Fortinet

Exam Questions FCP_FAZ_AN-7.6

Fortinet NSE 5 - FortiAnalyzer 7.6 Analyst

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1
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.

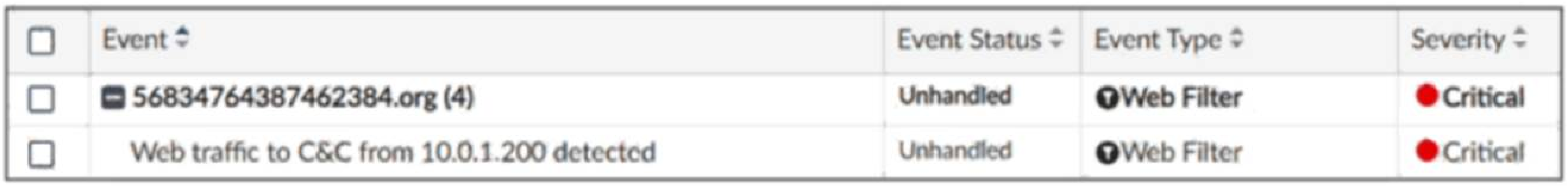
Answer: A

NEW QUESTION 2
You mustfind 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 3
Refer to the exhibit.



☐	Event	Event Status	Event Type	Severity
☐	⊟ 56834764387462384.org (4)	Unhandled	Web Filter	● Critical
☐	Web traffic to C&C from 10.0.1.200 detected	Unhandled	Web Filter	● Critical

Which statement about the displayed event is correct? (Choose one answer))

A. An incident was created from this event.
B. The risk source is isolated.
C. The security risk was escalated.
D. The security event risk is considered open.

Answer: D

Explanation:
Comprehensive and Detailed Explanation: From Exact Extract of knowledge of FortiAnalyzer 7.6 Study guide documents:
In the exhibit, theEvent Statusshown isUnhandled(Event Type: Web Filter; Severity: Critical). The FortiAnalyzer study guide definesUnhandledevents as events whose security risk has not been addressed and is therefore still active/open. Specifically, it states:??Unhandled: The security risk is considered open.??
This directly matches optionD.
The other options correspond to different statuses or actions:
* Isolated/Containedapplies when the risk source is isolated (statusContained), notUnhandled.
* Escalatedrefers to events moved/raised for further action (statusEscalated), notUnhandled.
* Whether an incident was created cannot be concluded solely from the status ??Unhandled?? in the exhibit; the study guide ties incident creation to incident management workflows rather than equating ??Unhandled?? with an incident being created.

NEW QUESTION 4
What are the two methods you can use to send notifications when an event is generated by an event handler? (Choose two answers)

A. Send SNMP trap.
B. Send an alert through the FortiGuard server.
C. Send an alert through Fabric connectors.
D. Send SMS notification

Answer: AC

Explanation:
From Exact Extract of knowledge of FortiAnalyzer 7.6 Study guide documents:
FortiAnalyzer event handlers support alerting when a rule match generates an event. The study guide states that, for an event handler,??You can select a notification profile to send alerts whenever an event is generated by the handler.??In FortiAnalyzer, notification profiles are the mechanism used to deliver alerts outward (for example, via an SNMP trap), which directly aligns with optionA.
In addition, FortiAnalyzer supports sending notifications to external platforms through integrations:??You can configure FortiAnalyzer to send a notification to external platforms using preconfigured Fabric connectors.??This validates the use ofFabric connectorsas a notification delivery method, aligning with optionC.
OptionBis not a notification delivery method for event-handler-generated alerts in the workflow described (FortiGuard is used for threat intelligence/enrichment rather than relaying alerts). OptionDis not presented in the study guide??s described notification mechanisms for event-handler alerting in the referenced sections.

NEW QUESTION 5
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:
Enablingauto-cachein 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:
* When auto-cache is enabled, FortiAnalyzer can use previously cached data instead of reprocessing all log datafrom scratch each time a report is generated. This results in faster report generation times, especially for recurring reports that use similar datasets.
* Conclusion:Correct.
* Option B - Hard-Cache Data is Automatically Updated When New Logs are Received:
* Enabling auto-cache does not immediately update the cache with every new log received. Instead, the cache is updated when reports are generated, based on the existing logs up to that point. Therefore, auto-cache does not constantly refresh with each incoming log, which would be inefficient.
* Conclusion:Incorrect.
* Option C - FortiAnalyzer Local Cache is Used to Store Generated Reports:
* Auto-cache utilizes FortiAnalyzer??s local cache to store data used in reports, reducing the need to retrieve and process logs repeatedly. This cached data can be reused for subsequent report generation, enhancing performance.
* Conclusion:Correct.
* Option D - The Size of Newly Generated Reports is Optimized to Conserve Disk Space:
* Auto-cache does not directly impact the size ofthe report files themselves. It focuses on performance optimization through cached data for faster access, but it does not compress or optimize the storage size of the generated report.
* Conclusion:Incorrect.Conclusion:
* Correct Answer A. The generation time for reports is decreasedandC. 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 6
(An analyst is using FortiAI on FortiAnalyzer to simplify certain tasks but is worried about exceeding the monthly token limit. Which query will take the fewest FortiAI tokens? (Choose one answer))

A. Show logs for 192.168.1.10 (past week)
B. Show all logs from the past week
C. Can you show me all the log entries for the endpoint 192.168.1.10?
D. Show logs for 192.168.1.10

Answer: A

Explanation:
From Exact Extract of knowledge of FortiAnalyzer 7.6 Study guide documents:
The study guide explains that FortiAI token usage includesboth the prompt (input) and the response (output), and that ??generally, more text in the query and response results in using more tokens.?? It provides two comparison examples and concludes that the more verbose request for ??all the log entries?? consumes more tokens because it hasmore textand also triggers alarger response; whereas limiting the query to a time range (for example, ??(past week)??) reduces output volume and therefore token usage.
Applying that guidance to the options:
* Cis the most verbose and explicitly requests ??all the log entries,?? which drives higher input and output token usage.
* Brequests ??all logs?? for the week (broad scope), which typically increases output tokens.
* Dis short, but it doesnotconstrain the time range, which can increase the response size (output tokens).
* Ais concise and includes a time constraint ??(past week),?? matching the study guide??s example of a lower-token query pattern.

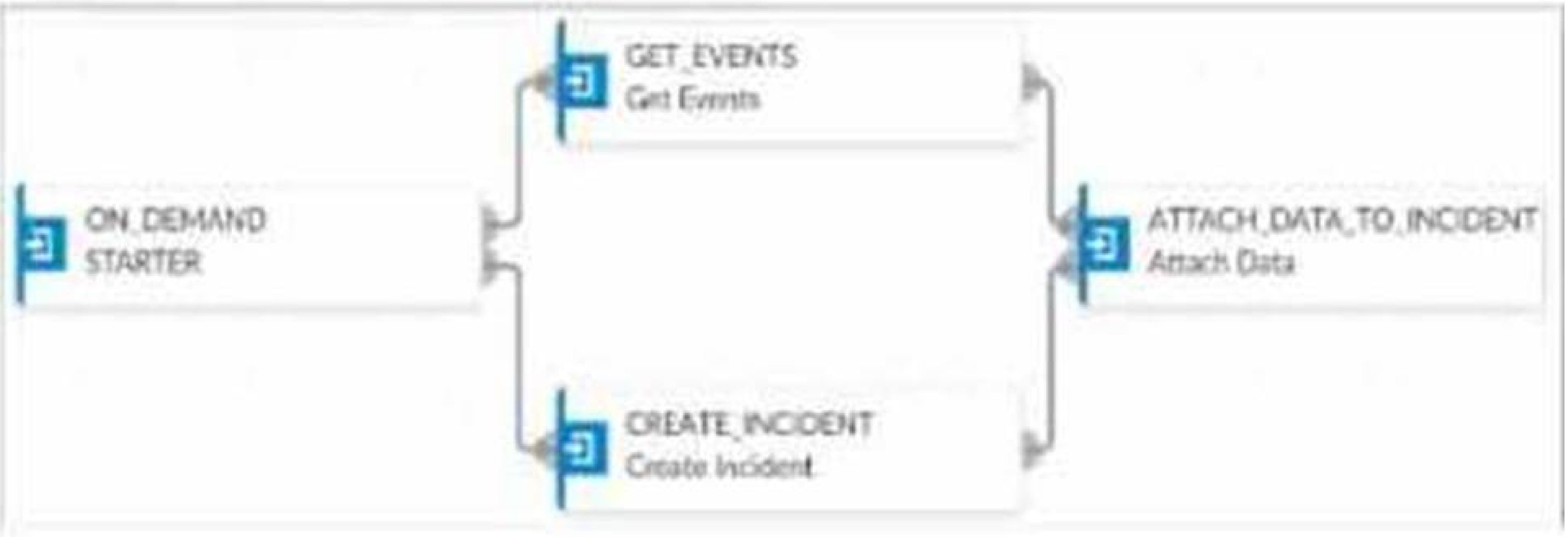
NEW QUESTION 7
Whathappens when the indicator of compromise (IOC) engine on FortiAnalyzer finds web logs that match blacklisted IP addresses?

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.

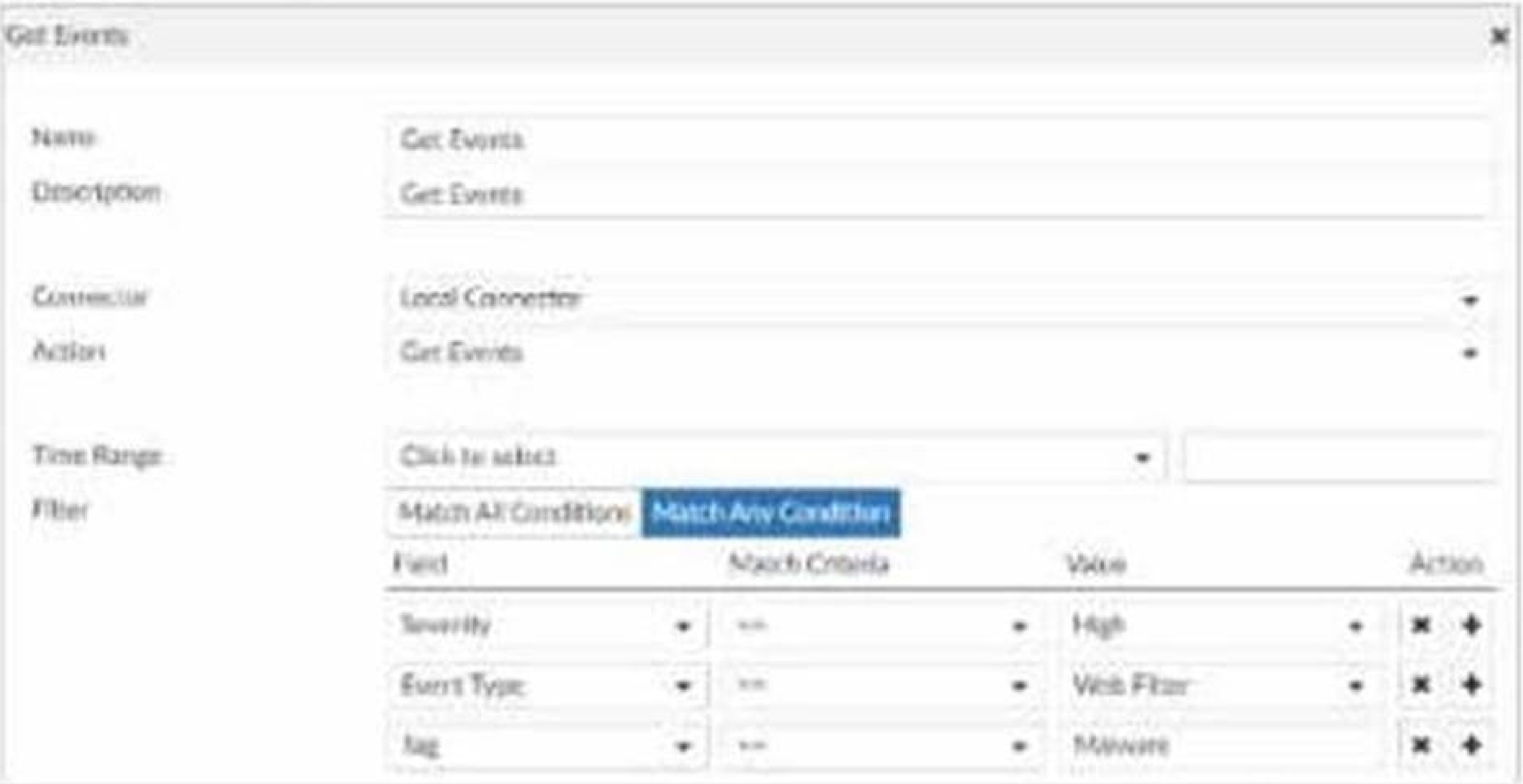
Answer: B

NEW QUESTION 8
Exhibit.

Playbook Editor



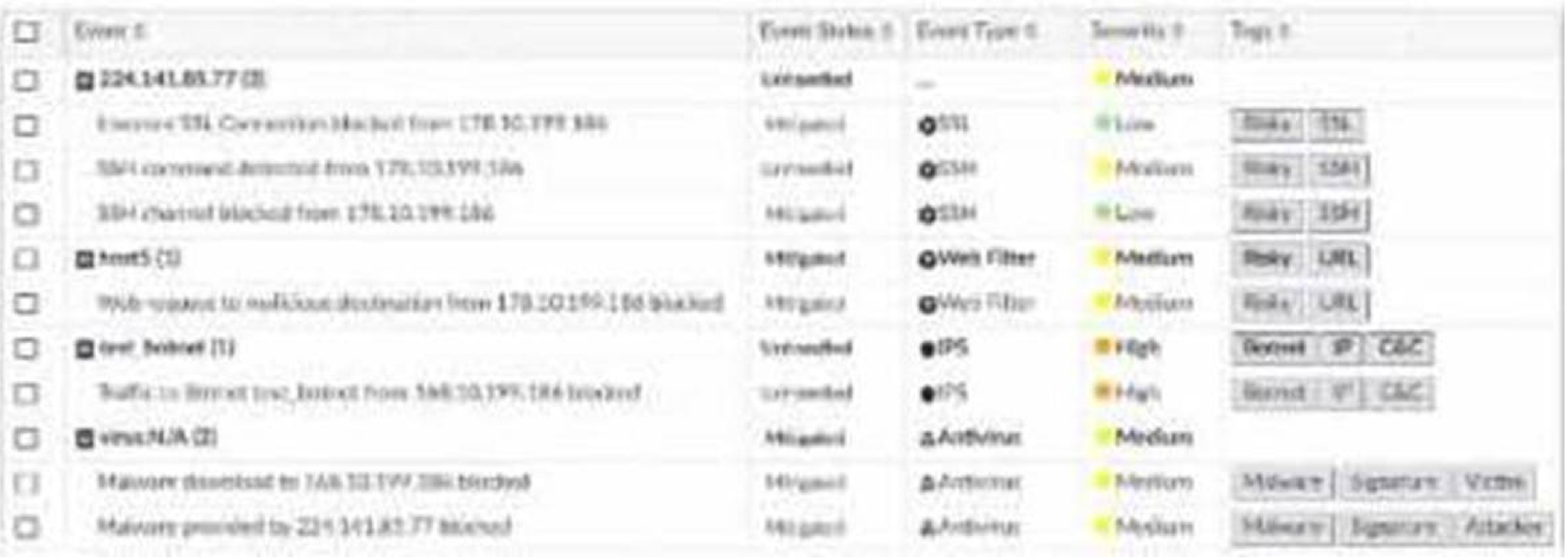
Get Event task configuration



Name	Get Events
Description	Get Events
Connector	Local Connector
Action	Get Events
Time Range	Click to select
Filter	Match All Conditions / **Match Any Condition**

Field	Match Criteria	Value	Action
Severity	==	High	✖ ✚
Event Type	==	Web Filter	✖ ✚
Tag	==	Malware	✖ ✚

FortiAnalyzer Event Monitor



☐	Event	Event Status	Event Type	Severity	Tags
☐	⊟ 224.141.85.77 (3)	Unhandled	—	Medium	
☐	Insecure SSL Connection blocked from 178.10.199.186	Mitigated	SSL	Low	Risky SSL
☐	SSH command detected from 178.10.199.186	Unhandled	SSH	Medium	Risky SSH
☐	SSH channel blocked from 178.10.199.186	Mitigated	SSH	Low	Risky SSH
☐	⊟ host5 (1)	Mitigated	Web Filter	Medium	Risky URL
☐	Web request to malicious destination from 178.10.199.186 blocked	Mitigated	Web Filter	Medium	Risky URL
☐	⊟ test_botnet (1)	Unhandled	IPS	High	Botnet IP C&C
☐	Traffic to Botnet test_botnet from 168.10.199.186 blocked	Unhandled	IPS	High	Botnet IP C&C
☐	⊟ virus:N/A (2)	Mitigated	Antivirus	Medium	
☐	Malware download to 168.10.199.186 blocked	Mitigated	Antivirus	Medium	Malware Signature Victim
☐	Malware provided by 224.141.85.77 blocked	Mitigated	Antivirus	Medium	Malware Signature Attacker

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.

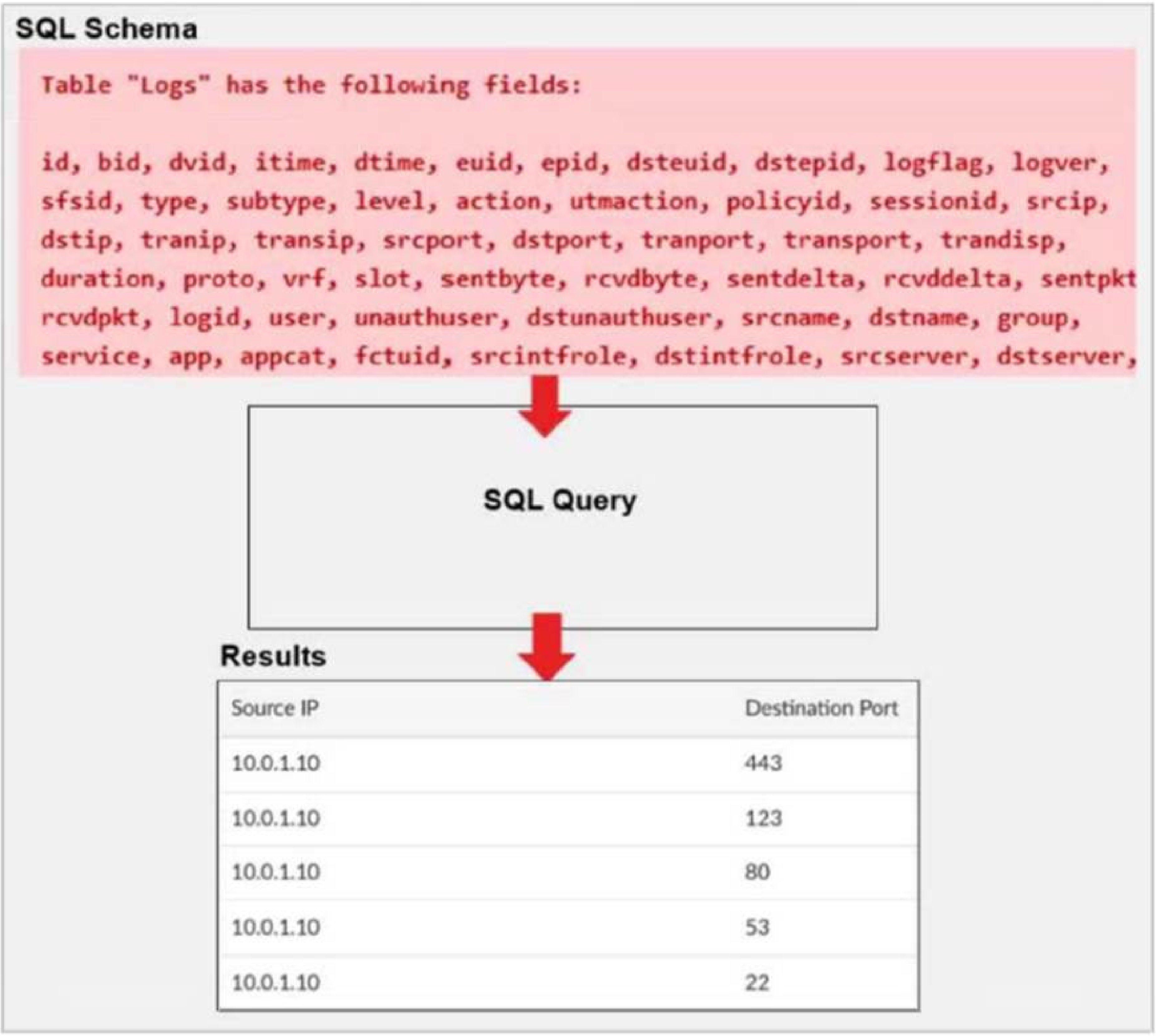
B. Seven events will beadded
C. No events will be added.
D. Four events will be added.

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:
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 arefour 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 9
Exhibit.

SQL query



SQL Schema

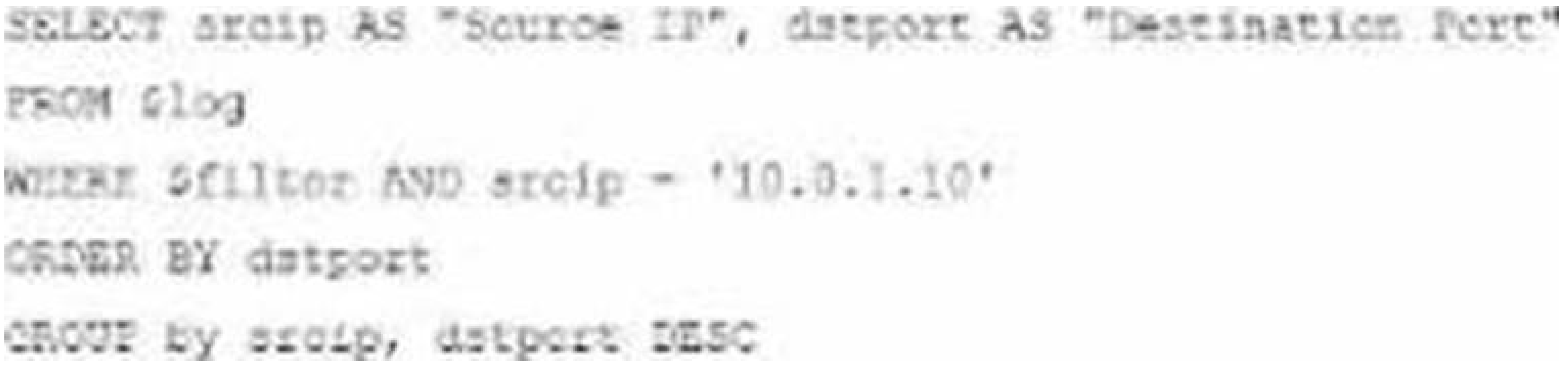
```
Table "Logs" has the following fields:

id, bid, dvid, itime, dtime, euid, epid, dsteuid, dstepid, logflag, logver,
sfsid, type, subtype, level, action, utmaction, policyid, sessionid, srcip,
dstip, tranip, transip, srcport, dstport, tranport, transport, trandisp,
duration, proto, vrf, slot, sentbyte, rcvdbyte, sentdelta, rcvddelta, sentpkt
rcvdpkt, logid, user, unauthuser, dstunauthuser, srcname, dstname, group,
service, app, appcat, fctuid, srcintfrole, dstintfrole, srcserver, dstserver,
```

SQL Query

Results

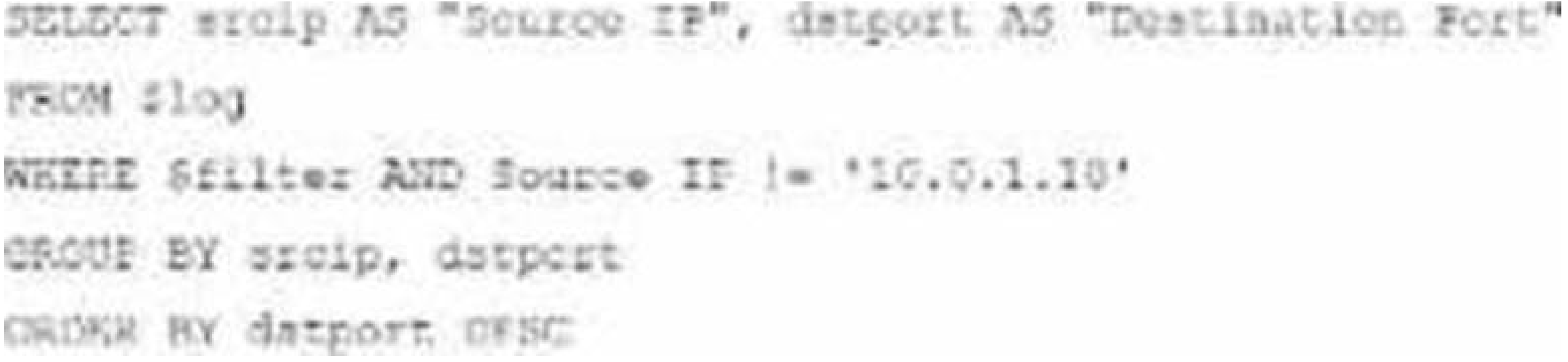
Source IP	Destination Port
10.0.1.10	443
10.0.1.10	123
10.0.1.10	80
10.0.1.10	53
10.0.1.10	22

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' GROUP BY srcip, dstport - ORDER BY dstport DESC



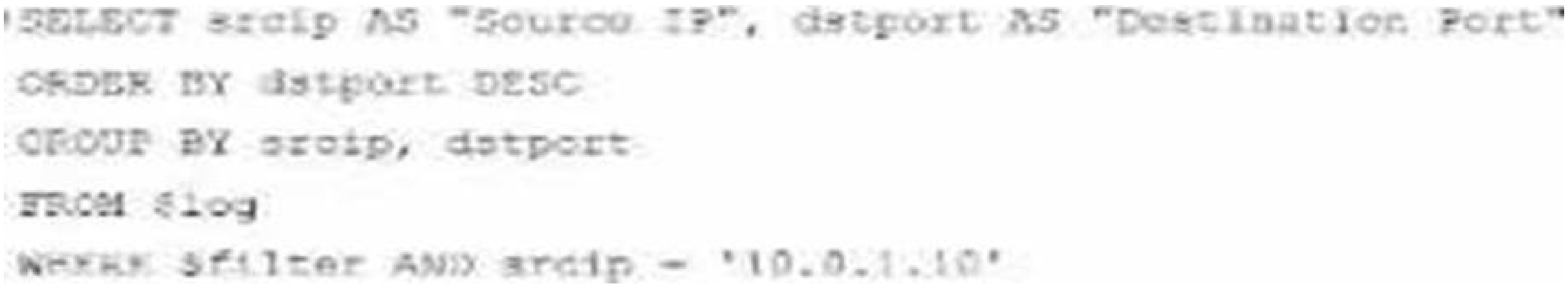
```
SELECT srcip AS "Source IP", dstport AS "Destination Port"
FROM $log
WHERE $filter AND srcip = '10.0.1.10'
ORDER BY dstport
GROUP BY srcip, dstport DESC
```

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



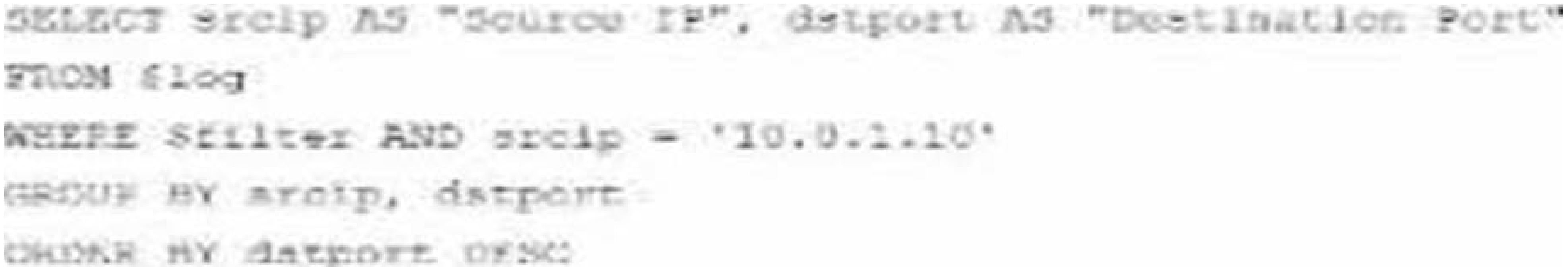
```
SELECT srcip AS "Source IP", dstport AS "Destination Port"
FROM $log
WHERE $filter AND Source IP != '10.0.1.10'
GROUP BY srcip, dstport
ORDER BY dstport DESC
```

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'



```
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' ORDER BY dstport - GROUP by srcip, dstport DESC



```
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

Answer: A

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 forselecting, 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 dstportDESC: 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 Answer 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.
[References:, FortiAnalyzer 7.4.1 SQL query capabilities and syntax for report customization.,]

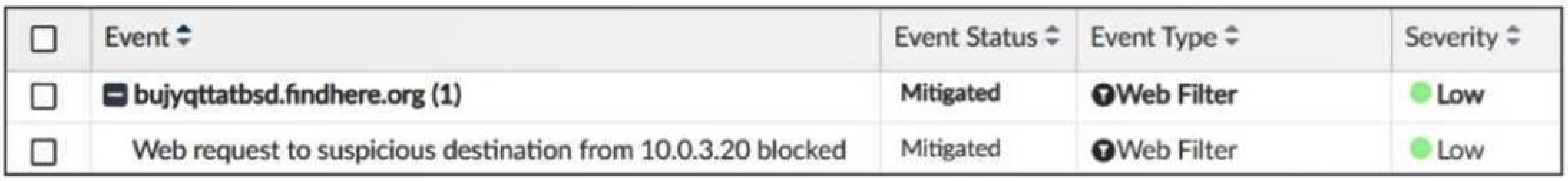
NEW QUESTION 10
How does FortiAnalyzer block indicators? (Choose one answer))

A. It uses an automation script to update FortiGate with the block list.
B. It uses a FortiManager connector to send the block list.
C. It uses a FortiClient EMS connector to send the block list.
D. It uses a webhook to allow FortiGate to send the block list.

Answer: B

Explanation:
Comprehensive and Detailed Explanation From Exact Extract of knowledge of FortiAnalyzer 7.6 Study guide documents:
The FortiAnalyzer study guide states that blocking suspicious indicators is performed by integrating FortiAnalyzer withFortiManager(not by directly pushing a block list to FortiGate). Specifically:"To use this feature, you must set up an authorized FortiManager connector for the FortiAnalyzer on the Fabric Connector page of FortiAnalyzer."
It then explains the backend mechanism:"In the back end, a playbook called Block_indicator runs every 5 minutes to send the information to FortiManager."After a successful run,"the blocked indicator is pushed to the FortiManager External Resource list."From there, FortiManager can create threat feeds/security profiles/policy blocks and push policies to FortiGate as needed—however, the study guide clarifies:??The Blocked status on FortiAnalyzer confirms that the list is updated on FortiManager, but it is not synced to FortiGate.??
Therefore, FortiAnalyzer blocks indicators by using aFortiManager connectorand sending the block information to FortiManager (Option B).

NEW QUESTION 10
Refer to the exhibit.



□	Event	Event Status	Event Type	Severity
□	⊟ bujyqttatbsd.findhere.org (1)	Mitigated	Web Filter	● Low
□	Web request to suspicious destination from 10.0.3.20 blocked	Mitigated	Web Filter	● Low

Which statement about the displayed event is correct? (Choose one answer))

A. The security risk was dropped.B.The risk source is isolated.
B. The security risk was blocked.
C. The security event risk is from an application control log.

Answer: C

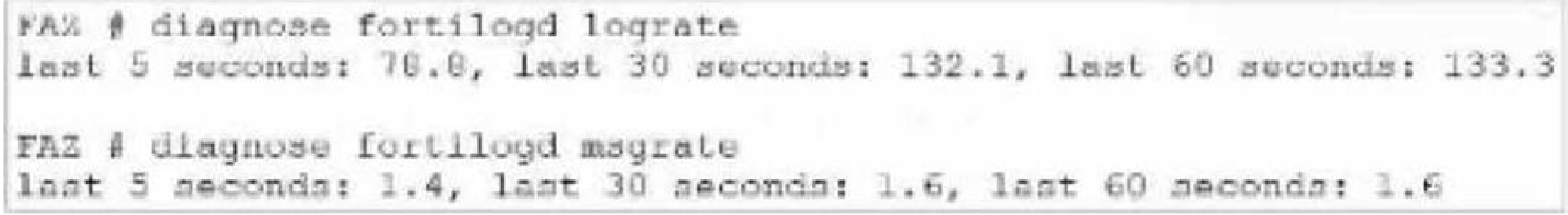
Explanation:
Comprehensive and Detailed Explanation From Exact Extract of knowledge of FortiAnalyzer 7.6 Study guide documents:
The exhibit shows the eventEvent Status = MitigatedandEvent Type = Web Filter, with the event message indicating the web request wasblocked.
The study guide definesMitigatedevents as follows:"Mitigated: The security risk is mitigated by being blocked or dropped."This means a mitigated status corresponds to enforcement that prevented the risk (block/drop), not a condition where the source is isolated.
It also distinguishesContainedevents from mitigated ones:"Contained: The risk source is isolated."Since the exhibit clearly showsMitigated(not Contained), optionBis incorrect.
Additionally, the study guide notes:??Generally, you can acknowledge mitigated events because the related traffic was blocked by the firewall."This aligns directly with the exhibit's "blocked" wording and supports that the correct interpretation is that the security risk was blocked.
Finally, the event type displayed isWeb Filter, not application control, so optionDis incorrect.
Therefore, the correct statement isC. The security risk was blocked.

NEW QUESTION 13
You discover that a few reports are taking a long tine lo generate. Which two steps can you Like 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: AB

NEW QUESTION 17
Exhibit.



```
FAZ # diagnose fortilogd lograte
last 5 seconds: 70.0, 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 thenormal 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.,]

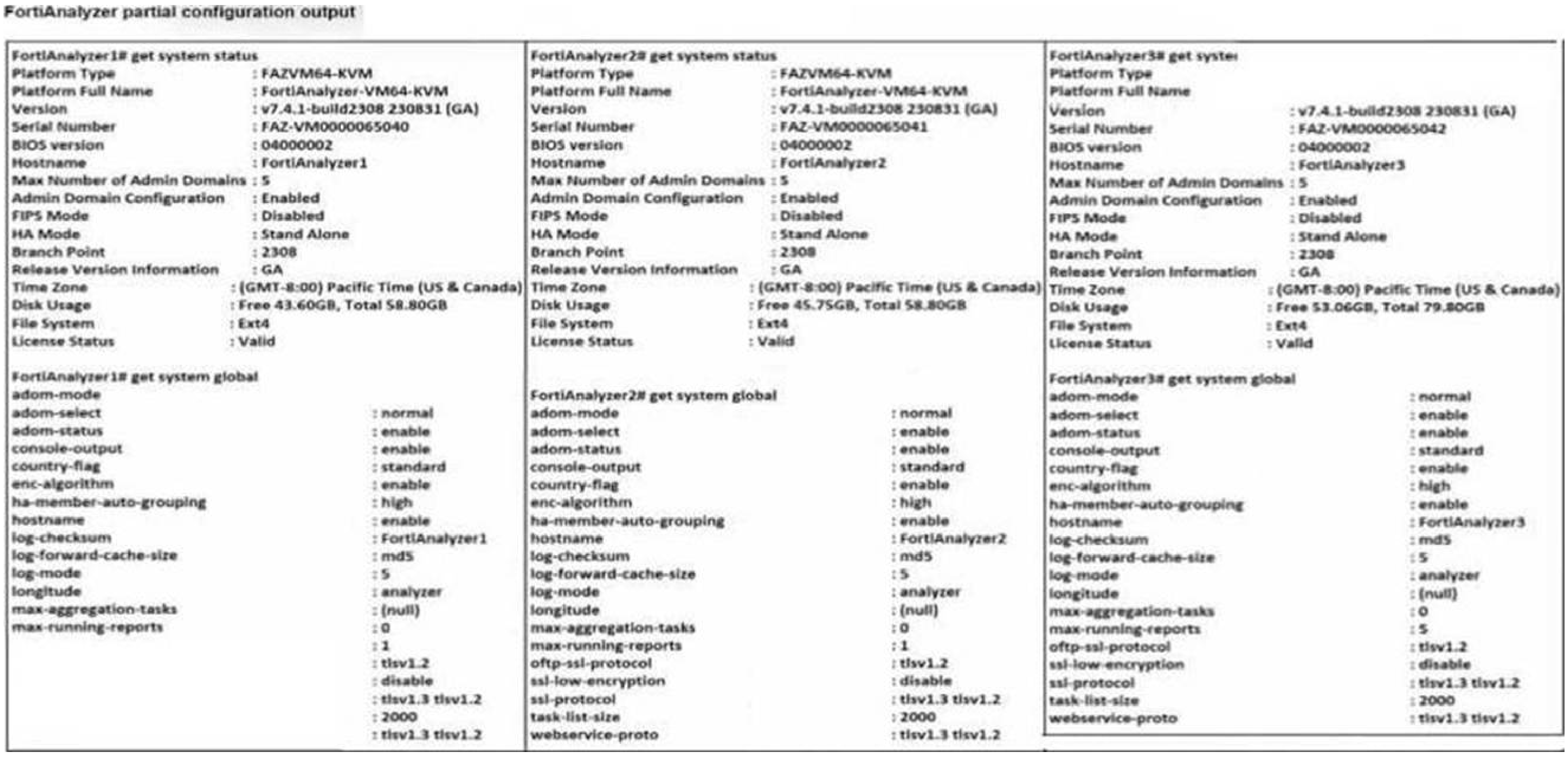
NEW QUESTION 18
Which SQL query is in the correct order to query to database in the FortiAnalyzer?

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:
SELECT devid FROM $log: This specifies that the query is selecting the devid column from the $log table.
WHERE 'user' = ': This part of the query is intended to filter results based on a condition involving the user column. Although there appears to be a minor typographical issue (possibly missing the user value after =), it structurally adheres to the correct SQL order.
GROUP BY devid: This groups the results by devid, which is correctly positioned at the end of the query.
Let's briefly examine why the other options are incorrect:
Option A: SELECT devid FROM $log GROUP BY devid WHERE 'user', 'users1'
This is incorrect because the GROUP BY clause appears before the WHERE clause, which is out of order in SQL syntax.
Option B: SELECT FROM $log WHERE devid 'user', USER1' GROUP BY devid
This is incorrect because it lacks a column in the SELECT statement and the WHERE clause syntax is malformed.
Option C: SELCT devid WHERE 'user' - 'USER1' FROM $log GROUP BY devid
This is incorrect because the SELECT keyword is misspelled as SELCT, and the WHERE condition syntax is invalid.
Reference: 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 20
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
adom-select                                 : normal
adom-status                                 : enable
console-output                              : enable
country-flag                                : standard
enc-algorithm                               : enable
ha-member-auto-grouping                     : high
hostname                                    : enable
log-checksum                                : FortiAnalyzer1
log-forward-cache-size                      : md5
log-mode                                    : 5
longitude                                   : analyzer
max-aggregation-tasks                       : (null)
max-running-reports                         : 0
                                            : 1
                                            : tlsv1.2
                                            : disable
                                            : tlsv1.3 tlsv1.2
                                            : 2000
                                            : 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:
All three devices, FortiAnalyzer1, FortiAnalyzer2, and FortiAnalyzer3, are running version v7.4.1-build0238, which is the same across the board. This version alignment is crucial because FortiAnalyzer Fabric requires that devices run compatible firmware versions for seamless communication and management.
Platform Type and Configuration:
All three devices are configured as Standalone in the HA mode, which allows them to operate independently but does not restrict their participation in a FortiAnalyzer Fabric. Each device is also on the FAZVM64-KVM platform type, ensuring hardware compatibility.
Global Settings:
Key settings such as adm-mode, adm-status, and adom-mode are consistent across all devices (adm-mode: normal, adm-status: enable, adom-mode: normal), which aligns with requirements for fabric integration and role assignment flexibility.
Each device also has the log-forward-cache-size set, which is relevant for forwarding logs within a fabric environment.
Based on the above analysis, all devices (FortiAnalyzer1, FortiAnalyzer2, and FortiAnalyzer3) meet the requirements to be part of a FortiAnalyzer Fabric.
Reference: 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 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
This is correct. FortiAnalyzer allows analysts to manually attach reports to incidents, which is beneficial for providing additional context, evidence, or analysis related to the incident. This functionality is part of the incident management process and helps streamline information for tracking and resolution.
Option B: The status of the incident is always linked to the status of the attached event
This is incorrect. The status of an incident on FortiAnalyzer is managed independently of the status of any attached events. An incident can contain multiple events, each with different statuses, but the incident itself is tracked separately.
Option C: Severity incidents rated with the level High have an initial service-level agreement (SLA) response time of 1 hour
This is incorrect. While incidents have severity levels, specific SLA response times are typically set according to the organization??s incident response policy, and FortiAnalyzer does not impose a default
SLA response time of 1 hour for high-severity incidents.
Option D: Incidents must be acknowledged before they can be analyzed
This is incorrect. Incidents on FortiAnalyzer can be analyzed even if they are not yet acknowledged. Acknowledging an incident is often part of the workflow to mark it as being actively addressed, but it is not a prerequisite for analysis.
Reference: 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
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.

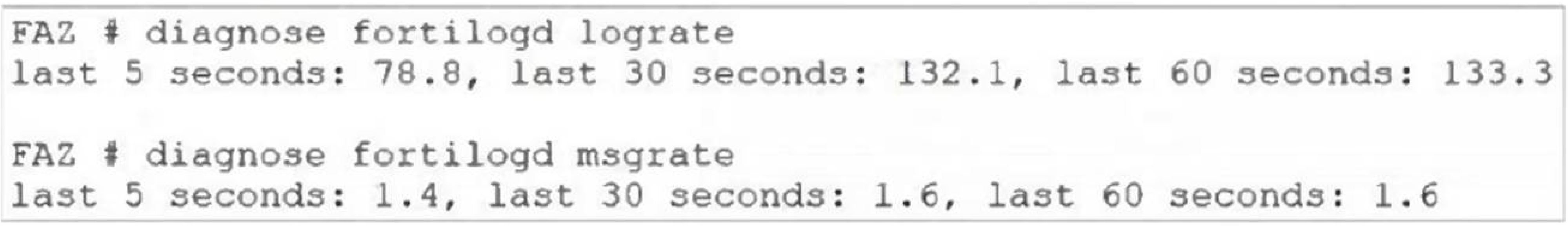
Answer: C

NEW QUESTION 29
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.

Answer: C

NEW QUESTION 31
Refer to the 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 low indexing values require investigation.
B. The output is not ADOM specific.
C. There are more event logs thantraffic logs.
D. The log rate higher than the message rate is not normal.

Answer: D

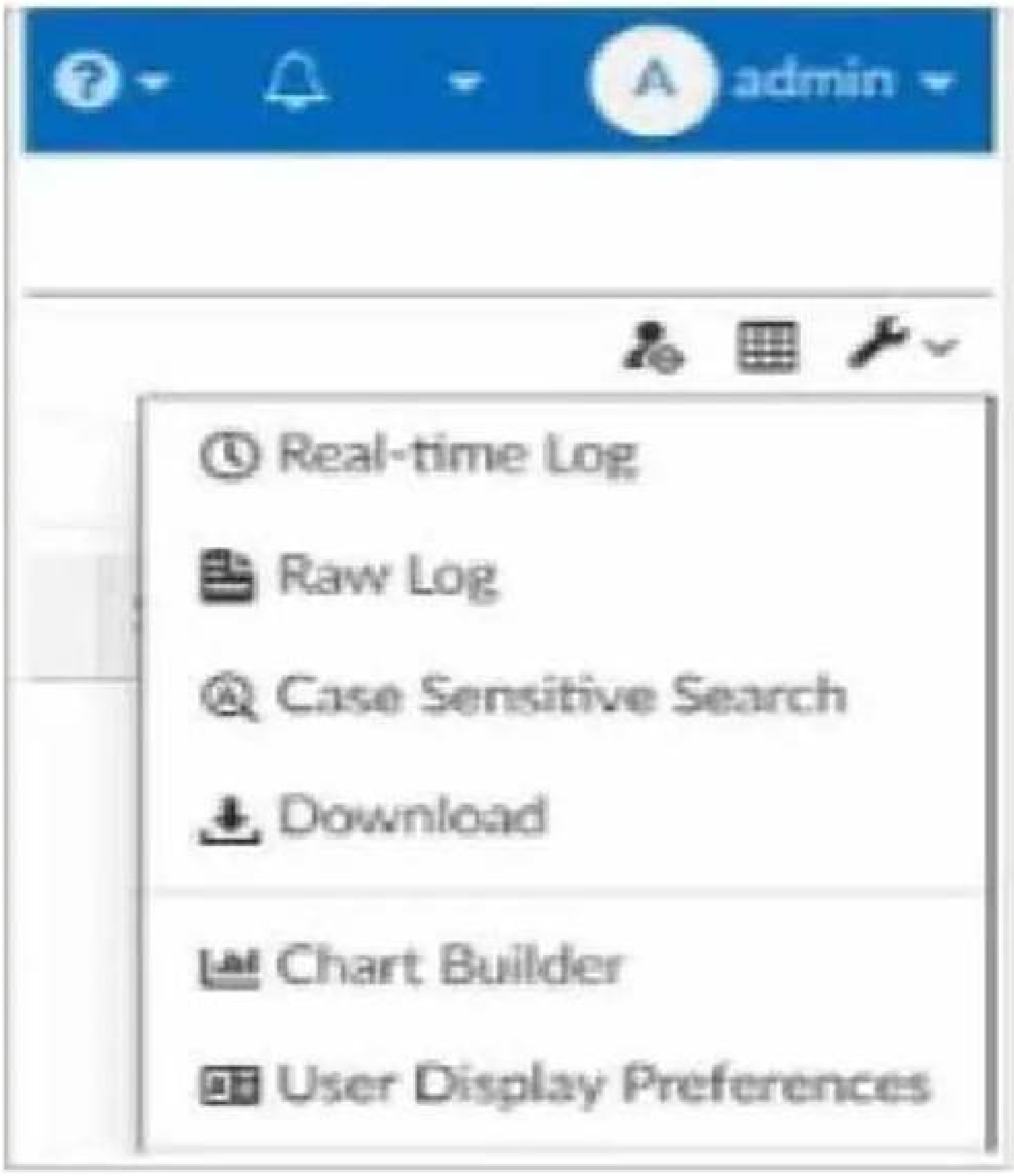
NEW QUESTION 35
Which statement about the FortiSIEM management extension is correct?

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: D

NEW QUESTION 36
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 generatereports 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

NEW QUESTION 40
What two things should an administrator do to view Compromised Hosts on FortiAnalyzer? (Choose two.)

A. Enable web filtering in firewall policies on FortiGate devices, and make sure these logs are sent to FortiAnalyzer.
B. Enable device detection on an interface on the FortiGate devices that are connected to the FortiAnalyzer.
C. Subscribe FortiAnalyzer to FortiGuard to keep its local threat database up-to-date.
D. Make sure all endpoints are reachable by FortiAnalyzer.

Answer: AC

NEW QUESTION 43
......

Relate Links

100% Pass Your FCP_FAZ_AN-7.6 Exam with Exambible Prep Materials

https://www.exambible.com/FCP_FAZ_AN-7.6-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/