Fortinet

Exam Questions FCP_FAZ_AN-7.4

FCP - FortiAnalyzer 7.4 Analyst

NEW QUESTION 1
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 in FortiAnalyzer is identified as a false positive and its status is updated to "Closed: False Positive," certain records and logs are updated to reflect this change.
? Option A - The Audit History Log Will Be Updated:
? Option B - The Corresponding Event Will Be Marked as Mitigated:
? Option C - The Incident Will Be Deleted:
? Option D - The Incident Number Will Be Changed:
Conclusion:
? Correct Answer: A. The audit history log will be updated.
? This is the most accurate answer, as the update to "Closed: False Positive" is recorded in FortiAnalyzer??s audit history log for accountability and tracking purposes.
References:
? FortiAnalyzer 7.4.1 documentation on incident management and audit history logging.

NEW QUESTION 2
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 3
What is the purpose of running the command diagnose sql status sqlreportd?

A. To view a list of scheduled reports
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: C

Explanation:
The command diagnose sql status sqlreportd is used in FortiAnalyzer to obtain specific information about the SQL reporting process and caching status. Here??s what this command accomplishes and an analysis of each option:
? Command Functionality:
? Option Analysis:
Conclusion:
? Correct Answer: C. To display the SQL query connections and hcache status
? This command is used to monitor SQL reporting activities and cache status, aiding in the analysis of report generation performance and connection health.
References:
? FortiAnalyzer 7.4.1 documentation on SQL diagnostic commands, particularly those related to reporting (sqlreportd) and caching mechanisms.

NEW QUESTION 4
Which SQL query is in the correct order to query to database in the FortiAnalyzer?

A. SELECT devid FROM $log GROUP BY devid WHERE ??user??,,?? users1??
B. SELECT FROM $log WHERE devid ??user??,, USER1?? GROUP BY devid
C. SELCT devid WHERE ??user??-?? USER1?? FROM $log GROUP By devid
D. SELECT devid FROM $log WHERE ??user??=?? GROUP BY devid

Answer: D

Explanation:
In FortiAnalyzer??s SQL query syntax, the typical order for querying the database follows the standard SQL format, which is:
SELECT <column(s)> FROM <table> WHERE <condition(s)> GROUP BY <column(s)>
? Option D correctly follows this structure:
Let??s briefly examine why the other options are incorrect:
? Option A: SELECT devid FROM $log GROUP BY devid WHERE 'user', 'users1'
? Option B: SELECT FROM $log WHERE devid 'user', USER1' GROUP BY devid
? Option C: SELCT devid WHERE 'user' - 'USER1' FROM $log GROUP BY devid References: FortiAnalyzer documentation for SQL queries indicates that the standard SQL order should be followed when querying logs in FortiAnalyzer. Queries should follow the format SELECT ... FROM ... WHERE ... GROUP BY ..., as demonstrated in option D.

NEW QUESTION 5
Why must you wait for several minutes before you run a playbook that you just created?

A. FortiAnalyzer needs that time to parse the new playbook.
B. FortiAnalyzer needs that time to debug the new playbook.
C. FortiAnalyzer needs that time to back up the current playbooks.
D. FortiAnalyzer needs that time to ensure there are no other playbooks running.

Answer: A

Explanation:
When a new playbook is created on FortiAnalyzer, the system requires some time to parse and validate the playbook before it can be executed. Parsing involves checking the playbook's structure, ensuring that all syntax and logic are correct, and preparing the playbook for execution within FortiAnalyzer??s automation engine. This initial parsing step is necessary for FortiAnalyzer to load the playbook into its operational environment correctly.
Here??s why the other options are incorrect:
? Option A: FortiAnalyzer needs that time to parse the new playbook
? Option B: FortiAnalyzer needs that time to debug the new playbook
? Option C: FortiAnalyzer needs that time to back up the current playbooks
? Option D: FortiAnalyzer needs that time to ensure there are no other playbooks running
References: FortiAnalyzer documentation states that after creating a playbook, a brief delay is expected as the system parses and validates the playbook. This ensures that any syntax errors or logical inconsistencies are resolved before the playbook is executed, making option A the correct answer.

