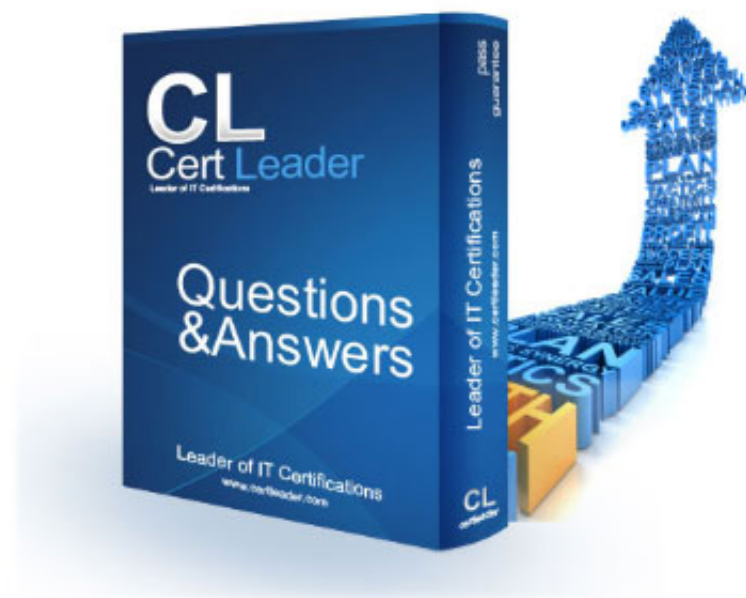


## FCP\_FAZ\_AN-7.6 Dumps

### Fortinet NSE 5 - FortiAnalyzer 7.6 Analyst

[https://www.certleader.com/FCP\\_FAZ\\_AN-7.6-dumps.html](https://www.certleader.com/FCP_FAZ_AN-7.6-dumps.html)



**NEW QUESTION 1**

What is the purpose of playbook trigger variables?

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

**Answer:** B

**NEW QUESTION 2**

Which statement about sending notifications with incident 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.

:According to FortiOS and FortiAnalyzer 7.4.1 documentation, notifications for incidents can be configured across various platforms by using multiple connectors, and they are not limited to email alone. This capability is part of the Fortinet Security Fabric, allowing for a broad range of integrations with external systems and platforms for effective incident response.

**NEW QUESTION 3**

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 Answer A. Attention required

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

References:

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

**NEW QUESTION 4**

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

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: AB

NEW QUESTION 5

Refer to the exhibit.

| <input type="checkbox"/> | Event ↕                                     | Event Status ↕ | Event Type ↕ | Severity ↕ |
|--------------------------|---------------------------------------------|----------------|--------------|------------|
| <input type="checkbox"/> | 56834764387462384.org (4)                   | Unhandled      | Web Filter   | Critical   |
| <input type="checkbox"/> | Web traffic to C&C from 10.0.1.200 detected | Unhandled      | Web Filter   | Critical   |

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

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

Answer: D

Explanation:

Comprehensive and Detailed Explanation: From Exact Extract of knowledge of FortiAnalyzer 7.6 Study guide documents:  
In the exhibit, theEvent Statusshown isUnhandled(Event Type: Web Filter; Severity: Critical). The FortiAnalyzer study guide definesUnhandledevents as events whose security risk has not been addressed and is therefore still active/open. Specifically, it states:??Unhandled: The security risk is considered open.?? This directly matches optionD.  
The other options correspond to different statuses or actions:  
\* Isolated/Containedapplies when the risk source is isolated (statusContained), notUnhandled.  
\* Escalatedrefers to events moved/raised for further action (statusEscalated), notUnhandled.  
\* Whether an incident was created cannot be concluded solely from the status ??Unhandled?? in the exhibit; the study guide ties incident creation to incident management workflows rather than equating ??Unhandled?? with an incident being created.

NEW QUESTION 6

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: AC

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 optionA.  
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 ofFabric connectorsas a notification delivery method, aligning with optionC.  
OptionBis 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). OptionDis not presented in the study guide??s described notification mechanisms for event-handler alerting in the referenced sections.

NEW QUESTION 7

Which two statement regarding the outbreak detection service are true? (Choose two.)

- A. An additional license is required.
- B. It automatically downloads new event handlers and reports.
- C. Outbreak alerts are available on the root ADOM only.
- D. New alerts are received by email.

Answer: BC

NEW QUESTION 8

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

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

Answer: AC

Explanation:

Enablingauto-cachein FortiAnalyzer reports is designed to improve the efficiency and speed of report generation by leveraging cached data. Let??s analyze each option to determine which effects are correct.  
\* Option A - The Generation Time for Reports is Decreased:

\* When auto-cache is enabled, FortiAnalyzer can use previously cached data instead of reprocessing all log 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 Answer 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.

References:

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

**NEW QUESTION 9**

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 if the playbook status is Failed, individual tasks may have succeeded.

**Answer:** AB

**NEW QUESTION 10**

Exhibit.

## Playbook Editor



## Get Event task configuration

Get Events ✕

Name

Get Events

Description

Get Events

Connector

Local Connector

Action

Get Events

Time Range

Click to select

Filter

Match All Conditions

Match Any Condition

| Field      | Match Criteria | Value      | Action                        |
|------------|----------------|------------|-------------------------------|
| Severity   | is             | High       | <span>✕</span> <span>+</span> |
| Event Type | is             | Web Filter | <span>✕</span> <span>+</span> |
| Tag        | is             | Malware    | <span>✕</span> <span>+</span> |

## FortiAnalyzer Event Monitor

| <input type="checkbox"/> | Event ID                                                         | Event Status ID | Event Type ID | Severity ID | Tags ID                    |
|--------------------------|------------------------------------------------------------------|-----------------|---------------|-------------|----------------------------|
| <input type="checkbox"/> | 224.141.83.77 (2)                                                | Unassigned      | ---           | Medium      |                            |
| <input type="checkbox"/> | Encrypted SSH Connection blocked from 178.10.199.186             | Assigned        | SSH           | Low         | Block SSH                  |
| <input type="checkbox"/> | SSH connection detected from 178.10.199.186                      | Unassigned      | SSH           | Medium      | Block SSH                  |
| <input type="checkbox"/> | SSH channel blocked from 178.10.199.186                          | Assigned        | SSH           | Low         | Block SSH                  |
| <input type="checkbox"/> | Host5 (1)                                                        | Assigned        | Web Filter    | Medium      | Block URL                  |
| <input type="checkbox"/> | IPv6 request for unknown destination from 178.10.199.186 blocked | Assigned        | Web Filter    | Medium      | Block URL                  |
| <input type="checkbox"/> | out Internet (1)                                                 | Unassigned      | IPS           | High        | Detect IP C&C              |
| <input type="checkbox"/> | Traffic to Internet (out Internet) from 178.10.199.186 blocked   | Unassigned      | IPS           | High        | Block IP C&C               |
| <input type="checkbox"/> | virus:MLA (2)                                                    | Assigned        | Antivirus     | Medium      |                            |
| <input type="checkbox"/> | Malware detected to 178.10.199.186 blocked                       | Assigned        | Antivirus     | Medium      | Malware Signature Victim   |
| <input type="checkbox"/> | Malware provided by 224.141.83.77 blocked                        | Assigned        | Antivirus     | Medium      | Malware Signature Attacker |

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 Answer: D. Four events will be added.

This answer matches the conditions set in the playbook filter configuration and the events listed in the Event Monitor.

[References:., FortiAnalyzer 7.4.1 documentation on event filtering, playbook configuration, and incident management criteria., ]

**NEW QUESTION 10**

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

- A. FortiAnalyzer needs that time to parse the new playbook.
- B. FortiAnalyzer needs that time to debug the new playbook.
- C. FortiAnalyzer needs that time to back up the current playbooks.
- D. FortiAnalyzer needs that time to ensure there are no other playbooks running.

**Answer:** A

**Explanation:**

When a new playbook is created on FortiAnalyzer, the system requires some time 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.

[.: FortiAnalyzer documentation states that after creating a playbook, a brief delay is expected as the system parses and validates the playbook. This ensures that any syntax errors or logical inconsistencies are resolved before the playbook is executed, making option A the correct answer., ]

**NEW QUESTION 12**

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 ElasticSearch 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 sqlplugin daemon." This "SQL database" in 7.6 corresponds to the ClickHouse-backed log database described in the Fortinet documentation.

**NEW QUESTION 17**

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 withFortiManager(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 aFortiManager connectorand sending the block information to FortiManager (Option B).

NEW QUESTION 21

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

NEW QUESTION 24

Exhibit.

| <input type="checkbox"/> | Event ⌵                                                                                                          | Event Status ⌵ | Event Type ⌵                                                                                   | Severity ⌵                                                                              |
|--------------------------|------------------------------------------------------------------------------------------------------------------|----------------|------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------|
| <input type="checkbox"/> |  bujqttatbsd.findhere.org (1) | Mitigated      |  Web Filter |  Low |
| <input type="checkbox"/> | Web request to suspicious destination from 10.0.3.20 blocked                                                     | Mitigated      |  Web Filter |  Low |

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

NEW QUESTION 25

Which two statements about FortiAnalyzer Fabric deployments are true? (Choose two answers)

- A. Supervisors can be in high availability (HA) for redundancy purposes only.
- B. Fabric members can operate in analyzer mode only.
- C. Fabric members do not forward their logs to the supervisor.
- D. Supervisors and members must be in the same time zone.

Answer: BC

Explanation:

From Exact Extract of knowledge of FortiAnalyzer 7.6 Study guide documents:  
B is true (members operate in analyzer mode, not collector mode): The study guide defines Fabric members as FortiAnalyzer devices that "retain access to the features described in the FortiAnalyzer Administration Guide" and that "each member can create or raise incidents and events." In contrast, it states that a FortiAnalyzer operating in collector mode "does not provide capabilities for event management or reporting," and also notes that "in collector mode, the GUI doesn't include FortiView, Reports, or Incidents & Events." Since Fabric members must be able to generate/manage incidents and events, they must be operating with analyzer capabilities rather than collector-only functionality.  
C is true (members do not forward their logs to the supervisor): The supervisor provides centralized visibility, but the study guide describes the supervisor's log access as viewing logs collected on members, not receiving/storing forwarded log files. It states: "In the FortiAnalyzer Fabric supervisor, Log View displays logs collected on all FortiAnalyzer Fabric members," and clarifies "the logs contain the same information as displayed in the host FortiAnalyzer device they were collected on." This indicates the logs remain on the member (host) and are made visible to the supervisor for centralized monitoring rather than being forwarded and stored on the supervisor.  
For completeness, the study guide also explicitly states "HA is not available on the supervisor" (so A is false) and members do not need the same time zone as the supervisor (so D is false).

NEW QUESTION 29

Which statement about SQL SELECT queries is true?

- A. They can be used to purge log entries from the database.  
They must be followed immediately by a WHERE clause.
- B. They can be used to display the database schema.
- C. They are not used in macros.
- D.

**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 Answer 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

**NEW QUESTION 32**

Which two actions should an administrator take to view Compromised Hosts on FortiAnalyzer? (Choose two.)

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

**Answer:** AB

**Explanation:**

To view Compromised Hosts on FortiAnalyzer, certain configurations need to be in place on both FortiGate and FortiAnalyzer. Compromised Host data on FortiAnalyzer relies on log information from FortiGate to analyze threats and compromised activities effectively.

Here's why the selected answers are correct:

Option A: Enable device detection on the FortiGate devices that are sending logs to FortiAnalyzer

Enabling device detection on FortiGate allows it to recognize and log devices within the network, sending critical information about hosts that could be compromised. This is essential because FortiAnalyzer relies on these logs to determine which hosts may be at risk based on suspicious activities observed by FortiGate. This setting enables FortiGate to provide device-level insights, which FortiAnalyzer uses to populate the Compromised Hosts view.

Option B: Enable web filtering in firewall policies on FortiGate devices, and make sure these logs are sent to FortiAnalyzer Web filtering is crucial in identifying potentially compromised hosts since it logs any access to malicious sites or blocked categories. FortiAnalyzer uses these web filter logs to detect suspicious or malicious web activity, which can indicate compromised hosts. By ensuring that FortiGate sends these web filtering logs to FortiAnalyzer, the administrator enables FortiAnalyzer to analyze and identify hosts engaging in risky behavior.

Let's review the other options for clarity:

Option C: Make sure all endpoints are reachable by FortiAnalyzer

This is incorrect. FortiAnalyzer does not need direct access to all endpoints. Instead, it collects data indirectly from FortiGate logs. FortiGate devices are the ones that interact with endpoints and then forward relevant logs to FortiAnalyzer for analysis.

Option D: Subscribe FortiAnalyzer to FortiGuard to keep its local threat database up to date

Although subscribing to FortiGuard helps keep threat intelligence updated, it is not a requirement specifically to view compromised hosts. FortiAnalyzer primarily uses logs from FortiGate (such as web filtering and device detection) to detect compromised hosts.

Reference: According to FortiOS and FortiAnalyzer documentation, device detection on FortiGate and enabling web filtering logs are both recommended steps for populating the Compromised Hosts view on FortiAnalyzer. These logs provide insights into device behaviors and web activity, which are essential for identifying and tracking potentially compromised hosts.

**NEW QUESTION 33**

Which log will generate an event with the status Unhandled?

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

**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 with action=dropped: WebFilter logs with the action "dropped" indicate that web traffic was blocked according to the configured web filtering policies. Again, this is a specific action taken, not an "Unhandled" event.

An AppControl log with action=blocked: Application Control logs with the action "blocked" mean that an application was denied access based on the defined application control rules. This is also a clear action, not "Unhandled."

**NEW QUESTION 38**

Which SQL query is in the correct order to query to database in the FortiAnalyzer?

- SELECT devid FROM \$log GROUP BY devid WHERE 'user',, 'users1'
- A. SELECT FROM \$log WHERE devid 'user',, USER1' GROUP BY devid
- B. SELCT devid WHERE 'user'- 'USER1' FROM \$log GROUP By devid
- C. SELECT devid FROM \$log WHERE 'user'=' GROUP BY devid
- D.

**Answer:** D

**Explanation:**

In FortiAnalyzer's SQL query syntax, the typical order for querying the database follows the standard SQL format, which is:

SELECT <column(s)> FROM <table> WHERE <condition(s)> GROUP BY <column(s)>

Option D correctly follows this structure:

SELECT devid FROM \$log: This specifies that the query is selecting the devid column from the \$log table.

WHERE 'user' = ': This part of the query is intended to filter results based on a condition involving the user column. Although there appears to be a minor typographical issue (possibly missing the user value after =), it structurally adheres to the correct SQL order.

GROUP BY devid: This groups the results by devid, which is correctly positioned at the end of the query.

Let's briefly examine why the other options are incorrect:

Option A: SELECT devid FROM \$log GROUP BY devid WHERE 'user', 'users1'

This is incorrect because the GROUP BY clause appears before the WHERE clause, which is out of order in SQL syntax.

Option B: SELECT FROM \$log WHERE devid 'user', USER1' GROUP BY devid

This is incorrect because it lacks a column in the SELECT statement and the WHERE clause syntax is malformed.

Option C: SELCT devid WHERE 'user' - 'USER1' FROM \$log GROUP BY devid

This is incorrect because the SELECT keyword is misspelled as SELCT, and the WHERE condition syntax is invalid.

Reference: FortiAnalyzer documentation for SQL queries indicates that the standard SQL order should be followed when querying logs in FortiAnalyzer. Queries should follow the format SELECT ... FROM ... WHERE ... GROUP BY ..., as demonstrated in option D?.

**NEW QUESTION 41**

When managing incidents on FortiAnalyzer, what must an analyst be aware of?

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

**Answer:** A

**Explanation:**

In FortiAnalyzer's incident management system, analysts have the option to manually manage incidents, which includes attaching relevant reports to an incident for further investigation and documentation. This feature allows analysts to consolidate information, such as detailed reports on suspicious activity, into an incident record, providing a comprehensive view for incident response.

Let's review the other options to clarify why they are incorrect:

Option A: You can manually attach generated reports to incidents

This is correct. FortiAnalyzer allows analysts to manually attach reports to incidents, which is beneficial for providing additional context, evidence, or analysis related to the incident. This functionality is part of the incident management process and helps streamline information for tracking and resolution.

Option B: The status of the incident is always linked to the status of the attached event

This is incorrect. The status of an incident on FortiAnalyzer is managed independently of the status of any attached events. An incident can contain multiple events, each with different statuses, but the incident itself is tracked separately.

Option C: Severity incidents rated with the level High have an initial service-level agreement (SLA) response time of 1 hour

This is incorrect. While incidents have severity levels, specific SLA response times are typically set according to the organization's incident response policy, and FortiAnalyzer does not impose a default

SLA response time of 1 hour for high-severity incidents.

Option D: Incidents must be acknowledged before they can be analyzed

This is incorrect. Incidents on FortiAnalyzer can be analyzed even if they are not yet acknowledged. Acknowledging an incident is often part of the workflow to mark it as being actively addressed, but it is not a prerequisite for analysis.

Reference: According to FortiAnalyzer documentation, analysts can attach reports to incidents manually, making option A correct. This feature enables better tracking and documentation within the incident management system on FortiAnalyzer.

**NEW QUESTION 44**

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

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

**Answer:** AD

**Explanation:**

When a generated report does not contain the expected information even though the logs are confirmed to be present, it typically indicates 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 auto-cache would typically only be relevant if the report is pulling outdated data from cache, but it doesn't directly affect whether specific logs are included in a report.

Conclusion:Incorrect.

Option C - Increase the Report Utilization Quota:

The report utilization quota is related to the resource limits for generating reports. It does not directly influence whether certain data appears in a report. Increasing this quota would help only if there are resource issues preventing the report from completing, not if specific logs are missing from the report.

Conclusion:Incorrect.

Option D - Test the Dataset:

Datasets determine which logs and data fields are pulled into the report. If a dataset is configured incorrectly or does not include the required log fields, it could lead to missing information. Testing the dataset allows you to verify that it's correctly configured and pulling the expected data.

Conclusion:Correct.

Conclusion:

Correct Answer:A. Check the time frame covered by the reportandD. Test the dataset.

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

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

## NEW QUESTION 45

Refer to Exhibit:



What does the data point at 21:20 indicate?

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

**Answer: A**

### Explanation:

The exhibit shows a graph that tracks two metrics over time:Receive RateandInsert Rate. These two rates are crucial for understanding the log processing behavior in FortiAnalyzer.

Understanding Receive Rate and Insert Rate:

Receive Rate: This is the rate at which FortiAnalyzer is receiving logs from connected devices.

Insert Rate: This is the rate at which FortiAnalyzer is indexing (inserting) logs into its database for storage and analysis.

Data Point at 21:20:

At 21:20, theInsert Rateline is above theReceive Rateline, indicating that FortiAnalyzer is inserting logs into its database at a faster rate than it is receiving them. This situation suggests that FortiAnalyzer is able to keep up with the incoming logs and is possibly processing a backlog or temporarily received logs faster than new logs are coming in.

Option Analysis:

Option A - FortiAnalyzer is Indexing Logs Faster Than Logs are Being Received: This accurately describes the scenario at 21:20, where the Insert Rate exceeds the Receive Rate. This indicates that FortiAnalyzer is handling logs efficiently at that moment, with no backlog in processing.

Option B - The fortilogd Daemon is Ahead in Indexing by One Log: The data does not provide specific information about the fortilogd daemon's log count, only the rates. This option is incorrect.

Option C - SQL Database Requires a Rebuild: High receive lag would imply a backlog in receiving and indexing logs, typically visible if the Receive Rate were significantly above the Insert Rate, which is not the case here.

Option D - FortiAnalyzer is Temporarily Buffering Logs to Index Older Logs First: There is no indication of buffering in this scenario. Buffering would usually occur if the Receive Rate were higher than the Insert Rate, indicating that FortiAnalyzer is storing logs temporarily due to indexing lag.

Conclusion:

Correct Answer:A. FortiAnalyzer is indexing logs faster than logs are being received.

The graph at 21:20 shows a higher Insert Rate than Receive Rate, indicating efficient log processing by FortiAnalyzer.

[References:, FortiAnalyzer 7.4.1 documentation on log processing metrics, Receive Rate, and Insert Rate indicators., ]

## NEW QUESTION 46

You are trying to configure a task in the playbook editor to run a report.

However, when you try to select the desired playbook, you do to see it listed.

What is the reason?

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

**Answer: C**

## NEW QUESTION 47

Which statement about the FortiSIEM management extension is correct?

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

**Answer:** D

#### NEW QUESTION 48

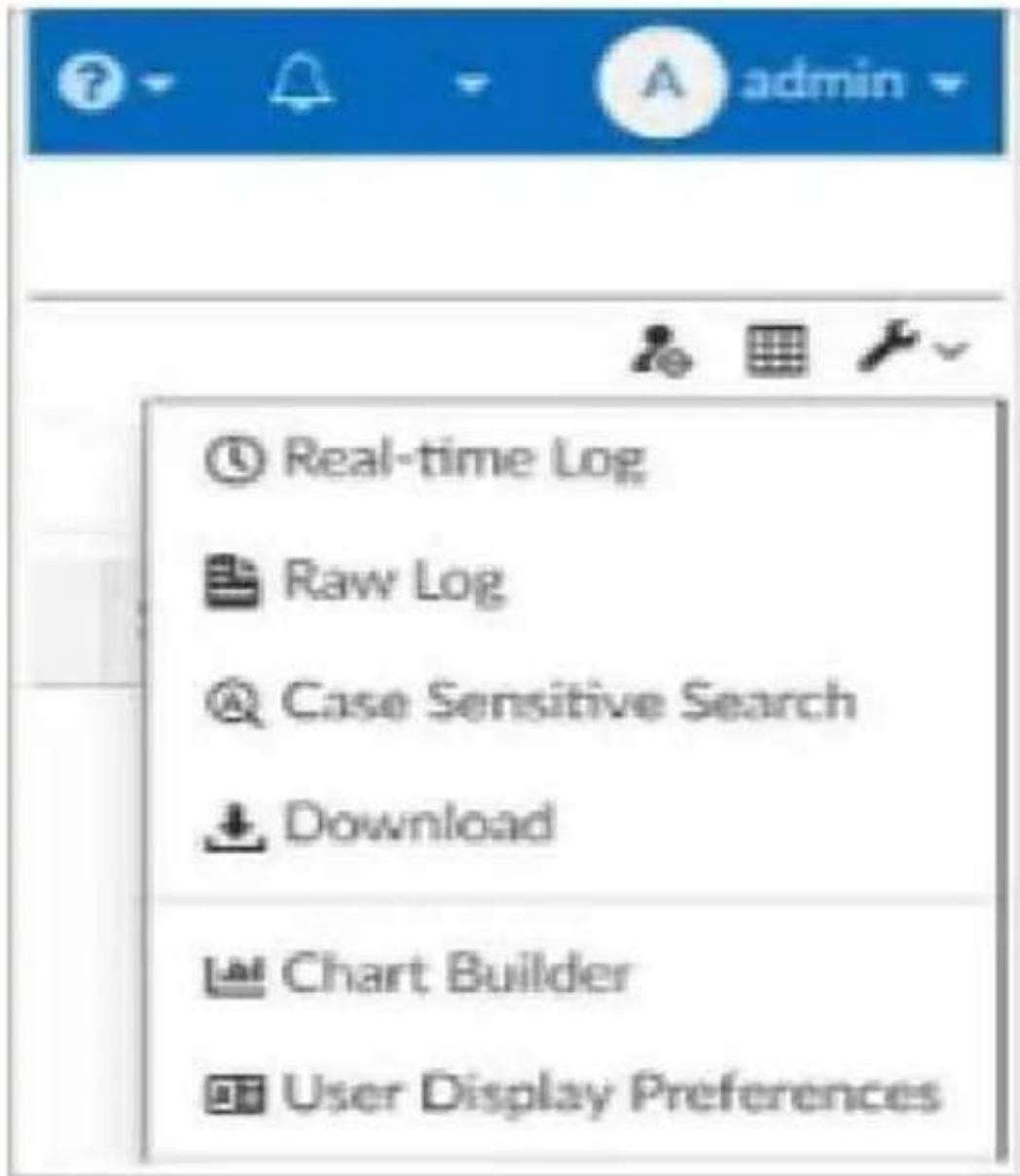
What is the purpose of using data selectors when configuring event handlers?

- A. They filter the types of logs that FortiAnalyzer can accept from registered devices.
- B. They download new filters can be used in event handlers.
- C. They apply their filter criteria to the entire event handler so that you don't have to configure the same criteria in the individual rules.
- D. They are common filters that can be applied simultaneously to all event handlers.

**Answer:** C

#### NEW QUESTION 52

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

#### NEW QUESTION 56

Which statement correctly describes one Difference between templates and reports?

- A. Reports provide more 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 group
- E. while reports are mapped to ADOMs

**Answer:** D

#### NEW QUESTION 59

.....

## Thank You for Trying Our Product

\* 100% Pass or Money Back

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

\* One year free update

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

\* Trusted by Millions

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

\* Shop Securely

All transactions are protected by VeriSign!

**100% Pass Your FCP\_FAZ\_AN-7.6 Exam with Our Prep Materials Via below:**

[https://www.certleader.com/FCP\\_FAZ\\_AN-7.6-dumps.html](https://www.certleader.com/FCP_FAZ_AN-7.6-dumps.html)