

Fortinet

Exam Questions NSE5_FAZ-7.2

Fortinet NSE 5 - FortiAnalyzer 7.2



NEW QUESTION 1

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 2

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 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

When working with FortiAnalyzer reports, what is the purpose of a dataset?

- A. To provide the layout used for reports
- B. To define the chart type to be used
- C. To retrieve data from the database
- D. To set the data included in templates

Answer: C

NEW QUESTION 5

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 6

Which two methods can you use to send event notifications when an event occurs that matches a configured event handler? (Choose two.)

- A. SMS
- B. Email
- C. SNMP
- D. IM

Answer: BC

NEW QUESTION 7

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

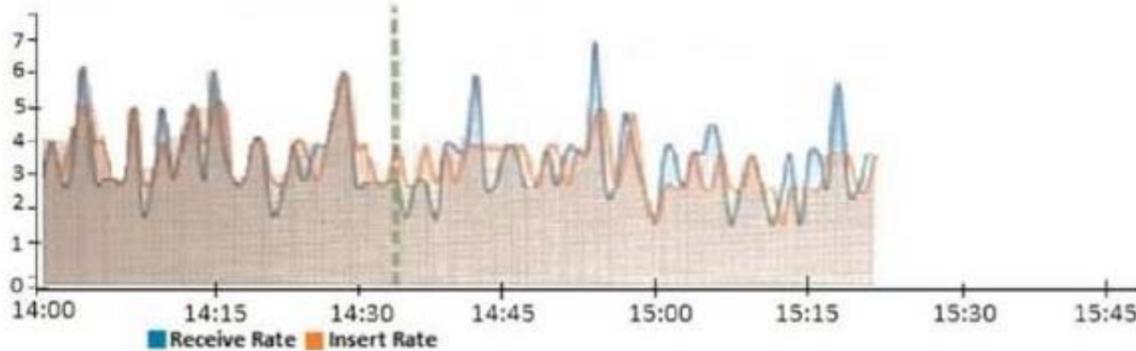
Explanation:

<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 8

View the exhibit.

Insert Rate vs Receive Rate - Last 1 hour



What does the data point at 14:35 tell you?

- A. FortiAnalyzer is dropping logs.
- B. FortiAnalyzer is indexing logs faster than logs are being received.
- C. FortiAnalyzer has temporarily stopped receiving logs so older logs' can be indexed.
- D. The sqlplugind daemon is ahead in indexing by one log.

Answer: B

Explanation:

<https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/47690/insert-rate-vs-receive-rate-wi>

NEW QUESTION 9

What are two of the key features of FortiAnalyzer? (Choose two.)

- A. Centralized log repository
- B. Cloud-based management
- C. Reports
- D. Virtual domains (VDOMs)

Answer: AC

NEW QUESTION 10

Why should you use an NTP server on FortiAnalyzer and all registered devices that log into FortiAnalyzer?

- A. To properly correlate logs
- B. To use real-time forwarding
- C. To resolve host names
- D. To improve DNS response times

Answer: A

Explanation:

[https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/368682/disk-space-allocation](#)

- Synchronize the time on FortiAnalyzer and all registered devices with an NTP server for proper log correlation

NEW QUESTION 10

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 14

<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 23

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 28

Which statements are true of Administrative Domains (ADOMs) in FortiAnalyzer? (Choose two.)

- A. ADOMs are enabled by default.
- B. ADOMs constrain other administrator's access privileges to a subset of devices in the device list.
- C. Once enabled, the Device Manager, FortiView, Event Management, and Reports tab display per ADOM.
- D. All administrators can create ADOMs--not just the admin administrator.

Answer: BC

NEW QUESTION 31

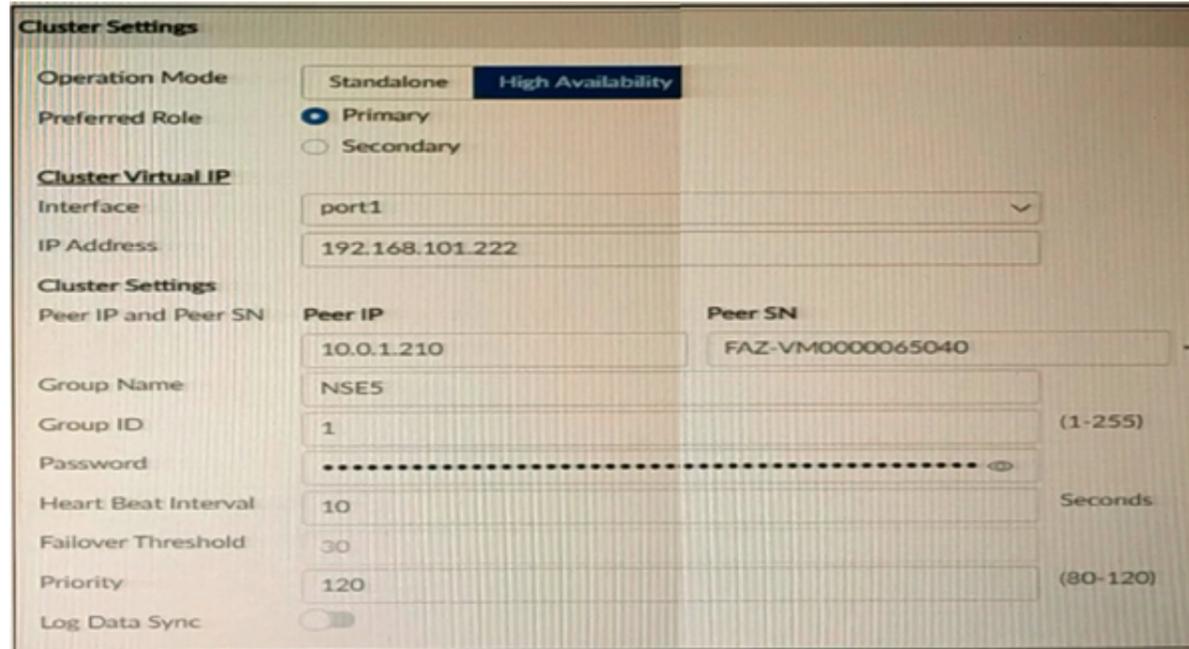
Which two statements are true regarding fabric connectors? (Choose two.)

- A. Configuring fabric connectors to send notification to ITSM platform upon incident creation is more efficient than third-party information from the FortiAnalyzer API.
- B. Fabric connectors allow to save storage costs and improve redundancy.
- C. Storage connector service does not require a separate license to send logs to cloud platform.
- D. Cloud-Out connections allow you to send real-time logs to public cloud accounts like Amazon S3, Azure Blob , and Google Cloud.

Answer: AD

NEW QUESTION 35

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 38

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 40

Which two statements are true regarding high availability (HA) on FortiAnalyzer? (Choose two.)

- A. FortiAnalyzer HA can function without VRR
- B. and VRRP is required only if you have more than two FortiAnalyzer devices in a cluster.
- C. FortiAnalyzer HA supports synchronization of logs as well as some system and configuration settings.
- D. All devices in a FortiAnalyzer HA cluster must run in the same operation mode: analyzer or collector.
- E. FortiAnalyzer HA implementation is supported by many public cloud infrastructures such as AWS, Microsoft Azure, and Google Cloud.

Answer: BC

NEW QUESTION 41

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 45

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 50

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 54

What statements are true regarding the "store and upload" log transfer option between FortiAnalyzer and FortiGate? (Choose three.)

- A. All FortiGates can send logs to FortiAnalyzer using the store and upload option.
- B. Only FortiGate models with hard disks can send logs to FortiAnalyzer using the store and upload option.
- C. Both secure communications methods (SSL and IPsec) allow the store and upload option.
- D. Disk logging is enabled on the FortiGate through the CLI only.
- E. Disk logging is enabled by default on the FortiGate.

Answer: BCD

NEW QUESTION 58

What is required to authorize a FortiGate on FortiAnalyzer using Fabric authorization?

- A. A FortiGate ADOM
- B. The FortiGate serial number
- C. A pre-shared key
- D. Valid FortiAnalyzer credentials

Answer: C

NEW QUESTION 59

What FortiView tool can you use to automatically build a dataset and chart based on a filtered search result?

- A. Chart Builder
- B. Export to Report Chart
- C. Dataset Library
- D. Custom View

Answer: A

Explanation:

<https://docs.fortinet.com/document/fortianalyzer/6.2.0/cookbook/989203/building-charts-with-chart-builder>

NEW QUESTION 64

How can you configure FortiAnalyzer to permit administrator logins from only specific locations?

- A. Use static routes
- B. Use administrative profiles
- C. Use trusted hosts
- D. Use secure protocols

Answer: C

Explanation:

<https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/186508/trusted-hosts>

NEW QUESTION 69

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 73

Which daemon is responsible for enforcing the log file size?

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

Answer: B

NEW QUESTION 76

An administrator has configured the following settings:

```
config system global
set log-checksum md5-auth end
```

What is the significance of executing this command?

- A. This command records the log file MD5 hash value.
- B. This command records passwords in log files and encrypts them.
- C. This command encrypts log transfer between FortiAnalyzer and other devices.
- D. This command records the log file MD5 hash value and authentication code.

Answer: D

NEW QUESTION 77

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 81

Which two statements are true regarding log fetching on FortiAnalyzer? (Choose two.)

- A. A FortiAnalyzer device can perform either the fetch server or client role, and it can perform two roles at the same time with the same FortiAnalyzer devices at the other end.
- B. Log fetching can be done only on two FortiAnalyzer devices that are running the same firmware version.
- C. Log fetching allows the administrator to fetch analytics logs from another FortiAnalyzer for redundancy.
- D. Log fetching allows the administrator to run queries and reports against historical data by retrieving archived logs from one FortiAnalyzer device and sending them to another FortiAnalyzer device.

Answer: BD

NEW QUESTION 86

If you upgrade your FortiAnalyzer firmware, what report elements can be affected?

- A. Output profiles
- B. Report settings
- C. Report scheduling
- D. Custom datasets

Answer: D

NEW QUESTION 91

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 93

Which statements are true regarding securing communications between FortiAnalyzer and FortiGate with IPsec? (Choose two.)

- A. Must configure the FortiAnalyzer end of the tunnel only--the FortiGate end is auto-negotiated.
- B. Must establish an IPsec tunnel ID and pre-shared key.
- C. IPsec cannot be enabled if SSL is enabled as well.
- D. IPsec is only enabled through the CLI on FortiAnalyzer.

Answer: C

NEW QUESTION 98

What are two advantages of setting up fabric ADOM? (Choose two.)

- A. It can be used for fast data processing and log correlation
- B. It can be used to facilitate communication between devices in same Security Fabric
- C. It can include all Fortinet devices that are part of the same Security Fabric
- D. It can include only FortiGate devices that are part of the same Security Fabric

Answer: AC

Explanation:

<https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/448471/creating-a-security-fabric-a>

NEW QUESTION 99

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 100

An administrator has moved FortiGate A from the root ADOM to ADOM1. Which two statements are true regarding logs? (Choose two.)

- A. Analytics logs will be moved to ADOM1 from the root ADOM automatically.
- B. Archived logs will be moved to ADOM1 from the root ADOM automatically.
- C. Logs will be presented in both ADOMs immediately after the move.
- D. Analytics logs will be moved to ADOM1 from the root ADOM after you rebuild the ADOM1 SQL database.

Answer: BD

NEW QUESTION 105

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 106

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 110

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 114

What can you do on FortiAnalyzer to restrict administrative access from specific locations?

- A. Configure trusted hosts for that administrator.
- B. Enable geo-location services on accessible interface.
- C. Configure two-factor authentication with a remote RADIUS server.
- D. Configure an ADOM for respective location.

Answer: A

NEW QUESTION 116

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 118

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 119

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 120

You are using RAID with a FortiAnalyzer that supports software RAID, and one of the hard disks on FortiAnalyzer has failed. What is the recommended method to replace the disk?

- A. Shut down FortiAnalyzer and then replace the disk
- B. Downgrade your RAID level, replace the disk, and then upgrade your RAID level
- C. Clear all RAID alarms and replace the disk while FortiAnalyzer is still running
- D. Perform a hot swap

Answer: A

Explanation:

supports hot swapping on hardware RAID only, so it is recommended that on FortiAnalyzer devices with software RAID you should shutdown FortiAnalyzer prior to exchanging the hard disk.

<https://community.fortinet.com/t5/FortiAnalyzer/Technical-Note-How-to-swap-Hard-Disk-on-FortiAnalyzer/ta->

NEW QUESTION 123

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 126

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 128

.....

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-7.2 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](#)