



Fortinet

Exam Questions FCP_FAZ_AN-7.6

Fortinet NSE 5 - FortiAnalyzer 7.6 Analyst

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

What is the purpose of playbook trigger variables?

- A. To display statistics about the playbook runtime
- B. To use information from the trigger to filter the action in a task
- C. To provide the trigger information to make the playbook start running
- D. To store the start the times of playbooks with On_Schedule triggers

Answer: B

NEW QUESTION 2

You must find a specific security event log in the FortiAnalyzer logs displayed in FortiView, but, so far, you have been unsuccessful. 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 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:

* FortiView is a visualization tool that provides real-time and historical insights into network traffic, threats, and logs. While it gives visibility into network activity, it is generally more reactive than proactive, as it relies on existing log data and incidents.

* Conclusion: Incorrect.

* Option B - Outbreak Alert Services:

* Outbreak Alert Services in FortiAnalyzer notify administrators of emerging threats and outbreaks based on FortiGuard intelligence. This is beneficial for awareness of potential threats but does not offer a hands-on, investigative approach. It's more of a notification service rather than an active, proactive investigation tool.

* Conclusion: Incorrect.

* Option C - Incidents Dashboard:

* The Incidents Dashboard provides a summary of incidents and current security statuses within the network. While it assists with ongoing incident response, it is used to manage and track existing incidents rather than proactively identifying new threats.

* Conclusion: Incorrect.

* Option D - Threat Hunting:

* Threat Hunting in FortiAnalyzer enables security analysts to actively search for hidden threats or malicious activities within the network by leveraging historical data, analytics, and intelligence. This is a proactive approach as it allows analysts to seek out threats before they escalate into incidents.

* Conclusion: Correct.

* 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

Refer to the exhibit.

☐	Event ↕	Event Status ↕	Event Type ↕	Severity ↕
☐	56834764387462384.org (4)	Unhandled	Web Filter	Critical
☐	Web traffic to C&C from 10.0.1.200 detected	Unhandled	Web Filter	Critical

Which statement about the displayed event is correct? (Choose one answer))

- A. An incident was created from this event.
- B. The risk source is isolated.
- C. The security risk was escalated.
- D. The security event risk is considered open.

Answer: D

Explanation:

Comprehensive and Detailed Explanation: From Exact Extract of knowledge of FortiAnalyzer 7.6 Study guide documents:

In the exhibit, the Event Status shown is Unhandled (Event Type: Web Filter; Severity: Critical). The FortiAnalyzer study guide defines Unhandled events as events

whose security risk has not been addressed and is therefore still active/open. Specifically, it states:??Unhandled: The security risk is considered open.?? This directly matches optionD.

The other options correspond to different statuses or actions:

* Isolated/Containedapplies when the risk source is isolated (statusContained), notUnhandled.

* Escalatedrefers to events moved/raised for further action (statusEscalated), notUnhandled.

* Whether an incident was created cannot be concluded solely from the status ??Unhandled?? in the exhibit; the study guide ties incident creation to incident management workflows rather than equating ??Unhandled?? with an incident being created.

NEW QUESTION 5

What are the two methods you can use to send notifications when an event is generated by an event handler? (Choose two answers)

- A. Send SNMP trap.
- B. Send an alert through the FortiGuard server.
- C. Send an alert through Fabric connectors.
- D. Send SMS notification

Answer: AC

Explanation:

From Exact Extract of knowledge of FortiAnalyzer 7.6 Study guide documents:

FortiAnalyzer event handlers support alerting when a rule match generates an event. The study guide states that, for an event handler,??You can select a notification profile to send alerts whenever an event is generated by the handler.??In FortiAnalyzer, notification profiles are the mechanism used to deliver alerts outward (for example, via an SNMP trap), which directly aligns with optionA.

In addition, FortiAnalyzer supports sending notifications to external platforms through integrations:??You can configure FortiAnalyzer to send a notification to external platforms using preconfigured Fabric connectors.??This validates the use ofFabric connectorsas a notification delivery method, aligning with optionC. OptionBis not a notification delivery method for event-handler-generated alerts in the workflow described (FortiGuard is used for threat intelligence/enrichment rather than relaying alerts). OptionDis not presented in the study guide??s described notification mechanisms for event-handler alerting in the referenced sections.

NEW QUESTION 6

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:

Enablingauto-cachein 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:

* When auto-cache is enabled, FortiAnalyzer can use previously cached data instead of reprocessing all log datafrom scratch each time a report is generated. This results in faster report generation times, especially for recurring reports that use similar datasets.

* Conclusion:Correct.

* Option B - Hard-Cache Data is Automatically Updated When New Logs are Received:

* Enabling auto-cache does not immediately update the cache with every new log received. Instead, the cache is updated when reports are generated, based on the existing logs up to that point. Therefore, auto-cache does not constantly refresh with each incoming log, which would be inefficient.

* Conclusion:Incorrect.

* Option C - FortiAnalyzer Local Cache is Used to Store Generated Reports:

* Auto-cache utilizes FortiAnalyzer??s local cache to store data used in reports, reducing the need to retrieve and process logs repeatedly. This cached data can be reused for subsequent report generation, enhancing performance.

* Conclusion:Correct.

* Option D - The Size of Newly Generated Reports is Optimized to Conserve Disk Space:

* Auto-cache does not directly impact the size ofthe report files themselves. It focuses on performance optimization through cached data for faster access, but it does not compress or optimize the storage size of the generated report.

* Conclusion:Incorrect.Conclusion:

* Correct Answer A. The generation time for reports is decreasedandC. 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 7

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

Answer: A

Explanation:

When a new playbook is created on FortiAnalyzer, the system requires some time toparse and validatethe playbook before it can be executed. Parsing involves checking the playbook's structure, ensuring that all syntax and logic are correct, and preparing the playbook for execution within FortiAnalyzer??s automation engine. This initial parsing step is necessary for FortiAnalyzer to load the playbook into its operational environment correctly.

Here's why the other options are incorrect:

Option A: FortiAnalyzer needs that time to parse the new playbook

This is correct. The delay is due to the parsing and setup process required to prepare the new playbook for execution. FortiAnalyzer??s automation engine checks

for any issues or dependencies within the playbook, ensuring that it can run without errors.

Option B: FortiAnalyzer needs that time to debug the new playbook

This is incorrect. Debugging is not an automatic process that FortiAnalyzer undertakes after playbook creation. Debugging, if necessary, is a manual task performed by the administrator if there are issues with the playbook execution.

Option C: FortiAnalyzer needs that time to back up the current playbooks

This is incorrect. FortiAnalyzer does not automatically back up playbooks every time a new one is created. Backups of configuration and playbooks are typically scheduled as part of routine maintenance and are not triggered by playbook creation.

Option D: FortiAnalyzer needs that time to ensure there are no other playbooks running

This is incorrect. FortiAnalyzer can manage multiple playbooks running simultaneously, so it does not require waiting for other playbooks to finish before initiating a new one. The waiting time specifically relates to the parsing process of the newly created playbook.

[: FortiAnalyzer documentation states that after creating a playbook, a brief delay is expected as the system parses and validates the playbook. This ensures that any syntax errors or logical inconsistencies are resolved before the playbook is executed, making option A the correct answer?.,]

NEW QUESTION 8

How does FortiAnalyzer block indicators? (Choose one answer))

- A. It uses an automation script to update FortiGate with the block list.
- B. It uses a FortiManager connector to send the block list.
- C. It uses a FortiClient EMS connector to send the block list.
- D. It uses a webhook to allow FortiGate to send the block list.

Answer: B

Explanation:

Comprehensive and Detailed Explanation From Exact Extract of knowledge of FortiAnalyzer 7.6 Study guide documents:

The FortiAnalyzer study guide states that blocking suspicious indicators is performed by integrating FortiAnalyzer with FortiManager(not by directly pushing a block list to FortiGate). Specifically:"To use this feature, you must set up an authorized FortiManager connector for the FortiAnalyzer on the Fabric Connector page of FortiAnalyzer."

It then explains the backend mechanism:"In the back end, a playbook called Block_indicator runs every 5 minutes to send the information to FortiManager."After a successful run,"the blocked indicator is pushed to the FortiManager External Resource list."From there, FortiManager can create threat feeds/security profiles/policy blocks and push policies to FortiGate as needed—however, the study guide clarifies:??The Blocked status on FortiAnalyzer confirms that the list is updated on FortiManager, but it is not synced to FortiGate.??

Therefore, FortiAnalyzer blocks indicators by using a FortiManager connector and sending the block information to FortiManager (Option B).

NEW QUESTION 9

Exhibit.

☐	Event ⇅	Event Status ⇅	Event Type ⇅	Severity ⇅
☐	 buyqttatbsd.findhere.org (1)	Mitigated	 Web Filter	 Low
☐	Web request to suspicious destination from 10.0.3.20 blocked	Mitigated	 Web Filter	 Low

Which statement about the event displayed is correct?

- A. The risk source is isolated.
- B. The security risk was blocked or dropped.
- C. The security event risk is considered open.
- D. An incident was created from this event.

Answer: C

NEW QUESTION 10

When there are no matching parsers for a device log, what does FortiAnalyzer do? (Choose one answer))

- A. Drops the log
- B. Applies the generic SYSLOG parser
- C. Stores the log but doesn't normalize it
- D. Archives the log for future analysis

Answer: C

Explanation:

Comprehensive and Detailed Explanation From Exact Extract of knowledge of FortiAnalyzer 7.6 Study guide documents:

FortiAnalyzer's ingestion pipeline does not "drop" logs simply because a parser is unavailable. The study guide states that when devices send logs,"Logs received are decompressed and saved in a log file on the FortiAnalyzer disk??(with a .log extension). This establishes that the raw log is still accepted and stored on disk as part of the normal workflow.

Normalization, however, depends on having a suitable parser. The study guide explains that "FortiAnalyzer uses predefined parsers to extract key fields from ingested logs and maps them to a consistent, standardized set of field names."It further emphasizes that??Log parsers ?? are central to log normalization" because they convert unstructured/native logs into a standardized schema.

Therefore, if no matching parser exists for a given device log, FortiAnalyzer can still store the incoming log(it is received, decompressed, and written to disk), but it cannot perform the "extract key fields" and "map to standardized field names" steps required for normalization. In practical terms, the log remains in its native/unstructured form (not normalized), which aligns exactly with option C.

NEW QUESTION 10

Which statement about SQL SELECT queries is true?

- A. They can be used to purge log entries from the database.
They must be followed immediately by a WHERE clause.
- B. They can be used to display the database schema.
- C. They are not used in macros.
- D.

Answer: D

Explanation:

Option A - Purging Log Entries:

A SELECT query in SQL is used to retrieve data from a database and does not have the capability to delete or purge log entries. Purging logs typically requires a DELETE or TRUNCATE command.

Conclusion: Incorrect.

Option B - WHERE Clause Requirement:

In SQL, a SELECT query does not require a WHERE clause. The WHERE clause is optional and is used only when filtering results. A SELECT query can be executed without it, meaning this statement is false.

Conclusion: Incorrect.

Option C - Displaying Database Schema:

A SELECT query retrieves data from specified tables, but it is not used to display the structure or schema of the database. Commands like DESCRIBE, SHOW TABLES, or SHOW COLUMNS are typically used to view schema information.

Conclusion: Incorrect.

Option D - Usage in Macros:

FortiAnalyzer and similar systems often use macros for automated functions or specific query-based tasks. SELECT queries are typically not included in macros because macros focus on procedural or repetitive actions, rather than simple data retrieval.

Conclusion: Correct.

Conclusion:

Correct Answer D They are not used in macros.

This aligns with typical SQL usage and the specific functionalities of FortiAnalyzer.

Reference: FortiAnalyzer 7.4.1 documentation on SQL queries, database operations, and macro usage

NEW QUESTION 14

Exhibit.



#	Detailed Information
1	<code>date=2023-12-05 time=10:36:21 id=7309181279985991762 ltime=2023-12-05 10:36:22 euid=3 epid=101 dteuid=3 dtepid=101 type=traffic subtype=forward level=notice action=accept policyid=1 sessionid=4927418 srrip=10.0.1.10 dstrip=8.8.8.8 transip=10.200.1.10 srport=35228 dstport=53 transport=35228 transp=snat duration=217 proto=17 sentbyte=126 rcvbyte=272 sentdelta=126 rcvdelta=272 sentpkt=2 rcvpkt=2 logid=0000000020 service=DNS app=DNS appcat=unclassified srctrole=undefined dstntrole=undefined policytype=policy eventtime=1701801382117936850 poluid=b11ac58c-791b-51e7-4600-12f829a689d9 srcountry=Reserved dstcountry=United States srinif=port3 dstinif=port1 policynome=Full_Access tr=0800 devid=FGVM010000064692 vd=root dtime=2023-12-05 10:36:21 ltime_t=1701801382</code>
2	<code>date=2023-12-05 time=10:36:21 id=7309181279985991757 ltime=2023-12-05 10:36:22 euid=3 epid=101 dteuid=3 dtepid=101 type=traffic subtype=forward level=notice action=accept policyid=1 sessionid=4940127 srrip=10.0.1.10 dstrip=8.8.8.8 transip=10.200.1.10 srport=33741 dstport=53 transport=33741 transp=snat duration=124 proto=17 sentbyte=64 rcvbyte=124 sentdelta=64 rcvdelta=124 sentpkt=1 rcvpkt=1 logid=0000000020 service=DNS app=DNS appcat=unclassified srctrole=undefined dstntrole=undefined policytype=policy eventtime=1701801382077420512 poluid=b11ac58c-791b-51e7-4600-12f829a689d9 srcountry=Reserved dstcountry=United States srinif=port3 dstinif=port1 policynome=Full_Access tr=0800 devid=FGVM010000064692 vd=root dtime=2023-12-05 10:36:21 ltime_t=1701801382</code>

