NSE5 FORTI ANALYZER 6.4 DUMPS
Real exam

Fortinet NSE 5 FortiAnalyzer 6.4 NSE5_FAZ

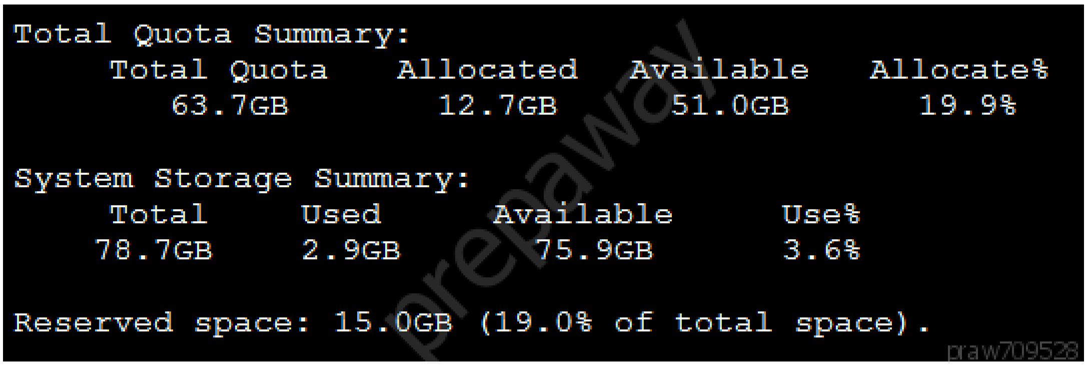
Question #1

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

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

Question #3

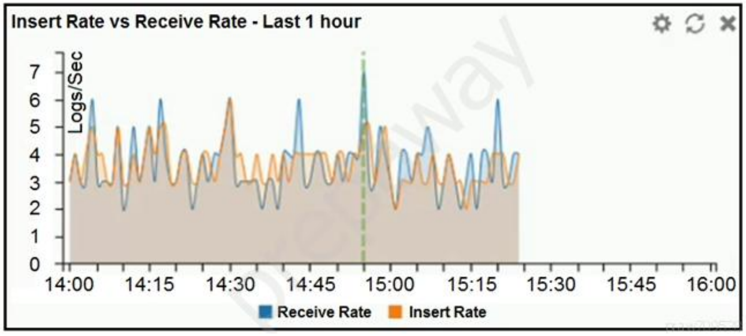
For which two purposes would you use the command set log checksum? (Choose two.)

- A. To help protect against man-in-the-middle attacks during log 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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Question #26

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

C & D

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

Question #27

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

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

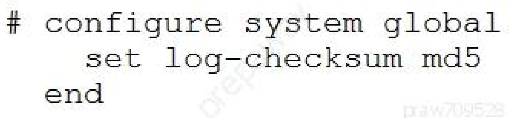
Question #28

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 migrates analytics logs to the new ADOM.
- B. FortiAnalyzer removes analytics logs from the old ADOM.
- C. FortiAnalyzer resets the disk quota of the new ADOM to default.
- D. FortiAnalyzer migrates archive logs to the new ADOM.

Question #29

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 add the MD5 hash value and authentication code
- C. To add a log file checksum
- D. To encrypt log communications

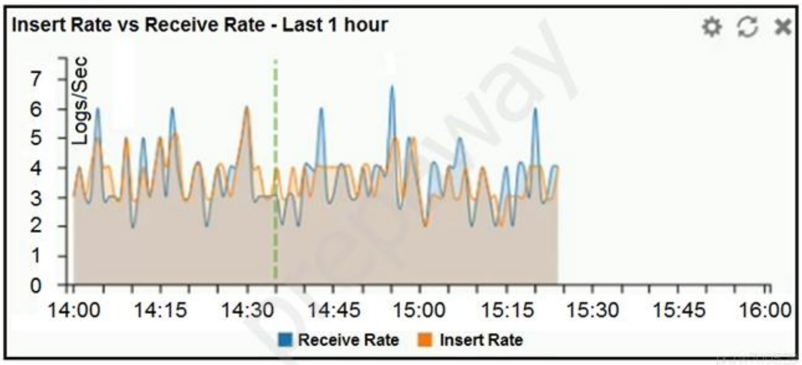
Question #30

How are logs forwarded when FortiAnalyzer is configured to use aggregation mode?

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

Question #31

Refer to the exhibit.



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

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

Question #32

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

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

Question #33

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 encrypt log communication between devices
- C. To upload logs to an SFTP server

- D. To prevent log modification during backup

Question #34

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

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

Question #35

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

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

Question #36

How does FortiAnalyzer retrieve specific log data from the database?

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

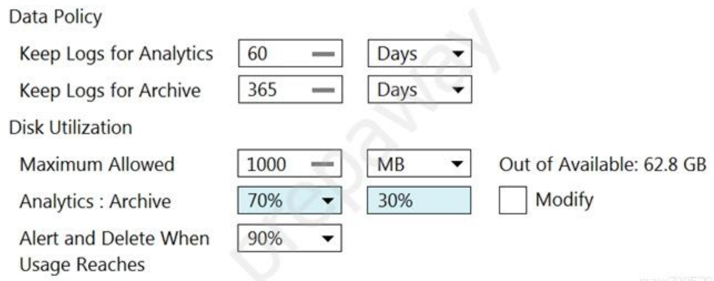
Question #37

Which FortiGate process caches logs when FortiAnalyzer is not reachable?

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

Question #38

Refer to 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 1000MB maximum for disk utilization refer to?

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

Question #39

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

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

Question #40

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

Question #41

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 virtual disk and rebuild your RAID array

Question #42

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

Question #43

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

Question #44

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

Question #45

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

Question #46

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

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

Question #47

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

Question #48

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

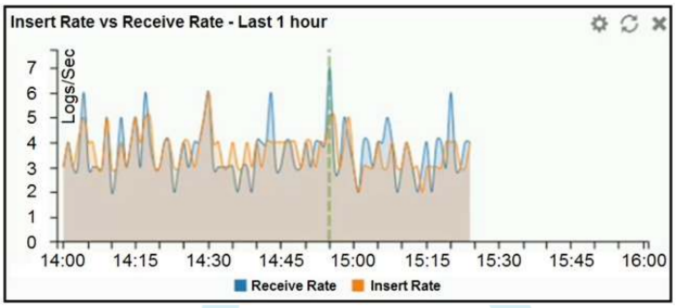
Question #49

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

Question #50

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

Question #51

What are event handlers?

a) Threats identified by FortiGuard
b) Specific matched conditions in the raw logs
c) Alert notifications
d) SNMP traps

Question #52

Which two FortiAnalyzer features allow you to automatically build a dataset and chart based on a filtered search result?
(Choose two.)

a) Export to Report Chart (FortiView)
b) Custom View
c) Dataset Library
d) Chart Builder

Question #53

What is the main purpose of deploying RAID with FortiAnalyzer?

a) To back up your logs
b) To make an identical copy of log data on two separate physical drives
c) To provide redundancy of your log data
d) To store data in chunks across multiple drives

Question #54

It is a best practice to upload FortiAnalyzer local logs to a remote server. Which three remote servers are supported for the upload?
(Choose three.)

a) SFTP
b) SCP
c) FTP
d) UDP
e) TCP

Question #55

Which database language does FortiAnalyzer support for the purposes of logging and reporting?

a) LDAP
b) SSH
c) SQL
d) XML

Question #56

What should you always do after erasing the FortiAnalyzer configuration on flash?

a) Run the execute reset all-settings command
b) Run the execute format disk command
c) Run the execute reboot command
d) Perform a system backup

Question #57

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

Question #58

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

Question #59

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

Question #60

Which two external servers can you configure to validate administrator logins?

(Choose two.)
a) Syslog
b) LDAP
c) RADIUS
d) Only locally by FortiAnalyzer

Question #61

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 migrates analytics logs to the new ADOM.
b) FortiAnalyzer removes analytics logs from the old ADOM.
c) FortiAnalyzer resets the disk quota of the new ADOM to default.
d) FortiAnalyzer migrates archive logs to the new ADOM.

NEW QUESTIONS - EXAM 29.10.2021

Question #1

What are **analytics** logs on FortiAnalyzer?

A. Logs that are indexed and stored in the SQL
B. Raw logs that are compressed and saved to a log file
C. Logs that roll over when the log file reaches a specific size
D. Log type **Traffic** logs

Question #2

Which two statements are true regarding **Initial Logs Sync** and **Log Data Sync** for HA on FortiAnalyzer? (Choose two)

B and D correct answer

A. By default, Log Data Sync is disabled on all backup devices
B. With Initial Logs Sync when you add a unit to an HA cluster the primary device synchronizes its logs with the backup
C. When Log Data Sync is tuned on the backup device will reboot and then rebuild the log database with the synchronized logs
D. Log Data Sync provides real-time log synchronization to all backup devices

Question #3

Refer to de exhibit

What is the purpose of using the **Chart Builder** feauture on FortiAnalyzer?

A. This feature allows you to build a chart under FortiView
B. In Log View this feature allows you to build a chart automatically based on the top 100 log entries
C. In Log View this feature allows you to build a dataset and chart automatically, based on the filtered search results
D. You can add charts directly to generated reports using this feature

Question #4

What is the purpose of a dataset query in FortiAnalyzer?

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

Question #5

Refer to the exhibit

The exhibit shows “remoteservergroup” is an authentication server group with LDAP and RADIUS servers. Which two statements express the significate of enabling **Match all users on remote server** when configuring a new administrator? (Choose two.)

A. Administrators can log in to FortiAnalyzer using their credentials on remote servers LDAP and RADIUS
B. It allows administrator to use two-factor authentication
C. It creates a wildcard administrator using LDAP and RADIUS servers
D. User **remoteadmin** from LDAP and RADIUS servers will be able to log in to FortiAnalyzer at any time

Question #6

What two things should an administrator do to view Compromised Hosts on FortiAnalyzer? (Choose two)

A. Subscribe FortiAnalyzer to FortiGuard to keep its local threat database up-to-date
B. Enable device detection on an interface on the FortiGate devices that are connected to the FortiAnalyzer device
C. Make sure all endpoints are reachable by FortiAnalyzer

D. Enable web filtering in firewall policies on FortiGate devices, and make sure these logs are sent to FortiAnalyzer

Question #7

Which two statements express the advantages of grouping similar reports? (Choose two)

A. Reduce the number of hcache tables and improve auto-hcache completion time
B. Conserve disk space on FortiAnalyzer by grouping multiple similar reports
C. Provides a better summary of reports
D. Improve report completion time

Question #8

Refer to the exhibit

Which two statements are true regarding enabling auto-cache on FortiAnalyzer? (Choose two)

A. Enabling auto-cache reduces report generation time for reports that require a long time to assemble datasets
B. Report size will be optimized to conserve disk space on FortiAnalyzer
C. Reports will be cached in the memory
D. This feature is automatically enabled for scheduled reports

Question #9

What is Log Insert Lag Time on FortiAnalyzer?

A. The number of times in the logs where end users experienced slowness while accessing resources
B. The amount of lag time that occurs when the administrator is rebuilding the ADOM database
C. The amount of time that passes between the time a log was received and when it was indexed on FortiAnalyzer
D. The amount of time FortiAnalyzer takes to receive logs from a registered device

Question #10 A and B

Which two statements are true regarding fabric connectors? (Choose two)

A. Configuring fabric connectors to send notifications to ITSM platforms upon incident creation is more efficient than third-party polling information from the FortiAnalyzer API
B. Fabric connectors allow you to save storage costs improve redundancy
C. Storage connector service does not require a separate license to send logs to cloud platform A and B
D. Cloud-out connectors allow you to send real-time logs to public cloud accounts like Amazon S3, Azure Blob, and Google Cloud.

Question #11

Which statement is true regarding Macros on FortiAnalyze?

A. Macros are useful in generating excel log files automatically based on the report settings
B. Macros are predefined templates for reports and cannot be customized
C. Macros are ADOM specific and each ADOM will have unique macros relevant to that ADOM
D. Macros are supported only on the FortiGate ADOM

Question #12

What does the disk status Degraded mean for RAID management?

A. For FortiAnalyzer device is writing data to a newly added hard drive in order to restore the hard drive to an optimal state
B. The hard drive is no longer being used by the RAID controller
C. One ore more drives are missing from the fortiAnalyzer unit. The drive is no longer available to the operating system
D. The FortiAnalyzer device is writing to all the hard drives on the device in order to make the array fault tollerant

Question #13

An Administrator has moved FortiGate A from root ADMIN to ADOM1
Which two statements are true regarding logs?

A. Archived logs will be moved to ADOM1 from the root ADOM automatically
B. Analytics logs will be moved to ADOM1 from the root ADOM after you rebuild the ADMOM1 SQL database
C. Logs will be present in both ADOMs immediately after the move
D. Analytics logs will be moved to ADOM1 from the root ADOM automatically

Question #14

Which two statements are true regarding FortiAnalyzer log forwarding? (Choose two)

A. Aggregation mode stores logs and content files and uploads from them to another FortiAnalyzer device at a scheduled time A and C correct answer
B. In aggregation mode, you can forward logs to syslog and CEF servers as well
C. Both modes, forwarding and aggregation, support encryption of logs between devices
D. Forwarding mode forwards logs in real time only to other FortiAnalyzer devices

Question #15

Which two statements are true regarding log fetching on FortiAnalyzer? (Choose two)

A) Log fetching allows the administrator to fetch analytics logs from another FortiAnalyzer for redundancy A and C correct answer
B) Log fetching can be done only on two FortiAnalyzer devices that are running the same firmware version
C) A FortiAnalyzer device can perform either the fetch server or client role, and it can perform two roles at the same time with the same FortiAnalyzer devices at the other end
D) Log fetching allows the administrator to run query and reports against historical data by retrieving archived logs from one FortiAnalyzer device and sending them to another FortiAnalyzer device

Question #16

An administrator fortinet, is able to view logs and perform device management task, such us adding and removing registered device. However, administrator fortinet is not able to create a mail server that can be used to send alert emails. What could be the problem?

A) fortinet is assigned the Standard_User administrative profile
B) ADOM mode is configured with Advanced mode
C) fortinet is assigned the Restricted_User admistrative profile
D) A trusted host is configured

Question #17

Which two statements are true regarding high availability (HA) on FortiAnalyzer? (Choose two)

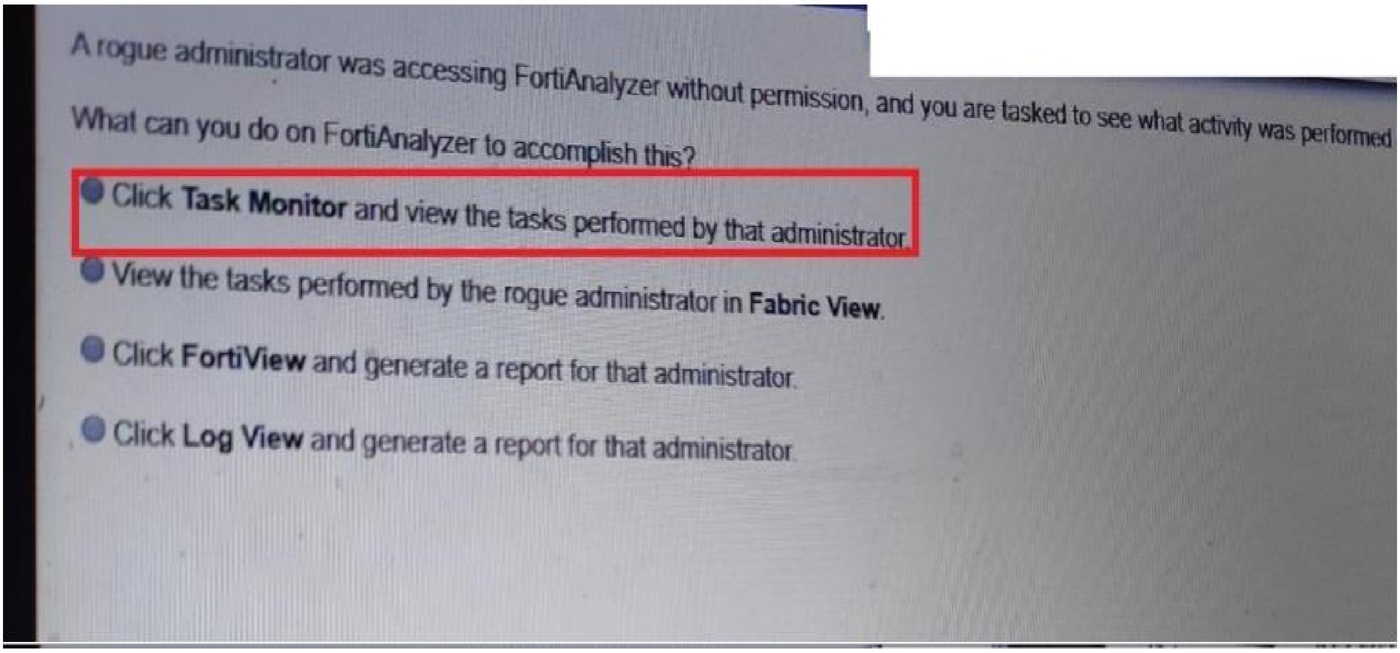
A) FortiAnalyzer HA supports synchronization of logs as wellas some system and configuration settings A & B correct answer
B) All devices in a FortiAnalyzer HA cluster must run in the same operation mode: analyzer or collector
C) FortiAnalyzer HA implementation is supported by many public cloud infrastructures such as AWS, Microsoft Azure, and Google Cloud
D) FortiAnalyzer HA can function without VRRP, and VRRP is required only if you have more then two FortiAnalyzer devices in a cluster

Question #18

Which daemon is responsible for enforcing raw log file size?

A) Sqlplugind
B) oftpd
C) logfiled C correct answer
D) miglogd

New question FAZ 6.4



A rogue administrator was accessing FortiAnalyzer without permission, and you are tasked to see what activity was performed

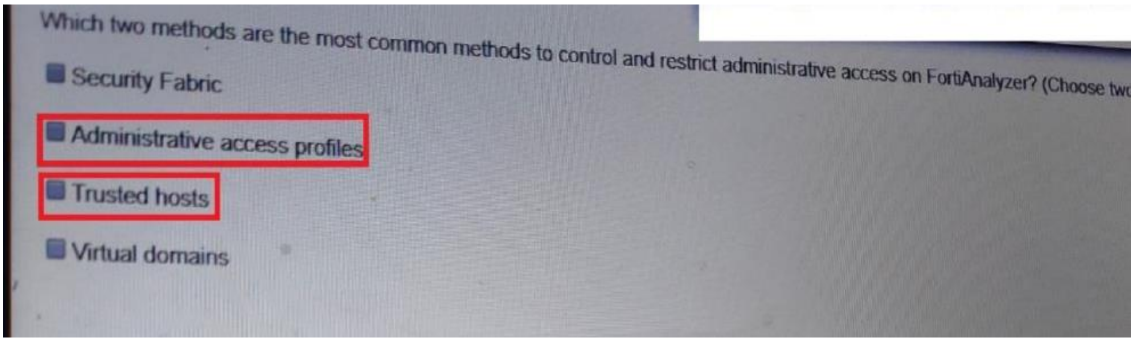
What can you do on FortiAnalyzer to accomplish this?

