# Fortinet.FCP_FAZ_AN-7.6.v2026-02-03.q34

| | |
|---|---|
| **Exam Code:** | FCP_FAZ_AN-7.6 |
| **Exam Name:** | FCP - FortiAnalyzer 7.6 Analyst |
| **Certification Provider:** | Fortinet |
| **Free Question Number:** | 34 |
| **Version:** | v2026-02-03 |
| **# of views:** | 117 |
| **# of Questions views:** | 340 |
| https://www.freepdfdumps.com/Fortinet.FCP_FAZ_AN-7.6.v2026-02-03.q34.html | |

**NEW QUESTION: 1**
Which statement about sending notifications with incident updates is true?
**A.** You must configure an output profile to send notifications by email.
**B.** Each connector used can have different notification settings
**C.** Notifications can be sent only when an incident is created oi deleted.
**D.** Each incident can send notification to a single external platform.
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 2**
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: (SHOW ANSWER)**
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).

**NEW QUESTION: 3**
(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 (LEAVE A REPLY)**
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).

**NEW QUESTION: 4**

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: (SHOW ANSWER)**

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 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: 5**

Exhibit.


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 (LEAVE A REPLY)**

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: 6**
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: (SHOW ANSWER)**

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

**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: B,C (LEAVE A REPLY)**

**NEW QUESTION: 8**
What happens when the indicator of compromise (IOC) engine on FortiAnalyzer finds web logs that match blacklisted IP addresses?
**A.** A new infected entry is added for the corresponding endpoint under Compromised Hosts.
**B.** FortiAnalyzer flags the associated host for further analysis.
**C.** The endpoint is marked as Compromised and, optionally, can be put in quarantine.
**D.** The detection engine classifies those logs as Suspicious.
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 9**
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.** You must create a trigger to run the report first.
**C.** The playbook is currently running and will be available after it is finished.
**D.** The report has no result and must be reconfigured.
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 10**
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 (LEAVE A REPLY)**
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 Answer: B. Configure a custom view.
* Custom views allow you to save specific search filters, enabling quick access to frequently used parameters in Log View.
References:
FortiAnalyzer 7.4.1 documentation on creating and using custom views for log searches.

**NEW QUESTION: 11**
What is the purpose of using data selectors when configuring event handlers?
**A.** 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.
**B.** They filter the types of logs that FortiAnalyzer can accept from registered devices.
**C.** They are common filters that can be applied simultaneously to all event handlers.
**D.** They download new filters can be used in event handlers.
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 12**
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 (LEAVE A REPLY)**
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: 13**
(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: (SHOW ANSWER)**
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.

**NEW QUESTION: 14**
Refer to the exhibit.

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

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

What can you conclude about the output?
**A.** The low indexing values require investigation.
**B.** The log rate higher than the message rate is not normal.
**C.** There are more event logs than traffic logs.
**D.** The output is not ADOM specific.
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 15**
Exhibit.

| Event | Event Status | Event Type | Severity |
|---|---|---|---|
| bujyqttatbsd.fndhere.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 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 (LEAVE A REPLY)**

**NEW QUESTION: 16**
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.** Fabric View
**B.** Log Browse
**C.** FortiView
**D.** Log View
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 17**

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 (LEAVE A REPLY)**

In the exhibit, the playbook configuration shows the analyst working with the "Attach Data" action within a playbook. Here's a breakdown of key aspects:

* Incident ID: This field is linked to the "Playbook Starter," which indicates that the playbook will attach data to an existing incident.

* Attachment: The analyst is configuring an attachment by selecting Run_REPORT with a placeholder ID for report_uuid. This suggests that the report's UUID will dynamically populate as part of the playbook execution.

