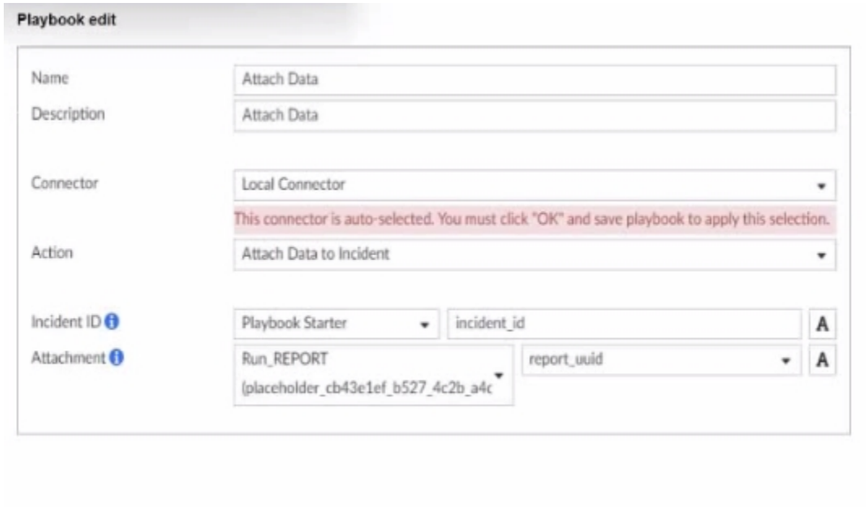
Number: FCP_FAZ_AN-7.4
Passing Score: 800
Time Limit: 120
File Version: 2.3

Exam Code: FCP_FAZ_AN-7.4

Exam Name: FCP - FortiAnalyzer 7.4 Analyst

Exam A

QUESTION 1
Exhibit.



What is the analyst trying to create?

A. The analyst is trying to create a trigger variable to the used in the playbook.
B. The analyst is trying to create an output variable to be used in the playbook.
C. The analyst is trying to create a report in the playbook.
D. The analyst is trying to create a SOC report in the playbook.

Correct Answer: B
Section:
Explanation:
In the exhibit, the playbook configuration shows the analyst working with the 'Attach Data' action within a playbook. Here's a breakdown of key aspects:
Incident ID: This field is linked to the 'Playbook Starter,' which indicates that the playbook will attach data to an existing incident.
Attachment: The analyst is configuring an attachment by selecting Run_REPORT with a placeholder ID for report_uuid. This suggests that the report's UUID will dynamically populate as part of the playbook execution.
Analysis of Options:
Option A - Creating a Trigger Variable:
A trigger variable would typically be set up in the playbook starter or initiation configuration, not within the 'Attach Data' action. The setup here does not indicate a trigger, as it's focusing on data attachment.
Conclusion: Incorrect.
Option B - Creating an Output Variable:
The field Attachment with a report_uuid placeholder suggests that the analyst is defining an output variable that will store the report data or ID, allowing it to be attached to the incident. This variable can then be referenced or passed within the playbook for further actions or reporting.
Conclusion: Correct.
Option C - Creating a Report in the Playbook:
While Run_REPORT is selected, it appears to be an attachment action rather than a report generation task. The purpose here is to attach an existing or dynamically generated report to an incident, not to create the report itself.
Conclusion: Incorrect.
Option D - Creating a SOC Report:

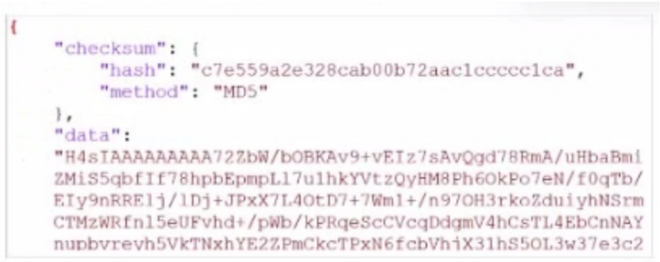
Similarly, this configuration is focused on attaching data, not specifically generating a SOC report. SOC reports are generally predefined and generated outside the playbook.
Conclusion: Incorrect.
Conclusion:
Correct Answe r : B. The analyst is trying to create an output variable to be used in the playbook.
The setup allows the playbook to dynamically assign the report_uuid as an output variable, which can then be used in further actions within the playbook.
FortiAnalyzer 7.4.1 documentation on playbook configurations, output variables, and data attachment functionalities.

QUESTION 2
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

Correct Answer: D
Section:
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 Answe r : 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.
FortiAnalyzer 7.4.1 documentation on Threat Hunting and proactive security measures.

QUESTION 3
Refer to the exhibit with partial output:

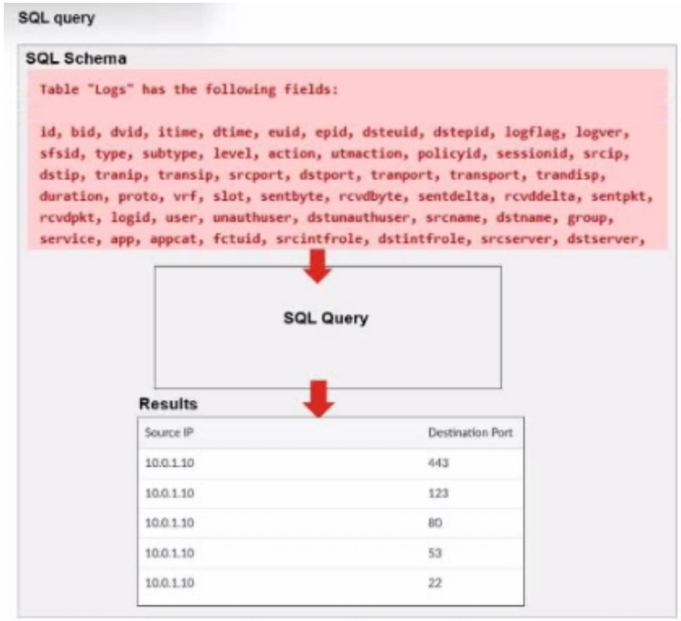


Your colleague exported a playbook and has sent it to you for review. You open the file in a text editor and observer the output as shown in the exhibit.
Which statement about the export is true?

A. The export data type is zipped.
B. The playbook is misconfigured.
C. The option to include the connector was not selected.
D. Your colleague put a password on the export.

Correct Answer: A
Section:
Explanation:
In the exhibit, the data structure shows a checksum field and a data field with a long, seemingly encoded string. This format is indicative of a file that has been compressed or encoded for storage and transfer.
Export Data Type:
The data field is likely a base64-encoded string, which is commonly used to represent binary data in text format. Base64 encoding is often applied to data that has been compressed (zipped) for easier handling and transfer.
The checksum field, with an MD5 hash, provides a way to verify the integrity of the data after decompression.
Option Analysis:
A . The export data type is zipped: Correct. The compressed and encoded format of the data suggests that the export is in a zipped format, allowing for efficient storage and transfer.
B . The playbook is misconfigured: There is no indication of misconfiguration in this exhibit. The presence of the checksum and data fields aligns with standard export practices.
C . The option to include the connector was not selected: There is no evidence in the output to conclude that connectors are missing. Connectors are typically listed separately and would not directly affect the checksum and encoded data structure.
D . Your colleague put a password on the export: There's no indication of password protection in the exhibit. Password protection would likely alter the data structure, and there would be some mention of encryption.
Conclusion:
Correct Answe r : A. The export data type is zipped.
This answer is consistent with the typical use of base64 encoding for compressed (zipped) data exports in FortiAnalyzer.
FortiAnalyzer 7.4.1 documentation on exporting playbooks and data compression methods.

QUESTION 4
Exhibit.



A fortiAnalyzer analyst is customizing a SQL query to use in a report.
Which SQL query should the analyst run to get the expected results?
A)

```
SELECT srcip AS "Source IP", dstport AS "Destination Port"
FROM $log
WHERE $filter AND srcip = '10.0.1.10'
ORDER BY dstport
GROUP by srcip, dstport DESC
```

B)

```
SELECT srcip AS "Source IP", dstport AS "Destination Port"
FROM $log
WHERE $filter AND Source IP != '10.0.1.10'
GROUP BY srcip, dstport
ORDER BY dstport DESC
```

C)

```
SELECT srcip AS "Source IP", dstport AS "Destination Port"
ORDER BY dstport DESC
GROUP BY srcip, dstport
FROM $log
WHERE $filter AND srcip = '10.0.1.10'
```

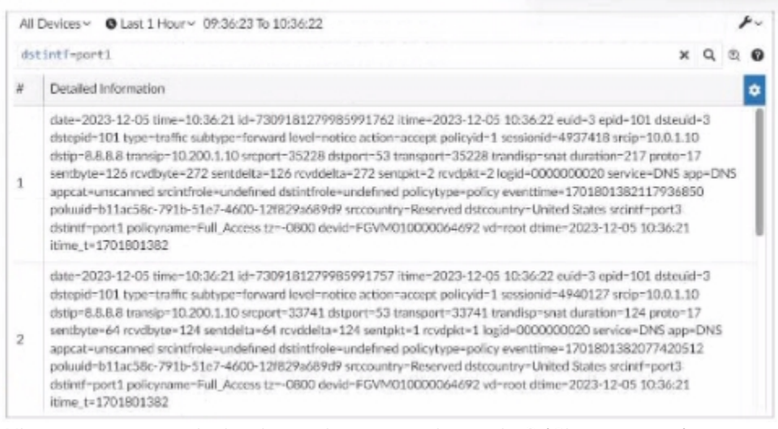
D)

```
SELECT srcip AS "Source IP", dstport AS "Destination Port"
FROM $log
WHERE $filter AND srcip = '10.0.1.10'
GROUP BY srcip, dstport
ORDER BY dstport DESC
```

A. Option A
B. Option B
C. Option C
D. Option D

Correct Answer: A
Section:
Explanation:
The requirement here is to construct a SQL query that retrieves logs with specific fields, namely 'Source IP' and 'Destination Port,' for entries where the source IP address matches 10.0.1.10. The correct syntax is essential for selecting, filtering, ordering, and grouping the results as shown in the expected outcome.
Analysis of the Options:
Option A Explanation:
SELECT srcip AS 'Source IP', dstport AS 'Destination Port': This syntax selects srcip and dstport, renaming them to 'Source IP' and 'Destination Port' respectively in the output.
FROM $log: Specifies the log table as the data source.
WHERE $filter AND srcip = '10.0.1.10': This line filters logs to only include entries with srcip equal to 10.0.1.10.
ORDER BY dstport DESC: Orders the results in descending order by dstport.
GROUP BY srcip, dstport: Groups results by srcip and dstport, which is valid SQL syntax.
This option meets all the requirements to get the expected results accurately.
Option B Explanation:
WHERE $filter AND Source IP != '10.0.1.10': Uses != instead of =. This would exclude logs from the specified IP 10.0.1.10, which is contrary to the expected result.
Option C Explanation:
The ORDER BY clause appears before the FROM clause, which is incorrect syntax. SQL requires the FROM clause to follow the SELECT clause directly.
Option D Explanation:
The GROUP BY clause should follow the FROM clause. However, here, it's located after WHERE, making it syntactically incorrect.
Conclusion:
Correct Answe r : A. Option A
This option aligns perfectly with standard SQL syntax and filters correctly for srcip = '10.0.1.10', while ordering and grouping as required.
FortiAnalyzer 7.4.1 SQL query capabilities and syntax for report customization.

QUESTION 5
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.

Correct Answer: A, D
Section:
Explanation:

In this exhibit, we observe a search query on the FortiAnalyzer interface displaying log data with details about the connection events, including fields like date, srcip, dstip, service, and dstintf. This setup allows for several functionalities within FortiAnalyzer.
Option A - Download Capability:
FortiAnalyzer provides the option to download search results and reports to a file in multiple formats, such as CSV or PDF, allowing for further offline analysis or archival. This makes it possible to save the search results shown in the exhibit to a file.
Conclusion: Correct.
Option B - Sorting and Customization:
The FortiAnalyzer interface allows users to sort and customize columns for search results. This helps in organizing and viewing the logs in a manner that fits the analyst's needs, such as ordering logs by time, srcip, dstip, or other fields.
Conclusion: Correct.
Option C - Availability in FortiView:
FortiView is a tool within FortiAnalyzer that visualizes data and provides analysis capabilities, including traffic and security event logs. Since these are traffic logs, they are typically available for visualization and analysis within FortiView.
Conclusion: Incorrect.
Option D - Text Mode Search:
The search displayed here appears to be in a structured format, which implies it might be utilizing filters rather than a free-text search. FortiAnalyzer allows both structured searches and text searches, but there's no indication here that text mode was used.
Conclusion: Incorrect.
Conclusion:
Correct Answe r : A. They can be downloaded to a file. and B. They are sortable by columns and customizable.
These options are consistent with FortiAnalyzer's capabilities for managing, exporting, and customizing log data.
FortiAnalyzer 7.4.1 documentation on search, export functionalities, and customizable views.

QUESTION 6
Which two methods can you use to send notifications when an event occurs that matches a configured event handler? (Choose two.)

A. Send Alert through Fabric Connectors
B. Send SNMP trap
C. Send SMS notification
D. Send Alert through FortiSIEM MEA

Correct Answer: B, C
Section:
Explanation:
In FortiAnalyzer, event handlers can be configured to trigger specific notifications when an event matches defined criteria. These notifications are designed to alert administrators in real time about critical events.
Option B - Send SNMP Trap:
FortiAnalyzer supports sending SNMP traps as one of the notification methods when an event matches an event handler. This allows integration with SNMP-enabled network management systems, which can then trigger further alerts or actions based on the trap received.
Conclusion: Correct.
Option C - Send SMS Notification:
FortiAnalyzer also supports SMS notifications, enabling alerts to be sent via SMS to predefined recipients. This method is useful for administrators who require immediate alerts but may not have access to email or other notification systems at all times.
Conclusion: Correct.
Option A - Send Alert through Fabric Connectors:
While Fabric Connectors allow FortiAnalyzer to interact with other parts of the Security Fabric, they are primarily used for data sharing and automation rather than directly for sending alerts or notifications.
Conclusion: Incorrect.
Option D - Send Alert through FortiSIEM MEA:
FortiSIEM integration allows for data sharing and further analysis within the Fortinet ecosystem, but it does not directly act as a notification method from FortiAnalyzer itself.
Conclusion: Incorrect.

Conclusion:
Correct Answe r : B. Send SNMP trap and C. Send SMS notification
These options represent valid notification methods for FortiAnalyzer's event handler configuration.
FortiAnalyzer 7.4.1 documentation on event handler configuration and available notification methods.

QUESTION 7
Exhibit.

```
FAZ # diagnose log device
Device Name           Device ID           Used Space(logs / quarantine / content / IPS) Allocated Space  Used%
FGT-A                 FGVM010000077646      332.0KB( 332.0KB/   0.0KB/   0.0KB/   0.0KB) unlimited        n/a
FGT-B                 FGVM010000064692      600.7MB( 600.7MB/   0.0KB/   0.0KB/   0.0KB) unlimited        n/a
FGT-C                 FGVM010000065036        1.2MB(   1.2MB/   0.0KB/   0.0KB/   0.0KB) unlimited        n/a
Total: 3 log devices, used=602.3MB quota=unlimited

AdomName          AdomOID  Type                                  Logs                                                    Database
                           [Retention   Quota      Used(    logs/quaranti/ content/     IPS) Used%]  [Retention   Quota      Used(  SiemDB/  hcache) Used%]
ADOM1             185      FSF  1000days   900.0MB  601.0MB( 601.0MB/   0.0KB/   0.0KB/   0.0KB) 66.8%   1000days    2.1GB    1.9GB(  67.9MB/  17.8KB) 92.4%
```

What can you conclude from this output?

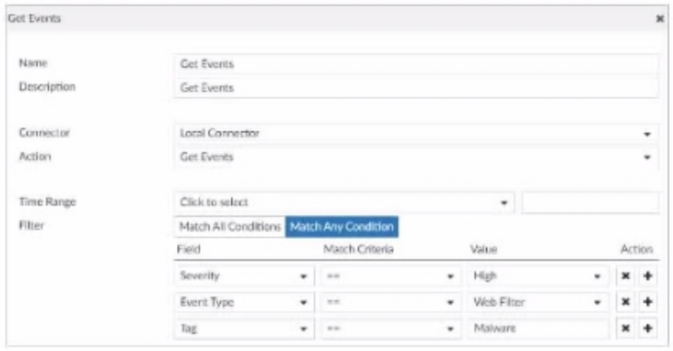
A. There is not disk quota allocated to quarantining files.
B. FGT_B is the Security Fabric root.
C. The allocated disk quote to ADOM1 is 3 GB.
D. Archive logs are using more space than analytic logs.

Correct Answer: C
Section:
Explanation:
The exhibit displays a diagnose log device output on a FortiAnalyzer, showing details about disk space usage and quotas for different FortiGate devices and ADOMs (Administrative Domains). Here's a breakdown of key details:
Disk Quota for Quarantined Files:
The output includes columns labeled for used space in categories such as 'logs,' 'quarantine,' 'content,' and 'DB.' For each device, the quarantine column consistently shows 0.0KB used, indicating that there is no disk quota allocated or utilized for quarantining files.
Conclusion: Correct.
FGT_B as Security Fabric Root:
There is no direct indication from this output that specifies FGT_B is the root of the Security Fabric. Information on Security Fabric topology or root designation would typically come from a Security Fabric configuration command rather than a disk usage summary.
Conclusion: Incorrect.
Allocated Disk Quota for ADOM1:
The output shows the quota for ADOM1 is 'unlimited,' not a fixed 3 GB quota. Therefore, there is no set 3 GB limit for ADOM1.
Conclusion: Incorrect.
Comparison of Archive Logs and Analytic Logs:
The output does not differentiate between archive logs and analytic logs; it only shows overall disk usage by type (e.g., logs, quarantine). Therefore, no conclusion can be made about which type of logs (archive or analytic) is using more space.
Conclusion: Incorrect.
Conclusion:
Correct Answe r : A. There is no disk quota allocated to quarantining files.
This answer aligns with the observed data, where no disk space is used or allocated for quarantine files.
FortiAnalyzer 7.4.1 documentation on diagnose log device command usage and disk quota settings.

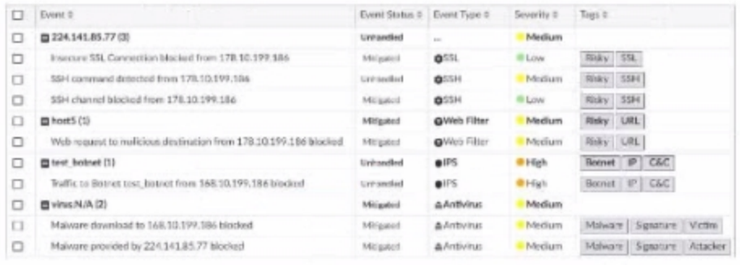
QUESTION 8
Exhibit.

Playbook Editor

Get Event task configuration



FortiAnalyzer Event Monitor



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.

Correct Answer: D
Section:
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 Answe r : 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.
FortiAnalyzer 7.4.1 documentation on event filtering, playbook configuration, and incident management criteria.

QUESTION 9
Which statement about SQL SELECT queries is true?

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

Correct Answer: D
Section:
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 Answe r : D. They are not used in macros.
This aligns with typical SQL usage and the specific functionalities of FortiAnalyzer.
FortiAnalyzer 7.4.1 documentation on SQL queries, database operations, and macro usage.

QUESTION 10
You find that as part of your role as an analyst, you frequently search log View using the same parameters.

Instead of defining your search filters repeatedly, what can you do to save time?

A. Configure a custom dashboard.
B. Configure a custom view.
C. Configure a data selector.
D. Configure a marco and apply it to device groups.

Correct Answer: B
Section:
Explanation:
When you frequently use the same search parameters in FortiAnalyzer's Log View, setting up a reusable filter or view can save considerable time. Here's an analysis of each option:
Option A - Configure a Custom Dashboard:
Custom dashboards are useful for displaying a variety of widgets and summaries on network activity, performance, and threat data, but they are not designed for storing specific search filters for log views.
Conclusion: Incorrect.
Option B - Configure a Custom View:
Custom views in FortiAnalyzer allow analysts to save specific search filters and configurations. By setting up a custom view, you can retain your frequently used search parameters and quickly access them without needing to reapply filters each time. This option is specifically designed to streamline the process of recurring log searches.
Conclusion: Correct.
Option C - Configure a Data Selector:
Data selectors are used to define specific types of data for FortiAnalyzer reports and widgets. They are useful in reports but are not meant for saving and reusing log search parameters in Log View.
Conclusion: Incorrect.
Option D - Configure a Macro and Apply It to Device Groups:
Macros in FortiAnalyzer are generally used for automation tasks, not for saving log search filters. Applying macros to device groups does not fulfill the requirement of saving specific log view search parameters.
Conclusion: Incorrect.
Conclusion:
Correct Answe r : B. Configure a custom view.
Custom views allow you to save specific search filters, enabling quick access to frequently used parameters in Log View.
FortiAnalyzer 7.4.1 documentation on creating and using custom views for log searches.

