Fortinet

Exam Questions FCP_FAZ_AN-7.6

Fortinet NSE 5 - FortiAnalyzer 7.6 Analyst

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
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 3
Aplaybook 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. Attention required
B. Upstream_failed
C. Failed
D. Success

Answer: A

Explanation:
In FortiAnalyzer, when a playbook is run, each task??s status impacts the overall playbook status. Here??s what happens based on task outcomes:
* Status When All Tasks Succeed:
* If all tasks finish successfully, the playbook status ismarked asSuccess.
* Status When Some Tasks Fail:
* If one or more tasks in the playbook fail, but others succeed, the playbook status generally changes toAttention required. This status indicates that the playbook completed execution but requires review due to one or more tasks failing.
* This is different from a completeFailedstatus, which is used if the playbook cannot proceed due to a critical error in an early task, often one that upstream tasks depend on.
* Option Analysis:
* A. Attention required: This is correct as the playbook has completed, but with partial success and a task requiring review.
* B. Upstream_failed: This status is used if a task cannot run because a prerequisite or "upstream" task failed. Since four out of five tasks completed, this is not the case here.
* C. Failed: This status would imply that the playbook completely failed, which does not match the scenario where only one task out of five failed.
* D. Success: This status would apply if all tasks had completed successfully, which is not the case here.
Conclusion:
* Correct Answer A. Attention required
* The playbook status reflects that it completed, but an error occurred in one of the tasks, prompting the administrator to review the failed task.
References:
FortiAnalyzer 7.4.1documentation on playbook execution statuses and task error handling.

NEW QUESTION 4
Which FortiAnalyzer feature allows you to use a proactive approach when managing your network security?

A. FortiView Monitor
B. Outbreak alert services
C. Incidentsdashboard
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.Conclusion:
* Correct Answer D. Threat hunting
* Threat hunting is the most proactive feature among the options, as it involves actively searching for threatswithin the network rather than reacting to already detected incidents.
References:
FortiAnalyzer 7.4.1 documentation on Threat Hunting and proactive security measures.

NEW QUESTION 5
You find that as part of your role as an analyst, you frequently search log View using the same parameters. Instead of defining your search filters repeatedly, what can you do to save time?

A. Configure a custom dashboard.
B. Configure a custom view.
C. Configure a data selector.
D. Configure a marco and apply it to device groups.

Answer: B

Explanation:
When you frequently use the same search parameters in FortiAnalyzer??s Log View, setting up a reusable filter or view can saveconsiderable time. Here??s an analysis of each option:
* Option A - Configure a Custom Dashboard:
* Custom dashboards are useful for displaying a variety of widgets and summaries on network activity, performance, and threat data, but they are not designed for storing specific search filters for log views.
* Conclusion:Incorrect.
* Option B - Configure a Custom View:
* Custom views in FortiAnalyzer allow analysts to save specific search filters and configurations.
By setting up a custom view, you can retain your frequently used search parameters and quickly access them without needing to reapply filters each time. This option is specifically designed to streamline the process of recurring log searches.
* Conclusion:Correct.
* Option C - Configure a Data Selector:
* Data selectors are used to define specific types of data for FortiAnalyzer reports and widgets.
They are useful in reports but are not meant for saving and reusing log search parameters in Log View.
* Conclusion:Incorrect.
* Option D - Configure a Macro and Apply It to Device Groups:
* Macros in FortiAnalyzer are generally used for automation tasks, not for saving log search filters.
Applying macros to device groups does not fulfill the requirement of saving specific log view search parameters.
* Conclusion:Incorrect.
Conclusion:
* Correct Answer B. Configure a custom view.
Custom views allow you to save specific search filters, enabling quick access to frequently used parameters in Log View.
References:
FortiAnalyzer 7.4.1 documentation on creating and using custom views for log searches.

NEW QUESTION 6
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, theEvent Statusshown isUnhandled(Event Type: Web Filter; Severity: Critical). The FortiAnalyzer study guide definesUnhandledevents 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 7
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 8
Exhibit.

```
FAZ # diagnose log device
Device Name        Device ID          Used Space(logs / quarantine / content / IPS) Allocated Space  Used%
FGT-A              [illegible]        532.0KB( 532.0KB/   0.0KB/   0.0KB/   0.0KB) unlimited     n/a
FGT-B              [illegible]        600.7MB( 600.7MB/   0.0KB/   0.0KB/   0.0KB) unlimited     n/a
FGT-C              [illegible]          1.2MB(   1.2MB/   0.0KB/   0.0KB/   0.0KB) unlimited     n/a
Total: 3 log devices, used=602.3MB quota=unlimited

AdomName     AdomOID  Type                       Logs                                                                  Database
                           [Retention  Quota     Used(    logs/quaranti/ content/    IPS) Used%]  [Retention  Quota   Used(   SizeDB/   hcache) Used%]
ADOM1        [illegible] FGT  1000days  900.0MB  601.3MB( 601.0MB/  0.0KB/   0.0KB/   0.0KB) 66.8%    1000days   2.1GB   1.9GB(  67.9MB/  17.9KB) 92.4%
```

What can you conclude from this output?

A. There is not disk quota allocated to quarantining files.
B. FGT_B is the Security Fabric root.
C. The allocated disk quote to ADOM1 is 3 GB.
D. Archive logs are using more space than analytic logs.

Answer: B

NEW QUESTION 9
In a FortiAnalyzer Fabric deployment, which three modules from Fabric members are available for analysis on the supervisor? (Choose three answers))

A. Playbooks
B. Indicators
C. Logs
D. Events
E. Reports

Answer: CDE

Explanation:
From Exact Extract of knowledge of FortiAnalyzer 7.6 Study guide documents:
The study guide explicitly describes what content fromFabric membersis visible/usable on theFabric supervisor:
* Logs:??In the FortiAnalyzer Fabric supervisor,Log View displays logs collected on all FortiAnalyzer Fabric members.??
* Reports:??For reports, the FortiAnalyzer Fabric supervisorcan fetch and aggregate data from multiple membersin the FortiAnalyzer Fabric.??
* Events:??Events generated by event handlers on the FortiAnalyzer Fabric members are visible on the supervisor.??
By contrast, the study guide lists a key limitation that rules outPlaybooksas a supervisor capability over members: ??You are not able to perform configuration changes or torun automation playbooks from the Fabric supervisor to members.??
Therefore, the three modules available for analysis on the supervisor areLogs, Events, and Reports(C, D, E).

NEW QUESTION 10
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.

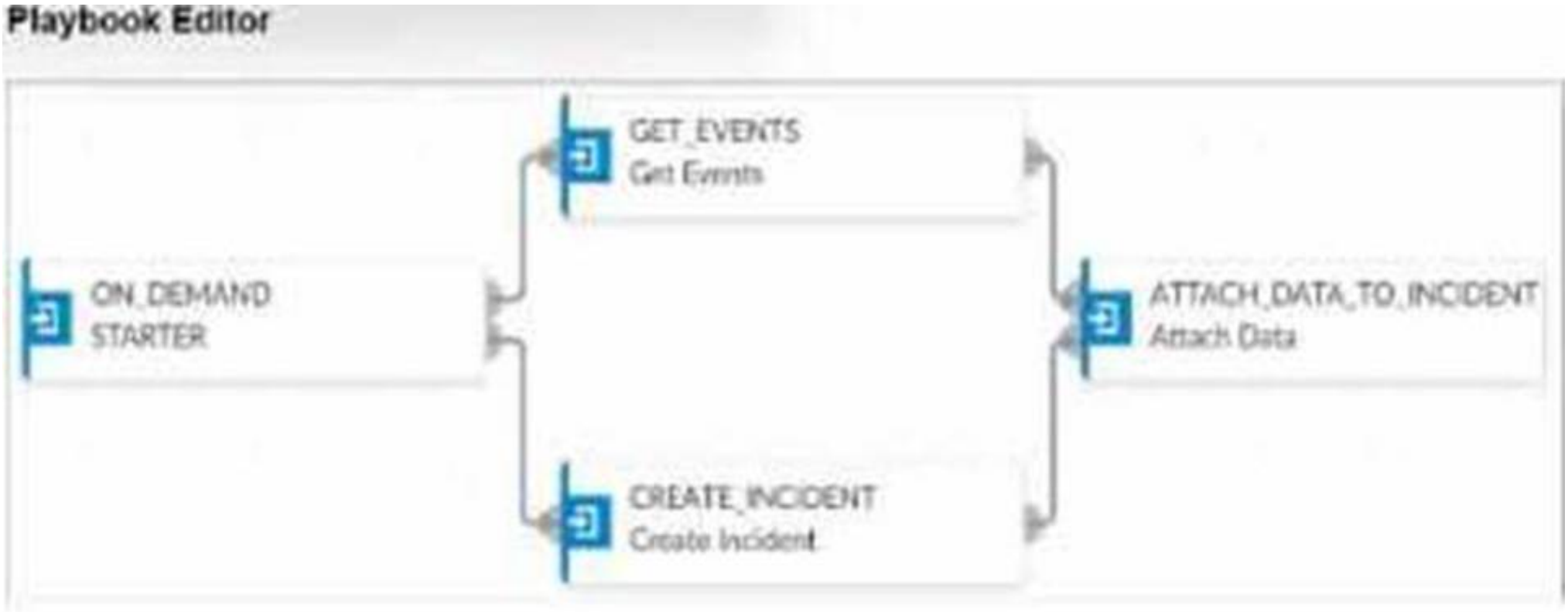
NEW QUESTION 10
(An analyst is using FortiAI on FortiAnalyzer to simplify certain tasks but is worried about exceeding the monthly token limit. Which query will take the fewest FortiAI tokens? (Choose one answer))

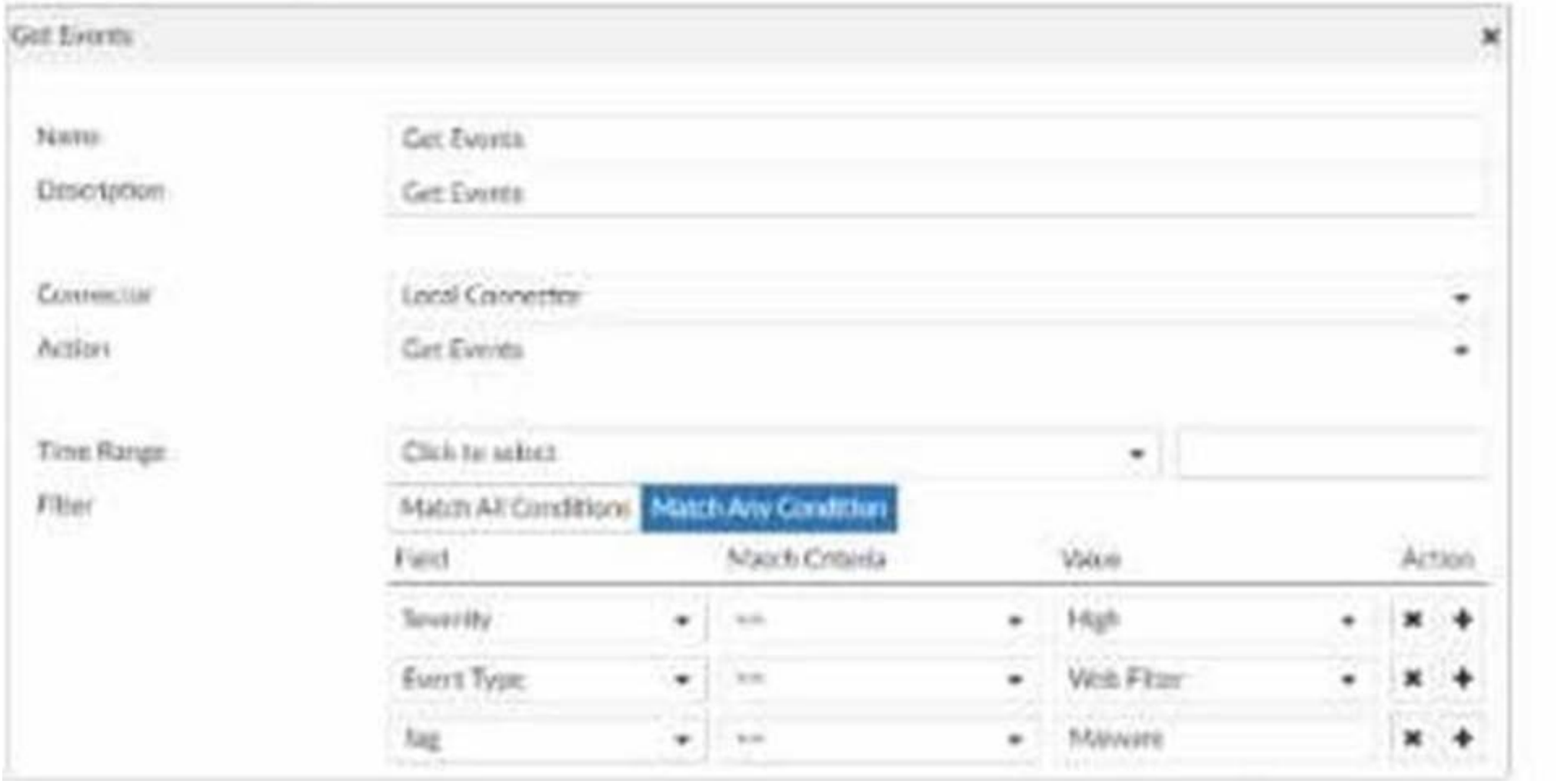
A. Show logs for 192.168.1.10 (past week)
B. Show all logs from the past week
C. Can you show me all the log entries for the endpoint 192.168.1.10?
D. Show logs for 192.168.1.10

Answer: A

Explanation:
From Exact Extract of knowledge of FortiAnalyzer 7.6 Study guide documents:
The study guide explains that FortiAI token usage includesboth the prompt (input) and the response (output), and that ??generally, more text in the query and response results in using more tokens.?? It provides two comparison examples and concludes that the more verbose request for ??all the log entries?? consumes more tokens because it hasmore textand also triggers alarger response; whereas limiting the query to a time range (for example, ??(past week)??) reduces output volume and therefore token usage.
Applying that guidance to the options:
* Cis the most verbose and explicitly requests ??all the log entries,?? which drives higher input and output token usage.
* Brequests ??all logs?? for the week (broad scope), which typically increases output tokens.
* Dis short, but it doesnotconstrain the time range, which can increase the response size (output tokens).
* Ais concise and includes a time constraint ??(past week),?? matching the study guide??s example of a lower-token query pattern.

NEW QUESTION 14
Exhibit.





Assume these are all the events that exist on the FortiAnalyzer device.
How many events will be added to the incident created after running this playbook?

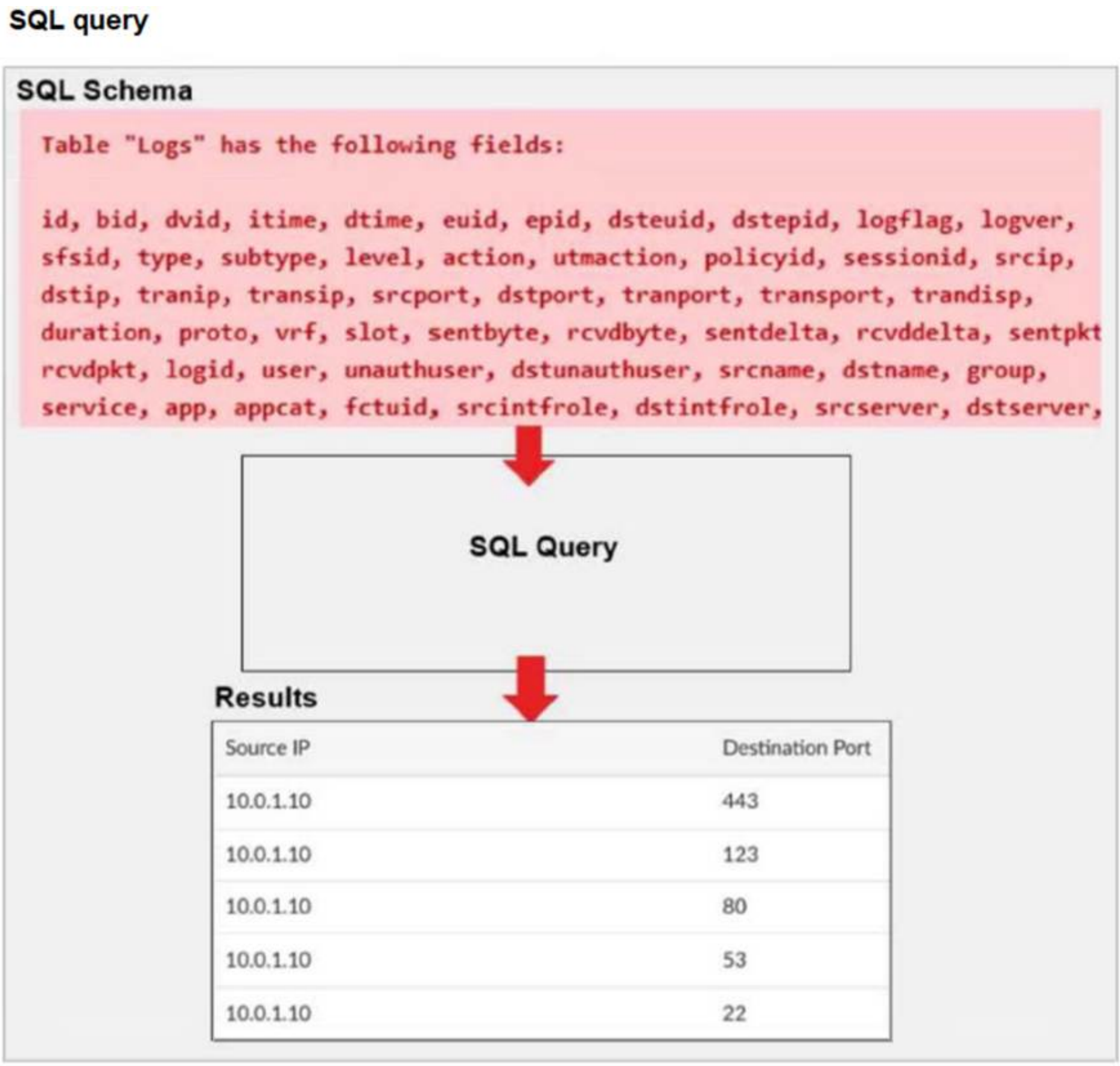
A. Eleven events will be added.

B. Seven events will beadded
C. No events will be added.
D. Four events will be added.

Answer: D

Explanation:
In the exhibit, we see a playbook in FortiAnalyzer designed to retrieve events based on specific criteria, create an incident, and attach relevant data to that incident. The "Get Event" task configuration specifies filters to match any of the following conditions:
Severity= High
Event Type= Web Filter
Tag= Malware
Analysis of Events:
In the FortiAnalyzer Event Monitor list:
We need to identify events that meet any one of the specified conditions (since the filter is set to "Match Any Condition").
Events Matching Criteria:
Severity = High:
There are two events with "High" severity, both with the "Event Type" IPS.
Event Type = Web Filter:
There are two events with the "Event Type" Web Filter. One has a "Medium" severity, and the other has a "Low" severity.
Tag = Malware:
There are two events tagged with "Malware," both with the "Event Type" Antivirus and "Medium" severity.
After filtering based on these criteria, there arefour distinct events:
Two from the "Severity = High" filter.
One from the "Event Type = Web Filter" filter.
One from the "Tag = Malware" filter.
Conclusion:
Correct Answer:D. Four events will be added.
This answer matches the conditions set in the playbook filter configuration and the events listed in the Event Monitor.
[References:, FortiAnalyzer 7.4.1 documentation on event filtering, playbook configuration, and incident management criteria.,]

NEW QUESTION 15
Exhibit.



A fortiAnalyzer analyst is customizing a SQL query to use in a report.
Which SQL query should the analyst run to get the expected results?
A)SELECT srcip AS "Source IP", dstport AS "Destination Port" FROM $log - WHERE $filter AND srcip = '10.0.1.10' GROUP BY srcip, dstport - ORDER BY dstport DESC

```
SELECT srcip AS "Source IP", dstport AS "Destination Port"
FROM $log
WHERE $filter AND srcip = '10.0.1.10'
ORDER BY dstport
GROUP by srcip, dstport DESC
```

B)SELECT srcip AS "Source IP", dstport AS "Destination Port" FROM $log - WHERE $filter AND Source IP != '10.0.1.10' GROUP BY srcip, dstport - ORDER BY dstport DESC

```
SELECT srcip AS "Source IP", dstport AS "Destination Port"
FROM $log
WHERE $filter AND Source IP != '10.0.1.10'
GROUP BY srcip, dstport
ORDER BY dstport DESC
```

C)SELECT srcip AS "Source IP", dstport AS "Destination Port" ORDER BY dstport DESC - GROUP BY srcip, dstport - FROM $log - WHERE $filter AND srcip = '10.0.1.10'

```
SELECT srcip AS "Source IP", dstport AS "Destination Port"
ORDER BY dstport DESC
GROUP BY srcip, dstport
FROM $log
WHERE $filter AND srcip = '10.0.1.10'
```

D)SELECT srcip AS "Source IP", dstport AS "Destination Port" FROM $log - WHERE $filter AND srcip = '10.0.1.10' ORDER BY dstport - GROUP by srcip, dstport DESC

```
SELECT srcip AS "Source IP", dstport AS "Destination Port"
FROM $log
WHERE $filter AND srcip = '10.0.1.10'
GROUP BY srcip, dstport
ORDER BY dstport DESC
```

A. Option A
B. Option B
C. Option C
D. Option D

Answer: A

Explanation:
The requirement here is to construct a SQL query that retrieves logs with specific fields, namely "Source IP" and "Destination Port," for entries where the source IP address matches 10.0.1.10. The correct syntax is essential forselecting, filtering, ordering, and grouping the results as shown in the expected outcome.
Analysis of the Options:
Option A Explanation:
SELECT srcip AS "Source IP", dstport AS "Destination Port": This syntax selects srcip and dstport, renaming them to "Source IP" and "Destination Port" respectively in the output.
FROM $log: Specifies the log table as the data source.
WHERE $filter AND srcip = '10.0.1.10': This line filters logs to only include entries with srcip equal to 10.0.1.10.
ORDER BY dstportDESC: Orders the results in descending order by dstport.
GROUP BY srcip, dstport: Groups results by srcip and dstport, which is valid SQL syntax.
This option meets all the requirements to get the expected results accurately.
Option B Explanation:
WHERE $filter AND Source IP != '10.0.1.10': Uses != instead of =. This would exclude logs from the specified IP 10.0.1.10, which is contrary to the expected result.
Option C Explanation:
The ORDER BY clause appears before the FROM clause, which is incorrect syntax. SQL requires the FROM clause to follow the SELECT clause directly.
Option D Explanation:
The GROUP BY clause should follow the FROM clause. However, here, it??s located after WHERE, making it syntactically incorrect.
Conclusion:
Correct Answer A. Option A
This option aligns perfectly with standard SQL syntax and filters correctly for srcip = '10.0.1.10', while ordering and grouping as required.
[References:, FortiAnalyzer 7.4.1 SQL query capabilities and syntax for report customization.,]

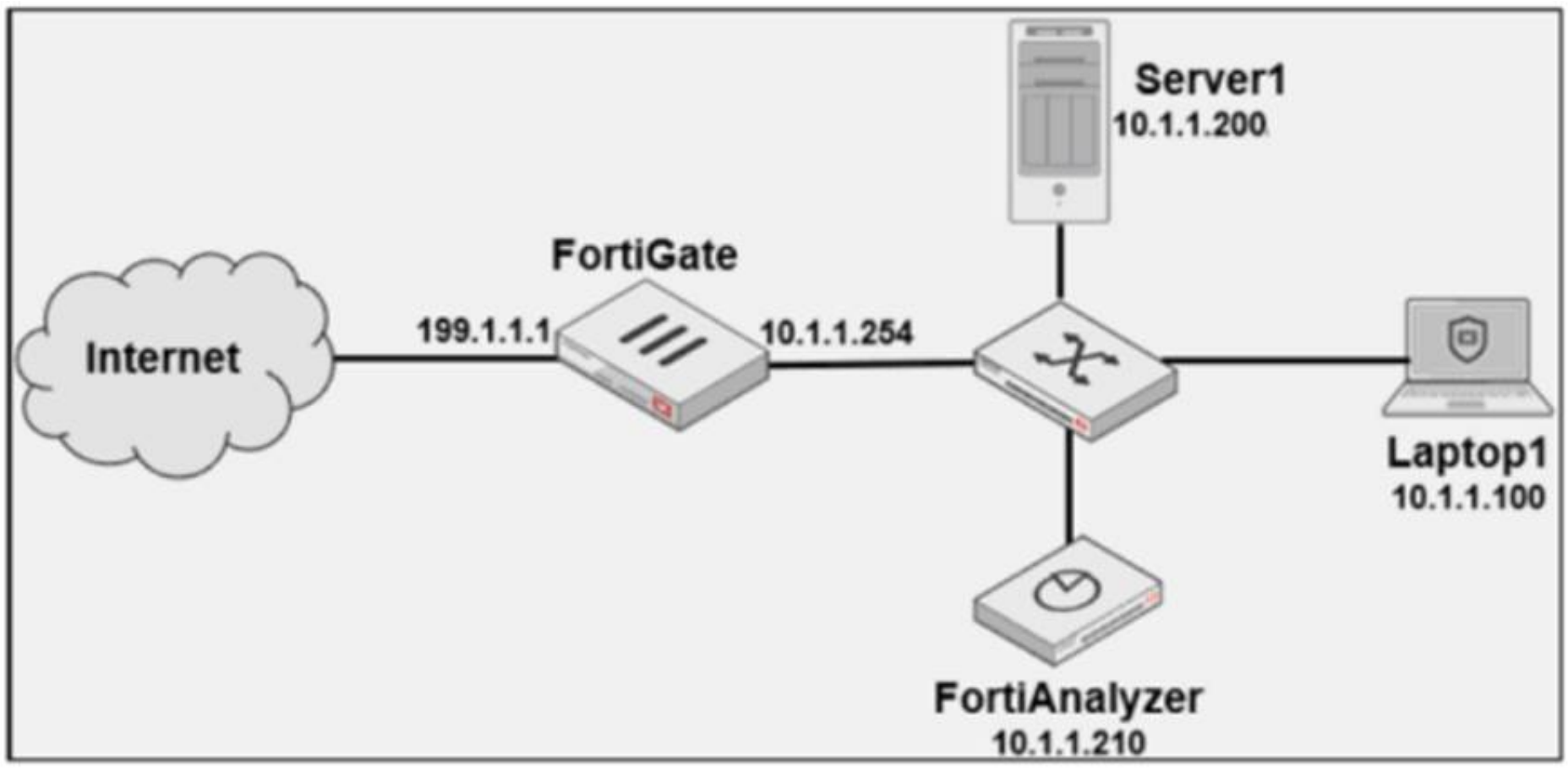
NEW QUESTION 18
In firmware version 7.6, how does on-premises FortiAnalyzer store logs? (Choose one answer)

A. Uses ClickHouse database
B. Uses MySQL database
C. Uses Postgres SQL database
D. Uses ElasticSeach database

Answer: A

Explanation:
Comprehensive and Detailed Explanation From Exact Extract of knowledge of FortiAnalyzer 7.6 Study guide documents:
FortiAnalyzer 7.6 stores on-premises logs in aClickHouse SQL database(not MySQL, Postgres, or Elasticsearch). Fortinet??s FortiAnalyzer 7.6 SQL Query documentation explicitly states that log data is inserted into the SQL database and that "FortiAnalyzer uses a ClickHouse SQL database."
This is consistent with how the study guide describes the storage/analytics pipeline in 7.6: it explains that FortiAnalyzer indexes incoming raw logs (insert rate)"by the SQL database and the sqlplugind daemon." This "SQL database" in 7.6 corresponds to the ClickHouse-backed log database described in the Fortinet documentation.

NEW QUESTION 22
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 anddstip==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 fromLaptop1(IP 10.1.1.100) and excludes the admin user. This filter should match any user other than admin.
Filter Components Analysis:
Operation-login: This portion of the filter will target login actions specifically, which is correct for filtering login attempts.
performed_on=="GUI(10.1.1.100)': This indicates that the login attempt must occur on the GUI interface and originate from the specified IP, which matches Laptop1's IP address (10.1.1.100). This ensures that the filter only matches GUI logins from this specific device.
user!=admin: This part excludes logins by the admin user, meeting the requirement to capture only non-admin users.
Option Analysis:
Option A: Correctly specifies theOperation-login,performed_on=="GUI(10.1.1.100)', anduser!=admin. This setup effectively filters login attempts to the GUI from Laptop1, excluding the admin user.
Option B: Uses the incorrect IP 10.1.1.120 in the performed_on filter, which does not match Laptop1's IP (10.1.1.100).
Option C: This option includessrcip==10.1.1.100anddstip==10.1.1.210but incorrectly specifiesuser==admininstead ofuser!=admin, which does not match the requirement to exclude admin users.
Option D: This option does not specify theperformed_onfield to restrict it to the GUI and only includesdstip(destination IP) withoutsrcip. It also incorrectly uses user!-admin instead of the correct syntaxuser!=admin.
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 27
Refer to the exhibit.

```
adom_oid=198 itime=2025-05-27 08:35:24 loguid=7509149554218893312 epid=3 euid=3 data_parsername=FortiGate Log Parser data_sourceid=FGVM02TM24013423
data_sourcename=HQ-NGFW-1 root data_sourcetype=FortiGate data_timestamp=1748334923 app_cat=unscanned app_name=NTP app_service=NTP dst_intf=port2(undefined)
dst_ip=208.91.112.63 dst_port=123 event_action=accept event_id=13 event_policy=3 event_ref=751261e0-ce9e-51ef-f12e-a382acaf16d6 event_severity=notice
event_subtype=forward event_type=traffic host_location=Reserved host_owner=fortinet.com net_proto=17 net_rcvdpkts=1 net_rcvbytes=76 net_sentbytes=76 net_sentpkts=1
net_sessionduration=180 net_sessionid=1357 src_intf=port6(undefined) src_ip=10.0.13.125 src_natip=100.65.0.101 src_natport=50403 src_port=50403 dstepid=101 dsteuid=3
dst_geo_country=United States event_creation_time=27800868 event_uuid=0000000013 src_geo_country=Reserved logflag=1 data_sourcedom=root dst_intf_role=undefined
event_policyid=3 event_policytype=policy src_intf_role=undefined itime_t=1748360124 _logMeta=undefined
```

Which two observations can you make after reviewing this log entry? (Choose two answers))

A. This is a normalized log.
B. This is a formatted view of the log.
C. This is the original log that FortiAnalyzer received from FortiGate.
D. This log is in a raw log format.

Answer: AD

Explanation:
Comprehensive and Detailed Explanation From Exact Extract of knowledge of FortiAnalyzer 7.6 Study guide documents:
The exhibit shows the log as a single-line key/value entry (not a columnar/table display), which aligns with FortiAnalyzer'sraw log formatview option. The study guide states:"You can toggle between viewing formatted and raw logs."This directly supports observationD.
At the same time, what you are viewing in FortiAnalyzer Log View isnormalizeddata (FortiAnalyzer parses and maps device logs into standardized fields for consistent searching and analysis). The study guide explicitly states:"The log view allows you to view all log types received by FortiAnalyzer in normalized log

format.??It also explains that FortiAnalyzer "uses predefined parsers to extract key fields from ingested logs and maps them to a consistent, standardized set of field names," then stores them as normalized logs in the SIEM database. This supports observationA.
Finally, the study guide clarifies that even when you switch to raw log format in FortiAnalyzer, you are still observing the normalized-field representation produced by FortiAnalyzer's parser/normalization process (rather than the untouched original device message). It notes that a FortiGate event log "has been normalized by FortiAnalyzer," and when you switch "to raw log format," you can observe the effect of normalization on common fields. This is whyCis not the best description for the exhibit.

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 thenormal 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 32
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, ifno matching parserexists for a given device log, FortiAnalyzer can stillstore 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 optionC.

NEW QUESTION 36
Which two statements about FortiAnalyzer Fabric deployments are true? (Choose two answers)

A. Supervisors can be in high availability (HA) for redundancy purposes only.
B. Fabric members can operate in analyzer mode only.
C. Fabric members do not forward their logs to the supervisor.
D. Supervisors and members must be in the same time zone.

Answer: BC

Explanation:

From Exact Extract of knowledge of FortiAnalyzer 7.6 Study guide documents:
B is true (members operate in analyzer mode, not collector mode): The study guide defines Fabric members as FortiAnalyzer devices that "retain access to the features described in the FortiAnalyzer Administration Guide" and that "each member can create or raise incidents and events." In contrast, it states that a FortiAnalyzer operating in collector mode "does not provide capabilities for event management or reporting," and also notes that "in collector mode, the GUI doesn't include FortiView, Reports, or Incidents & Events." Since Fabric members must be able to generate/manage incidents and events, they must be operating with analyzer capabilities rather than collector-only functionality.
C is true (members do not forward their logs to the supervisor): The supervisor provides centralized visibility, but the study guide describes the supervisor's log access as viewing logs collected on members, not receiving/storing forwarded log files. It states: "In the FortiAnalyzer Fabric supervisor, Log View displays logs collected on all FortiAnalyzer Fabric members," and clarifies "the logs contain the same information as displayed in the host FortiAnalyzer device they were collected on." This indicates the logs remain on the member (host) and are made visible to the supervisor for centralized monitoring rather than being forwarded and stored on the supervisor.
For completeness, the study guide also explicitly states "HA is not available on the supervisor" (so A is false) and members do not need the same time zone as the supervisor (so D is false).

NEW QUESTION 38
Which statement regarding macros on FortiAnalyzer is true?
A. Macros are predefined templates for reports and cannot be customized.
B. Macros are useful in generating excel log files automatically based on the report settings.
C. Macros are ADOM-specific and each ADOM type have unique macros relevant to that ADOM.
D. Macros are supported only on the FortiGate ADOMs.

A.

Answer: B

Explanation:
Macros in FortiAnalyzer are used to streamline reporting tasks by automating data extraction and report generation. Here's a breakdown of each option to determine the correct answer:
Option A - Macros are Predefined Templates for Reports and Cannot be Customized:
This statement is incorrect. Macros in FortiAnalyzer are not simply fixed templates; they allow for customization to tailor data extraction and reporting based on specific needs and configurations.
Conclusion: Incorrect.
Option B - Macros are Useful in Generating Excel Log Files Automatically Based on the Report Settings:
This statement is accurate. Macros in FortiAnalyzer can be configured to automate the generation of reports, including outputting log data to Excel format based on predefined report settings. This makes them especially useful for scheduled reporting and data analysis.
Conclusion: Correct.
Option C - Macros are ADOM-Specific and Each ADOM Type Has Unique Macros Relevant to that ADOM:
Macros are not limited to specific ADOMs, nor are they ADOM-specific. Macros can be applied across various ADOMs based on report configurations but are not inherently tied to or unique for each ADOM type.
Conclusion: Incorrect.
Option D - Macros are Supported Only on the FortiGate ADOMs:
This is not true. Macros in FortiAnalyzer are not restricted to FortiGate ADOMs; they can be utilized across different ADOMs that FortiAnalyzer manages.
Conclusion: Incorrect.Conclusion:
Correct Answer B. Macros are useful in generating excel log files automatically based on the report settings.
This answer correctly describes the functionality of macros in FortiAnalyzer, emphasizing their role in automating report generation, especially for Excel log files.
FortiAnalyzer 7.4.1 documentation on macros and report generation functionalities.

NEW QUESTION 39
Exhibit.

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

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

Answer: AD

NEW QUESTION 42
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 V
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
This is incorrect. FortiSOAR operates independently of FortiManager. While FortiSOAR can receive input or data from FortiGate (often managed by FortiManager), it does not require FortiManager to be part of its setup.
Option B: It runs as a docker container on FortiAnalyzer
This is incorrect. FortiSOAR does not run as a container within FortiAnalyzer. It requires its own dedicated environment, either as a physical device or a virtual machine, due to the resource requirements and specialized functions it performs.
Option C: It requires a dedicated FortiSOAR device or VM
This is correct. FortiSOAR is deployed as a standalone device or VM, which enables it to handle the intensive processing needed for orchestrating security operations, integrating with third-party tools, and automating responses across an organization's security infrastructure.
Option D: It does not include a limited trial by default
This is incorrect. FortiSOAR installations may come with trial options or demos in specific scenarios, especially for evaluation purposes. This depends on licensing and deployment policies.
Reference: 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 44
Exhibit.

FortiAnalyzer partial configuration output

```
FortiAnalyzer1# get system status
Platform Type                : FAZVM64-KVM
Platform Full Name           : FortiAnalyzer-VM64-KVM
Version                      : v7.4.1-build2308 230831 (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                 : 2308
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

FortiAnalyzer1# get system global
adom-mode                    : normal
adom-select                  : enable
adom-status                  : enable
console-output               : standard
country-flag                 : enable
enc-algorithm                : high
ha-member-auto-grouping      : enable
hostname                     : FortiAnalyzer1
log-checksum                 : md5
log-forward-cache-size       : 5
log-mode                     : analyzer
longitude                    : (null)
max-aggregation-tasks        : 0
max-running-reports          : 1
oftp-ssl-protocol            : tlsv1.2
ssl-low-encryption           : disable
ssl-protocol                 : tlsv1.3 tlsv1.2
task-list-size               : 2000
webservice-proto             : tlsv1.3 tlsv1.2
```

```
FortiAnalyzer2# get system status
Platform Type                : FAZVM64-KVM
Platform Full Name           : FortiAnalyzer-VM64-KVM
Version                      : v7.4.1-build2308 230831 (GA)
Serial Number                : FAZ-VM0000065041
BIOS version                 : 04000002
Hostname                     : FortiAnalyzer2
Max Number of Admin Domains  : 5
Admin Domain Configuration   : Enabled
FIPS Mode                    : Disabled
HA Mode                      : Stand Alone
Branch Point                 : 2308
Release Version Information  : GA
Time Zone                    : (GMT-8:00) Pacific Time (US & Canada)
Disk Usage                   : Free 45.75GB, Total 58.80GB
File System                  : Ext4
License Status               : Valid

FortiAnalyzer2# get system global
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            : tlsv1.2
ssl-low-encryption           : disable
ssl-protocol                 : tlsv1.3 tlsv1.2
task-list-size               : 2000
webservice-proto             : tlsv1.3 tlsv1.2
```

```
FortiAnalyzer3# get syste
Platform Type
Platform Full Name
Version                      : v7.4.1-build2308 230831 (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                 : 2308
Release Version Information  : GA
Time Zone                    : (GMT-8:00) Pacific Time (US & Canada)
Disk Usage                   : Free 53.06GB, Total 79.80GB
File System                  : Ext4
License Status               : Valid

FortiAnalyzer3# get system global
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            : tlsv1.2
ssl-low-encryption           : disable
ssl-protocol                 : tlsv1.3 tlsv1.2
task-list-size               : 2000
webservice-proto             : tlsv1.3 tlsv1.2
```

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

A. FortiAnalayzer1 and FortiAnalyzer3
B. FortiAnalyzer1 and FortiAnalyzer2
C. FortiAnalyzer2 and FortiAnalyzer3
D. All devices listed can be members.

Answer: D

Explanation:
In a FortiAnalyzer Fabric, devices can participate in a cluster or grouping if they meet specific compatibility criteria.
Based on the outputs provided, let's evaluate these criteria:
Version Compatibility:
All three devices, FortiAnalyzer1, FortiAnalyzer2, and FortiAnalyzer3, are running version v7.4.1-build0238, which is the same across the board. This version alignment is crucial because FortiAnalyzer Fabric requires that devices run compatible firmware versions for seamless communication and management.
Platform Type and Configuration:
All three devices are configured as Standalone in the HA mode, which allows them to operate independently but does not restrict their participation in a FortiAnalyzer Fabric. Each device is also on the FAZVM64-KVM platform type, ensuring hardware compatibility.
Global Settings:
Key settings such as adm-mode, adm-status, and adom-mode are consistent across all devices (adm-mode: normal, adm-status: enable, adom-mode: normal), which aligns with requirements for fabric integration and role assignment flexibility.
Each device also has the log-forward-cache-size set, which is relevant for forwarding logs within a fabric environment.
Based on the above analysis, all devices (FortiAnalyzer1, FortiAnalyzer2, and FortiAnalyzer3) meet the requirements to be part of a FortiAnalyzer Fabric.
Reference: FortiAnalyzer 7.4.1 documentation outlines that devices within a FortiAnalyzer Fabric should be on the same or compatible firmware versions and hardware platforms, and they must be configured for integration. Given that all devices match the version, platform, and mode criteria, they can all be part of the FortiAnalyzer Fabric.

NEW QUESTION 46
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 stich are available in the FortiOS connector?

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

Answer: D

Explanation:
When using FortiAnalyzer to create playbooks that interact with FortiOS devices, an Incoming Webhook trigger is required on the FortiGate side to make the actions in an automation stitch accessible through the FortiOS connector. The incoming webhook trigger allows FortiAnalyzer to initiate actions on FortiGate by sending HTTP POST requests to specified endpoints, which in turn trigger automation stitches defined on the FortiGate.
Here's an analysis of each option:
Option A: FortiAnalyzer Event Handler
This is incorrect. The FortiAnalyzer Event Handler is used within FortiAnalyzer itself for handling log events and alerts, but it does not trigger automation stitches on FortiGate.
Option B: Fabric Connector event
This is incorrect. Fabric Connector events are related to Fortinet's Security Fabric integrations but are not specifically used to trigger FortiGate automation stitches from FortiAnalyzer.
Option C: FortiOS Event Log
This is incorrect. While FortiOS event logs can be used for monitoring, they are not designed to trigger automation stitches directly from FortiAnalyzer.
Option D: Incoming webhook
This is correct. The Incoming Webhook trigger on FortiGate enables it to receive requests from FortiAnalyzer, allowing playbooks to activate automation stitches defined on the FortiGate device. This method is commonly used to integrate actions from FortiAnalyzer to FortiGate via the FortiOS connector.
Reference: According to FortiOS and FortiAnalyzer documentation, when integrating FortiAnalyzer
playbooks with FortiGate automation stitches, the recommended trigger type on FortiGate is an Incoming Webhook, allowing FortiAnalyzer to interact with FortiGate??s automation framework through the FortiOS connector.

NEW QUESTION 50
When managing incidents on FortiAnlyzer, what must an analyst be aware of?

A. You can manually attach generated reports to incidents.
B. The status of the incident is always linked to the status of the attach event.
C. Severity incidents rated with the level High have an initial service-level agreement (SLA) response time of 1 hour.
D. Incidents must be acknowledged before they can be analyzed.

Answer: A

Explanation:
In FortiAnalyzer's incident management system, analysts have the option to manually manage incidents, which includes attaching relevant reports to an incident for further investigation and documentation. This feature allows analysts to consolidate information, such as detailed reports on suspicious activity, into an incident record, providing a comprehensive view for incident response.
Let's review the other options to clarify why they are incorrect:
Option A: You can manually attach generated reports to incidents
This is correct. FortiAnalyzer allows analysts to manually attach reports to incidents, which is beneficial for providing additional context, evidence, or analysis related to the incident. This functionality is part of the incident management process and helps streamline information for tracking and resolution.
Option B: The status of the incident is always linked to the status of the attached event
This is incorrect. The status of an incident on FortiAnalyzer is managed independently of the status of any attached events. An incident can contain multiple events, each with different statuses, but the incident itself is tracked separately.
Option C: Severity incidents rated with the level High have an initial service-level agreement (SLA) response time of 1 hour
This is incorrect. While incidents have severity levels, specific SLA response times are typically set according to the organization??s incident response policy, and FortiAnalyzer does not impose a default
SLA response time of 1 hour for high-severity incidents.
Option D: Incidents must be acknowledged before they can be analyzed
This is incorrect. Incidents on FortiAnalyzer can be analyzed even if they are not yet acknowledged. Acknowledging an incident is often part of the workflow to mark it as being actively addressed, but it is not a prerequisite for analysis.
Reference: According to FortiAnalyzer documentation, analysts can attach reports to incidents manually, making option A correct. This feature enables better tracking and documentation within the incident management system on FortiAnalyzer.

NEW QUESTION 52
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 53
You are trying to configure a task in the playbook editor to run a report.
However, when you try to select the desired playbook, you do to see it listed.
What is the reason?

A. The report does not have auto-cache and extended log filtering enabled.
B. The playbook is currently running and will be available after it is finished.
C. You must create a trigger to run the report first.
D. The report has no result and must be reconfigured.

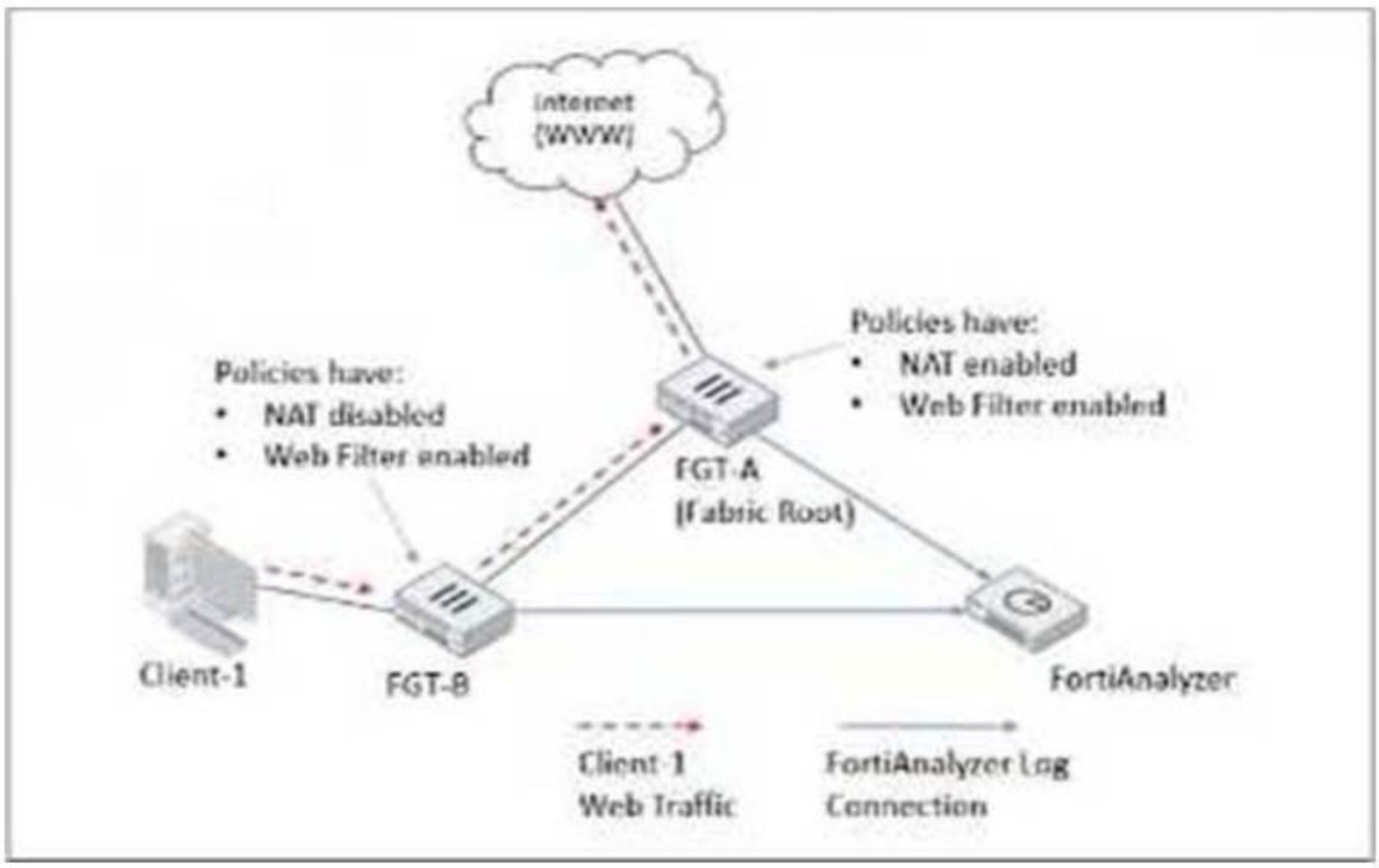
Answer: C

NEW QUESTION 58
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 appliedsimultaneously to all event handlers.

Answer: C

NEW QUESTION 62
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 duplicatedacross 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 tolog 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 theupstreamFortiGate (FGT-A). Therefore,only FGT-A will create web filter logs if it detects a violation(Option D)

NEW QUESTION 65
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 isIncoming 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 66
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 bedeleted.
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:
FortiAnalyzer maintains an audit history log that records changes to incidents, including updates to their status. When an incident status is marked as "Closed: False Positive," this action is logged in the audit history to ensure traceability of changes. This log provides accountability and a record of how incidents have been handled over time.
Conclusion:Correct.
Option B - The Corresponding Event Will Be Marked as Mitigated:
Changing an incident to "Closed: False Positive" does not affect the status of the original event itself. Marking an incident as a false positive signifies that it does not represent a real threat, but it
does not imply that the event has been mitigated.
Conclusion:Incorrect.
Option C - The Incident Will Be Deleted:
Marking an incident as "Closed: False Positive" does not delete the incident from FortiAnalyzer.
Instead, it updates the status to reflect that it is not a real threat, allowing for historical analysis or by a different administrative action.
Conclusion:Incorrect.
Option D - The Incident Number Will Be Changed:
The incident number is a unique identifier and does not change when thestatus of the incident is updated. This identifier remains constant throughout the incident's lifecycle for tracking and reference purposes.
Conclusion:Incorrect.
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 68
What two things should an administrator do to view Compromised Hosts on FortiAnalyzer? (Choose two.)

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

Answer: AC

NEW QUESTION 72

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 76
.....

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-7.6 Practice Exam Features:

* FCP_FAZ_AN-7.6 Questions and Answers Updated Frequently

* FCP_FAZ_AN-7.6 Practice Questions Verified by Expert Senior Certified Staff

* FCP_FAZ_AN-7.6 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* FCP_FAZ_AN-7.6 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year