Fortinet

Exam Questions FCP_FAZ_AN-7.6

Fortinet NSE 5 - FortiAnalyzer 7.6 Analyst

NEW QUESTION 1
What is the purpose of playbook trigger variables?

A. To display statistics about the playbook runtime
B. To use information from the trigger to filter the action in a task
C. To provide the trigger information to make the playbook start running
D. To store the start the times of playbooks with On_Schedule triggers

Answer: B

NEW QUESTION 2
Which statement about sending notifications with incident update is true?

A. You can send notifications to multiple external platforms.
B. Notifications can be sent only by email.
C. If you use multiple fabric connectors, all connectors must have the same settings.
D. Notifications can be sent only when an incident is updated or deleted.

Answer: A

Explanation:
In FortiOS and FortiAnalyzer,incident notificationscan be sent to multiple external platforms, not limited to a single method such as email. Fortinet's security fabric and integration capabilities allow notifications to be
sent through various fabric connectors and third-party integrations. This flexibility is designed to ensure that incident updates reach relevant personnel or systems using preferred communication channels, such as email, Syslog, SNMP, or integration with SIEM platforms.
Let??s review each answer option for clarity:
* Option A: You can send notifications to multiple external platforms
* This is correct. Fortinet??s notification system is capable of sending updates to multiple platforms, thanks to its support for fabric connectors and external integrations. This includes options such as email, Syslog, SNMP, and others based on configured connectors.
* Option B: Notifications can be sent only by email
* This is incorrect. Although email is a common method, FortiOS and FortiAnalyzer support multiple notification methods through various connectors, allowing notifications to be directed to different platforms as per the organization??s setup.
* Option C: If you use multiple fabric connectors, all connectors must have the same settings
* This is incorrect. Each fabric connector can have its unique configuration, allowing different connectors to be tailored for specific notification and integration requirements.
* Option D: Notifications can be sent only when an incident is updated or deleted
* This is incorrect. Notifications can be sent upon the creation of incidents, as well as upon updates or deletion, depending on the configuration.
:According to FortiOS and FortiAnalyzer 7.4.1 documentation, notifications for incidents can be configured across various platforms by using multiple connectors, and they are not limited to email alone. This capability is part of the Fortinet Security Fabric, allowing for a broad range of integrations with external systems and platforms for effective incident response.

NEW QUESTION 3
An administrator on your team has configured multiple reports to run periodically. Management has an additional request that all new generated reports be sent to a company email inbox for accessibility. The mail server has already been configured on FortiAnalyzer.
Which item must configure on FortiAnalyzer so that emails are sent when the reports are generated?

A. Enable the option to email all repots under the mail server.
B. Add amailto:<emailaddress> option within the report layouts.
C. Enable email notification under the report calendar.
D. Enable an output profile on the reports.

Answer: D

Explanation:
To ensure that reports generated by FortiAnalyzer are automatically sent to an email inbox, you need to set up an output profile for the reports. Output profiles specify where and how reports should be delivered, including the option to send them via email.
* Option A - Enable the Option to Email All Reports Under the Mail Server:
* The mail server configuration allows FortiAnalyzer to send emails but does not automatically enable email distribution for reports. This setting alone does not specify which reports to send or to whom.
* Conclusion:Incorrect.
* Option B - Add a mailto:<email address> Option Within the Report Layouts:
* Adding an email address within the report layout is not a standard configuration option for report distribution. Report layouts define the format andcontent of the report but not its distribution method.
* Conclusion:Incorrect.
* Option C - Enable Email Notification Under the Report Calendar:
* The report calendar is used to schedule when reports are generated. While it triggers report generation at specific times, it does not handle email distribution. Emailing reports requires a configured output profile.
* Conclusion:Incorrect.
* Option D - Enable an Output Profile on the Reports:
* An output profile can be configured on FortiAnalyzer to define delivery options, including emailing the report to specified recipients. This setup ensures that every time a report is generated according to the schedule, it is automatically emailed to the configured address.
* Conclusion:Correct. Conclusion:
* Correct Answer D. Enable an output profile on the reports.
* Configuring an output profile is the correct way to set up automatic email distribution of generated reports in FortiAnalyzer.
References:
FortiAnalyzer 7.4.1 documentation on configuring output profiles and report distribution settings.

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
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

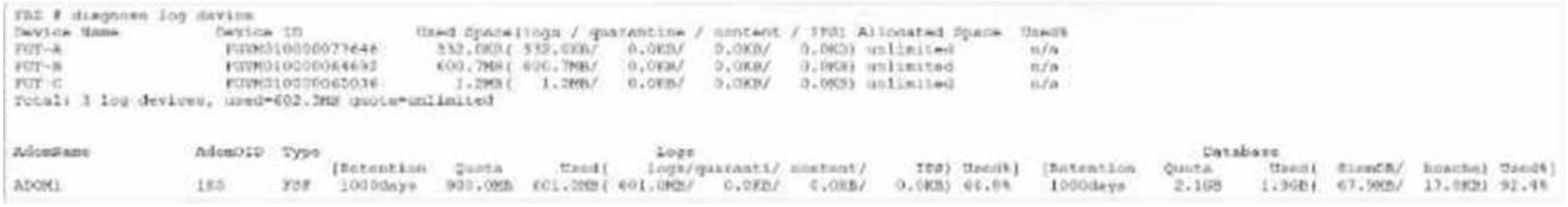
Explanation:
Comprehensive and Detailed Explanation: From Exact Extract of knowledge of FortiAnalyzer 7.6 Study guide documents:
In the exhibit, theEvent Statusshown isUnhandled(Event Type: Web Filter; Severity: Critical). The FortiAnalyzer study guide definesUnhandledevents as events whose security 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 6
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 7
Exhibit.



```
FAZ # diagnose log device
Device Name           Device ID           Used Space(logs / quarantine / content / IOC) Allocated Space  Used%
FGT-A                 FGVM010000077646      532.0KB( 532.0KB/   0.0KB/   0.0KB/   0.0KB) unlimited        n/a
FGT-B                 FGVM010000064692      600.7MB( 600.7MB/   0.0KB/   0.0KB/   0.0KB) unlimited        n/a
FGT-C                 FGVM010000060036        1.2MB(   1.2MB/   0.0KB/   0.0KB/   0.0KB) unlimited        n/a
Total: 3 log devices, used=602.3MB quota=unlimited

AdomName          AdomOID  Type                                  Logs                                                    Database
                           [Retention   Quota      Used(    logs/quaranti/ content/      IOC) Used%] [Retention   Quota      Used(  Size(GB/  Logs(GB) Used%]
ADOM1             180      FOS  1000days   900.0MB  601.2MB( 601.0MB/   0.0KB/   0.0KB   0.0KB) 66.8% 1000days   2.1GB    1.3GB(  67.9MB/  17.9MB) 92.4%
```

What can you conclude from this output?

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

Answer: B

NEW QUESTION 8
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 9
What are two effects of enabling auto-cache in a FortiAnalyzer report? (Choose two.)

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

Answer: AC

Explanation:
Enablingauto-cachein FortiAnalyzer reports is designed to improve the efficiency and speed of report generation by leveraging cached data. Let??s analyze each option to determine which effects are correct.
* Option A - The Generation Time for Reports is Decreased:
* When auto-cache is enabled, FortiAnalyzer can use previously cached data instead of reprocessing all log datafrom scratch each time a report is generated. This results in faster report generation times, especially for recurring reports that use similar datasets.
* Conclusion:Correct.
* Option B - Hard-Cache Data is Automatically Updated When New Logs are Received:
* Enabling auto-cache does not immediately update the cache with every new log received. Instead, the cache is updated when reports are generated, based on the existing logs up to that point. Therefore, auto-cache does not constantly refresh with each incoming log, which would be inefficient.
* Conclusion:Incorrect.
* Option C - FortiAnalyzer Local Cache is Used to Store Generated Reports:
* Auto-cache utilizes FortiAnalyzer??s local cache to store data used in reports, reducing the need to retrieve and process logs repeatedly. This cached data can be reused for subsequent report generation, enhancing performance.
* Conclusion:Correct.
* Option D - The Size of Newly Generated Reports is Optimized to Conserve Disk Space:
* Auto-cache does not directly impact the size ofthe report files themselves. It focuses on performance optimization through cached data for faster access, but it does not compress or optimize the storage size of the generated report.
* Conclusion:Incorrect.Conclusion:
* Correct Answer A. The generation time for reports is decreasedandC. FortiAnalyzer local cache is used to store generated reports.
* Enabling auto-cache helps reduce report generation time by using locally cached data and optimizes report processing, though it does not impact report size or continuously update with each new log.
References:
FortiAnalyzer 7.4.1 documentation on report caching, auto-cache functionality, and report generation optimizations.

