Fortinet

Exam Questions FCP_FAZ_AN-7.4

FCP - FortiAnalyzer 7.4 Analyst

NEW QUESTION 1
As part of your analysis, you discover that an incident is a false positive. You change the incident status to Closed: False Positive.
Which statement about your update is true?

A. The audit history log will be updated.
B. The corresponding event will be marked as mitigated.
C. The incident will be deleted.
D. The incident number will be changed

Answer: A

Explanation:
When an incident in FortiAnalyzer is identified as a false positive and its status is updated to "Closed: False Positive," certain records and logs are updated to reflect this change.
? Option A - The Audit History Log Will Be Updated:
? Option B - The Corresponding Event Will Be Marked as Mitigated:
? Option C - The Incident Will Be Deleted:
? Option D - The Incident Number Will Be Changed:
Conclusion:
? Correct Answer: A. The audit history log will be updated.
? This is the most accurate answer, as the update to "Closed: False Positive" is recorded in FortiAnalyzer??s audit history log for accountability and tracking purposes.
References:
? FortiAnalyzer 7.4.1 documentation on incident management and audit history logging.

NEW QUESTION 2
Which SQL query is in the correct order to query to database in the FortiAnalyzer?

A. SELECT devid FROM $log GROUP BY devid WHERE ??user??,,?? users1??
B. SELECT FROM $log WHERE devid ??user??,, USER1?? GROUP BY devid
C. SELCT devid WHERE ??user??-?? USER1?? FROM $log GROUP By devid
D. SELECT devid FROM $log WHERE ??user??=?? GROUP BY devid

Answer: D

Explanation:
In FortiAnalyzer??s SQL query syntax, the typical order for querying the database follows the standard SQL format, which is:
SELECT <column(s)> FROM <table> WHERE <condition(s)> GROUP BY <column(s)>
? Option D correctly follows this structure:
Let??s briefly examine why the other options are incorrect:
? Option A: SELECT devid FROM $log GROUP BY devid WHERE 'user', 'users1'
? Option B: SELECT FROM $log WHERE devid 'user', USER1' GROUP BY devid
? Option C: SELCT devid WHERE 'user' - 'USER1' FROM $log GROUP BY devid References: FortiAnalyzer documentation for SQL queries indicates that the standard SQL order should be followed when querying logs in FortiAnalyzer. Queries should follow the format SELECT ... FROM ... WHERE ... GROUP BY ..., as demonstrated in option D.

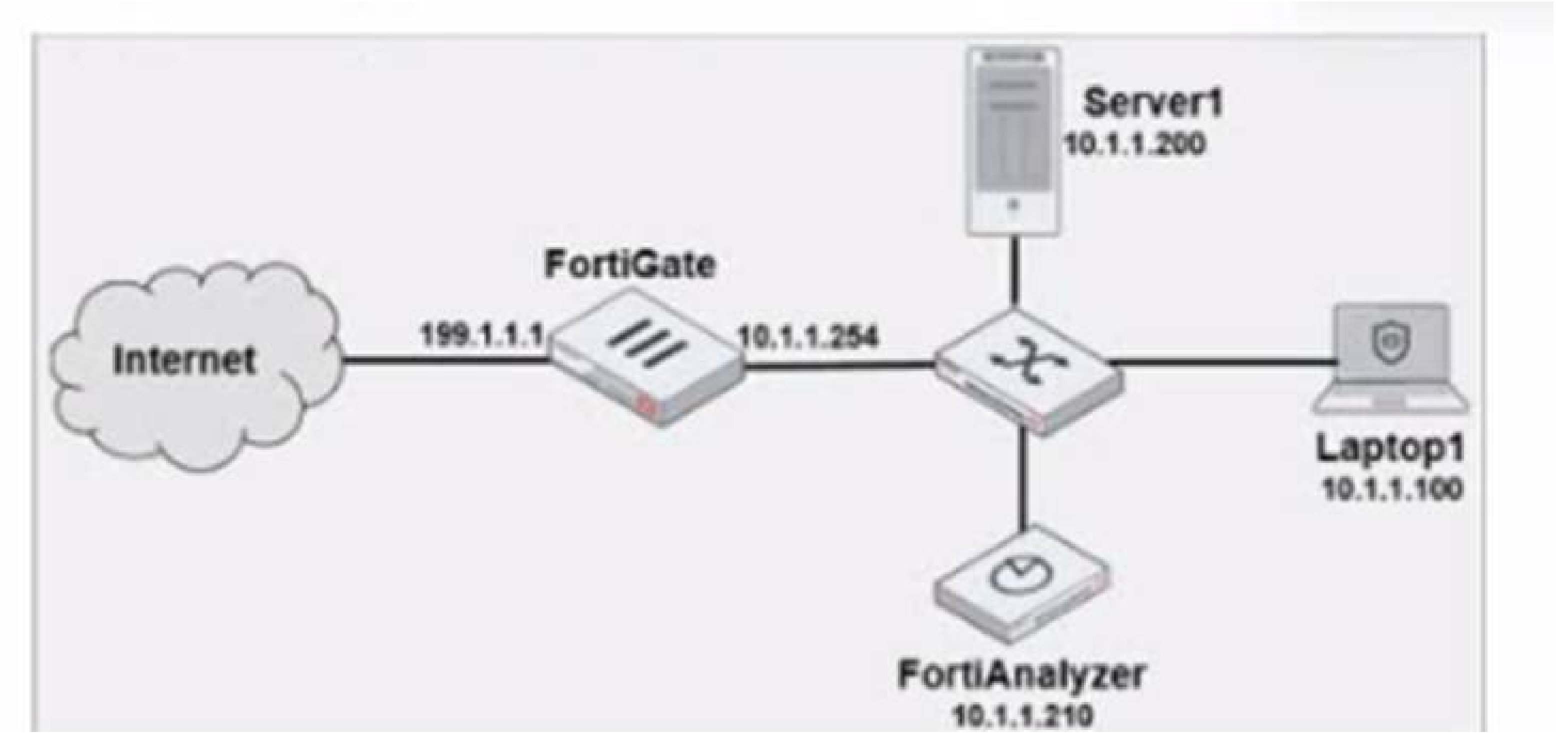
NEW QUESTION 3
Which FortiAnalyzer feature allows you to use a proactive approach when managing your network security?

A. FortiView Monitor
B. Outbreak alert services
C. Incidents dashboard
D. Threat hunting

Answer: D

Explanation:
FortiAnalyzer offers several features for monitoring, alerting, and incident management, each serving different purposes. Let's examine each option to determine which one best supports a proactive security approach.
? Option A - FortiView Monitor:
? Option B - Outbreak Alert Services:
? Option C - Incidents Dashboard:
? Option D - Threat Hunting:
Conclusion:
? Correct Answer: D. Threat hunting
? Threat hunting is the most proactive feature among the options, as it involves actively searching for threats within the network rather than reacting to already detected incidents.
References:
? FortiAnalyzer 7.4.1 documentation on Threat Hunting and proactive security measures.

NEW QUESTION 4
Exhibit.



Laptop1 is used by several administrators to manage FotiAnalyzer. 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 and performed_on==????GUI(10.1.1.100)?? and user!=admin
B. Operation-login and performed_on==????GU (10.1.1.120)?? and user!=admin
C. Operation-login and srcip== 10.1.1.100 and dstip==10.1.1.1.210 and user==admin
D. Operation-login and dstip==10.1.1.210 and user!-admin

Answer: A

Explanation:
The objective is to create a filter that identifies all login attempts to the FortiAnalyzer web interface (GUI) coming from Laptop1 (IP 10.1.1.100) and excludes the admin user. This filter should match any user other than admin.
? Filter Components Analysis:
? Option Analysis:
Conclusion:
? Correct Answer: A. Operation-login and performed_on==????GUI(10.1.1.100)?? and user!=admin
? This filter precisely captures the required conditions: login attempts from Laptop1 to the GUI interface by any user except admin.
References:
? FortiAnalyzer 7.4.1 documentation on log filters, syntax for login operations, and GUI login tracking.

