Exam Questions FCP_FAZ_AN-7.6

Fortinet NSE 5 - FortiAnalyzer 7.6 Analyst

https://www.2passeasy.com/dumps/FCP_FAZ_AN-7.6/

NEW QUESTION 1
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 2
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 3
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 4
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 5
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 6
Which two statements about playbook execution are true? (Choose two)

A. FortiAnalyzer will not commit changes made by a Failed playbook
B. The Playbook Monitor provides troubleshooting logs
C. You can run the default debugging playbook to investigate playbook errors.
D. Even I the playbook status is Failed, individual tasks may have succeeded.

Answer: AB

NEW QUESTION 7
(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 8
Whathappens 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 9
Refer to the exhibit with partial output:

```
{
    "checksum": {
        "hash": "c7e559a2e328cab00b72aac1cccccc1ca",
        "method": "MD5"
    },
    "data":
    "H4sIAAAAAAAAA72ZbW/bORKAv9+vEIz7sAvQgd78RmA/uHbaRm1
    ZMiS5qbfIf78hpbEpmpL17u1hkYVtzQyHM8Ph6OkPo7eN/f0qTb/
    EIy9nRRElj/1Dj+JPxX7L4OtD7+7Wm1+/n97OH3rkoZduiyhNSrm
    CTMzWRfn15eUFvhd+/pWb/kPRqeScCVcqDdqmV4hCsTL4EbCnNAY
    nupbvrevh5VkTNxhYE2ZPmCkcTPxN6fcbVhiX31hS5OL3w37e3c2
```

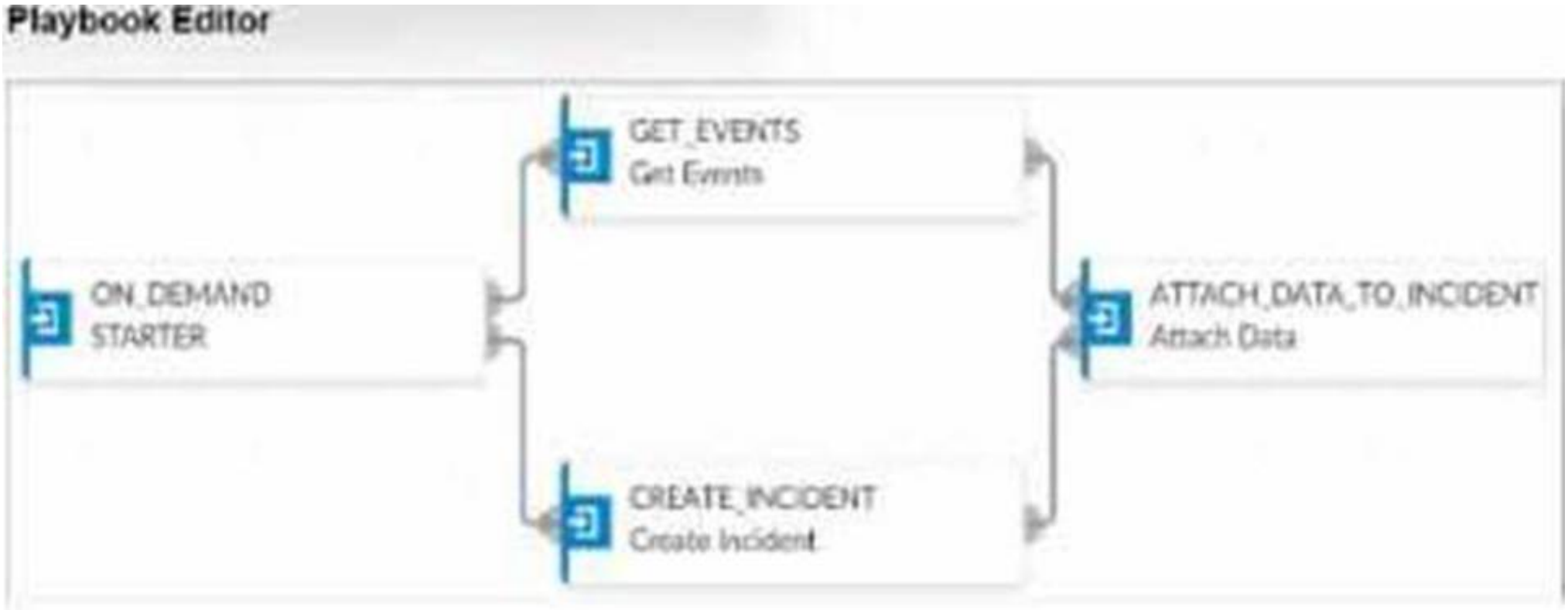
Your colleague exported a playbook and has sent it to you for review. You open the file in a text editor and observer the output as shown in the exhibit.
Which statement about the export is true?

A. The export data type is zipped.
B. The playbook is misconfigured.
C. The option to include the connector was not selected.
D. Your colleague put a password on the export.

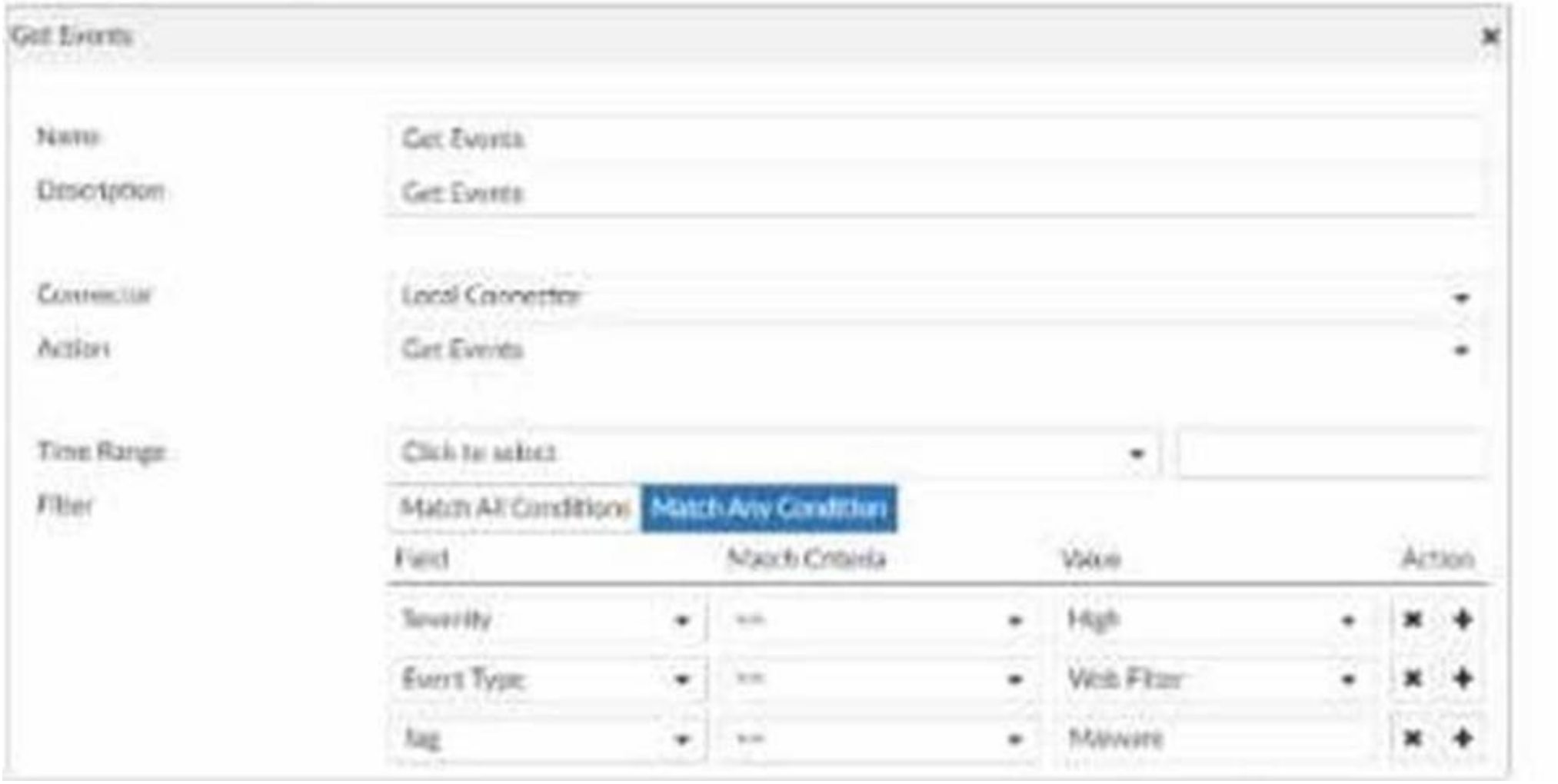
Answer: A

Explanation:
In the exhibit, the data structure shows a checksum field and a data field with a long, seemingly encoded string. This format is indicative of a file that has been compressed or encoded for storage and transfer.
Export Data Type:
The data field is likely a base64-encoded string, which is commonly used to represent binary data in text format. Base64 encoding is often applied to data that has been compressed (zipped) for easier handling and transfer. The checksum field, with an MD5 hash, provides a way to verify the integrity of the data after decompression.
Option Analysis:
* A. The export data type is zipped: Correct. The compressed and encoded format of the data suggests that the export is in a zipped format, allowing for efficient storage and transfer.
* B. The playbook is misconfigured: There is no indication of misconfiguration in this exhibit. The presence of the checksum and data fields aligns with standard export practices.
* C. The option to include the connector was not selected: There is no evidence in the output to conclude that connectors are missing. Connectors are typically listed separately and would not directly affect the checksum and encoded data structure.
* D. Your colleague put a password on the export: There??s no indication of password protection in the exhibit. Password protection would likely alter the data structure, and there would be some mention of encryption.
Conclusion:
Correct Answer:A. The export data type is zipped.
This answer is consistent with the typical use of base64 encoding for compressed (zipped) data exports in FortiAnalyzer.
[References:, FortiAnalyzer 7.4.1 documentation on exporting playbooks and data compression methods.,]

NEW QUESTION 10
Exhibit.



Get Event task configuration



FortiAnalyzer Event Monitor

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 10
Exhibit.

SQL query

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

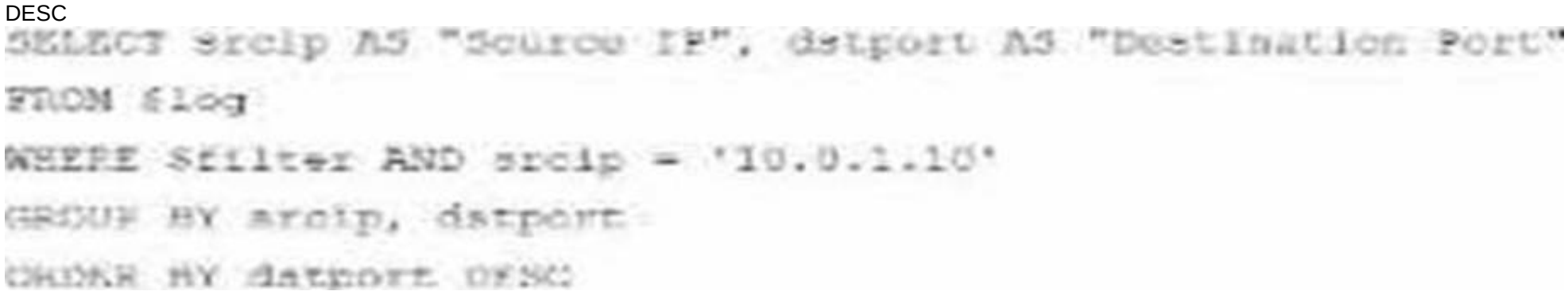
```
SELECT srcip AS "Source IP", dstport AS "Destination Port"
FROM $log
WHERE $filter AND srcip = '10.0.1.10'
ORDER BY dstport
GROUP by srcip, dstport DESC
```

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'

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



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.,]

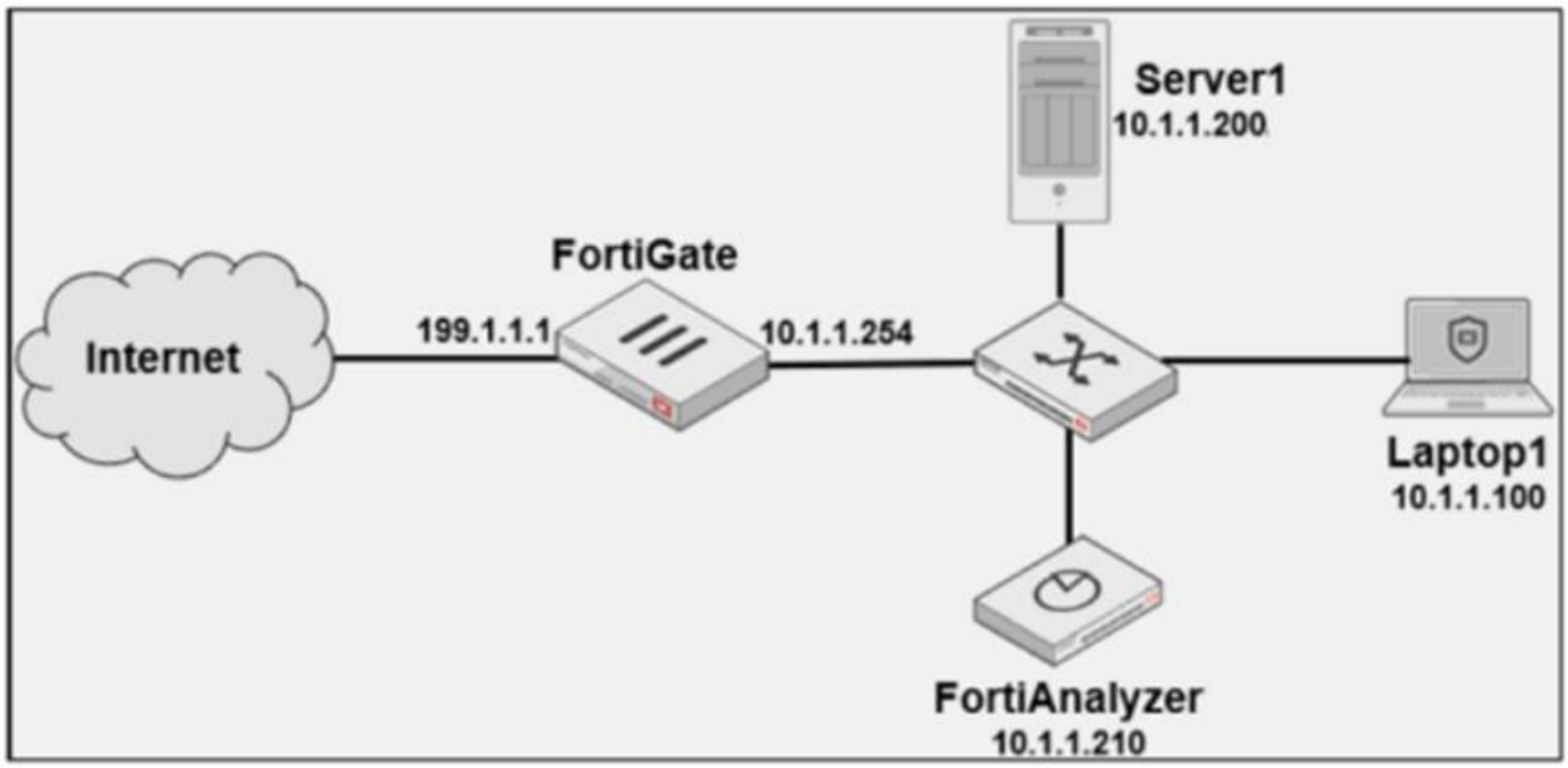
NEW QUESTION 11
Why must you wait for several minutes before you run a playbook that you just created?

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 16
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 20
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 withFortiManager(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 aFortiManager connectorand sending the block information to FortiManager (Option B).

NEW QUESTION 22
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 26
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 27
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 28
Which statement about SQL SELECT queries is true?

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

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 29
Which two actions should an administrator take to vide Compromised Hosts on FortiAnalyzer? (Choose two.)