NEW QUESTION 10
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 10
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 12
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 15
Exhibit.

```
FAZ # diagnose fortilogd lograte
last 5 seconds: 70.0, last 30 seconds: 132.1, last 60 seconds: 133.3

FAZ # diagnose fortilogd msgrate
last 5 seconds: 1.4, last 30 seconds: 1.6, last 60 seconds: 1.6
```

What can you conclude about the output?

A. The message rate being lower that the log rate is normal.
B. Both messages and logs are almost finished indexing.
C. There are more traffic logs than event logs.
D. The output is ADOM specific

Answer: A

Explanation:
In this output, we see two diagnostic commands executed on a FortiAnalyzer device:
diagnose fortilogd lograte: This command shows the rate at which logs are being processed by the FortiAnalyzer in terms of log entries per second.
diagnose fortilogd msgrate: This command displays the message rate, or the rate at which individual messages are being processed.
The values provided in the exhibit output show:
Log rate (lograte): Consistently high, showing values such as 70.0, 132.1, and 133.3 logs per second over different time intervals.
Message rate (msgrate): Lower values, around 1.4 to 1.6 messages per second. Explanation
Interpretation of log rate vs. message rate: In FortiAnalyzer, the log rate typically refers to the rate of logs being stored or indexed, while the message rate refers to individual messages within these logs. Given that a single log entry can contain multiple messages, it's common to see a lower message rate relative to the log rate.

Understanding normal operation: In this case, the message rate being lower than the log rate is expected and typical behavior. This discrepancy can arise because each log entry may bundle multiple related messages, reducing the message rate relative to the log rate.
Conclusion
Correct Answer A. The message rate being lower than the log rate is normal.
This aligns with thenormal operational behavior of FortiAnalyzer in processing logs and messages.
There is no indication that both logs and messages are nearly finished indexing, as that would typically show diminishing rates toward zero, which is not the case here. Additionally, there's no information in this output about specific ADOMs or a comparison between traffic logs and event logs. Thus, options B, C, and D are incorrect.
[References:, FortiOS 7.4.1 and FortiAnalyzer 7.4.1 command guides for diagnose fortilogd lograte and diagnose fortilogd msgrate.,]

NEW QUESTION 20
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 21
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 24
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 26
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 29
Which statement about the FortiSOAR management extension is correct?

A. It requires a FortiManager configured to manage FortiGate.
B. It runs as a docker container on FortiAnalyzer.
C. It requires a dedicated FortiSOAR device or V
D. It does not include a limited trial by default.

Answer: C

Explanation:

The FortiSOAR management extension is designed as an independent security orchestration, automation, and response (SOAR) solution that integrates with other Fortinet products but requires its own dedicated device or virtual machine (VM) environment. FortiSOAR is not natively integrated as a container or service within FortiAnalyzer or FortiManager, and it operates separately to manage complex security workflows and incident responses across various platforms.
Let's examine each option to determine the correct answer:
Option A: It requires a FortiManager configured to manage FortiGate
This is incorrect. FortiSOAR operates independently of FortiManager. While FortiSOAR can receive input or data from FortiGate (often managed by FortiManager), it does not require FortiManager to be part of its setup.
Option B: It runs as a docker container on FortiAnalyzer
This is incorrect. FortiSOAR does not run as a container within FortiAnalyzer. It requires its own dedicated environment, either as a physical device or a virtual machine, due to the resource requirements and specialized functions it performs.
Option C: It requires a dedicated FortiSOAR device or VM
This is correct. FortiSOAR is deployed as a standalone device or VM, which enables it to handle the intensive processing needed for orchestrating security operations, integrating with third-party tools, and automating responses across an organization's security infrastructure.
Option D: It does not include a limited trial by default
This is incorrect. FortiSOAR installations may come with trial options or demos in specific scenarios, especially for evaluation purposes. This depends on licensing and deployment policies.
Reference: The FortiSOAR platform, as outlined in Fortinet product documentation, is a standalone SOAR solution that requires a dedicated device or VM for deployment. It integrates with Fortinet's Security Fabric but operates separately from FortiAnalyzer, FortiManager, and FortiGate, focusing on advanced incident management and security automation.

NEW QUESTION 34
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 38
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 39
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 42
Refer to the exhibit.

```
FAZ # diagnose fortilogd lograte
last 5 seconds: 78.8, last 30 seconds: 132.1, last 60 seconds: 133.3

FAZ # diagnose fortilogd msgrate
last 5 seconds: 1.4, last 30 seconds: 1.6, last 60 seconds: 1.6
```

What can you conclude about the output?

A. The low indexing values require investigation.
B. The output is not ADOM specific.
C. There are more event logs thantraffic logs.
D. The log rate higher than the message rate is not normal.

Answer: D

NEW QUESTION 47
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 51
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 54
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

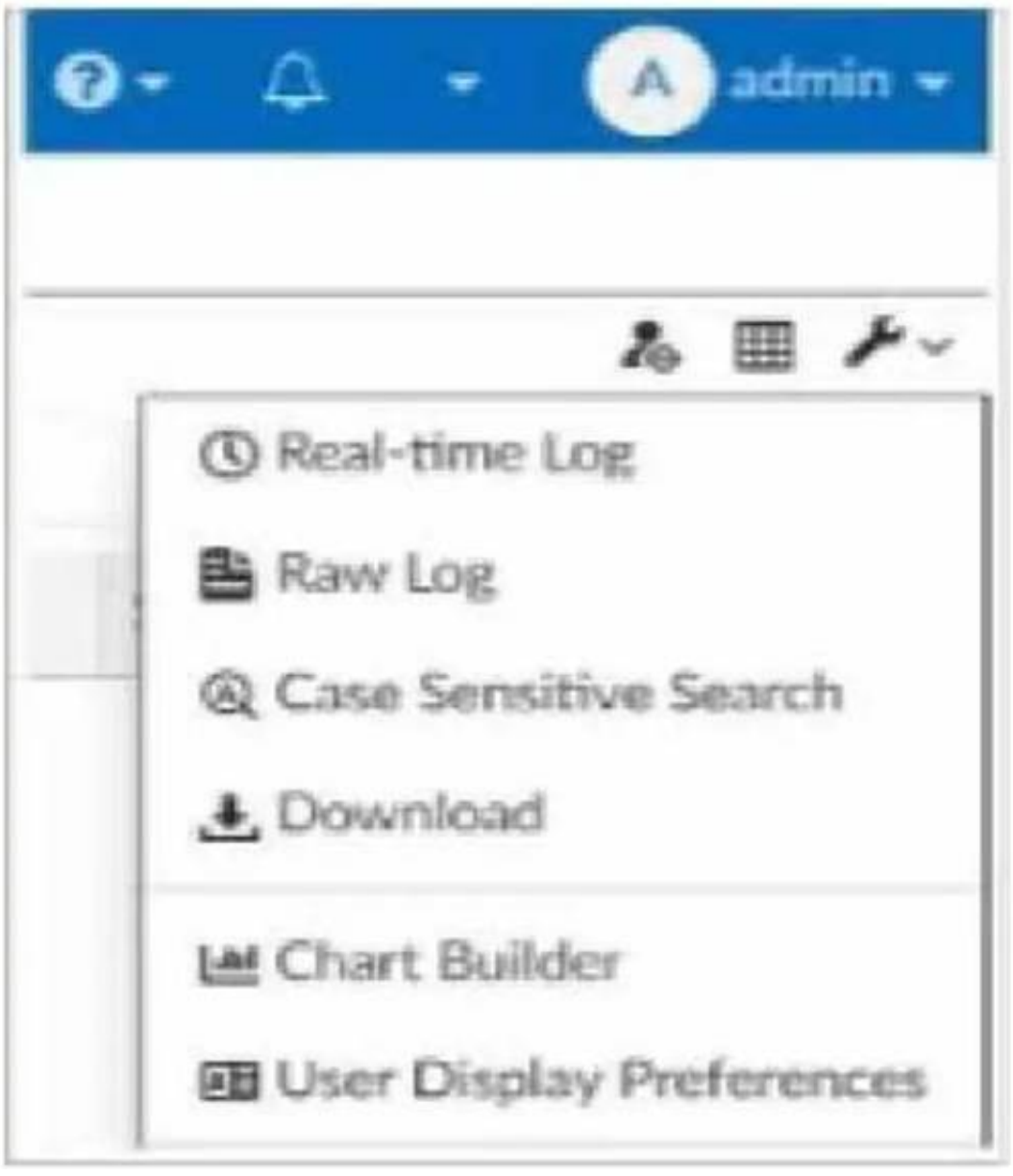
Explanation:
The exhibit shows a graph that tracks two metrics over time:Receive RateandInsert Rate. These two rates are crucial for understanding the log processing behavior in FortiAnalyzer.
Understanding Receive Rate and Insert Rate:
Receive Rate: This is the rate at which FortiAnalyzer is receiving 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 57
You are trying to configure a task in the playbook editor to run a report.
However, when you try to select the desired playbook, you do to see it listed.
What is the reason?

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

Answer: C

NEW QUESTION 62
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 63
Which two parameters does FortiAnalyzer use to identify an indicator of compromise (IOC)? (Choose two answers)

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

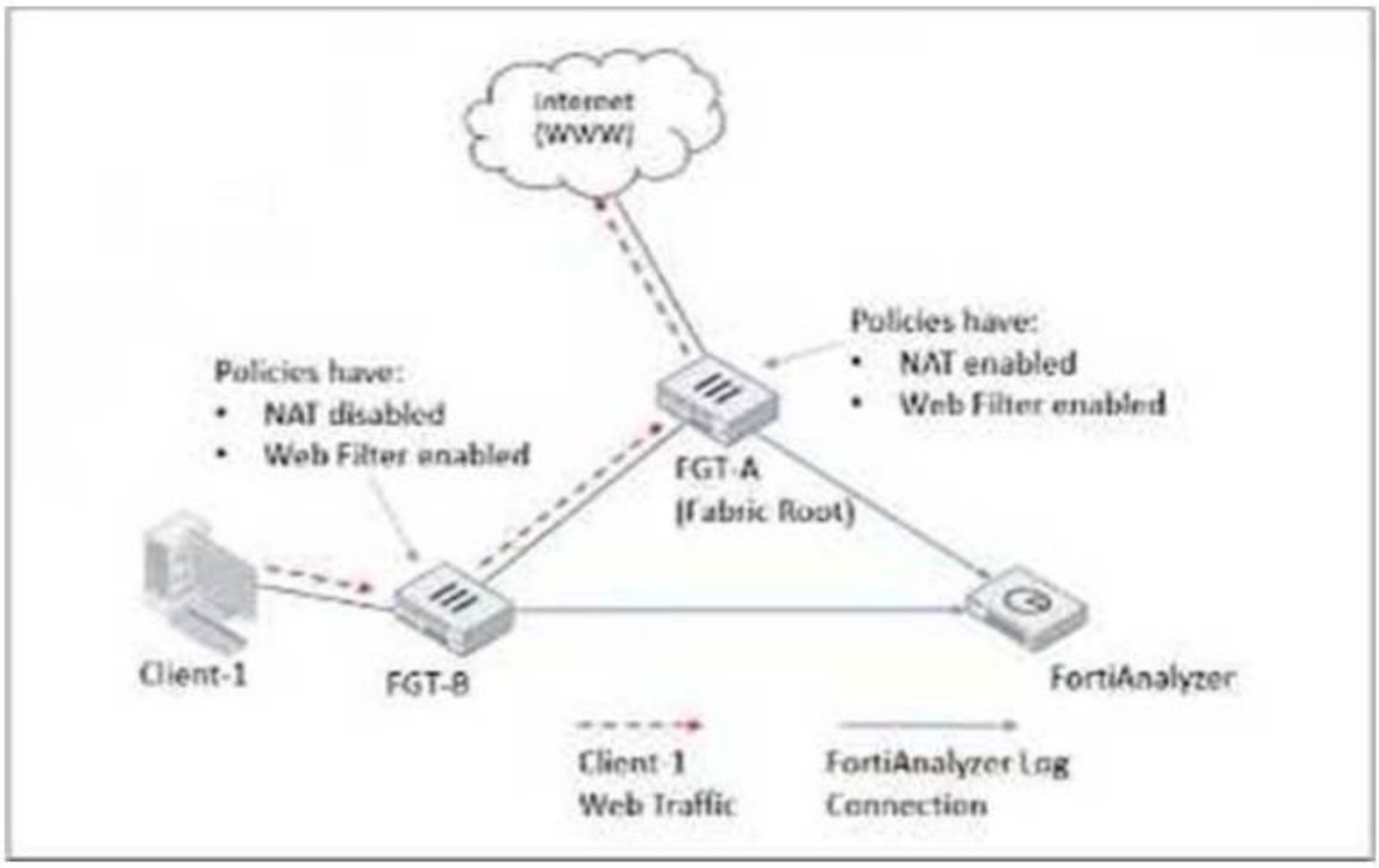
Answer: AB

NEW QUESTION 67
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 70
Refer to Exhibit:



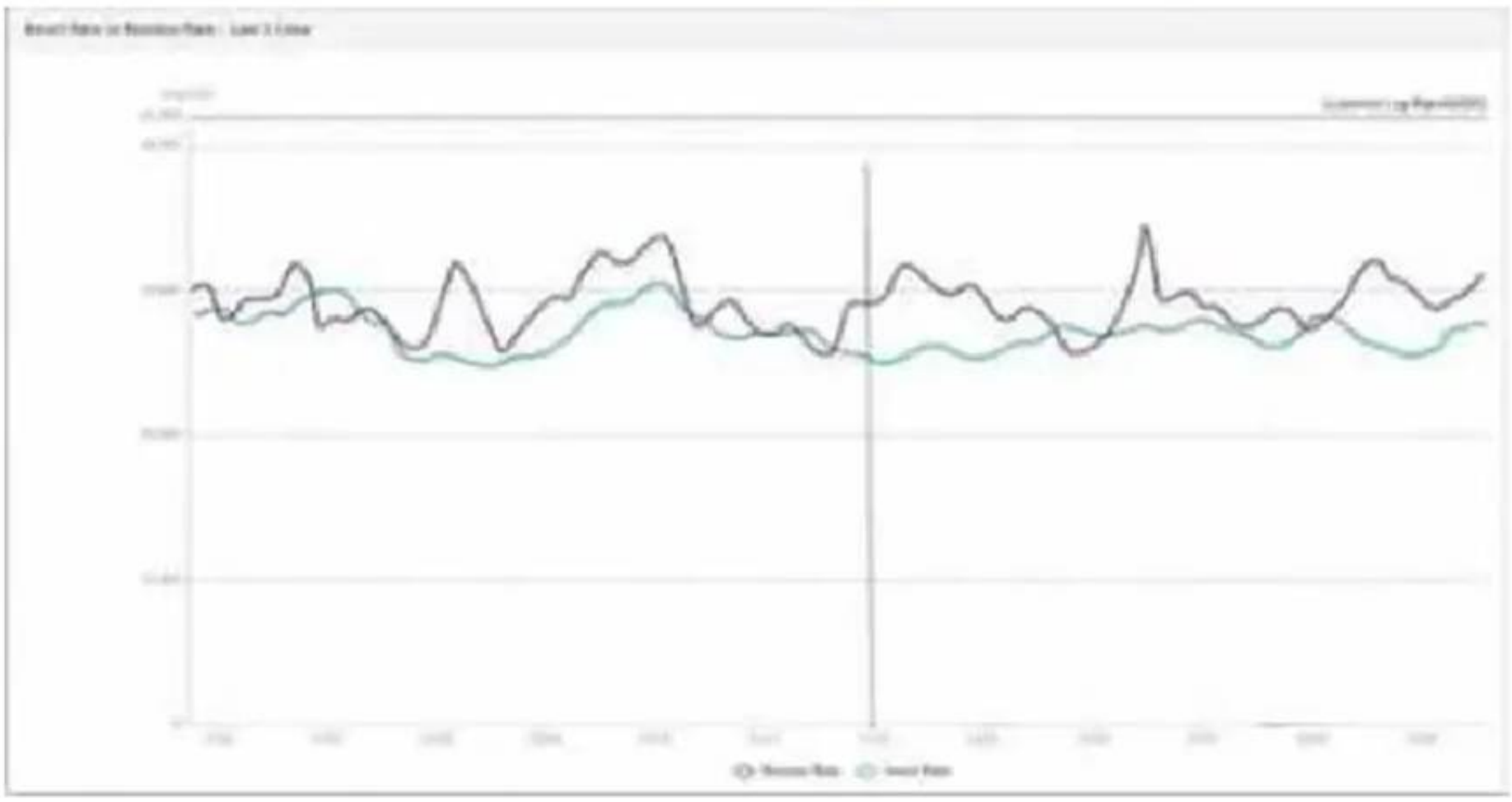
Client-1 is trying to access the internet for web browsing.
All FortiGate devices in the topology are part of a Security Fabric with logging to FortiAnalyzer configured. All firewall policies have logging enabled. All web filter profiles are configured to log only violations.
Which statement about the 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 74
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 77
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 78
A FortiAnalyzer device could use which security method to secure the transfer of log data from FortiGate devices?

A. SSL

B. IPSec
C. Direct serial connection
D. S/MIME

Answer: B

NEW QUESTION 80
.....

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