NSE5-FAZ-5.4.exam.14q

Number: NSE5-FAZ-5.4
Passing Score: 800
Time Limit: 120 min
File Version: 1

NSE5_FAZ-5.4

FortiAnalyzer 5.4 Specialist

Exam B

QUESTION 1
FortiAnalyzer uses the Optimized Fabric Transfer Protocol (OFTP) over SSL for what purpose?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
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, add an additional disk and rebuild your RAID array
D. From the VM host manager, expand the size of the existing virtual disk and use the `# execute format disk` command to reformat the disk

Correct Answer: A
Section: (none)

Explanation

Explanation/Reference:
Reference: http://kb.fortinet.com/kb/microsites/microsite.do?cmd=displayKC&docType=kc&externalId=FD40848

QUESTION 3
What FortiGate process caches logs when FortiAnalyzer is not reachable?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
In FortiAnalyzer's FortiView, 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 `# set resolve-ip enable` in the system FortiView settings
B. Resolve IPs on FortiGate
C. Configure local DNS servers on FortiAnalyzer
D. Resolve IPs on a per-ADOM basis to reduce delay on FortiView while IPs resolve

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
What is the purpose of employing RAID with FortiAnalyzer?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
What happens when a log file saved on FortiAnalyzer disks reaches the size specified in the device log settings?

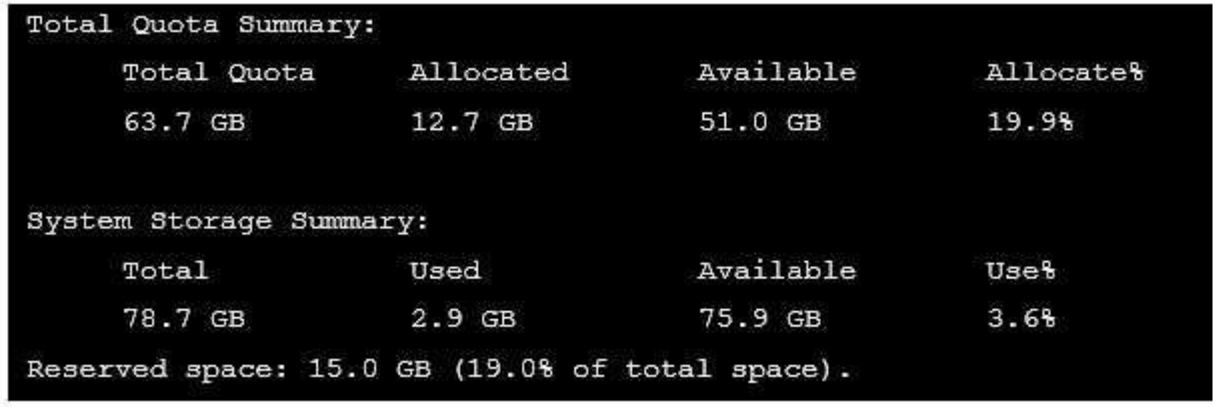
A. The log file is stored as a raw log and is available for analytic support
B. The log file rolls over and is archived
C. The log file is purged from the database
D. The log file is overwritten

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7

View the exhibit.



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

System Storage Summary:
     Total            Used             Available        Use%
     78.7 GB          2.9 GB           75.9 GB          3.6%
Reserved space: 15.0 GB (19.0% of total space).
```

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

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8

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

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

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

QUESTION 9
How are logs forwarded when FortiAnalyzer is using aggregation mode?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
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 an NTP server
D. Use real-time forwarding

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11

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

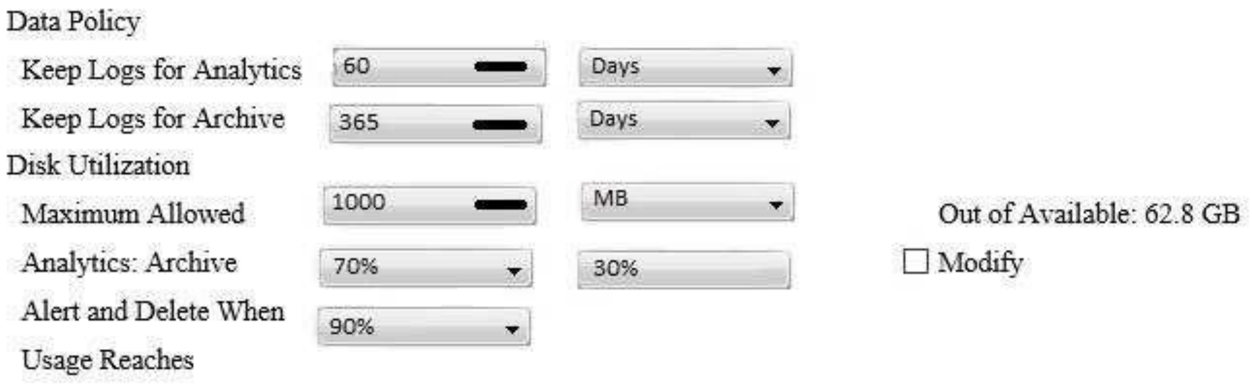
A. Report scheduling
B. Output profile
C. SFTP, FTP, or SCP server
D. Mail server

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12

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 1000 MB maximum for disk utilization refer to?

A. The disk quota for each device in the ADOM

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13

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

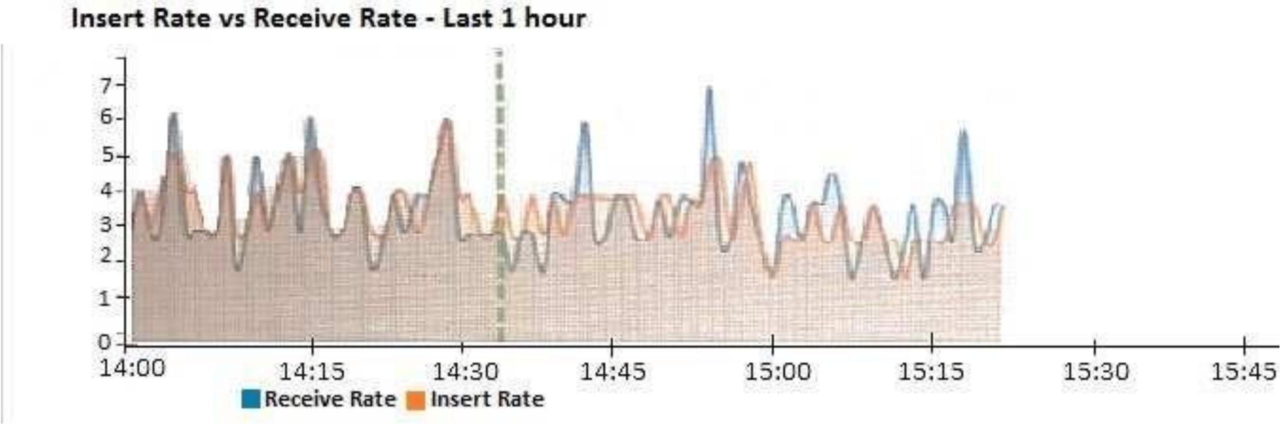
A. To automatically update the hcache when new logs arrive
B. To provide diagnostics on report generation time
C. To reduce the log insert lag rate
D. To reduce report generation time

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14

View the exhibit.



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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference: