- **Vendor:** Fortinet
- **Exam Code:** NSE5_FAZ-7.0
- **Exam Name:** Fortinet NSE 5 - FortiAnalyzer 7.0
- **New Updated Questions from Braindump2go (Updated in October/2022)**

QUESTION 71
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?

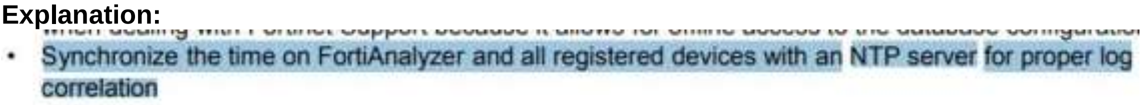
A. The maximum disk utilization for each device in the ADOM
B. The maximum disk utilization for the FortiAnalyzer model
C. The maximum disk utilization for the ADOM type
D. The maximum disk utilization for all devices in the ADOM

Answer: D

QUESTION 72
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

Answer: A
Explanation:



when dealing with Fortinet Support because it allows for offline access to the database configuratio

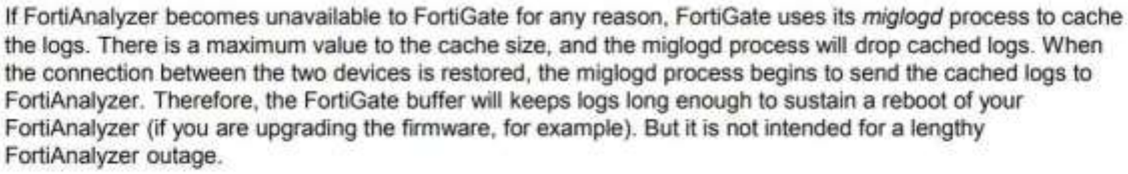
- Synchronize the time on FortiAnalyzer and all registered devices with an NTP server for proper log correlation

QUESTION 73
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

Answer: B

Explanation:



If FortiAnalyzer becomes unavailable to FortiGate for any reason, FortiGate uses its *miglogd* process to cache the logs. There is a maximum value to the cache size, and the miglogd process will drop cached logs. When the connection between the two devices is restored, the miglogd process begins to send the cached logs to FortiAnalyzer. Therefore, the FortiGate buffer will keeps logs long enough to sustain a reboot of your FortiAnalyzer (if you are upgrading the firmware, for example). But it is not intended for a lengthy FortiAnalyzer outage.

QUESTION 74

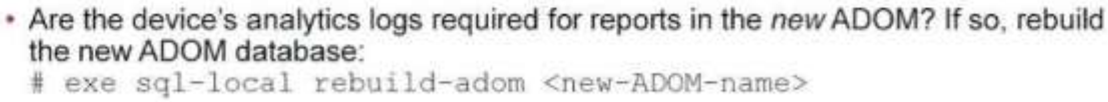
After you have moved a registered logging device out of one ADOM and into a new ADOM, what is the purpose of running the following CLI command?

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

Answer: D

Explanation:



- Are the device's analytics logs required for reports in the *new* ADOM? If so, rebuild the new ADOM database:

```
# exe sql-local rebuild-adom <new-ADOM-name>
```

QUESTION 75

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

Answer: D

Explanation:

If a hard disk on a FortiAnalyzer unit fails, it must be replaced. On FortiAnalyzer devices that support hardware RAID, the hard disk can be replaced while the unit is still running-known as hot swapping. On FortiAnalyzer units with software RAID, the device must be shutdown prior to exchanging the hard disk.

QUESTION 76

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

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

Answer: B

Explanation:

https://docs.fortinet.com/document/fortianalyzer/6.2.5/upgrade-guide/669300/checking-reports

QUESTION 77

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

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

QUESTION 78
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

Answer: B

QUESTION 79
What is included in the disk quota for each ADOM on the FortiAnalyzer?

A. SQL tables and archive files
B. Raw logs and archive files
C. Archive logs and analytics logs
D. Raw logs, archive files, SQL database tables

Answer: D

QUESTION 80
When generating reports on FortiAnalyzer, macros can be used to include additional data. Which two statements about macros are true? (Choose two.)

A. Macros are abbreviated dataset queries
B. Macros do not need to be associated with a chart
C. Macros are supported in FortiGate ADOMs only
D. Macros cannot be customized

Answer: AB

QUESTION 81
When you move a FortiGate device from one ADOM to a new ADOM, what is the purpose of rebuilding the new ADOM database?

A. To migrate the archive logs to the new ADOM
B. To reset the disk quota enforcement to default
C. To remove the device's analytics logs from the old ADOM

D. To run reports on the device's analytics logs in the new ADOM

Answer: D

QUESTION 82
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

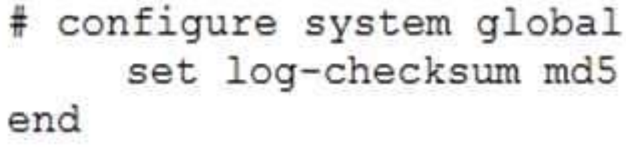
Answer: C
Explanation:
https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/186508/trusted-hosts

QUESTION 83
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.

Answer: C

QUESTION 84
What is the purpose of the following CLI command?

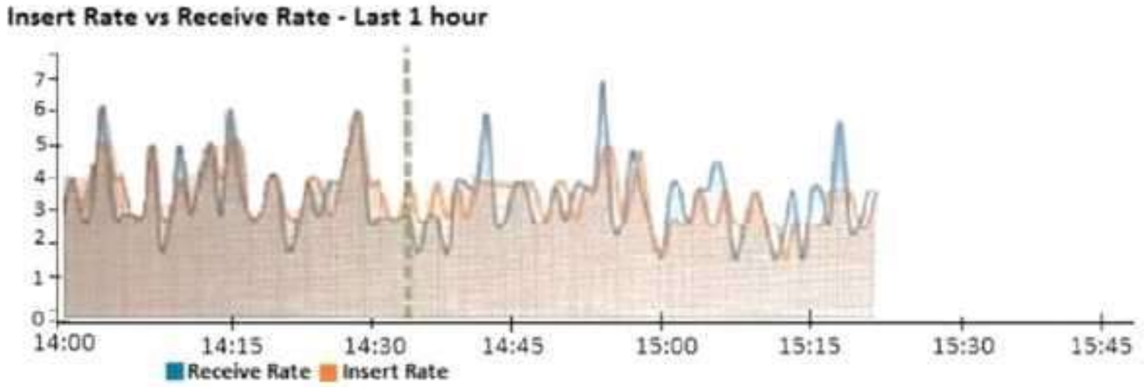


```
# configure system global
      set log-checksum md5
end
```

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

Answer: A
Explanation:
https://docs2.fortinet.com/document/fortianalyzer/6.0.3/cli-reference/849211/global

QUESTION 85
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.

Answer: B
Explanation:
https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/47690/insert-rate-vs-receive-rate-widget

QUESTION 86
What remote authentication servers can you configure to validate your FortiAnalyzer administrator logons? (Choose three)

A. RADIUS
B. Local
C. LDAP
D. PKI
E. TACACS+

Answer: ACE

QUESTION 87
What statements are true regarding disk log quota? (Choose two)

A. The FortiAnalyzer stops logging once the disk log quota is met.
B. The FortiAnalyzer automatically sets the disk log quota based on the device.
C. The FortiAnalyzer can overwrite the oldest logs or stop logging once the disk log quota is met.
D. The FortiAnalyzer disk log quota is configurable, but has a minimum o 100mb a maximum based on the reserved system space.

Answer: CD

QUESTION 88
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.

Answer: AB

QUESTION 89
What are the operating modes of FortiAnalyzer? (Choose two)

A. Standalone
B. Manager
C. Analyzer
D. Collector

Answer: CD

QUESTION 90
Which two external servers can you configure to validate administrator logins? (Choose two.)

A. Syslog
B. LDAP
C. RADIUS
D. Only locally by FortiAnalyzer

Answer: BC

QUESTION 91
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

Answer: C
Explanation:
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 92
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

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

QUESTION 93
When you perform a system backup, what does the backup configuration contain? (Choose two.)

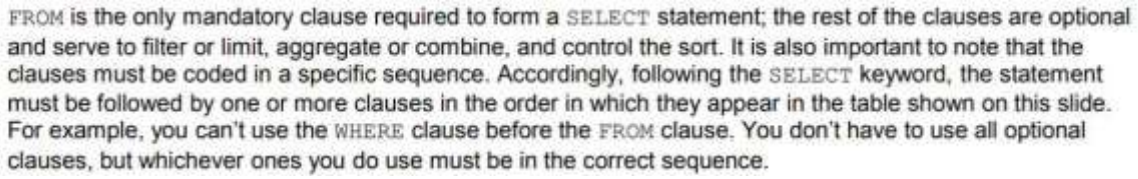
A. Generated reports
B. Device list
C. Authorized devices logs
D. System information

Answer: BD
Explanation:
https://help.fortinet.com/fa/cli-olh/5-6-5/Content/Document/1400_execute/backup.htm

QUESTION 94
Which clause is considered mandatory in SELECT statements used by the FortiAnalyzer to generate reports?

A. FROM
B. LIMIT
C. WHERE
D. ORDER BY

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



FROM is the only mandatory clause required to form a SELECT statement; the rest of the clauses are optional and serve to filter or limit, aggregate or combine, and control the sort. It is also important to note that the clauses must be coded in a specific sequence. Accordingly, following the SELECT keyword, the statement must be followed by one or more clauses in the order in which they appear in the table shown on this slide. For example, you can't use the WHERE clause before the FROM clause. You don't have to use all optional clauses, but whichever ones you do use must be in the correct sequence.

QUESTION 95
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

Answer: C
Explanation:
Reference: https://docs2.fortinet.com/document/fortianalyzer/6.0.4/administration-guide/148744/creating-datasets