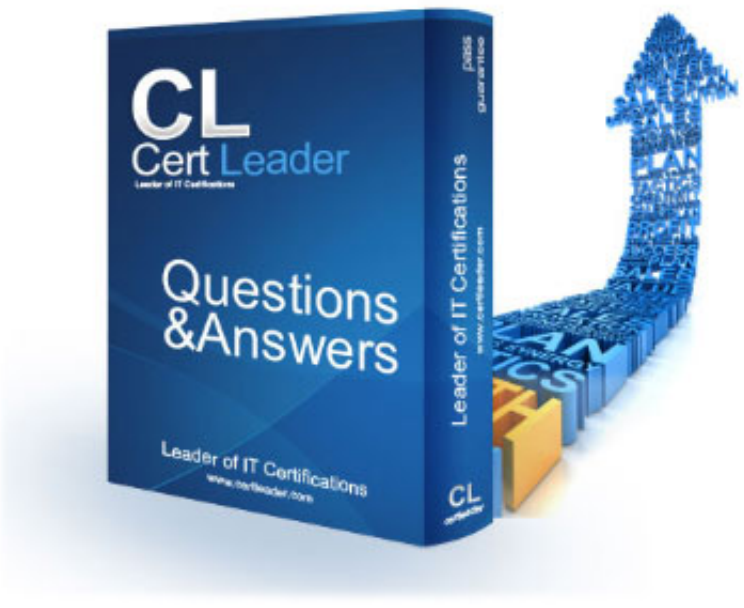
FCP_FAZ_AN-7.6 Dumps

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
Aplaybook contains five tasks in total. An administrator runs the playbook and four out of five tasks finish successfully, but one task fails.
What will be the status of the playbook after it is run?

A. Attention required
B. Upstream_failed
C. Failed
D. Success

Answer: A

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

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

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

Answer: D

Explanation:
FortiAnalyzer offers several features for monitoring, alerting, and incident management, each serving different purposes. Let's examine each option to determine which one best supports a proactive security approach.
* Option A - FortiView Monitor:
* FortiView is a visualization tool that provides real-time and historical insights into network traffic, threats, and logs. While it gives visibility into network activity, it is generally more reactive than proactive, as it relies on existing log data and incidents.
* Conclusion:Incorrect.
* Option B - Outbreak Alert Services:
* Outbreak Alert Services in FortiAnalyzer notify administrators of emerging threats and outbreaks based on FortiGuard intelligence. This is beneficial for awareness of potential threats but does not offer a hands-on, investigative approach. It??s more of a notification service rather than an active, proactive investigation tool.
* Conclusion:Incorrect.
* Option C - Incidents Dashboard:
* The Incidents Dashboard provides a summary of incidents and current security statuses within the network. While it assists with ongoing incident response, it is used to manage and track existing incidents rather than proactively identifying new threats.
* Conclusion:Incorrect.

* Option D - Threat Hunting:
* Threat Hunting in FortiAnalyzer enables security analysts to actively search for hidden threats or malicious activities within the network by leveraging historical data, analytics, and intelligence. This is a proactive approach as it allows analysts to seek out threats before they escalate into incidents.
* Conclusion:Correct.Conclusion:
* Correct Answer D. Threat hunting
* Threat hunting is the most proactive feature among the options, as it involves actively searching for threatswithin the network rather than reacting to already detected incidents.
References:
FortiAnalyzer 7.4.1 documentation on Threat Hunting and proactive security measures.

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

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

Answer: B

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

NEW QUESTION 6
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
What are two effects of enabling auto-cache in a FortiAnalyzer report? (Choose two.)