QUESTION 11
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.

Correct Answer: D
Section:
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 Answe r : 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.
FortiAnalyzer 7.4.1 documentation on configuring output profiles and report distribution settings.

QUESTION 12
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 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.

Correct Answer: C
Section:

QUESTION 13
Which statement about exporting items in Report Definitions is true?

A. Templates can be exported.
B. Template exports contain associated charts and datasets.
C. Chart exports contain associated datasets.
D. Datasets can be exported.

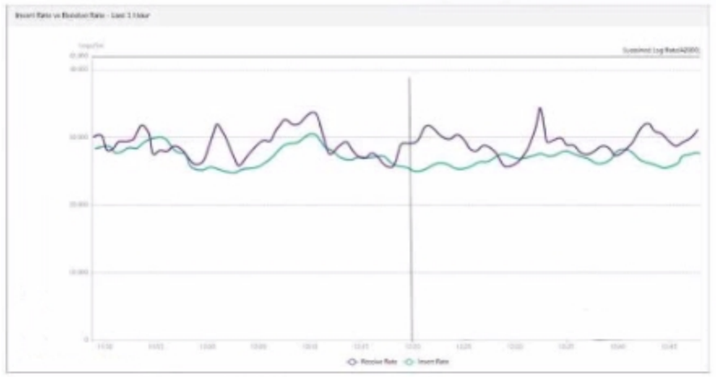
Correct Answer: B
Section:

QUESTION 14
Which log will generate an event with the status Contained?

A. An AV log with action=quarantine.
B. An IPS log with action=pass.
C. A WebFilter log will action=dropped.
D. An AppControl log with action=blocked.

Correct Answer: A
Section:

QUESTION 15
Exhibit.



What does the data point at 12:20 indicate?

A. The log insert log time is increasing.
B. FortiAnalyzer is using its cache to avoid dropping logs.
C. The performance of FortiAnalyzer is below the baseline.
D. The sqiplugind service is caught up with the logs

Correct Answer: A
Section:

QUESTION 16
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.

Correct Answer: B
Section:

QUESTION 17
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 to 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.

Correct Answer: A
Section:

QUESTION 18

What happens when the indicator of compromise (IOC) engine on FortiAnalyzer finds web logs that match blacklisted IP addresses?

A. FortiAnalyzer flags the associated host for further analysis.
B. A new infected entry is added for the corresponding endpoint under Compromised Hosts.
C. The detection engine classifies those logs as Suspicious.
D. The endpoint is marked as Compromised and, optionally, can be put in quarantine.

Correct Answer: B
Section:

QUESTION 19
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.

Correct Answer: B
Section:
Explanation:
Macros in FortiAnalyzer are used to streamline reporting tasks by automating data extraction and report generation. Here's a breakdown of each option to determine the correct answer:
Option A - Macros are Predefined Templates for Reports and Cannot be Customized:
This statement is incorrect. Macros in FortiAnalyzer are not simply fixed templates; they allow for customization to tailor data extraction and reporting based on specific needs and configurations.
Conclusion: Incorrect.
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.
Conclusion: Correct.
Option C - Macros are ADOM-Specific and Each ADOM Type Has Unique Macros Relevant to that ADOM:
Macros are not limited to specific ADOMs, nor are they ADOM-specific. Macros can be applied across various ADOMs based on report configurations but are not inherently tied to or unique for each ADOM type.
Conclusion: Incorrect.
Option D - Macros are Supported Only on the FortiGate ADOMs:
This is not true. Macros in FortiAnalyzer are not restricted to FortiGate ADOMs; they can be utilized across different ADOMs that FortiAnalyzer manages.
Conclusion: Incorrect.
Conclusion:
Correct Answe r : B. Macros are useful in generating excel log files automatically based on the report settings.
This answer correctly describes the functionality of macros in FortiAnalyzer, emphasizing their role in automating report generation, especially for Excel log files.
FortiAnalyzer 7.4.1 documentation on macros and report generation functionalities.

QUESTION 20
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.

Correct Answer: D
Section: