Prepare Smart for Success Free Fortinet FCP_FAZ_AN-7.6 Exam Questions and Answers

Ready to pass faster? Grab free and updated Fortinet NSE 5 - FortiAnalyzer 7.6 Analyst exam PDF questions now. Get authentic FCP_FAZ_AN-7.6 dumps packed with verified answers and secure your certification success with PrepBolt FCP_FAZ_AN-7.6 exam pdf questions and answers.

Thank you for Downloading FCP_FAZ_AN-7.6 exam PDF Demo

https://prepbolt.com/FCP_FAZ_AN-7.6.html

Question 1

Question Type: MultipleChoice

Which two actions should an administrator take to vide Compromised Hosts on FortiAnalyzer? (Choose 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

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

Options:

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

Explanation:

Enabling auto-cache in FortiAnalyzer reports is designed to improve the efficiency and speed of report generation by leveraging cached data. Let's analyze each option to determine which effects are correct.

Option A - The Generation Time for Reports is Decreased:

When auto-cache is enabled, FortiAnalyzer can use previously cached data instead of reprocessing all log data from scratch each time a report is generated. This results in faster report generation times, especially for recurring reports that use similar datasets.

Conclusion: Correct.

Option B - Hard-Cache Data is Automatically Updated When New Logs are Received:

Enabling auto-cache does not immediately update the cache with every new log received. Instead, the

cache is updated when reports are generated, based on the existing logs up to that point. Therefore, auto-cache does not constantly refresh with each incoming log, which would be inefficient.

Conclusion: Incorrect.

Option C - FortiAnalyzer Local Cache is Used to Store Generated Reports:

Auto-cache utilizes FortiAnalyzer's local cache to store data used in reports, reducing the need to retrieve and process logs repeatedly. This cached data can be reused for subsequent report generation, enhancing performance.

Conclusion: Correct.

Option D - The Size of Newly Generated Reports is Optimized to Conserve Disk Space:

Auto-cache does not directly impact the size of the report files themselves. It focuses on performance optimization through cached data for faster access, but it does not compress or optimize the storage size of the generated report.

Conclusion: Incorrect.

Conclusion:

Correct Answe r: A. The generation time for reports is decreased and C. FortiAnalyzer local cache is used to store generated reports.

Enabling auto-cache helps reduce report generation time by using locally cached data and optimizes report processing, though it does not impact report size or continuously update with each new log.

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

Question 3

Question Type: MultipleChoice

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?

Options:

A- Attention required
B- Upstream_failed
C- Failed

D- Success

Answer:

A

Explanation:

In FortiAnalyzer, when a playbook is run, each task's status impacts the overall playbook status. Here's what happens based on task outcomes:

Status When All Tasks Succeed:

If all tasks finish successfully, the playbook status is marked as Success.

Status When Some Tasks Fail:

If one or more tasks in the playbook fail, but others succeed, the playbook status generally changes to Attention required. This status indicates that the playbook completed execution but requires review due to one or more tasks failing.

This is different from a complete Failed status, which is used if the playbook cannot proceed due to a critical error in an early task, often one that upstream tasks depend on.

Option Analysis:

A . Attention required: This is correct as the playbook has completed, but with partial success and a task requiring review.

B . Upstream_failed: This status is used if a task cannot run because a prerequisite or 'upstream' task failed. Since four out of five tasks completed, this is not the case here.

C . Failed: This status would imply that the playbook completely failed, which does not match the scenario where only one task out of five failed.

D . Success: This status would apply if all tasks had completed successfully, which is not the case here.

Conclusion:

Correct Answe r: A. Attention required

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

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

Question 4

Question Type: MultipleChoice

After a generated a repot, you notice the information you were expecting to see in not included in it. However, you confirm that the logs are there:

Which two actions should you perform? (Choose two.)

Options:

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

Answer:

A, D

Explanation:

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

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

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

Conclusion: Correct.

Option B - Disable Auto-Cache:

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

Conclusion: Incorrect.

Option C - Increase the Report Utilization Quota:

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

Conclusion: Incorrect.

Option D - Test the Dataset:

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

Conclusion: Correct.

Conclusion:

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

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

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

Question 5

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 6

Question Type: MultipleChoice

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

Options:

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

Answer:

A, C

Explanation:

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

FortiAnalyzer event handlers support alerting when a rule match generates an event. The study guide

states that, for an event handler, ''You can select a notification profile to send alerts whenever an event is generated by the handler.'' In FortiAnalyzer, notification profiles are the mechanism used to deliver alerts outward (for example, via an SNMP trap), which directly aligns with option A.

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

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

Question 7

Question Type: MultipleChoice

Which two statements regarding FortiAnalyzer operating modes are true? (Choose two.)

Options:

A- When running in collector mode, FortiAnalyzer can forward logs to a syslog server.
B- FortiAnalyzer runs in collector mode by default unless it is configured for HA.
C- You can create and edit reports when FortiAnalyzer is running in collector mode.
D- A topology with FortiAnalyzeer devices running in both modes can improve their performance.

Answer:

B, D

Explanation:

FortiAnalyzer has two primary operating modes: Analyzer mode and Collector mode. Each mode serves specific purposes and has distinct capabilities.

Option A - Forwarding Logs to a Syslog Server in Collector Mode:

In Collector mode, FortiAnalyzer collects logs from Fortinet devices but does not process or analyze them. Instead, it forwards the logs to other FortiAnalyzer units in Analyzer mode or to specific storage locations. However, forwarding logs to a syslog server is not a function of Collector mode. Logs are generally stored or sent to other FortiAnalyzer devices.

Conclusion: Incorrect.

Option B - Default Mode is Collector Mode Unless Configured for HA:

When a FortiAnalyzer is initially set up, it runs in Collector mode by default unless it is configured as part of a High Availability (HA) setup, which would set it to Analyzer mode. Collector mode prioritizes log collection and storage rather than analysis, 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 Answe r: B. FortiAnalyzer runs in collector mode by default unless it is configured for HA and D. A topology with FortiAnalyzer devices running in both modes can improve their performance.

These answers correctly describe the functionality and default configuration of FortiAnalyzer operating modes, along with how a mixed-mode topology can enhance performance.

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

Question 8

Question Type: MultipleChoice

(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))

Options:

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

Answer:

A

Explanation:

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

The study guide explains that FortiAI token usage includes both the prompt (input) and the response (output), and that ''generally, more text in the query and response results in using more tokens.'' It provides two comparison examples and concludes that the more verbose request for ''all the log entries'' consumes more tokens because it has more text and also triggers a larger response; whereas limiting the query to a time range (for example, ''(past week)'') reduces output volume and therefore token usage.

Applying that guidance to the options:

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

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

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

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

Question 9

Question Type: MultipleChoice

You discover that a few reports are taking a long tine lo generate. Which two steps can you Like to troubleshoot? (Choose two.)

Options:

A- Remove old reports from the hcache

B- Enable auto-cache and run the reports again
C- Increase the ADOM reports quota
D- Review report diagnostics

Answer:

A, B

Thank You for trying FCP_FAZ_AN-7.6 PDF Demo

To try our FCP_FAZ_AN-7.6 practice exam software visit link below

https://prepbolt.com/FCP_FAZ_AN-7.6.html

Start Your FCP_FAZ_AN-7.6 Preparation

Use Coupon “SAVE50” for extra 50% discount on the purchase of Practice Test Software. Test your FCP_FAZ_AN-7.6 preparation with actual exam questions.