



Fortinet

Exam Questions FCP_FAZ_AN-7.6

Fortinet NSE 5 - FortiAnalyzer 7.6 Analyst

NEW QUESTION 1

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 2

An administrator on your team has configured multiple reports to run periodically. Management has an additional request that all new generated reports be sent to a company email inbox for accessibility. The mail server has already been configured on FortiAnalyzer.

Which item must be configured on FortiAnalyzer so that emails are sent when the reports are generated?

- A. Enable the option to email all reports under the mail server.
- B. Add a mailto:<email address> option within the report layouts.
- C. Enable email notification under the report calendar.
- D. Enable an output profile on the reports.

Answer: D

Explanation:

To ensure that reports generated by FortiAnalyzer are automatically sent to an email inbox, you need to set up an output profile for the reports. Output profiles specify where and how reports should be delivered, including the option to send them via email.

* Option A - Enable the Option to Email All Reports Under the Mail Server:

* The mail server configuration allows FortiAnalyzer to send emails but does not automatically enable email distribution for reports. This setting alone does not specify which reports to send or to whom.

* Conclusion: Incorrect.

* Option B - Add a mailto:<email address> Option Within the Report Layouts:

* Adding an email address within the report layout is not a standard configuration option for report distribution. Report layouts define the format and content of the report but not its distribution method.

* Conclusion: Incorrect.

* Option C - Enable Email Notification Under the Report Calendar:

* The report calendar is used to schedule when reports are generated. While it triggers report generation at specific times, it does not handle email distribution. Emailing reports requires a configured output profile.

* Conclusion: Incorrect.

* Option D - Enable an Output Profile on the Reports:

* An output profile can be configured on FortiAnalyzer to define delivery options, including emailing the report to specified recipients. This setup ensures that every time a report is generated according to the schedule, it is automatically emailed to the configured address.

* Conclusion: Correct. Conclusion:

* Correct Answer D. Enable an output profile on the reports.

* Configuring an output profile is the correct way to set up automatic email distribution of generated reports in FortiAnalyzer.

References:

FortiAnalyzer 7.4.1 documentation on configuring output profiles and report distribution settings.

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.

* Correct Answer D. Threat hunting

* Threat hunting is the most proactive feature among the options, as it involves actively searching for threats within 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

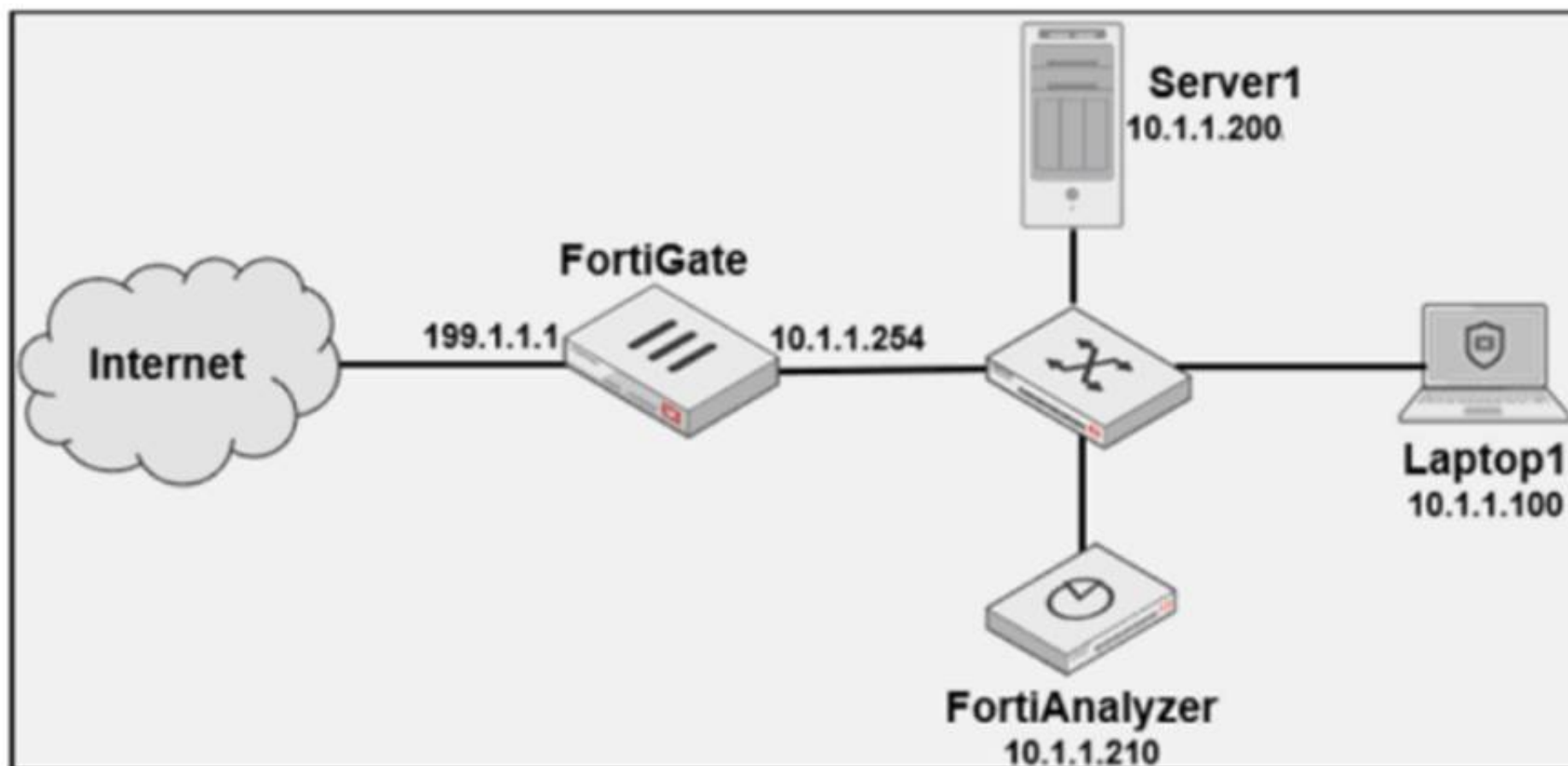
Which statement about automation connectors in FortiAnalyzer is true?

- A. An ADOM with the Fabric type comes with multiple connectors configured.
- B. The local connector becomes available after you configured any external connector.
- C. The local connector becomes available after you connectors are displayed.
- D. The actions available with FortiOS connectors are determined by automation rules configured on FortiGate.

Answer: D

NEW QUESTION 5

Exhibit.



Laptop1 is used by several administrators to manage FortiAnalyzer. You want to configure a generic text filter that matches all login attempts to the web interface generated by any user other than admin, and coming from Laptop1.

Which filter will achieve the desired result?

- A. Operation-login and performed_on=="GUI(10.1.1.100)" and user!=admin
- B. Operation-login and performed_on=="GUI (10.1.1.120)" and user!=admin
- C. Operation-login and srcip== 10.1.1.100 anddstip==10.1.1.210 and user==admin
- D. Operation-login and dstip==10.1.1.210 and user!=admin

Answer: A

Explanation:

The objective is to create a filter that identifies all login attempts to the FortiAnalyzer web interface (GUI) coming from Laptop1 (IP 10.1.1.100) and excludes the admin user. This filter should match any user other than admin.

Filter Components Analysis:

Operation-login: This portion of the filter will target login actions specifically, which is correct for filtering login attempts.

performed_on=="GUI(10.1.1.100)": This indicates that the login attempt must occur on the GUI interface and originate from the specified IP, which matches

Laptop1's IP address (10.1.1.100). This ensures that the filter only matches GUI logins from this specific device.

user!=admin: This part excludes logins by the admin user, meeting the requirement to capture only non-admin users.

Option Analysis:

Option A: Correctly specifies the Operation-login, performed_on=="GUI(10.1.1.100)", and user!=admin. This setup effectively filters login attempts to the GUI from Laptop1, excluding the admin user.

Option B: Uses the incorrect IP 10.1.1.120 in the performed_on filter, which does not match Laptop1's IP (10.1.1.100).

Option C: This option includes srcip==10.1.1.100 and dstip==10.1.1.210 but incorrectly specifies user==admin instead of user!=admin, which does not match the requirement to exclude admin users.

