NSE5_FAZ-6.2 Q&As

Fortinet NSE 5 - FortiAnalyzer 6.2

Pass Fortinet NSE5_FAZ-6.2 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.certbus.com/nse5_faz-6-2.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Fortinet Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

In the FortiAnalyzer FortiView, source and destination IP addresses from FortiGate devices are not resolving to a hostname.

How can you resolve the source and destination IP addresses, without introducing any additional performance impact to FortiAnalyzer?

A. Resolve IP addresses on a per-ADOM basis to reduce delay on FortiView while IPs resolve

B. Configure # set resolve-ip enable in the system FortiView settings

C. Configure local DNS servers on FortiAnalyzer

D. Resolve IP addresses on FortiGate

Correct Answer: B

Reference: https://forum.fortinet.com/tm.aspx?m=156950

QUESTION 2

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.

Correct Answer: AD

QUESTION 3

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

Correct Answer: BD

QUESTION 4

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

Correct Answer: B

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

QUESTION 5

If you upgrade the FortiAnalyzer firmware, which report element can be affected?

A. Custom datasets

B. Report scheduling

C. Report settings

D. Output profiles

Correct Answer: A

QUESTION 6

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

Correct Answer: D

QUESTION 7

What statements are true regarding FortiAnalyzer \\'s treatment of high availability (HA) dusters? (Choose two)

A. FortiAnalyzer distinguishes different devices by their serial number.

B. FortiAnalyzer receives logs from d devices in a duster.

C. FortiAnalyzer receives bgs only from the primary device in the cluster.

D. FortiAnalyzer only needs to know (he serial number of the primary device in the cluster-it automaticaly discovers the other devices.

Correct Answer: AB

QUESTION 8

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

Correct Answer: B

QUESTION 9

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

Correct Answer: C

Reference: https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/4cb0dce6-dbef-11e9-897700505692583a/FortiAnalyzer-5.6.10-Administration-Guide.pdf (40)

QUESTION 10

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

A. The total disk space is insufficient and you need to add other disk.

B. CPU resources are too high.

C. The ADOM disk quota is set too low based on log rates.

D. Logs in that ADOM are being forwarded in real-time to another FortiAnalyzer device.

Correct Answer: C

QUESTION 11

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

Correct Answer: AC

QUESTION 12

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

Correct Answer: B

Reference: https://help.fortinet.com/fa/faz50hlp/60/6-0-2/Content/FortiAnalyzer_Admin_Guide/3600_FortiView/0200_Using_FortiView/1200_Compromised_hosts_page.htm?TocPath=FortiView%7CUsing%20FortiView%7C_____6

QUESTION 13

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

Correct Answer: AB

Reference: https://kb.fortinet.com/kb/documentLink.do?externalID=FD38567

QUESTION 14

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.

Correct Answer: C

QUESTION 15

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

A. Standalone

B. Manager

C. Analyzer

D. Collector

Correct Answer: CD