What can you conclude about these search results? (Choose two.)

- They can be downloaded to a file.
- A. They are sortable by columns and customizable.
- B. They are not available for analysis in FortiView.
- C. They were searched by using text mode.
- D.

Answer: AD

NEW QUESTION 19

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

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

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:
SELECT devid FROM \$log: This specifies that the query is selecting the devid column from the \$log table.
WHERE 'user' = ': This part of the query is intended to filter results based on a condition involving the user column. Although there appears to be a minor typographical issue (possibly missing the user value after =), it structurally adheres to the correct SQL order.
GROUP BY devid: This groups the results by devid, which is correctly positioned at the end of the query.
Let's briefly examine why the other options are incorrect:
Option A: SELECT devid FROM \$log GROUP BY devid WHERE 'user', 'users1'
This is incorrect because the GROUP BY clause appears before the WHERE clause, which is out of order in SQL syntax.
Option B: SELECT FROM \$log WHERE devid 'user', USER1' GROUP BY devid
This is incorrect because it lacks a column in the SELECT statement and the WHERE clause syntax is malformed.
Option C: SELCT devid WHERE 'user' - 'USER1' FROM \$log GROUP BY devid
This is incorrect because the SELECT keyword is misspelled as SELCT, and the WHERE condition syntax is invalid.
Reference: 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 21

Exhibit.

Playbook edit

Name	Attach Data		
Description	Attach Data		
Connector	Local Connector		
	This connector is auto-selected. You must click "OK" and save playbook to apply this selection.		
Action	Attach Data to Incident		
Incident ID	Playbook Starter	incident_id	A
Attachment	Run_REPORT	report_uuid	A
	(placeholder_cb43e1ef_b527_4c2b_a4c		

What is the analyst trying to create?

- The analyst is trying to create a trigger variable to the used in the playbook.
- A. The analyst is trying to create an output variable to be used in the playbook.
- B. The analyst is trying to create a report in the playbook.
- C. The analyst is trying to create a SOC report in the playbook.
- D.

Answer: B

Explanation:

In the exhibit, the playbook configuration shows the analyst working with the "Attach Data" action within a playbook. Here's a breakdown of key aspects:
Incident ID: This field is linked to the "Playbook Starter," which indicates that the playbook will attach data to an existing incident.
Attachment: The analyst is configuring an attachment by selecting Run_REPORT with a placeholder ID for report_uuid. This suggests that the report's UUID will dynamically populate as part of the playbook execution.
Analysis of Options:
Option A - Creating a Trigger Variable:
A trigger variable would typically be set up in the playbook starter or initiation configuration, not within the "Attach Data" action. The setup here does not indicate a trigger, as it's focusing on data attachment.
Conclusion: Incorrect.
Option B - Creating an Output Variable:
The field Attachment with a report_uuid placeholder suggests that the analyst is defining an output variable that will store the report data or ID, allowing it to be attached to the incident. This variable can then be referenced or passed within the playbook for further actions or reporting.
Conclusion: Correct.
Option C - Creating a Report in the Playbook:
While Run_REPORT is selected, it appears to be an attachment action rather than a report generation task. The purpose here is to attach an existing or dynamically generated report to an incident, not to create the report itself.
Conclusion: Incorrect.
Option D - Creating a SOC Report:
Similarly, this configuration is focused on attaching data, not specifically generating a SOC report.
SOC reports are generally predefined and generated outside the playbook.
Conclusion: Incorrect.
Conclusion:
Correct Answer B. The analyst is trying to create an output variable to be used in the playbook.
The setup allows the playbook to dynamically assign the report_uuid as an output variable, which can then be used in further actions within the playbook.