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

Answer: AC

Explanation:
Enablingauto-cachein FortiAnalyzer reports is designed to improve the efficiency and speed of report generation by leveraging cached data. Let??s analyze each option to determine which effects are correct.
* Option A - The Generation Time for Reports is Decreased:
* When auto-cache is enabled, FortiAnalyzer can use previously cached data instead of reprocessing all log datafrom scratch each time a report is generated. This results in faster report generation times, especially for recurring reports that use similar datasets.
* Conclusion:Correct.
* Option B - Hard-Cache Data is Automatically Updated When New Logs are Received:
* Enabling auto-cache does not immediately update the cache with every new log received. Instead, the cache is updated when reports are generated, based on the existing logs up to that point. Therefore, auto-cache does not constantly refresh with each incoming log, which would be inefficient.
* Conclusion:Incorrect.
* Option C - FortiAnalyzer Local Cache is Used to Store Generated Reports:
* Auto-cache utilizes FortiAnalyzer??s local cache to store data used in reports, reducing the need to retrieve and process logs repeatedly. This cached data can

be reused for subsequent report generation, enhancing performance.
* Conclusion:Correct.
* Option D - The Size of Newly Generated Reports is Optimized to Conserve Disk Space:
* Auto-cache does not directly impact the size ofthe report files themselves. It focuses on performance optimization through cached data for faster access, but it does not compress or optimize the storage size of the generated report.
* Conclusion:Incorrect.Conclusion:
* Correct Answer A. The generation time for reports is decreasedandC. FortiAnalyzer local cache is used to store generated reports.
* Enabling auto-cache helps reduce report generation time by using locally cached data and optimizes report processing, though it does not impact report size or continuously update with each new log.
References:
FortiAnalyzer 7.4.1 documentation on report caching, auto-cache functionality, and report generation optimizations.

NEW QUESTION 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:

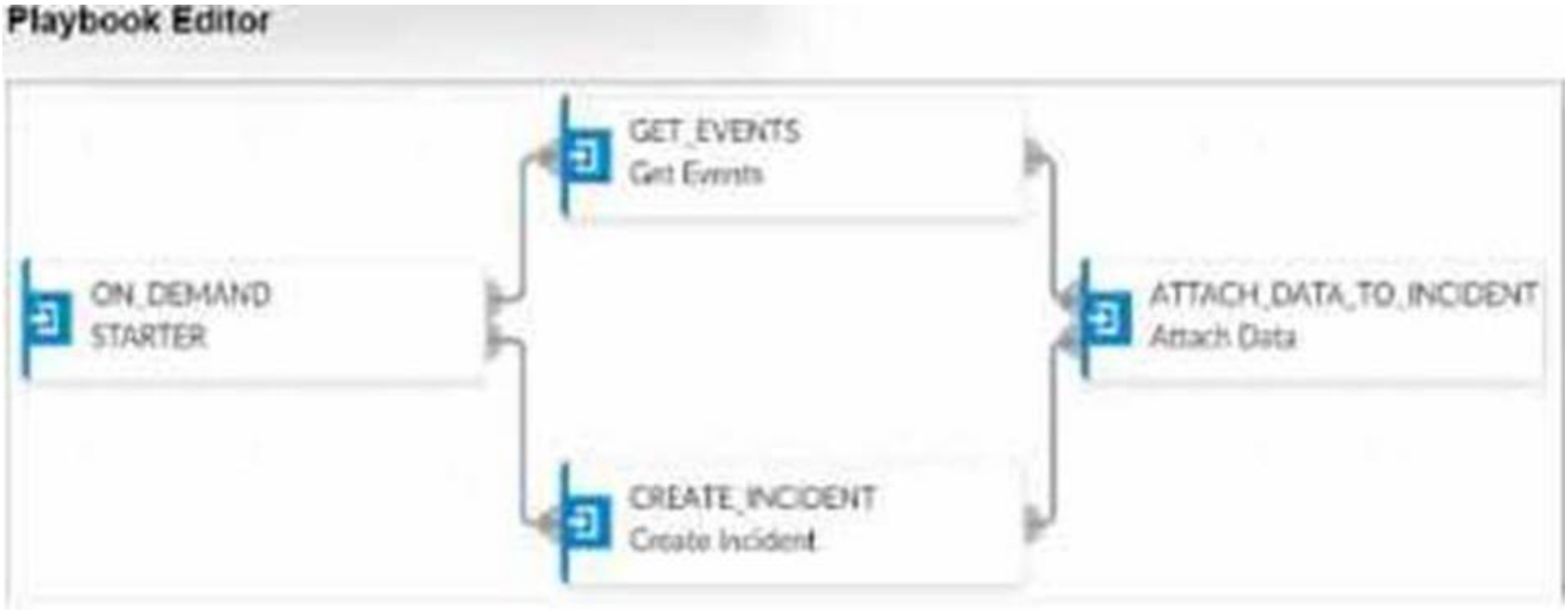
Your colleague exported a playbook and has sent it to you for review. You open the file in a text editor and observer the output as shown in the exhibit.
Which statement about the export is true?

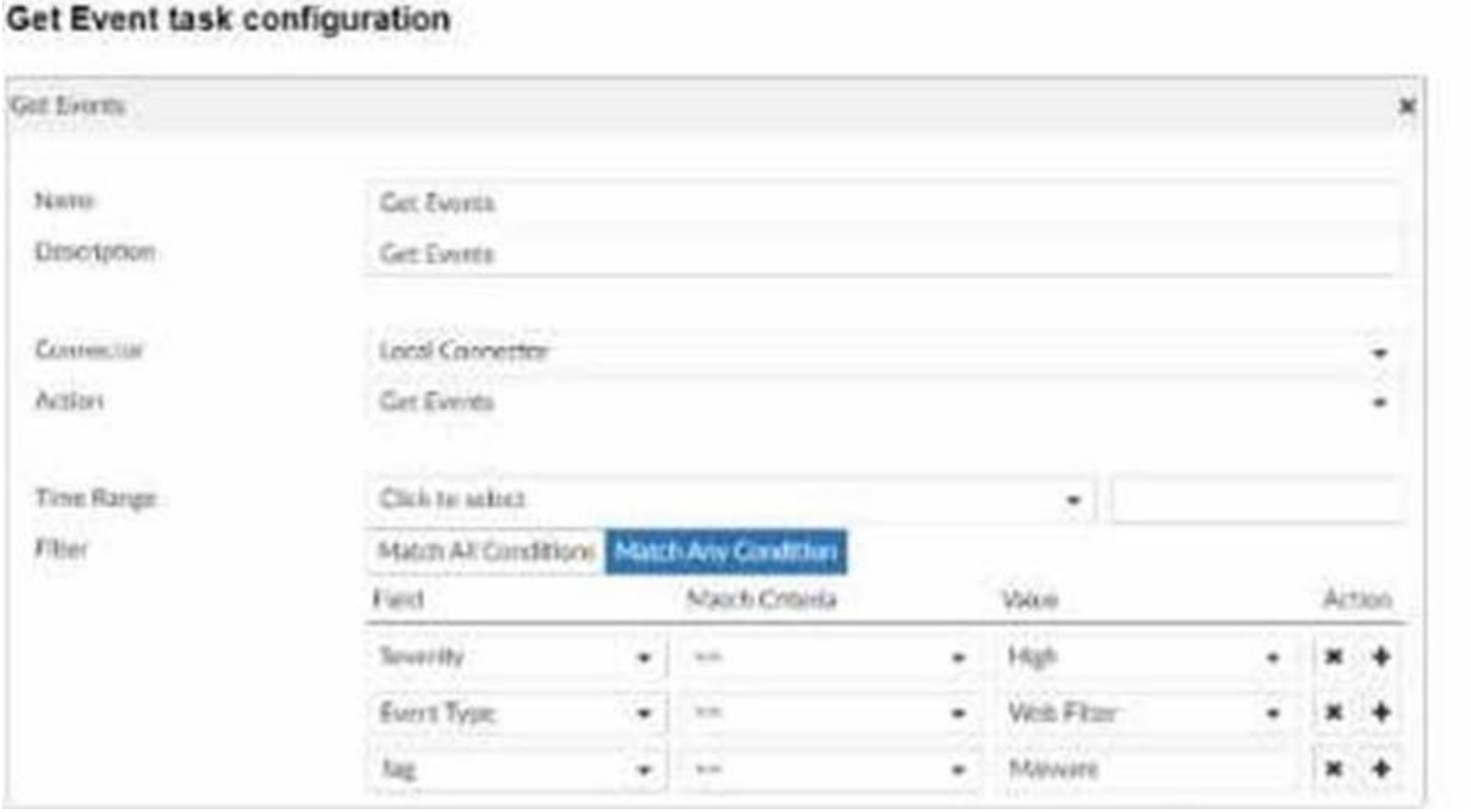
A. The export data type is zipped.
B. The playbook is misconfigured.
C. The option to include the connector was not selected.
D. Your colleague put a password on the export.

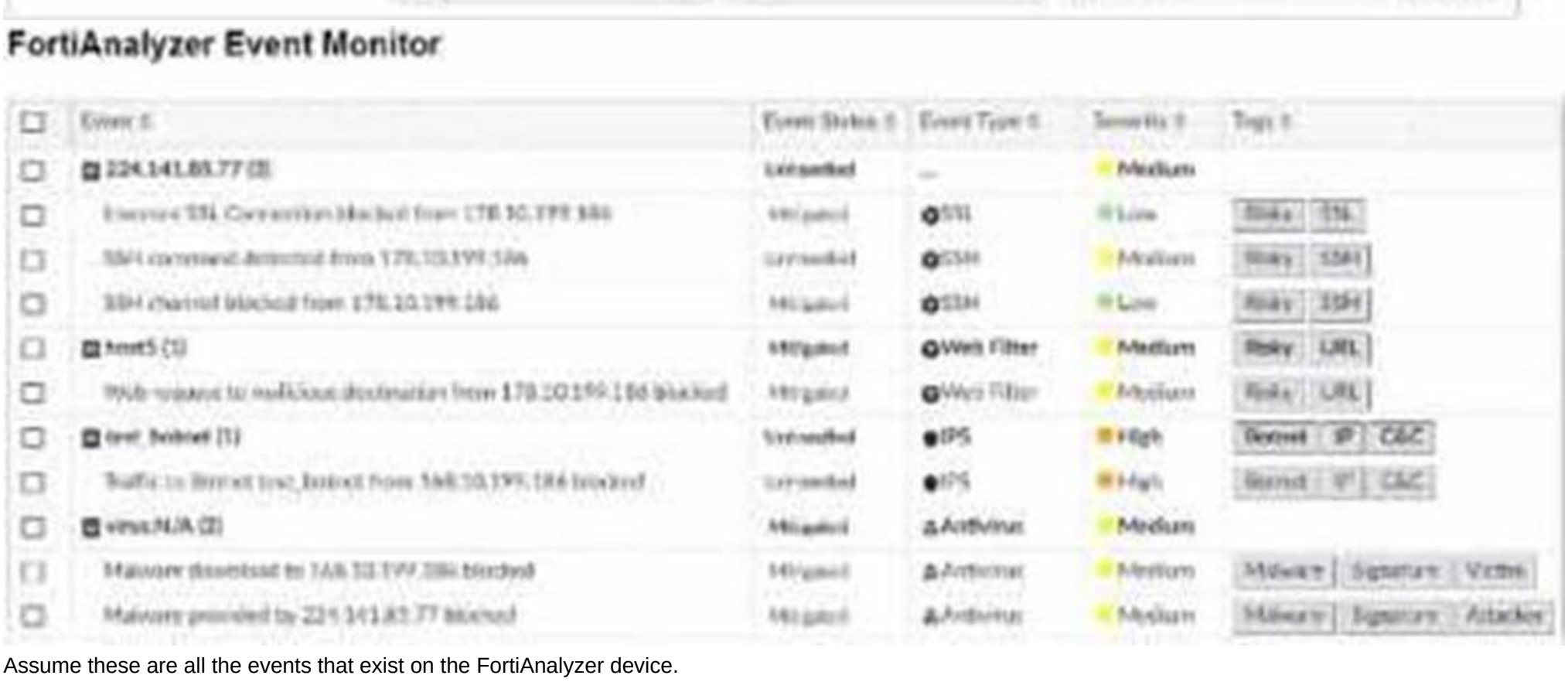
Answer: A

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.,]

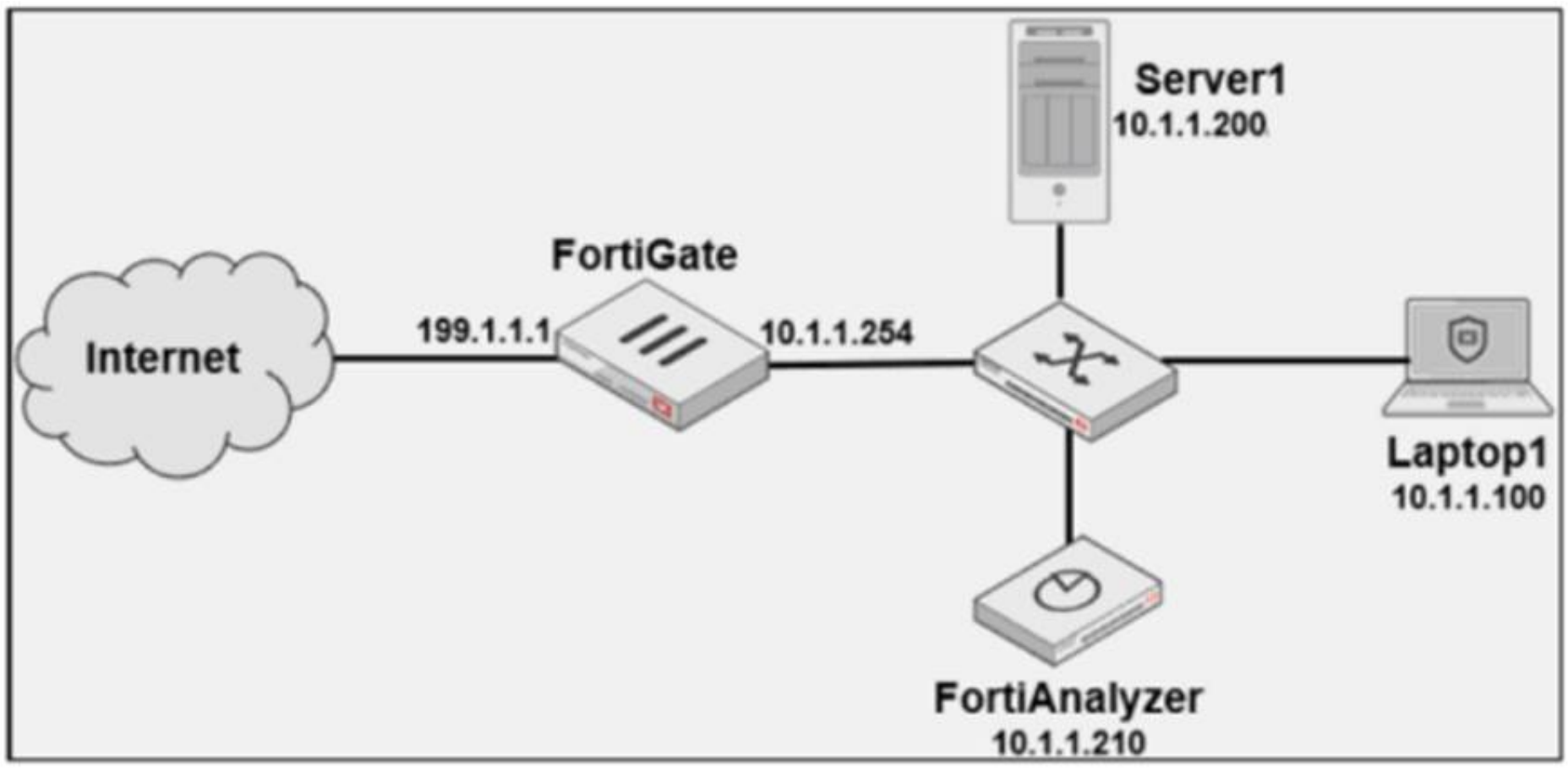
NEW QUESTION 10
Why must you wait for several minutes before you run a playbook that you just created?

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 12
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 15
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 19
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
adom-select                  : normal
adom-status                  : enable
console-output               : enable
country-flag                 : standard
enc-algorithm                : enable
ha-member-auto-grouping      : high
hostname                     : enable
log-checksum                 : FortiAnalyzer1
log-forward-cache-size       : md5
log-mode                     : 5
longitude                    : analyzer
max-aggregation-tasks        : (null)
max-running-reports          : 0
                             : 1
                             : tlsv1.2
                             : disable
                             : tlsv1.3 tlsv1.2
                             : 2000
                             : 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 21
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 22
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 24
Which statement about the FortiSIEM management extension is correct?

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

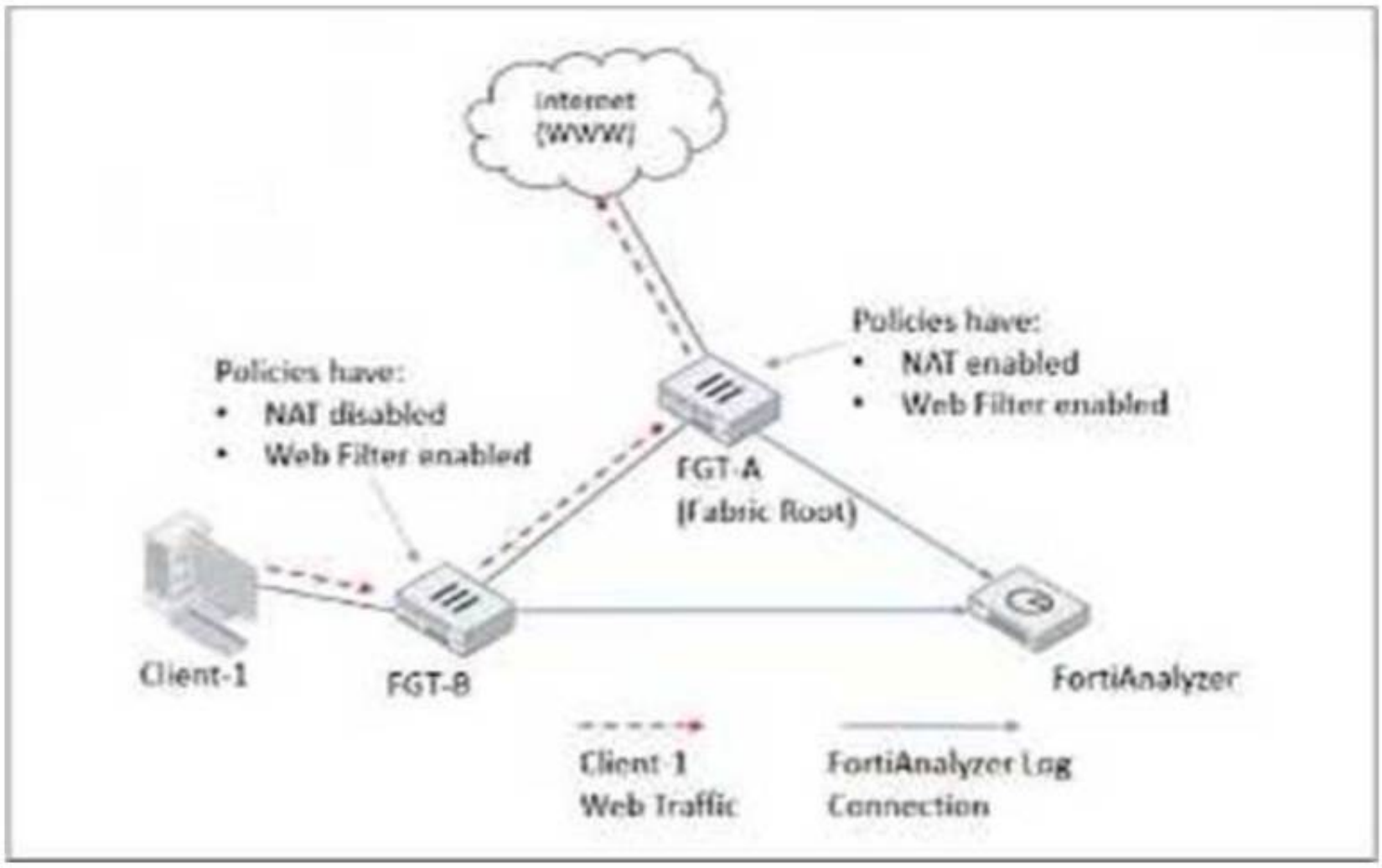
Answer: D

NEW QUESTION 27
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 31
Refer to Exhibit:



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

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

Answer: D

Explanation:
The study guide explains that in a Security Fabric,traffic logging is not 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 35
What two things should an administrator do to view Compromised Hosts on FortiAnalyzer? (Choose two.)

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

Answer: AC

NEW QUESTION 38
.....

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