Vendor: Fortinet

Exam Code: FCP_FAZ_AN-7.4

Exam Name: FCP - FortiAnalyzer 7.4 Analyst

Version: DEMO

QUESTION 1
You crested 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:
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.

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:
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.

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 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:
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 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.

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: B
Explanation:
Macros in FortiAnalyzer are used to streamline reporting tasks by automating data extraction and report generation.
Option B - Macros are Useful in Generating Excel Log Files Automatically Based on the Report Settings:
This statement is accurate. Macros in FortiAnalyzer can be configured to automate the generation of reports, including outputting log data to Excel format based on predefined report settings. This makes them especially useful for scheduled reporting and data analysis.

QUESTION 5
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.)

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:
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.
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.

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: AD
Explanation:
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.
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.

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