NEW QUESTION 1
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?

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

Answer: B
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.

NEW 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

NEW 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.

NEW 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

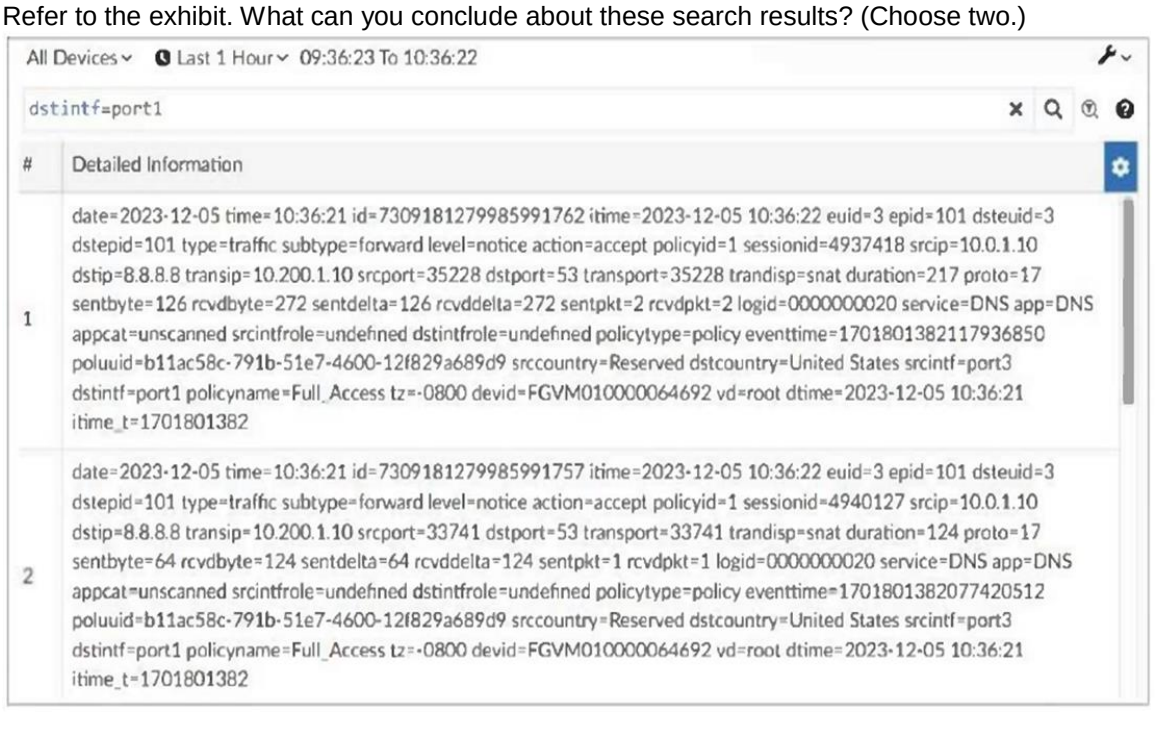
NEW QUESTION 5
After generating a report, you notice the information you were expecting to see is not included in it. However, you confirm that the logs are there.
Which two actions should you perform? (Choose two.)

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.

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



A. The logs have been parsed by FortiGate log parser.
B. They were searched using text mode.
C. They are sortable by columns and customizable.
D. They can be downloaded to a CSV file.

Answer: BD
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.

NEW 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.

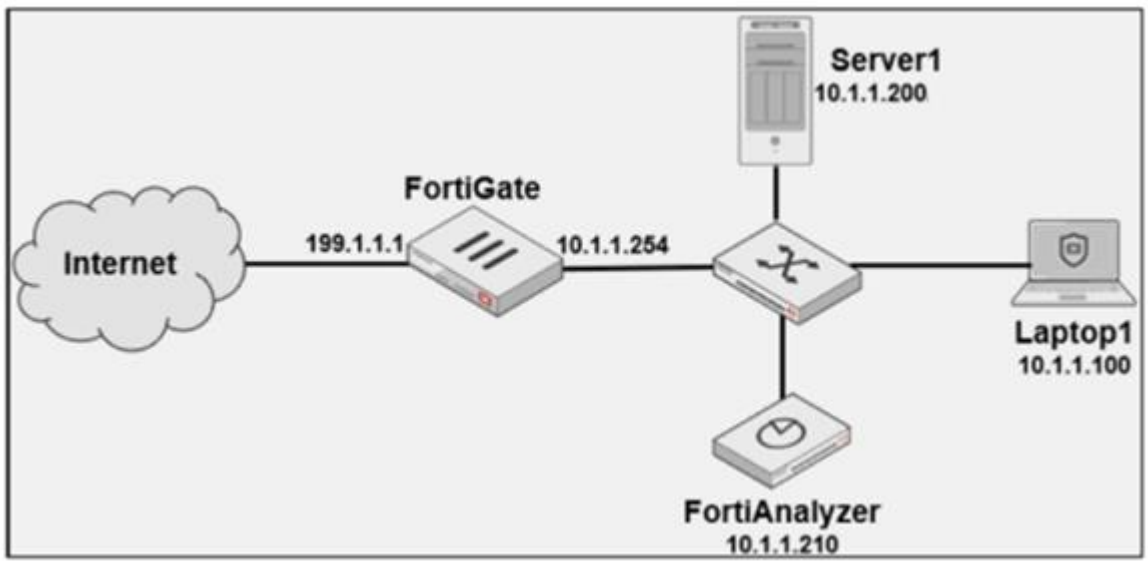
Deploying FortiAnalyzer units in both analyzer and collector modes distributes log collection across sites while centralizing analysis. Collectors at branches forward logs to central analyzers, optimizing performance and reducing WAN bandwidth.

NEW 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.

NEW 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

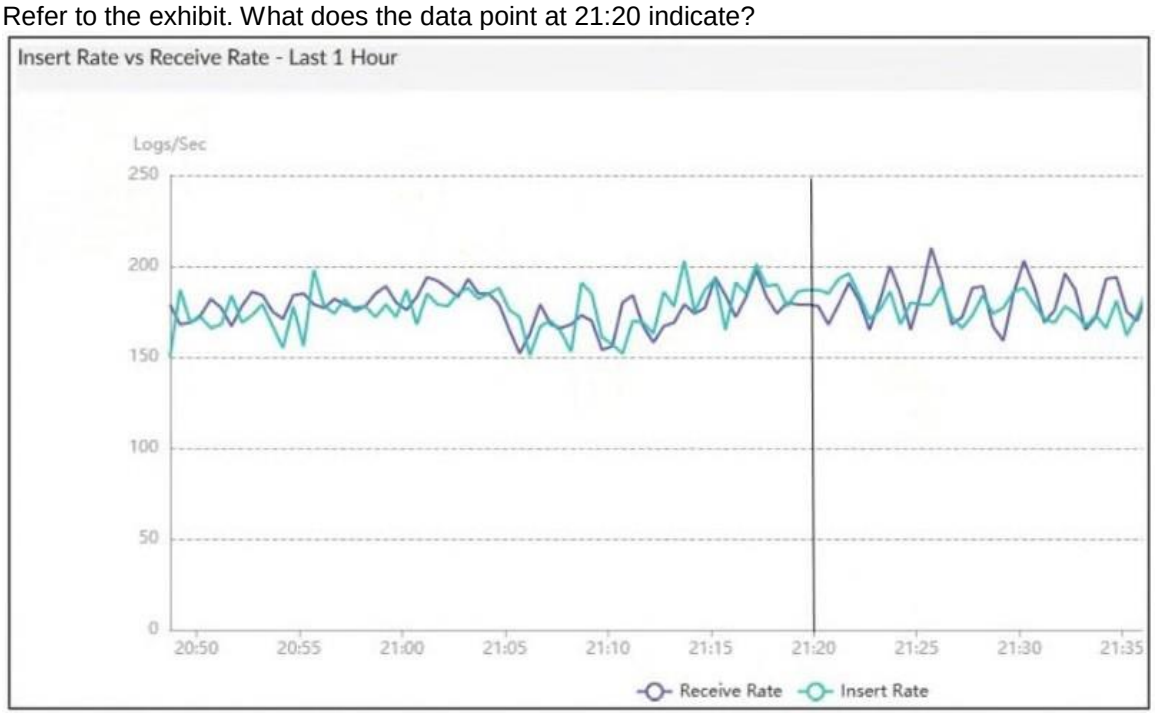
Answer: A
Explanation:
On there the task was to create a filter for failed logins from any other location but the local computer:
"Add the text performed_on!~10.0.1.10.
This includes any attempts coming from devices with an IP address that is not the one configured on the Local-Client computer."

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

A. Local logs are not displayed in FortiView.
B. Playbook logs for all ADOMs are in the root ADOM.
C. Application control logs are ADOM specific.
D. Event logs are available 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

NEW QUESTION 11
Refer to the exhibit. What does the data point at 21:20 indicate?



A. FortiAnalyzer is indexing logs faster than logs are being received.
B. The `sqlpugind` daemon is behind in receiving logs by one log.
C. The `fortilogd` daemon is ahead in indexing by one log.
D. The log insert lag time is high.

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

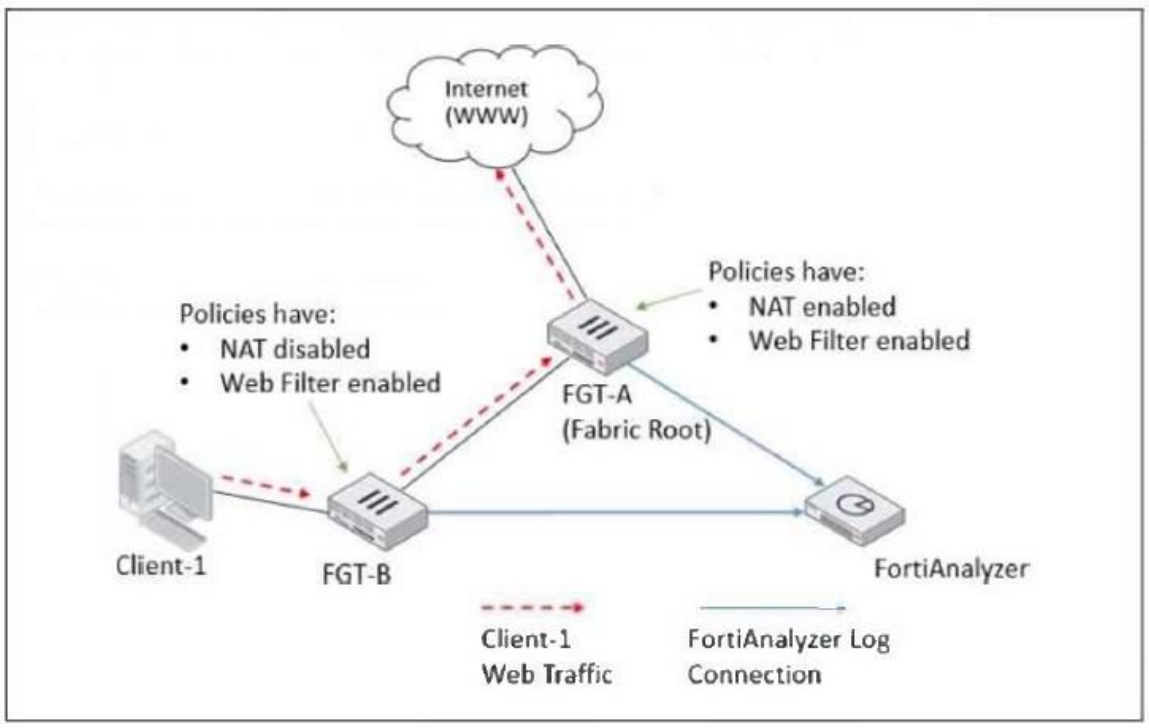
situation suggests that FortiAnalyzer is able to keep up with the incoming logs and is possibly processing a backlog or temporarily received logs faster than new logs are coming in.

NEW 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.

NEW 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. FGT-A will create all traffic logs except for security logs.

Answer: A
Explanation:
Each FortiGate independently logs all sessions that pass through it when logging is enabled on its policies. In this topology, both FGT-B (where Client-1's traffic first enters) and FGT-A (which forwards the traffic to the internet) see and log the session, so both devices generate traffic logs for this web-browsing flow.

NEW QUESTION 14
What are two effects of enabling auto-cache in a FortiAnalyzer report? (Choose two.)

A. The size of newly generated reports is optimized to conserve disk space.
B. The hcache data is updated automatically when new logs are received.
C. The report generation time is reduced.
D. FortiAnalyzer local cache is used to store generated reports.

Answer: BC
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.

NEW QUESTION 15
What is the purpose of running the command `diagnose sql status sqlplugind`?

A. To view the amount of time between log received and log inserted into the database
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: D
Explanation:
The command diagnose sql status sqlplugind checks the status of log insertion into the SQL database, showing how many logs have been received, inserted, or are pending, which helps monitor FortiAnalyzer's log processing performance.

NEW QUESTION 16

Refer to the exhibit. What can you conclude about the output?

```
FAZ # diagnose fortilogd lograte
last 5 seconds: 78.8, last 30 seconds: 132.1, last 60 seconds: 133.3

FAZ # diagnose fortilogd msgrate
last 5 seconds: 1.4, last 30 seconds: 1.6, last 60 seconds: 1.6
```

A. The low indexing values require investigation.
B. The output is not ADOM specific.
C. There are more event logs than traffic logs.
D. The log rate higher than the message rate is not normal.

Answer: B
Explanation:
The commands diagnose fortilogd lograte and diagnose fortilogd msgrate shown are global FortiAnalyzer diagnostic commands that provide log and message rates without reference to any specific ADOM (Administrative Domain). Therefore, the output is not ADOM specific.

NEW QUESTION 17
As part of your analysis, you discover that a Medium severity level incident is fully remediated.
You change the incident status to Closed: Remediated.
Which statement about your update is true?

A. The incident can no longer be deleted.
B. The corresponding event will be marked as Mitigated.
C. The incident dashboard will be updated.
D. The incident severity will be lowered.

Answer: C
Explanation:
Changing an incident's status to Closed: Remediated means the incident has been resolved and no longer requires active attention. This action inherently impacts the incident dashboard, which tracks key metrics like active incidents, mean time to resolution, and incident status distribution. The dashboard dynamically updates to reflect the current state of all incidents, including those newly closed.

NEW QUESTION 18
What is the purpose of playbook trigger variables?

A. To display statistics about the playbook runtime
B. To use information from the trigger to filter the action in a task
C. To provide the trigger information to make the playbook start running
D. To store the start the times of playbooks with On_Schedule triggers

Answer: B
Explanation:
Trigger variables allow you to use information from the trigger of a playbook when it has been configured with an incident or event trigger. For example, a single playbook can be triggered by more than one device. A Run Report action can include a filter for the endpoint IP address from the event that triggered the playbook.

NEW QUESTION 19
Which statement correctly describes one difference between templates and reports?

A. Reports provide more configuration options than templates
B. Templates can be cloned, but reports cannot be cloned
C. Reports support macros, but templates do not
D. Templates are mapped to device groups, while reports are mapped to ADOMs

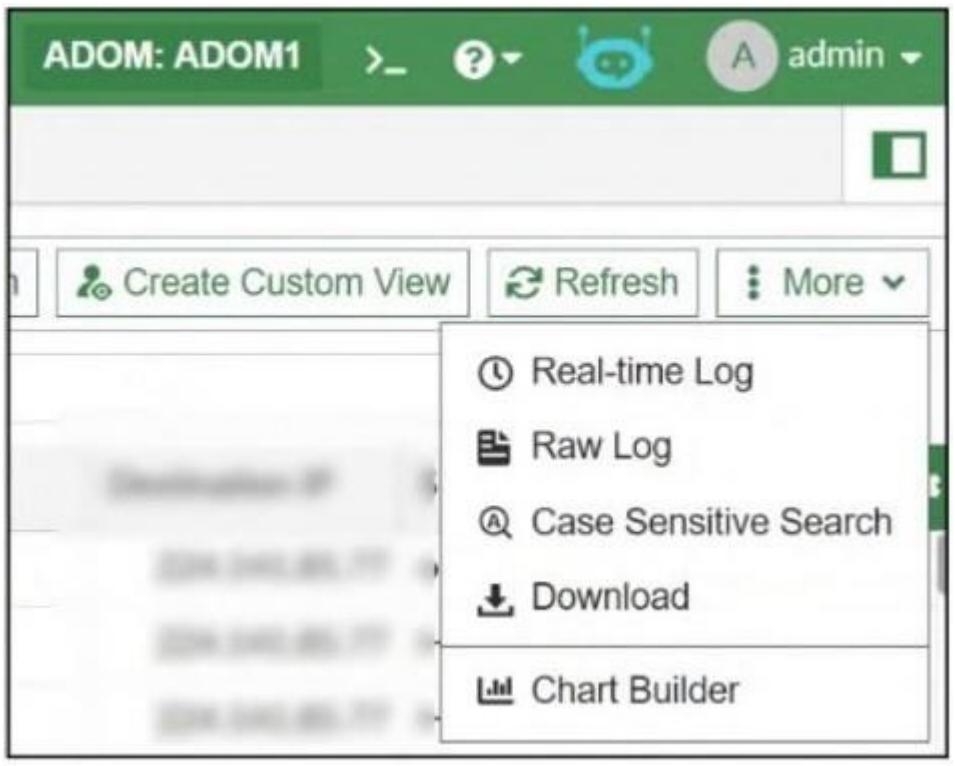
Answer: A
Explanation:
In the context of some network management or reporting systems (like FortiAnalyzer, which is implied by the exam NEW QUESTIONs in the search results), reports and templates have different functionalities:
- Templates are pre-defined layouts for generating reports, and while they can be customized to an extent (often by cloning and then editing the clone), they have a more limited scope for configuration than a full report. Predefined templates, specifically, cannot be edited directly, only cloned.
- Reports, when being generated or configured, allow for more extensive customization and configuration options at the time of creation or execution, such as data sources, time ranges, filters, and output formats.

NEW QUESTION 20
Which statement about sending notifications with incident updates is true?

A. Each connector used can have different notification settings
B. Each incident can send notification to a single external platform.
C. You must configure an output profile to send notifications by email.
D. Notifications can be sent only when an incident is created oi deleted.

Answer: A
Explanation:
Incidents will usually go through several stages during the analysis process. In most cases, it is important to make sure all parties involved are notified when the incident status is updated.
You can add more than one fabric connector, each with the same or different notification settings. The receiving side of the connector must be configured for the notifications to be sent successfully.

NEW QUESTION 21
Refer to the 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
Explanation:
A quick way to build a custom dataset and chart is to use the chart builder tool. This tool is located in LogView, and allows you to build a dataset and chart automatically, based on your filtered search results. In LogView, set filters to return the logs you want.

NEW QUESTION 22
Which two statements 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: AB
Explanation:
The FortiAnalyzer Outbreak Detection Service is a licensed feature that requires a valid license to access outbreak alerts, event handlers, and reports. Without a valid license, these features are not available, and only a default alert page is shown.
When licensed, the service automatically downloads outbreak-related event handlers and reports from FortiGuard, enabling timely detection and response to emerging malware outbreaks.
https://docs.fortinet.com/document/fortianalyzer/7.0.0/new-features/371125/fortiguard-outbreak-detection-service
https://docs.fortinet.com/document/fortianalyzer/7.6.3/administration-guide/658619/outbreak-alerts

NEW QUESTION 23
You must find a specific security event log in the FortiAnalyzer logs displayed in FortiView, but, so far, you have been unsuccessful.
Which two tasks should you perform to investigate why you are having this issue? (Choose two.)

A. Disable FortiView using the CLI and then enable it again.
B. Rebuild the SQL database and check FortiView.
C. Review the ADOM data policy.
D. Check logs in Log Browse.

Answer: CD
Explanation:
Checking logs directly in Log Browse helps verify if the event logs exist and are correctly ingested.
Reviewing the ADOM data policy ensures that the logs are permitted and visible within the current ADOM context, which can affect log visibility in FortiView.

NEW QUESTION 24
Which two statements about playbook execution are true? (Choose two.)

A. FortiAnalyzer will commit changes made by a Failed playbook.
B. You can run the default debugging playbook to investigate playbook errors.
C. The Playbook Monitor provides troubleshooting logs.
D. If the playbook status is Failed, all individual tasks in the playbook will fail.

Answer: BC
Explanation:
FortiAnalyzer provides a default debugging playbook that can be used to help investigate and troubleshoot playbook execution errors. The Playbook Monitor displays execution details and logs, which assist in identifying the cause of failures and analyzing task behavior during playbook runs.

NEW QUESTION 25
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: BD
Explanation:
Reviewing report diagnostics helps identify performance bottlenecks and errors during report generation.
Enabling auto-cache improves report generation speed by caching report data for faster retrieval on subsequent runs.

NEW QUESTION 26
Which two statements about exporting and importing playbacks are true? (Choose two.)

A. A playbook that was disabled when it was exported mil be disabled when it is imported.
B. Playbooks can so imported 10 a different FortiAnayzer device, but only if the connectors already exist
C. You can import a playbook even if there is another one win the same name in the destination
D. You can export only one playbook at a time.

Answer: AC
Explanation:
Playbooks are imported with the same status they had (enabled or disabled) when they were exported.
If the imported playbook has the same name as an existing one, FortiAnalyzer will create a new name that includes a timestamp to avoid conflicts.
……