NEW QUESTION 6
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 7
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 8
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 9
You must find a specific security event log in the FortiAnalyzer logs displayed in FortiView, but, so far, you have been uncuccessful.
Which two tasks should you perform to investigate why you are having this issue? (Choose two.)

A. Open .gz log files in FortiView.
B. Rebuild the SQL database and check FortiView.
C. Review the ADOM data policy
D. Check logs in the Log Browse

Answer: AB

NEW QUESTION 10
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 10
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.

Answer: A

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:
? Option Analysis:
Conclusion:
? Correct Answer: 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.
References:
? FortiAnalyzer 7.4.1 documentation on exporting playbooks and data compression methods.

NEW QUESTION 14
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.

Answer: C

NEW QUESTION 17
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.

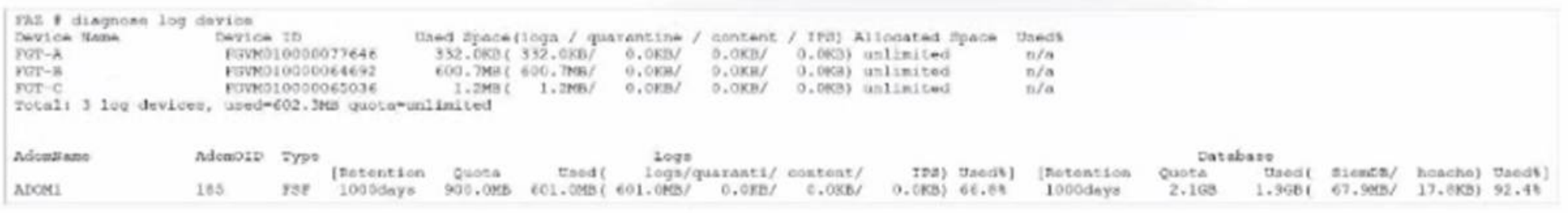
Answer: A

NEW QUESTION 22
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.

Answer: D

NEW QUESTION 23
Exhibit.



```
FAZ # diagnose log device
Device Name          Device ID           Used Space(logs / quarantine / content / IPS) Allocated Space  Used%
FGT-A                FGVM010000077646      352.0KB( 352.0KB/   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.

Answer: C

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:
? FGT_B as Security Fabric Root:
? Allocated Disk Quota for ADOM1:
? Comparison of Archive Logs and Analytic Logs:
Conclusion:
? Correct Answer: 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.
References:
? FortiAnalyzer 7.4.1 documentation on diagnose log device command usage and disk quota settings.

NEW QUESTION 24
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 29
Exhibit.

FortiAnalyzer partial configuration output

```
FortiAnalyzer1# get system status
Platform Type                : FAZVM64-KVM
Platform Full Name           : FortiAnalyzer-VM64-KVM
Version                      : v7.4.1-build2308 230831 (GA)
Serial Number                : FAZ-VM0000065040
BIOS version                 : 04000002
Hostname                     : FortiAnalyzer1
Max Number of Admin Domains  : 5
Admin Domain Configuration   : Enabled
FIPS Mode                    : Disabled
HA Mode                      : Stand Alone
Branch Point                 : 2308
Release Version Information  : GA
Time Zone                    : (GMT-8:00) Pacific Time (US & Canada)
Disk Usage                   : Free 43.60GB, Total 58.80GB
File System                  : Ext4
License Status               : Valid

FortiAnalyzer1# get system global
adom-mode                    : normal
adom-select                  : enable
adom-status                  : enable
console-output               : standard
country-flag                 : enable
enc-algorithm                : high
ha-member-auto-grouping      : enable
hostname                     : FortiAnalyzer1
log-checksum                 : md5
log-forward-cache-size       : 5
log-mode                     : analyzer
longitude                    : (null)
max-aggregation-tasks        : 0
max-running-reports          : 1
oftp-ssl-protocol            : tlsv1.2
ssl-low-encryption           : disable
ssl-protocol                 : tlsv1.3 tlsv1.2
task-list-size               : 2000
webservice-proto             : tlsv1.3 tlsv1.2
```

```
FortiAnalyzer2# get system status
Platform Type                : FAZVM64-KVM
Platform Full Name           : FortiAnalyzer-VM64-KVM
Version                      : v7.4.1-build2308 230831 (GA)
Serial Number                : FAZ-VM0000065041
BIOS version                 : 04000002
Hostname                     : FortiAnalyzer2
Max Number of Admin Domains  : 5
Admin Domain Configuration   : Enabled
FIPS Mode                    : Disabled
HA Mode                      : Stand Alone
Branch Point                 : 2308
Release Version Information  : GA
Time Zone                    : (GMT-8:00) Pacific Time (US & Canada)
Disk Usage                   : Free 45.75GB, Total 58.80GB
File System                  : Ext4
License Status               : Valid

FortiAnalyzer2# get system global
adom-mode                    : normal
adom-select                  : enable
adom-status                  : enable
console-output               : standard
country-flag                 : enable
enc-algorithm                : high
ha-member-auto-grouping      : enable
hostname                     : FortiAnalyzer2
log-checksum                 : md5
log-forward-cache-size       : 5
log-mode                     : analyzer
longitude                    : (null)
max-aggregation-tasks        : 0
max-running-reports          : 1
oftp-ssl-protocol            : tlsv1.2
ssl-low-encryption           : disable
ssl-protocol                 : tlsv1.3 tlsv1.2
task-list-size               : 2000
webservice-proto             : tlsv1.3 tlsv1.2
```

```
FortiAnalyzer3# get syste
Platform Type
Platform Full Name
Version                      : v7.4.1-build2308 230831 (GA)
Serial Number                : FAZ-VM0000065042
BIOS version                 : 04000002
Hostname                     : FortiAnalyzer3
Max Number of Admin Domains  : 5
Admin Domain Configuration   : Enabled
FIPS Mode                    : Disabled
HA Mode                      : Stand Alone
Branch Point                 : 2308
Release Version Information  : GA
Time Zone                    : (GMT-8:00) Pacific Time (US & Canada)
Disk Usage                   : Free 53.06GB, Total 79.80GB
File System                  : Ext4
License Status               : Valid

FortiAnalyzer3# get system global
adom-mode                    : normal
adom-select                  : enable
adom-status                  : enable
console-output               : standard
country-flag                 : enable
enc-algorithm                : high
ha-member-auto-grouping      : enable
hostname                     : FortiAnalyzer3
log-checksum                 : md5
log-forward-cache-size       : 5
log-mode                     : analyzer
longitude                    : (null)
max-aggregation-tasks        : 0
max-running-reports          : 5
oftp-ssl-protocol            : tlsv1.2
ssl-low-encryption           : disable
ssl-protocol                 : tlsv1.3 tlsv1.2
task-list-size               : 2000
webservice-proto             : tlsv1.3 tlsv1.2
```

Based on the partial outputs displayed, which devices can be members of a FotiAnalyzer Fabric?

A. FortiAnalayzer1 and FortiAnalyzer3
B. FortiAnalyzer1 and FortiAnalyzer2
C. FortiAnalyzer2 and FortiAnalyzer3
D. All devices listed can be members.

Answer: D

Explanation:
In a FortiAnalyzer Fabric, devices can participate in a cluster or grouping if they meet specific compatibility criteria. Based on the outputs provided, let??s evaluate these criteria:
? Version Compatibility:
? Platform Type and Configuration:
? Global Settings:
Based on the above analysis, all devices (FortiAnalyzer1, FortiAnalyzer2, and FortiAnalyzer3) meet the requirements to be part of a FortiAnalyzer Fabric.
References: FortiAnalyzer 7.4.1 documentation outlines that devices within a FortiAnalyzer
Fabric should be on the same or compatible firmware versions and hardware platforms, and they must be configured for integration. Given that all devices match the version, platform, and mode criteria, they can all be part of the FortiAnalyzer Fabric.

NEW QUESTION 30
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.

Answer: B

NEW QUESTION 35
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 39
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:
FortiAnalyzer manages and stores various types of logs, including local logs, across different ADOMs (Administrative Domains). Each type of log serves specific purposes, with some logs being ADOM-specific and others providing system-wide information.
? Option A - Local Logs Not Supported in FortiView:
? Option B - Playbook Logs for All ADOMs in the Root ADOM:
? Option C - Event Logs vs. Application Logs:
? Option D - Event Logs Only in Root ADOM:
Conclusion:
? Correct Answer: B. You can view playbook logs for all ADOMs in the root ADOM and C. Event logs show system-wide information, whereas application logs are ADOM specific.
? These answers correctly describe the characteristics and visibility of local logs within FortiAnalyzer.
References:
? FortiAnalyzer 7.4.1 documentation on log types, ADOM configuration, and FortiView functionality.

NEW QUESTION 41
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

Answer: BC

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:
? Option C - Send SMS Notification:
? Option A - Send Alert through Fabric Connectors:
? Option D - Send Alert through FortiSIEM MEA:
Conclusion:
? Correct Answer: B. Send SNMP trap and C. Send SMS notification
? These options represent valid notification methods for FortiAnalyzer??s event handler configuration.
References:
? FortiAnalyzer 7.4.1 documentation on event handler configuration and available notification methods.

NEW QUESTION 46
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

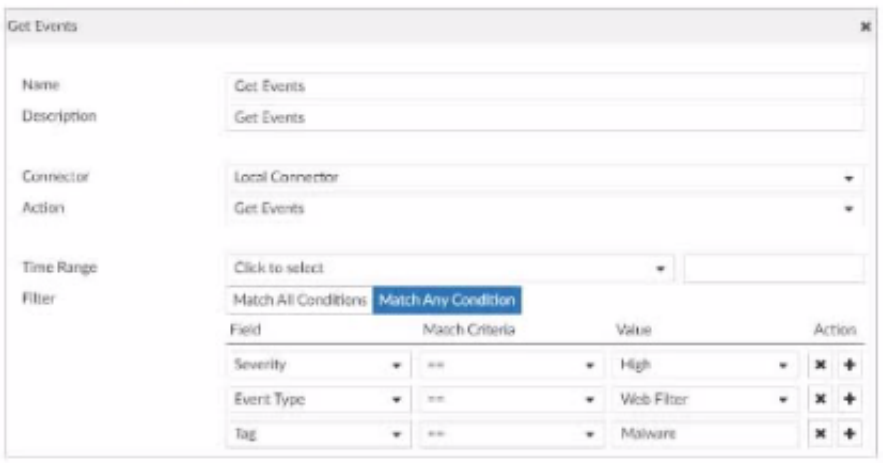
NEW QUESTION 47
What are two effects of enabling auto-cache in a FortiAnalyzer report? (Choose two.)

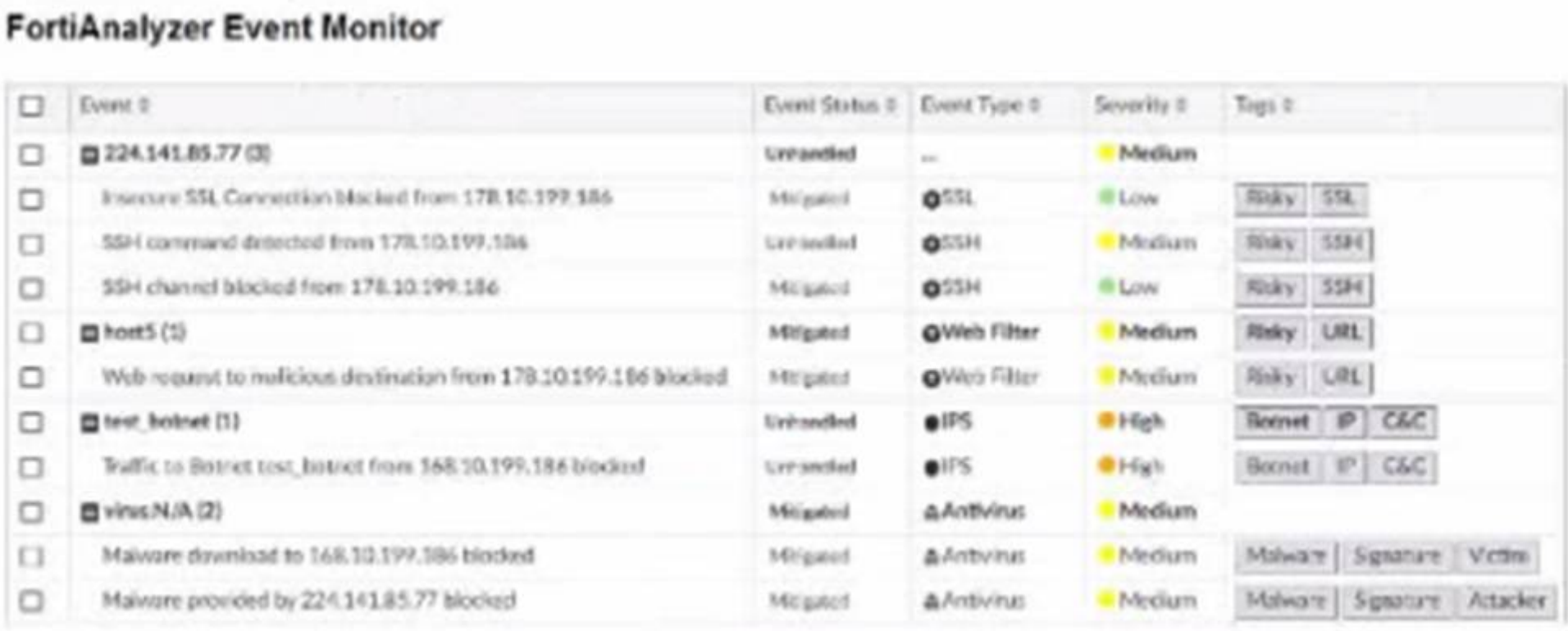
A. The generation time for reports is decreased.
B. When new logs are received, the hard-cache data is updated automatically.
C. FortiAnalyzer local cache is used to store generated reports.
D. The size of newly generated reports is optimized to conserve disk space.

Answer: AC

Explanation:
Enabling auto-cache in FortiAnalyzer reports is designed to improve the efficiency and speed of report generation by leveraging cached data. Let??s analyze each option to determine which effects are correct.
? Option A - The Generation Time for Reports is Decreased:
? Option B - Hard-Cache Data is Automatically Updated When New Logs are Received:
? Option C - FortiAnalyzer Local Cache is Used to Store Generated Reports:
? Option D - The Size of Newly Generated Reports is Optimized to Conserve Disk Space:
Conclusion:
? Correct Answer: A. The generation time for reports is decreased and C. FortiAnalyzer local cache is used to store generated reports.
? Enabling auto-cache helps reduce report generation time by using locally cached data and optimizes report processing, though it does not impact report size or continuously update with each new log.
References:
? FortiAnalyzer 7.4.1 documentation on report caching, auto-cache functionality, and report generation optimizations.

NEW QUESTION 49
Exhibit.





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.

Answer: D

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:
? Event Type = Web Filter:
? Tag = Malware:
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 Answer: 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.
References:
? FortiAnalyzer 7.4.1 documentation on event filtering, playbook configuration, and incident management criteria.

NEW QUESTION 52

.....

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