Fortinet

Exam Questions FCP_FAZ_AN-7.6

Fortinet NSE 5 - FortiAnalyzer 7.6 Analyst

NEW QUESTION 1
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 2
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 3
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 4
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 5
You discover that a few reports are taking a long tine lo generate. Which two steps can you Like to troubleshoot? (Choose two.)

A. Remove old reports from the hcache
B. Enable auto-cache and run the reports again
C. Increase the ADOM reports quota
D. Review report diagnostics

Answer: AB

NEW QUESTION 6
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 7
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 8
Exhibit.

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

They can be downloaded to a file.

A. They are sortable by columns and customizable.

B. They are not available for analysis in FortiView.

C. They were searched by using text mode.

D.

Answer: AD

NEW QUESTION 9

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 syste

Platform Type	
Platform Full Name	
Version	: v7.4.1-build2308 230831 (GA)
Serial Number	: FAZ-VM0000065042
BIOS version	: 04000002
Hostname	: FortiAnalyzer3
Max Number of Admin Domains	: 5
Admin Domain Configuration	: Enabled
FIPS Mode	: Disabled
HA Mode	: Stand Alone
Branch Point	: 2308
Release Version Information	: GA
Time Zone	: (GMT-8:00) Pacific Time (US & Canada)
Disk Usage	: Free 53.06GB, Total 79.80GB
File System	: Ext4
License Status	: Valid

FortiAnalyzer3# get system global

adom-mode	: normal
adom-select	: enable
adom-status	: enable
console-output	: standard
country-flag	: enable
enc-algorithm	: high
ha-member-auto-grouping	: enable
hostname	: FortiAnalyzer3
log-checksum	: md5
log-forward-cache-size	: 5
log-mode	: analyzer
longitude	: (null)
max-aggregation-tasks	: 0
max-running-reports	: 5
oftp-ssl-protocol	: tlsv1.2
ssl-low-encryption	: disable
ssl-protocol	: tlsv1.3 tlsv1.2
task-list-size	: 2000
webservice-proto	: tlsv1.3 tlsv1.2

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

A. FortiAnalayzer1 and FortiAnalyzer3

B. FortiAnalyzer1 and FortiAnalyzer2

C. FortiAnalyzer2 and FortiAnalyzer3

D. All devices listed can be members.

Answer: D

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

NEW QUESTION 10

You created a playbook on FortiAnalyzer that uses a FortiOS connector. When configuring the FortiGate side, which type of trigger must be used so that the actions in an automation stich are available in the FortiOS connector?

A. FortiAnalyzer Event Handler

B. Fabric Connector event

C. FortiOS Event Log

D. Incoming webhook

Answer: D

Explanation:
When using FortiAnalyzer to create playbooks that interact with FortiOS devices, an Incoming Webhook trigger is required on the FortiGate side to make the actions in an automation stitch accessible through the FortiOS connector. The incoming webhook trigger allows FortiAnalyzer to initiate actions on FortiGate by sending HTTP POST requests to specified endpoints, which in turn trigger automation stitches defined on the FortiGate.

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

NEW QUESTION 10
When managing incidents on FortiAnlyzer, what must an analyst be aware of?

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

Answer: A

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

NEW QUESTION 13
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 15
What is the purpose of running the command diagnose sql status sqlreportd?

A. To view a list of scheduled reports
B. To list the current SQL processes running
C. To display the SQL query connections and hcache status
D. To identify the database log insertion status

Answer: C

Explanation:
The command diagnose sql statussqlreportd is used in FortiAnalyzer to obtain specific information about the SQL reporting process and caching status. Here??s what this command accomplishes and an analysis of each option:
Command Functionality:
sqlreportd is the FortiAnalyzer daemon responsible for managing SQL-based reporting processes.
The diagnose sql status sqlreportd command provides information on active SQL query connections and thehcache(historical cache) status, which helps in monitoring and troubleshooting SQL report generation.
Option Analysis:
Option A - To View a List of Scheduled Reports:
This option is incorrect because the command does not list scheduled reports. Instead, it focuses on SQL reporting processes and cache details.

Option B - To List the Current SQL Processes Running:
While the command may show active SQL connections, its primary focus is not a detailed list of all SQL processes but rather the connections and cache status for reporting.
Option C - To Display the SQL Query Connections and hcache Status:
This is correct. The command specifically provides information on SQL query connections related to the reporting process (sqlreportd) and displays thehcachestatus.
Option D - To Identify the Database Log Insertion Status:
This is incorrect. The command does not provide details on log insertion status. Log insertion status is typically monitored through different diagnostic commands focused on database processes and log handling.
Conclusion:
Correct Answer C. To display the SQL query connections and hcache status
This command is used to monitor SQL reporting activities and cache status, aiding in the analysis of report generation performance and connection health.
[References:, FortiAnalyzer 7.4.1 documentation on SQL diagnostic commands, particularly those related to reporting (sqlreportd) and caching mechanisms., ,]

NEW QUESTION 19
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 22
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.

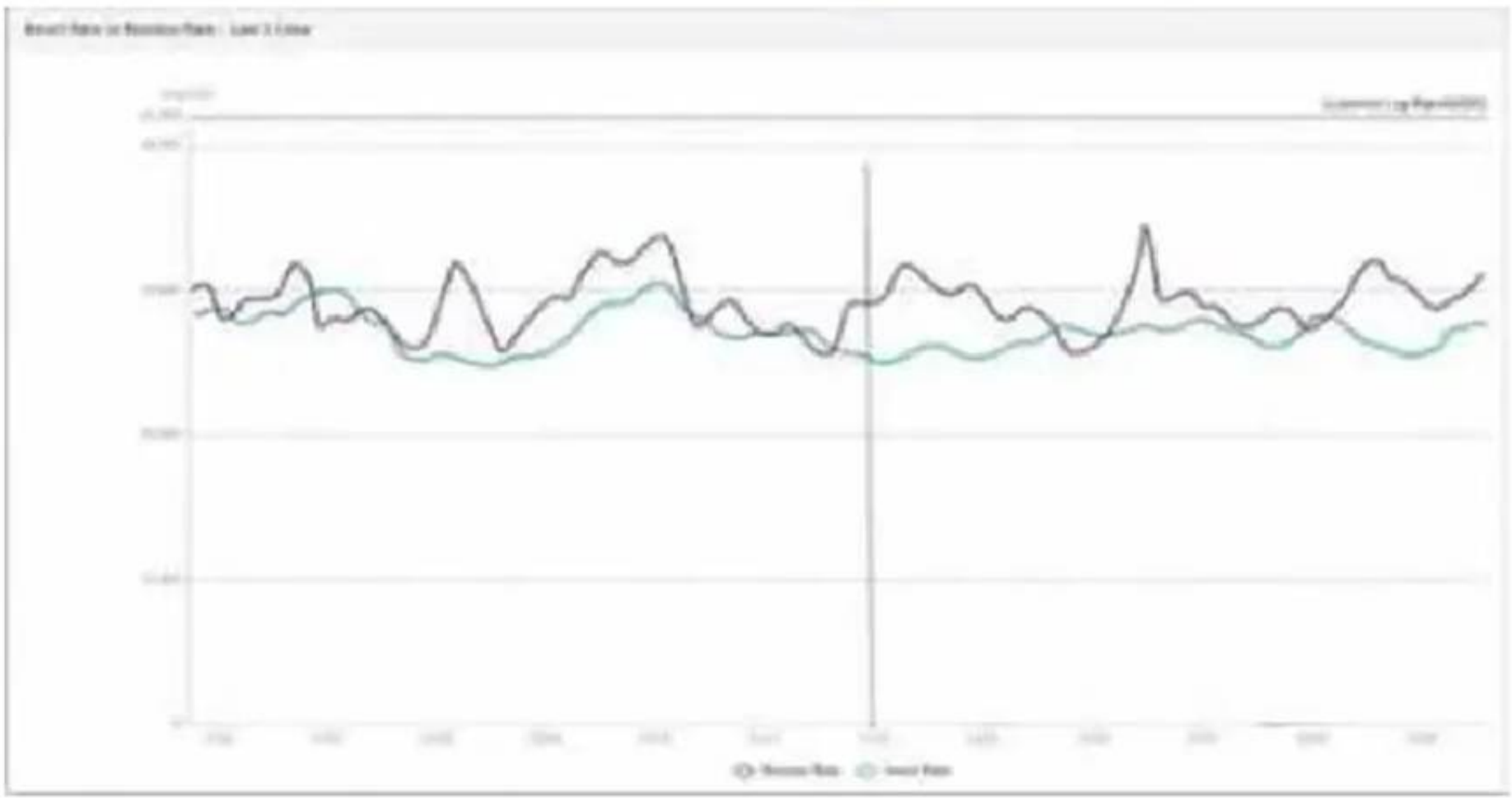
Answer: C

NEW QUESTION 26
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 30
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 33
You created a playbook on FortiAnalyzer that uses a FortiOS connector. When you configure FortiGate, which type of trigger must you use so that the actions in an automation stitch are available in the FortiOS connector? (Choose one answer))

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

Answer: B

Explanation:
From Exact Extract of knowledge of FortiAnalyzer 7.6 Study guide documents:
The study guide explains that FortiAnalyzer playbook tasks rely on connectors, and that the FortiOS connector will not show its available actions until FortiGate is configured with the correct automation trigger. The guide states:"For example, the FortiOS connector will be listed as soon as the first FortiGate device is added to FortiAnalyzer. However, to see the actions related to that FortiOS connector, you must enable an automation rule using the Incoming Webhook Call trigger on FortiGate."
This is why the required FortiGate trigger type 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 37
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

FCP_FAZ_AN-7.6 Practice Exam Features:

* FCP_FAZ_AN-7.6 Questions and Answers Updated Frequently

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

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

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