NEW QUESTION 5
Which statement describes archive logs on FortiAnalyzer?

A. Logs that are indexed and stored in the SQL database
B. Logs a FortiAnalyzer administrator can access in FortiView
C. Logs compressed and saved in files with the .gz extension
D. Logs previously collected from devices that are offline

Answer: C

Explanation:
In FortiAnalyzer, archive logs refer to logs that have been compressed and stored to save space. This process involves compressing the raw log files into the .gz format, which is a common compression format used in Fortinet systems for archived data. Archiving is essential in FortiAnalyzer to optimize storage and manage long-term retention of logs without impacting performance.
Let??s examine each option for clarity:
? Option A: Logs that are indexed and stored in the SQL database
? Option B: Logs a FortiAnalyzer administrator can access in FortiView
? Option C: Logs compressed and saved in files with the .gz extension
? Option D: Logs previously collected from devices that are offline
References: FortiAnalyzer 7.4.1 documentation and configuration guides outline that archived logs are stored in compressed files with the .gz extension to conserve storage space, ensuring FortiAnalyzer can handle a larger volume of logs over extended periods.

NEW QUESTION 6
What happens when the indicator of compromise (IOC) engine on FortiAnalyzer finds web logs that match blacklisted IP addresses?

A. FortiAnalyzer flags the associated host for further analysis.
B. A new infected entry is added for the corresponding endpoint under Compromised Hosts.
C. The detection engine classifies those logs as Suspicious.
D. The endpoint is marked as Compromised and, optionally, can be put in quarantine.

Answer: B

NEW QUESTION 7
You must find a specific security event log in the FortiAnalyzer logs displayed in FortiView, but, so far, you have been uncuccessful.
Which two tasks should you perform to investigate why you are having this issue? (Choose two.)

A. Open .gz log files in FortiView.
B. Rebuild the SQL database and check FortiView.
C. Review the ADOM data policy
D. Check logs in the Log Browse

Answer: AB

NEW QUESTION 8
As part of your analysis, you discover that a Medium severity level incident is fully remediated.
You change the incident status to Closed:Remediated. Which statement about your update is true?

A. The incident can no longer be deleted.
B. The corresponding event will be marked as Mitigated.
C. The incident dashboard will be updated.
D. The incident severity will be lowered.

Answer: C

NEW QUESTION 9
Which statement about the FortiSOAR management extension is correct?

A. It requires a FortiManager configured to manage FortiGate.
B. It runs as a docker container on FortiAnalyzer.
C. It requires a dedicated FortiSOAR device or VM.
D. It does not include a limited trial by default.

Answer: C

Explanation:
The FortiSOAR management extension is designed as an independent security orchestration, automation, and response (SOAR) solution that integrates with other Fortinet products but requires its own dedicated device or virtual machine (VM) environment. FortiSOAR is not natively integrated as a container or service within FortiAnalyzer or FortiManager, and it operates separately to manage complex security workflows and incident responses across various platforms.
Let??s examine each option to determine the correct Answer:
? Option A: It requires a FortiManager configured to manage FortiGate
? Option B: It runs as a docker container on FortiAnalyzer
? Option C: It requires a dedicated FortiSOAR device or VM
? Option D: It does not include a limited trial by default
References: The FortiSOAR platform, as outlined in Fortinet product documentation, is a standalone SOAR solution that requires a dedicated device or VM for deployment. It integrates with Fortinet??s Security Fabric but operates separately from FortiAnalyzer, FortiManager, and FortiGate, focusing on advanced incident management and security automation.

NEW QUESTION 10
Which statement about sending notifications with incident updates is true?

A. Each connector used can have different notification settings
B. Each incident can send notification to a single external platform.
C. You must configure an output profile to send notifications by email.
D. Notifications can be sent only when an incident is created oi deleted.