● [✓ Click **Task Monitor** and view the tasks performed by that administrator.]

● View the tasks performed by the rogue administrator in **Fabric View**.

● Click **FortiView** and generate a report for that administrator.

● Click **Log View** and generate a report for that administrator.



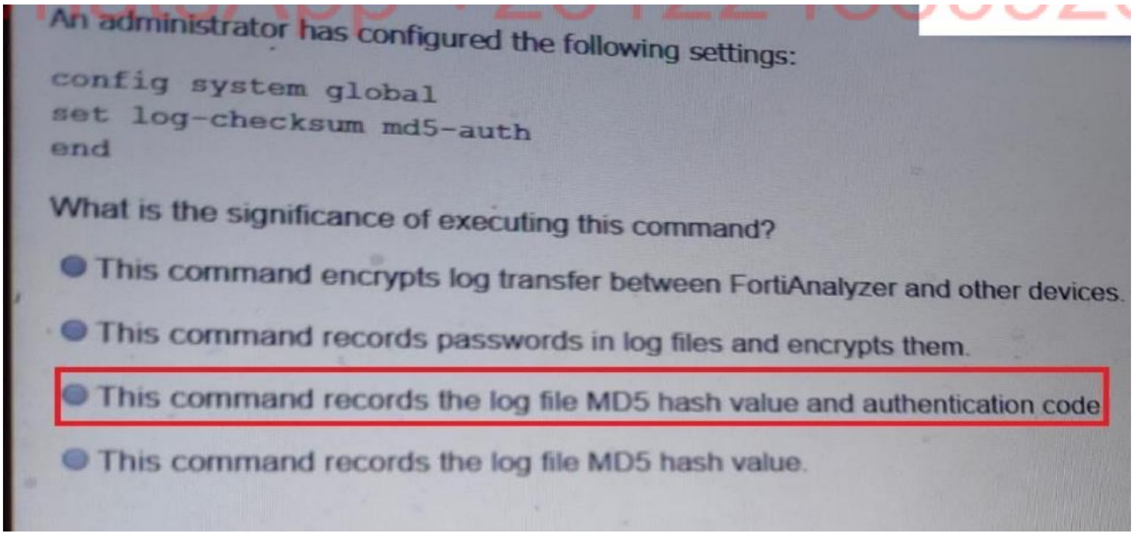
Which two methods are the most common methods to control and restrict administrative access on FortiAnalyzer? (Choose two

■ Security Fabric

■ [✓ Administrative access profiles]

■ [✓ Trusted hosts]

■ Virtual domains



An administrator has configured the following settings:

```
config system global
set log-checksum md5-auth
end
```

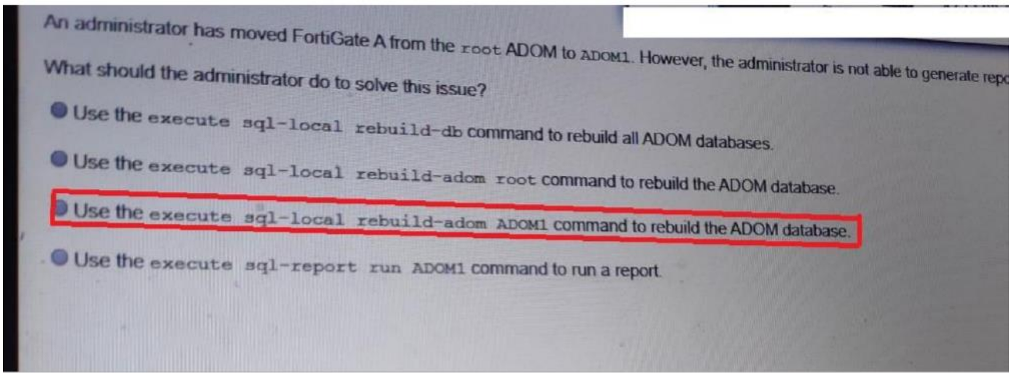
What is the significance of executing this command?

● This command encrypts log transfer between FortiAnalyzer and other devices.

● This command records passwords in log files and encrypts them.

● [✓ This command records the log file MD5 hash value and authentication code]

● This command records the log file MD5 hash value.



An administrator has moved FortiGate A from the `root` ADOM to `ADOM1`. However, the administrator is not able to generate repo

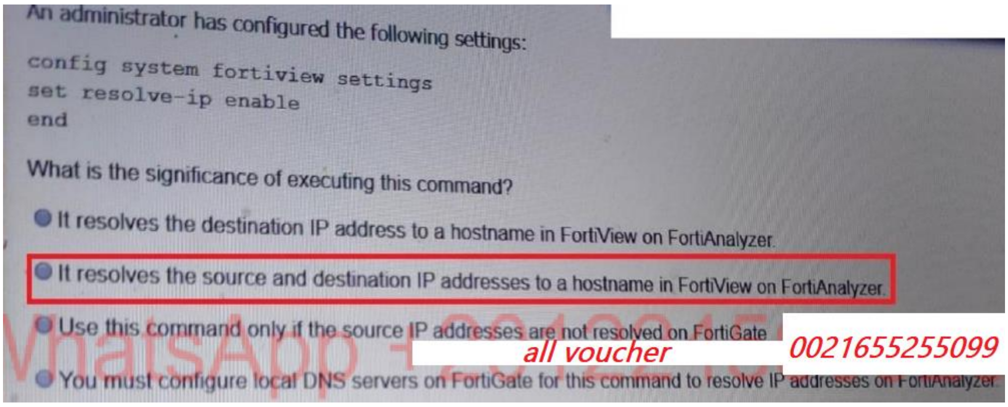
What should the administrator do to solve this issue?

○ Use the `execute sql-local rebuild-db` command to rebuild all ADOM databases.

○ Use the `execute sql-local rebuild-adom root` command to rebuild the ADOM database.

[✓ ○ Use the `execute sql-local rebuild-adom ADOM1` command to rebuild the ADOM database.]

○ Use the `execute sql-report run ADOM1` command to run a report.



An administrator has configured the following settings:

```
config system fortiview settings
set resolve-ip enable
end
```

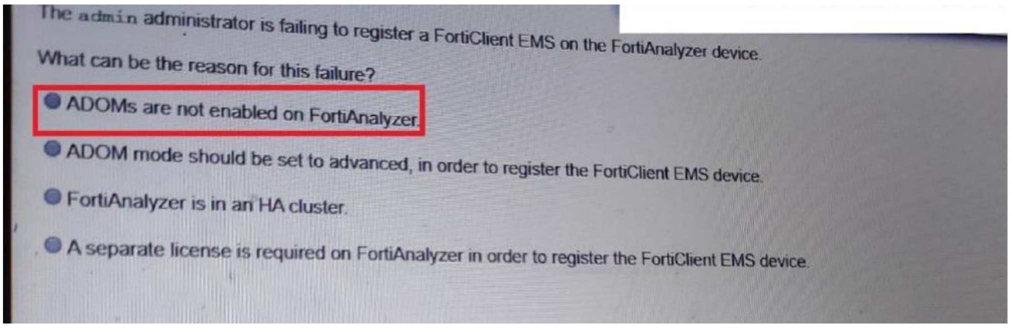
What is the significance of executing this command?

○ It resolves the destination IP address to a hostname in FortiView on FortiAnalyzer.

[✓ ○ It resolves the source and destination IP addresses to a hostname in FortiView on FortiAnalyzer.]

○ Use this command only if the source IP addresses are not resolved on FortiGate.

○ You must configure local DNS servers on FortiGate for this command to resolve IP addresses on FortiAnalyzer.



The `admin` administrator is failing to register a FortiClient EMS on the FortiAnalyzer device.

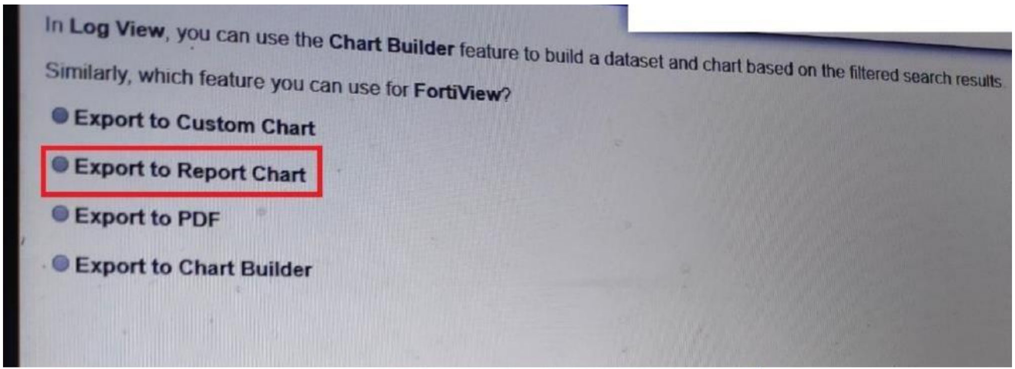
What can be the reason for this failure?

[✓ ○ ADOMs are not enabled on FortiAnalyzer.]

○ ADOM mode should be set to advanced, in order to register the FortiClient EMS device.

○ FortiAnalyzer is in an HA cluster.

○ A separate license is required on FortiAnalyzer in order to register the FortiClient EMS device.



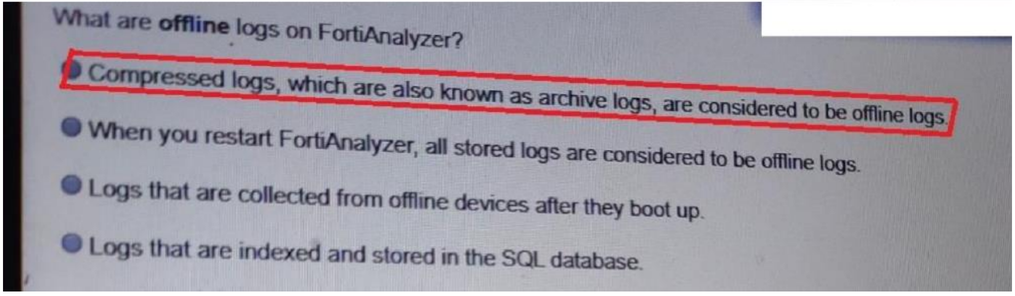
In **Log View**, you can use the **Chart Builder** feature to build a dataset and chart based on the filtered search results. Similarly, which feature you can use for **FortiView**?

○ **Export to Custom Chart**

[✓ ○ **Export to Report Chart**]

○ **Export to PDF**

○ **Export to Chart Builder**



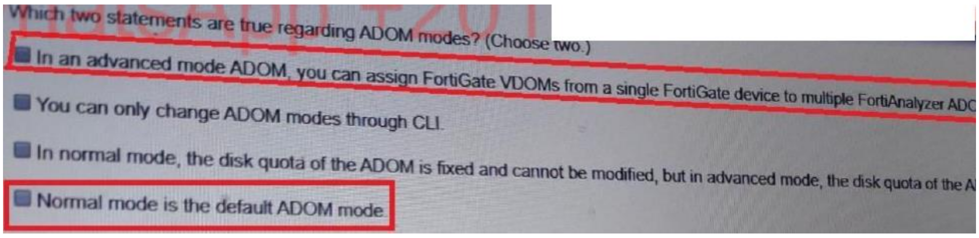
What are **offline** logs on FortiAnalyzer?

[✓ ○ Compressed logs, which are also known as archive logs, are considered to be offline logs.]

○ When you restart FortiAnalyzer, all stored logs are considered to be offline logs.

○ Logs that are collected from offline devices after they boot up.

○ Logs that are indexed and stored in the SQL database.



Which two statements are true regarding ADOM modes? (Choose two.)

[✓ □ In an advanced mode ADOM, you can assign FortiGate VDOMs from a single FortiGate device to multiple FortiAnalyzer ADO]

□ You can only change ADOM modes through CLI.

□ In normal mode, the disk quota of the ADOM is fixed and cannot be modified, but in advanced mode, the disk quota of the A

[✓ □ Normal mode is the default ADOM mode.]

Exam	NSE5_FAZ-6.4
Title	Fortinet NSE 5 - FortiAnalyzer 6.4
Version	1.0
Product Type	30 Q&A with explanations

"Best Material, Great Results". www.certkingdom.com 1 of 1

QUESTION 1
Which clause is considered mandatory in SELECT statements used by the FortiAnalyzer to generate reports?

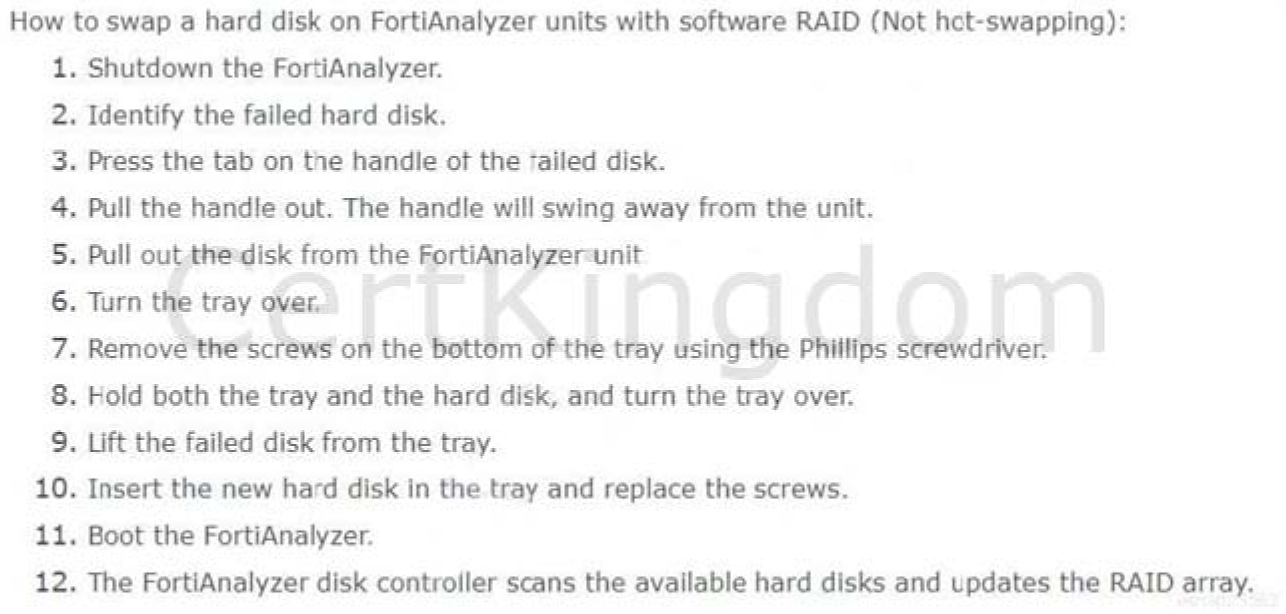
A. FROM
B. ORDER BY
C. LIMIT
D. WHERE

Answer: A
Section: (none)
Explanation
Explanation/Reference:

QUESTION 2
If a hard disk on FortiAnalyzer that supports hardware RAID fails, what can be done on FortiAnalyzer?

A. Shut down FortiAnalyzer and replace the disk.
B. Run execute format disk to format and restart the FortiAnalyzer device.
C. No need to do anything because the disk will self-recover.
D. Hot swap the disk

Answer: A
Section: (none)
Explanation
Explanation/Reference:
Reference: https://community.fortinet.com/t5/FortiAnalyzer/Technical-Note-How-to-swap-Hard-Disk-on-FortiAnalyzer/ta-p/194997?externalID=FD41397#:~:text=If%20a%20hard%20disk%20on,process%20known%20as%20hot%20swapping



How to swap a hard disk on FortiAnalyzer units with software RAID (Not hot-swapping):

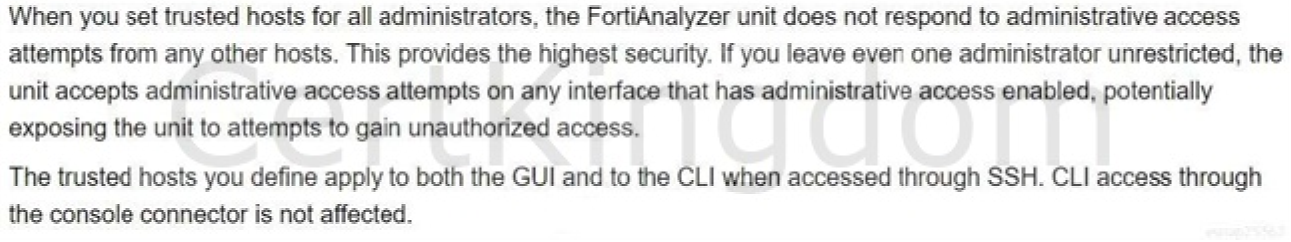
1. Shutdown the FortiAnalyzer.
2. Identify the failed hard disk.
3. Press the tab on the handle of the failed disk.
4. Pull the handle out. The handle will swing away from the unit.
5. Pull out the disk from the FortiAnalyzer unit
6. Turn the tray over.
7. Remove the screws on the bottom of the tray using the Phillips screwdriver.
8. Hold both the tray and the hard disk, and turn the tray over.
9. Lift the failed disk from the tray.
10. Insert the new hard disk in the tray and replace the screws.
11. Boot the FortiAnalyzer.
12. The FortiAnalyzer disk controller scans the available hard disks and updates the RAID array.

QUESTION 3
Which two methods are the most common methods to control and restrict administrative access on FortiAnalyzer? (Choose two.)

A. Virtual domains

B. Administrative access profiles
C. Trusted hosts
D. Security Fabric

Answer: B,C
Section: (none)
Explanation
Explanation/Reference:
Reference: https://docs2.fortinet.com/document/fortianalyzer/6.0.0/administration-guide/219292/administratorprofiles
https://docs2.fortinet.com/document/fortianalyzer/6.0.0/administration-guide/581222/trusted-hosts



When you set trusted hosts for all administrators, the FortiAnalyzer unit does not respond to administrative access attempts from any other hosts. This provides the highest security. If you leave even one administrator unrestricted, the unit accepts administrative access attempts on any interface that has administrative access enabled, potentially exposing the unit to attempts to gain unauthorized access.

The trusted hosts you define apply to both the GUI and to the CLI when accessed through SSH. CLI access through the console connector is not affected.

QUESTION 4
Which daemon is responsible for enforcing raw log file size?

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

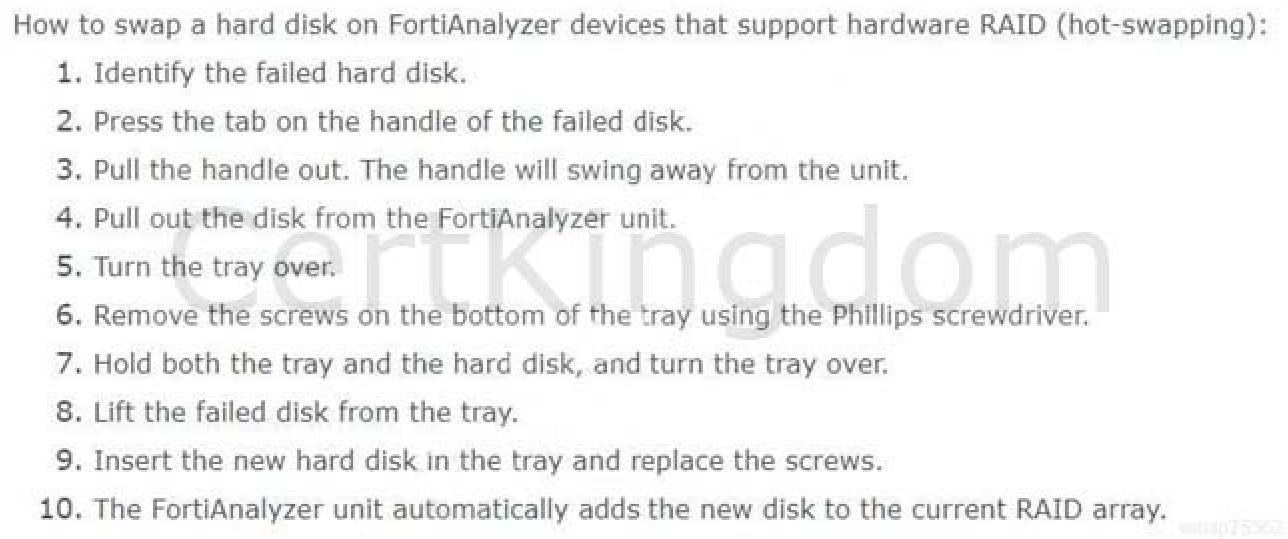
Answer: A
Section: (none)
Explanation
Explanation/Reference:

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

Answer: D
Section: (none)
Explanation
Explanation/Reference:
Reference: https://community.fortinet.com/t5/FortiAnalyzer/Technical-Note-How-to-swap-Hard-Disk-on-FortiAnalyzer/ta-p/194997?externalID=FD41397#:~:text=If%20a%20hard%20disk%20on,process%20known%

20as%20hot%20swapping



How to swap a hard disk on FortiAnalyzer devices that support hardware RAID (hot-swapping):

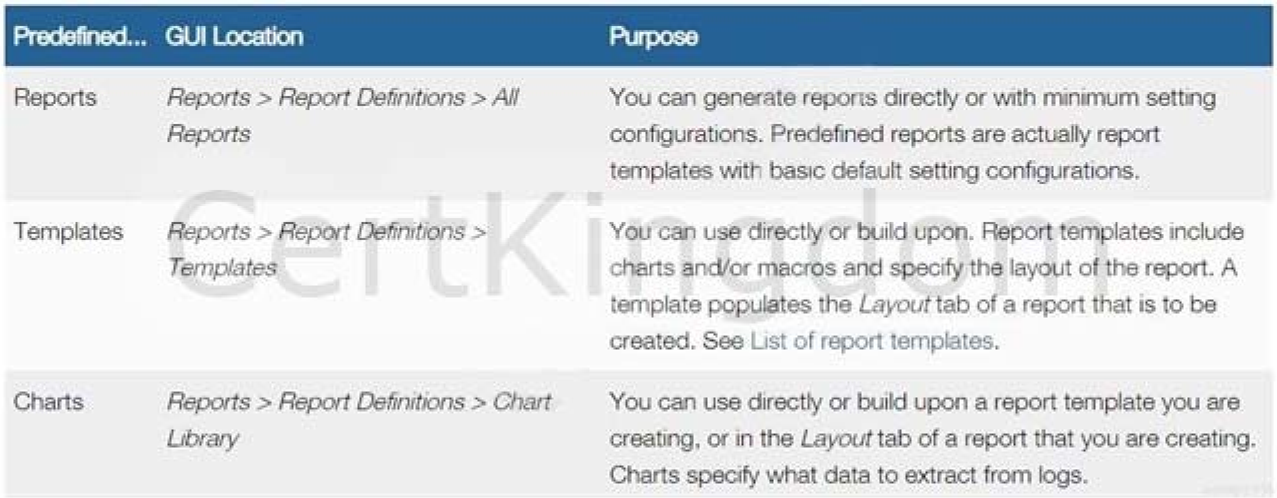
1. Identify the failed hard disk.
2. Press the tab on the handle of the failed disk.
3. Pull the handle out. The handle will swing away from the unit.
4. Pull out the disk from the FortiAnalyzer unit.
5. Turn the tray over.
6. Remove the screws on the bottom of the tray using the Phillips screwdriver.
7. Hold both the tray and the hard disk, and turn the tray over.
8. Lift the failed disk from the tray.
9. Insert the new hard disk in the tray and replace the screws.
10. The FortiAnalyzer unit automatically adds the new disk to the current RAID array.

QUESTION 6

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

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

Answer: A
Section: (none)
Explanation
Explanation/Reference:
Reference: https://docs2.fortinet.com/document/fortianalyzer/6.0.8/administration-guide/618245/predefinedreports-
templates-charts-and-macros



Predefined...	GUI Location	Purpose
Reports	*Reports > Report Definitions > All Reports*	You can generate reports directly or with minimum setting configurations. Predefined reports are actually report templates with basic default setting configurations.
Templates	*Reports > Report Definitions > Templates*	You can use directly or build upon. Report templates include charts and/or macros and specify the layout of the report. A template populates the *Layout* tab of a report that is to be created. See List of report templates.
Charts	*Reports > Report Definitions > Chart Library*	You can use directly or build upon a report template you are creating, or in the *Layout* tab of a report that you are creating. Charts specify what data to extract from logs.

QUESTION 7

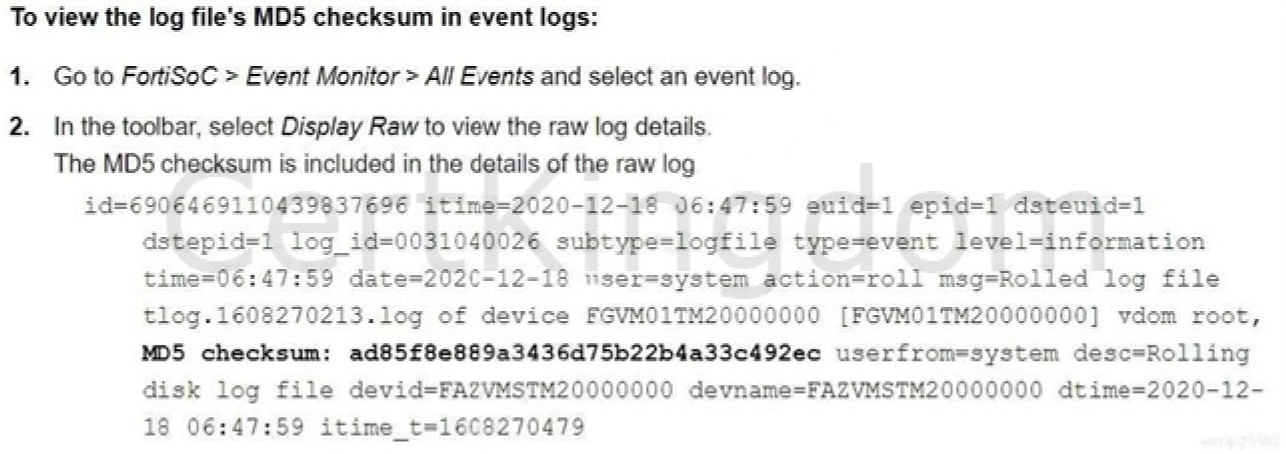
An administrator has configured the following settings:

```
config system global
set log-checksum md5-auth
end
```

What is the significance of executing this command?

A. This command records the log file MD5 hash value.
B. This command records passwords in log files and encrypts them.
C. This command encrypts log transfer between FortiAnalyzer and other devices.
D. This command records the log file MD5 hash value and authentication code.

Answer: D
Section: (none)
Explanation
Explanation/Reference:
Reference: https://docs.fortinet.com/document/fortianalyzer/6.4.6/administration-guide/410387/appendix-b-logintegrity-
and-secure-log-transfer



To view the log file's MD5 checksum in event logs:

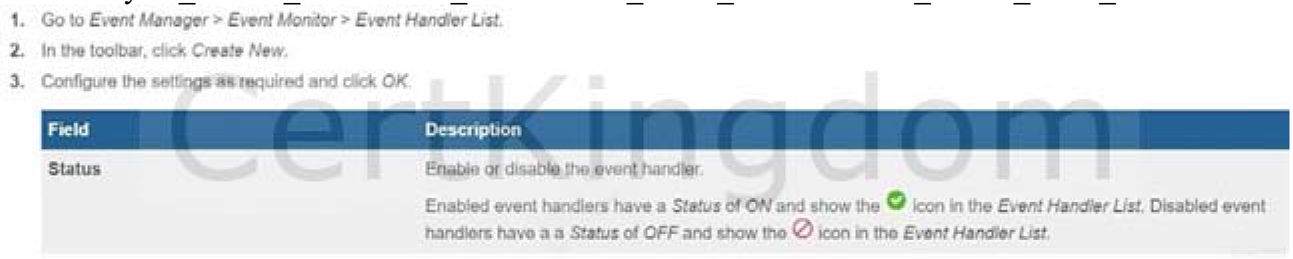
1. Go to *FortiSoC* > *Event Monitor* > *All Events* and select an event log.
2. In the toolbar, select *Display Raw* to view the raw log details.
   The MD5 checksum is included in the details of the raw log

```
id=6906469110439837696 itime=2020-12-18 06:47:59 euid=1 epid=1 dsteuid=1
    dstepid=1 log_id=0031040026 subtype=logfile type=event level=information
    time=06:47:59 date=2020-12-18 user=system action=roll msg=Rolled log file
    tlog.1608270213.log of device FGVM01TM20000000 [FGVM01TM20000000] vdom root,
    MD5 checksum: ad85f8e889a3436d75b22b4a33c492ec userfrom=system desc=Rolling
    disk log file devid=FAZVMSTM20000000 devname=FAZVMSTM20000000 dtime=2020-12-
    18 06:47:59 itime_t=1608270479
```

QUESTION 8
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. IM
C. SMS
D. Email

Answer: A,D
Section: (none)
Explanation
Explanation/Reference:
Reference: https://help.fortinet.com/fa/faz50hlp/60/6-0-2/Content/
FortiAnalyzer_Admin_Guide/1800_Events/0200_Event_handlers/0600_Create_event_handlers.htm



1. Go to *Event Manager* > *Event Monitor* > *Event Handler List*.
2. In the toolbar, click *Create New*.
3. Configure the settings as required and click *OK*.

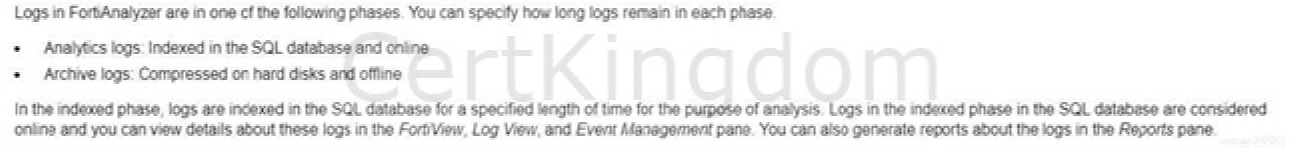
Field	Description
Status	Enable or disable the event handler. Enabled event handlers have a *Status* of *ON* and show the ✓ icon in the *Event Handler List*. Disabled event handlers have a a *Status* of *OFF* and show the ⊘ icon in the *Event Handler List*.

QUESTION 9

What are offline logs on FortiAnalyzer?

A. Compressed logs, which are also known as archive logs, are considered to be offline logs.
B. When you restart FortiAnalyzer, all stored logs are considered to be offline logs.
C. Logs that are indexed and stored in the SQL database.
D. Logs that are collected from offline devices after they boot up.

Answer: A
Section: (none)
Explanation
Explanation/Reference:
Reference: https://help.fortinet.com/fa/faz50hlp/56/5-6-6/Content/FortiAnalyzer_Admin_Guide/0300_Key_concepts/0600_Log_Storage/0400_Archive_analytics_logs.htm



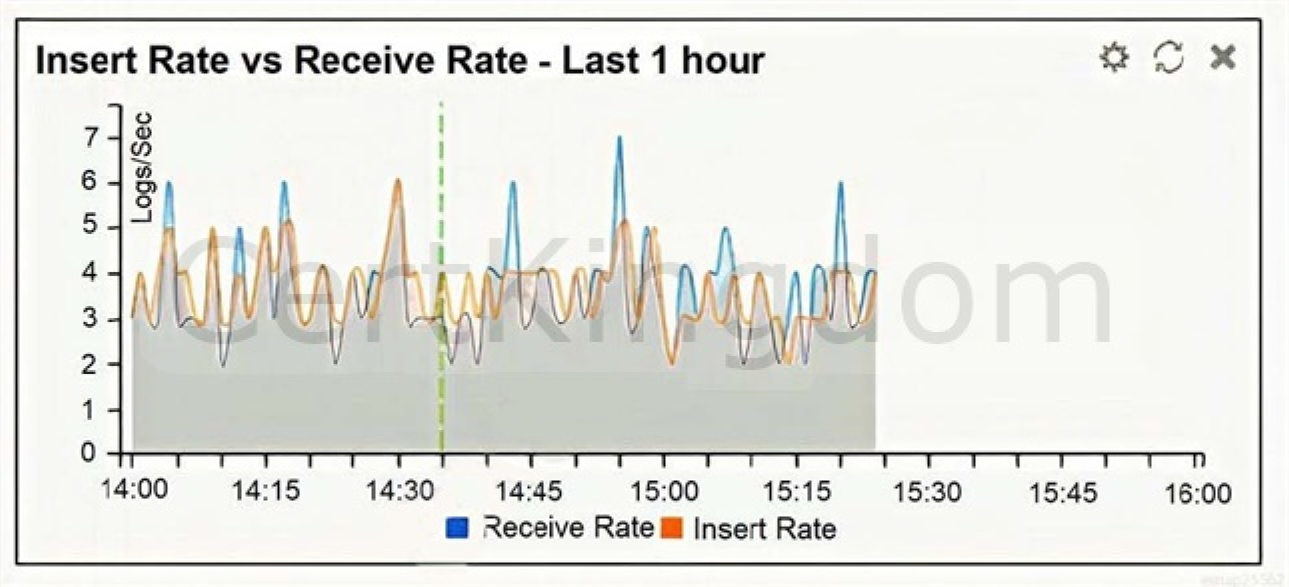
Logs in FortiAnalyzer are in one cf the following phases. You can specify how long logs remain in each phase.

- Analytics logs: Indexed in the SQL database and online
- Archive logs: Compressed on hard disks and offline

In the indexed phase, logs are indexed in the SQL database for a specified length of time for the purpose of analysis. Logs in the indexed phase in the SQL database are considered online and you can view details about these logs in the *FortiView*, *Log View*, and *Event Management* pane. You can also generate reports about the logs in the *Reports* pane.

QUESTION 10

Refer to the exhibit.

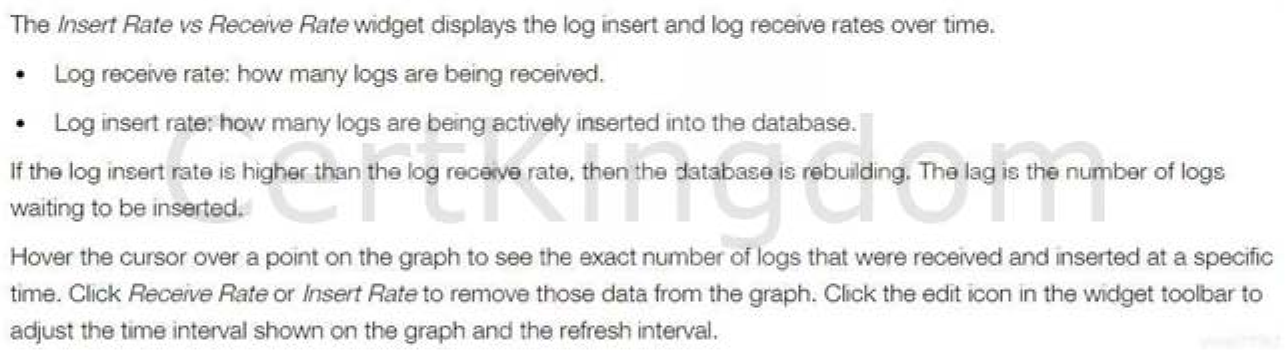


What does the data point at 14:35 tell you?

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

Answer: B
Section: (none)
Explanation
Explanation/Reference:
Reference: https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/47690/insert-rate-vsreceive-

rate-widget



The *Insert Rate vs Receive Rate* widget displays the log insert and log receive rates over time.

- Log receive rate: how many logs are being received.
- Log insert rate: how many logs are being actively inserted into the database.

If the log insert rate is higher than the log receive rate, then the database is rebuilding. The lag is the number of logs waiting to be inserted.

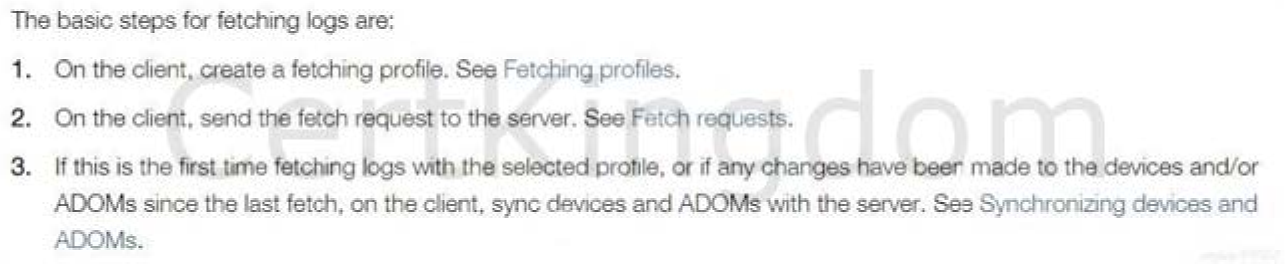
Hover the cursor over a point on the graph to see the exact number of logs that were received and inserted at a specific time. Click *Receive Rate* or *Insert Rate* to remove those data from the graph. Click the edit icon in the widget toolbar to adjust the time interval shown on the graph and the refresh interval.

QUESTION 11

Which two statements are true regarding log fetching on FortiAnalyzer? (Choose two.)

A. A FortiAnalyzer device can perform either the fetch server or client role, and it can perform two roles at the same time with the same FortiAnalyzer devices at the other end.
B. Log fetching can be done only on two FortiAnalyzer devices that are running the same firmware version.
C. Log fetching allows the administrator to fetch analytics logs from another FortiAnalyzer for redundancy.
D. Log fetching allows the administrator to run queries and reports against historical data by retrieving archived logs from one FortiAnalyzer device and sending them to another FortiAnalyzer device.

Answer: A,B
Section: (none)
Explanation
Explanation/Reference:
Reference: https://docs.fortinet.com/document/fortianalyzer/7.0.1/administration-guide/651442/fetchermanagement



The basic steps for fetching logs are:

1. On the client, create a fetching profile. See Fetching profiles.
2. On the client, send the fetch request to the server. See Fetch requests.
3. If this is the first time fetching logs with the selected profile, or if any changes have been made to the devices and/or ADOMs since the last fetch, on the client, sync devices and ADOMs with the server. See Synchronizing devices and ADOMs.

QUESTION 12

An administrator has configured the following settings:

```
config system fortiview settings
set resolve-ip enable
end
```

What is the significance of executing this command?

A. Use this command only if the source IP addresses are not resolved on FortiGate.
B. It resolves the source and destination IP addresses to a hostname in FortiView on FortiAnalyzer.
C. You must configure local DNS servers on FortiGate for this command to resolve IP addresses on FortiAnalyzer.
D. It resolves the destination IP address to a hostname in FortiView on FortiAnalyzer.

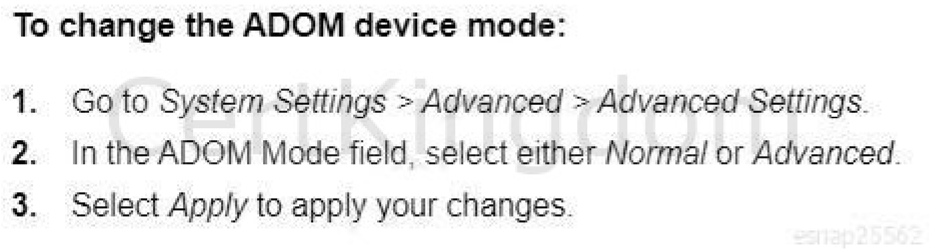
Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://community.fortinet.com/t5/Fortinet-Forum/Hostnames-in-FortiAnalyzer/m-p/95351?m=156950

QUESTION 13
Which two statements are true regarding ADOM modes? (Choose two.)

A. You can only change ADOM modes through CLI.
B. In normal mode, the disk quota of the ADOM is fixed and cannot be modified, but in advance mode, the disk quota of the ADOM is flexible because new devices are added to the ADOM.
C. In an advanced mode ADOM, you can assign FortiGate VDOMs from a single FortiGate device to multiple FortiAnalyzer ADOMs.
D. Normal mode is the default ADOM mode.

Answer: C,D
Section: (none)
Explanation
Explanation/Reference:
Reference: https://help.fortinet.com/fa/faz50hlp/56/5-6-1/FMG-FAZ/0800_ADOMs/0400_ADOM%20Device%20Modes.htm



To change the ADOM device mode:

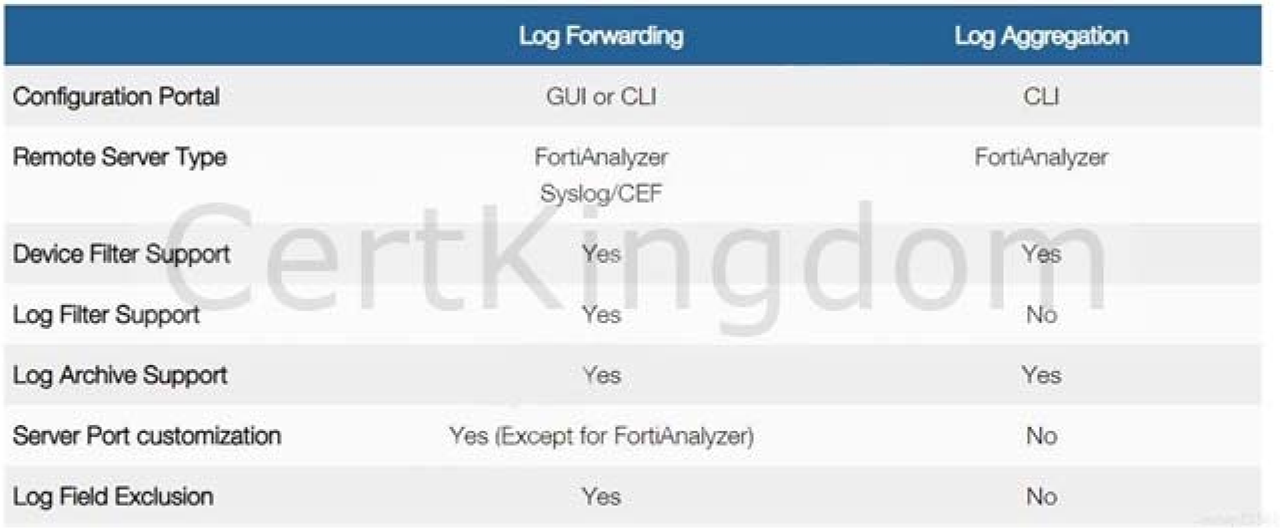
1. Go to *System Settings > Advanced > Advanced Settings*.
2. In the ADOM Mode field, select either *Normal* or *Advanced*.
3. Select *Apply* to apply your changes.

QUESTION 14
Which two statements are true regarding FortiAnalyzer log forwarding? (Choose two.)

A. In aggregation mode, you can forward logs to syslog and CEF servers as well.
B. Forwarding mode forwards logs in real time only to other FortiAnalyzer devices.
C. Aggregation mode stores logs and content files and uploads them to another FortiAnalyzer device at a scheduled time.
D. Both modes, forwarding and aggregation, support encryption of logs between devices.

Answer: C,D
Section: (none)
Explanation
Explanation/Reference:
Reference: https://docs.fortinet.com/document/fortianalyzer/6.2.0/cookbook/63238/what-is-the-differencebetween-

log-forward-and-log-aggregation-modes

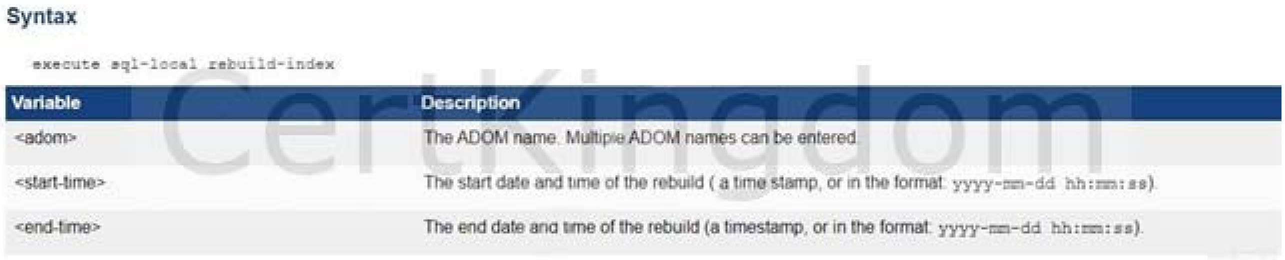


	Log Forwarding	Log Aggregation
Configuration Portal	GUI or CLI	CLI
Remote Server Type	FortiAnalyzer Syslog/CEF	FortiAnalyzer
Device Filter Support	Yes	Yes
Log Filter Support	Yes	No
Log Archive Support	Yes	Yes
Server Port customization	Yes (Except for FortiAnalyzer)	No
Log Field Exclusion	Yes	No

QUESTION 15
An administrator has moved FortiGate A from the root ADOM to ADOM1. However, the administrator is not able to generate reports for FortiGate A in ADOM1.
What should the administrator do to solve this issue?

A. Use the execute sql-local rebuild-db command to rebuild all ADOM databases.
B. Use the execute sql-local rebuild-adom ADOM1 command to rebuild the ADOM database.
C. Use the execute sql-report run ADOM1 command to run a report.
D. Use the execute sql-local rebuild-adom root command to rebuild the ADOM database.

Answer: B
Section: (none)
Explanation
Explanation/Reference:
Reference: https://help.fortinet.com/fmgr/cli/5-6-1/FortiManager_CLI_Reference/700_execute/sql-local+.htm



Syntax

```
execute sql-local rebuild-index
```

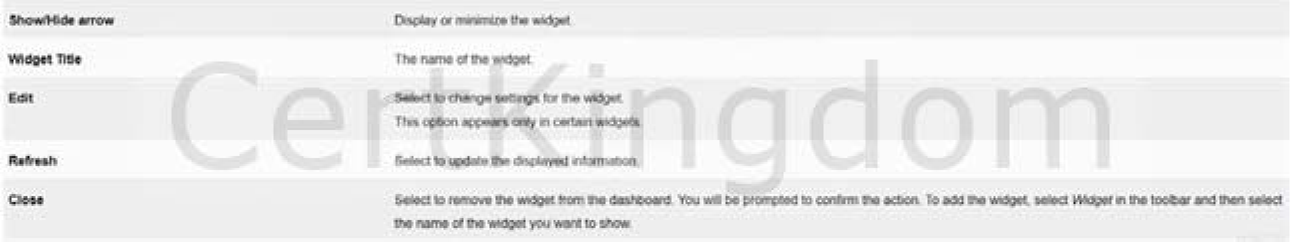
Variable	Description
<adom>	The ADOM name. Multiple ADOM names can be entered.
<start-time>	The start date and time of the rebuild (a time stamp, or in the format: yyyy-mm-dd hh:mm:ss).
<end-time>	The end date and time of the rebuild (a timestamp, or in the format: yyyy-mm-dd hh:mm:ss).

QUESTION 16
When you perform a system backup, what does the backup configuration contain? (Choose two.)

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

Answer: A,B
Section: (none)
Explanation
Explanation/Reference:

Reference: https://help.fortinet.com/fauth/5-2/Content/Admin%20Guides/5_2%20Admin%20Guide/300/301_Dashboard.htm



Show/Hide arrow	Display or minimize the widget.
Widget Title	The name of the widget.
Edit	Select to change settings for the widget. This option appears only in certain widgets.
Refresh	Select to update the displayed information.
Close	Select to remove the widget from the dashboard. You will be prompted to confirm the action. To add the widget, select *Widget* in the toolbar and then select the name of the widget you want to show.

QUESTION 17

Which statement is true regarding Macros on FortiAnalyzer?

A. Macros are ADOM specific and each ADOM will have unique macros relevant to that ADOM.
B. Macros are supported only on the FortiGate ADOM.
C. Macros are useful in generating excel log files automatically based on the reports settings.
D. Macros are predefined templates for reports and cannot be customized.

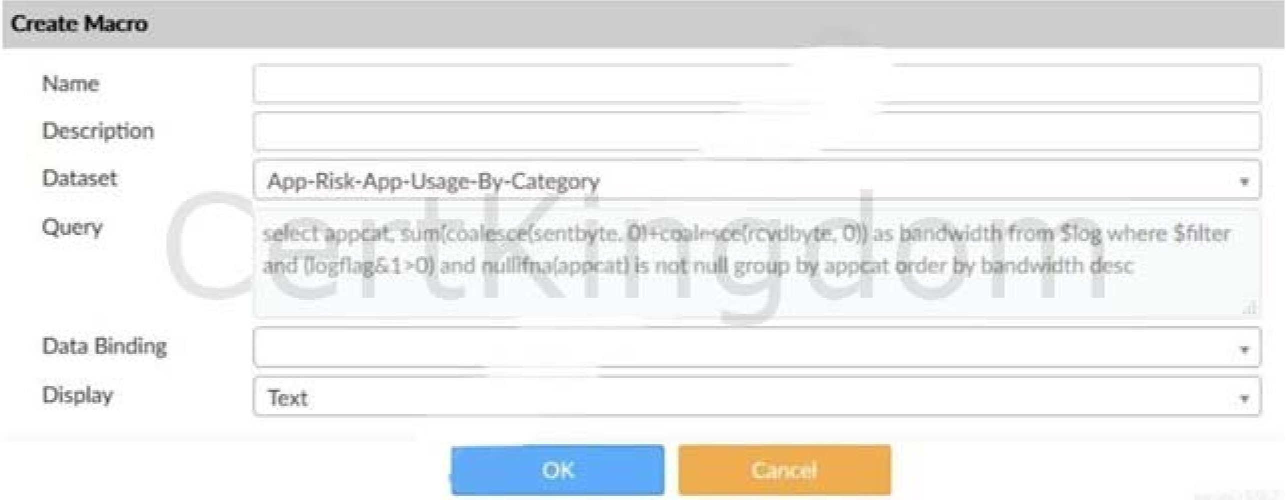
Answer: D

Section: (none)

Explanation

Explanation/Reference:

Reference: https://docs2.fortinet.com/document/fortianalyzer/6.2.3/administration-guide/617380/creatingmacros



Create Macro

Name	
Description	
Dataset	App-Risk-App-Usage-By-Category
Query	select appcat, sum(coalesce(sentbyte, 0)+coalesce(rcvdbyte, 0)) as bandwidth from $log where $filter and (logflag&1>0) and nullifna(appcat) is not null group by appcat order by bandwidth desc
Data Binding	
Display	Text

QUESTION 18

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

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

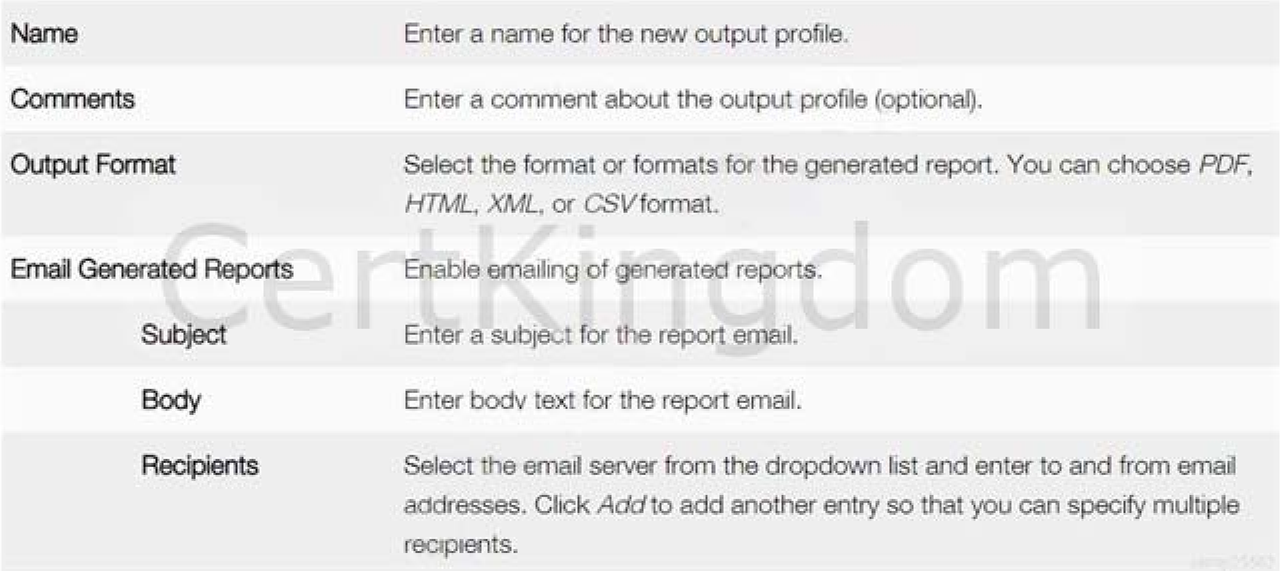
Answer: A,C

Section: (none)

Explanation

Explanation/Reference:

Reference: https://docs.fortinet.com/document/fortianalyzer/6.0.2/administration-guide/598322/creating-outputprofiles



Name	Enter a name for the new output profile.
Comments	Enter a comment about the output profile (optional).
Output Format	Select the format or formats for the generated report. You can choose *PDF*, *HTML*, *XML*, or *CSV* format.
Email Generated Reports	Enable emailing of generated reports.
Subject	Enter a subject for the report email.
Body	Enter bodv text for the report email.
Recipients	Select the email server from the dropdown list and enter to and from email addresses. Click *Add* to add another entry so that you can specify multiple recipients.

QUESTION 19
Which two statements are true regarding FortiAnalyzer operating modes? (Choose two.)

A. When in collector mode, FortiAnalyzer collects logs from multiple devices and forwards these logs in the original binary format.
B. Collector mode is the default operating mode.
C. When in collector mode, FortiAnalyzer supports event management and reporting features.
D. By deploying different FortiAnalyzer devices with collector and analyzer mode in a network, you can improve the overall performance of log receiving, analysis, and reporting.

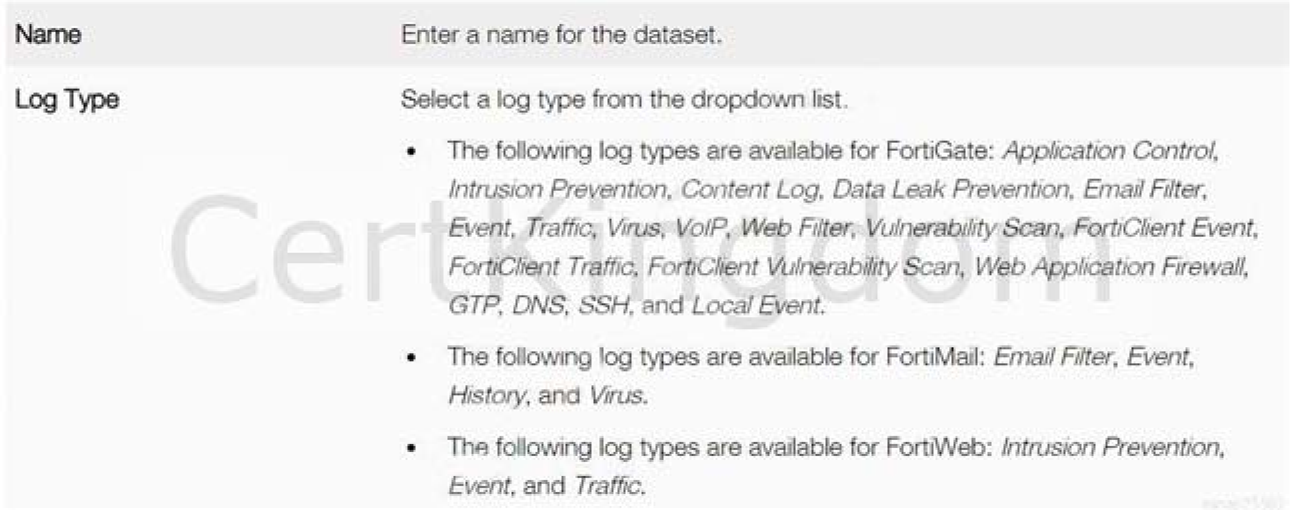
Answer: A,D
Section: (none)
Explanation
Explanation/Reference:
Reference: https://docs.fortinet.com/document/fortianalyzer/7.0.0/administration-guide/227478/collector-mode
https://docs.fortinet.com/document/fortianalyzer/7.0.0/administration-guide/312644/analyzer-collectorcollaboration

QUESTION 20
What the purpose of a dataset query in FortiAnalyzer?

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

Answer: B
Section: (none)
Explanation
Explanation/Reference:
Reference: https://docs2.fortinet.com/document/fortianalyzer/6.0.4/administration-

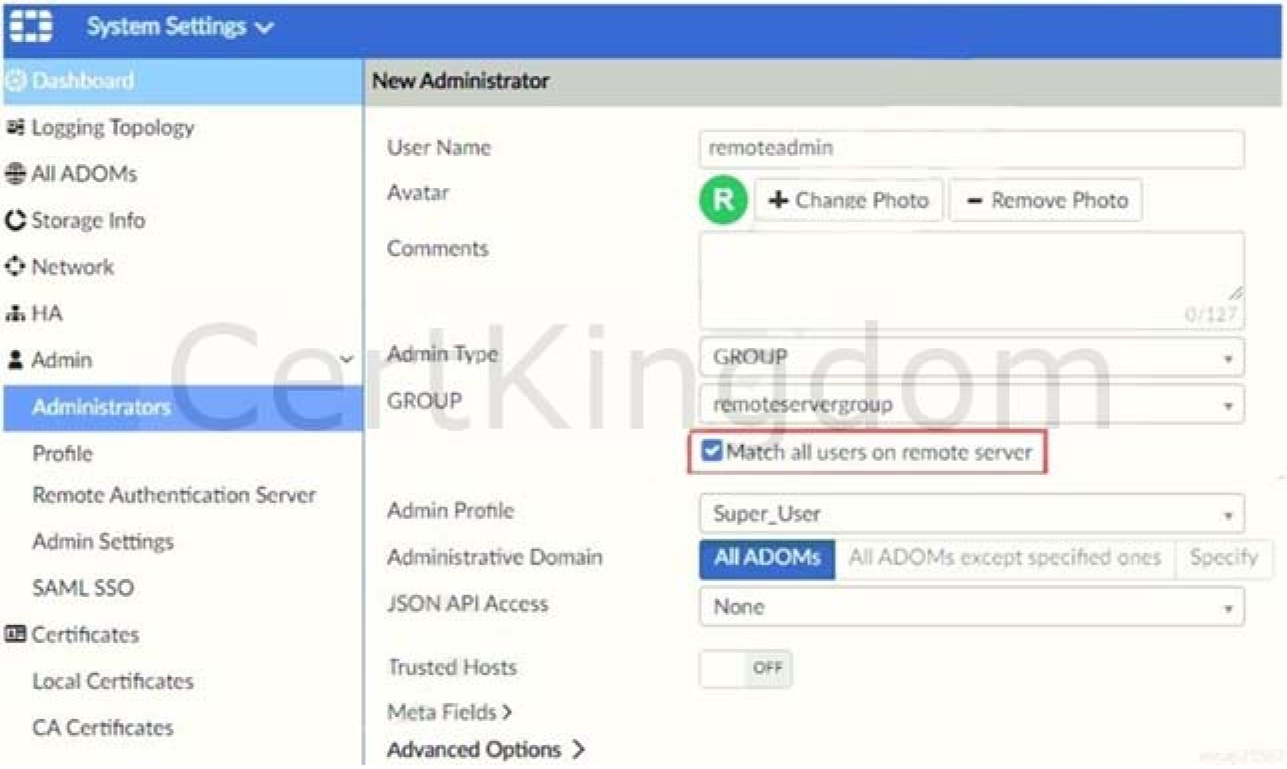
guide/148744/creatingdatasets



Name	Enter a name for the dataset.
Log Type	Select a log type from the dropdown list. • The following log types are available for FortiGate: *Application Control, Intrusion Prevention, Content Log, Data Leak Prevention, Email Filter, Event, Traffic, Virus, VoIP, Web Filter, Vulnerability Scan, FortiClient Event, FortiClient Traffic, FortiClient Vulnerability Scan, Web Application Firewall, GTP, DNS, SSH,* and *Local Event.* • The following log types are available for FortiMail: *Email Filter, Event, History,* and *Virus.* • The following log types are available for FortiWeb: *Intrusion Prevention, Event,* and *Traffic.*

QUESTION 21

Refer to the exhibit.



New Administrator

User Name: remoteadmin

Avatar

Comments

Admin Type: GROUP

GROUP: remoteservergroup

☑ Match all users on remote server

Admin Profile: Super_User

Administrative Domain: All ADOMs | All ADOMs except specified ones | Specify

JSON API Access: None

Trusted Hosts: OFF

The exhibit shows ‘remoteservergroupâ€ is an authentication server group with LDAP and RADIUS servers. Which two statements express the significance of enabling ‘Match all users on remote serverâ€ when configuring a new administrator? (Choose two.)

A. It creates a wildcard administrator using LDAP and RADIUS servers.
B. Administrator can log in to FortiAnalyzer using their credentials on remote servers LDAP and RADIUS.
C. Use remoteadmin from LDAP and RADIUS servers will be able to log in to FortiAnalyzer at any time.
D. It allows administrators to use two-factor authentication.

Answer: B,C
Section: (none)
Explanation
Explanation/Reference:

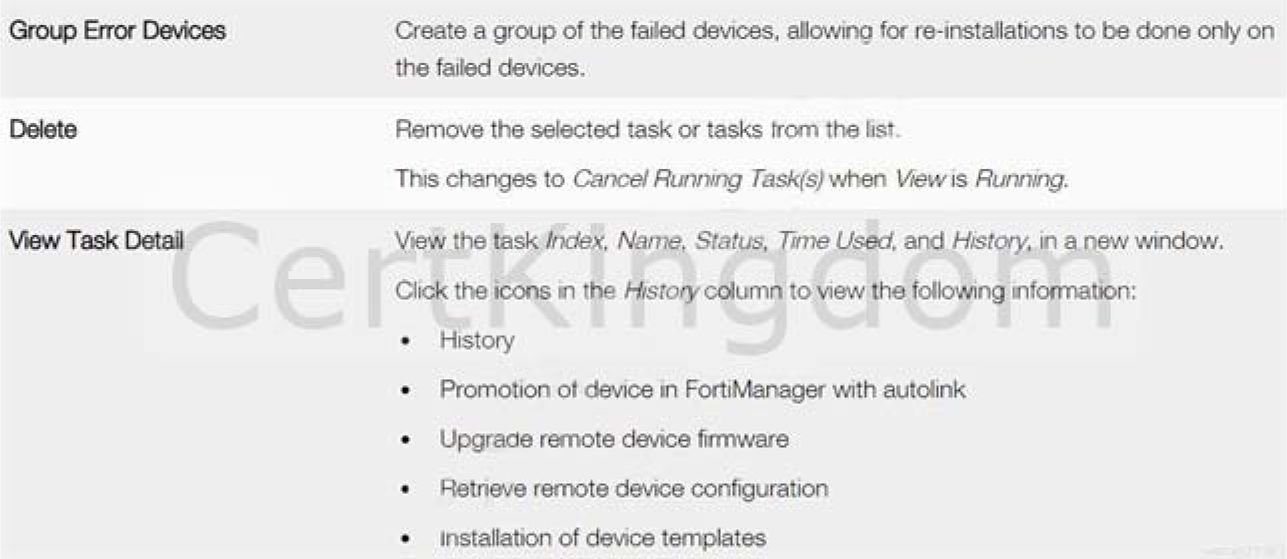
Reference: https://docs.fortinet.com/document/fortimanager/7.0.1/administration-guide/858351/creatingadministrators

QUESTION 22

A rogue administrator was accessing FortiAnalyzer without permission, and you are tasked to see what activity was performed by that rogue administrator on FortiAnalyzer.
What can you do on FortiAnalyzer to accomplish this?

A. Click FortiView and generate a report for that administrator.
B. Click Task Monitor and view the tasks performed by that administrator.
C. Click Log View and generate a report for that administrator.
D. View the tasks performed by the rogue administrator in Fabric View.

Answer: B
Section: (none)
Explanation
Explanation/Reference:
Reference: https://docs.fortinet.com/document/fortimanager/6.4.1/administration-guide/792943/task-monitor



Group Error Devices	Create a group of the failed devices, allowing for re-installations to be done only on the failed devices.
Delete	Remove the selected task or tasks from the list. This changes to *Cancel Running Task(s)* when *View* is *Running*.
View Task Detail	View the task *Index*, *Name*, *Status*, *Time Used*, and *History*, in a new window. Click the icons in the *History* column to view the following information: • History • Promotion of device in FortiManager with autolink • Upgrade remote device firmware • Retrieve remote device configuration • Installation of device templates

QUESTION 23

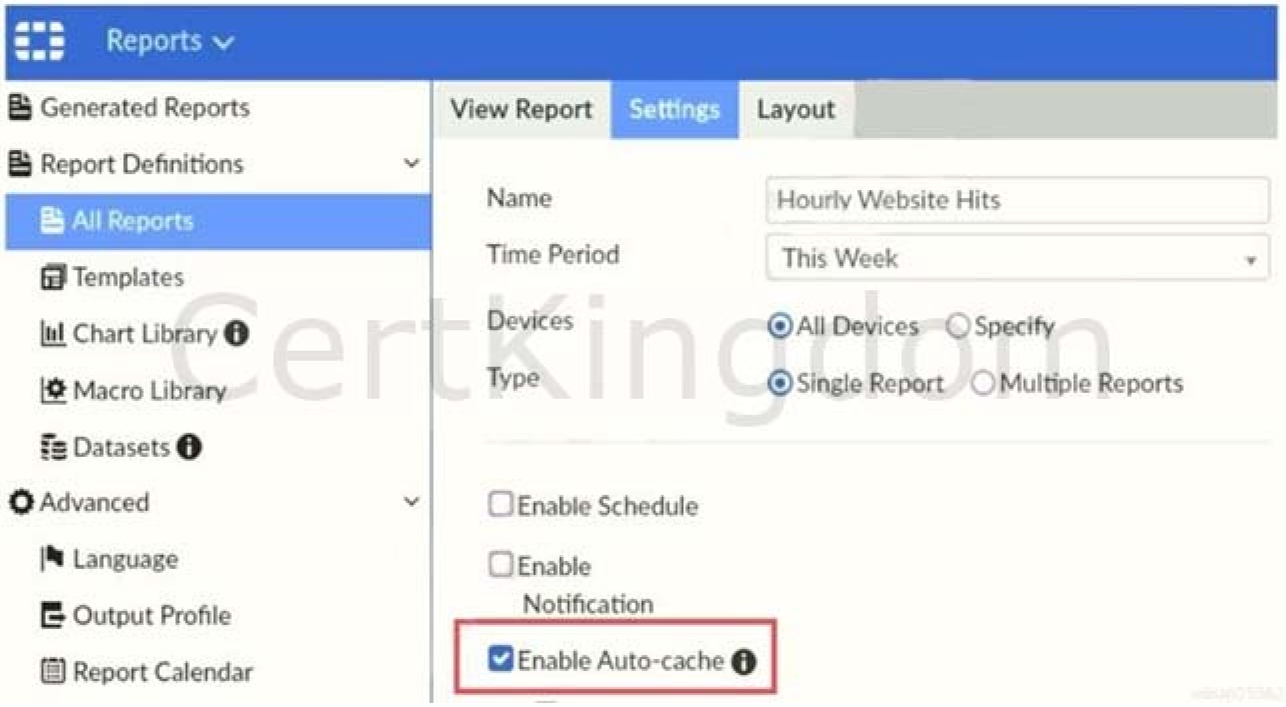
The admin administrator is failing to register a FortiClient EMS on the FortiAnalyzer device.
What can be the reason for this failure?

A. FortiAnalyzer is in an HA cluster.
B. ADOM mode should be set to advanced, in order to register the FortiClient EMS device.
C. ADOMs are not enabled on FortiAnalyzer.
D. A separate license is required on FortiAnalyzer in order to register the FortiClient EMS device.

Answer: C
Section: (none)
Explanation
Explanation/Reference:
Reference: https://help.fortinet.com/fa/faz50hlp/56/5-6-2/FMG-FAZ/0800_ADOMs/0015_FortiClient%20and%20ADOMs.htm

QUESTION 24

Refer to the exhibit.



Name: Hourly Website Hits

Time Period: This Week

Devices: ● All Devices ○ Specify

Type: ● Single Report ○ Multiple Reports

□ Enable Schedule

□ Enable Notification

☑ Enable Auto-cache

Which two statements are true regarding enabling auto-cache on FortiAnalyzer? (Choose two.)

A. Report size will be optimized to conserve disk space on FortiAnalyzer.
B. Reports will be cached in the memory.
C. This feature is automatically enabled for scheduled reports.
D. Enabling auto-cache reduces report generation time for reports that require a long time to assemble datasets.

Answer: A,D
Section: (none)
Explanation
Explanation/Reference:
Reference: https://help.fortinet.com/fa/faz50hlp/56/5-6-2/FMG-FAZ/2300_Reports/0025_Auto-cache.htm

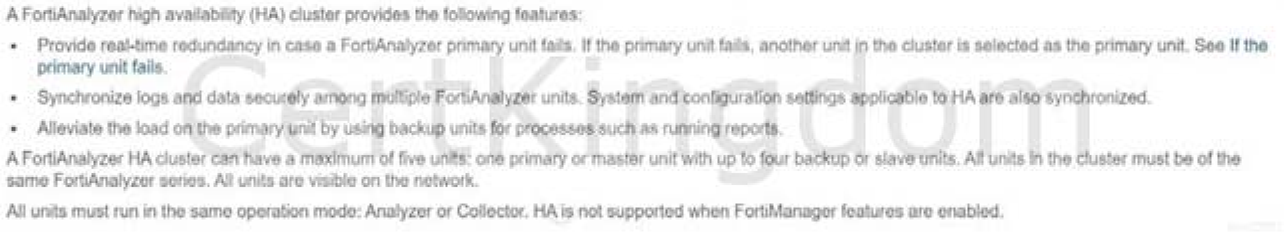
QUESTION 25

Which two statements are true regarding high availability (HA) on FortiAnalyzer? (Choose two.)

A. FortiAnalyzer HA can function without VRRP, and VRRP is required only if you have more than two FortiAnalyzer devices in a cluster.
B. FortiAnalyzer HA supports synchronization of logs as well as some system and configuration settings.
C. All devices in a FortiAnalyzer HA cluster must run in the same operation mode: analyzer or collector.
D. FortiAnalyzer HA implementation is supported by many public cloud infrastructures such as AWS, Microsoft Azure, and Google Cloud.

Answer: B,C
Section: (none)
Explanation
Explanation/Reference:
Reference: https://help.fortinet.com/fa/faz50hlp/60/6-0-2/Content/FMG-FAZ/4600_HA/0000_HA.htm?

TocPath=High%20Availability%7C_____0



A FortiAnalyzer high availability (HA) cluster provides the following features:

- Provide real-time redundancy in case a FortiAnalyzer primary unit fails. If the primary unit fails, another unit in the cluster is selected as the primary unit. See If the primary unit fails.
- Synchronize logs and data securely among multiple FortiAnalyzer units. System and configuration settings applicable to HA are also synchronized.
- Alleviate the load on the primary unit by using backup units for processes such as running reports.

A FortiAnalyzer HA cluster can have a maximum of five units: one primary or master unit with up to four backup or slave units. All units in the cluster must be of the same FortiAnalyzer series. All units are visible on the network.

All units must run in the same operation mode: Analyzer or Collector. HA is not supported when FortiManager features are enabled.

QUESTION 26

An administrator has moved FortiGate A from the root ADOM to ADOM1.
Which two statements are true regarding logs? (Choose two.)

A. Analytics logs will be moved to ADOM1 from the root ADOM automatically.
B. Archived logs will be moved to ADOM1 from the root ADOM automatically.
C. Logs will be presented in both ADOMs immediately after the move.
D. Analytics logs will be moved to ADOM1 from the root ADOM after you rebuild the ADOM1 SQL database.

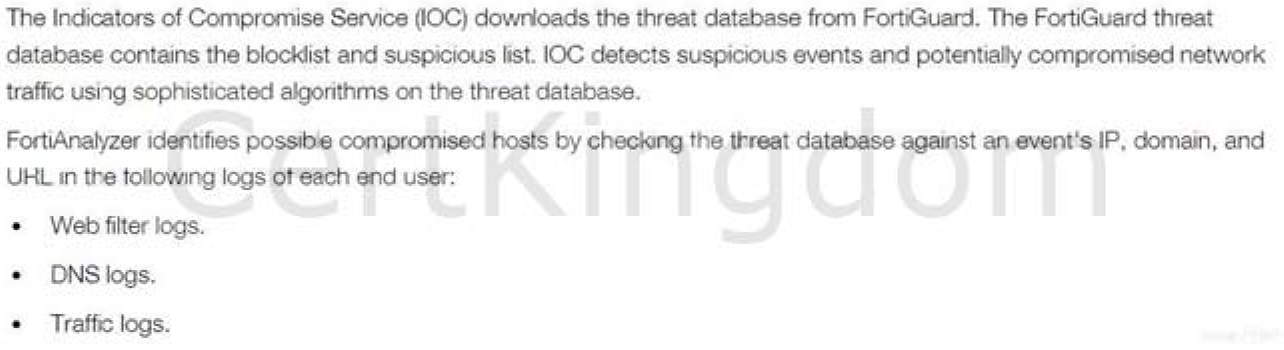
Answer: B,C
Section: (none)
Explanation
Explanation/Reference:
Reference: https://community.fortinet.com/t5/Fortinet-Forum/FW-Migration-between-ADOMs/m-p/32683?m=158008

QUESTION 27

What two things should an administrator do to view Compromised Hosts on FortiAnalyzer? (Choose two.)

A. Enable web filtering in firewall policies on FortiGate devices, and make sure these logs are sent to FortiAnalyzer.
B. Enable device detection on an interface on the FortiGate devices that are connected to the FortiAnalyzer.
C. Subscribe FortiAnalyzer to FortiGuard to keep its local threat database up-to-date.
D. Make sure all endpoints are reachable by FortiAnalyzer.

Answer: A,C
Section: (none)
Explanation
Explanation/Reference:
Reference: https://docs.fortinet.com/document/fortianalyzer/6.4.0/administration-guide/137635/viewingcompromised-hosts



The Indicators of Compromise Service (IOC) downloads the threat database from FortiGuard. The FortiGuard threat database contains the blocklist and suspicious list. IOC detects suspicious events and potentially compromised network traffic using sophisticated algorithms on the threat database.

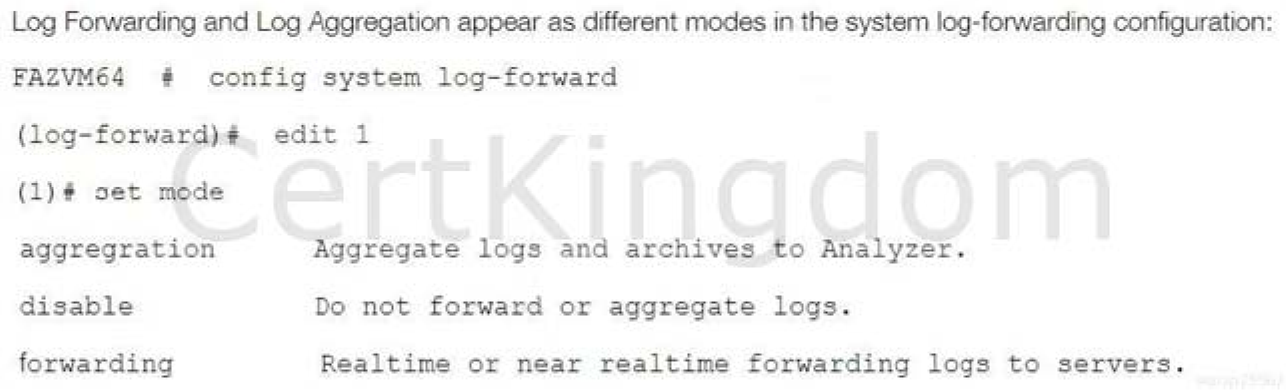
FortiAnalyzer identifies possible compromised hosts by checking the threat database against an event's IP, domain, and URL in the following logs of each end user:

- Web filter logs.
- DNS logs.
- Traffic logs.

QUESTION 28
How are logs forwarded when FortiAnalyzer is configured to use aggregation mode?

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

Answer: D
Section: (none)
Explanation
Explanation/Reference:
Reference: https://docs.fortinet.com/document/fortianalyzer/6.2.0/cookbook/63238/what-is-the-differencebetween-
log-forward-and-log-aggregation-modes



Log Forwarding and Log Aggregation appear as different modes in the system log-forwarding configuration:

```
FAZVM64  #  config system log-forward

(log-forward)#  edit 1

(1)# set mode

aggregration       Aggregate logs and archives to Analyzer.

disable            Do not forward or aggregate logs.

forwarding         Realtime or near realtime forwarding logs to servers.
```

QUESTION 29
In Log View, you can use the Chart Builder feature to build a dataset and chart based on the filtered search results.
Similarly, which feature you can use for FortiView?

A. Export to Report Chart
B. Export to PDF
C. Export to Chart Builder
D. Export to Custom Chart

Answer: A
Section: (none)
Explanation
Explanation/Reference:
Reference: https://community.fortinet.com/t5/FortiAnalyzer/Creating-a-Custom-report-from-FortiView-Exportto-
Report-Chart/ta-p/190154?externalID=FD40483

QUESTION 30
What can you do on FortiAnalyzer to restrict administrative access from specific locations?

A. Configure trusted hosts for that administrator.
B. Enable geo-location services on accessible interface.
C. Configure two-factor authentication with a remote RADIUS server.
D. Configure an ADOM for respective location.

Answer: A

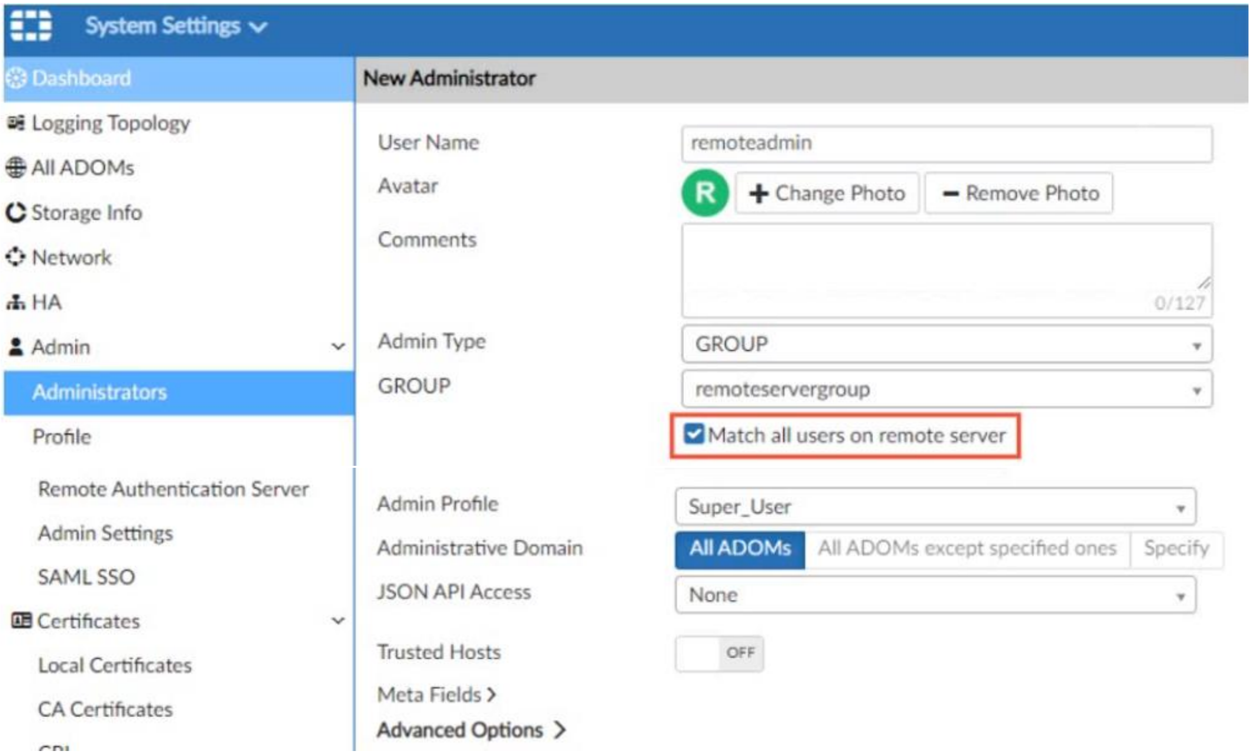
Section: (none)

Explanation

Explanation/Reference:

Reference: https://docs.fortinet.com/document/fortigate/6.2.0/hardening-your-fortigate/582009/systemadministrator-
best-practices

best-practices



New Administrator

User Name	remoteadmin
Avatar	R
Comments	
Admin Type	GROUP
GROUP	remoteservergroup
	☑ Match all users on remote server
Admin Profile	Super_User
Administrative Domain	[✓ All ADOMs] All ADOMs except specified ones Specify
JSON API Access	None
Trusted Hosts	OFF

Refer to the exhibit.

The exhibit shows “remoteservergroup” is an authentication server group with LDAP and RADIUS servers.

Which two statements express the significance of enabling **Match all users on remote server** when configuring a new administrator? (Choose two.)

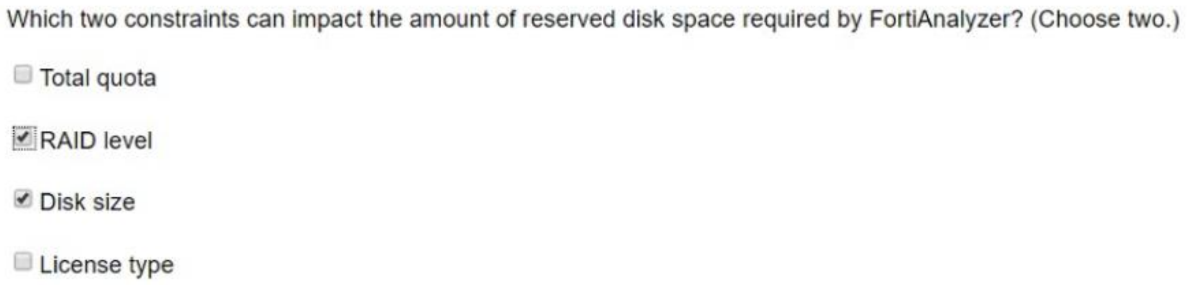
☑ It creates a wildcard administrator using LDAP and RADIUS servers.

☐ User **remoteadmin** from LDAP and RADIUS servers will be able to log in to FortiAnalyzer at any time.

☑ Administrators can log in to FortiAnalyzer using their credentials on remote severs LDAP and RADIUS.

☐ It allows administrators to use two-factor authentication.

NSE5 FAZ 6.4 Real Exam Questions



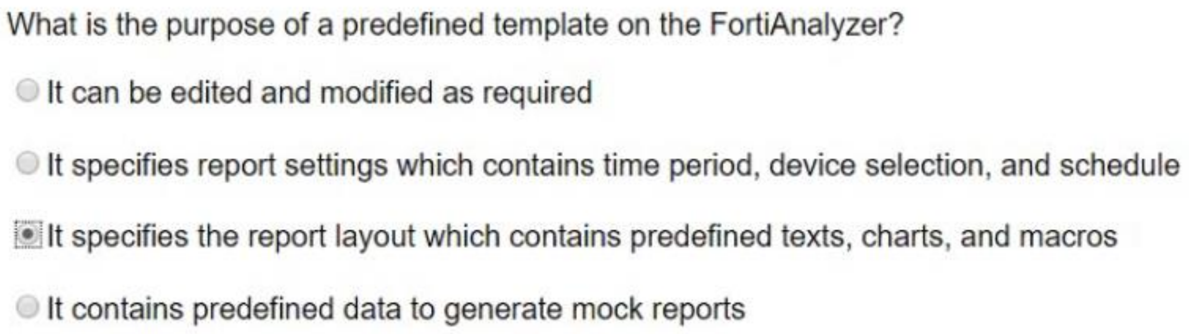
Which two constraints can impact the amount of reserved disk space required by FortiAnalyzer? (Choose two.)

☐ Total quota

☑ RAID level

☑ Disk size

☐ License type



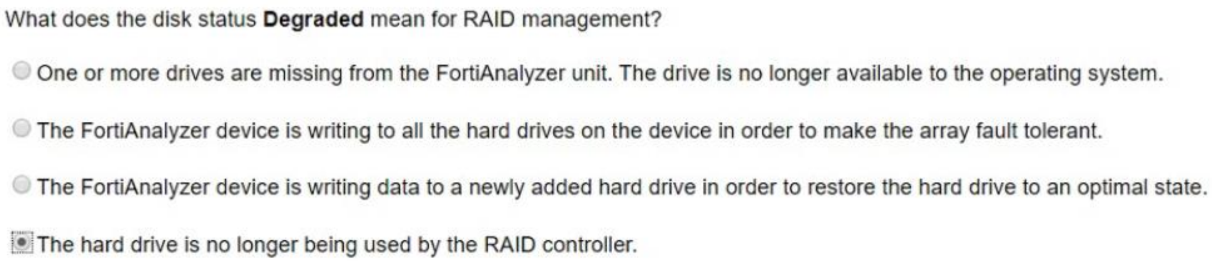
What is the purpose of a predefined template on the FortiAnalyzer?

○ It can be edited and modified as required

○ It specifies report settings which contains time period, device selection, and schedule

● It specifies the report layout which contains predefined texts, charts, and macros

○ It contains predefined data to generate mock reports



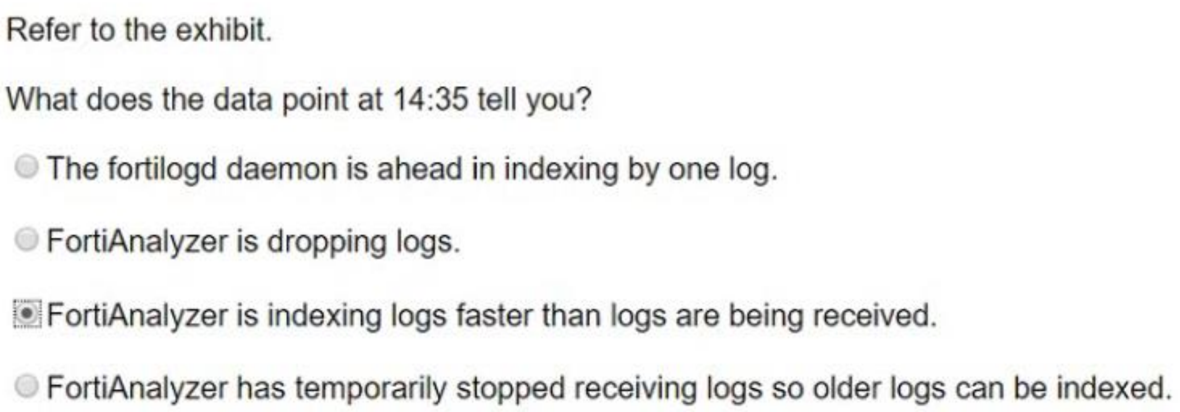
What does the disk status **Degraded** mean for RAID management?

○ One or more drives are missing from the FortiAnalyzer unit. The drive is no longer available to the operating system.

○ The FortiAnalyzer device is writing to all the hard drives on the device in order to make the array fault tolerant.

○ The FortiAnalyzer device is writing data to a newly added hard drive in order to restore the hard drive to an optimal state.

● The hard drive is no longer being used by the RAID controller.



Refer to the exhibit.

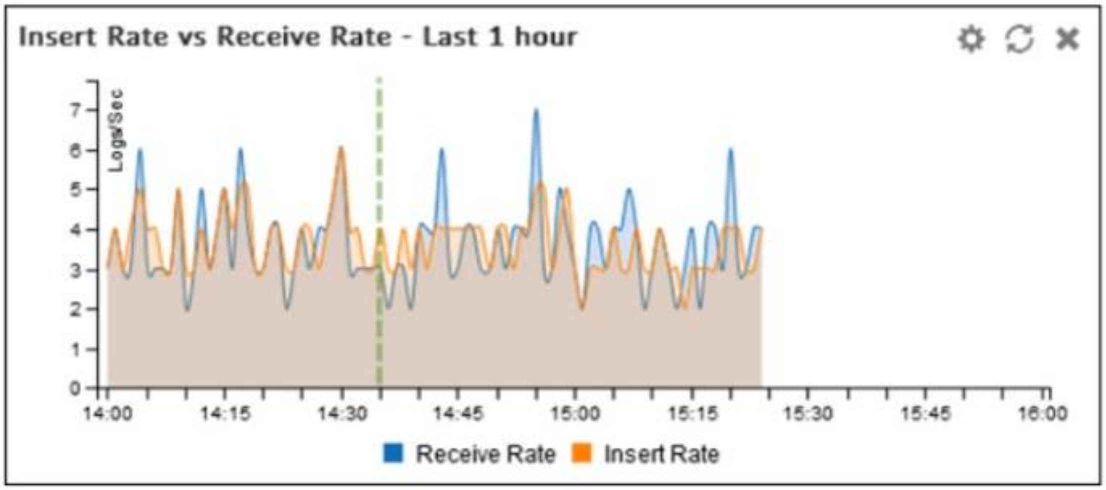
What does the data point at 14:35 tell you?

○ The fortilogd daemon is ahead in indexing by one log.

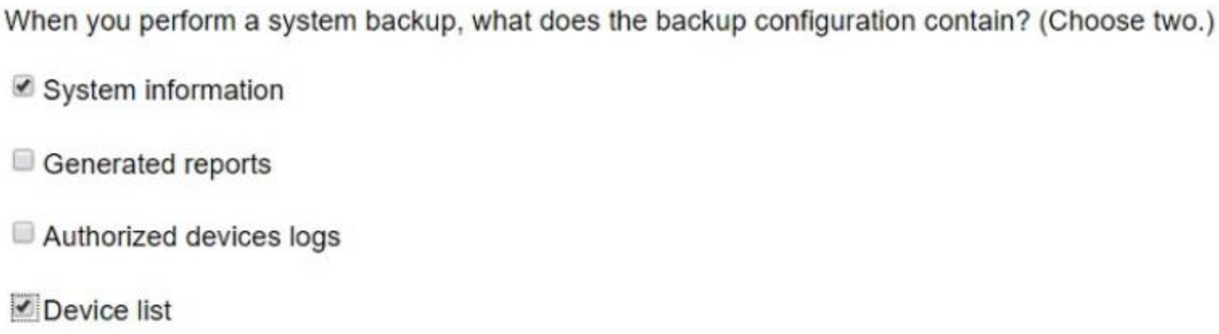
○ FortiAnalyzer is dropping logs.

● FortiAnalyzer is indexing logs faster than logs are being received.

○ FortiAnalyzer has temporarily stopped receiving logs so older logs can be indexed.



NSE5 FAZ 6.4 Real Exam Questions



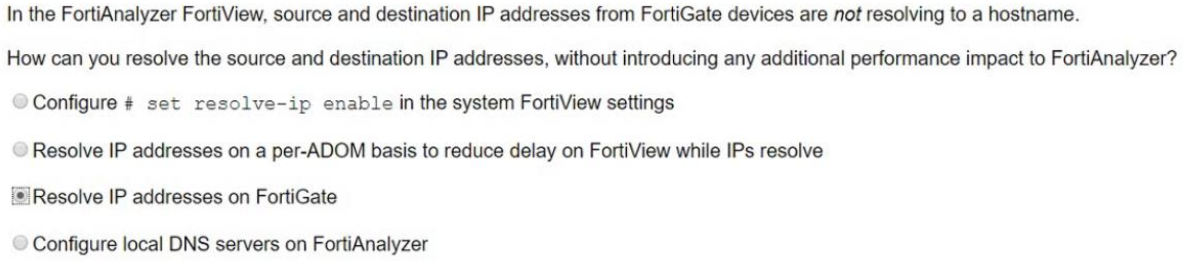
When you perform a system backup, what does the backup configuration contain? (Choose two.)

☑ System information

□ Generated reports

□ Authorized devices logs

☑ Device list



In the FortiAnalyzer FortiView, source and destination IP addresses from FortiGate devices are *not* resolving to a hostname.

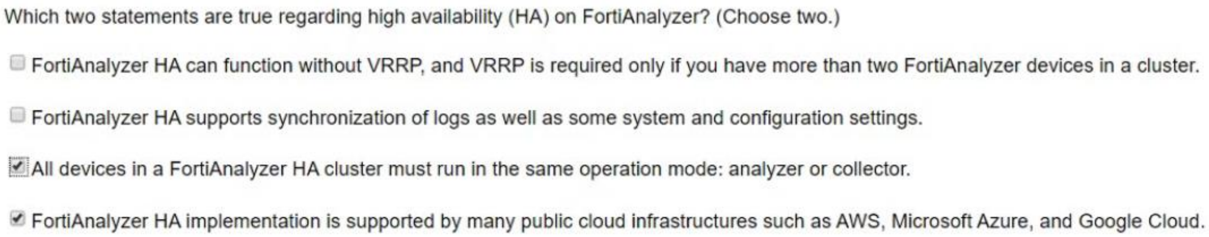
How can you resolve the source and destination IP addresses, without introducing any additional performance impact to FortiAnalyzer?

○ Configure `# set resolve-ip enable` in the system FortiView settings

○ Resolve IP addresses on a per-ADOM basis to reduce delay on FortiView while IPs resolve

● Resolve IP addresses on FortiGate

○ Configure local DNS servers on FortiAnalyzer



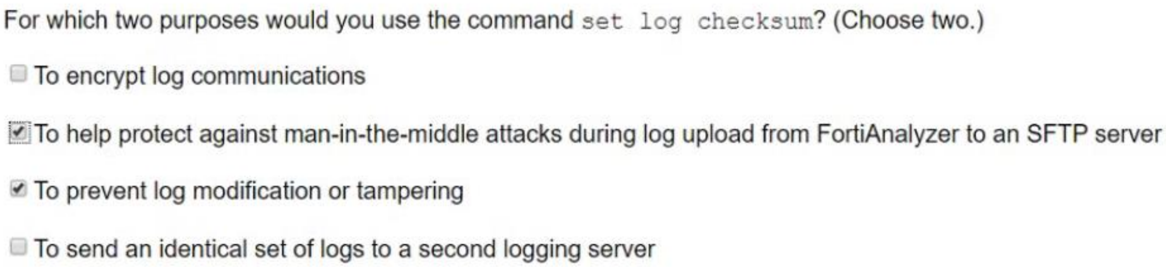
Which two statements are true regarding high availability (HA) on FortiAnalyzer? (Choose two.)

□ FortiAnalyzer HA can function without VRRP, and VRRP is required only if you have more than two FortiAnalyzer devices in a cluster.

□ FortiAnalyzer HA supports synchronization of logs as well as some system and configuration settings.

☑ All devices in a FortiAnalyzer HA cluster must run in the same operation mode: analyzer or collector.

☑ FortiAnalyzer HA implementation is supported by many public cloud infrastructures such as AWS, Microsoft Azure, and Google Cloud.



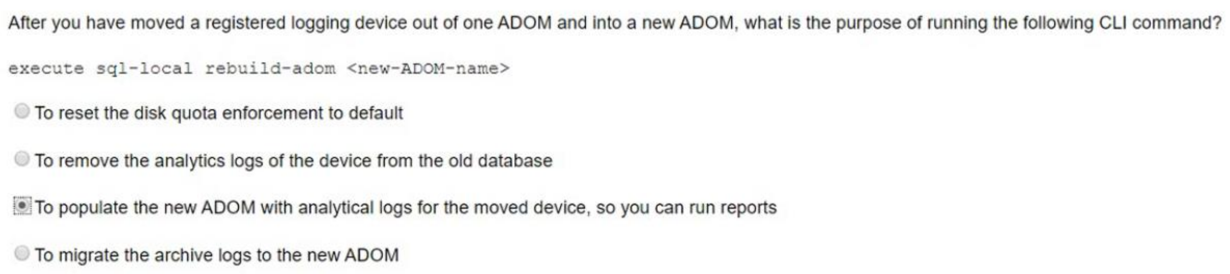
For which two purposes would you use the command `set log checksum`? (Choose two.)

□ To encrypt log communications

☑ To help protect against man-in-the-middle attacks during log upload from FortiAnalyzer to an SFTP server

☑ To prevent log modification or tampering

□ To send an identical set of logs to a second logging server



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?

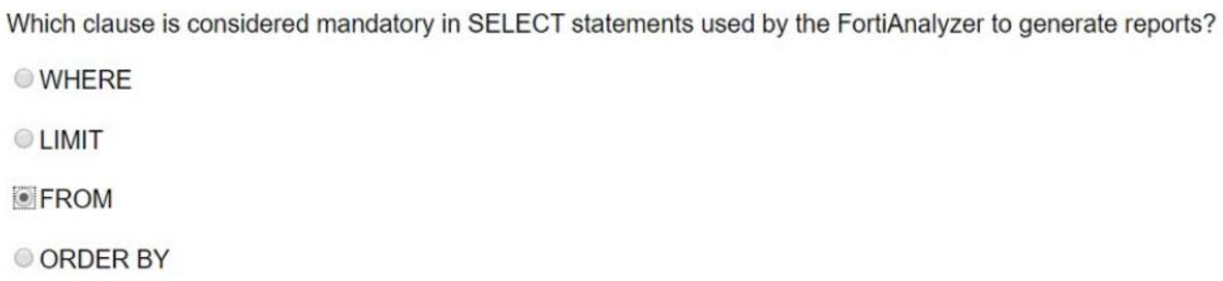
```
execute sql-local rebuild-adom <new-ADOM-name>
```

○ To reset the disk quota enforcement to default

○ To remove the analytics logs of the device from the old database

● To populate the new ADOM with analytical logs for the moved device, so you can run reports

○ To migrate the archive logs to the new ADOM



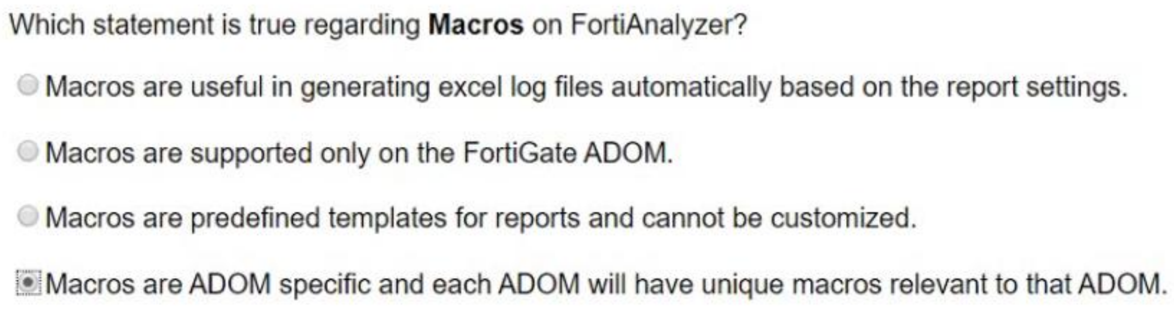
Which clause is considered mandatory in SELECT statements used by the FortiAnalyzer to generate reports?

○ WHERE

○ LIMIT

● FROM

○ ORDER BY



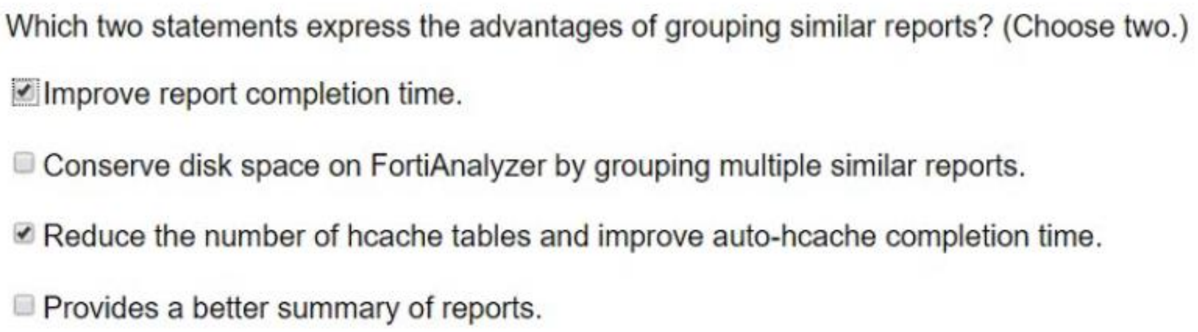
Which statement is true regarding **Macros** on FortiAnalyzer?

○ Macros are useful in generating excel log files automatically based on the report settings.

○ Macros are supported only on the FortiGate ADOM.

○ Macros are predefined templates for reports and cannot be customized.

● Macros are ADOM specific and each ADOM will have unique macros relevant to that ADOM.



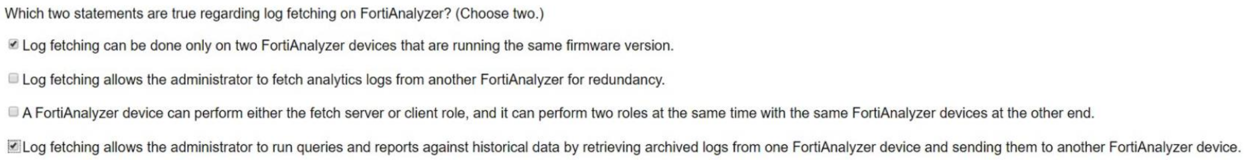
Which two statements express the advantages of grouping similar reports? (Choose two.)

☑ Improve report completion time.

□ Conserve disk space on FortiAnalyzer by grouping multiple similar reports.

☑ Reduce the number of hcache tables and improve auto-hcache completion time.

□ Provides a better summary of reports.



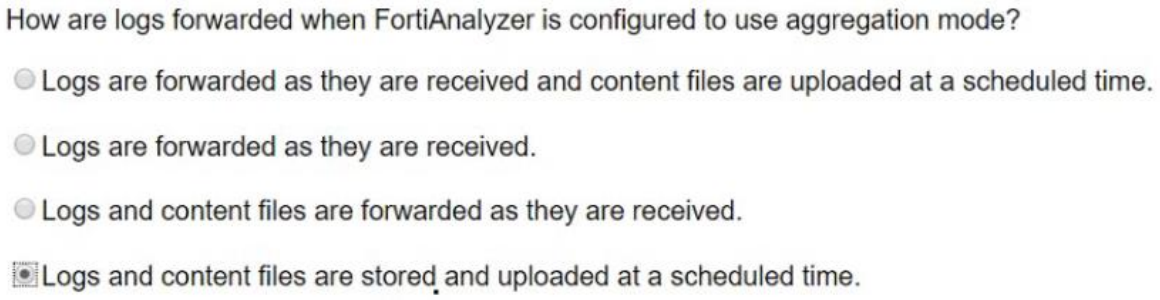
Which two statements are true regarding log fetching on FortiAnalyzer? (Choose two.)

☑ Log fetching can be done only on two FortiAnalyzer devices that are running the same firmware version.

□ Log fetching allows the administrator to fetch analytics logs from another FortiAnalyzer for redundancy.

□ A FortiAnalyzer device can perform either the fetch server or client role, and it can perform two roles at the same time with the same FortiAnalyzer devices at the other end.

☑ Log fetching allows the administrator to run queries and reports against historical data by retrieving archived logs from one FortiAnalyzer device and sending them to another FortiAnalyzer device.



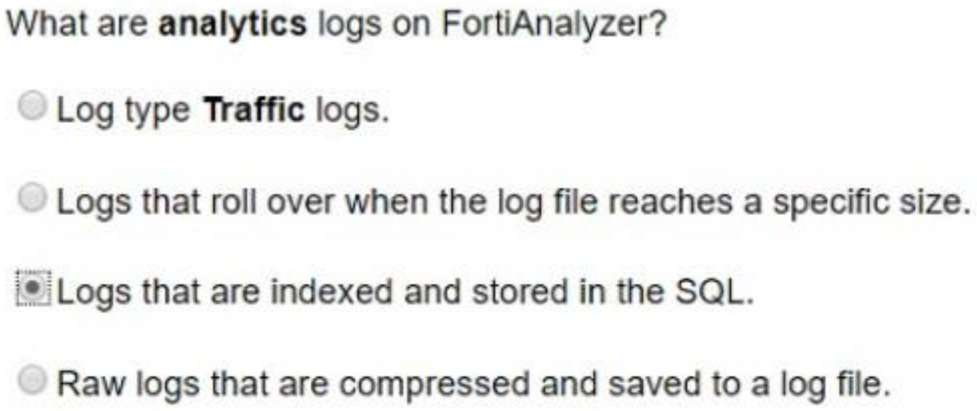
How are logs forwarded when FortiAnalyzer is configured to use aggregation mode?

○ Logs are forwarded as they are received and content files are uploaded at a scheduled time.

○ Logs are forwarded as they are received.

○ Logs and content files are forwarded as they are received.

● Logs and content files are stored and uploaded at a scheduled time.



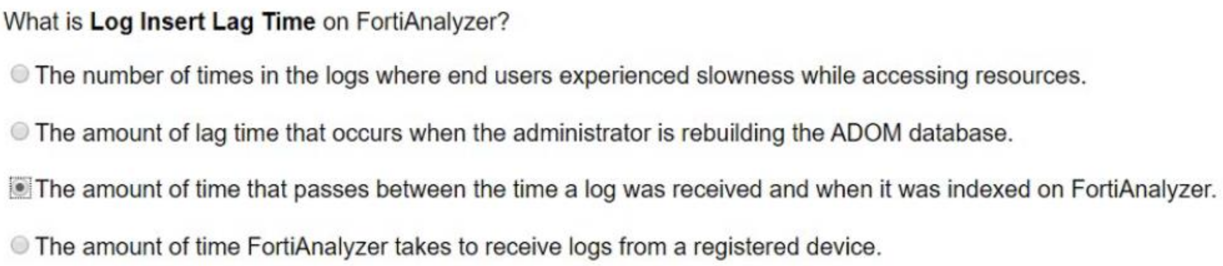
What are **analytics** logs on FortiAnalyzer?

○ Log type **Traffic** logs.

○ Logs that roll over when the log file reaches a specific size.

● Logs that are indexed and stored in the SQL.

○ Raw logs that are compressed and saved to a log file.



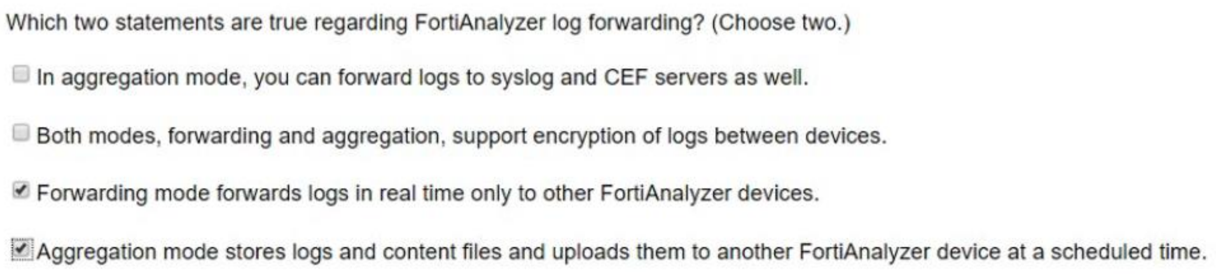
What is **Log Insert Lag Time** on FortiAnalyzer?

○ The number of times in the logs where end users experienced slowness while accessing resources.

○ The amount of lag time that occurs when the administrator is rebuilding the ADOM database.

● The amount of time that passes between the time a log was received and when it was indexed on FortiAnalyzer.

○ The amount of time FortiAnalyzer takes to receive logs from a registered device.



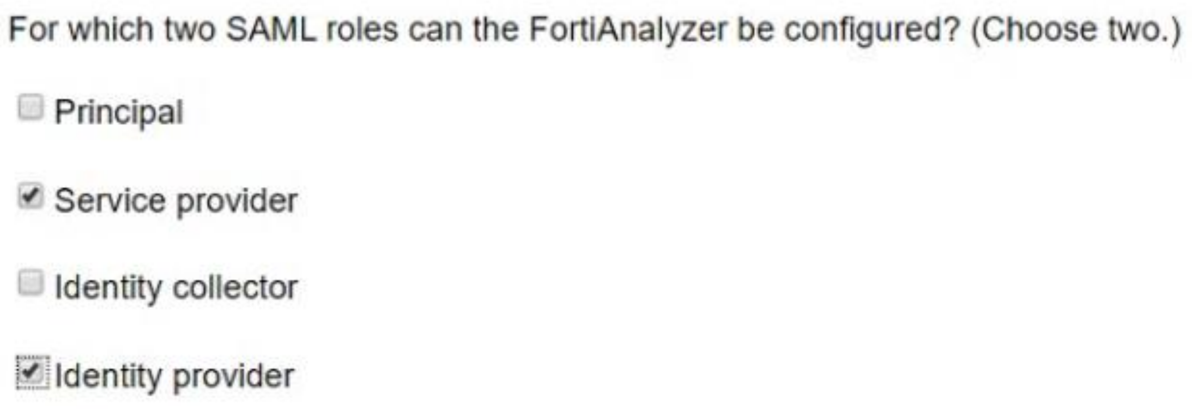
Which two statements are true regarding FortiAnalyzer log forwarding? (Choose two.)

□ In aggregation mode, you can forward logs to syslog and CEF servers as well.

□ Both modes, forwarding and aggregation, support encryption of logs between devices.

☑ Forwarding mode forwards logs in real time only to other FortiAnalyzer devices.

☑ Aggregation mode stores logs and content files and uploads them to another FortiAnalyzer device at a scheduled time.



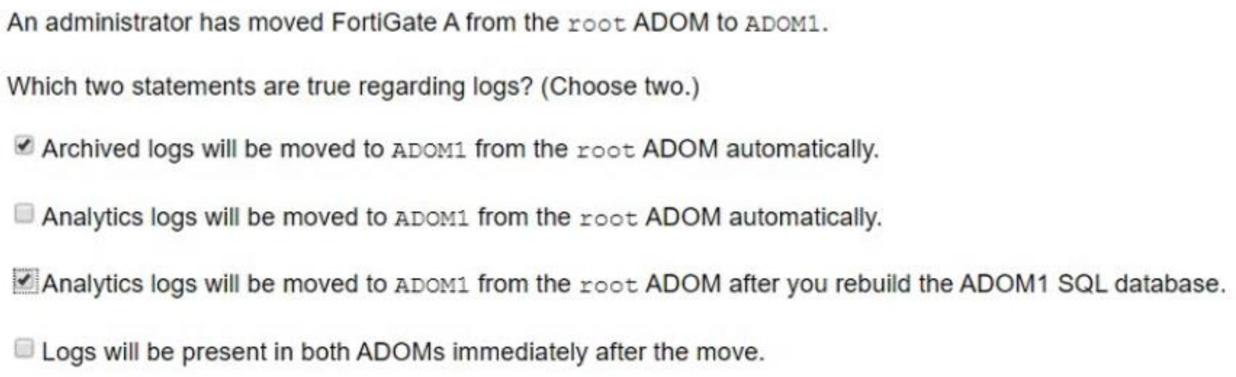
For which two SAML roles can the FortiAnalyzer be configured? (Choose two.)

□ Principal

☑ Service provider

□ Identity collector

☑ Identity provider



An administrator has moved FortiGate A from the `root` ADOM to `ADOM1`.

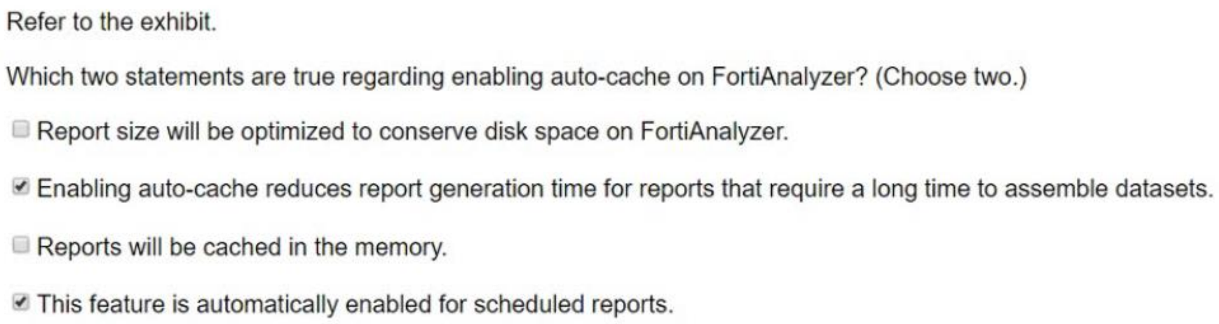
Which two statements are true regarding logs? (Choose two.)

☑ Archived logs will be moved to `ADOM1` from the `root` ADOM automatically.

□ Analytics logs will be moved to `ADOM1` from the `root` ADOM automatically.

☑ Analytics logs will be moved to `ADOM1` from the `root` ADOM after you rebuild the ADOM1 SQL database.

□ Logs will be present in both ADOMs immediately after the move.



Refer to the exhibit.

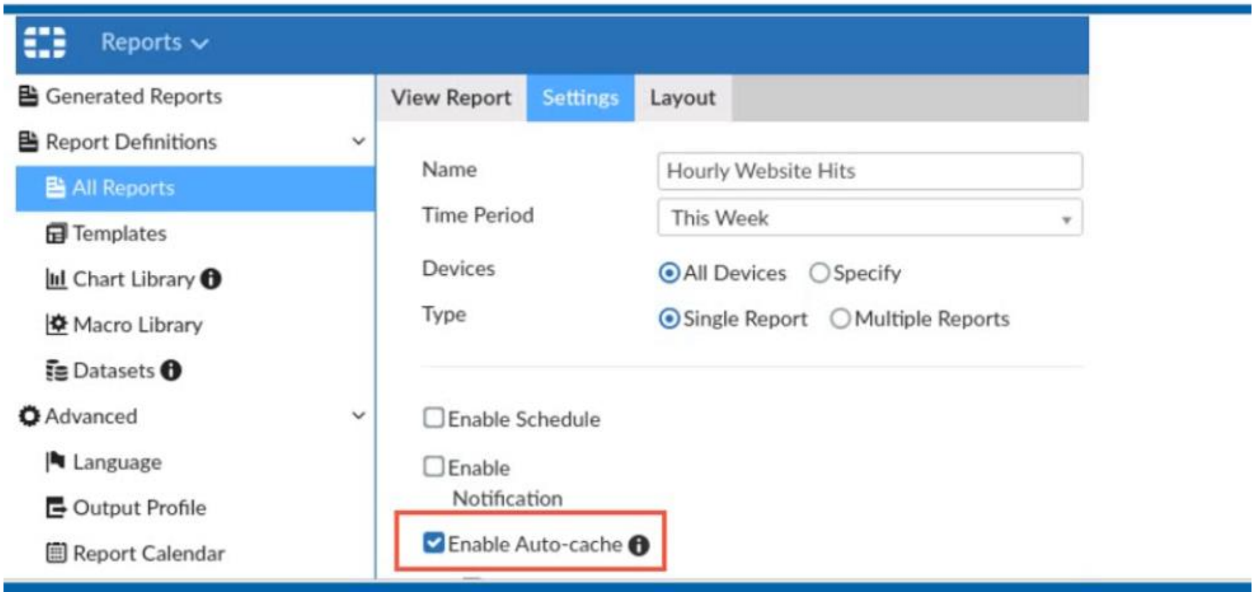
Which two statements are true regarding enabling auto-cache on FortiAnalyzer? (Choose two.)

□ Report size will be optimized to conserve disk space on FortiAnalyzer.

☑ Enabling auto-cache reduces report generation time for reports that require a long time to assemble datasets.

□ Reports will be cached in the memory.

☑ This feature is automatically enabled for scheduled reports.



Name: Hourly Website Hits

Time Period: This Week

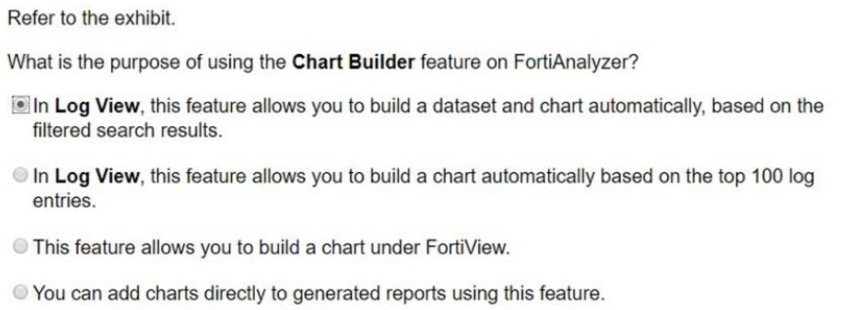
Devices: ● All Devices ○ Specify

Type: ● Single Report ○ Multiple Reports

□ Enable Schedule

□ Enable Notification

☑ Enable Auto-cache



Refer to the exhibit.

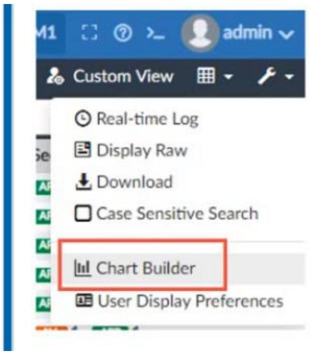
What is the purpose of using the **Chart Builder** feature on FortiAnalyzer?

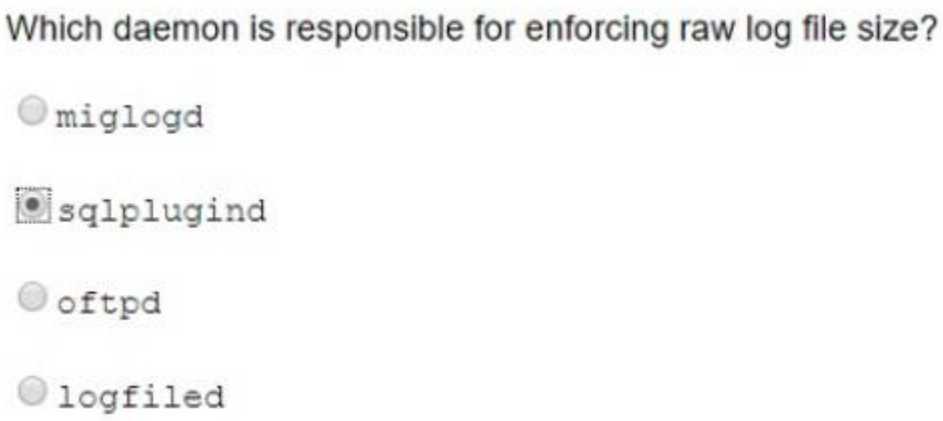
● In **Log View**, this feature allows you to build a dataset and chart automatically, based on the filtered search results.

○ In **Log View**, this feature allows you to build a chart automatically based on the top 100 log entries.

○ This feature allows you to build a chart under FortiView.

○ You can add charts directly to generated reports using this feature.





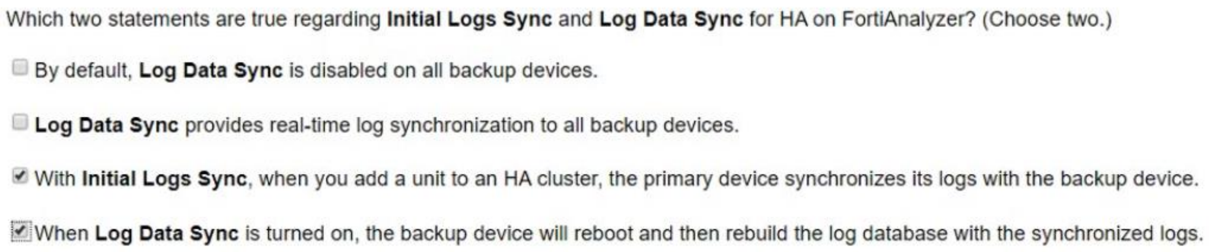
Which daemon is responsible for enforcing raw log file size?

○ `miglogd`

● `sqlplugind`

○ `oftpd`

○ `logfiled`



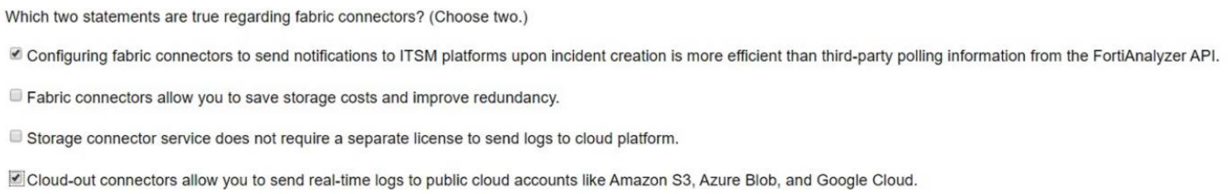
Which two statements are true regarding **Initial Logs Sync** and **Log Data Sync** for HA on FortiAnalyzer? (Choose two.)

□ By default, **Log Data Sync** is disabled on all backup devices.

□ **Log Data Sync** provides real-time log synchronization to all backup devices.

☑ With **Initial Logs Sync**, when you add a unit to an HA cluster, the primary device synchronizes its logs with the backup device.

☑ When **Log Data Sync** is turned on, the backup device will reboot and then rebuild the log database with the synchronized logs.



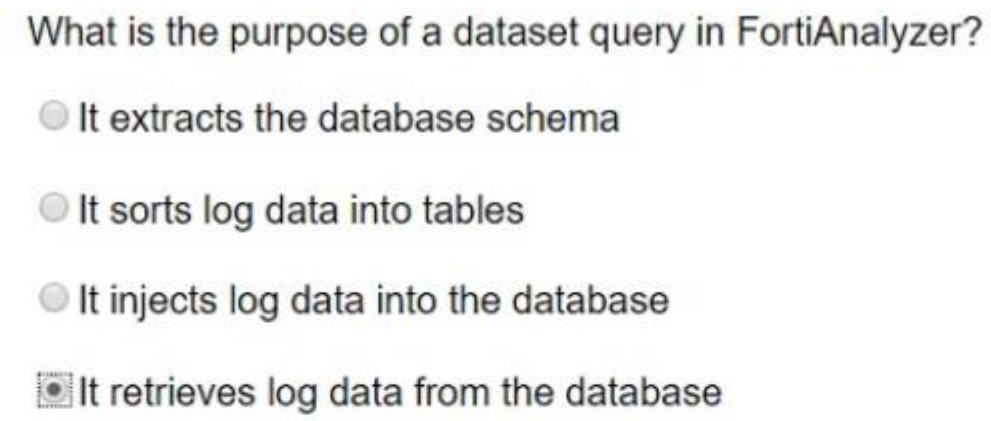
Which two statements are true regarding fabric connectors? (Choose two.)

☑ Configuring fabric connectors to send notifications to ITSM platforms upon incident creation is more efficient than third-party polling information from the FortiAnalyzer API.

□ Fabric connectors allow you to save storage costs and improve redundancy.

□ Storage connector service does not require a separate license to send logs to cloud platform.

☑ Cloud-out connectors allow you to send real-time logs to public cloud accounts like Amazon S3, Azure Blob, and Google Cloud.



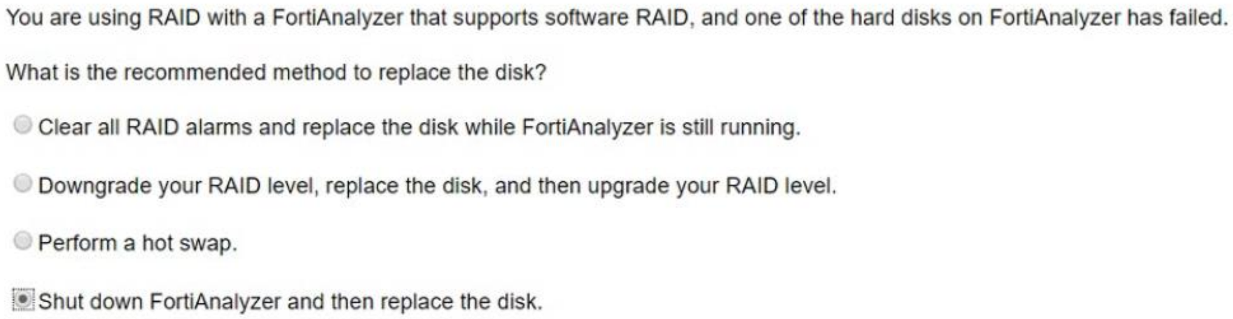
What is the purpose of a dataset query in FortiAnalyzer?

○ It extracts the database schema

○ It sorts log data into tables

○ It injects log data into the database

● It retrieves log data from the database



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?

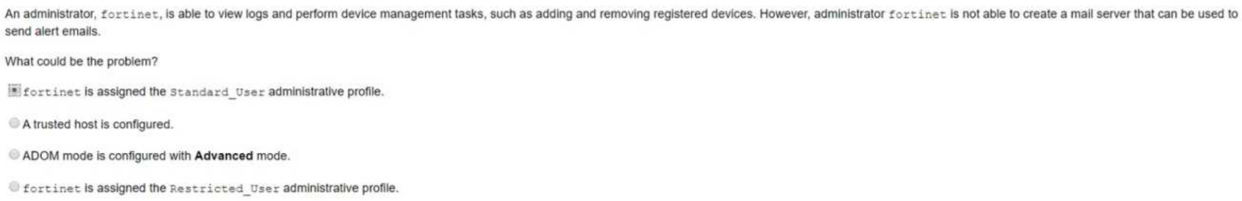
○ Clear all RAID alarms and replace the disk while FortiAnalyzer is still running.

○ Downgrade your RAID level, replace the disk, and then upgrade your RAID level.

○ Perform a hot swap.

● Shut down FortiAnalyzer and then replace the disk.

NSE5 FAZ 6.4 Real Exam Questions



An administrator, `fortinet`, is able to view logs and perform device management tasks, such as adding and removing registered devices. However, administrator `fortinet` is not able to create a mail server that can be used to send alert emails.

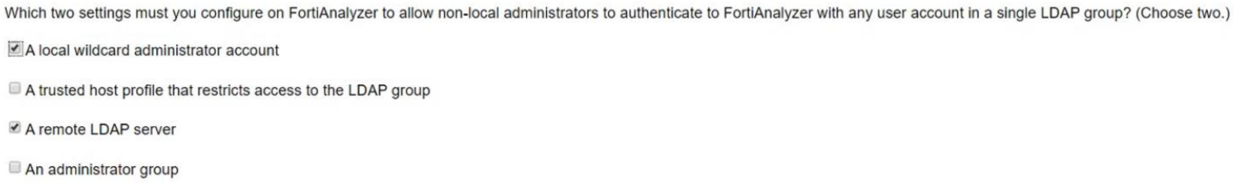
What could be the problem?

● `fortinet` is assigned the `Standard_User` administrative profile.

○ A trusted host is configured.

○ ADOM mode is configured with **Advanced** mode.

○ `fortinet` is assigned the `Restricted_User` administrative profile.



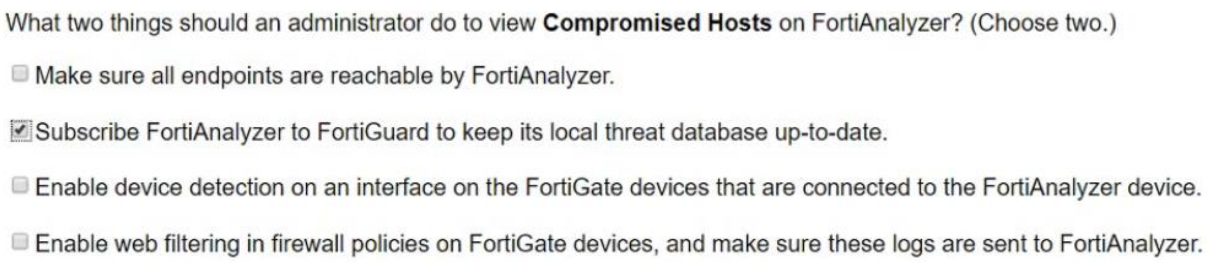
Which two settings must you configure on FortiAnalyzer to allow non-local administrators to authenticate to FortiAnalyzer with any user account in a single LDAP group? (Choose two.)

☑ A local wildcard administrator account

□ A trusted host profile that restricts access to the LDAP group

☑ A remote LDAP server

□ An administrator group



What two things should an administrator do to view **Compromised Hosts** on FortiAnalyzer? (Choose two.)

□ Make sure all endpoints are reachable by FortiAnalyzer.

☑ Subscribe FortiAnalyzer to FortiGuard to keep its local threat database up-to-date.

□ Enable device detection on an interface on the FortiGate devices that are connected to the FortiAnalyzer device.

□ Enable web filtering in firewall policies on FortiGate devices, and make sure these logs are sent to FortiAnalyzer.