



Fortinet

Exam Questions NSE5_FAZ-7.0

Fortinet NSE 5 - FortiAnalyzer 7.0

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 statements express the advantages of grouping similar reports? (Choose two.)

- A. Improve report completion time.
- B. Conserve disk space on FortiAnalyzer by grouping multiple similar reports.
- C. Reduce the number of hcache tables and improve auto-hcache completion time.
- D. Provides a better summary of reports.

Answer: AC

NEW QUESTION 3

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

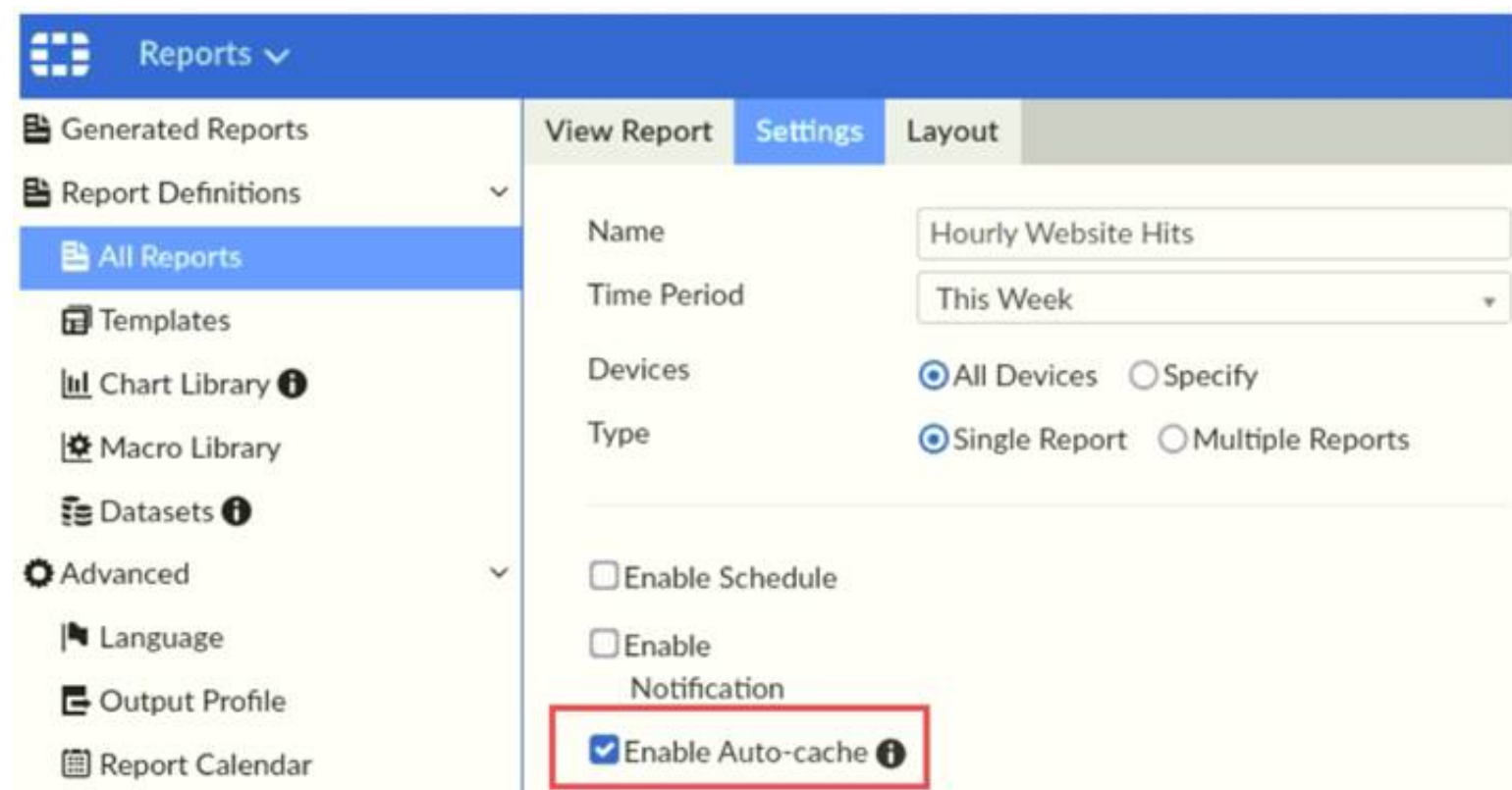
Answer: BD

Explanation:

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

NEW QUESTION 4

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 5

View the exhibit.

```

Total Quota Summary:
      Total Quota    Allocated    Available    Allocate%
      63.7GB        12.7GB        51.0GB        19.9%

System Storage Summary:
      Total      Used      Available      Use%
      78.7GB    2.9GB      75.9GB        3.6%

Reserved space: 15.0GB (19.0% of total space).

```

Why is the total quota less than the total system storage?

- A. 3.6% of the system storage is already being used.
- B. Some space is reserved for system use, such as storage of compression files, upload files, and temporary report files
- C. The oftpd process has not archived the logs yet
- D. The logfiled process is just estimating the total quota

Answer: B

Explanation:

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

NEW QUESTION 6

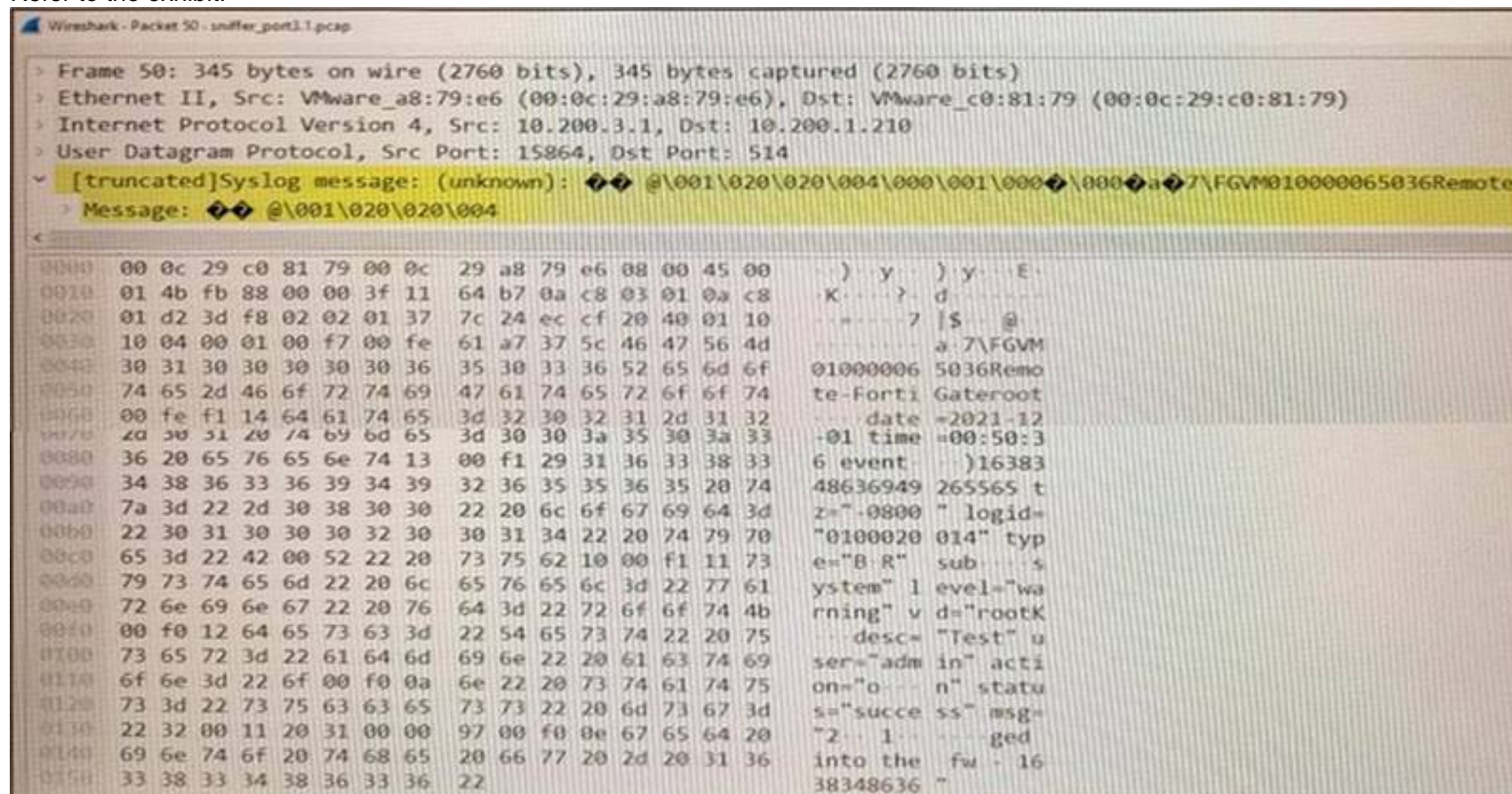
Which SQL query is in the correct order to query the database in the FortiAnalyzer?

- A. SELECT devid FROM Slog GROOP BY devid WHERE * user' =* USER!
B. SELECT devid WHERE 'u3er'='USER!' FROM \$ log GROUP BY devid
C. SELECT devid FROM Slog- WHERE *user' = ' USER!' GROUP BY devid
D. FROM Slog WHERE 'user* = ' USER!' SELECT devid GROUP BY devid

Answer: C

NEW QUESTION 7

Refer to the exhibit.



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

A)

Device Manager					
+ Add Device Edit Delete More Column Settings					
<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

B)

Device Manager					
+ Add Device Edit Delete More Column Settings					
<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

C)



<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

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 8

FortiAnalyzer reports are dropping analytical data from 15 days ago, even though the data policy setting for analytics logs is 60 days. What is the most likely problem?

- A. Quota enforcement is acting on analytical data before a report is complete
- B. Logs are rolling before the report is run
- C. CPU resources are too high
- D. Disk utilization for archive logs is set for 15 days

Answer: B

NEW QUESTION 9

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

In order for FortiAnalyzer to collect logs from a FortiGate device, what configuration is required? (Choose two.)

- A. Remote logging must be enabled on FortiGate
- B. Log encryption must be enabled
- C. ADOMs must be enabled
- D. FortiGate must be registered with FortiAnalyzer

Answer: AD

Explanation:

Pg 70: "after you add and register a FortiGate device with the FortiAnalyzer unit, you must also ensure that the FortiGate device is configured to send logs to the FortiAnalyzer unit."

<https://docs.fortinet.com/uploaded/files/4614/FortiAnalyzer-5.4.6-Administration%20Guide.pdf>

Pg 45: "ADOMs must be enabled to support the logging and reporting of NON-FORTIGATE devices, such as FortiCarrier, FortiClientEMS, FortiMail, FortiWeb, FortiCache, and FortiSandbox."

NEW QUESTION 10

How does FortiAnalyzer retrieve specific log data from the database?

- A. SQL FROM statement
- B. SQL GET statement
- C. SQL SELECT statement
- D. SQL EXTRACT statement

Answer: A

Explanation:

<https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/137bb60e-ff37-11e8-8524-f8bc1258b8>

NEW QUESTION 11

After you have moved a registered logging device out of one ADOM and into a new ADOM, what is the purpose of running the following CLI command?
execute sql-local rebuild-adom <new-ADOM-name>

- A. To reset the disk quota enforcement to default
- B. To remove the analytics logs of the device from the old database
- C. To migrate the archive logs to the new ADOM
- D. To populate the new ADOM with analytical logs for the moved device, so you can run reports

Answer: D

Explanation:

- Are the device's analytics logs required for reports in the *new* ADOM? If so, rebuild the new ADOM database:
exe sql-local rebuild-adom <new-ADOM-name>

NEW QUESTION 14

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 16

Refer to the exhibit.

Event	Event Status	Event Type	Count	Severity
151.101.54.62 (1) Insecure SSL Connection blocked from 10.0.3.20	Mitigated	SSL	1	Low

Which statement is correct regarding the event displayed?

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

Answer: A

NEW QUESTION 19

An administrator has moved FortiGate A from the root ADOM to ADOM1. However, the administrator is not able to generate reports for FortiGate A in ADOM1. What should the administrator do to solve this issue?

- A. Use the execute sql-local rebuild-db command to rebuild all ADOM databases.
- B. Use the execute sql-local rebuild-adom ADOM1 command to rebuild the ADOM database.
- C. Use the execute sql-report run ADOM1 command to run a report.
- D. Use the execute sql-local rebuild-adom root command to rebuild the ADOM database.

Answer: B

NEW QUESTION 23

What happens when a log file saved on FortiAnalyzer disks reaches the size specified in the device log settings?

- A. The log file is stored as a raw log and is available for analytic support.
- B. The log file rolls over and is archived.
- C. The log file is purged from the database.
- D. The log file is overwritten.

Answer: B

NEW QUESTION 26

Which statement is true regarding Macros on FortiAnalyzer?

- A. Macros are ADOM specific and each ADOM will have unique macros relevant to that ADOM.
- B. Macros are supported only on the FortiGate ADOM.
- C. Macros are useful in generating excel log files automatically based on the reports settings.
- D. Macros are predefined templates for reports and cannot be customized.

Answer: A

NEW QUESTION 28

How are logs forwarded when FortiAnalyzer is using aggregation mode?

- A. Logs are forwarded as they are received and content files are uploaded at a scheduled time.
- B. Logs and content files are stored and uploaded at a scheduled time.
- C. Logs are forwarded as they are received.
- D. Logs and content files are forwarded as they are received.

Answer: B

Explanation:

<https://www.fortinetguru.com/2020/07/log-forwarding-fortianalyzer-fortios-6-2-3/> <https://docs.fortinet.com/document/fortianalyzer/6.2.0/administration-guide/420493/modes>

NEW QUESTION 30

What is the purpose of output variables?

- A. To store playbook execution statistics
- B. To use the output of the previous task as the input of the current task
- C. To display details of the connectors used by a playbook
- D. To save all the task settings when a playbook is exported

Answer: A

NEW QUESTION 35

What is the purpose of a dataset query in FortiAnalyzer?

- A. It sorts log data into tables
- B. It extracts the database schema
- C. It retrieves log data from the database
- D. It injects log data into the database

Answer: C

NEW QUESTION 38

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

- A. FortiAnalyzer provides the ability to create custom reports.
- B. FortiAnalyzer allows 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 39

Which statement is true when you are upgrading the firmware on an HA cluster made up of two FortiAnalyzer devices?

- A. First, upgrade the secondary device, and then upgrade the primary device.
- B. Both FortiAnalyzer devices will be upgraded at the same time.
- C. You can enable uninterruptible-upgrade so that the normal FortiAnalyzer operations are not interrupted while the cluster firmware upgrades.
- D. You can perform the firmware upgrade using only a console connection.

Answer: D

NEW QUESTION 43

Which statement correctly describes the management extensions available on FortiAnalyzer?

- A. Management extensions do not require additional licenses.
- B. Management extensions allow FortiAnalyzer to act as a FortiSIEM supervisor.
- C. Management extensions require a dedicated VM for best performance.
- D. Management extensions may require a minimum number of CPU cores to run.

Answer: A

NEW QUESTION 48

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

NEW QUESTION 49

Which log type does the FortiAnalyzer indicators of compromise feature use to identify infected hosts?

- A. Antivirus logs
- B. Web filter logs
- C. IPS logs
- D. Application control logs

Answer: B

NEW QUESTION 50

What remote authentication servers can you configure to validate your FortiAnalyzer administrator logons? (Choose three)

- A. RADIUS
- B. Local
- C. LDAP
- D. PKI
- E. TACACS+

Answer: ACE

NEW QUESTION 55

What must you configure on FortiAnalyzer to upload a FortiAnalyzer report to a supported external server? (Choose two.)

- A. SFTP, FTP, or SCP server
- B. Mail server
- C. Output profile
- D. Report scheduling

Answer: BC

Explanation:

<https://docs.fortinet.com/document/fortianalyzer/6.0.2/administration-guide/598322/creating-output-profiles>

NEW QUESTION 59

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 60

Which two statement are true regardless initial Logs sync and Log Data Sync for Ha on FortiAnalyzer?

- A. By default, Log Data Sync is disabled on all backup device.
- B. Log Data Sync provides real-time log synchronization to all backup devices.
- C. With initial Logs Sync, when you add a unit to an HA cluster, the primary device synchronizes its logs with the backup device.
- D. When Logs Data Sync is turned on, the backup device will reboot and then rebuilt the log database with the synchronized logs.

Answer: CD

NEW QUESTION 64

What are analytics logs on FortiAnalyzer?

- A. Log type Traffic logs.
- B. Logs that roll over when the log file reaches a specific size.
- C. Logs that are indexed and stored in the SQL.
- D. Raw logs that are compressed and saved to a log file.

Answer: C

NEW QUESTION 65

For which two SAML roles can the FortiAnalyzer be configured? (Choose two.)

- A. Principal
- B. Service provider
- C. Identity collector
- D. Identity provider

Answer: BD

NEW QUESTION 68

For proper log correlation between the logging devices and FortiAnalyzer, FortiAnalyzer and all registered devices should:

- A. Use DNS
- B. Use host name resolution
- C. Use real-time forwarding
- D. Use an NTP server

Answer: D

NEW QUESTION 70

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 72

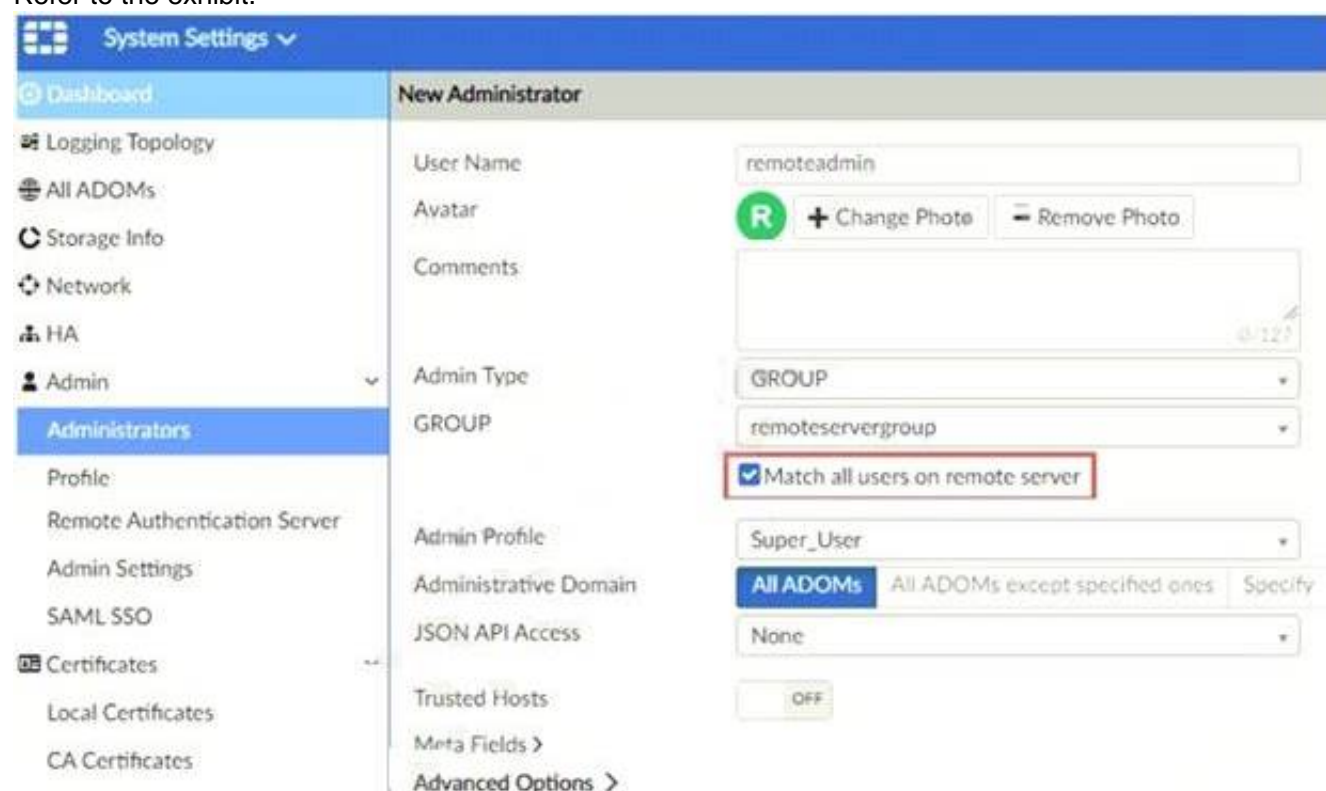
In FortiAnalyzer's FormView, source and destination IP addresses from FortiGate devices are not resolving to a hostname. How can you resolve the source and destination IPs, without introducing any additional performance impact to FortiAnalyzer?

- A. Configure local DNS servers on FortiAnalyzer
- B. Resolve IPs on FortiGate
- C. Configure # set resolve-ip enable in the system FortiView settings
- D. Resolve IPs on a per-ADOM basis to reduce delay on FortiView while IPs resolve

Answer: B

NEW QUESTION 77

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 81

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 85

What can the CLI command # diagnose test application oftpd 3 help you to determine?

- A. What devices and IP addresses are connecting to FortiAnalyzer
- B. What logs, if any, are reaching FortiAnalyzer
- C. What ADOMs are enabled and configured
- D. What devices are registered and unregistered

Answer: A

Explanation:

https://docs.fortinet.com/document/fortianalyzer/6.2.5/cli-reference/395556/test#test_application

NEW QUESTION 87

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 89

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

NSE5_FAZ-7.0 Practice Exam Features:

- * NSE5_FAZ-7.0 Questions and Answers Updated Frequently
- * NSE5_FAZ-7.0 Practice Questions Verified by Expert Senior Certified Staff
- * NSE5_FAZ-7.0 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * NSE5_FAZ-7.0 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The NSE5_FAZ-7.0 Practice Test Here](#)