Answer: A

NEW QUESTION 10
Which statement correctly describes one Difference between templates and reports?

A. Reports provide mora configuration options than templates
B. Templates can be cloned, but reports cannot be cloned.
C. Reports support macros, but templates do not.
D. Template are mapped to device group
E. while reports are mapped to ADOMs

Answer: A

NEW QUESTION 11
What is the purpose of using data selectors when configuring event handlers?

A. They filter the types of logs that FortiAnalyzer can accept from registered devices.
B. They download new filters can be used in event handlers.
C. They apply their filter criteria to the entire event handler so that you don??t have to configure the same criteria in the individual rules.
D. They are common filters that can be applied simultaneously to all event handlers.

Answer: C

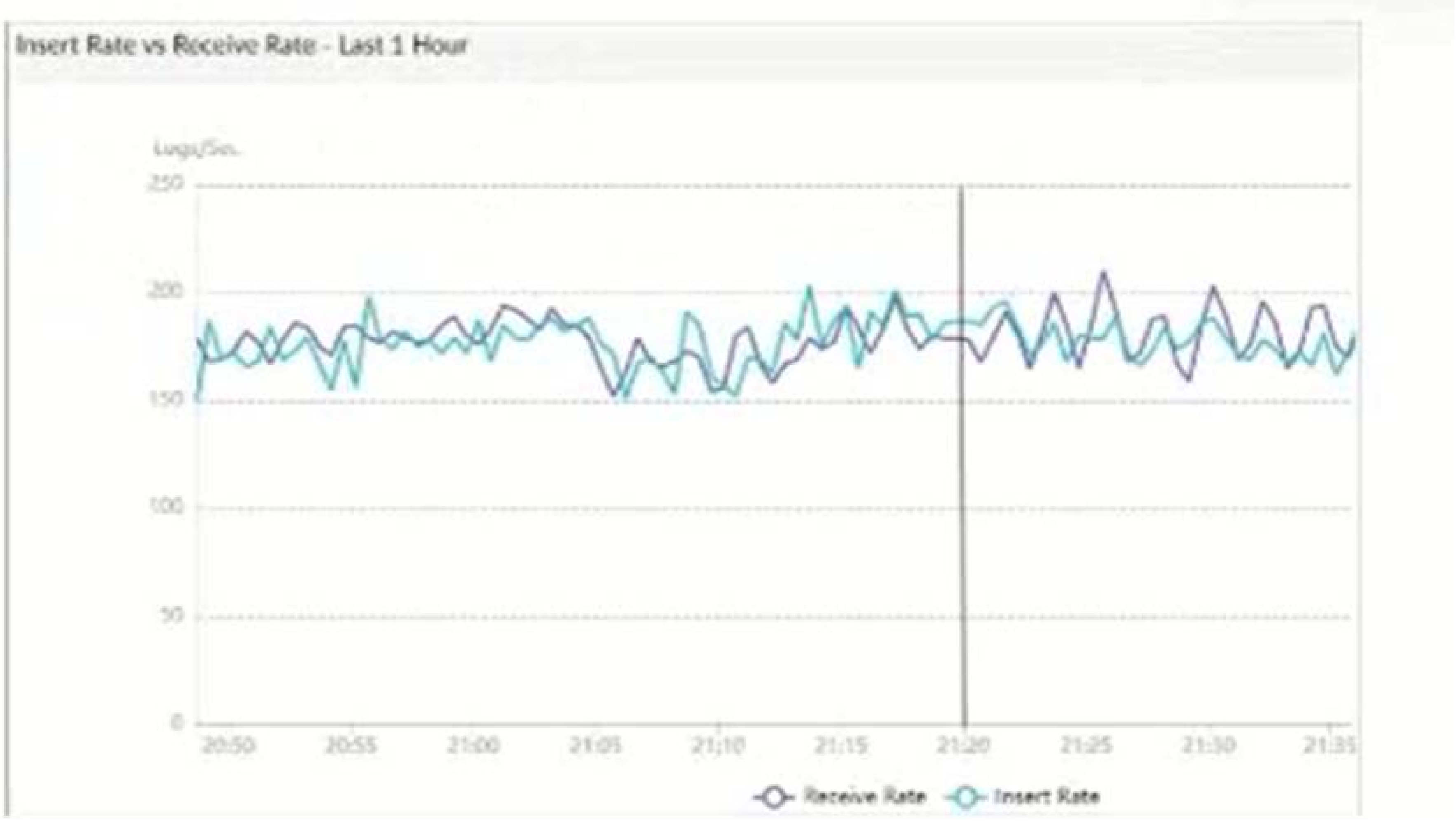
NEW QUESTION 13
Which log will generate an event with the status Contained?

