

DUMPS ARENA

Fortinet NSE 5 FortiAnalyzer 7.6 Analyst

Fortinet FCP FAZ AN-7.6

Version Demo

Total Demo Questions: 8

Total Premium Questions: 89

Buy Premium PDF

<https://dumpsarena.co>

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1 - (SIMULATION)

SIMULATION

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 flog
WHERE sfilter 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 flog
WHERE sfilter 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 flog
WHERE sfilter 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
```

ANSWER: Check the explanation for the answer

Explanation:

Correct answer: D

The analyst should run the query shown in option 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
```

This query matches the expected report output because it:

Selects the source IP and destination port fields: `srcip` and `dstport`.

Uses the correct FortiAnalyzer report log table variable: `$log`.

Applies the required report filter with `$filter`.

Filters only traffic where `srcip = '10.0.1.10'`.

Groups the results by both selected fields using `GROUP BY srcip, dstport`.

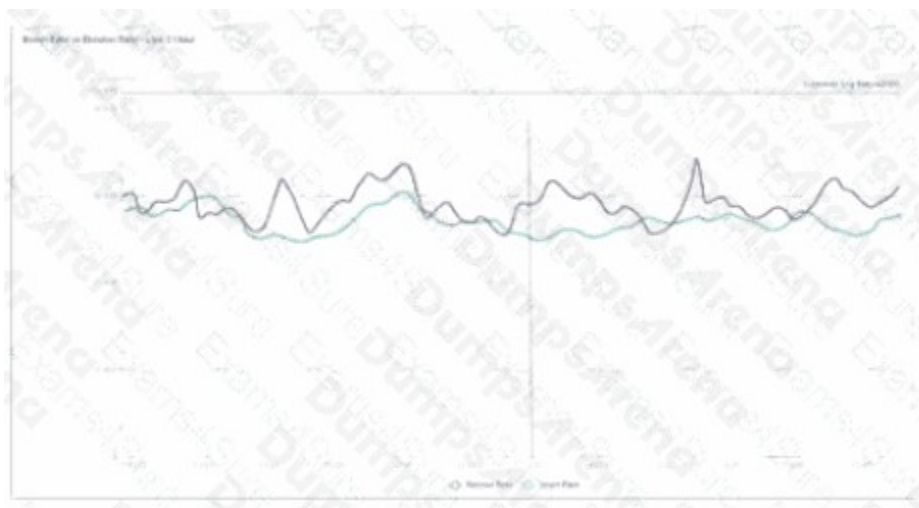
Sorts the destination ports in descending order using `ORDER BY dstport DESC`, which produces the displayed order such as 443, 123, 80, 53, and 22.

The other options are incorrect because they either use the wrong filter condition, reference an alias incorrectly, or place SQL clauses in the wrong order.

QUESTION NO: 2 - (SIMULATION)

SIMULATION

Exhibit.



What does the data point at 12:20 indicate?

ANSWER: Check the explanation for the answer

Explanation:

The data point at **12:20** indicates that the **current/observed rate was higher than the learned or baseline rate** at that time.

In the exhibit, the darker line represents the actual observed value, while the green line represents the learned baseline/expected value. At 12:20, the actual value is above the learned baseline, meaning there was an increase in activity compared with what FortiAnalyzer expected for that time period.

QUESTION NO: 3

Refer to the exhibit with partial output:

```
{
  "checksum": {
    "hash": "c7e559a2e328cab00b72aacbccccc1ca",
    "method": "MD5"
  },
  "data":
  "H4sIAAAAAAAAAA72BbW/bC4KAv9+vEiZ/sAyQgd78Rma/uHBaRm1
  ZM1S5qbFJf78hpbEpmpLI7uIhkYVtzQyHM8Ph60kPo7eN/f0qTb/
  EIy9nRRElj/1Dj+jPxX7L40tD7+7Wm1+/n970H3rko7duiyhNSrm
  CTMzWRfn15eUFvhd+/pWb/kPRqeScCVcqQdqmV4hCsT14EbCnNAY
  nunbvrevi5VKTNxhYEZZ8mCkcTPxN6fcbVhiX31hS5OL3w37e3e2
  .
```

Your colleague exported a playbook and has sent it to you for review. You open the file in a text editor and observe the output as shown in the exhibit.

Which statement about the export is true?

- A. The export data type is zipped.
The export data type is zipped.
This answer is consistent with the typical use of base64 encoding for compressed (zipped) data exports in FortiAnalyzer.
Reference:
FortiAnalyzer 7.4.1 documentation on exporting playbooks and data compression methods.
- 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:

The export data type is zipped is correct. When a FortiAnalyzer playbook is exported, the exported file can appear in a text editor as a structured object containing metadata such as a checksum and a large encoded data payload. That payload is not meant to be manually interpreted as plain playbook logic; it represents the packaged export contents, commonly compressed and encoded so that the playbook definition and related export data can be transferred safely and later re-imported with integrity validation. The checksum shown in the exhibit supports this interpretation because it is used to validate that the packaged data has not been altered or corrupted during transfer. In FortiAnalyzer administration workflows, playbooks are managed as portable objects that can be exported and imported between systems, and the exported representation may therefore look like encoded compressed data rather than readable JSON rules or task steps. This behavior is consistent with Fortinet's documented playbook management and FortiAnalyzer administrative export/import model. For related product documentation, see the [FortiAnalyzer 7.6 documentation](#) and the [FortiAnalyzer 7.6 Administration Guide](#).

QUESTION NO: 4

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: A B

Explanation:

Enabling auto-cache in a FortiAnalyzer report improves report performance by allowing FortiAnalyzer to use hard-cache, or hcache, data for report datasets instead of recalculating the same SQL results from the raw log database every time the report runs. This is why “The generation time for reports is decreased” is correct: cached dataset results can be reused during report generation, which is especially useful for scheduled or recurring reports that query large volumes of logs. “When new logs are received, the hard-cache data is updated automatically” is also correct because auto-cache maintains the hcache data as new relevant log entries are inserted, keeping the cached dataset information current for later report runs. In practice, auto-cache is a performance feature for report datasets, reducing the processing overhead required at report generation time while keeping the cached analytical data refreshed. Fortinet describes report and dataset behavior in the FortiAnalyzer documentation, including reporting configuration and SQL dataset concepts, in the [FortiAnalyzer 7.6 Administration Guide](#) and related Fortinet reporting documentation at [FortiAnalyzer 7.6 documentation](#).

QUESTION NO: 5

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 event displayed is correct?

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

ANSWER: C

Explanation:

The security event risk is considered open is correct because FortiAnalyzer treats security events in the SOC/Event Monitor workflow as actionable findings that remain in an open state until they are reviewed, handled, or otherwise closed through the analysis workflow. In the displayed event context, the event is being shown as an active security risk rather than as a completed response action such as quarantine, source isolation, or confirmed prevention. FortiAnalyzer's analyst workflow is designed to let administrators inspect the event details, correlate related logs, assign or escalate the finding, and then close it only after the investigation or remediation decision is complete. This matches the FortiAnalyzer 7.6 SOC analysis model, where event status and incident workflow help analysts track whether a detected risk still requires attention. For more about FortiAnalyzer 7.6 features and administration workflows, see the official [FortiAnalyzer 7.6 documentation](#) and the [FortiAnalyzer 7.6 Administration Guide](#).

QUESTION NO: 6

Exhibit.



The screenshot shows the FortiAnalyzer Log View interface. At the top, there's a filter bar with 'All Devices', 'Last 1 Hour', and a time range '2023-12-05 09:36:22 To 10:36:22'. Below this is a search bar containing 'dstintf=port1'. The main area displays a table of search results with two columns: '#', 'Detailed Information', and a settings icon. Two log entries are visible, both with identical details.

#	Detailed Information
1	<code>date=2023-12-05 time=10:36:21 id=7309181279985991762 itime=2023-12-05 10:36:22 euid=3 epid=101 dsteuid=3 dstepid=101 type=traffic subtype=forward level=notice action=accept policyid=1 sessionid=4937418 srcip=10.0.1.10 dstip=8.8.8.8 transip=10.200.1.10 srcport=35228 dstport=53 transport=35228 trandisp=snat duration=217 proto=17 sentbyte=126 rcvdbyte=272 sentdelta=126 rcvddelta=272 sentpkt=2 rcvdpkt=2 logid=0000000020 service=DNS app=DNS appcat=unscanned srcintfrole=undefined dstintfrole=undefined policytype=policy eventtime=1701801362117936850 poluuid=b11ac58e-791b-51e7-4600-12f829a689d9 srccountry=Reserved dstcountry=United States srcintf=port3 dstintf=port1 policyname=Full_Access tz=-0800 devid=FGVM010000364692 vd=root dtime=2023-12-05 10:36:21 itime_t=1701801362</code>
2	<code>date=2023-12-05 time=10:36:21 id=7309181279985991767 itime=2023-12-05 10:36:22 euid=3 epid=101 dsteuid=3 dstepid=101 type=traffic subtype=forward level=notice action=accept policyid=1 sessionid=4937418 srcip=10.0.1.10 dstip=8.8.8.8 transip=10.200.1.10 srcport=35228 dstport=53 transport=35228 trandisp=snat duration=217 proto=17 sentbyte=16 rcvdbyte=272 sentdelta=64 rcvddelta=272 sentpkt=2 rcvdpkt=2 logid=0000000020 service=DNS app=DNS appcat=unscanned srcintfrole=undefined dstintfrole=undefined policytype=policy eventtime=1701801362117936850 poluuid=b11ac58e-791b-51e7-4600-12f829a689d9 srccountry=Reserved dstcountry=United States srcintf=port3 dstintf=port1 policyname=Full_Access tz=-0800 devid=FGVM010000364692 vd=root dtime=2023-12-05 10:36:21 itime_t=1701801362</code>

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: A D

Explanation:

The correct conclusions are that "They can be downloaded to a file." and "They were searched by using text mode." In FortiAnalyzer Log View, search results can be exported or downloaded from the results page, which is useful when an analyst needs to preserve matching log entries, share them with another team, or use them for offline investigation. The exhibit also indicates that the query was entered as a free-form text search rather than built entirely from structured field

filters. FortiAnalyzer supports this text-mode style of searching so analysts can quickly locate log entries containing specific strings or expressions across the log data. This is commonly used during investigations when the analyst knows part of an event message, IP address, username, host name, or other log value and wants to search directly. Fortinet documents Log View searching and log handling in the FortiAnalyzer administration documentation, including working with log searches and exporting log data. See the [FortiAnalyzer 7.6 Administration Guide](#) and the [FortiAnalyzer 7.6 documentation library](#) for related Log View and search functionality.

QUESTION NO: 7

Exhibit.

FortiAnalyzer partial configuration output		
<pre> 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 ssl-ssl-protocol : disable ssl-ssl-encryption : disable ssl-protocol : tlsv1.3 tlsv1.2 task-list-size : 2000 web-service-protocol : tlsv1.3 tlsv1.2 </pre>	<pre> 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 ssl-ssl-protocol : tlsv1.2 ssl-ssl-encryption : disable ssl-protocol : tlsv1.3 tlsv1.2 task-list-size : 2000 web-service-protocol : tlsv1.3 tlsv1.2 </pre>	<pre> FortiAnalyzer3# get system status Platform Type : FAZVM64-KVM Platform Full Name : FortiAnalyzer-VM64-KVM 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 ssl-ssl-protocol : tlsv1.2 ssl-ssl-encryption : disable ssl-protocol : tlsv1.3 tlsv1.2 task-list-size : 2000 web-service-protocol : tlsv1.3 tlsv1.2 </pre>

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

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

ANSWER: D

Explanation:

All devices listed can be members. A FortiAnalyzer Fabric is intended to group compatible FortiAnalyzer units so they can work together while still being managed as independent FortiAnalyzer systems. The key requirements shown in the exhibit are that the units are running the same FortiAnalyzer firmware release, are using compatible FortiAnalyzer platforms, have ADOM support enabled with a compatible ADOM mode, and are operating as standalone FortiAnalyzer systems rather than being tied into a conflicting HA configuration. The displayed outputs indicate that FortiAnalyzer1, FortiAnalyzer2, and FortiAnalyzer3 match those membership conditions, so there is no compatibility conflict preventing any of them from participating in the FortiAnalyzer Fabric. In practice, matching firmware and compatible global settings are especially important because Fabric operations rely on consistent behavior between members for communication, ADOM handling, and log-management workflows. Fortinet's FortiAnalyzer documentation describes the Fabric feature and related administration requirements in the FortiAnalyzer 7.6 documentation set; see the [FortiAnalyzer 7.6 documentation library](#) and the [FortiAnalyzer 7.6 Administration Guide](#).

QUESTION NO: 8

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: C D

Explanation:

FortiAnalyzer local logs are generated by FortiAnalyzer itself and are separated by scope. “Event logs show system-wide information, whereas application logs are ADOM-specific” is correct because FortiAnalyzer event logs record platform-level activity, such as administrative and system events that apply to the appliance rather than to one individual ADOM. Application logs, on the other hand, are tied to FortiAnalyzer features and activity within an ADOM context, so their visibility follows the selected ADOM. “Event logs are available only in the root ADOM” is also correct because system-wide local event logging is exposed from the root ADOM, while non-root ADOMs focus on ADOM-specific application log visibility. This distinction is important for troubleshooting: if you are investigating FortiAnalyzer appliance behavior or administrative/system events, you should check local event logs from the root ADOM; if you are investigating activity related to features running inside a specific ADOM, you should review the relevant application logs in that ADOM. Fortinet’s FortiAnalyzer documentation organizes administration and log-view behavior around ADOM context and local FortiAnalyzer logs; see the [FortiAnalyzer 7.6 documentation](#) and the [FortiAnalyzer 7.6 Administration Guide](#).