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

Answer: AB

Explanation:
To view Compromised Hosts on FortiAnalyzer, certain configurations need to be in place on both FortiGate and FortiAnalyzer. Compromised Host data on FortiAnalyzer relies on log information from FortiGate to analyze threats and compromised activities effectively.
Here's why the selected answers are correct:
Option A: Enable device detection on the FortiGate devices that are sending logs to FortiAnalyzer
Enabling device detection on FortiGate allows it to recognize and log devices within the network, sending critical information about hosts that could be compromised. This is essential because FortiAnalyzer relies on these logs to determine which hosts may be at risk based on suspicious activities observed by FortiGate. This setting enables FortiGate to provide device-level insights, which FortiAnalyzer uses to populate the Compromised Hosts view.
Option B: Enable web filtering in firewall policies on FortiGate devices, and make sure these logs are sent to FortiAnalyzer Web filtering is crucial in identifying potentially compromised hosts since it logs any access to malicious sites or blocked categories. FortiAnalyzer uses these web filter logs to detect suspicious or malicious web activity, which can indicate compromised hosts. By ensuring that FortiGate sends these web filtering logs to FortiAnalyzer, the administrator enables FortiAnalyzer to analyze and identify hosts engaging in risky behavior.
Let's review the other options for clarity:
Option C: Make sure all endpoints are reachable by FortiAnalyzer
This is incorrect. FortiAnalyzer does not need direct access to all endpoints. Instead, it collects data indirectly from FortiGate logs. FortiGate devices are the ones that interact with endpoints and then forward relevant logs to FortiAnalyzer for analysis.
Option D: Subscribe FortiAnalyzer to FortiGuard to keep its local threat database up to date
Although subscribing to FortiGuard helps keep threat intelligence updated, it is not a requirement specifically to view compromised hosts. FortiAnalyzer primarily uses logs from FortiGate (such as web filtering and device detection) to detect compromised hosts.
Reference: According to FortiOS and FortiAnalyzer documentation, device detection on FortiGate and enabling web filtering logs are both recommended steps for populating the Compromised Hosts view on FortiAnalyzer. These logs provide insights into device behaviors and web activity, which are essential for identifying and tracking potentially compromised hosts.

NEW QUESTION 30
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 31
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:
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 35
Exhibit.

What is the analyst trying to create?

