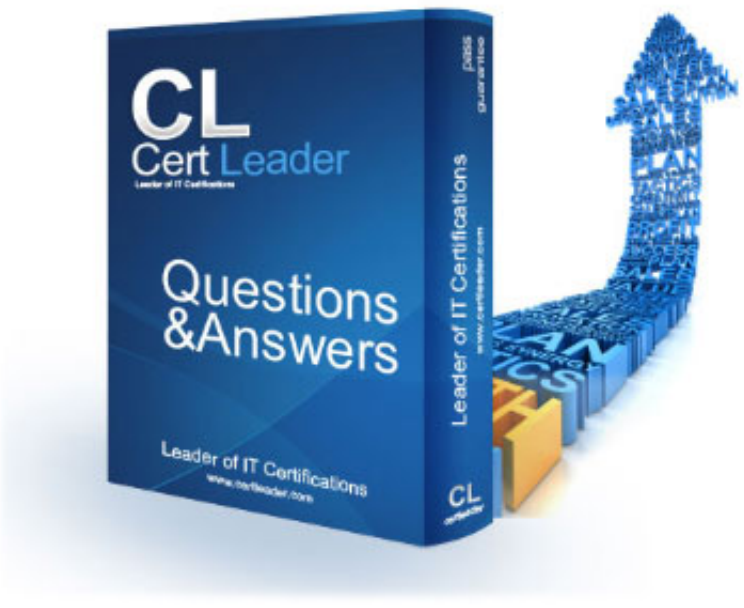
FCP_FAZ_AN-7.6 Dumps

Fortinet NSE 5 - FortiAnalyzer 7.6 Analyst

https://www.certleader.com/FCP_FAZ_AN-7.6-dumps.html



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
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 4
Refer to the exhibit.

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

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

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

Answer: D

Explanation:
Comprehensive and Detailed Explanation: From Exact Extract of knowledge of FortiAnalyzer 7.6 Study guide documents:
In the exhibit, 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 5
Which statement about automation connectors in FortiAnalyzer is true?

A. An ADOM with the Fabric type comes with multiple connectors configured.
B. The local connector becomes available after you configured any external connector.
C. The local connector becomes available after you connectors are displayed.
D. The actions available with FortiOS connectors are determined by automation rules configured on FortiGate.

Answer: D

NEW QUESTION 6
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 7
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 8
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 9
Refer to the exhibit with partial output:

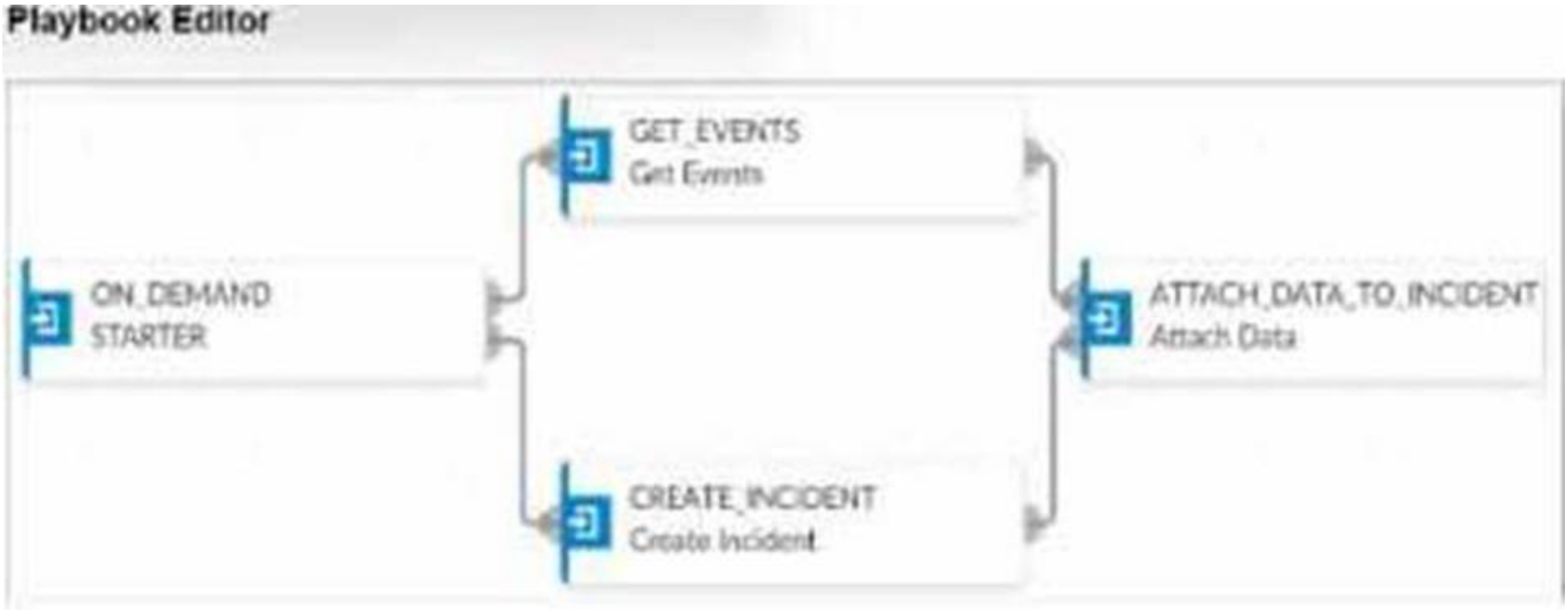
Your colleague exported a playbook and has sent it to you for review. You open the file in a text editor and observer the output as shown in the exhibit.
Which statement about the export is true?

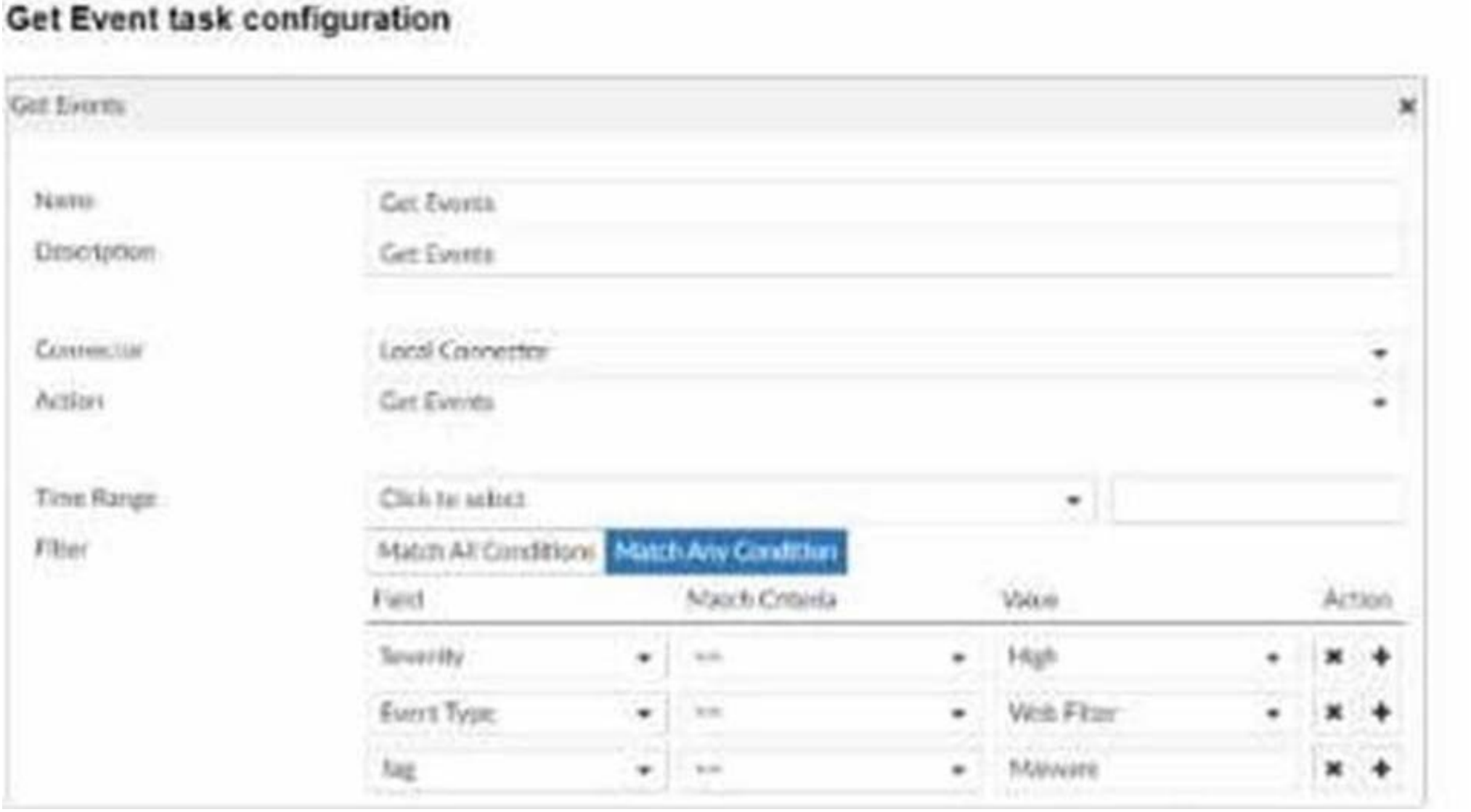
A. The export data type is zipped.
B. The playbook is misconfigured.
C. The option to include the connector was not selected.
D. Your colleague put a password on the export.

