Fortinet

Exam Questions FCP_FAZ_AN-7.4

FCP - FortiAnalyzer 7.4 Analyst

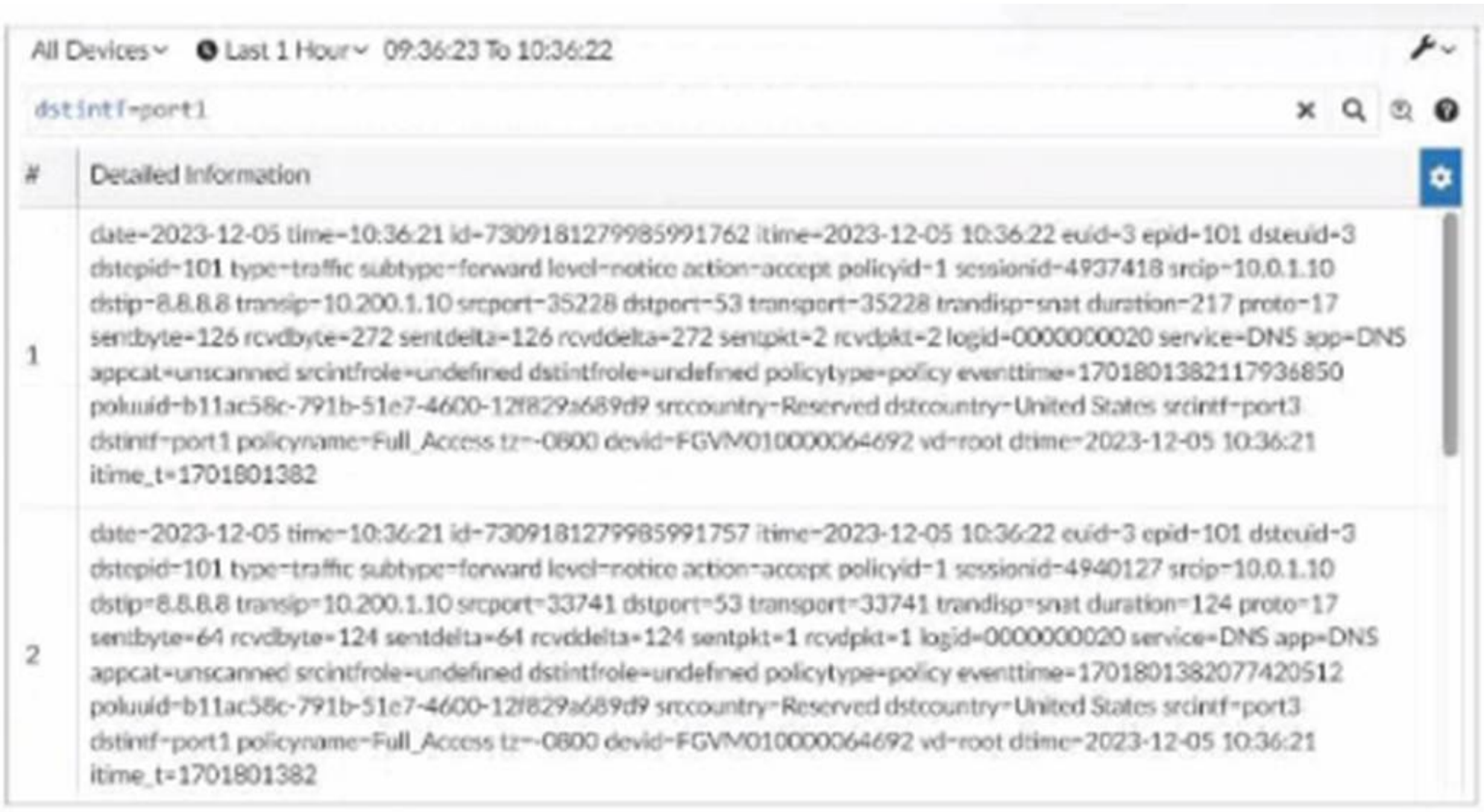
NEW QUESTION 1
After a generated a repot, you notice the information you were expecting to see in not included in it. However, you confirm that the logs are there:
Which two actions should you perform? (Choose two.)

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:
? Option B - Disable Auto-Cache:
? Option C - Increase the Report Utilization Quota:
? Option D - Test the Dataset:
Conclusion:
? Correct Answer: A. Check the time frame covered by the report and D. Test the dataset.
? These actions directly address the issues that could cause missing information in a report when logs are available but not displayed.
References:
? FortiAnalyzer 7.4.1 documentation on report generation settings, time frames, and dataset configuration.

NEW QUESTION 2
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:
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:
? Option B - Sorting and Customization:
? Option C - Availability in FortiView:
? Option D - Text Mode Search:
Conclusion:
? Correct Answer: 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.
References:
? FortiAnalyzer 7.4.1 documentation on search, export functionalities, and customizable views.

NEW QUESTION 3
Which statement about sending notifications with incident update is true?

A. You can send notifications to multiple external platforms.
B. Notifications can be sent only by email.
C. If you use multiple fabric connectors, all connectors must have the same settings.
D. Notifications can be sent only when an incident is updated or deleted.

Answer: A

Explanation:
In FortiOS and FortiAnalyzer, incident notifications can be sent to multiple external platforms, not limited to a single method such as email. Fortinet's security fabric and integration capabilities allow notifications to be sent through various fabric connectors and third-party integrations. This flexibility is designed to ensure that incident updates reach relevant personnel or systems using preferred communication channels, such as email, Syslog, SNMP, or integration with SIEM platforms.
Let??s review each answer option for clarity:
? Option A: You can send notifications to multiple external platforms
? Option B: Notifications can be sent only by email
? Option C: If you use multiple fabric connectors, all connectors must have the same settings
? Option D: Notifications can be sent only when an incident is updated or deleted
References: According to FortiOS and FortiAnalyzer 7.4.1 documentation, notifications for incidents can be configured across various platforms by using multiple connectors, and they are not limited to email alone. This capability is part of the Fortinet Security Fabric, allowing for a broad range of integrations with external systems and platforms for effective incident response.

NEW QUESTION 4
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.

Answer: B

NEW QUESTION 5
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.

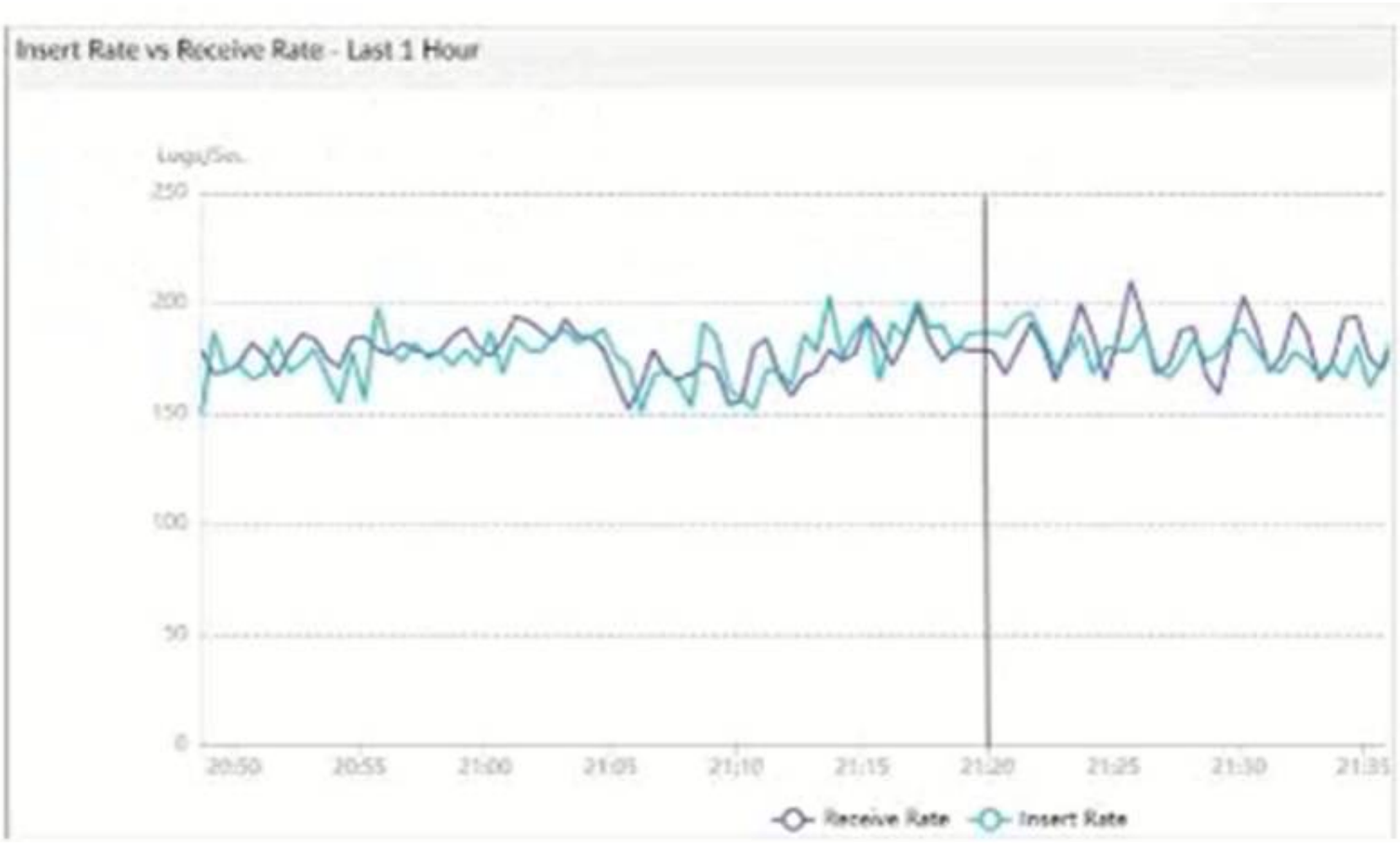
Answer: A

NEW QUESTION 6
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.

Answer: A

NEW QUESTION 7
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:
? Data Point at 21:20:
? Option Analysis:
Conclusion:
? Correct Answer: A. FortiAnalyzer is indexing logs faster than logs are being received.
? The graph at 21:20 shows a higher Insert Rate than Receive Rate, indicating efficient log processing by FortiAnalyzer.
References:
? FortiAnalyzer 7.4.1 documentation on log processing metrics, Receive Rate, and Insert Rate indicators.

NEW QUESTION 8
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. Here??s a breakdown of each option to determine the correct Answer
? Option A - Macros are Predefined Templates for Reports and Cannot be
Customized:
? Option B - Macros are Useful in Generating Excel Log Files Automatically Based on the Report Settings:
? Option C - Macros are ADOM-Specific and Each ADOM Type Has Unique Macros Relevant to that ADOM:
? Option D - Macros are Supported Only on the FortiGate ADOMs:
Conclusion:
? Correct Answer: 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.
References:
? FortiAnalyzer 7.4.1 documentation on macros and report generation functionalities.

NEW QUESTION 9
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.

Answer: B

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:
? Option B - Configure a Custom View:
? Option C - Configure a Data Selector:
? Option D - Configure a Macro and Apply It to Device Groups:
Conclusion:
? Correct Answer: B. Configure a custom view.
? Custom views allow you to save specific search filters, enabling quick access to frequently used parameters in Log View.
References:
? FortiAnalyzer 7.4.1 documentation on creating and using custom views for log searches.

NEW QUESTION 10
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 A - Forwarding Logs to a Syslog Server in Collector Mode:
? Option B - Default Mode is Collector Mode Unless Configured for HA:
? Option C - Report Creation and Editing in Collector Mode:
? Option D - Performance Improvement with Both Modes in Topology:
Conclusion:
? Correct Answer: B. FortiAnalyzer runs in collector mode by default unless it is configured for HA and D. A topology with FortiAnalyzer devices running in both modes can improve their performance.
? These answers correctly describe the functionality and default configuration of FortiAnalyzer operating modes, along with how a mixed-mode topology can enhance performance.
References:
? FortiAnalyzer 7.4.1 documentation on operating modes (Collector and Analyzer) and their respective capabilities.

NEW QUESTION 10
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: A

NEW QUESTION 11
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.

Answer: A

NEW QUESTION 14
Exhibit.

```
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
```

What can you conclude about the output?

A. The message rate being lower that the log rate is normal.
B. Both messages and logs are almost finished indexing.

C. There are more traffic logs than event logs.
D. The output is ADOM specific

Answer: A

Explanation:
In this output, we see two diagnostic commands executed on a FortiAnalyzer device:
? diagnose fortilogd lograte: This command shows the rate at which logs are being processed by the FortiAnalyzer in terms of log entries per second.
? diagnose fortilogd msgrate: This command displays the message rate, or the rate at which individual messages are being processed.
The values provided in the exhibit output show:
? Log rate (lograte): Consistently high, showing values such as 70.0, 132.1, and 133.3 logs per second over different time intervals.
? Message rate (msgrate): Lower values, around 1.4 to 1.6 messages per second. Explanation
? Interpretation of log rate vs. message rate: In FortiAnalyzer, the log rate typically refers to the rate of logs being stored or indexed, while the message rate refers to individual messages within these logs. Given that a single log entry can contain multiple messages, it's common to see a lower message rate relative to the log rate.
? Understanding normal operation: In this case, the message rate being lower than the log rate is expected and typical behavior. This discrepancy can arise because each log entry may bundle multiple related messages, reducing the message rate relative to the log rate.
Conclusion
? Correct Answer: A. The message rate being lower than the log rate is normal.
? This aligns with the normal operational behavior of FortiAnalyzer in processing logs and messages.
There is no indication that both logs and messages are nearly finished indexing, as that would typically show diminishing rates toward zero, which is not the case here. Additionally, there??s no information in this output about specific ADOMs or a comparison between traffic logs and event logs. Thus, options B, C, and D are incorrect.
References:
? FortiOS 7.4.1 and FortiAnalyzer 7.4.1 command guides for diagnose fortilogd lograte and diagnose fortilogd msgrate.

NEW QUESTION 19
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: CD

NEW QUESTION 21
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.
Let's review the other options to clarify why they are incorrect:
? Option A: You can manually attach generated reports to incidents
? Option B: The status of the incident is always linked to the status of the attached event
? Option C: Severity incidents rated with the level High have an initial service-level agreement (SLA) response time of 1 hour
? Option D: Incidents must be acknowledged before they can be analyzed References: 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 25
Which log will generate an event with the status Unhandled?

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.

Answer: B

Explanation:
In FortiOS 7.4.1 and FortiAnalyzer 7.4.1, the "Unhandled" status in logs typically signifies that the FortiGate encountered a security event but did not take any specific action to block or alter it. This usually occurs in the context of Intrusion Prevention System (IPS) logs.
? IPS logs with action=pass: When the IPS engine inspects traffic and determines
that it does not match any known attack signatures or violate any configured policies, it assigns the action "pass". Since no action is taken to block or modify this traffic, the status is logged as "Unhandled."
Let's look at why the other options are incorrect:
? An AV log with action=quarantine: Antivirus (AV) logs with the action "quarantine" indicate that a file was detected as malicious and moved to quarantine. This is a definitive action, so the status wouldn't be "Unhandled."
? A WebFilter log will action=dropped: WebFilter logs with the action "dropped" indicate that web traffic was blocked according to the configured web filtering policies. Again, this is a specific action taken, not an "Unhandled" event.
? An AppControl log with action=blocked: Application Control logs with the action "blocked" mean that an application was denied access based on the defined application control rules. This is also a clear action, not "Unhandled."

NEW QUESTION 26

.....

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-7.4 Practice Exam Features:

* FCP_FAZ_AN-7.4 Questions and Answers Updated Frequently

* FCP_FAZ_AN-7.4 Practice Questions Verified by Expert Senior Certified Staff

* FCP_FAZ_AN-7.4 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* FCP_FAZ_AN-7.4 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year