A. An AV log with action=quarantine.
B. An IPS log with action=pass.

C. A WebFilter log will action=dropped.
D. An AppControl log with action=blocked.

Answer: A

NEW QUESTION 15
Refer to Exhibit:



What does the data point at 21:20 indicate?

A. FortiAnalyzer is indexing logs faster than logs are being received.
B. The fortilogd daemon is ahead in indexing by one log.
C. The SQL database requires a rebuild because of high receive lag.
D. FortiAnalyzer is temporarily buffering received logs so older logs can be indexed first.

Answer: A

Explanation:
The exhibit shows a graph that tracks two metrics over time: Receive Rate and Insert Rate. These two rates are crucial for understanding the log processing behavior in FortiAnalyzer.
? Understanding Receive Rate and Insert Rate:
? Data Point at 21:20:
? Option Analysis:
Conclusion:
? Correct Answer: A. FortiAnalyzer is indexing logs faster than logs are being received.
? The graph at 21:20 shows a higher Insert Rate than Receive Rate, indicating efficient log processing by FortiAnalyzer.
References:
? FortiAnalyzer 7.4.1 documentation on log processing metrics, Receive Rate, and Insert Rate indicators.

NEW QUESTION 17
Which statement about exporting items in Report Definitions is true?

A. Templates can be exported.
B. Template exports contain associated charts and datasets.
C. Chart exports contain associated datasets.
D. Datasets can be exported.

Answer: B

NEW QUESTION 19
Which statement about the FortiSIEM management extension is correct?

A. It allows you to manage the entire life cycle of a threat or breach.
B. It can be installed as a dedicated VM.
C. Its use of the available disk space is capped at 50%.
D. It requires a licensed FortiSIEM supervisor.

Answer: B

NEW QUESTION 23
Which two statement regarding the outbreak detection service are true? (Choose two.)

A. An additional license is required.
B. It automatically downloads new event handlers and reports.
C. Outbreak alerts are available on the root ADOM only.
D. New alerts are received by email.

Answer: BC

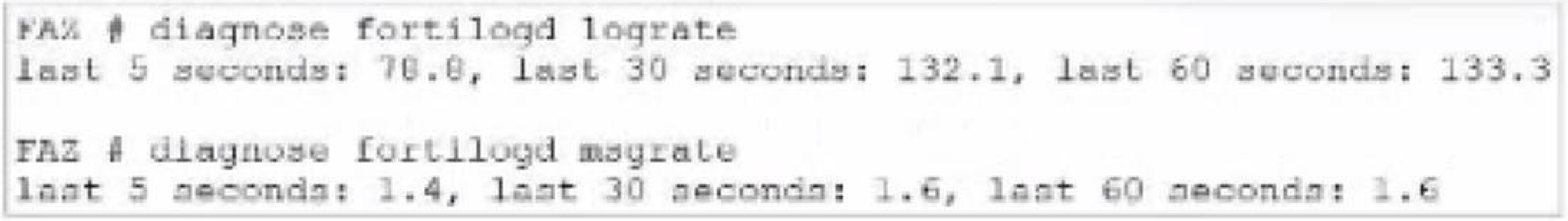
NEW QUESTION 24
An administrator on your team has configured multiple reports to run periodically. Management has an additional request that all new generated reports be sent to a company email inbox for accessibility. The mail server has already been configured on FortiAnalyzer.
Which item must configure on FortiAnalyzer so that emails are sent when the reports are generated?