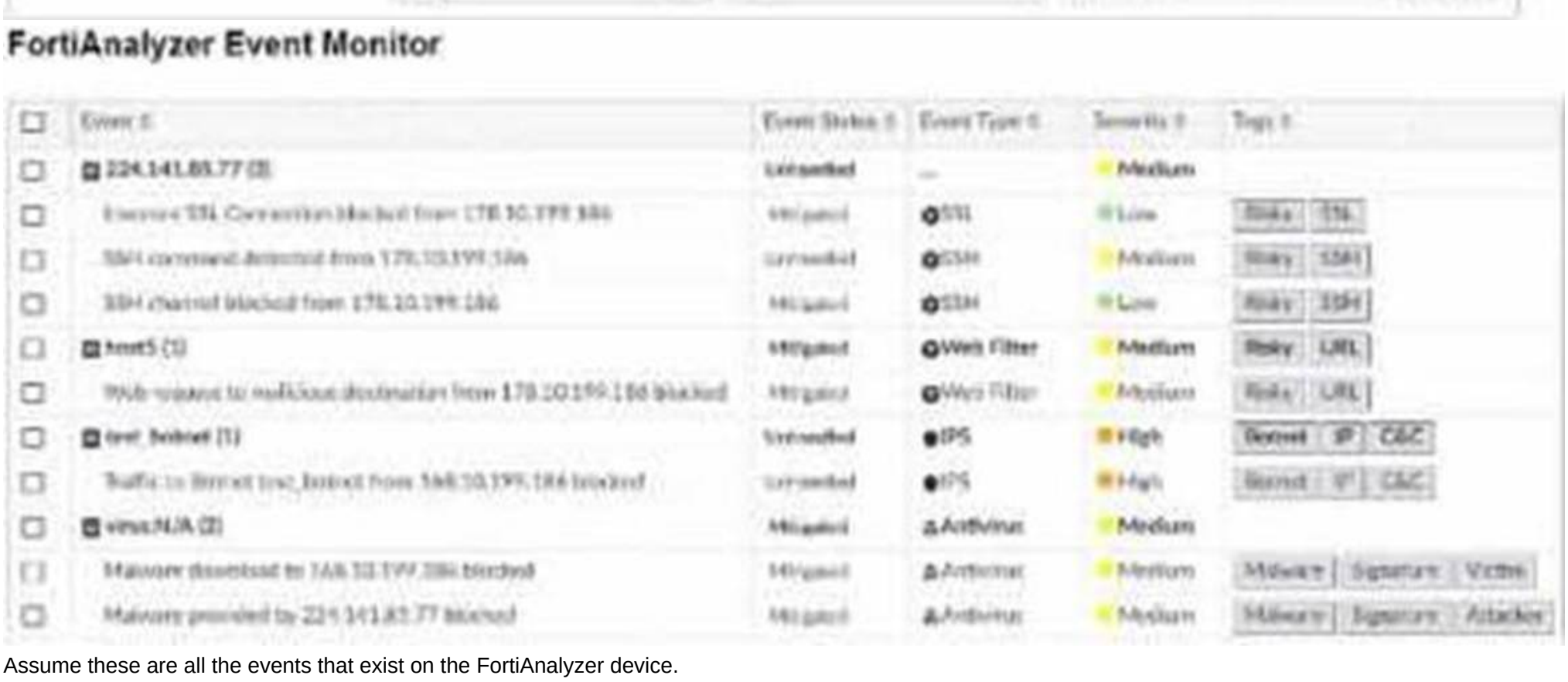
Answer: A

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.







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
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 15
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 19

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 21
Refer to the exhibit.

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

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

A. The security risk was dropped.B.The risk source is isolated.
B. The security risk was blocked.
C. The security event risk is from an application control log.

Answer: C

Explanation:
Comprehensive and Detailed Explanation From Exact Extract of knowledge of FortiAnalyzer 7.6 Study guide documents:
The exhibit shows the eventEvent Status = MitigatedandEvent Type = Web Filter, with the event message indicating the web request wasblocked.
The study guide definesMitigatedevents as follows:"Mitigated: The security risk is mitigated by being blocked or dropped."This means a mitigated status corresponds to enforcement that prevented the risk (block/drop), not a condition where the source is isolated.
It also distinguishesContainedevents from mitigated ones:"Contained: The risk source is isolated."Since the exhibit clearly showsMitigated(not Contained), optionBis incorrect.
Additionally, the study guide notes:??Generally, you can acknowledge mitigated events because the related traffic was blocked by the firewall."This aligns directly with the exhibit's "blocked" wording and supports that the correct interpretation is that the security risk was blocked.
Finally, the event type displayed isWeb Filter, not application control, so optionDis incorrect.
Therefore, the correct statement isC. The security risk was blocked.

NEW QUESTION 23
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.

