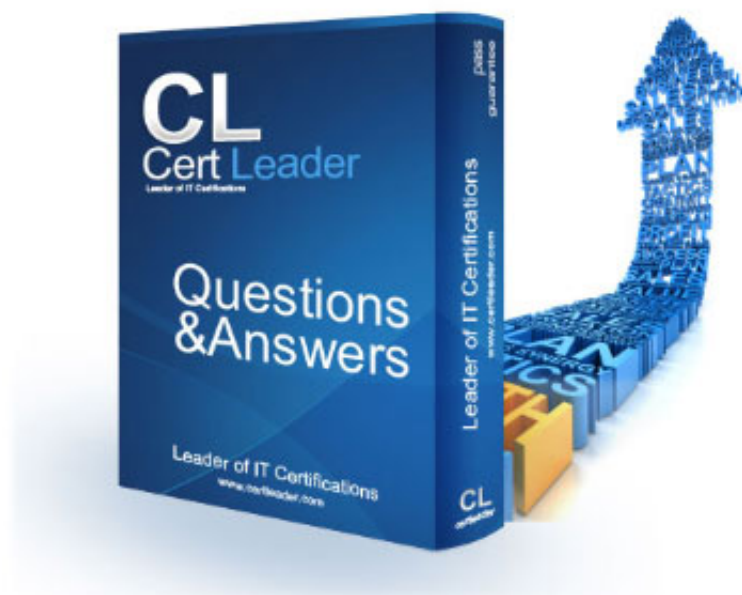


FCP_FAZ_AN-7.6 Dumps

Fortinet NSE 5 - FortiAnalyzer 7.6 Analyst

https://www.certleader.com/FCP_FAZ_AN-7.6-dumps.html



NEW QUESTION 1

Which statement about sending notifications with incident update is true?

- A. You can send notifications to multiple external platforms.
- B. Notifications can be sent only by email.
- C. If you use multiple fabric connectors, all connectors must have the same settings.
- D. Notifications can be sent only when an incident is updated or deleted.

Answer: A

Explanation:

In FortiOS and FortiAnalyzer, incident notifications can be sent to multiple external platforms, not limited to a single method such as email. Fortinet's security fabric and integration capabilities allow notifications to be sent through various fabric connectors and third-party integrations. This flexibility is designed to ensure that incident updates reach relevant personnel or systems using preferred communication channels, such as email, Syslog, SNMP, or integration with SIEM platforms.

Let's review each answer option for clarity:

* Option A: You can send notifications to multiple external platforms

* This is correct. Fortinet's notification system is capable of sending updates to multiple platforms, thanks to its support for fabric connectors and external integrations. This includes options such as email, Syslog, SNMP, and others based on configured connectors.

* Option B: Notifications can be sent only by email

* This is incorrect. Although email is a common method, FortiOS and FortiAnalyzer support multiple notification methods through various connectors, allowing notifications to be directed to different platforms as per the organization's setup.

* Option C: If you use multiple fabric connectors, all connectors must have the same settings

* This is incorrect. Each fabric connector can have its unique configuration, allowing different connectors to be tailored for specific notification and integration requirements.

* Option D: Notifications can be sent only when an incident is updated or deleted

* This is incorrect. Notifications can be sent upon the creation of incidents, as well as upon updates or deletion, depending on the configuration.

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

NEW QUESTION 2

A playbook contains five tasks in total. An administrator runs the playbook and four out of five tasks finish successfully, but one task fails.

What will be the status of the playbook after it is run?

- A. Attention required
- B. Upstream_failed
- C. Failed
- D. Success

Answer: A

Explanation:

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

* Status When All Tasks Succeed:

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

* Status When Some Tasks Fail:

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

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

* Option Analysis:

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

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

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

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

Conclusion:

* Correct Answer A. Attention required

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

References:

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

NEW QUESTION 3

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

- A. FortiView Monitor
- B. Outbreak alert services
- C. Incidents dashboard
- D. Threat hunting

Answer: D

Explanation:

FortiAnalyzer offers several features for monitoring, alerting, and incident management, each serving different purposes. Let's examine each option to determine which one best supports a proactive security approach.

* Option A - FortiView Monitor:

* FortiView is a visualization tool that provides real-time and historical insights into network traffic, threats, and logs. While it gives visibility into network activity, it is generally more reactive than proactive, as it relies on existing log data and incidents.

* Conclusion:Incorrect.

* Option B - Outbreak Alert Services:

* Outbreak Alert Services in FortiAnalyzer notify administrators of emerging threats and outbreaks based on FortiGuard intelligence. This is beneficial for awareness of potential threats but does not offer a hands-on, investigative approach. It??s more of a notification service rather than an active, proactive investigation tool.

* Conclusion:Incorrect.

* Option C - Incidents Dashboard:

* The Incidents Dashboard provides a summary of incidents and current security statuses within the network. While it assists with ongoing incident response, it is used to manage and track existing incidents rather than proactively identifying new threats.

* Conclusion:Incorrect.

* Option D - Threat Hunting:

* Threat Hunting in FortiAnalyzer enables security analysts to actively search for hidden threats or malicious activities within the network by leveraging historical data, analytics, and intelligence. This is a proactive approach as it allows analysts to seek out threats before they escalate into incidents.

* Conclusion:Correct.

Conclusion:

* Correct Answer D. Threat hunting

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

References:

FortiAnalyzer 7.4.1 documentation on Threat Hunting and proactive security measures.

NEW QUESTION 4

Refer to the exhibit.

☐	Event ↕	Event Status ↕	Event Type ↕	Severity ↕
☐	📧 56834764387462384.org (4)	Unhandled	🔍 Web Filter	🔴 Critical
☐	Web traffic to C&C from 10.0.1.200 detected	Unhandled	🔍 Web Filter	🔴 Critical

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

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

Answer: D

Explanation:

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

In the exhibit, theEvent Statusshown isUnhandled(Event Type: Web Filter; Severity: Critical). The FortiAnalyzer study guide definesUnhandledevents as events whose security risk has not been addressed and is therefore still active/open. Specifically, it states:??Unhandled: The security risk is considered open.?? This directly matches optionD.

The other options correspond to different statuses or actions:

- * Isolated/Containedapplies when the risk source is isolated (statusContained), notUnhandled.
- * Escalatedrefers to events moved/raised for further action (statusEscalated), notUnhandled.
- * Whether an incident was created cannot be concluded solely from the status ??Unhandled?? in the exhibit; the study guide ties incident creation to incident management workflows rather than equating ??Unhandled?? with an incident being created.

NEW QUESTION 5

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

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

Answer: BC

NEW QUESTION 6

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

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

Answer: AC

Explanation:

Enablingauto-cachein FortiAnalyzer reports is designed to improve the efficiency and speed of report generation by leveraging cached data. Let??s analyze each option to determine which effects are correct.

* Option A - The Generation Time for Reports is Decreased:

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

* Correct Answer A. The generation time for reports is decreased and C. FortiAnalyzer local cache is used to store generated reports.

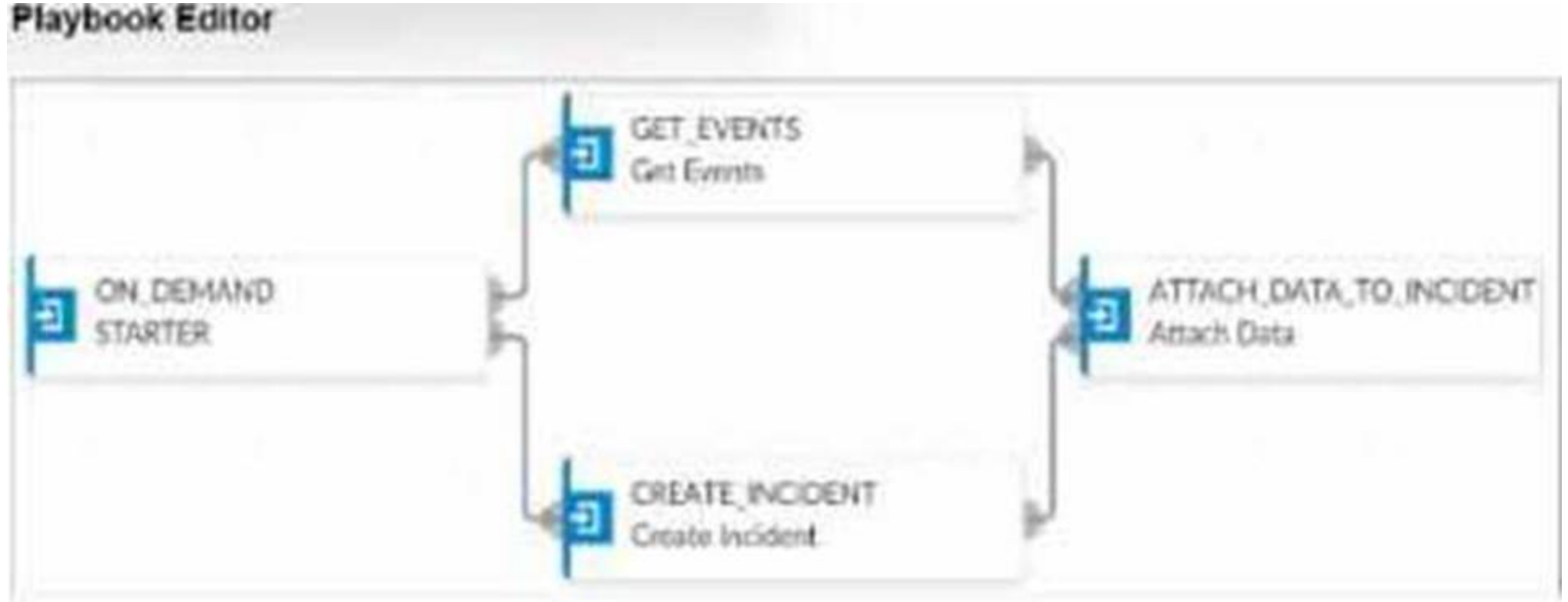
* Enabling auto-cache helps reduce report generation time by using locally cached data and optimizes report processing, though it does not impact report size or continuously update with each new log.

References:

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

NEW QUESTION 7

Exhibit.



Get Event task configuration

Get Events

Name

Get Events

Description

Get Events

Connector

Local Connector

Action

Get Events

Time Range

Click to select

Filter

Match All Conditions

Match Any Condition

Field	Match Criteria	Value	Action
Severity	is	High	✕ +
Event Type	is	Web Filter	✕ +
Tag	is	Malware	✕ +

FortiAnalyzer Event Monitor

Event ID	Event Status	Event Type	Severity	Tag
224.141.85.77 (2)	Unresolved	---	Medium	
Event: SSH Connection blocked from 178.30.199.186	Resolved	SSH	Low	Block SSH
SSH connection detected from 178.30.199.186	Unresolved	SSH	Medium	Block SSH
SSH channel blocked from 178.30.199.186	Resolved	SSH	Low	Block SSH
Host5 (1)	Resolved	Web Filter	Medium	Block URL
Web request to malicious destination from 178.30.199.186 blocked	Resolved	Web Filter	Medium	Block URL
Host: Botnet (1)	Unresolved	IPS	High	Block IP C&C
Traffic to Botnet host, Botnet from 178.30.199.186 blocked	Unresolved	IPS	High	Block IP C&C
virus/M/A (2)	Attacked	Antivirus	Medium	
Malware detected by 178.30.199.186 blocked	Resolved	Antivirus	Medium	Malware Signature Victim
Malware provided by 224.141.85.77 blocked	Resolved	Antivirus	Medium	Malware Signature Attacker

Assume these are all the events that exist on the FortiAnalyzer device.
How many events will be added to the incident created after running this playbook?

- A. Eleven events will be added.
- B. Seven events will be added
- C. No events will be added.
- D. Four events will be added.

Answer: D

Explanation:

In the exhibit, we see a playbook in FortiAnalyzer designed to retrieve events based on specific criteria, create an incident, and attach relevant data to that incident. The "Get Event" task configuration specifies filters to match any of the following conditions:

Severity= High

Event Type= Web Filter

Tag= Malware

Analysis of Events:

In the FortiAnalyzer Event Monitor list:

We need to identify events that meet any one of the specified conditions (since the filter is set to "Match Any Condition").

Events Matching Criteria:

Severity = High:

There are two events with "High" severity, both with the "Event Type" IPS.

Event Type = Web Filter:

There are two events with the "Event Type" Web Filter. One has a "Medium" severity, and the other has a "Low" severity.

Tag = Malware:

There are two events tagged with "Malware," both with the "Event Type" Antivirus and "Medium" severity.

After filtering based on these criteria, there are four distinct events:

Two from the "Severity = High" filter.

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

One from the "Tag = Malware" filter.

Conclusion:

Correct Answer:D. Four events will be added.

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

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

NEW QUESTION 8

Which statement about SQL SELECT queries is true?

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

Answer: D

Explanation:

Option A - Purging Log Entries:

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

Conclusion: Incorrect.

Option B - WHERE Clause Requirement:

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

Conclusion: Incorrect.

Option C - Displaying Database Schema:

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

Conclusion: Incorrect.

Option D - Usage in Macros:

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

Conclusion: Correct.

Conclusion:

Correct Answer D They are not used in macros.

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

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

NEW QUESTION 9

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: BD

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 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 10

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 not see it listed.

What is the reason?

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

Answer: C

NEW QUESTION 10

Which statement about the FortiSIEM management extension is correct?

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

Answer: D

NEW QUESTION 13

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

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

Answer: C

NEW QUESTION 15

A FortiAnalyzer device could use which security method to secure the transfer of log data from FortiGate devices?

- A. SSL
- B. IPSec
- C. Direct serial connection
- D. S/MIME

Answer: B

NEW QUESTION 20

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

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

* One year free update

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

* Trusted by Millions

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

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your FCP_FAZ_AN-7.6 Exam with Our Prep Materials Via below:

https://www.certleader.com/FCP_FAZ_AN-7.6-dumps.html