Fortinet FCP_FAZ_AN-7.6 NSE 5 Practice Questions

Shared by English on 17-08-2026

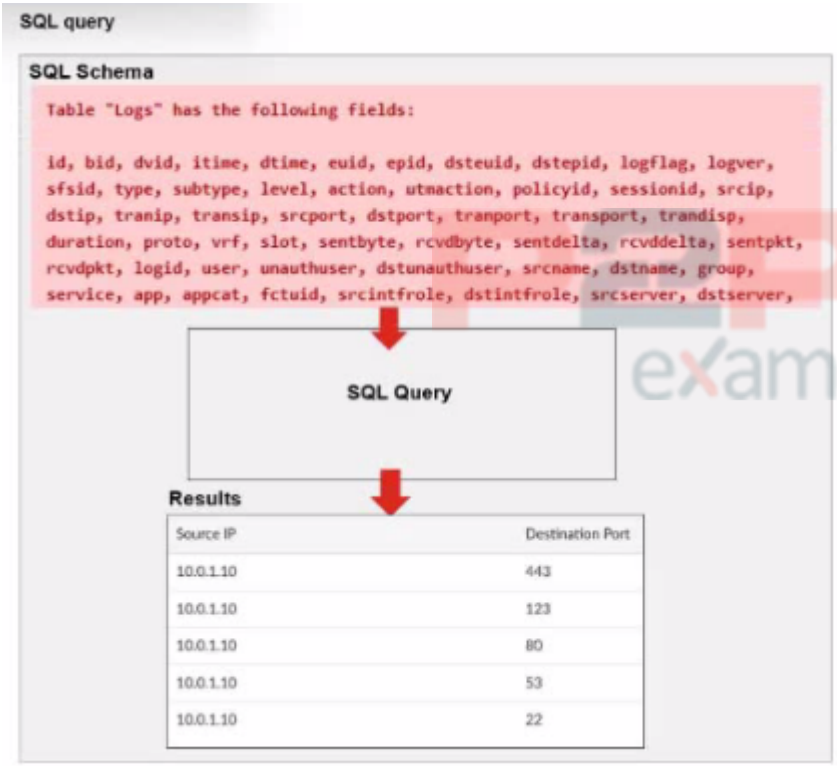
For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Exhibit.



A FortiAnalyzer analyst is customizing a SQL query to use in a report.

Which SQL query should the analyst run to get the expected results?

A)

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

B)

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

C)

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

D)

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

Options:

A- Option A
B- Option B
C- Option C
D- Option D

Answer:

A

Explanation:

Study Guide p.157-p.158: report datasets use SQL SELECT queries, and clauses must be in the correct order.

Technical Deep Dive: The correct answer is A. The valid query must select the required fields, read from $log, apply the filter for the source IP, group the selected values, and order the output as expected. Option A follows the SQL structure FortiAnalyzer expects for report datasets. The incorrect options either reverse the filter logic, place clauses in the wrong order, or use malformed aliases/conditions. In FortiAnalyzer reporting, a syntactically correct dataset is mandatory because the chart receives only the data returned by that SQL SELECT query.

Question 2

Question Type: MultipleChoice

(Which two statements about FortiAnalyzer Fabric deployments are true? (Select two answers))

Options:

A- Supervisors can be in high availability (HA) for redundancy purposes only.
B- Fabric members can operate in analyzer mode only.
C- Fabric members do not forward their logs to the supervisor.
D- Supervisors and members must be in the same time zone.

Answer:

B, C

Explanation:

Comprehensive and Detailed Explanation From Exact Extract of knowledge of FortiAnalyzer 7.6 Study guide documents:

B is true (members operate in analyzer mode, not collector mode): The study guide defines Fabric members as FortiAnalyzer devices that ''retain access to the features described in the FortiAnalyzer Administration Guide'' and that ''each member can create or raise incidents and events.'' In contrast, it states that a FortiAnalyzer operating in collector mode ''does not provide capabilities for event management or reporting,'' and also notes that ''in collector mode, the GUI doesn't include FortiView, Reports, or Incidents & Events.'' Since Fabric members must be able to generate/manage incidents and events, they must be operating with analyzer capabilities rather than collector-only functionality.

C is true (members do not forward their logs to the supervisor): The supervisor provides centralized visibility, but the study guide describes the supervisor's log access as viewing logs collected on members, not receiving/storing forwarded log files. It states: ''In the FortiAnalyzer Fabric supervisor, Log View displays logs collected on all FortiAnalyzer Fabric members,'' and clarifies ''the logs contain the same information as displayed in the host FortiAnalyzer device they were collected on.'' This indicates the logs remain on the member (host) and are made visible to the supervisor for centralized monitoring rather than being forwarded and stored on the supervisor.

For completeness, the study guide also explicitly states ''HA is not available on the supervisor'' (so A is false) and members do not need the same time zone as the supervisor (so D is false).

Question 3

Question Type: MultipleChoice

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

Options:

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

Answer:

A, C

Explanation:

Comprehensive and Detailed 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 option A.

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 of Fabric connectors as a notification delivery method, aligning with option C.

Option B is 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). Option D is not presented in the study guide's described notification mechanisms for event-handler alerting in the referenced sections.

Question 4

Question Type: MultipleChoice

(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? (Select one answer))

Options:

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:

Comprehensive and Detailed Explanation From Exact Extract of knowledge of FortiAnalyzer 7.6 Study guide documents:

The study guide explains that FortiAI token usage includes both 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 has more text and also triggers a larger 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:

C is the most verbose and explicitly requests ''all the log entries,'' which drives higher input and output token usage.

B requests ''all logs'' for the week (broad scope), which typically increases output tokens.

D is short, but it does not constrain the time range, which can increase the response size (output tokens).

A is concise and includes a time constraint ''(past week),'' matching the study guide's example of a lower-token query pattern.

Question 5

Question Type: MultipleChoice

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

Options:

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.

Question 6

Question Type: MultipleChoice

After generating a report, you notice the information you where expecting to see is not included in it. However, you confirm that the logs are there.

Options:

A- Check the time frame covered by the report.
B- Disable auto-cache.
C- Increase the report utilization quota.
D- Test the dataset

Answer:

A, D

Explanation:

When a generated report does not contain the expected information even though the logs are confirmed to be present, it typically indicates an issue with the report's configuration. There are a few common reasons this might happen:

Option A - Check the Time Frame Covered by the Report:

Reports are generated based on a specific time frame. If the report's time frame does not cover the period when the relevant logs were collected, those logs won't appear in the report output. Verifying and adjusting the time frame is essential to ensure the report includes all relevant data.

Conclusion: Correct.

Option B - Disable Auto-Cache:

Auto-cache is designed to improve report generation speed by using cached data. Disabling auto-cache would typically only be relevant if the report is pulling outdated data from cache, but it doesn't directly affect whether specific logs are included in a report.

Conclusion: Incorrect.

Option C - Increase the Report Utilization Quota:

The report utilization quota is related to the resource limits for generating reports. It does not directly influence whether certain data appears in a report. Increasing this quota would help only if there are resource issues preventing the report from completing, not if specific logs are missing from the report.

Conclusion: Incorrect.

Option D - Test the Dataset:

Datasets determine which logs and data fields are pulled into the report. If a dataset is

configured incorrectly or does not include the required log fields, it could lead to missing information. Testing the dataset allows you to verify that it's correctly configured and pulling the expected data.

Conclusion: Correct.

Conclusion:

Correct Answe r: A. Check the time frame covered by the report and D. Test the dataset.

These steps directly address the issues that could lead to missing information in a report when logs are available but not displayed.

FortiAnalyzer 7.4.1 documentation on report generation settings, time frames, and dataset configuration for accurate report results.

Question 7

Question Type: MultipleChoice

Which two statements about playbook execution are true? (Choose two)

Options:

A- FortiAnalyzer will not commit changes made by a Failed playbook
B- The Playbook Monitor provides troubleshooting logs
C- You can run the default debugging playbook to investigate playbook errors.
D- Even I the playbook status is Failed, individual tasks may have succeeded.

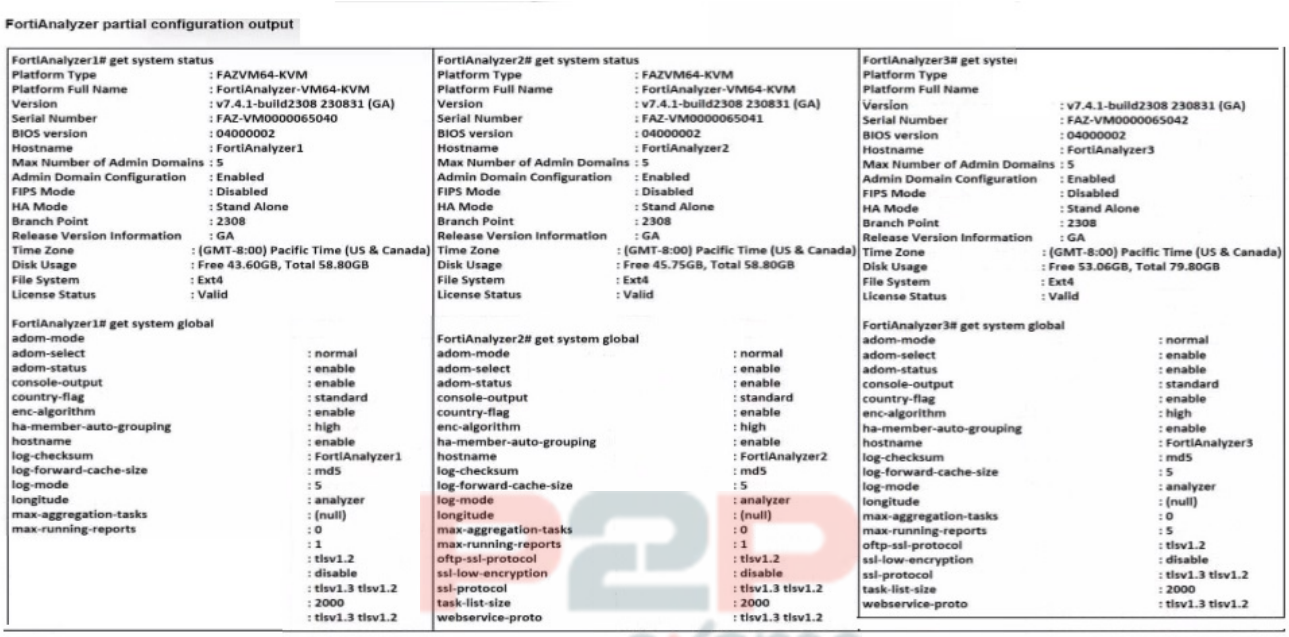
Answer:

A, B

Question 8

Question Type: MultipleChoice

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?

Options:

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:

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.

Question 9

Question Type: MultipleChoice

You discover that a few reports are taking a long tine lo generate. Which two steps can you Like to troubleshoot? (Select two.)

Options:

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:

A, B