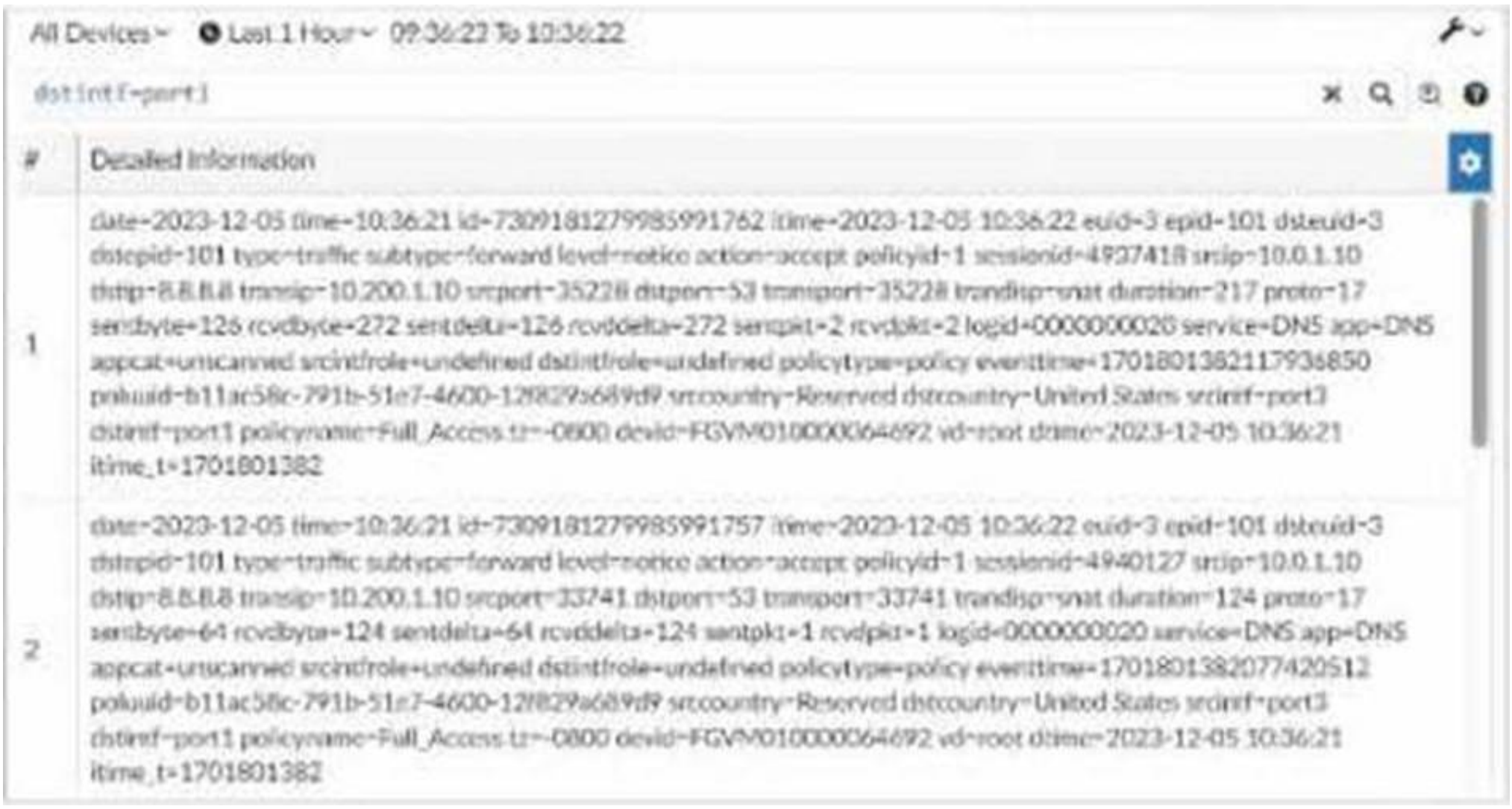
NEW QUESTION 25
Which log will generate an event with the status Unhandled?

A. An AV log with action=quarantine.
B. An IPS log with action=pass.
C. A WebFilter log will action=dropped.
D. An AppControl log with action=blocked.

Answer: B

Explanation:
In FortiOS 7.4.1 and FortiAnalyzer 7.4.1, the "Unhandled" status in logs typically signifies that the FortiGate encountered a security event but did not take any specific action to block or alter it. This usually occurs in the context of Intrusion Prevention System (IPS) logs.
IPS logs with action=pass: When the IPS engine inspects traffic and determines that it does not match any known attack signatures or violate any configured policies, it assigns the action "pass". Since no action is taken to block or modify this traffic, the status is logged as "Unhandled."
Let's look at why the other options are incorrect:
An AV log with action=quarantine: Antivirus (AV) logs with the action "quarantine" indicate that a file was detected as malicious and moved to quarantine. This is a definitive action, so the status wouldn't be "Unhandled."
A WebFilter log will action=dropped: WebFilter logs with the action "dropped" indicate that web traffic was blocked according to the configured web filtering policies. Again, this is a specific action taken, not an "Unhandled" event.
An AppControl log with action=blocked: Application Control logs with the action "blocked" mean that an application was denied access based on the defined application control rules. This is also a clear action, not "Unhandled."

NEW QUESTION 26
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 28
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 syster
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 33
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 38
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

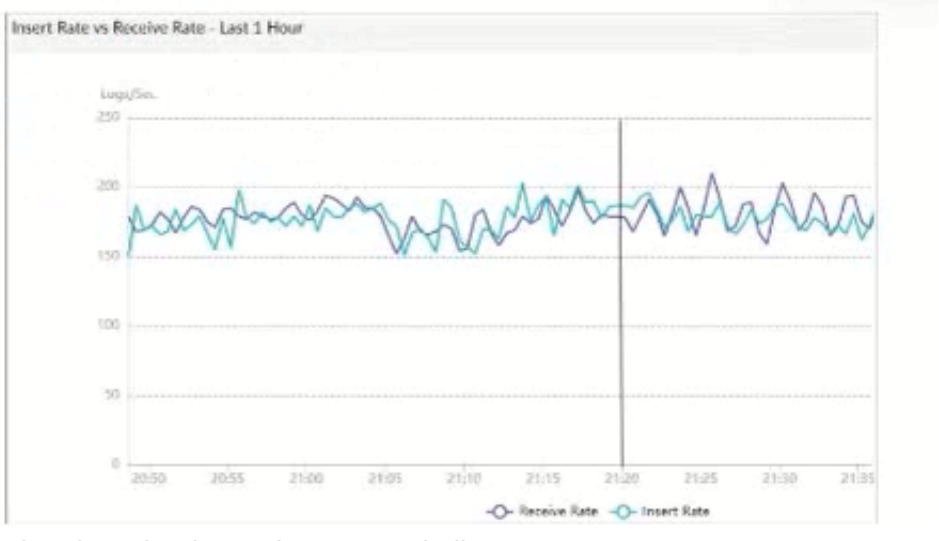
NEW QUESTION 41
After generating a report, you notice the information you where expecting to see is not included in it. However, you confirm that the logs are there.
Which two actions should you perform? (Choose two.)

A. Check the time frame covered by the report.
B. Disable auto-cache.
C. Increase the report utilization quota.
D. Test the dataset

Answer: AD

Explanation:
When a generated report does not contain the expected information even though the logs are confirmed to be present, it typically indicates anissue with the report's configuration. There are a few common reasons this might happen:
Option A - Check the Time Frame Covered by the Report:
Reports are generated based on a specific time frame. If the report's time frame does not cover the period when the relevant logs were collected, those logs won??t appear in the report output. Verifying and adjusting the time frame is essential to ensure the report includes all relevant data.
Conclusion:Correct.
Option B - Disable Auto-Cache:
Auto-cache is designed to improve report generation speed by using cached data. Disabling auto-cache would typically only be relevant if the report is pulling outdated data from cache, but it doesn??t directly affect whether specific logs are included in a report.
Conclusion:Incorrect.
Option C - Increase the Report Utilization Quota:
The report utilization quota is related to the resource limits for generating reports. It does not directly influence whether certain data appears in a report. Increasing this quota would help only if there are resource issues preventing the report from completing, not if specific logs are missing from the report.
Conclusion:Incorrect.
Option D - Test the Dataset:
Datasets determine which logs and data fields are pulled into the report. If a dataset is configured incorrectly or does not include the required log fields, it could lead to missing information. Testing the dataset allows you to verify that it??s correctly configured and pulling the expected data.
Conclusion:Correct.
Conclusion:
Correct Answer:A. Check the time frame covered by the reportandD. Test the dataset.
These steps directly address the issues that could lead to missing information in a report when logs are available but not displayed.
[References:, FortiAnalyzer 7.4.1 documentation on report generation settings, time frames, and dataset configuration for accurate report results.,]

NEW QUESTION 45
Refer to Exhibit:



What does the data point at 21:20 indicate?

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

Answer: A

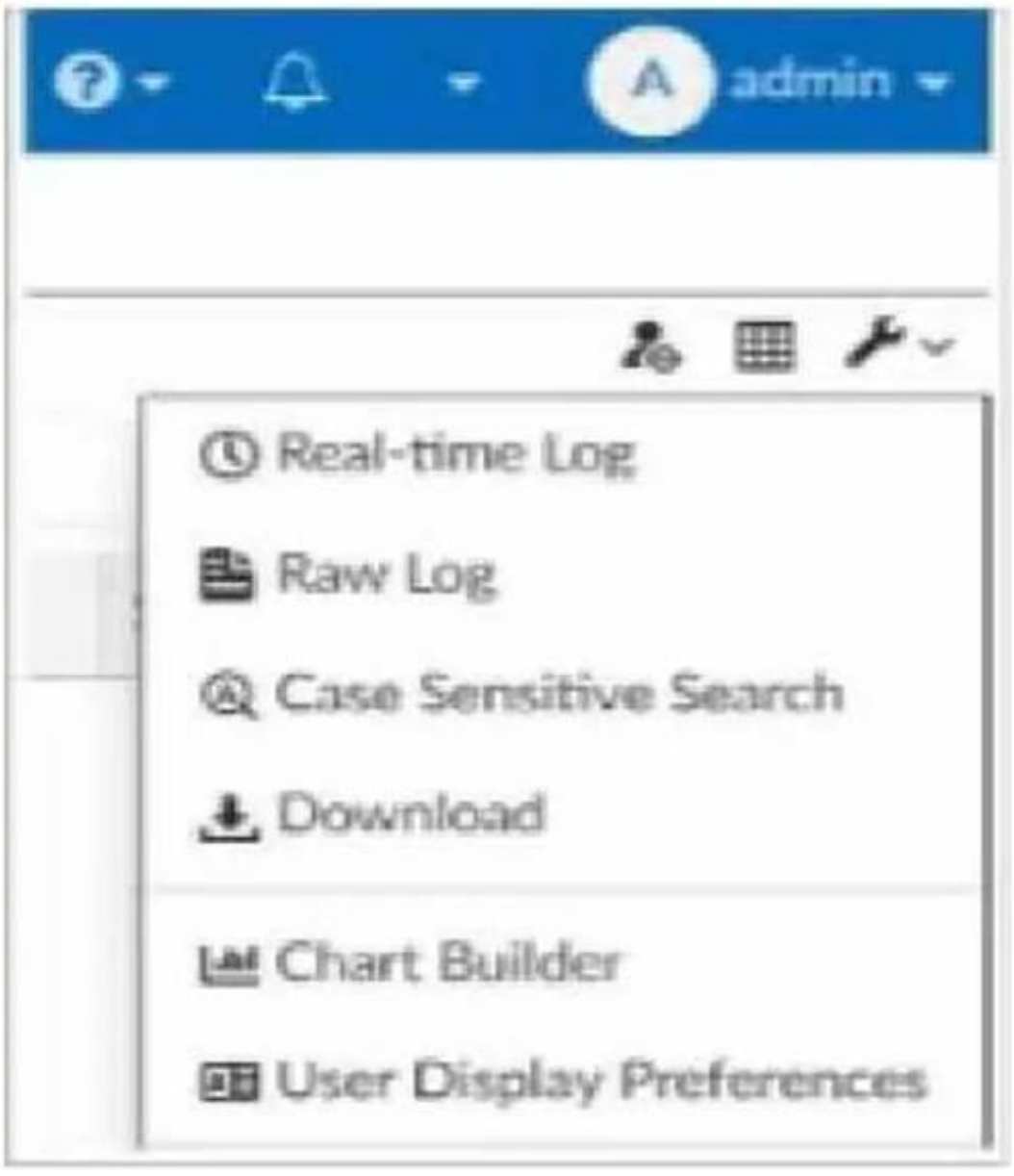
Explanation:
The exhibit shows a graph that tracks two metrics over time:Receive RateandInsert Rate. These two rates are crucial for understanding the log processing behavior in FortiAnalyzer.
Understanding Receive Rate and Insert Rate:
Receive Rate: This is the rate at which FortiAnalyzer is receiving logs from connected devices.
Insert Rate: This is the rate at which FortiAnalyzer is indexing (inserting) logs into its database for storage and analysis.
Data Point at 21:20:
At 21:20, theInsert Rateline is above theReceive Rateline, indicating that FortiAnalyzer is inserting logs into its database at a faster rate than it is receiving them. This situation suggests that FortiAnalyzer is able to keep up with the incoming logs and is possibly processing a backlog or temporarily received logs faster than new logs are coming in.
Option Analysis:
Option A - FortiAnalyzer is Indexing Logs Faster Than Logs are Being Received: This accurately describes the scenario at 21:20, where the Insert Rate exceeds the Receive Rate. This indicates that FortiAnalyzer is handling logs efficiently at that moment, with no backlog in processing.
Option B - The fortilogd Daemon is Ahead in Indexing by One Log: The data does not provide specific information about the fortilogd daemon??s log count, only the rates. This option is incorrect.
Option C - SQL Database Requires a Rebuild: High receive lag would imply a backlog in receiving and indexing logs, typically visible if the Receive Rate were significantly above the Insert Rate, which is not the case here.
Option D - FortiAnalyzer is Temporarily Buffering Logs to Index Older Logs First: There is no indication of buffering in this scenario. Buffering would usually occur if the Receive Rate were higher than the Insert Rate, indicating that FortiAnalyzer is storing logs temporarily due to indexing lag.
Conclusion:
Correct Answer:A. FortiAnalyzer is indexing logs faster than logs are being received.
The graph at 21:20 shows a higher Insert Rate than Receive Rate, indicating efficient log processing by FortiAnalyzer.
[References:, FortiAnalyzer 7.4.1 documentation on log processing metrics, Receive Rate, and Insert Rate indicators.,]

NEW QUESTION 48
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 50
Exhibit.



What is the purpose of using the Chart Builder feature On FortiAnalyzer?

A. To build a chart automatically based on the top 100 log entries
B. To add charts directly to generatereports in the current ADOM.
C. To add a new chart under FortiView to be used in new reports
D. To build a dataset and chart based on the filtered search results

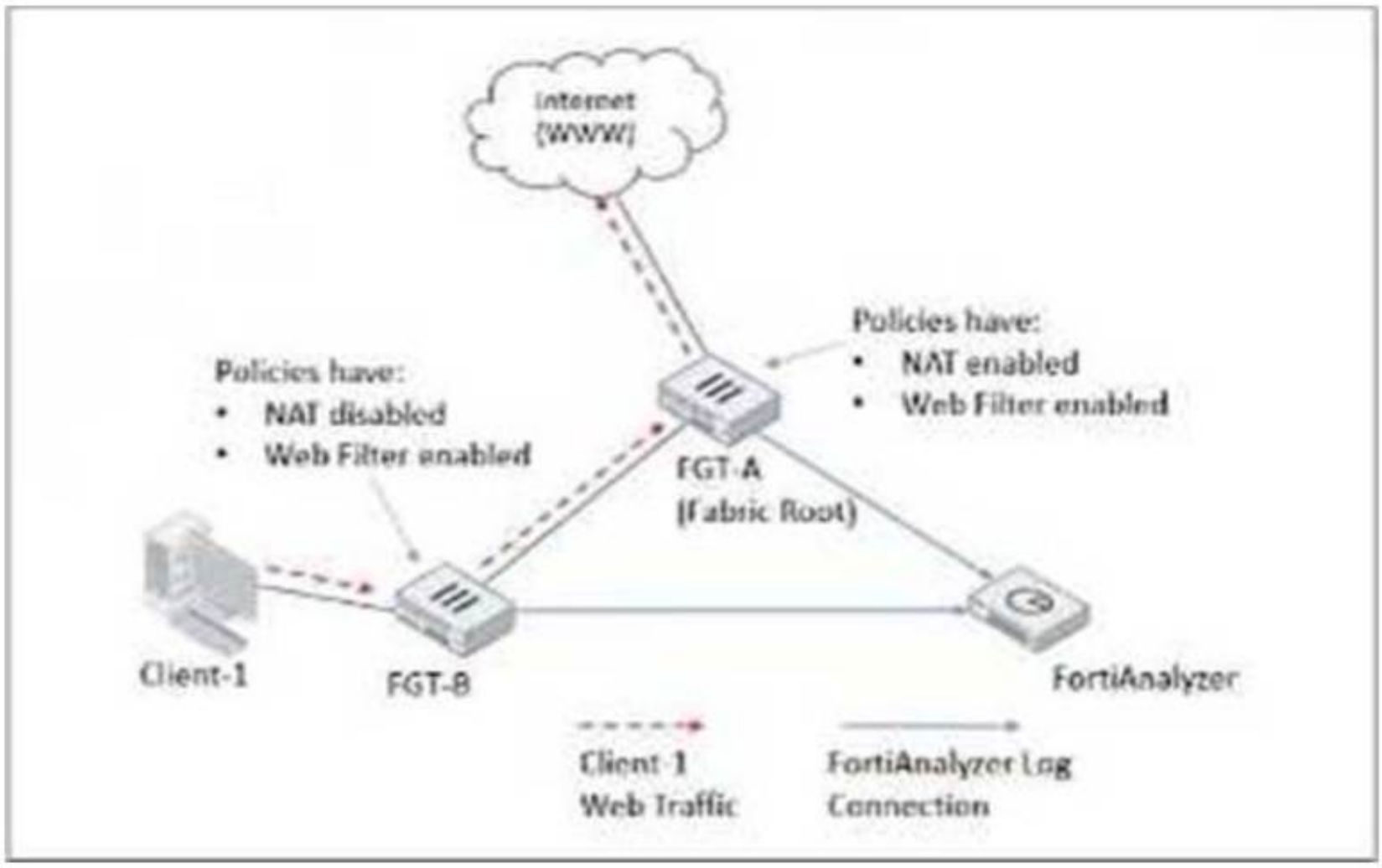
Answer: D

NEW QUESTION 52
Which statement correctly describes one Difference between templates and reports?

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

Answer: D

NEW QUESTION 54
Refer to Exhibit:



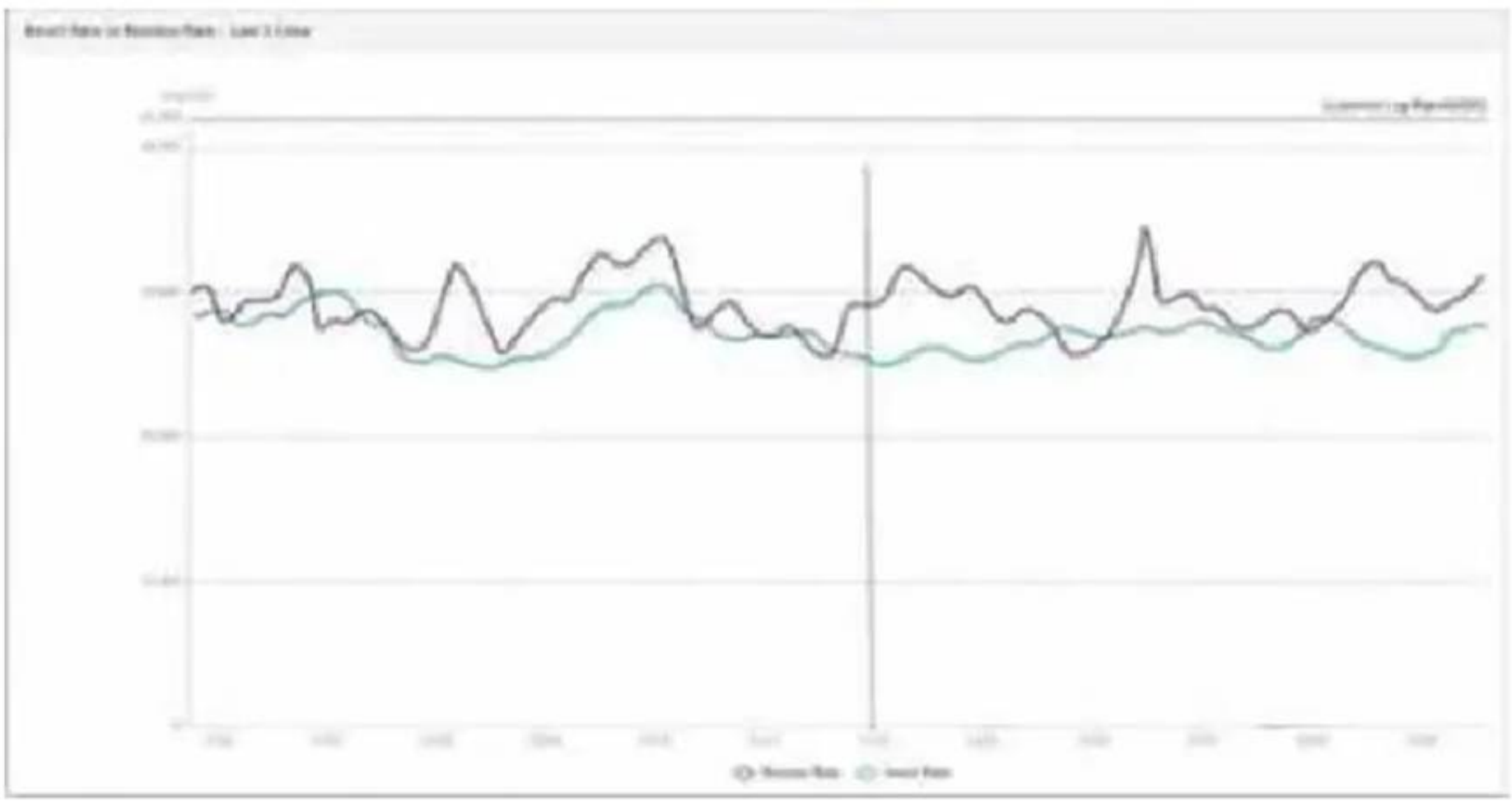
Client-1 is trying to access the internet for web browsing.
All FortiGate devices in the topology are part of a Security Fabric with logging to FortiAnalyzer configured. All firewall policies have logging enabled. All web filter profiles are configured to log only violations.
Which statement about the 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 55
Exhibit.



What does the data point at 12:20 indicate?

A. The loginsert log time is increasing.
B. FortiAnalyzer is using its cache to avoid dropping logs.
C. The performance of FortiAnalyzer is below the baseline.
D. The sqiplugind service is caught up with the logs

Answer: A

NEW QUESTION 59
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 61
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your FCP_FAZ_AN-7.6 Exam with Our Prep Materials Via below:

https://www.certleader.com/FCP_FAZ_AN-7.6-dumps.html