ATMIC NETWORKS
YOUR GUIDE TO GLOBAL CERTIFIATION

"Please note that these files may not be up to date. However, the questions will help you understand the exam format and typical question patterns."

www.atmicnetworks .com

Warning: Keep connected with our support team for latest updates

Question: 1

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."

Question: 2

Exhibit.

Which statement about the event displayed is correct?

A. The risk source is isolated.

B. The security risk was blocked or dropped.

C. The security event risk is considered open.

D. An incident was created from this event.

Answer: C

Explanation:

Question: 3

Which statement describes archive logs on FortiAnalyzer?

A. Logs that are indexed and stored in the SQL database

B. Logs a FortiAnalyzer administrator can access in FortiView

C. Logs compressed and saved in files with the .gz extension

D. Logs previously collected from devices that are ofline

Answer: C

Explanation:

In FortiAnalyzer, archive logs refer to logs that have been compressed and stored to save space. This process involves compressing the raw log files into the .gz format, which is a common compression format used in Fortinet systems for archived data. Archiving is essential in FortiAnalyzer to optimize storage and manage long-term retention of logs without impacting performance.

Let's examine each option for clarity:

Option A: Logs that are indexed and stored in the SQL database

This is incorrect. While some logs are indexed and stored in an SQL database for quick access and searchability, these are not classified as archive logs. Archived logs are typically moved out of the database and compressed.

Option B: Logs a FortiAnalyzer administrator can access in FortiView

This is incorrect because FortiView primarily accesses logs that are active and indexed, not archived logs. Archived logs are stored for long-term retention but are not readily available for immediate analysis in FortiView.

Option C: Logs compressed and saved in files with the .gz extension

This is correct. Archive logs on FortiAnalyzer are stored in compressed .gz files to reduce space usage. This archived format is used for logs that are no longer immediately needed in the SQL database but are retained for historical or compliance purposes.

Option D: Logs previously collected from devices that are ofline

This is incorrect. Although archived logs may include data from devices that are no longer online, this is not a defining characteristic of archive logs.

Reference: FortiAnalyzer 7.4.1 documentation and configuration guides outline that archived logs are stored in compressed files with the .gz extension to conserve storage space, ensuring FortiAnalyzer can handle a larger volume of logs over extended periods.

Question: 4

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 notifications can 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.

Reference: 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.

Question: 5

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 VM.

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.

Question: 6

Exhibit.

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 (admmode: 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.

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.

Question: 8

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.

Question: 9

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.

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.

Question: 11

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

A. FortiAnalyzer needs that time to parse the new playbook.

B. FortiAnalyzer needs that time to debug the new playbook.

C. FortiAnalyzer needs that time to back up the current playbooks.

D. FortiAnalyzer needs that time to ensure there are no other playbooks running.

Answer: A

Explanation:

When a new playbook is created on FortiAnalyzer, the system requires some time to parse and validate the 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.

Reference: 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.

Question: 12

Exhibit.

```
tAZ f diagnose; fortl le>qd Inqratt
laaL 5 suc-onds: U.l, IBBL 30 scccnass 132.1* lasl cJ auconass 133.3

FAZ J dlajtLQBu fuxlllugd nayiBLe lagt ■ 3B OBdB? -4* l*nt 30 fj^condas ..0, lunt GO neccmd.n;        .»'
```

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 Answe r: A. The message rate being lower than the log rate is normal.

This aligns with the normal 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.

Reference:

FortiOS 7.4.1 and FortiAnalyzer 7.4.1 command guides for diagnose fortilogd lograte and diagnose fortilogd msgrate.

Question: 13

Exhibit.

SQL query

SQL Schema

fable 'LOfi' has the (D11MIII(fields:

14, bid» dvid, itUe, 4tUe» euld* epid, dsteuld, dstcpld, laffUg* hew* Usid, type, subtype* level* eel lon. wtauution* policyid. scssioold. snip* ds lip, trenip. triftsip, sreport. dstport, venport, transport* Iran (lisp, dUfethMi, proto, tri, slot* sell tbyte, revdbyte, sent delta, 'cvcMella, senlpit rcvdpkt, logid, user, wiauthusrr, dstMnauthuse* , srcname, dslnaar, group, service, upp* appeal* fetusd, wcinifrale, dsliutfcdej preserver, dstserver*

SQL Qu*ry

Results

I Vw^r P	Omonmw fa
I MULUO	443
I 1AAU0	III
I iso on	n
I IOJOI SO	BI
I 10A1 JO	21

A fortiAnalyzer analyst is customizing a SQL query to use in a report.

Which SQL query should the analyst run to get the expected results?

A)

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

B)

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

C)

r,""T -: t *t~S*, "5 I : ■-", :-r_ ■ ',5 ""■.•- i,.t) - :"
Cries BY mpiut oesc irwi BY :xvip, isvpcrt
75.C3 flog
»-M Bfilter MW ^.ip - '10.0. .IC

D)

SELECT sicif AS •flCIUW IF*, dslfoll AS *tteeUl>»Usr. Bort"
5Ti.CS flog
KSttt Stllxt-x ASO axels - ' 10. J.1.1C
egtlOT HY -"C'l^ 4srp"rr ;.-.::•',>• hv Isttiv u'Ml

A. Option A

B. Option B

C. Option C

D. Option D

Answer: A

Explanation:

The requirement here is to construct a SQL query that retrieves logs with specific fields, namely "Source IP" and "Destination Port," for entries where the source IP address matches 10.0.1.10. The correct syntax is essential for selecting, filtering, ordering, and grouping the results as shown in the expected outcome.

Analysis of the Options:

Option A

SELECT srcip AS "Source IP", dstport AS "Destination Port": This syntax selects srcip and dstport, renaming them to "Source IP" and "Destination Port" respectively in the output.

FROM $log: Specifies the log table as the data source.

WHERE $filter AND srcip = '10.0.1.10': This line filters logs to only include entries with srcip equal to 10.0.1.10.

ORDER BY dstport DESC: Orders the results in descending order by dstport.

GROUP BY srcip, dstport: Groups results by srcip and dstport, which is valid SQL syntax.

This option meets all the requirements to get the expected results accurately.

Option B

WHERE $filter AND Source IP != '10.0.1.10': Uses != instead of =. This would exclude logs from the specified IP 10.0.1.10, which is contrary to the expected result.

Option C

The ORDER BY clause appears before the FROM clause, which is incorrect syntax. SQL requires the FROM clause to follow the SELECT clause directly.

Option D

The GROUP BY clause should follow the FROM clause. However, here, it's located after WHERE, making it syntactically incorrect.

Conclusion:

Correct Answe r: A. Option A

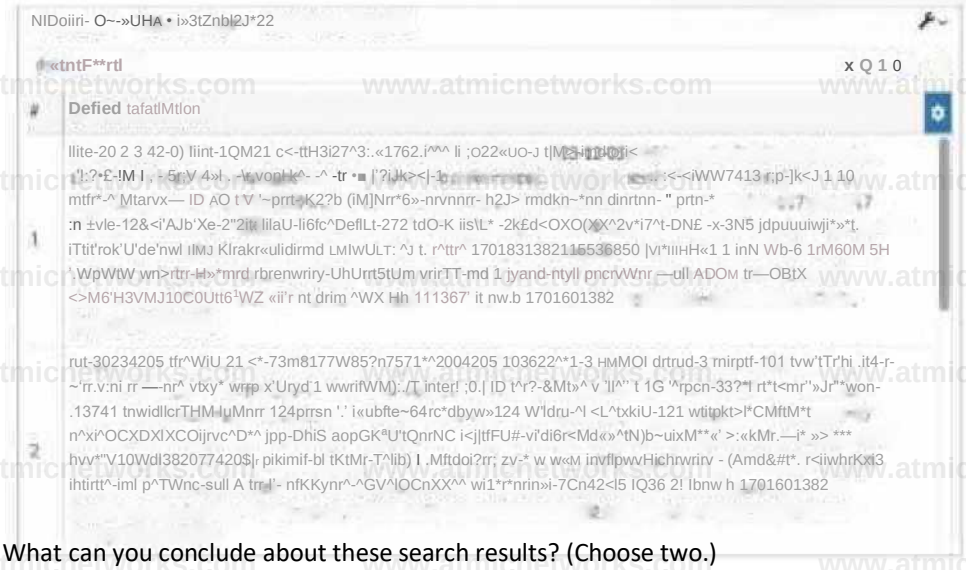
This option aligns perfectly with standard SQL syntax and filters correctly for srcip = '10.0.1.10', while ordering and grouping as required.

Reference:

FortiAnalyzer 7.4.1 SQL query capabilities and syntax for report customization.

Question: 14

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: A, D

Explanation:

Question: 15

Exhibit.

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

Explanation:

Question: 16

Exhibit.

Playbook Editor

Get Event task configuration

FortiAnalyzer Event Monitor

Assume these are all the events that exist on the FortiAnalyzer device.

How many events will be added to the incident created after running this playbook?

A. Eleven events will be added.

B. Seven events will be added

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 are four distinct events:

Two from the "Severity = High" filter.

One from the "Event Type = Web Filter" filter.

One from the "Tag = Malware" filter.

Conclusion:

Correct Answe r: 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.

Reference:

FortiAnalyzer 7.4.1 documentation on event filtering, playbook configuration, and incident management criteria.

Question: 17

Which statement about SQL SELECT queries is true?

A. They can be used to purge log entries from the database.

B. They must be followed immediately by a WHERE clause.

C. They can be used to display the database schema.

D. They are not used in macros.

Answer: D

Explanation:

Option A - Purging Log Entries:

A SELECT query in SQL is used to retrieve data from a database and does not have the capability to delete or purge log entries. Purging logs typically requires a DELETE or TRUNCATE command.

Conclusion: Incorrect.

Option B - WHERE Clause Requirement:

In SQL, a SELECT query does not require a WHERE clause. The WHERE clause is optional and is used only when filtering results. A SELECT query can be executed without it, meaning this statement is false.

Conclusion: Incorrect.

Option C - Displaying Database Schema:

A SELECT query retrieves data from specified tables, but it is not used to display the structure or schema of the database. Commands like DESCRIBE, SHOW TABLES, or SHOW COLUMNS are typically used to view schema information.

Conclusion: Incorrect.

Option D - Usage in Macros:

FortiAnalyzer and similar systems often use macros for automated functions or specific query-based tasks. SELECT queries are typically not included in macros because macros focus on procedural or repetitive actions, rather than simple data retrieval.

Conclusion: Correct.

Conclusion:

Correct Answe r: D. They are not used in macros.

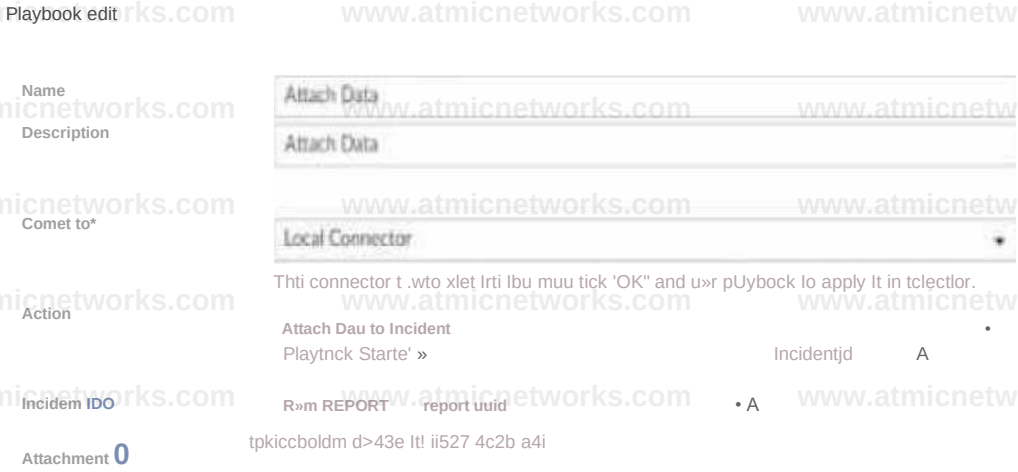
This aligns with typical SQL usage and the specific functionalities of FortiAnalyzer.

Reference:

FortiAnalyzer 7.4.1 documentation on SQL queries, database operations, and macro usage.

Question: 18

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 Answe r: 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.

Question: 19

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

A. FortiView Monitor

B. Outbreak alert services

C. Incidents dashboard

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 Answe r: D. Threat hunting

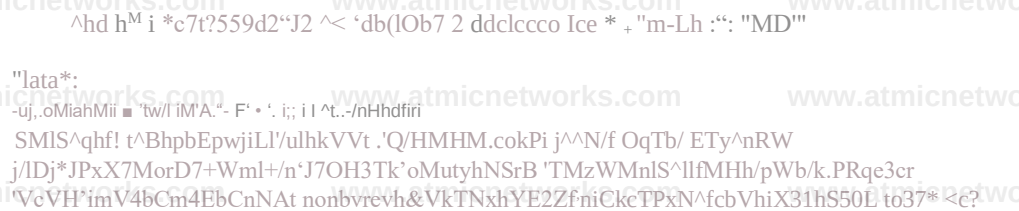
Threat hunting is the most proactive feature among the options, as it involves actively searching for threats within the network rather than reacting to already detected incidents.

Reference:

FortiAnalyzer 7.4.1 documentation on Threat Hunting and proactive security measures.

Question: 20

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 Answe r: 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.

Reference:

FortiAnalyzer 7.4.1 documentation on exporting playbooks and data compression methods.

Question: 21

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 save considerable 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 Answe r: B. Configure a custom view.

Custom views allow you to save specific search filters, enabling quick access to frequently used parameters in Log View.

Reference:

FortiAnalyzer 7.4.1 documentation on creating and using custom views for log searches.

Question: 22

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 a mailto:<email address> 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 and content 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 Answe r: 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.

Reference:

FortiAnalyzer 7.4.1 documentation on configuring output profiles and report distribution settings.

Question: 23

Which statement regarding macros on FortiAnalyzer is true?

A. Macros are predefined templates for reports and cannot be customized.

B. Macros are useful in generating excel log files automatically based on the report settings.

C. Macros are ADOM-specific and each ADOM type have unique macros relevant to that ADOM.

D. Macros are supported only on the FortiGate ADOMs.

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 Answe r: 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.

Reference:

FortiAnalyzer 7.4.1 documentation on macros and report generation functionalities.

Question: 24

After a generated a repot, you notice the information you were expecting to see in 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: A, D

Explanation:

When a generated report does not include the expected information despite the logs being present, there are several factors to check to ensure accurate data representation in the report.

Option A - Check the Time Frame Covered by the Report:

Reports are generated based on a specified time frame. If the time frame does not encompass the period when the relevant logs were collected, those logs will not appear in the report. Ensuring the time frame is correctly set to cover the intended logs is crucial for accurate report content.

Conclusion: Correct.

Option B - Disable Auto-Cache:

Auto-cache is a feature in FortiAnalyzer that helps optimize report generation by using cached data for frequently used datasets. Disabling auto-cache is generally not necessary unless there is an issue with outdated data being used. In most cases, it does not directly impact whether certain logs are included in a report.

Conclusion: Incorrect.

Option C - Increase the Report Utilization Quota:

The report utilization quota controls the resource limits for generating reports. While insufficient quota might prevent a report from generating or completing, it does not typically cause specific log entries to be missing. Therefore, this option is not directly relevant to missing data within the report.

Conclusion: Incorrect.

Option D - Test the Dataset:

Datasets in FortiAnalyzer define which logs and fields are pulled into the report. If a dataset is misconfigured, it could exclude certain logs. Testing the dataset helps verify that the correct data is being pulled and that all required logs are included in the report parameters.

Conclusion: Correct.

Conclusion:

Correct Answe r: A. Check the time frame covered by the report and D. Test the dataset.

These actions directly address the issues that could cause missing information in a report when logs are available but not displayed.

Reference:

FortiAnalyzer 7.4.1 documentation on report generation settings, time frames, and dataset configuration.

Question: 25

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.

A. Check the time frame covered by the report.

B. Disable auto-cache.

C. Increase the report utilization quota.

D. Test the dataset

Answer: A, D

Explanation:

When a generated report does not contain the expected information even though the logs are confirmed to be present, it typically indicates an issue 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 autocache 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 Answe r: A. Check the time frame covered by the report and D. 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.

Reference:

FortiAnalyzer 7.4.1 documentation on report generation settings, time frames, and dataset configuration for accurate report results.

Question: 26

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: B, D

Explanation:

FortiAnalyzer has two primary operating modes: Analyzer mode and Collector 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, which would set it to Analyzer mode. Collector mode prioritizes log collection and storage rather than analysis, ofloading 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 Answe r: B. FortiAnalyzer runs in collector mode by default unless it is configured for HA and D. 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.

Reference:

FortiAnalyzer 7.4.1 documentation on operating modes (Collector and Analyzer) and their respective capabilities.

Question: 27

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 be deleted.

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 and preventing similar false positives in the future. Deletion would typically only occur manually 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 the status of the incident is updated. This identifier remains constant throughout the incident's lifecycle for tracking and reference purposes.

Conclusion: Incorrect.

Conclusion:

Correct Answe r: 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.

Reference:

FortiAnalyzer 7.4.1 documentation on incident management and audit history logging.

Question: 28

Which two statements about local logs on FortiAnalyzer are true? (Choose two.)

A. They are not supported in FortiView.

B. You can view playbook logs for all ADOMs in the root ADOM.

C. Event logs show system-wide information, whereas application logs are ADOM specific.

D. Event logs are available only in the root ADOM.

Answer: BC

Explanation:

FortiAnalyzer manages and stores various types of logs, including local logs, across different ADOMs (Administrative Domains). Each type of log serves specific purposes, with some logs being ADOM- specific and others providing system-wide information.

Option A - Local Logs Not Supported in FortiView:

Local logs are indeed supported in FortiView. FortiView provides visibility and analytics for different log types across the system, including local logs, allowing users to view and analyze data efficiently.

Conclusion: Incorrect.

Option B - Playbook Logs for All ADOMs in the Root ADOM:

FortiAnalyzer allows centralized viewing of playbook logs across all ADOMs from the root ADOM. This feature provides an overarching view of playbook executions, facilitating easier monitoring and management for administrators.

Conclusion: Correct.

Option C - Event Logs vs. Application Logs:

Event Logs provide information about system-wide events, such as login attempts, configuration changes, and other critical activities that impact the overall system. These logs apply across the FortiAnalyzer instance.

Application Logs are more specific to individual ADOMs, capturing details that pertain to ADOM- specific applications and configurations.

Conclusion: Correct.

Option D - Event Logs Only in Root ADOM:

Event logs are available across different ADOMs, not exclusively in the root ADOM. They capture system-wide events, but they can be accessed within specific ADOM contexts as needed.

Conclusion: Incorrect.

Conclusion:

Correct Answe r: B. You can view playbook logs for all ADOMs in the root ADOM and C. Event logs show system-wide information, whereas application logs are ADOM specific.

These answers correctly describe the characteristics and visibility of local logs within FortiAnalyzer.

Reference:

FortiAnalyzer 7.4.1 documentation on log types, ADOM configuration, and FortiView functionality.

Question: 29

Refer to Exhibit:

I »K« Kale **» Hvjr*^ RMi Usl 1 H)w*

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 Rate and Insert 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, the Insert Rate line is above the Receive Rate line, 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 Answe r: 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.

Reference:

FortiAnalyzer 7.4.1 documentation on log processing metrics, Receive Rate, and Insert Rate indicators.

Question: 30

A playbook 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 is marked as Success.

Status When Some Tasks Fail:

If one or more tasks in the playbook fail, but others succeed, the playbook status generally changes to Attention

required. This status indicates that the playbook completed execution but requires review due to one or more tasks failing.

This is different from a complete Failed status, 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 Answe r: A. Attention required

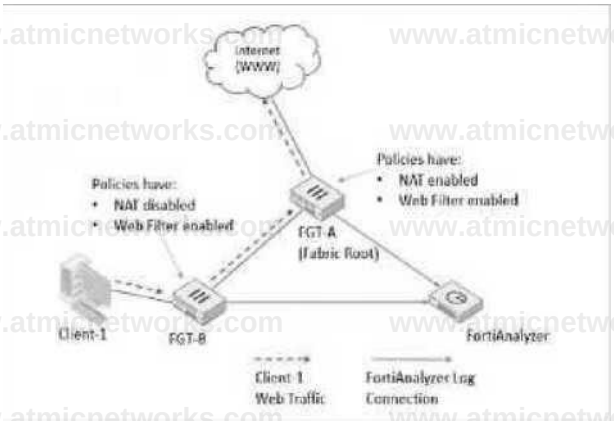
The playbook status reflects that it completed, but an error occurred in one of the tasks, prompting the administrator to review the failed task.

Reference:

FortiAnalyzer 7.4.1 documentation on playbook execution statuses and task error handling.

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 duplicated across 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 to log 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 the upstream FortiGate (FGT-A). Therefore, only FGT-A will create web filter logs if it detects a violation (Option D).

Question: 32

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:

Enabling auto-cache in 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 data from 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 of the 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 Answe r: A. The generation time for reports is decreased and C. 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.

Reference:

FortiAnalyzer 7.4.1 documentation on report caching, auto-cache functionality, and report generation optimizations.

Question: 33

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 status sqlreportd 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 the hcache (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 the hcache status.

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 Answe r: 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.

Reference:

FortiAnalyzer 7.4.1 documentation on SQL diagnostic commands, particularly those related to reporting (sqlreportd) and caching mechanisms.

Question: 34

Refer to the exhibit.

```
FAZ * diagnose fortilogd lograte
last 5 seconds:  78.8, last 30 seconds; 132     .1, last 60 seconds: 133.3

FAZ 1 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 than traffic logs.

D. The log rate higher than the message rate is not normal.

Answer: D

Explanation:

Question: 35

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

Explanation:

Question: 36

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

Explanation:

Question: 37

Which statement correctly describes one Difference between templates and reports?

A. Reports provide mora configuration options than templates

B. Templates can be cloned, but reports cannot be cloned.

C. Reports support macros, but templates do not.

D. Template are mapped to device groups. while reports are mapped to ADOMs

Answer: D

Explanation:

Question: 38

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

Explanation:

Question: 39

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 generate reports 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

Explanation:

Question: 40

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: B, C

Explanation:

Question: 41

You must find a specific security event log in the FortiAnalyzer logs displayed in FortiView, but, so far, you have been uncuccessful.

Which two tasks should you perform to investigate why you are having this issue? (Choose two.)

A. Open .gz log files in FortiView.

B. Rebuild the SQL database and check FortiView.

C. Review the ADOM data policy

D. Check logs in the Log Browse

Answer: A, B

Explanation:

Question: 42

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: A, B

Explanation:

Question: 43

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: A, B

Explanation:

Question: 44

Which two statements about exporting and importing playbacks are true? (Choose two.)

A. A playbook that was disabled when it was exported mil be disabled when it is imported.

B. Playbooks can so imported 10 a different FortiAnayzer device, but only if the connectors already exist

C. You can import a playbook even if there is another one win the same name in the destination

D. You can export only one playbook at a time.

Answer: A, B

Explanation:

Question: 45

You are tasked with finding logs corresponding to a suspected attack on your network.

You need to use an interface where all identified threats within timeframe are listed and organized.
You also need to be able to quickly export the information to a PDF file.

Where can you go to accomplish this task?

A. Log Browse

B. Log View

C. Fabric View

D. FortiView

Answer: B

Explanation:

Question: 46

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

Explanation:

Question: 47

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 applied simultaneously to all event handlers.

Answer: C

Explanation:

Question: 48

You need to move reports between two ADOMs.

Which two statements are true? (Choose two.)

A. The ADOMs must be compatible types.

B. The date and time will be appended to the original report name to avoid conflicts.

C. All charts and datasets associated with the report will be imported together.

D. You need to convert the reports into templates first.

Answer: A, C

Explanation:

Comprehensive and Detailed Explanation From Exact Extract of knowledge of FortiAnalyzer 7.6 Study guide documents:

FortiAnalyzer supports moving reporting content across ADOMs by importing/exporting reporting objects, but it enforces ADOM compatibility. The study guide states: "You can, however, import and export reports and charts … into different ADOMs …" and explicitly requires that "Both ADOMs must be of the same type." This directly validates statement A.

For report dependencies, the study guide clarifies how datasets are handled during transfer. While "You can't export templates and datasets," it also explains that when you export a chart, "the associated dataset is exported with it, so when you import an exported chart, the associated dataset is imported as well." Since reports are composed of charts (and charts depend on datasets), moving a report between ADOMs entails moving its charts; when those charts are exported/imported, their datasets come with them. This supports statement C based on the documented chart→dataset import/export behavior.

Statement D is not required because the study guide explicitly indicates you can "export and import reports" directly, and additionally notes that on import "you can save the layout of the report as a template" (optional, not a prerequisite).

Question: 49

Which statement about exporting items in Report Definitions is true?

A. Templates can be exported.

B. Template exports contain associated charts and datasets.

C. Chart exports contain associated datasets.

D. Datasets can be exported.

Answer: C

Explanation:

Question: 50

Which log will generate an event with the status Contained?

A. An AV log with action=quarantine.

B. An IPS log with action=pass.

C. A WebFilter log will action=dropped.

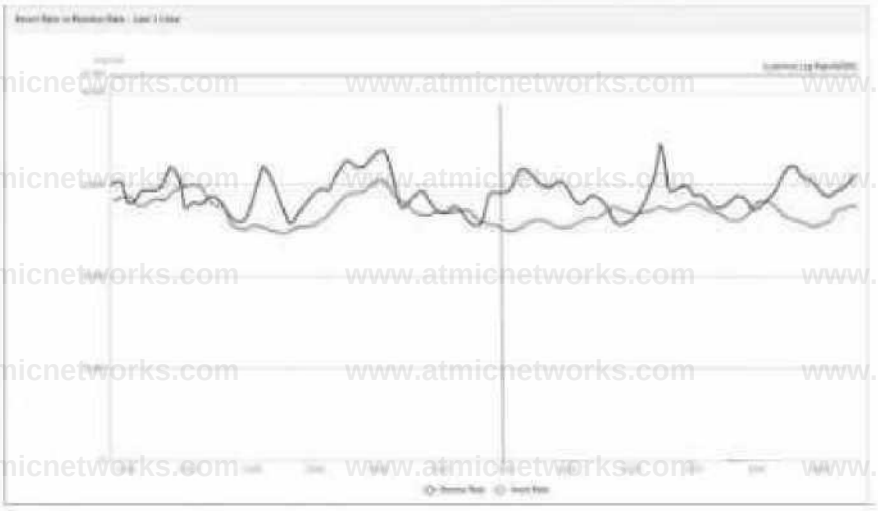
D. An AppControl log with action=blocked.

Answer: A

Explanation:

Question: 51

Exhibit.



What does the data point at 12:20 indicate?

A. The log insert 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

Explanation:

Question: 52

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

Explanation:

Question: 53

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

Explanation:

Question: 54

What happens when the indicator of compromise (IOC) engine on FortiAnalyzer finds web logs that match blacklisted IP addresses?

A. FortiAnalyzer flags the associated host for further analysis.

B. A new infected entry is added for the corresponding endpoint under Compromised Hosts.

C. The detection engine classifies those logs as Suspicious.

D. The endpoint is marked as Compromised and, optionally, can be put in quarantine.

Answer: B

Explanation:

Question: 55

(When there are no matching parsers for a device log, what does FortiAnalyzer do? (Choose one answer))

A. Drops the log

B. Applies the generic SYSLOG parser

C. Stores the log but doesn't normalize it

D. Archives the log for future analysis

Answer: C

Explanation:

Comprehensive and Detailed Explanation From Exact Extract of knowledge of FortiAnalyzer 7.6 Study guide documents:

FortiAnalyzer's ingestion pipeline does not "drop" logs simply because a parser is unavailable. The study guide states that when devices send logs, "Logs received are decompressed and saved in a log

file on the FortiAnalyzer disk" (with a .log extension). This establishes that the raw log is still accepted and

stored on disk as part of the normal workflow.

Normalization, however, depends on having a suitable parser. The study guide explains that "FortiAnalyzer uses predefined parsers to extract key fields from ingested logs and maps them to a consistent, standardized set of field names." It further emphasizes that "Log parsers … are central to log normalization" because they convert unstructured/native logs into a standardized schema.

Therefore, if no matching parser exists for a given device log, FortiAnalyzer can still store the incoming log (it is received, decompressed, and written to disk), but it cannot perform the "extract key fields" and "map to standardized field names" steps required for normalization. In practical terms, the log remains in its native/unstructured form (not normalized), which aligns exactly with option C.

Question: 56

(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: A, B

Explanation:

Comprehensive and Detailed Explanation From Exact Extract of knowledge of FortiAnalyzer 7.6 Study guide documents:

The FortiAnalyzer study guide explains that IOC identification is performed by comparing relevant log fields against the FortiGuard threat database. Specifically, it states: "Depending on the log type, FortiAnalyzer identifies possible compromised hosts by checking the threat database against the log's IP address, domain, and URL."

From this extract, two of the explicit parameters FortiAnalyzer uses for IOC detection are IP address and URL (both listed verbatim). Policy ID and application category are not part of the IOC matching parameters described for threat-database checks in this context.

This is further consistent with the study guide's definition of indicator types, which states: "There are three types of indicators: IP addresses, URLs, and domains."

Question: 57

(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: C, D, E

Explanation:

Comprehensive and Detailed Explanation From Exact Extract of knowledge of FortiAnalyzer 7.6 Study guide documents:

The study guide explicitly describes what content from Fabric members is visible/usable on the Fabric supervisor:

Logs: “In the FortiAnalyzer Fabric supervisor, Log View displays logs collected on all FortiAnalyzer Fabric members.”

Reports: “For reports, the FortiAnalyzer Fabric supervisor can fetch and aggregate data from multiple members in 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 out Playbooks as a supervisor capability over members: “You are not able to perform configuration changes or to run automation playbooks from the Fabric supervisor to members.”

Therefore, the three modules available for analysis on the supervisor are Logs, Events, and Reports (C, D, E).

Question: 58

(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:

Comprehensive and Detailed 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 is Incoming 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.

Question: 59

(Refer to the exhibit.

adoa_oid«198 itiae-2025-95 27 98:35:24 loguid-7509149554218893312 epid-3 euid-3 det ajiarsernaae-Fort iGate Log Parser data_soorceid-FGVM92TM24013423 data_sourcma«e=HQ-WiFW-1 root data^sourcetype-FortiGate data^tiaestaep'1748334923 app_cat=unscanned *pp_na*e=MTP app_service=HTP dst^intf«port2(undefined) dst_ip=208.91.112.63 dst_port=123 event_action=accept event_id=13 eventj»licy=3 event_ref=751261e0 ee9e-Sleffl2e a382acaf 16d6 event severity=notice eventsubtyp^forward event_type=traffic host_location=R«served bost_owner=fortinet .con net_proto=17 net_rcvdpkts-1 net_rcvbytes-76 net_sentbytes=76 net_sentpkts=l net sejsionduration*180 net_sessio<iid= 1357 »r<:_iritf*p<3rt6(undefined) srt_ip-10.0.13.125 src_natip=190,65.0.101 src_natport*50403 src_port =50403 dstepid=101 dsteuid=3 dst_geo_country=United States event_creation_tiM:27800868 event_uuid-0000000013 $r<_geo_country=Reserved logflag=l data_sourcedo«=rpot dst_intf_rcle=undefined event policyidg3 event policytype=policy src intf role=undefined itiee t=1748360124 logMeta=undefined

Which two observations can you make after reviewing this log entry? (Choose two answers))

A. This is a normalized log.
B. This is a formatted view of the log.
C. This is the original log that FortiAnalyzer received from FortiGate.
D. This log is in a raw log format.

Answer: A, D

Explanation:

Comprehensive and Detailed Explanation From Exact Extract of knowledge of FortiAnalyzer 7.6 Study guide documents:

The exhibit shows the log as a single-line key/value entry (not a columnar/table display), which aligns with FortiAnalyzer's raw log format view option. The study guide states: "You can toggle between viewing formatted and raw logs." This directly supports observation D.

At the same time, what you are viewing in FortiAnalyzer Log View is normalized data (FortiAnalyzer parses and maps device logs into standardized fields for consistent searching and analysis). The study guide explicitly states: "The log view allows you to view all log types received by FortiAnalyzer in normalized log format." It also explains that FortiAnalyzer "uses predefined parsers to extract key fields from ingested logs and maps them to a consistent, standardized set of field names," then
stores them as normalized logs in the SIEM database. This supports observation A.

Finally, the study guide clarifies that even when you switch to raw log format in FortiAnalyzer, you are still observing the normalized-field representation produced by FortiAnalyzer's parser/normalization process (rather than the untouched original device message). It notes that a FortiGate event log "has been normalized by FortiAnalyzer," and when you switch "to raw log format," you can observe the effect of normalization on common fields. This is why C is not the best description for the exhibit.

Question: 60