Option D: This option does not specify the performed_on field to restrict it to the GUI and only includes dstip (destination IP) without srcip. It also incorrectly uses user!-admin instead of the correct syntax user!=admin.

Conclusion:

Correct Answer: A. Operation-login and performed_on=="GUI(10.1.1.100)" and user!=admin

This filter precisely captures the required conditions: login attempts from Laptop1 to the GUI interface by any user except admin.

[References: , FortiAnalyzer 7.4.1 documentation on log filters, syntax for login operations, and GUI login tracking.,]

NEW QUESTION 6

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

- 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: AB

NEW QUESTION 7

When there are no matching parsers for a device log, what does FortiAnalyzer do? (Choose one answer))

- A. Drops the log
- B. Applies the generic SYSLOG parser
- C. Stores the log but doesn't normalize it
- D. Archives the log for future analysis

Answer: C

Explanation:

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

FortiAnalyzer's ingestion pipeline does not "drop" logs simply because a parser is unavailable. The study guide states that when devices send logs, "Logs received are decompressed and saved in a log file on the FortiAnalyzer disk??(with a .log extension). This establishes that the raw log is still accepted and stored on disk as part of the normal workflow.

Normalization, however, depends on having a suitable parser. The study guide explains that "FortiAnalyzer uses predefined parsers to extract key fields from ingested logs and maps them to a consistent, standardized set of field names." It further emphasizes that "Log parsers ?? are central to log normalization" because they convert unstructured/native logs into a standardized schema.

Therefore, if no matching parser exists for a given device log, FortiAnalyzer can still store the incoming log (it is received, decompressed, and written to disk), but it cannot perform the "extract key fields" and "map to standardized field names" steps required for normalization. In practical terms, the log remains in its native/unstructured form (not normalized), which aligns exactly with option C.

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

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

Answer: D

Explanation:

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

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

Option D correctly follows this structure:

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

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

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

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

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

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

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

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

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

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

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

NEW QUESTION 10

Which statement about the FortiSOAR management extension is correct?

- It requires a FortiManager configured to manage FortiGate.
- A. It runs as a docker container on FortiAnalyzer.
 - B. It requires a dedicated FortiSOAR device or V
 - C. It does not include a limited trial by default.
 - D.

Answer: C

Explanation:

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.

Reference: 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 10

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

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

Answer: A

Explanation:

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

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

Option A: You can manually attach generated reports to incidents

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

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

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

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

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

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

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

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

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

NEW QUESTION 12

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

Explanation:

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:

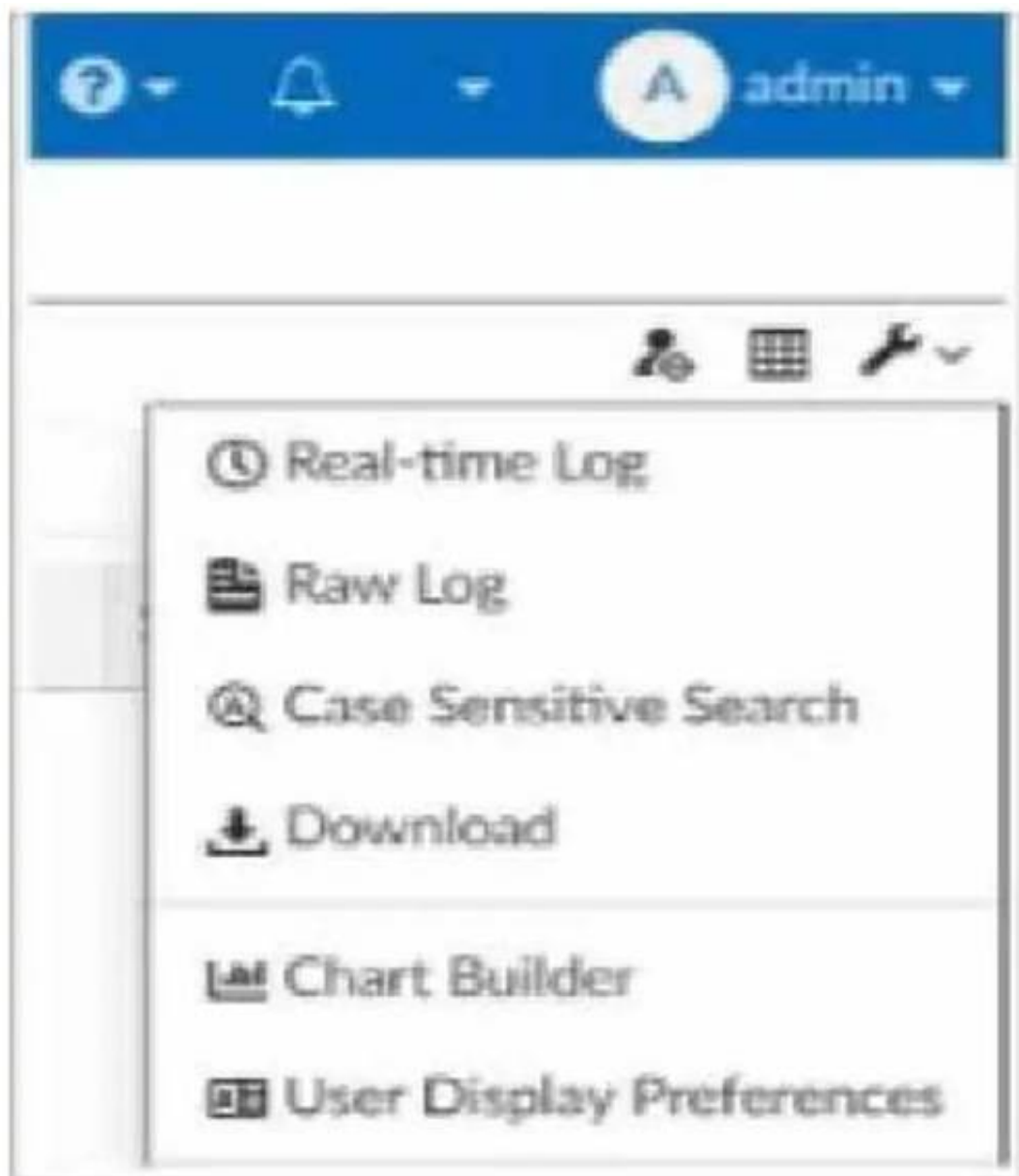
Correct Answer C. To display the SQL query connections and hcache status

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.]

NEW QUESTION 17

Exhibit.



What is the purpose of using the Chart Builder feature On FortiAnalyzer?

- A. To build a chart automatically based on the top 100 log entries
- B. To add charts directly to generate reports in the current ADOM.
- C. To add a new chart under FortiView to be used in new reports
- D. To build a dataset and chart based on the filtered search results

Answer: D

NEW QUESTION 18

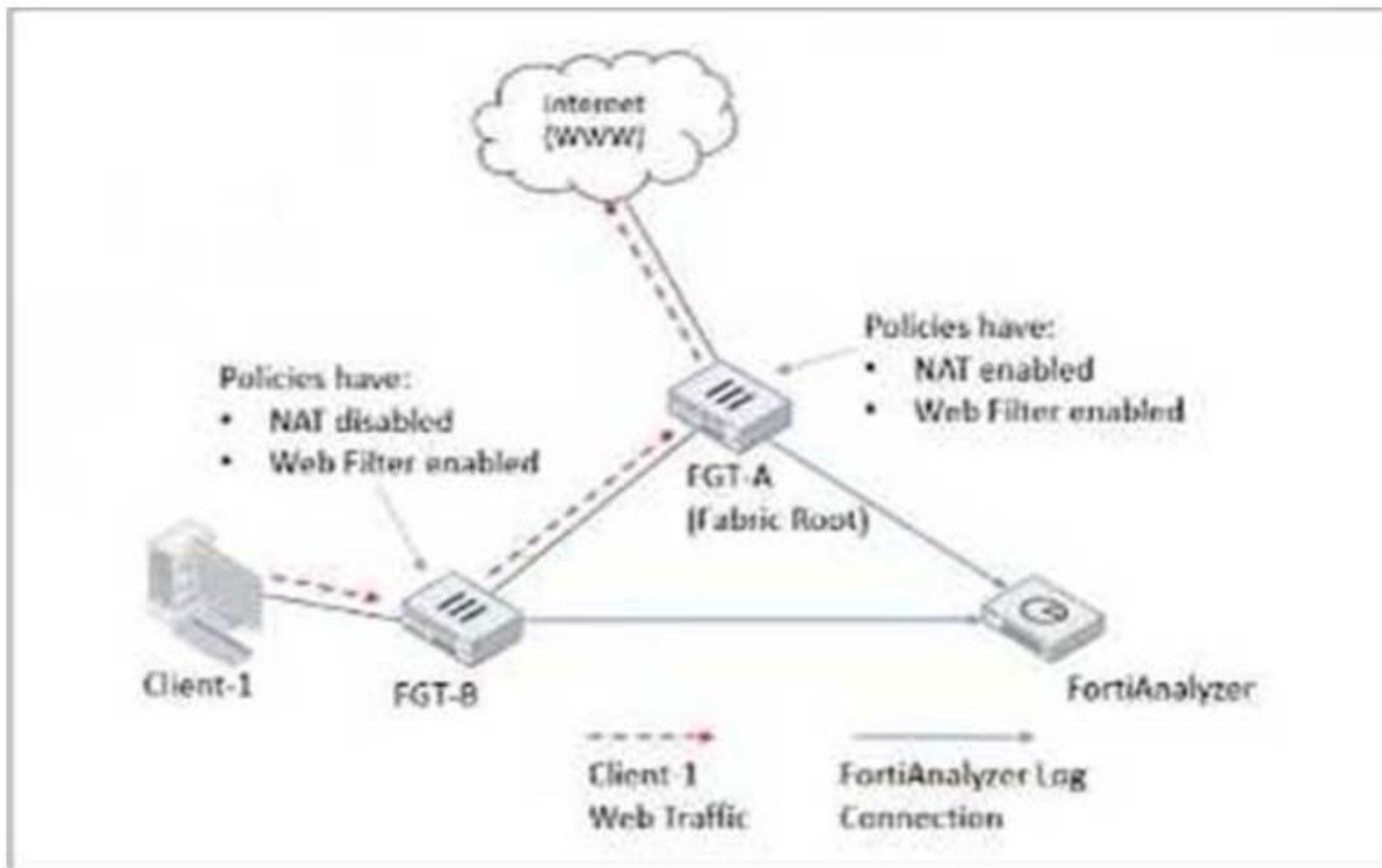
Which two parameters does FortiAnalyzer use to identify an indicator of compromise (IOC)? (Choose two answers)

- A. IP address
- B. URL
- C. Policy ID
- D. Application category

Answer: AB

NEW QUESTION 20

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: D

Explanation:

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. 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 24

You created a playbook on FortiAnalyzer that uses a FortiOS connector. When you configure FortiGate, which type of trigger must you use so that the actions in an automation stitch are available in the FortiOS connector? (Choose one answer)

- A. FortiAnalyzer Event Handler
- B. Incoming webhook
- C. Fabric Connector event
- D. IP ban

Answer: B

Explanation:

From Exact Extract of knowledge of FortiAnalyzer 7.6 Study guide documents:

The study guide explains that FortiAnalyzer playbook tasks rely on connectors, and that the FortiOS connector will not show its available actions until FortiGate is configured with the correct automation trigger. The guide states: "For example, the FortiOS connector will be listed as soon as the first FortiGate device is added to FortiAnalyzer. However, to see the actions related to that FortiOS connector, you must enable an automation rule using the Incoming Webhook Call trigger on FortiGate."

This is why the required FortiGate trigger type is Incoming webhook (option B): it is the specific trigger FortiOS must use so FortiAnalyzer can expose and use the FortiOS connector actions within the playbook workflow.

NEW QUESTION 26

Which two external servers can you configure to validate administrator logins? (Choose two.)

- A. Syslog
- B. LDAP
- C. RADIUS
- D. Only locally by FortiAnalyzer

Answer: ABC

NEW QUESTION 29

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

FCP_FAZ_AN-7.6 Practice Exam Features:

- * FCP_FAZ_AN-7.6 Questions and Answers Updated Frequently
- * FCP_FAZ_AN-7.6 Practice Questions Verified by Expert Senior Certified Staff
- * FCP_FAZ_AN-7.6 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * FCP_FAZ_AN-7.6 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The FCP_FAZ_AN-7.6 Practice Test Here](#)