NSE5_FAZ-6.0.VCEplus.premium.exam.25q

Number: NSE5_FAZ-6.0
Passing Score: 800
Time Limit: 120 min
File Version: 1.0

NSE5_FAZ-6.0

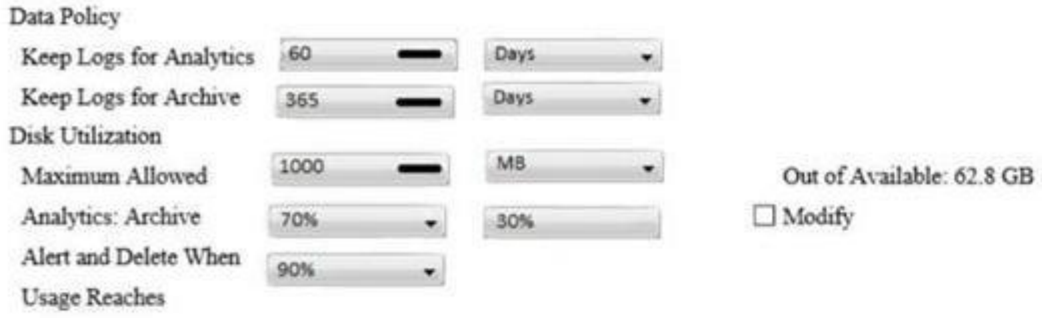
Fortinet NSE 5 - FortiAnalyzer 6.0

Version 1.0

Exam A

QUESTION 1

View the exhibit:



Data Policy

Keep Logs for Analytics 60 Days

Keep Logs for Archive 365 Days

Disk Utilization

Maximum Allowed 1000 MB Out of Available: 62.8 GB

Analytics: Archive 70% 30% □ Modify

Alert and Delete When Usage Reaches 90%

What does the 1000MB maximum for disk utilization refer to?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2

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.

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:

QUESTION 3 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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4 What is the purpose of employing RAID with FortiAnalyzer?

A. To introduce redundancy to your log data
B. To provide data separation between ADOMs
C. To separate analytical and archive data
D. To back up your logs

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6 What is the recommended method of expanding disk space on a FortiAnalyzer VM?

A. From the VM host manager, add an additional virtual disk and use the #execute lvm extend <disk number> command to expand the storage
B. From the VM host manager, expand the size of the existing virtual disk
C. From the VM host manager, expand the size of the existing virtual disk and use the # execute format disk command to reformat the diskD. From the VM host manager, add an additional virtual disk and rebuild your RAID array

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7 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.

Correct Answer: B
Section: (none)

Explanation

Explanation/Reference:

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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9 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

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
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

Correct Answer: B
Section: (none)

Explanation

Explanation/Reference:

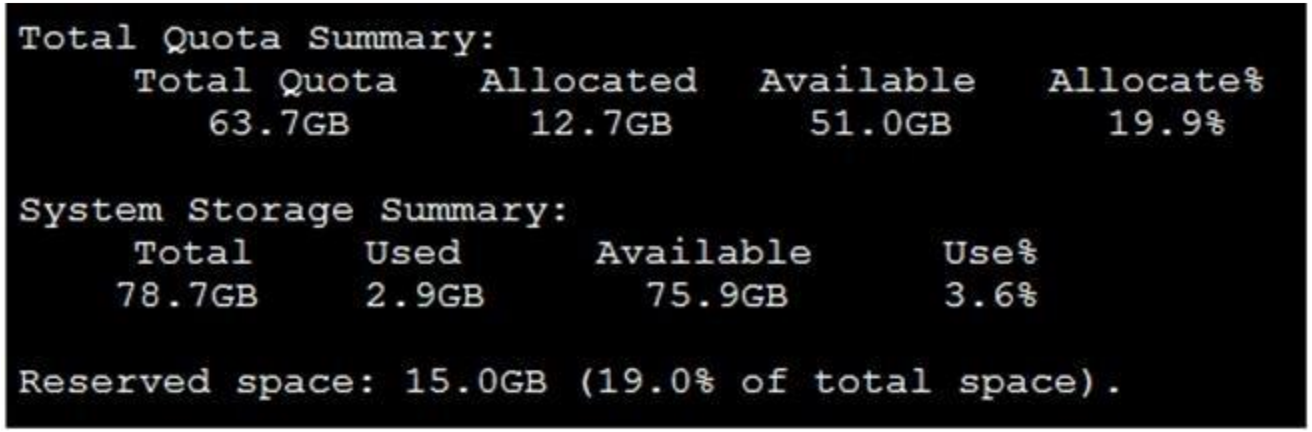
QUESTION 13 What must you configure on FortiAnalyzer to upload a FortiAnalyzer report to a supported external server? (Choose two.)

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

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15 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

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16 If you upgrade your FortiAnalyzer firmware, what report elements can be affected?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17 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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18 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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19 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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20 What FortiGate process caches logs when FortiAnalyzer is not reachable?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21 FortiAnalyzer uses the Optimized Fabric Transfer Protocok (OFTP) over SSL for what purpose?

A. To upload logs to an SFTP server
B. To prevent log modification during backup
C. To send an identical set of logs to a second logging server
D. To encrypt log communication between devices

Correct Answer: D
Section: (none)
Explanation
Explanation/Reference:

QUESTION 22 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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

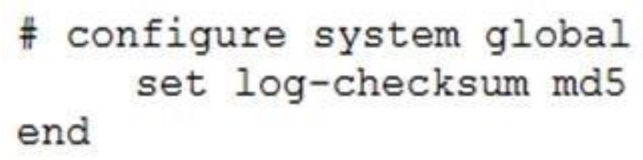
QUESTION 23
Logs are being deleted from one of your ADOMs earlier that the configured setting for archiving in your data policy. What is the most likely problem?

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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
What is the purpose of the following CLI command?



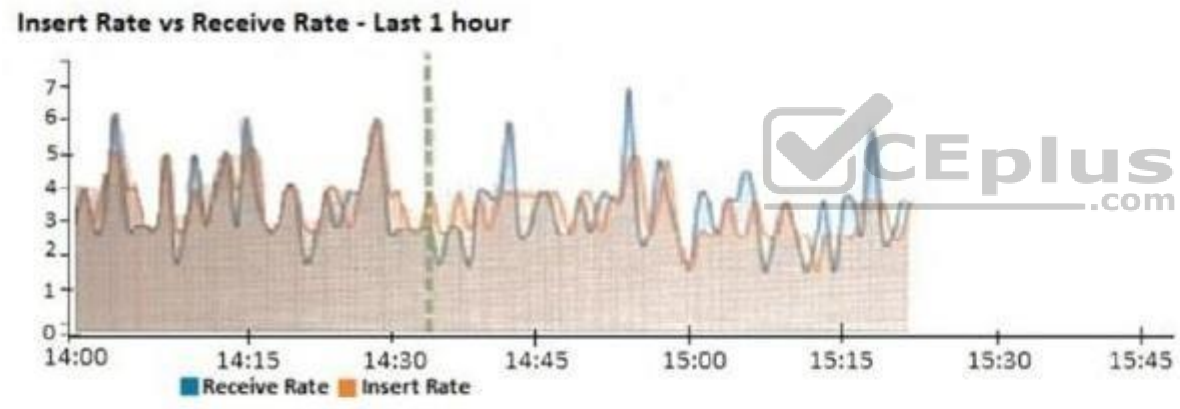
```
# configure system global
     set log-checksum md5
end
```

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
View the exhibit.



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.

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference: