Download Fortinet FCP_FAZ_AN-7.6 Exam Dumps Free

Shared by Franklin on 17-06-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

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

Options:

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:

A, B

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.

Question 2

Question Type: MultipleChoice

Which statement about the FortiSIEM management extension is correct?

Options:

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

Question 3

Question Type: MultipleChoice

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?

Options:

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.

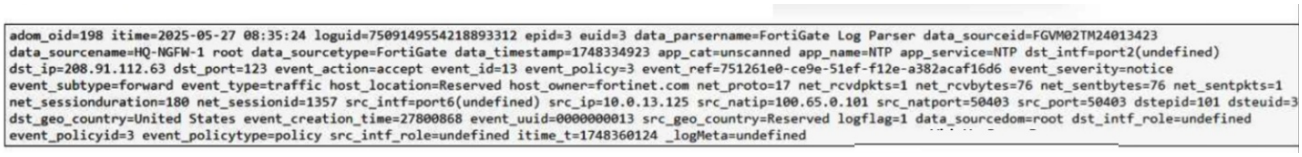
Option D: Incoming webhook

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.

Question 4

Question Type: MultipleChoice

(Refer to the exhibit.



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

Options:

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 5

Question Type: MultipleChoice

(Refer to the exhibit.

Event	Event Status	Event Type	Severity
bujyqttatbsd.findhere.org (1)	Mitigated	Web Filter	Low
Web request to suspicious destination from 10.0.3.20 blocked	Mitigated	Web Filter	Low

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

Options:

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 6

Question Type: MultipleChoice

Exhibit.

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

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

What can you conclude about the output?

Options:

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.

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

Question 7

Question Type: MultipleChoice

Refer to Exhibit:

What does the data point at 21:20 indicate?

Options:

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.

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

Question 8

Question Type: MultipleChoice

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?

Options:

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.

FortiAnalyzer 7.4.1 documentation on incident management and audit history logging.

Question 9

Question Type: MultipleChoice

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

Options:

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.

Question 10

Question Type: MultipleChoice

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?

Options:

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.

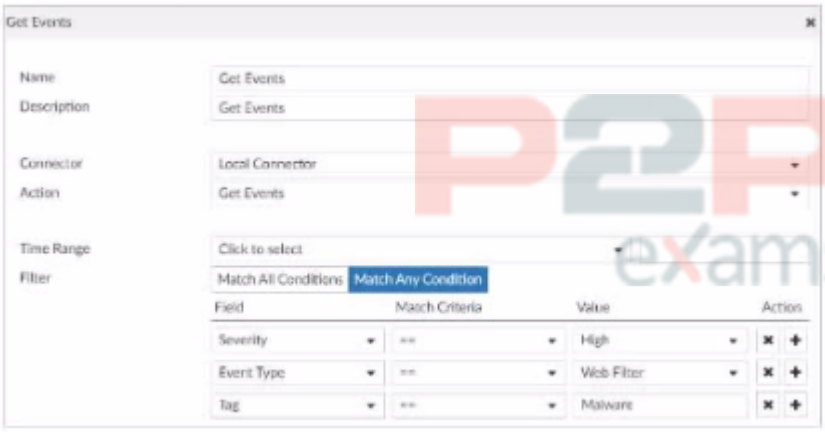
FortiAnalyzer 7.4.1 documentation on creating and using custom views for log searches.

Question 11

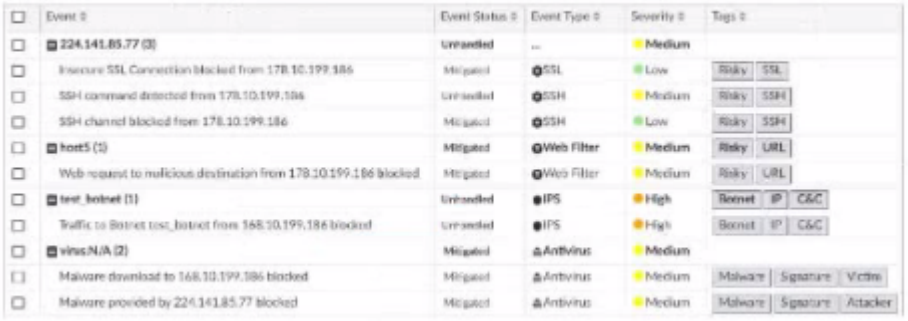
Question Type: MultipleChoice

Exhibit.

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?

Options:

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.

FortiAnalyzer 7.4.1 documentation on event filtering, playbook configuration, and incident

management criteria.