Fortinet

Exam Questions NSE5_FAZ-7.2

Fortinet NSE 5 - FortiAnalyzer 7.2

NEW QUESTION 1
What is the best approach to handle a hard disk failure on a FortiAnalyzer that supports hardware RAID?

A. Hot swap the disk.
B. There is no need to do anything because the disk will self-recover.
C. Run execute format disk to format and restart the FortiAnalyzer device.
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 2
Consider the CLI command:

```
# configure system global
    set log-checksum md5
  end
```

What is the purpose of the command?

A. To add a unique tag to each log to prove that it came from this FortiAnalyzer
B. To add the MD5 hash value and authentication code
C. To add a log file checksum
D. To encrypt log communications

Answer: C

Explanation:
https://docs.fortinet.com/document/fortianalyzer/6.2.5/cli-reference/849211/global

NEW QUESTION 3
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 4
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 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 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 7
Which SQL query is in the correct order to query the database in the FortiAnslyzer?

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

Answer: C

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
Which FortiAnalyzer feature allows you to retrieve the archived logs matching a specific timeframe from another FortiAnalyzer device?

A. Log upload
B. Indicators of Compromise
C. Log forwarding an aggregation mode
D. Log fetching

Answer: D

Explanation:
https://docs.fortinet.com/document/fortianalyzer/6.2.0/administration-guide/651442/fetcher-management

NEW QUESTION 10
Refer to the exhibit.

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 10
What are the operating modes of FortiAnalyzer? (Choose two)

A. Standalone
B. Manager
C. Analyzer
D. Collector

Answer: CD

NEW QUESTION 13
You have recently grouped multiple FortiGate devices into a single ADOM. System Settings > Storage Info shows the quota used.
What does the disk quota refer to?

A. The maximum disk utilization for each device in the ADOM
B. The maximum disk utilization for the FortiAnalyzer model
C. The maximum disk utilization for the ADOM type
D. The maximum disk utilization for all devices in the ADOM

Answer: D

NEW QUESTION 14
Which two methods are the most common methods to control and restrict administrative access on FortiAnalyzer? (Choose two.)

A. Virtual domains
B. Administrative access profiles
C. Trusted hosts
D. Security Fabric

Answer: BC

NEW QUESTION 17
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 19
An administrator has configured the following settings: config system fortiview settings
set resolve-ip enable end
What is the significance of executing this command?

A. Use this command only if the source IP addresses are not resolved on FortiGate.
B. It resolves the source and destination IP addresses to a hostname in FortiView on FortiAnalyzer.
C. You must configure local DNS servers on FortiGate for this command to resolve IP addresses on Forti Analyzer.
D. It resolves the destination IP address to a hostname in FortiView on FortiAnalyzer.

Answer: D

NEW QUESTION 24
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 25
What purposes does the auto-cache setting on reports serve? (Choose two.)

A. To reduce report generation time
B. To automatically update the hcache when new logs arrive
C. To reduce the log insert lag rate
D. To provide diagnostics on report generation time

Answer: AB

NEW QUESTION 26
A rogue administrator was accessing FortiAnalyzer without permission, and you are tasked to see what activity was performed by that rogue administrator on FortiAnalyzer.
What can you do on FortiAnalyzer to accomplish this?

A. Click FortiView and generate a report for that administrator.
B. Click Task Monitor and view the tasks performed by that administrator.
C. Click Log View and generate a report for that administrator.
D. View the tasks performed by the rogue administrator in Fabric View.

Answer: B

NEW QUESTION 31
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 34
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 37
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 ForbSIEM 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 38
What is the purpose of the following CLI command?

```
# configure system global
     set log-checksum md5
end
```

A. To add a log file checksum
B. To add the MD's hash value and authentication code
C. To add a unique tag to each log to prove that it came from this FortiAnalyzer
D. To encrypt log communications

Answer: A

Explanation:
https://docs2.fortinet.com/document/fortianalyzer/6.0.3/cli-reference/849211/global

NEW QUESTION 42
Which daemon is responsible for enforcing raw log file size?

A. logfiled
B. oftpd

C. sqlplugind
D. miglogd

Answer: A

NEW QUESTION 45
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 48
Which two statements are correct regarding the export and import of playbooks? (Choose two.)

A. You can export only one playbook at a time.
B. You can import a playbook even if there is another one with the same name in the destination.
C. Playbooks can be exported and imported only within the same FortiAnaryzer.
D. A playbook that was disabled when it was exported, will be disabled when it is imported.

Answer: BD

NEW QUESTION 50
Which two purposes does the auto cache setting on reports serve? (Choose two.)

A. It automatically updates the hcache when new logs arrive.
B. It provides diagnostics on report generation time.
C. It reduces the log insert lag rate.
D. It reduces report generation time.

Answer: AD

NEW QUESTION 53
The admin administrator is failing to register a FortiClient EMS on the FortiAnalyzer device. What can be the reason for this failure?

A. FortiAnalyzer is in an HA cluster.
B. ADOM mode should be set to advanced, in order to register the FortiClient EMS device.
C. ADOMs are not enabled on FortiAnalyzer.
D. A separate license is required on FortiAnalyzer in order to register the FortiClient EMS device.

Answer: C

NEW QUESTION 57
For which two purposes would you use the command set log checksum? (Choose two.)

A. To help protect against man-in-the-middle attacks during log upload from FortiAnalyzer to an SFTP server
B. To prevent log modification or tampering
C. To encrypt log communications
D. To send an identical set of logs to a second logging server

Answer: AB

NEW QUESTION 61
Which statements are true regarding securing communications between FortiAnalyzer and FortiGate with SSL? (Choose two.)

A. SSL is the default setting.
B. SSL communications are auto-negotiated between the two devices.
C. SSL can send logs in real-time only.
D. SSL encryption levels are globally set on FortiAnalyzer.
E. FortiAnalyzer encryption level must be equal to, or higher than, FortiGate.

Answer: AD

NEW QUESTION 64
Logs are being deleted from one of the ADOMs earlier than the configured setting for archiving in the data policy.
What is the most likely problem?

A. CPU resources are too high
B. Logs in that ADOM are being forwarded, in real-time, to another FortiAnalyzer device
C. The total disk space is insufficient and you need to add other disk
D. The ADOM disk quota is set too low, based on log rates

Answer: D

NEW QUESTION 68
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 73
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 77
Which clause is considered mandatory in SELECT statements used by the FortiAnalyzer to generate reports?

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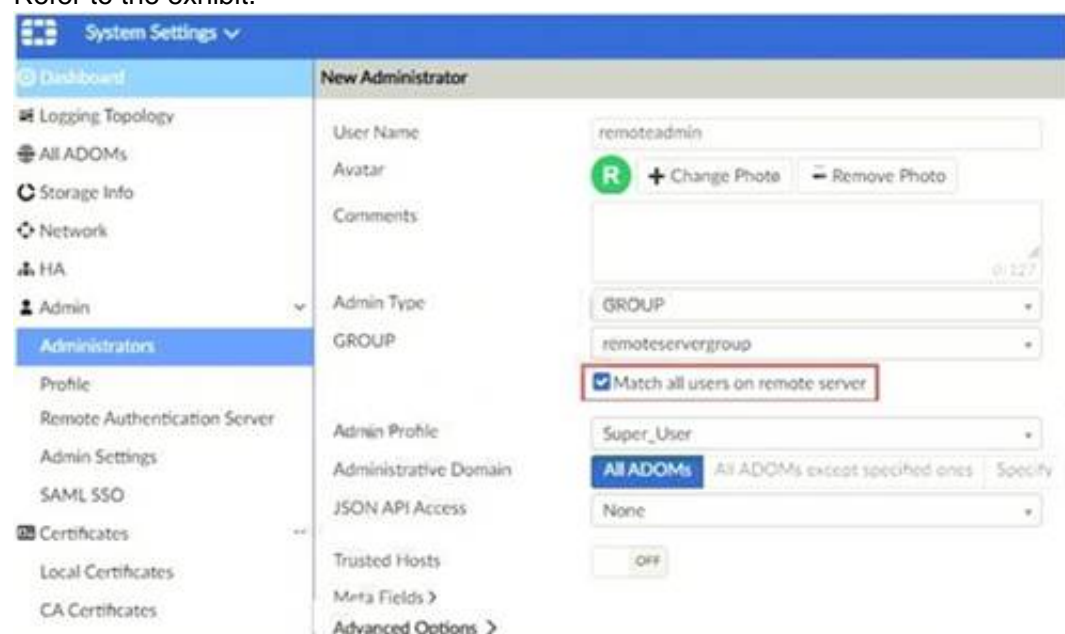C. WHERE
D. ORDER BY

Answer: A

NEW QUESTION 80
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 83
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 86

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 mall 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 91
What is the main purpose of using an NTP server on FortiAnalyzer and all of its registered devices?

A. Log correlation
B. Host name resolution
C. Log collection
D. Real-time forwarding

Answer: A

NEW QUESTION 93
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 97
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 101
......

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

NSE5_FAZ-7.2 Practice Exam Features:

* NSE5_FAZ-7.2 Questions and Answers Updated Frequently

* NSE5_FAZ-7.2 Practice Questions Verified by Expert Senior Certified Staff

* NSE5_FAZ-7.2 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* NSE5_FAZ-7.2 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The NSE5_FAZ-7.2 Practice Test Here](#)