Reference: FortiAnalyzer 7.4.1 documentation on playbook configurations, output variables, and data attachment functionalities.

NEW QUESTION 24

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: C

NEW QUESTION 27

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:

Receive Rate: This is the rate at which FortiAnalyzer is receiving logs from connected devices.

Insert Rate: This is the rate at which FortiAnalyzer is indexing (inserting) logs into its database for storage and analysis.

Data Point at 21:20:

At 21:20, the Insert Rate line is above the Receive Rate line, indicating that FortiAnalyzer is inserting logs into its database at a faster rate than it is receiving them. This situation suggests that FortiAnalyzer is able to keep up with the incoming logs and is possibly processing a backlog or temporarily received logs faster than new logs are coming in.

Option Analysis:

Option A - FortiAnalyzer is Indexing Logs Faster Than Logs are Being Received: This accurately describes the scenario at 21:20, where the Insert Rate exceeds the Receive Rate. This indicates that FortiAnalyzer is handling logs efficiently at that moment, with no backlog in processing.

Option B - The fortilogd Daemon is Ahead in Indexing by One Log: The data does not provide specific information about the fortilogd daemon's log count, only the rates. This option is incorrect.

Option C - SQL Database Requires a Rebuild: High receive lag would imply a backlog in receiving and indexing logs, typically visible if the Receive Rate were significantly above the Insert Rate, which is not the case here.

Option D - FortiAnalyzer is Temporarily Buffering Logs to Index Older Logs First: There is no indication of buffering in this scenario. Buffering would usually occur if the Receive Rate were higher than the Insert Rate, indicating that FortiAnalyzer is storing logs temporarily due to indexing lag.

Conclusion:

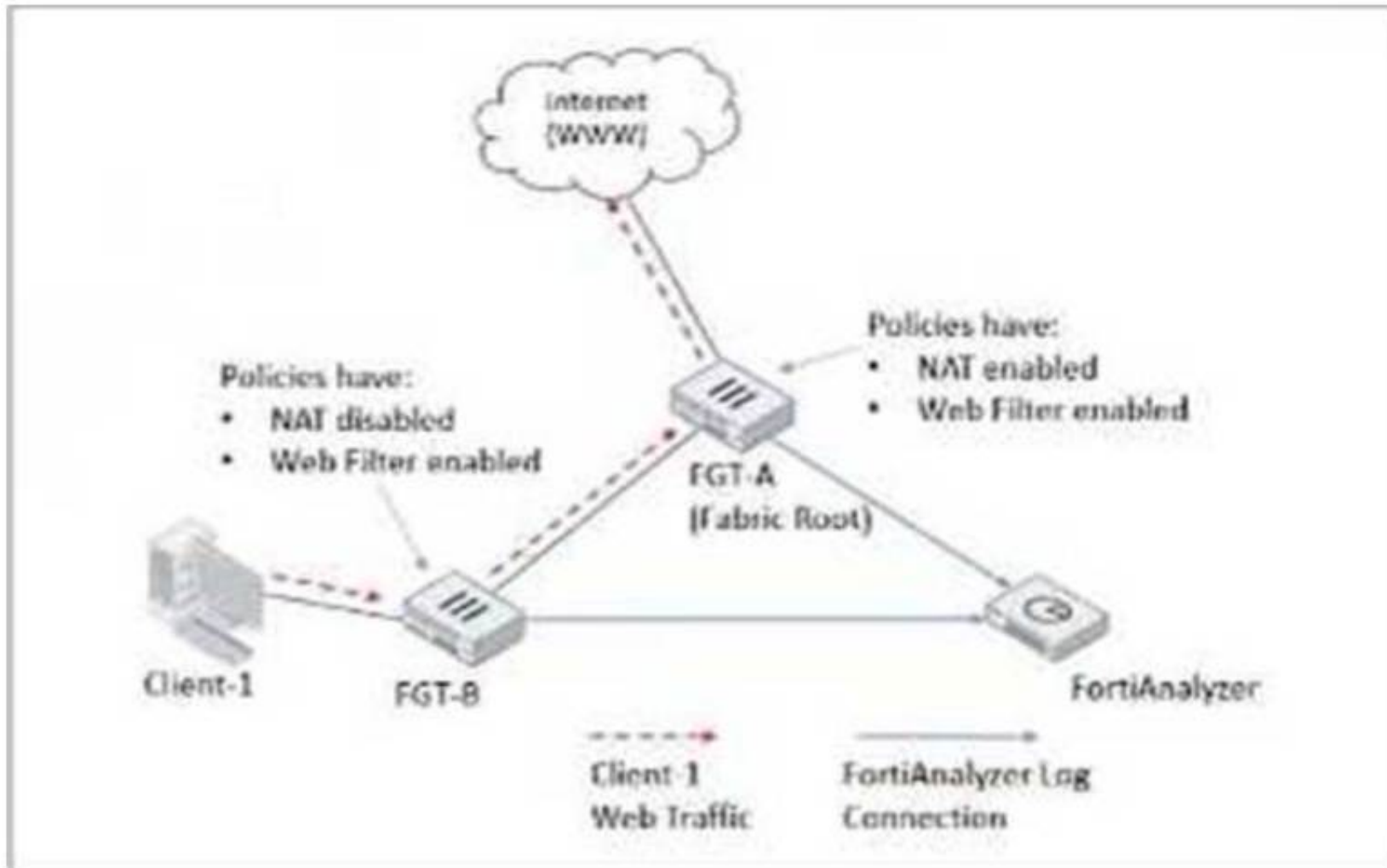
Correct Answer: A. FortiAnalyzer is indexing logs faster than logs are being received.

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 31

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: D

Explanation:

The study guide explains that in a Security Fabric, traffic logging is not duplicated across FortiGates for the same session: "Traffic logging for a session is always carried out by the first FortiGate that handled it and if a FortiGate receives traffic from a peer FortiGate MAC, it does not generate a new traffic log for that session."

For UTM (web filtering) logs, the study guide states: "When configured, upstream devices complete UTM logging."

In the illustrated example, it further clarifies the role split: "All traffic from Client-1 is first received by FGT-B, which creates traffic logs for the initial session [then] forwarded to FGT-A [and] FGT-A applies web filtering and generates the relevant UTM logs as necessary."

Because web filter profiles are configured to log only violations, web filter (UTM) logs will be generated only when a violation is detected—and per the study guide behavior, that UTM logging is done by the upstream FortiGate (FGT-A). Therefore, only FGT-A will create web filter logs if it detects a violation (Option D)

NEW QUESTION 33

You created a playbook on FortiAnalyzer that uses a FortiOS connector. When you configure FortiGate, which type of trigger must you use so that the actions in an automation stitch are available in the FortiOS connector? (Choose one answer)

- A. FortiAnalyzer Event Handler
- B. Incoming webhook
- C. Fabric Connector event
- D. IP ban

Answer: B

Explanation:

From Exact Extract of knowledge of FortiAnalyzer 7.6 Study guide documents:

The study guide explains that FortiAnalyzer playbook tasks rely on connectors, and that the FortiOS connector will not show its available actions until FortiGate is configured with the correct automation trigger. The guide states: "For example, the FortiOS connector will be listed as soon as the first FortiGate device is added to FortiAnalyzer. However, to see the actions related to that FortiOS connector, you must enable an automation rule using the Incoming Webhook Call trigger on FortiGate."

This is why the required FortiGate trigger type is Incoming webhook (option B): it is the specific trigger FortiOS must use so FortiAnalyzer can expose and use the FortiOS connector actions within the playbook workflow.

NEW QUESTION 36

What two things should an administrator do to view Compromised Hosts on FortiAnalyzer? (Choose two.)

- Enable web filtering in firewall policies on FortiGate devices, and make sure these logs are sent to FortiAnalyzer.
- A. Enable device detection on an interface on the FortiGate devices that are connected to the FortiAnalyzer.
- B. Subscribe FortiAnalyzer to FortiGuard to keep its local threat database up-to-date.
- C. Make sure all endpoints are reachable by FortiAnalyzer.
- D.

Answer: AC

NEW QUESTION 41

A FortiAnalyzer device could use which security method to secure the transfer of log data from FortiGate devices?

- A. SSL
- B. IPSec
- C. Direct serial connection
- D. S/MIME

Answer: B

NEW QUESTION 45

.....

Relate Links

100% Pass Your FCP_FAZ_AN-7.6 Exam with ExamBible Prep Materials

https://www.exambible.com/FCP_FAZ_AN-7.6-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/>