A. Enable the option to email all repots under the mail server.
B. Add a mailto:<email address> option within the report layouts.
C. Enable email notification under the report calendar.
D. Enable an output profile on the reports.

Answer: D

Explanation:
To ensure that reports generated by FortiAnalyzer are automatically sent to an email inbox, you need to set up an output profile for the reports. Output profiles specify where and how reports should be delivered, including the option to send them via email.
? Option A - Enable the Option to Email All Reports Under the Mail Server:
? Option B - Add a mailto:<email address> Option Within the Report Layouts:
? Option C - Enable Email Notification Under the Report Calendar:
? Option D - Enable an Output Profile on the Reports:
Conclusion:
? Correct Answer: D. Enable an output profile on the reports.
? Configuring an output profile is the correct way to set up automatic email distribution of generated reports in FortiAnalyzer.
References:
? FortiAnalyzer 7.4.1 documentation on configuring output profiles and report distribution settings.

NEW QUESTION 28
Exhibit.



```
FAZ # diagnose fortilogd lograte
last 5 seconds: 70.0, last 30 seconds: 132.1, last 60 seconds: 133.3

FAZ # diagnose fortilogd msgrate
last 5 seconds: 1.4, last 30 seconds: 1.6, last 60 seconds: 1.6
```

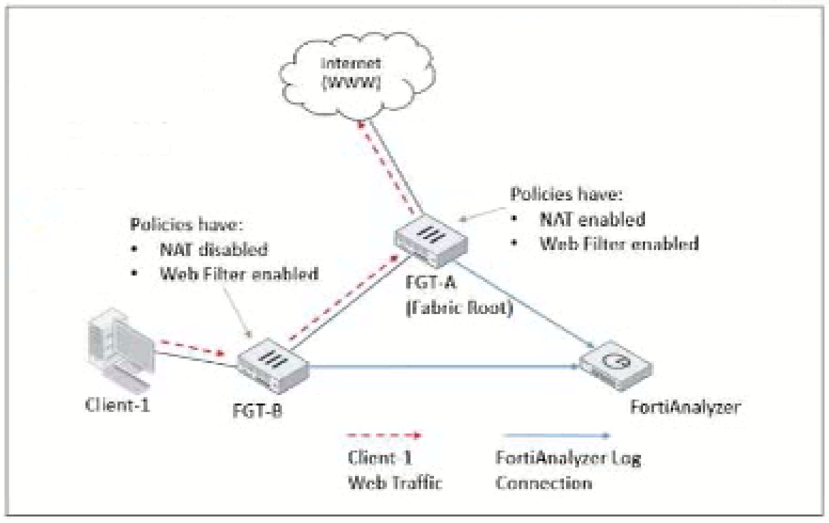
What can you conclude about the output?

A. The message rate being lower that the log rate is normal.
B. Both messages and logs are almost finished indexing.
C. There are more traffic logs than event logs.
D. The output is ADOM specific

Answer: A

Explanation:
In this output, we see two diagnostic commands executed on a FortiAnalyzer device:
? diagnose fortilogd lograte: This command shows the rate at which logs are being processed by the FortiAnalyzer in terms of log entries per second.
? diagnose fortilogd msgrate: This command displays the message rate, or the rate at which individual messages are being processed.
The values provided in the exhibit output show:
? Log rate (lograte): Consistently high, showing values such as 70.0, 132.1, and 133.3 logs per second over different time intervals.
? Message rate (msgrate): Lower values, around 1.4 to 1.6 messages per second. Explanation
? Interpretation of log rate vs. message rate: In FortiAnalyzer, the log rate typically refers to the rate of logs being stored or indexed, while the message rate refers to individual messages within these logs. Given that a single log entry can contain multiple messages, it's common to see a lower message rate relative to the log rate.
? Understanding normal operation: In this case, the message rate being lower than the log rate is expected and typical behavior. This discrepancy can arise because each log entry may bundle multiple related messages, reducing the message rate relative to the log rate.
Conclusion
? Correct Answer: A. The message rate being lower than the log rate is normal.
? This aligns with the normal operational behavior of FortiAnalyzer in processing logs and messages.
There is no indication that both logs and messages are nearly finished indexing, as that would typically show diminishing rates toward zero, which is not the case here. Additionally, there??s no information in this output about specific ADOMs or a comparison between traffic logs and event logs. Thus, options B, C, and D are incorrect.
References:
? FortiOS 7.4.1 and FortiAnalyzer 7.4.1 command guides for diagnose fortilogd lograte and diagnose fortilogd msgrate.

NEW QUESTION 33
Refer to Exhibit:



Client-1 is trying to access the internet for web browsing.
All FortiGate devices in the topology are part of a Security Fabric with logging to FortiAnalyzer configured. All firewall policies have logging enabled. All web filter profiles are configured to log only violations.
Which statement about the logging behavior for this specific traffic flow is true?

A. Only FGT-B will create traffic logs.
B. FGT-B will see the MAC address of FGT-A as the destination and notifies FGT-A to log this flow.
C. FGT B will create traffic logs and will create web filter logs if it detects a violation.
D. Only FGT-A will create web filter logs if it detects a violation.

Answer: C

Explanation:
The topology shows a Security Fabric setup involving FortiGate devices (FGT-A and FGT-B) and a FortiAnalyzer for centralized logging. Let??s break down the logging and traffic flow behavior:
? Traffic Flow Analysis:
? Policy and NAT Settings:
? Logging Behavior:
? Option Analysis:
Conclusion:
? Correct Answer: C. FGT-B will create traffic logs and will create web filter logs if it detects a violation.
? FGT-B is responsible for logging the traffic from Client-1 and will generate web filter logs if there is a policy violation, as configured.
References:
? FortiOS 7.4.1 documentation on Security Fabric logging behavior and FortiAnalyzer log integration.

NEW QUESTION 37
Which two statements about exporting and importing playbacks are true? (Choose two.)

A. A playbook that was disabled when it was exported mil be disabled when it is imported.
B. Playbooks can so imported 10 a different FortiAnayzer device, but only if the connectors already exist
C. You can import a playbook even if there is another one win the same name in the destination
D. You can export only one playbook at a time.

Answer: CD

NEW QUESTION 42
What are two effects of enabling auto-cache in a FortiAnalyzer report? (Choose two.)

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

Answer: AC

Explanation:
Enabling auto-cache in FortiAnalyzer reports is designed to improve the efficiency and speed of report generation by leveraging cached data. Let??s analyze each option to determine which effects are correct.
? Option A - The Generation Time for Reports is Decreased:
? Option B - Hard-Cache Data is Automatically Updated When New Logs are Received:
? Option C - FortiAnalyzer Local Cache is Used to Store Generated Reports:
? Option D - The Size of Newly Generated Reports is Optimized to Conserve Disk Space:
Conclusion:
? Correct Answer: A. The generation time for reports is decreased and C. FortiAnalyzer local cache is used to store generated reports.
? Enabling auto-cache helps reduce report generation time by using locally cached data and optimizes report processing, though it does not impact report size or continuously update with each new log.
References:
? FortiAnalyzer 7.4.1 documentation on report caching, auto-cache functionality, and report generation optimizations.

NEW QUESTION 43
......

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

FCP_FAZ_AN-7.4 Practice Exam Features:

* FCP_FAZ_AN-7.4 Questions and Answers Updated Frequently

* FCP_FAZ_AN-7.4 Practice Questions Verified by Expert Senior Certified Staff

* FCP_FAZ_AN-7.4 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* FCP_FAZ_AN-7.4 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
Order The FCP_FAZ_AN-7.4 Practice Test Here