

## NSE5\_FAZ-7.2 Dumps

### Fortinet NSE 5 - FortiAnalyzer 7.2

[https://www.certleader.com/NSE5\\_FAZ-7.2-dumps.html](https://www.certleader.com/NSE5_FAZ-7.2-dumps.html)



**NEW QUESTION 1**

What is Log Insert Lag Time on FortiAnalyzer?

- A. The number of times in the logs where end users experienced slowness while accessing resources.
- B. The amount of lag time that occurs when the administrator is rebuilding the ADOM database.
- C. The amount of time that passes between the time a log was received and when it was indexed on FortiAnalyzer.
- D. The amount of time FortiAnalyzer takes to receive logs from a registered device

**Answer: C**

**NEW QUESTION 2**

Which two of the following must you configure on FortiAnalyzer to email a FortiAnalyzer report externally? (Choose two.)

- A. Mail server
- B. Output profile
- C. SFTP server
- D. Report scheduling

**Answer: AB**

**NEW QUESTION 3**

On the RAID management page, the disk status is listed as Initializing.

What does the status Initializing indicate about what the FortiAnalyzer is currently doing?

- A. FortiAnalyzer is ensuring that the parity data of a redundant drive is valid
- B. FortiAnalyzer is writing data to a newly added hard drive to restore it to an optimal state
- C. FortiAnalyzer is writing to all of its hard drives to make the array fault tolerant
- D. FortiAnalyzer is functioning normally

**Answer: C**

**NEW QUESTION 4**

If a hard disk fails on a FortiAnalyzer that supports software RAID, what should you do to bring the FortiAnalyzer back to functioning normally, without losing data?

- A. Hot swap the disk
- B. Replace the disk and rebuild the RAID manually
- C. Take no action if the RAID level supports a failed disk
- D. Shut down FortiAnalyzer and replace the disk

**Answer: D**

**Explanation:**

<https://kb.fortinet.com/kb/documentLink.do?externalID=FD46446#:~:text=On%20FortiAnalyzer%2FFortiMana> If a hard disk on a FortiAnalyzer unit fails, it must be replaced. On FortiAnalyzer devices that support hardware RAID, the hard disk can be replaced while the unit is still running – known as hot swapping. On FortiAnalyzer units with software RAID, the device must be shutdown prior to exchanging the hard disk.

**NEW QUESTION 5**

Which two constraints can impact the amount of reserved disk space required by FortiAnalyzer? (Choose two.)

- A. License type
- B. Disk size
- C. Total quota
- D. RAID level

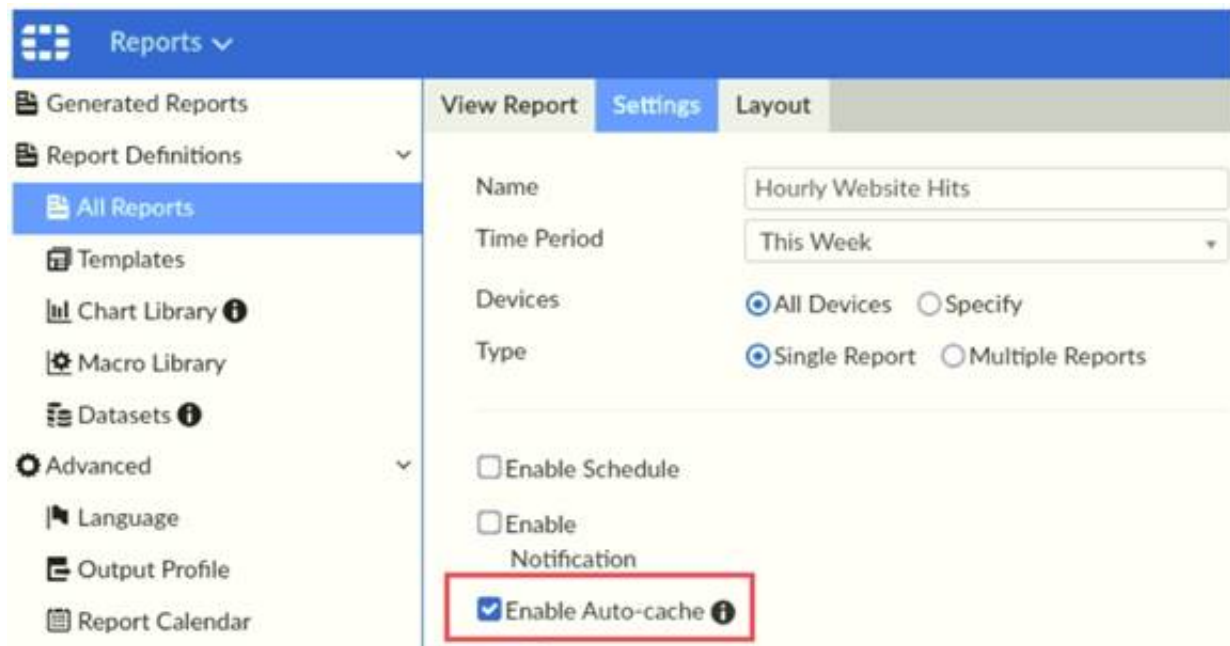
**Answer: BD**

**Explanation:**

<https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/368682/disk-space-allocation>

**NEW QUESTION 6**

Refer to the exhibit.



Which two statements are true regarding enabling auto-cache on FortiAnalyzer? (Choose two.)

- A. Report size will be optimized to conserve disk space on FortiAnalyzer.
- B. Reports will be cached in the memory.
- C. This feature is automatically enabled for scheduled reports.
- D. Enabling auto-cache reduces report generation time for reports that require a long time to assemble datasets.

**Answer: CD**

#### NEW QUESTION 7

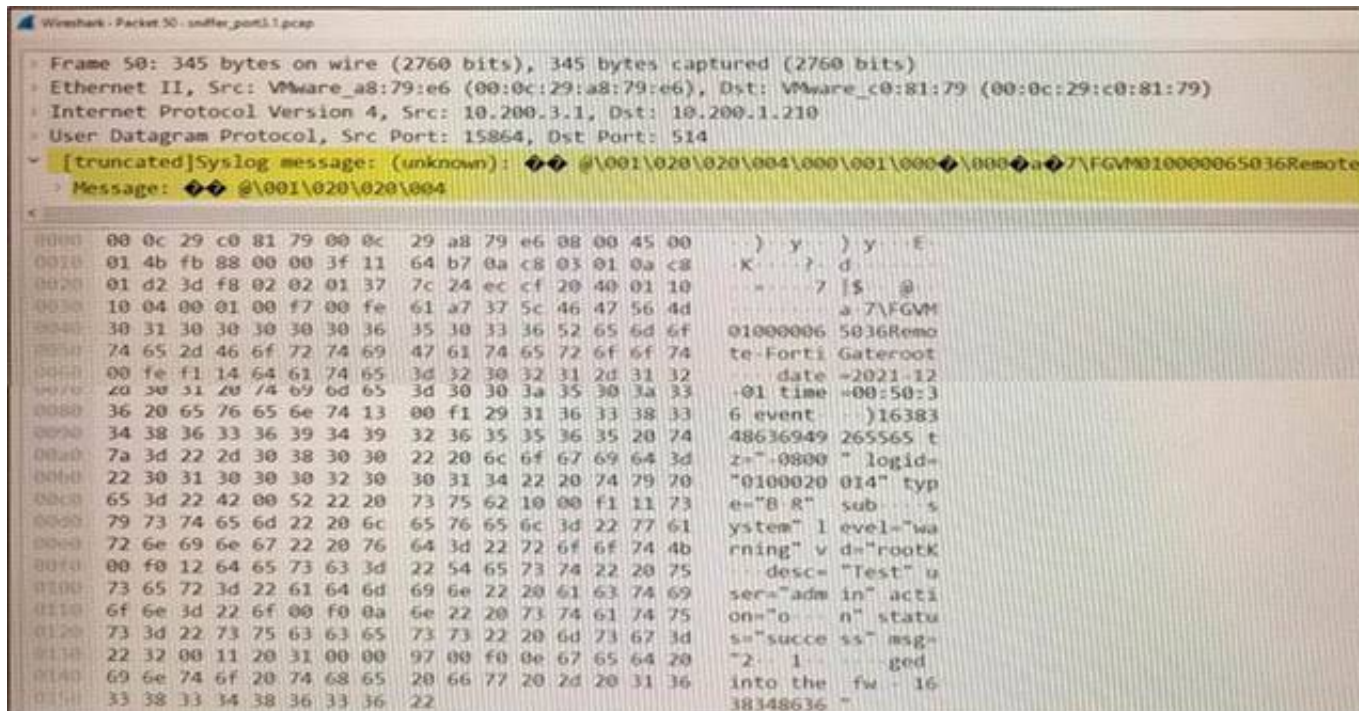
Which two statements are true regarding FortiAnalyzer operating modes? (Choose two.)

- A. When in collector mode, FortiAnalyzer collects logs from multiple devices and forwards these logs in the original binary format.
- B. Collector mode is the default operating mode.
- C. When in collector mod
- D. FortiAnalyzer supports event management and reporting features.
- E. By deploying different FortiAnalyzer devices with collector and analyzer mode in a network, you can improve the overall performance of log receiving, analysis, and reporting

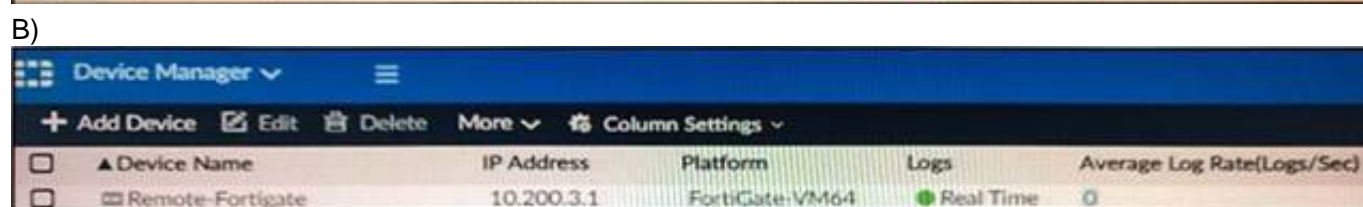
**Answer: AD**

#### NEW QUESTION 8

Refer to the exhibit.



Which image corresponds to the packet capture shown in the exhibit?





D)



<input type="checkbox"/>	▲ Device Name	IP Address	Platform	Logs	Average Log Rate(Logs/Sec)
<input type="checkbox"/>	Remote-Fortigate	10.200.3.1	FortiGate-VM64	Real Time	0

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

**Answer:** D**NEW QUESTION 9**

What FortiGate process caches logs when FortiAnalyzer is not reachable?

- A. logfiled
- B. sqlplugind
- C. oftpd
- D. miglogd

**Answer:** D**NEW QUESTION 10**

You've moved a registered logging device out of one ADOM and into a new ADOM. What happens when you rebuild the new ADOM database?

- A. FortiAnalyzer resets the disk quota of the new ADOM to default.
- B. FortiAnalyzer migrates archive logs to the new ADOM.
- C. FortiAnalyzer migrates analytics logs to the new ADOM.
- D. FortiAnalyzer removes logs from the old ADOM.

**Answer:** C**Explanation:**<https://kb.fortinet.com/kb/documentLink.do?externalID=FD40383>**NEW QUESTION 10**

Which FortiAnalyzer feature allows you to use a proactive approach when managing your network security?

- A. Incidents dashboards
- B. Threat hunting
- C. FortiView Monitor
- D. Outbreak alert services

**Answer:** B**NEW QUESTION 11**

Which two elements are contained in a system backup created on FortiAnalyzer? (Choose two.)

- A. System information
- B. Logs from registered devices
- C. Report information
- D. Database snapshot

**Answer:** AB**NEW QUESTION 14**

Which two statements about log forwarding are true? (Choose two.)

- A. Forwarded logs cannot be filtered to match specific criteria.
- B. Logs are forwarded in real-time only.
- C. The client retains a local copy of the logs after forwarding.
- D. You can use aggregation mode only with another FortiAnalyzer.

**Answer:** CD**Explanation:**<https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/420493/modes> <https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/621804/log-forwarding>**NEW QUESTION 18**

Refer to the exhibit.

The image displays the configuration of a FortiAnalyzer the administrator wants to join to an existing HA cluster. What can you conclude from the configuration displayed?