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

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 36
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 39
Refer to the exhibit.

```
FAZ # diagnose fortilogd lograte
last 5 seconds: 78.8, 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 low indexing values require investigation.
B. The output is not ADOM specific.
C. There are more event logs thantraffic logs.
D. The log rate higher than the message rate is not normal.

Answer: D

NEW QUESTION 42
Which two statements regarding FortiAnalyzer operating modes are true? (Choose two.)

A. When running in collector mode, FortiAnalyzer can forward logs to a syslog server.
B. FortiAnalyzer runs in collector mode by default unless it is configured for HA.
C. You can create and edit reports when FortiAnalyzer is running in collector mode.
D. A topology with FortiAnalyzeer devices running in both modes can improve their performance.

Answer: BD

Explanation:
FortiAnalyzer has two primary operating modes:Analyzer modeandCollector mode. Each mode serves specific purposes and has distinct capabilities.
Option A - Forwarding Logs to a Syslog Server in Collector Mode:
In Collector mode, FortiAnalyzer collects logs from Fortinet devices but does not process or analyze them. Instead, it forwards the logs to other FortiAnalyzer units in Analyzer mode or to specific storage locations. However, forwarding logs to a syslog server is not a function of Collector mode. Logs are generally stored or sent to other FortiAnalyzer devices.
Conclusion:Incorrect.
Option B - Default Mode is Collector Mode Unless Configured for HA:
When a FortiAnalyzer is initially set up, it runs in Collector mode by default unless it is configured as part of a High Availability (HA) setup, whichwould set it to Analyzer mode. Collector mode prioritizes log collection and storage rather than analysis, offloading analysis to other devices in the network.
Conclusion:Correct.
Option C - Report Creation and Editing in Collector Mode:
In Collector mode, FortiAnalyzer does not have the capability to create or edit reports. This mode is focused solely on log collection and forwarding, with analysis and report generation left to FortiAnalyzer units operating in Analyzer mode.
Conclusion:Incorrect.
Option D - Performance Improvement with Both Modes in Topology:
Deploying FortiAnalyzer devices in both Collector and Analyzer modes in a network topology can enhance performance. Collector mode devices handle log collection, reducing the workload on Analyzer mode devices, which focus on log processing, analysis, and reporting. This separation of tasks can optimize resource usage and improve the overall efficiency of log management.
Conclusion:Correct. Conclusion:
Correct Answer B. FortiAnalyzer runs in collector mode by default unless it is configured for HAandD. A topology with FortiAnalyzer devices running in both modes can improve their performance.
These answers correctly describe the functionality and default configuration of FortiAnalyzer operating modes, along with how a mixed-mode topology can enhance performance.
[References:, FortiAnalyzer 7.4.1 documentation on operating modes (Collector and Analyzer) and their respective capabilities.,]

NEW QUESTION 44
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 45
You are tasked with finding logs corresponding to a suspected attack on your network.
You need to use an interface where all identified threats within timeframe are listed and organized. You also need to be able to quickly export the information to a PDF file.
Where can you go to accomplish this task?

A. Log Browse
B. Log View
C. Fabric View
D. FortiView

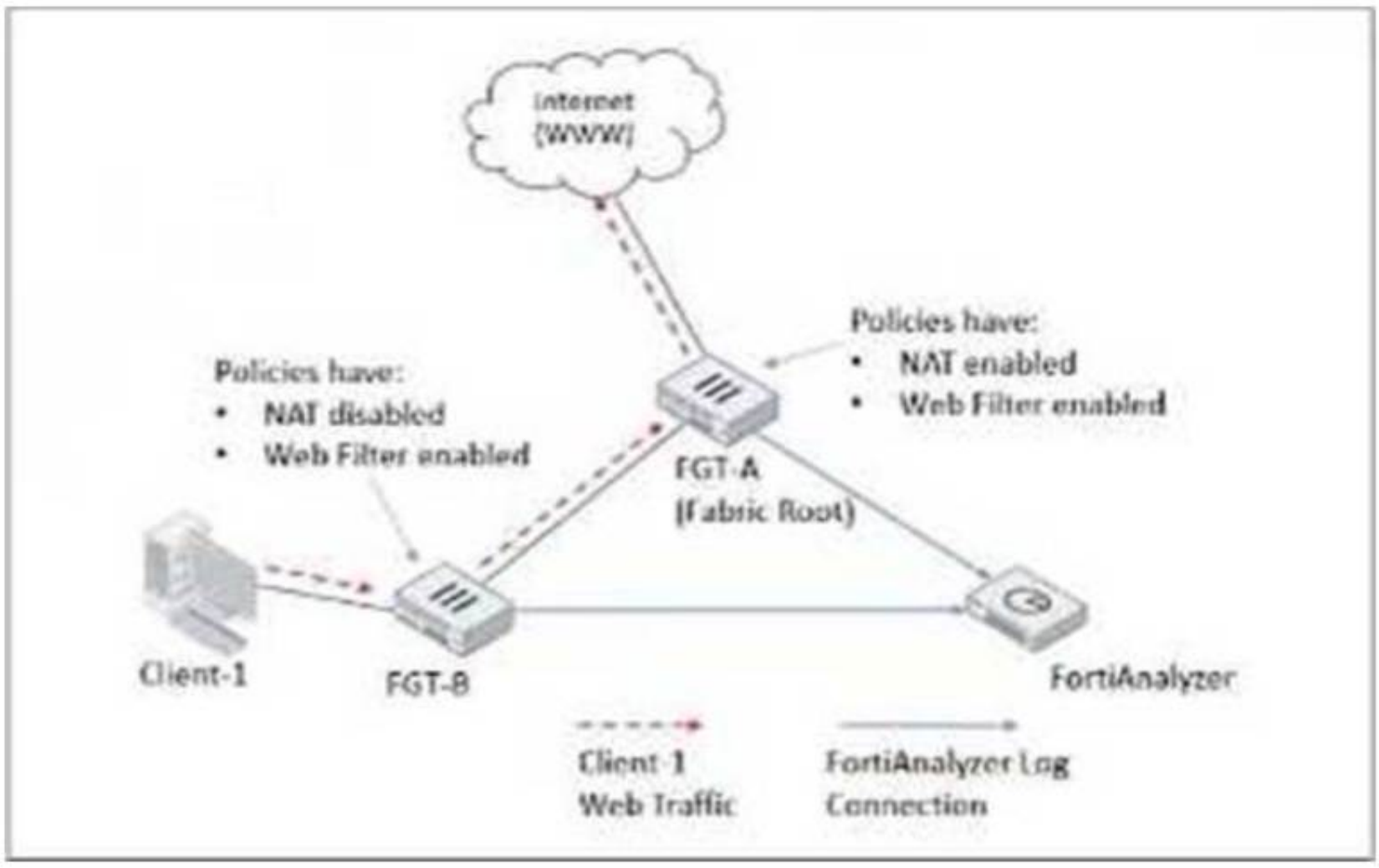
Answer: B

NEW QUESTION 49
Which two parameters does FortiAnalyzer use to identify an indicator of compromise (IOC)? (Choose two answers)

A. IP address
B. URL
C. Policy ID
D. Application category

Answer: AB

NEW QUESTION 52
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 57
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 61
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual FCP_FAZ_AN-7.6 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the FCP_FAZ_AN-7.6 Product From:

https://www.2passeasy.com/dumps/FCP_FAZ_AN-7.6/

Money Back Guarantee

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