What are the two methods you can use to send notifications when an event is generated by an event handler? (Choose two answers)

A. Send SNMP trap.
B. Send an alert through the FortiGuard server.
C. Send an alert through Fabric connectors.
D. Send SMS notification

Answer: A, C

Explanation:

Comprehensive and Detailed Explanation From Exact Extract of knowledge of FortiAnalyzer 7.6 Study guide documents:

FortiAnalyzer event handlers support alerting when a rule match generates an event. The study guide states that, for an event handler, "You can select a notification profile to send alerts whenever an event is generated by the handler." In FortiAnalyzer, notification profiles are the mechanism used to deliver alerts outward (for example, via an SNMP trap), which directly aligns with option A.

In addition, FortiAnalyzer supports sending notifications to external platforms through integrations: "You can configure FortiAnalyzer to send a notification to external platforms using preconfigured Fabric connectors." This validates the use of Fabric connectors as a notification delivery method, aligning with option C.

Option B is not a notification delivery method for event-handler-generated alerts in the workflow described (FortiGuard is used for threat intelligence/enrichment rather than relaying alerts). Option D is not presented in the study guide's described notification mechanisms for event-handler alerting in the referenced sections.

Question: 61

(An analyst is using FortiAI on FortiAnalyzer to simplify certain tasks but is worried about exceeding the monthly token limit. Which query will take the fewest FortiAI tokens? (Choose one answer))

A. Show logs for 192.168.1.10 (past week)
B. Show all logs from the past week
C. Can you show me all the log entries for the endpoint 192.168.1.10?
D. Show logs for 192.168.1.10

Answer: A

Explanation:

Comprehensive and Detailed Explanation From Exact Extract of knowledge of FortiAnalyzer 7.6 Study guide documents:

The study guide explains that FortiAI token usage includes both the prompt (input) and the response (output), and that "generally, more text in the query and response results in using more tokens." It provides two comparison

examples and concludes that the more verbose request for “all the log entries” consumes more tokens because it has more text and also triggers a larger response; whereas limiting the query to a time range (for example, “(past week)”) reduces output volume and therefore token usage.

Applying that guidance to the options:

C is the most verbose and explicitly requests “all the log entries,” which drives higher input and output token usage.

B requests “all logs” for the week (broad scope), which typically increases output tokens.

D is short, but it does not constrain the time range, which can increase the response size (output tokens).

A is concise and includes a time constraint “(past week),” matching the study guide’s example of a lower-token query pattern.

Question: 62

(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: B, C

Explanation:

Comprehensive and Detailed 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).

Question: 63

(Refer to the exhibit.

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

A. The security risk was dropped.
B. The risk source is isolated.
C. The security risk was blocked.
D. 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 event Event Status = Mitigated and Event Type = Web Filter, with the event message indicating the web request was blocked.

The study guide defines Mitigated events 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 distinguishes Contained events from mitigated ones: “Contained: The risk source is isolated.” Since the exhibit clearly shows Mitigated (not Contained), option B is 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 is Web Filter, not application control, so option D is incorrect.

Therefore, the correct statement is C. The security risk was blocked.

Question: 64

(Refer to the exhibit.

	Eventt	Event Status -	Event Type J	Severity I
	0 56834764387462384.org (4)	Unhandled	OWeb 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, the Event Status shown is Unhandled (Event Type: Web Filter; Severity: Critical). The FortiAnalyzer study guide defines Unhandled events 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 option D.

The other options correspond to different statuses or actions:

Isolated/Contained applies when the risk source is isolated (status Contained), not Unhandled.
Escalated refers to events moved/raised for further action (status Escalated), not Unhandled.

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.

Question: 65

(How does FortiAnalyzer block indicators? (Choose one answer))

A. It uses an automation script to update FortiGate with the block list.
B. It uses a FortiManager connector to send the block list.
C. It uses a FortiClient EMS connector to send the block list.
D. It uses a webhook to allow FortiGate to send the block list.

Answer: B

Explanation:

Comprehensive and Detailed Explanation From Exact Extract of knowledge of FortiAnalyzer 7.6 Study guide

documents:

The FortiAnalyzer study guide states that blocking suspicious indicators is performed by integrating FortiAnalyzer with FortiManager (not by directly pushing a block list to FortiGate). Specifically: “To use this feature, you must set up an authorized FortiManager connector for the FortiAnalyzer on the Fabric Connector page of FortiAnalyzer.”

It then explains the backend mechanism: “In the back end, a playbook called Block_indicator runs every 5 minutes to send the information to FortiManager.” After a successful run, “the blocked indicator is pushed to the FortiManager External Resource list.” From there, FortiManager can create threat feeds/security profiles/policy blocks and push policies to FortiGate as needed—however, the study guide clarifies: “The Blocked status on FortiAnalyzer confirms that the list is updated on FortiManager, but it is not synced to FortiGate.”

Therefore, FortiAnalyzer blocks indicators by using a FortiManager connector and sending the block information to FortiManager (Option B).

Question: 66

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 a ClickHouse 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.