Vendor: Fortinet

Exam Code: FCP_FAZ_AN-7.4

Exam Name: FCP - FortiAnalyzer 7.4 Analyst

Version: DEMO

QUESTION 1
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 stitch are available in the FortiOS connector?

A. FortiAnalyzer Event Handler
B. Fabric Connector event
C. FortiOS Event Log
D. Incoming webhook

Answer: D
Explanation:
FortiOS connector will be listed as soon as the first FortiGate is added to FortiAnalyzer. However, in order to see the actions related to that FortiOS connector, you must enable an automation rule using the Incoming Webhook Call trigger on the FortiGate side.

QUESTION 2
When managing incidents on FortiAnlyzer, what must an analyst be aware of?

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

Answer: A
Explanation:
You can attach reports to incidents to add historical data in addition to real-time events. These are the three ways that you can attach a report:
• Manually, from an existing report
• Manually, from an existing incident
• Automatically, through automation playbooks

QUESTION 3
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 you configure on FortiAnalyzer so that emails are sent when the reports are generated?

A. Enable the option to email all repots 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:

In FortiAnalyzer, reports can be sent by email only if an output profile is configured and assigned to them. The output profile defines the delivery method (such as email), and uses the already configured mail server to send the reports.

QUESTION 4
Which statement regarding macros on FortiAnalyzer is true?

A. Macros are predefined templates for reports and cannot be customized.
B. Macros are useful in generating excel log files automatically based on the report settings.
C. Macros are ADOM-specific and each ADOM type have unique macros relevant to that ADOM.
D. Macros are supported only on the FortiGate ADOMs.

Answer: C
Explanation:
Macros on FortiAnalyzer are predefined or custom query templates used in reports, and they are organized by ADOM (Administrative Domain). When using ADOMs, you must be in the correct ADOM to create or manage macros, indicating that macros are ADOM-specific and tailored to the device types or datasets relevant to that ADOM.
https://docs.fortinet.com/document/fortianalyzer/7.6.3/administration-guide/617380/creating-macros

QUESTION 5
After generating a report, you notice the information you were expecting to see is not included in it. However, you confirm that the logs are there.

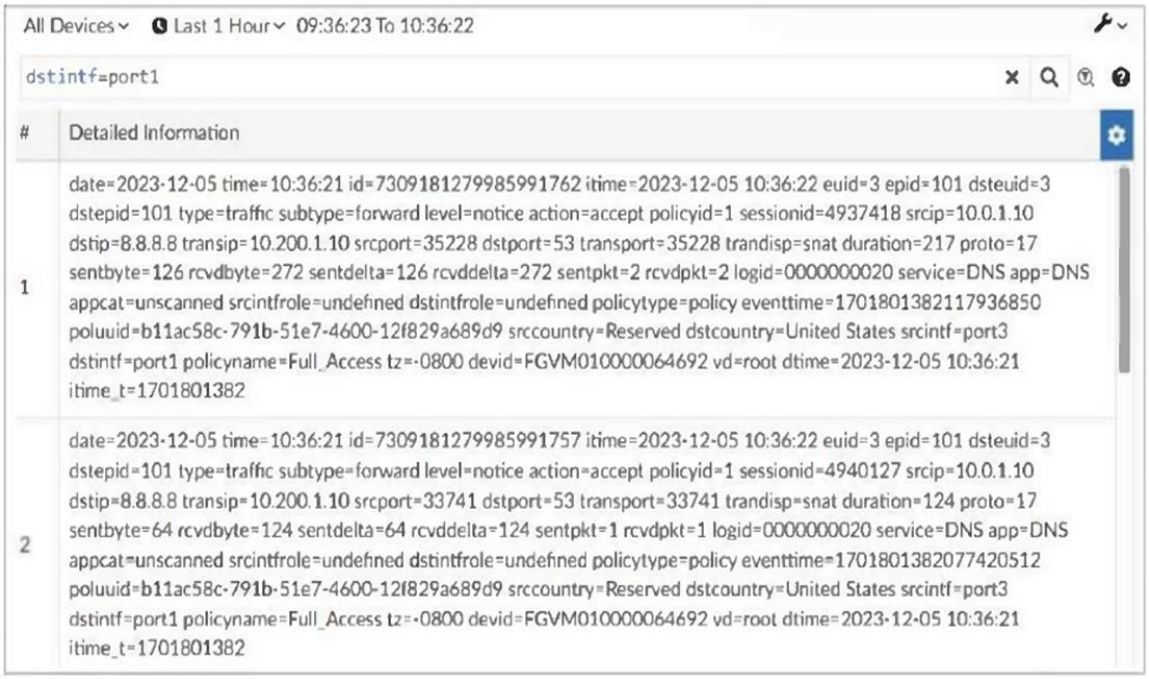
Which two actions should you perform? (Choose two.)

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

Answer: AD
Explanation:
Check the time frame covered by the report: If the report's time range does not match the period of the available logs, the expected information will not appear.

Test the dataset: Testing the dataset ensures that the query used to extract log information is correct and retrieving the intended data for the report.

QUESTION 6
Refer to the exhibit. What can you conclude about these search results? (Choose two.)



A. They can be downloaded to a file.
B. They are sortable by columns and customizable.
C. They are not available for analysis in FortiView.
D. They were searched by using text mode.

Answer: AD
Explanation:
The detailed, unstructured text format of the search results indicates the use of text mode.

Text mode search results in FortiAnalyzer can be exported or downloaded as a file for further analysis.

QUESTION 7
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: AD
Explanation:
FortiAnalyzer in collector mode receives logs from devices and forwards them to syslog servers or analyzer units. This mode supports basic log forwarding functionality without full analytics processing.

Deploying FortiAnalyzer units in both analyzer and collector modes distributes log collection across sites while centralizing analysis. Collectors at branches forward logs to central analyzers, optimizing performance and reducing WAN bandwidth.

QUESTION 8
As part of your analysis, you discover that an incident is a false positive.

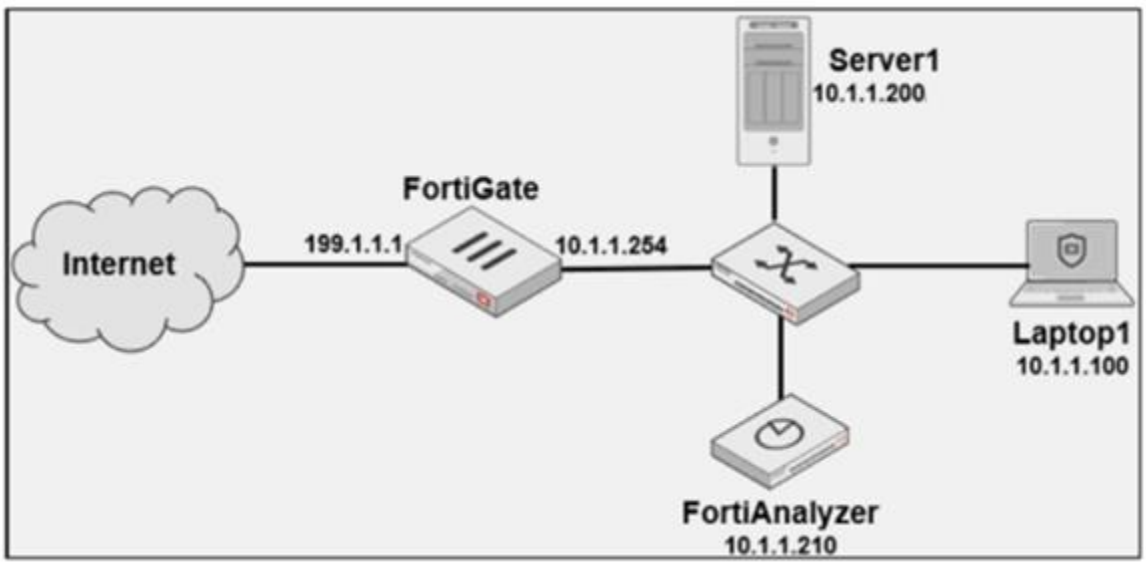
You change the incident status to **Closed: False Positive**.

Which statement about your update is true?

A. The audit history log will be updated.
B. The corresponding event will be marked as mitigated.
C. The incident will be deleted.
D. The incident number will be changed

Answer: A
Explanation:
When an incident is closed as a false positive in FortiAnalyzer, it is not deleted or renumbered. Instead, the closure action is recorded in the audit history, preserving a traceable record of analyst actions for accountability and compliance.

QUESTION 9
Refer to the 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 & performed_on=="GUI(10.1.1.100)' and user!=admin
B. Operation-login & performed_on=="GU (10.1.1.120)' and user!=admin
C. Operation-login & srcip== 10.1.1.100 and dstip==10.1.1.1.210 and user==admin
D. Operation-login & dstip==10.1.1.210 and user!-admin

Answer: A
Explanation:

On there the task was to create a filter for failed logins from any other location but the local computer:
"Add the text performed_on!~10.0.1.10.
This includes any attempts coming from devices with an IP address that is not the one configured on the Local-Client computer."

QUESTION 10
Which two statements about local logs on FortiAnalyzer are true? (Choose two.)

A. They are not supported in FortiView.
B. You can view playbook logs for all ADOMs in the root ADOM.
C. Event logs show system-wide information, whereas application logs are ADOM specific.
D. Event logs are available only in the root ADOM.

Answer: BC
Explanation:
Playbook logs, which relate to automated incident response actions, can be viewed centrally in the root ADOM, allowing visibility across all ADOMs.
Event logs on FortiAnalyzer typically provide system-wide information applicable to the entire FortiAnalyzer unit, while application logs are specific to each ADOM, reflecting the logs related to devices and activities managed within that ADOM.
https://docs.fortinet.com/document/fortianalyzer/7.6.3/administration-guide/208717/enabling-and-disabling-the-adom-feature

QUESTION 11
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: A
Explanation:
The exhibit shows a graph that tracks two metrics over time: Receive Rate and Insert Rate. These two rates are crucial for understanding the log processing behavior in FortiAnalyzer.
Understanding Receive Rate and Insert Rate:
Receive Rate: This is the rate at which FortiAnalyzer is receiving logs from connected devices.
Insert Rate: This is the rate at which FortiAnalyzer is indexing (inserting) logs into its database for storage and analysis.
Data Point at 21:20:
At 21:20, the Insert Rate line is above the Receive Rate line, indicating that FortiAnalyzer is inserting logs into its database at a faster rate than it is receiving them. This situation suggests that FortiAnalyzer is able to keep up with the incoming logs and is possibly processing a backlog or temporarily received logs faster than new logs are coming in.

QUESTION 12
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?

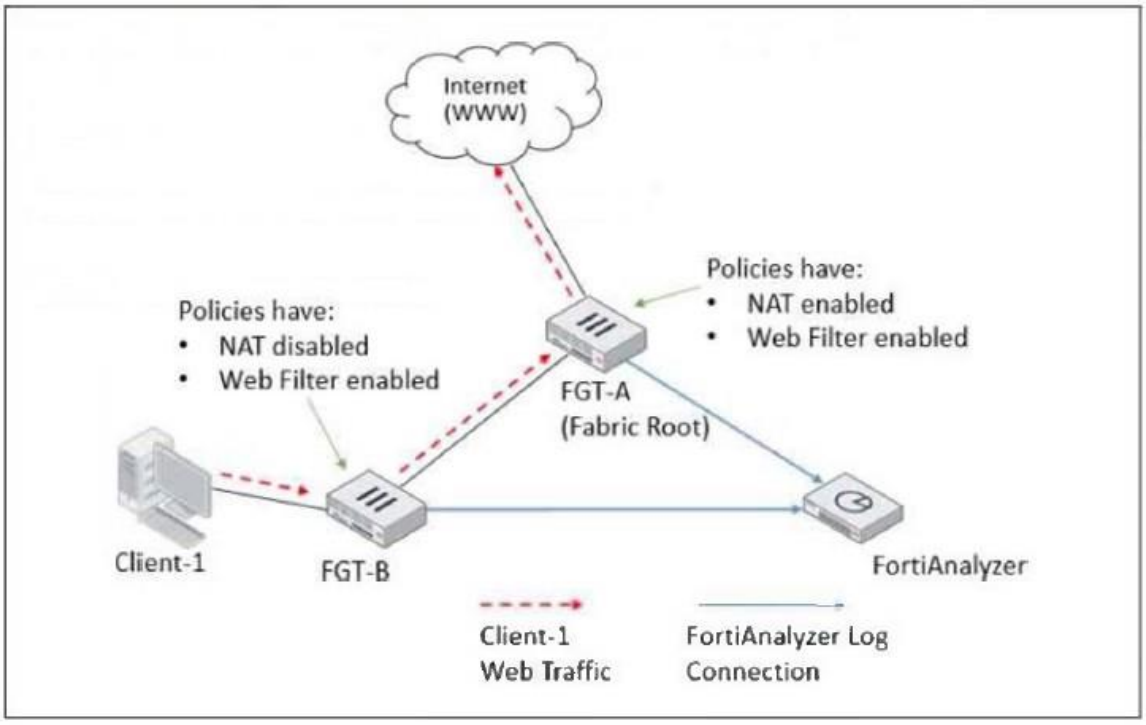
A. Attention required
B. Upstream_failed
C. Failed
D. Success

Answer: C
Explanation:
Playbook jobs that include one or more failed tasks are labeled as Failed in Playbook Monitor. A failed status, however, does not mean that all tasks failed. Some individual actions may have completed successfully.

QUESTION 13
Refer to the 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. Both FGT-A and FGT-B will create traffic logs.
B. FGT-A will see the MAC address of FGT-B in the packets and know it does not need to log this flow.
C. FGT-A will create logs for web filter events only if FGT-B did not already detect a violation.
D. Only FGT-A will create traffic logs.

Answer: A
Explanation:
- FGT-B will create log for initial session
- FGT-B will create log as a resultat of SNAT

QUESTION 14
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: AB
Explanation:
To boost the report performance and reduce report generation time, you can enable auto-cache in the settings of the report. In this case, the hcache is automatically updated when new logs come in and new log tables are generated.

Thank You for Trying Our Product

Braindump2go Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.braindump2go.com/all-products.html

10% Discount Coupon Code: **ASTR14**