NSE5-FAZ-5.4.exam.15q

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

NSE5_FAZ-5.4

FortiAnalyzer 5.4 Specialist

Exam A

QUESTION 1

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

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

Reference: http://help.fortinet.com/fmgr/50hlp/56/5-6-1/FMG-FAZ/1100_Storage/0017_Deleted%20device%20logs.htm

QUESTION 2

How do you restrict an administrator’s access to a subset of your organization’s ADOMs?

A. Set the ADOM mode to **Advanced**
B. Configure trusted hosts
C. Assign the ADOMs to the administrator’s account
D. Assign the default **Super_User** administrator profile

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4

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 5

What FortiGate process caches logs when FortiAnalyzer is not reachable?

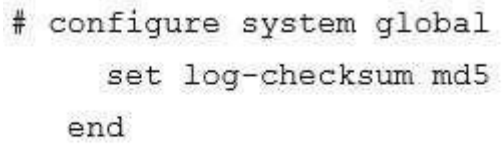
A. oftpd
B. miglogd

C. sqlplugind
D. logfiled

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
What is the purpose of the following CLI command?



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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
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:

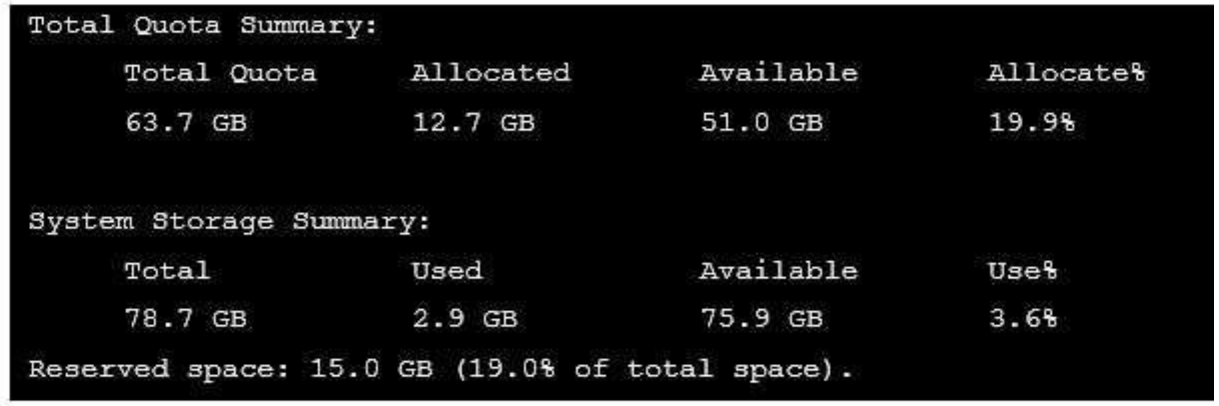
QUESTION 8
What happens when a log file saved on FortiAnalyzer disks reaches the size specified in the device log settings?

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 9
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 10
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 11
If you upgrade your FortiAnalyzer firmware, what report elements can be affected?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
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 13
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:

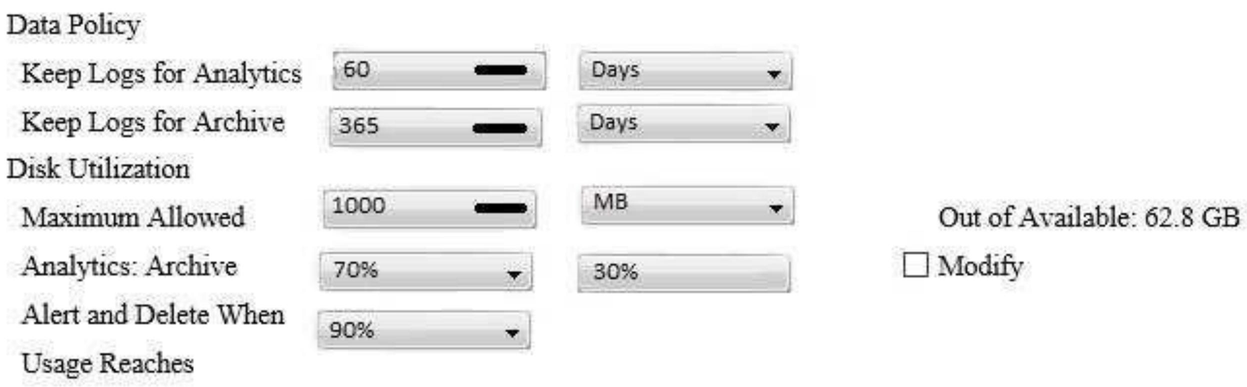
QUESTION 14
What must you configure on FortiAnalyzer to upload a Fortianalyzer report to a supported external server? (Choose two.)

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

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15
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: