1.
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. Configure local DNS servers on FortiAnalyzer
B. Configure # set resolve-ip enable in the system FortiView settings.
C. Resolve IP addresses on FortiGate.
D. Resolve IP addresses on a per-ADOM basis to reduce delay on FortiView while IPs resolve.

Answer: C
Reference:
https://packetplant.com/fortigate-and-fortianalyzer-resolve-source-and-destination-ip/

2.
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. Take no action if the RAID level supports a failed disk.
B. Replace the disk and rebuild the RAID manually.
C. Shut down FortiAnalyzer and replace the disk.
D. Hot swap the disk.

Answer: C
Reference:
https://kb.fortinet.com/kb/documentLink.do?externalID=FD46446#:~:text=On%20FortiAnalyzer%2FFortiManager%20devices%20that,to%20exchanging%20the%20hard%20disk.

3.
How are logs forwarded when FortiAnalyzer is configured to use 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 as they are received, and content files are uploaded at a scheduled time.
D. Logs are forwarded as they are received.

Answer: A
Reference:
https://docs.fortinet.com/document/fortianalyzer/6.2.0/administration-guide/420493/modes

4.
For which two SAML roles can the FortiAnalyzer be configured? (Choose two)

A. Service provider
B. Principal
C. Identity provider
D. Identity collector

Answer: AC

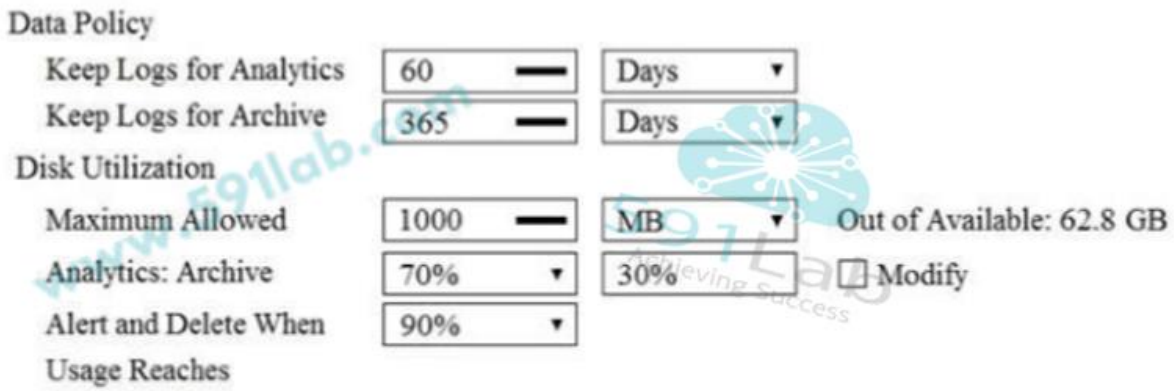
Reference:
https://docs.fortinet.com/document/fortianalyzer/6.2.0/administration-guide/981386/saml-admin-authentication

5.
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. ADOMs must be enabled.
C. Remote logging must be enabled on FortiGate
D. Log encryption must be enabled.

Answer: AC

6.
Refer to the exhibit:



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

Answer: B

Reference:
https://docs.fortinet.com/document/fortianalyzer/6.2.0/administration-guide/743670/configuring-log-storage-policy

7.
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

Answer: D
Reference:
https://docs.fortinet.com/document/fortianalyzer/6.2.0/administration-guide/651442/fetcher-management

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

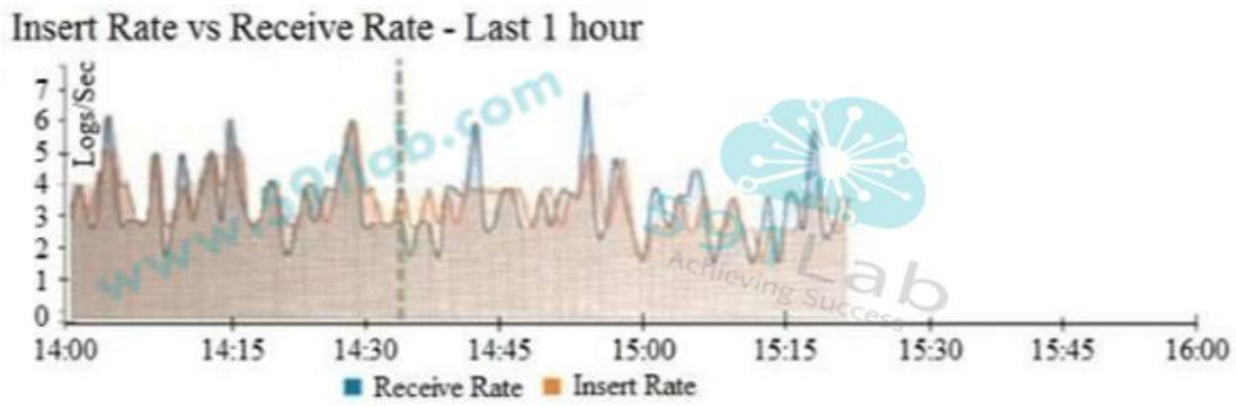
Answer: C
Reference:
https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/355632/log-browse

9.
Which two constraints can impact the amount of reserved disk space required by FortiAnalyzer? (Choose two)

A. RAID level
B. License type
C. Disk size
D. Total quota

Answer: AD
Reference:
https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/368682/disk-space-allocation

10.
Refer to 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 FortiLog daemon is ahead in indexing by one log.

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

11.
Which two methods can you use to send event notifications when an event occurs that matches a configured event handler? (Choose two.)

A. SNMP
B. SMS
C. IM
D. Email

Answer: AD

12.
Which FortiGate process caches logs when FortiAnalyzer is not reachable?

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

Answer: B
Reference:
https://forum.fortinet.com/tm.aspx?m=143106

13.
What is the purpose of a predefined template on the FortiAnalyzer?

A. It specifies report settings which contains time period, device selection, and schedule.
B. It contains predefined data to generate mock reports.
C. It specifies the report layout which contains predefined texts, charts, and macros.
D. It can be edited and modified as required.

Answer: C
Reference:
https://help.fortinet.com/fa/faz50hlp/56/5-6-2/FMG-FAZ/2300_Reports/0010_Predefined_reports.htm

14.
When you perform a system backup, what does the backup configuration contain? (Choose two.)

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

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

15.
If you upgrade the FortiAnalyzer firmware, which report element can be affected?

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

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

16.
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 writing to all of its hard drives to make the array fault tolerant.
B. FortiAnalyzer is functioning normally.
C. FortiAnalyzer is writing data to a newly added hard drive to restore it to an optimal state.
D. FortiAnalyzer is ensuring that the party data of a redundant drive is valid

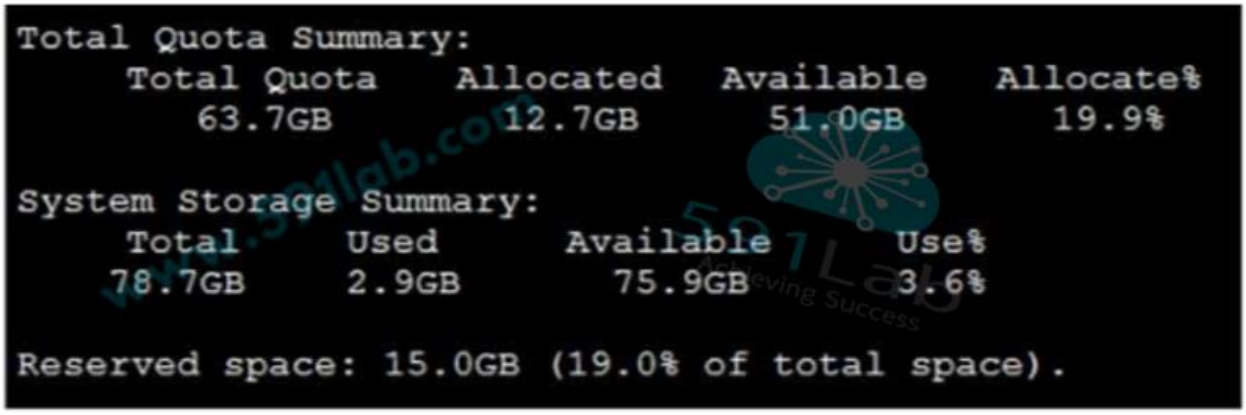
Answer: A
Reference:
https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/120929/monitoring-raid-status

17.
What are two advantages of setting up fabric ADOM? (Choose two.)

A. It can include all Fortinet devices that are part of the same Security Fabric.
B. It can include only FortiGate devices that are part of the same Security Fabric.
C. It can be used to facilitate communication between devices in same Security Fabric.
D. It can be used for fast data processing and log correlation.

Answer: AD
Reference:
https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/448471/creating-a-security-fabric-adom

18.
Refer to the exhibit.



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

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

Answer: C
Reference:
https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/368682/disk-space-allocation

19.
What is the main purpose of using an NTP server on FortiAnalyzer and all of its registered devices?

A. Host name resolution
B. Log collection
C. Real-time forwarding
D. Log correlation

Answer: D

Explanation:

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

20.

You have 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 analytics logs to the new ADOM.
C. FortiAnalyzer removes analytics logs from the old ADOM.
D. FortiAnalyzer migrates archive logs to the new ADOM.

Answer: B

Reference:

https://kb.fortinet.com/kb/documentLink.do?externalID=FD40383

21.

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 provides diagnostics on report generation time.
C. It reduces the log insert lag rate.
D. It reduces report generation time.

Answer: AD

Reference:

https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/384416/how-auto-cache-works

https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/86926/enabling-auto-cache

22.

How does FortiAnalyzer retrieve specific log data from the database?

A. SQL SELECT statement
B. SQL GET statement
C. SQL EXTRACT statement
D. SQL FROM statement

Answer: D

Reference:

https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/137bb60e-ff37-11e8-8524-f8bc1258b856/fortianalyzer-fortigate-sql-technote-40-mr2.pdf

23.
FortiAnalyzer uses the Optimized Fabric Transfer Protocol (OFTP) over SSL for which purpose?

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

Answer: D

Explanation:

OFTPS is the default setting for securing communications between FortiGate and FortiAnalyzer.

24.
Which two statements about log forwarding are true? (Choose two)

A. Forwarded logs cannot be filtered to match specific criteria.
B. The client retains a local copy of the logs after forwarding.
C. Logs are forwarded in real-time only.
D. You can use aggregation mode only with another FortiAnalyzer.

Answer: BD
Reference:
https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/420493/modes
https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/621804/log-forwarding

25.
Consider the CLI command:

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

What is the purpose of the command?

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

Answer: C
Reference:
https://docs.fortinet.com/document/fortianalyzer/6.2.5/cli-reference/849211/global

26.
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

Answer: A

Reference:
https://en.wikipedia.org/wiki/RAID#:~:text=RAID%20(%22Redundant%20Array%20of%20Inexpensive,%2C%20performance%20improvement%2C%20or%20both.

27.
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 disk
D. From the VM host manager, add an additional disk and rebuild your RAID array

Answer: A
Reference:
https://kb.fortinet.com/kb/documentLink.do?externalID=FD40848

28.
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

Answer: B
Reference:
https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/717578/assigning-administrators-to-an-adom

29.
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

Answer: A
Reference:
https://docs.fortinet.com/document/fortianalyzer/6.2.5/cli-reference/395556/test#test_application

30.
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

Answer: A
Reference:
https://docs.fortinet.com/document/fortianalyzer/6.2.0/cookbook/989203/building-charts-with-chart-builder

31.
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

Answer: BC
Reference:
https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/108255/creating-output-profiles

32.
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. 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
Reference:
https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/87802/automatic-deletion

33.
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

Answer: D

Explanation:

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

34.

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

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

35.

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

Answer: A

Reference:
https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/747268/configuring-wildcard-admin-accounts

36.

For which two purposes would you use the command act log checkout? (Choose two)

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

Answer: AD

37.

What is the purpose of a dataset query in FortiAnalyzer?

A. It extracts the database schema.
B. It injects log data into the database.
C. It sorts log data into tables.
D. It retrieves log data from the database.

Answer: D

Explanation:

database, it relies on a dataset query to extract that log data. A dataset is a specific SQL `SELECT` query—a read-only statement that retrieves data from the database.

38.
Which two of the following must you configure on FortiAnalyzer to email a FortiAnalyzer report externally? (Choose two:)

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

Answer: AD

Explanation:

In order to use any of these external storage methods, you must first set up the back end. This includes configuring a mail server (for emailed reports only) and an output profile. If ADOMs are enabled, each ADOM has its own output profiles.

39.
Which log type does the FortiAnalyzer indicators of compromise feature use to identity infected hosts?

A. Application control logs
B. Antivirus logs
C. Web filter logs
D. IPS logs

Answer: C

Explanation:

- Web Filter policies on FortiGate(s) that send traffic to FortiAnalyzer
  - Breach detection or analytic engine runs against the FortiGate web filter logs to identify breaches related to web traffic

40.
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 the FortiAnalyzer model.
B. The maximum disk utilization for each device in the ADOM.
C. The maximum disk utilization for the ADOM type.
D. The maximum disk utilization for all devices in the ADOM.

Answer: D

Explanation:

Once you create an ADOM, you can set the disk quota. This quota is assigned to the ADOM, and not the individual devices added to it. By Default, the **Maximum Allowed** disk quota is set to 50 GB.

41.
Which clause is considered mandatory in SELECT statements used by the FortiAnalyzer to generate reports?

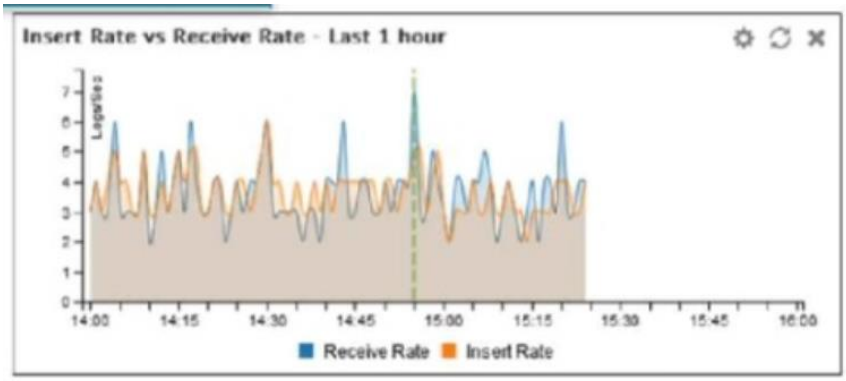
A. FROM
B. LIMIT
C. WHERE
D. ORDER BY

Answer: A

Explanation:

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.

42.



Refer to the exhibit.
What does the data point at 14:55 tell you?

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

Answer: A

Explanation:

Insert Rate vs. Receive Rate is a graph that shows the rate at which raw logs reach the FortiAnalyzer (received rate) and the rate at which they are indexed (insert rate) by the SQL database and the sqlplugind daemon.

43.
FortiAnalyzer reports are dropping analytical data from 16 days ago, even though the data policy setting for analytics logs is 60 days.
What is the most likely problem?

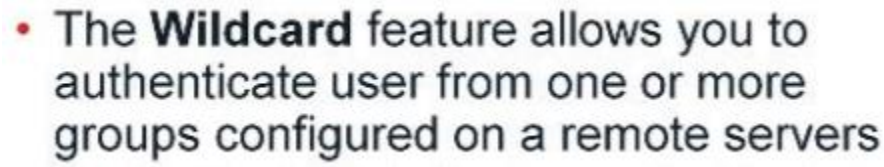
A. Quota enforcement is acting on analytical data before a report is complete.
B. CPU resources are too high.
C. Disk utilization for archive logs is set for 15 days.
D. Logs are rolling before the report is run.

Answer: D

44.
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 trusted host profile that restricts access to the LDAP group
B. An administrator group.
C. A remote LDAP server.
D. A local wildcard administrator account.

Answer: BC
Explanation:



45.
You need to upgrade your FortiAnalyzer firmware.
What happens to the logs being sent to FortiAnalyzer from FortiGate during the lime FortiAnalyzer is temporarily unavailable?

A. FortiAnalyzer uses log fetching to relieve 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.

46.
After you have moved 3 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 remove the analytics logs of the device from the old database.
B. To migrate the archive logs to the new ADOM.
C. To populate the new ADOM with analytical logs for the moved device, so you can run reports.
D. To reset the disk quota enforcement to default.

Answer: C

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>`

47.
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. Clear all RAID alarms and replace the disk while FortiAnalyzer is still running.
B. Perform a hot swap.
C. Downgrade your RAID level, replace the disk, and then upgrade your RAID level.
D. Shut down FortiAnalyzer and then replace the disk.

Answer: D

Explanation:

supports hot swapping on hardware RAID only, so it is recommended that on FortiAnalyzer devices with *software* RAID you should shutdown FortiAnalyzer prior to exchanging the hard disk.

48.
Why should you use an NTP server on FortiAnalyzer and all registered devices that log into FortiAnalyzer?

A. To resolve host names
B. To use real-time forwarding
C. To properly correlate logs
D. To improve DNS response times

Answer: C

Explanation:

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