NSE5_FAZ-6.2.VCEplus.premium.exam.25q

Number: NSE5_FAZ-6.2
Passing Score: 800
Time Limit: 120 min
File Version: 1.0

NSE5_FAZ-6.2

Fortinet NSE 5 - FortiAnalyzer 6.2

Version 1.0

Exam A

QUESTION 1
Which two of the following must you configure on FortiAnalyzer to email a FortiAnalyzer report externally? (Choose two.)

A. Mail server
B. Output profile
C. SFTP server
D. Report scheduling

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Reference: https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/6d9f8fb5-6cf4-11e9-81a4-00505692583a/FortiAnalyzer-6.0.5-Administration-Guide.pdf (119)

QUESTION 2
Refer to 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. Some space is reserved for system use
B. 3.6% of the system storage is already being used
C. The `logfiled` process is just estimating the total quota
D. The `oftpd` process has not archived the logs yet

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
For which two purposes would you use the command `set log checksum`? (Choose two.)

A. To help protect against man-in-the-middle attacks during log upload from FortiAnalyzer to an SFTP server B.
To prevent log modification or tampering
C. To encrypt log communications
D. To send an identical set of logs to a second logging server

Correct Answer: AB
Section: (none)
Explanation

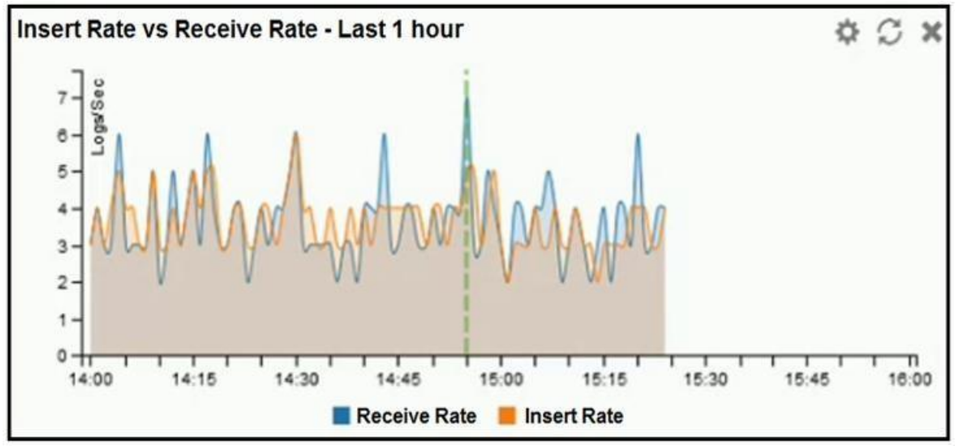
Explanation/Reference:
Explanation:

To prevent the log in the store from being modified, you can add a log checksum by using the config system global command. When the log is split, archived, and the log is uploaded (if the feature is enabled), you can configure the FortiAnalyzer to log the log file hash value, timestamp, and authentication code. This can help defend against man-in-the-middle attacks when uploading log transmission data from the FortiAnalyzer to the SFTP server.

QUESTION 4

Refer to the exhibit.

What does the data point at 14:55 tell you?



A. The received rate is almost at its maximum for this device
B. The sqlplugind daemon is behind in log indexing by two logs
C. Logs are being dropped
D. Raw logs are reaching FortiAnalyzer faster than they can be indexed

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.fortinetguru.com/2016/04/system-settings/6/

QUESTION 6 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
Section: (none)
Explanation

Explanation/Reference:
Reference: https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/4cb0dce6-dbef-11e9-8977-00505692583a/FortiAnalyzer-5.6.10-Administration-Guide.pdf (40)

QUESTION 7
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
Section: (none)
Explanation

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

QUESTION 8
You have recently grouped multiple FortiGate devices into a single ADOM. **System Settings** > **Storage Info** shows the quota used. What does the disk quota refer to?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9 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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
You need to upgrade your FortiAnalyzer firmware.

What happens to the logs being sent to FortiAnalyzer from FortiGate during the time FortiAnalyzer is temporarily unavailable?

A. FortiAnalyzer uses log fetching to retrieve the logs when back online
B. FortiGate uses the `miglogd` process to cache the logs
C. The `logfiled` process stores logs in offline mode
D. Logs are dropped

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
After you have moved a registered logging device out of one ADOM and into a new ADOM, what is the purpose of running the following CLI command?

```
execute sql-local rebuild-adom <new-ADOM-name>
```

A. To reset the disk quota enforcement to default
B. To remove the analytics logs of the device from the old database
C. To migrate the archive logs to the new ADOM
D. To populate the new ADOM with analytical logs for the moved device, so you can run reports

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.fortinet.com/document/fortianalyzer/6.0.2/cli-reference/551596/sql-local

QUESTION 12
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.fortinetguru.com/2020/06/raid-management-fortianalyzer-fortios-6-2-3-2/

QUESTION 13 Which FortiAnalyzer feature allows you to retrieve the archived logs matching a specific timeframe, from another FortiAnalyzer device?

A. Log fetching
B. Indicators of compromise
C. Log forwarding in aggregation mode
D. Log upload

Correct Answer: A

Section: (none)
Explanation
Explanation/Reference:

QUESTION 14 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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15
FortiAnalyzer reports are dropping analytical data from 15 days ago, even though the data policy setting for analytics logs is 60 days.

What is the most likely problem?

A. Quota enforcement is acting on analytical data before a report is complete
B. Logs are rolling before the report is run
C. CPU resources are too high
D. Disk utilization for archive logs is set for 15 days

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://forum.fortinet.com/tm.aspx?m=138806

QUESTION 16
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
Section: (none)
Explanation

Explanation/Reference:
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 17 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 reduces report generation time
C. It provides diagnostics on report generation time

D. It reduces the log insert lag rate
Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.fortinet.com/document/fortianalyzer/6.0.0/administration-guide/282280/enabling-auto-cache

QUESTION 18 In order for FortiAnalyzer to collect logs from a FortiGate device, which two configurations are required? (Choose two.)

A. FortiGate must be registered with FortiAnalyzer
B. Remote logging must be enabled on FortiGate
C. ADOMs must be enabled
D. Log encryption must be enabled

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
Reference: https://kb.fortinet.com/kb/documentLink.do?externalID=FD41272

QUESTION 19
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
Section: (none)
Explanation

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

QUESTION 20 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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21 Which clause is considered mandatory in SELECT statements used by the FortiAnalyzer to generate reports?

A. FROM
B. LIMIT

C. WHERE
D. ORDER BY
Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://kb.fortinet.com/kb/documentLink.do?externalID=FD48500

QUESTION 22 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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23 Logs are being deleted from one of the ADOMs earlier than the configured setting for archiving in the data policy.

What is the most likely problem?

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

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 24 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

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.fortinet.com/document/fortianalyzer/6.0.5/administration-guide/929977/disk-space-allocation

QUESTION 25 What happens when a log file saved on FortiAnalyzer disks reaches the size specified in the device log settings?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/6d9f8fb5-6cf4-11e9-81a4-00505692583a/FortiAnalyzer-6.0.5-Administration-Guide.pdf