Analysis of Options:

* Option A - Creating a Trigger Variable:
* A trigger variable would typically be set up in the playbook starter or initiation configuration, not within the "Attach Data" action. The setup here does not indicate a trigger, as it's focusing on data attachment.
* Conclusion: Incorrect.
* Option B - Creating an Output Variable:
* The field Attachment with a report_uuid placeholder suggests that the analyst is defining an output variable that will store the report data or ID, allowing it to be attached to the incident. This variable can then be referenced or passed within the playbook for further actions or reporting.
* Conclusion: Correct.
* Option C - Creating a Report in the Playbook:
* While Run_REPORT is selected, it appears to be an attachment action rather than a report generation task. The purpose here is to attach an existing or dynamically generated report to an incident, not to create the report itself.
* Conclusion: Incorrect.
* Option D - Creating a SOC Report:
* Similarly, this configuration is focused on attaching data, not specifically generating a SOC report. SOC reports are generally predefined and generated outside the playbook.
* Conclusion: Incorrect.
Conclusion:
* Correct Answer: B. The analyst is trying to create an output variable to be used in the playbook.
* The setup allows the playbook to dynamically assign the report_uuid as an output variable, which can then be used in further actions within the playbook.
References:
FortiAnalyzer 7.4.1 documentation on playbook configurations, output variables, and data attachment functionalities.

**NEW QUESTION: 18**
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: (SHOW ANSWER)**
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, offloading analysis to other devices in the network.
* Conclusion: Correct.
* Option C - Report Creation and Editing in Collector Mode:
* In Collector mode, FortiAnalyzer does not have the capability to create or edit reports. This mode is focused solely on log collection and forwarding, with analysis and report generation left to FortiAnalyzer units operating in Analyzer mode.
* Conclusion: Incorrect.
* Option D - Performance Improvement with Both Modes in Topology:
* Deploying FortiAnalyzer devices in both Collector and Analyzer modes in a network topology can enhance performance. Collector mode devices handle log collection, reducing the workload on Analyzer mode devices, which focus on log processing, analysis, and reporting. This separation of tasks can optimize resource usage and improve the overall efficiency of log management.
* Conclusion: Correct.
Conclusion:
* Correct Answer: B. FortiAnalyzer runs in collector mode by default unless it is configured for 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.
References:
FortiAnalyzer 7.4.1 documentation on operating modes (Collector and Analyzer) and their respective capabilities.

**NEW QUESTION: 19**
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 (LEAVE A REPLY)**
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.
* The FortiSOAR platform, as outlined in Fortinet product documentation, is a standalone SOAR solution that requires a dedicated device or VM for deployment. It integrates with Fortinet's Security Fabric but operates separately from FortiAnalyzer, FortiManager, and FortiGate, focusing on advanced incident management and security automation.

**NEW QUESTION: 20**
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: (SHOW ANSWER)**
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

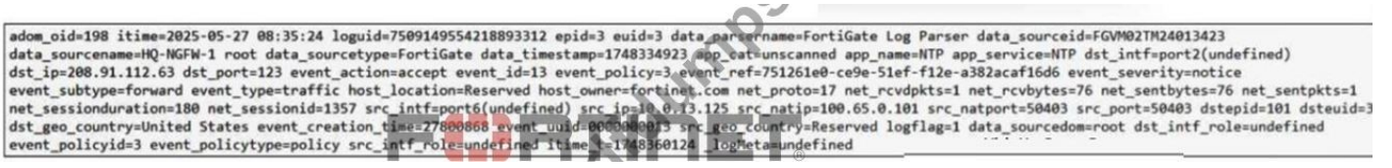
* This is incorrect. The FortiAnalyzer Event Handler is used within FortiAnalyzer itself for handling log events and alerts, but it does not trigger automation stitches on FortiGate.
* Option B: Fabric Connector event
* This is incorrect. Fabric Connector events are related to Fortinet's Security Fabric 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.
* According to FortiOS and FortiAnalyzer documentation, when integrating FortiAnalyzer playbooks with FortiGate automation stitches, the recommended trigger type on FortiGate is an Incoming Webhook, allowing FortiAnalyzer to interact with FortiGate's automation framework through the FortiOS connector.

**NEW QUESTION: 21**
Exhibit.


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 (LEAVE A REPLY)**
In this output, we see two diagnostic commands executed on a FortiAnalyzer device:
* diagnose fortilogd lograte: This command shows the rate at which logs are being processed by the FortiAnalyzer in terms of log entries per second.
* diagnose fortilogd msgrate: This command displays the message rate, or the rate at which individual messages are being processed.
The values provided in the exhibit output show:
* Log rate (lograte): Consistently high, showing values such as 70.0, 132.1, and 133.3 logs per second over different time intervals.
* Message rate (msgrate): Lower values, around 1.4 to 1.6 messages per second.
Explanation:

* Interpretation of log rate vs. message rate: In FortiAnalyzer, the log rate typically refers to the rate of logs being stored or indexed, while the message rate refers to individual messages within these logs.
Given that a single log entry can contain multiple messages, it's common to see a lower message rate relative to the log rate.
* Understanding normal operation: In this case, the message rate being lower than the log rate is expected and typical behavior. This discrepancy can arise because each log entry may bundle multiple related messages, reducing the message rate relative to the log rate.
Conclusion
* Correct Answer: A. The message rate being lower than the log rate is normal.
* This aligns with 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.
References:
FortiOS 7.4.1 and FortiAnalyzer 7.4.1 command guides for diagnose fortilogd lograte and diagnose fortilogd msgrate.

**NEW QUESTION: 22**
(Refer to the exhibit.




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 (LEAVE A REPLY)**
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.

**NEW QUESTION: 23**
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: A,C (LEAVE A REPLY)**
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 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: 24**
Which log will generate an event with the status Contained?
**A.** An IPS log with action=pass.
**B.** An AV log with action=quarantine.
**C.** An AppControl log with action=blocked.
**D.** A WebFilter log will action=dropped.
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 25**
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: (SHOW ANSWER)**
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.

**NEW QUESTION: 26**
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 (LEAVE A REPLY)**
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.

**NEW QUESTION: 27**
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 severity will be lowered.
**D.** The incident dashboard will be updated.
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 28**
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 offline
**Answer: (SHOW ANSWER)**
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 offline
* 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.
* 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.

**NEW QUESTION: 29**
You discover that a few reports are taking a long tine lo generate. Which two steps can you Like to troubleshoot? (Choose two.)
**A.** Review report diagnostics
**B.** Increase the ADOM reports quota
**C.** Enable auto-cache and run the reports again
**D.** Remove old reports from the hcache
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 30**
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 (LEAVE A REPLY)**
* 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.
References:
FortiAnalyzer 7.4.1 documentation on SQL queries, database operations, and macro usage.

**NEW QUESTION: 31**
(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 (LEAVE A REPLY)**
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).



**NEW QUESTION: 32**
What is the purpose of playbook trigger variables?
**A.** To use information from the trigger to filter the action in a task
**B.** To display statistics about the playbook runtime
**C.** To store the start the times of playbooks with On_Schedule triggers
**D.** To provide the trigger information to make the playbook start running
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 33**
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 (LEAVE A REPLY)**

In the exhibit, the data structure shows a checksum field and a data field with a long, seemingly encoded string. This format is indicative of a file that has been compressed or encoded for storage and transfer.

* Export Data Type:

* The data field is likely a base64-encoded string, which is commonly used to represent binary data in text format. Base64 encoding is often applied to data that has been compressed (zipped) for easier handling and transfer. The checksum field, with an MD5 hash, provides a way to verify the integrity of the data after decompression.

* Option Analysis:

* A. The export data type is zipped: Correct. The compressed and encoded format of the data suggests that the export is in a zipped format, allowing for efficient storage and transfer.

* B. The playbook is misconfigured: There is no indication of misconfiguration in this exhibit. The presence of the checksum and data fields aligns with standard export practices.

* C. The option to include the connector was not selected: There is no evidence in the output to conclude that connectors are missing. Connectors are typically listed separately and would not directly affect the checksum and encoded data structure.

* D. Your colleague put a password on the export: There's no indication of password protection in the exhibit. Password protection would likely alter the data structure, and there would be some mention of encryption.

Conclusion:

* Correct answer: A. The export data type is zipped.

* This answer is consistent with the typical use of base64 encoding for compressed (zipped) data exports in FortiAnalyzer.

References:

FortiAnalyzer 7.4.1 documentation on exporting playbooks and data compression methods.

**NEW QUESTION: 34**

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 (LEAVE A REPLY)**

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 Answer: C. To display the SQL query connections and hcache status
* This command is used to monitor SQL reporting activities and cache status, aiding in the analysis of report generation performance and connection health.
References:
FortiAnalyzer 7.4.1 documentation on SQL diagnostic commands, particularly those related to reporting (sqlreportd) and caching mechanisms.