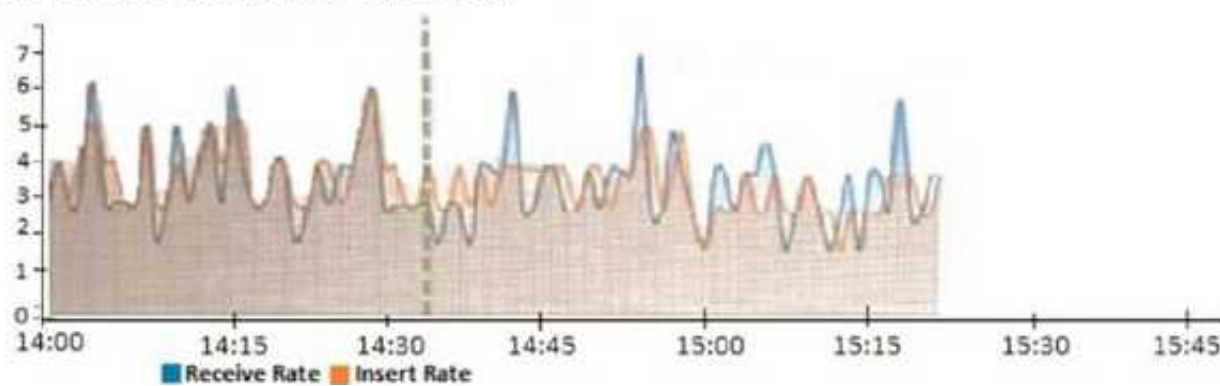
- C. The total disk space is insufficient and you need to add other disk  
D. The ADOM disk quota is set too low, based on log rates

**Answer: D**

#### NEW QUESTION 34

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 39

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

**Answer: A**

#### Explanation:

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->

#### NEW QUESTION 41

Which statement correctly describes the management extensions available on FortiAnalyzer?

- A. Management extensions do not require additional licenses.  
B. Management extensions allow FortiAnalyzer to act as a ForbSIEM supervisor.  
C. Management extensions require a dedicated VM for best performance.  
D. Management extensions may require a minimum number of CPU cores to run.

**Answer: D**

#### Explanation:

Events in FortiAnalyzer will be in one of four statuses. The current status will determine if more actions need to be taken by the security team or not. The possible statuses are:

Unhandled: The security event risk is not mitigated or contained, so it is considered open. Contained: The risk source is isolated.

Mitigated: The security risk is mitigated by being blocked or dropped. (Blank): Other scenarios.

FortiAnalyzer\_7.0\_Study\_Guide-Online pag. 189.

FortiAnalyzer\_7.0\_Study\_Guide-Online.pdf page 189: Review the hardware requirements before you enable a management extension application. Some of them require a minimum amount of memory or a minimum number of CPU cores.

#### NEW QUESTION 43

On the RAID management page, the disk status is listed as Initializing.

What does the status Initializing indicate about what the FortiAnalyzer is currently doing?

- A. FortiAnalyzer is ensuring that the parity data of a redundant drive is valid  
B. FortiAnalyzer is writing data to a newly added hard drive to restore it to an optimal state  
C. FortiAnalyzer is writing to all of its hard drives to make the array fault tolerant  
D. FortiAnalyzer is functioning normally

**Answer: C**

#### NEW QUESTION 44

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

**Answer:** A

#### NEW QUESTION 47

A playbook contains five tasks in total. An administrator runs the playbook and four out of five tasks finish successfully, but one task fails. What will be the status of the playbook after it is run?

- A. Running
- B. Failed
- C. Upstream\_failed
- D. Success

**Answer:** B

#### NEW QUESTION 51

Which two statements are true regarding fabric connectors? (Choose two.)

- A. Configuring fabric connectors to send notification to ITSM platform upon incident creation is more efficient than third-party information from the FortiAnalyzer API.
- B. Fabric connectors allow to save storage costs and improve redundancy.
- C. Storage connector service does not require a separate license to send logs to cloud platform.
- D. Cloud-Out connections allow you to send real-time logs to public cloud accounts like Amazon S3, Azure Blob, and Google Cloud.

**Answer:** AD

#### NEW QUESTION 52

Refer to the exhibit.

<b>FortiAnalyzer1# get system status</b> Platform Type : FAZVM64-KVM Platform Full Name : FortiAnalyzer-VM64-KVM Version : v7.2.1-build1215 220809 (GA) Serial Number : FAZ-VM0000065040 BIOS version : 04000002 Hostname : FortiAnalyzer1 Max Number of Admin Domains : 5 Admin Domain Configuration : Enabled FIPS Mode : Disabled HA Mode : Stand Alone Branch Point : 1215 Release Version Information : GA Time Zone : (GMT-8:00) Pacific Time (US & Canada) Disk Usage : Free 43.60GB, Total 58.80GB File System : Ext4 License Status : Valid  <b>FortiAnalyzer1# get system global</b> adom-mode : normal adom-select : enable adom-status : enable console-output : standard country-flag : enable enc-algorithm : high ha-member-auto-grouping : enable hostname : FortiAnalyzer2 log-checksum : md5 log-forward-cache-size : 5 log-mode : analyzer longitude : (null) max-aggregation-tasks : 0 max-running-reports : 1 oftp-ssl-protocol : tls1.2 ssl-low-encryption : disable ssl-protocol : tls1.3 tls1.2 : 2000 : tls1.3 tls1.2	<b>FortiAnalyzer3# get system status</b> Platform Type : FAZVM64-KVM Platform Full Name : FortiAnalyzer-VM64-KVM Version : v7.2.1-build1215 220809 (GA) Serial Number : FAZ-VM0000065042 BIOS version : 04000002 Hostname : FortiAnalyzer3 Max Number of Admin Domains : 5 Admin Domain Configuration : Enabled FIPS Mode : Disabled HA Mode : Stand Alone Branch Point : 1215 Release Version Information : GA Time Zone : (GMT-8:00) Pacific Time (US & Canada) Disk Usage : Free 12.98GB, Total 79.80GB File System : Ext4 License Status : Valid  <b>FortiAnalyzer3# get system global</b> adom-mode : normal adom-select : enable adom-status : enable console-output : standard country-flag : enable enc-algorithm : high ha-member-auto-grouping : enable hostname : FortiAnalyzer3 log-checksum : md5 log-forward-cache-size : 5 log-mode : analyzer longitude : (null) max-aggregation-tasks : 0 max-running-reports : 5 oftp-ssl-protocol : tls1.2 ssl-low-encryption : disable ssl-protocol : tls1.3 tls1.2 task-list-size : 2000 web-service-proto : tls1.3 tls1.2
---	--

Based on the partial outputs displayed, which devices can be members of a FortiAnalyzer Fabric?

- A. FortiAnalyzer1 and FortiAnalyzer3
- B. FortiAnalyzer1 and FortiAnalyzer2
- C. All devices listed can be members
- D. FortiAnalyzer2 and FortiAnalyzer3

**Answer:** C

#### NEW QUESTION 57

You created a playbook on FortiAnalyzer that uses a FortiOS connector

When configuring the FortiGate side, which type of trigger must be used so that the actions in an automation stitch are available in the FortiOS connector?

- A. FortiAnalyzer Event Handler
- B. Incoming webhook
- C. FortiOS Event Log
- D. Fabric Connector event

**Answer:** B

#### Explanation:

"One possible scenario is shown on the slide:

- \* 1. Traffic flows through the FortiGate
- \* 2. FortiGate sends logs to FortiAnalyzer
- \* 3. FortiAnalyzer detects some suspicious traffic and generates an event
- \* 4. The event triggers the execution of a playbook in FortiAnalyzer, which sends a webhook call to FortiGate so that it runs an automation stitch
- \* 5. FortiGate runs the automation stitch with the corrective or preventive actions" FortiAnalyzer\_7.0\_Study\_Guide-Online page 228

In order to see the actions related to the FOS connector, you must enable an automation rule using the Incoming Webhook Call trigger on the FortiGate side.

FortiAnalyzer\_7.0\_Study Guide page no 233

#### NEW QUESTION 61

What statements are true regarding FortiAnalyzer 's treatment of high availability (HA) clusters? (Choose two)

- A. FortiAnalyzer distinguishes different devices by their serial number.
- B. FortiAnalyzer receives logs from all devices in a cluster.
- C. FortiAnalyzer receives logs only from the primary device in the cluster.
- D. FortiAnalyzer only needs to know the serial number of the primary device in the cluster-it automatically discovers the other devices.

**Answer:** AB

#### NEW QUESTION 62

What are two effects of enabling auto-cache in a FortiAnalyzer report? (Choose two.)

- A. The size of newly generated reports is optimized to conserve disk space.
- B. FortiAnalyzer local cache is used to store generated reports.
- C. When new logs are received, the hard-cache data is updated automatically.
- D. The generation time for reports is decreased.

**Answer:** CD

#### NEW QUESTION 64

An administrator has configured the following settings: config system fortiview settings

set resolve-ip enable end

What is the significance of executing this command?

- A. Use this command only if the source IP addresses are not resolved on FortiGate.
- B. It resolves the source and destination IP addresses to a hostname in FortiView on FortiAnalyzer.
- C. You must configure local DNS servers on FortiGate for this command to resolve IP addresses on Forti Analyzer.
- D. It resolves the destination IP address to a hostname in FortiView on FortiAnalyzer.

**Answer:** D

#### NEW QUESTION 66

What FortiGate process caches logs when FortiAnalyzer is not reachable?

- A. logfiled
- B. sqlplugind
- C. oftpd
- D. miglogd

**Answer:** D

#### NEW QUESTION 68

What statements are true regarding disk log quota? (Choose two)

- A. The FortiAnalyzer stops logging once the disk log quota is met.
- B. The FortiAnalyzer automatically sets the disk log quota based on the device.
- C. The FortiAnalyzer can overwrite the oldest logs or stop logging once the disk log quota is met.
- D. The FortiAnalyzer disk log quota is configurable, but has a minimum of 100mb and a maximum based on the reserved system space.

**Answer:** CD



#### NEW QUESTION 71

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 72

Which two statements are correct regarding the export and import of playbooks? (Choose two.)

- A. You can export only one playbook at a time.
- B. You can import a playbook even if there is another one with the same name in the destination.
- C. Playbooks can be exported and imported only within the same FortiAnalyzer.
- D. A playbook that was disabled when it was exported, will be disabled when it is imported.

**Answer:** BD

#### Explanation:

If the imported playbook has the same name as an existing one, FortiAnalyzer will create a new name that includes a timestamp to avoid conflicts. Playbooks are imported with the same status they had (enabled or disabled) when they were exported. Playbooks set to run automatically should be exported while they are disabled to avoid unintended runs on the destination.

#### NEW QUESTION 73

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.

**Answer:** D

#### NEW QUESTION 77

Refer to the exhibit.



What does the data point at 12:20 indicate?

- A. The performance of FortiAnalyzer is below the baseline.
- B. FortiAnalyzer is using its cache to avoid dropping logs.
- C. The log insert lag time is increasing.
- D. The sqlplugind service is caught up with new logs.

**Answer:** C

#### NEW QUESTION 82

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

**Answer:** B

#### NEW QUESTION 83

If you upgrade your FortiAnalyzer firmware, what report elements can be affected?

- A. Output profiles
- B. Report settings
- C. Report scheduling
- D. Custom datasets

**Answer:** D

#### NEW QUESTION 84

Why must you wait for several minutes before you run a playbook that you just created?

- A. FortiAnalyzer needs that time to parse the new playbook.
- B. FortiAnalyzer needs that time to back up the current playbooks.
- C. FortiAnalyzer needs that time to ensure there are no other playbooks running.
- D. FortiAnalyzer needs that time to debug the new playbook.

**Answer:** A

#### NEW QUESTION 87

.....

## Relate Links

**100% Pass Your NSE5\_FAZ-7.2 Exam with Exambible Prep Materials**

[https://www.exambible.com/NSE5\\_FAZ-7.2-exam/](https://www.exambible.com/NSE5_FAZ-7.2-exam/)

## Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>