- A. This FortiAnalyzer will join to the existing HA cluster as the primary.
- B. This FortiAnalyzer is configured to receive logs in its port1.
- C. This FortiAnalyzer will trigger a failover after losing communication with its peers for 10 seconds.
- D. After joining to the cluster, this FortiAnalyzer will keep an updated log database.

**Answer: D**

### NEW QUESTION 23

Which statements are correct regarding FortiAnalyzer reports? (Choose two)

- A. FortiAnalyzer provides the ability to create custom reports.
- B. FortiAnalyzer glows you to schedule reports to run.
- C. FortiAnalyzer includes pre-defined reports only.
- D. FortiAnalyzer allows reporting for FortiGate devices only.

**Answer: AB**

### NEW QUESTION 25

Refer to the exhibits.

How many events will be added to the incident created after running this playbook?

- A. Ten events will be added.
- B. No events will be added.
- C. Five events will be added.
- D. Thirteen events will be added.

**Answer: C**

### NEW QUESTION 27

How do you restrict an administrator's access to a subset of your organization's ADOMs?

- A. Set the ADOM mode to Advanced
- B. Assign the ADOMs to the administrator's account
- C. Configure trusted hosts
- D. Assign the default Super\_User administrator profile

**Answer:** B

**Explanation:**

<https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/717578/assigning-administrators-to>

**NEW QUESTION 29**

Which daemon is responsible for enforcing raw log file size?

- A. logfiled
- B. oftpd
- C. sqlplugind
- D. miglogd

**Answer:** A

**NEW QUESTION 30**

Which daemon is responsible for enforcing the log file size?

- A. sqlplugind
- B. logfiled
- C. miglogd
- D. ofrpd

**Answer:** B

**NEW QUESTION 32**

Which tabs do not appear when FortiAnalyzer is operating in Collector mode?

- A. FortiView
- B. Event Management
- C. Device Manger
- D. Reporting

**Answer:** B

**NEW QUESTION 37**

When you perform a system backup, what does the backup configuration contain? (Choose two.)

- A. Generated reports
- B. Device list
- C. Authorized devices logs
- D. System information

**Answer:** BD

**Explanation:**

[https://help.fortinet.com/fa/cli-olh/5-6-5/Content/Document/1400\\_execute/backup.htm](https://help.fortinet.com/fa/cli-olh/5-6-5/Content/Document/1400_execute/backup.htm)

**NEW QUESTION 41**

On FortiAnalyzer, what is a wildcard administrator account?

- A. An account that permits access to members of an LDAP group
- B. An account that allows guest access with read-only privileges
- C. An account that requires two-factor authentication
- D. An account that validates against any user account on a FortiAuthenticator

**Answer:** A

**Explanation:**

<https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/747268/configuring-wildcard-admin-accounts>

**NEW QUESTION 43**

A play book contains five tasks in total. An administrator executed the playbook and four out of five tasks finished successfully, but one task failed. What will be the status of the playbook after its execution?

- A. Success
- B. Failed
- C. Running
- D. Upstream\_failed

**Answer:** A

**NEW QUESTION 46**

By default, what happens when a log file reaches its maximum file size?



- A. FortiAnalyzer overwrites the log files.
- B. FortiAnalyzer stops logging.
- C. FortiAnalyzer rolls the active log by renaming the file.
- D. FortiAnalyzer forwards logs to syslog.

**Answer:** C

#### NEW QUESTION 51

Which two settings must you configure on FortiAnalyzer to allow non-local administrators to authenticate to FortiAnalyzer with any user account in a single LDAP group? (Choose two.)

- A. A local wildcard administrator account
- B. A remote LDAP server
- C. A trusted host profile that restricts access to the LDAP group
- D. An administrator group

**Answer:** AB

#### NEW QUESTION 52

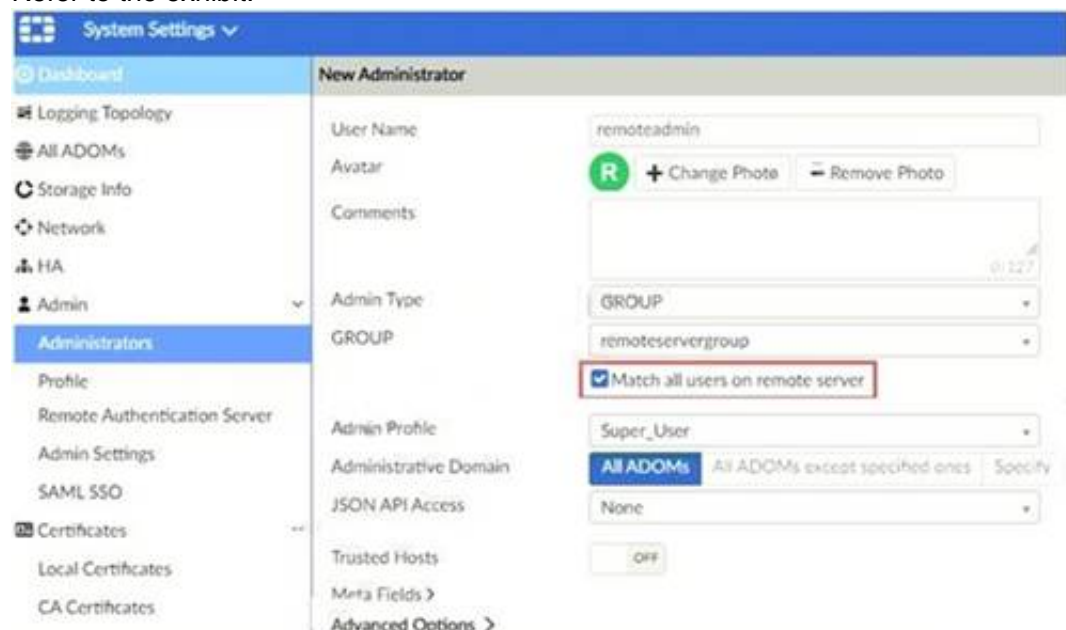
Which clause is considered mandatory in SELECT statements used by the FortiAnalyzer to generate reports?

- A. FROM
- B. LIMIT
- C. WHERE
- D. ORDER BY

**Answer:** A

#### NEW QUESTION 54

Refer to the exhibit.



The exhibit shows “remoteservergroup” is an authentication server group with LDAP and RADIUS servers. Which two statements express the significance of enabling “Match all users on remote server” when configuring a new administrator? (Choose two.)

- A. It creates a wildcard administrator using LDAP and RADIUS servers.
- B. Administrator can log in to FortiAnalyzer using their credentials on remote servers LDAP and RADIUS.
- C. Use remoteadmin from LDAP and RADIUS servers will be able to log in to FortiAnalyzer at anytime.
- D. It allows administrators to use two-factor authentication.

**Answer:** AB

#### NEW QUESTION 57

An administrator fortinet, is able to view logs and perform device management tasks, such as adding and removing registered devices. However, administrator fortinet is not able to create a mail server that can be used to send email. What could be the problem?

- A. Fortinet is assigned the Standard\_ User administrator profile.
- B. A trusted host is configured.
- C. ADOM mode is configured with Advanced mode.
- D. Fortinet is assigned the Restricted\_ User administrator profile.

**Answer:** A

#### NEW QUESTION 59

FortiAnalyzer centralizes which functions? (Choose three)

- A. Network analysis
- B. Graphical reporting
- C. Content archiving / data mining

- D. Vulnerability assessment
- E. Security log analysis / forensics

**Answer:** BCE

**NEW QUESTION 62**

In Log View, you can use the Chart Builder feature to build a dataset and chart based on the filtered search results. Similarly, which feature you can use for FortiView?

- A. Export to Report Chart
- B. Export to PDF
- C. Export to Chart Builder
- D. Export to Custom Chart

**Answer:** A

**NEW QUESTION 63**

.....



## Thank You for Trying Our Product

\* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

\* One year free update

You can enjoy free update one year. 24x7 online support.

\* Trusted by Millions

We currently serve more than 30,000,000 customers.

\* Shop Securely

All transactions are protected by VeriSign!

**100% Pass Your NSE5\_FAZ-7.2 Exam with Our Prep Materials Via below:**

[https://www.certleader.com/NSE5\\_FAZ-7.2-dumps.html](https://www.certleader.com/NSE5_FAZ-7.2-dumps.html)