Fortinet.Premium.NSE5_FAZ-6.4 .94q

Number: NSE5_FAZ-6.4
Passing Score: 800
Time Limit: 120 min
File Version: 1.7

Exam Code: NSE5_FAZ-6.4
Exam Name: Fortinet NSE 5 - FortiAnalyzer 6.4
Website: https://VCEup.com/
Free Exam: https://vceup.com

QUESTION 1
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

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://docs2.fortinet.com/document/fortianalyzer/6.0.0/administrationguide/219292/administrator-profiles
https://docs2.fortinet.com/document/fortianalyzer/6.0.0/administration-guide/581222/trustedhosts

QUESTION 2
Which daemon is responsible for enforcing raw log file size?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 3
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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://docs.fortinet.com/document/fortianalyzer/6.4.6/administrationguide/410387/appendix-b-log-integrity-and-secure-log-transfer

QUESTION 4
Which two of the following must you configure on FortiAnalyzer to email a FortiAnalyzer report externally?
(Choose two.)

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

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://docs.fortinet.com/document/fortianalyzer/6.0.2/administrationguide/598322/creating-output-profiles

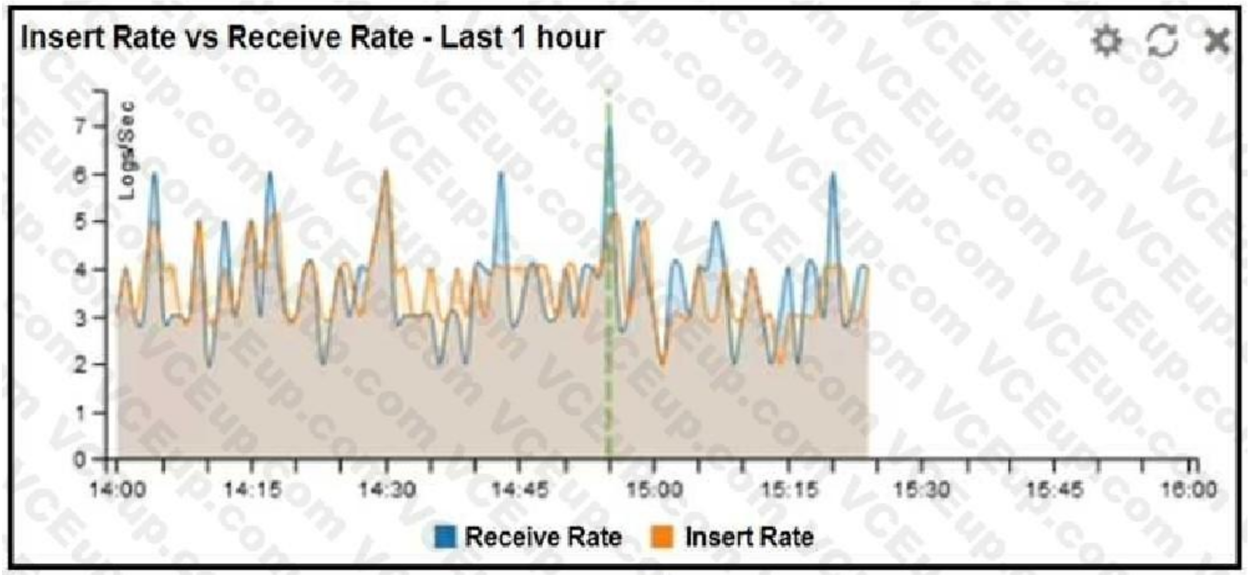
QUESTION 5
For which two purposes would you use the command set log checksum? (Choose two.)

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

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 6
Refer to the exhibit.



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

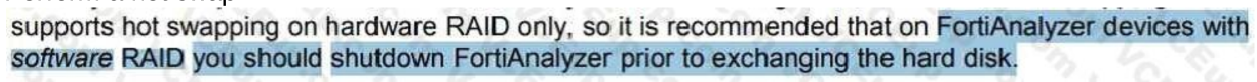
A. The received rate is almost at its maximum for this device
B. The sqlplugind daemon is behind in log indexing by two logs
C. Logs are being dropped
D. Raw logs are reaching FortiAnalyzer faster than they can be indexed

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 7
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



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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
https://community.fortinet.com/t5/FortiAnalyzer/Technical-Note-How-to-swap-Hard-Disk-on-FortiAnalyzer/tap/194997?externalID=FD41397#:~:text=If%20a%20hard%20disk%20on,process%20known%20as%20hot%20swapping

QUESTION 8
On the RAID management page, the disk status is listed as Initializing.
What does the status Initializing indicate about what the FortiAnalyzer is currently doing?

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

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 9
In the FortiAnalyzer FortiView, source and destination IP addresses from FortiGate devices are not resolving to a hostname.
How can you resolve the source and destination IP addresses, without introducing any additional performance impact to FortiAnalyzer?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
https://packetplant.com/fortigate-and-fortianalyzer-resolve-source-and-destination-ip/“As a best practice, it is recommended to resolve IPs on the FortiGate end. This is because you getboth source and destination, and it offloads the work from FortiAnalyzer. On FortiAnalyzer, this IPresolution does destination IPs only”

QUESTION 10
You have recently grouped multiple FortiGate devices into a single ADOM. System Settings > Storage Info shows the quota used.
What does the disk quota refer to?

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

D. The maximum disk utilization for all devices in the ADOM

Correct Answer: D
Section: (none)
Explanation

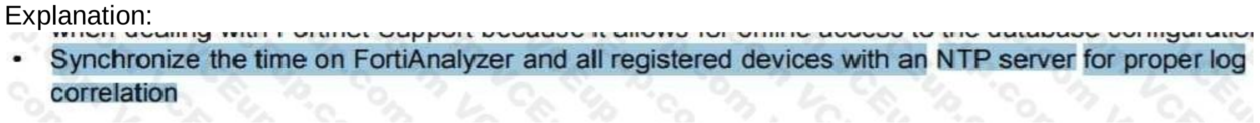
Explanation/Reference:
Explanation:

QUESTION 11
Why should you use an NTP server on FortiAnalyzer and all registered devices that log into FortiAnalyzer?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:



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

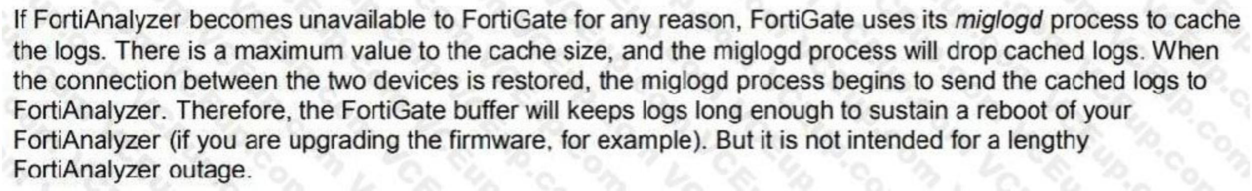
- Synchronize the time on FortiAnalyzer and all registered devices with an NTP server for proper log correlation

QUESTION 12
You need to upgrade your FortiAnalyzer firmware.
What happens to the logs being sent to FortiAnalyzer from FortiGate during the time FortiAnalyzer is temporarily unavailable?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:



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

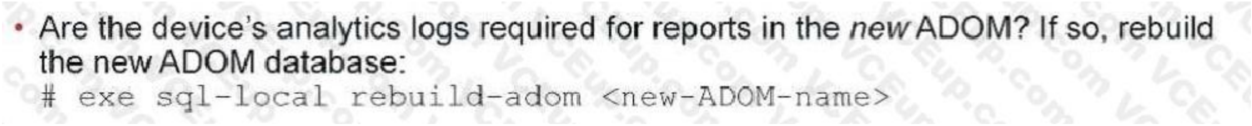
QUESTION 13
After you have moved a registered logging device out of one ADOM and into a new ADOM, what is the purpose of running the following CLI command? execute sql-local rebuild-adom <new-ADOM-name>

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

Correct Answer: D
Section: (none)

Explanation

Explanation/Reference:
Explanation:



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

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

QUESTION 14
If a hard disk fails on a FortiAnalyzer that supports software RAID, what should you do to bring the FortiAnalyzer back to functioning normally, without losing data?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
https://kb.fortinet.com/kb/documentLink.do?externalID=FD46446#:~:text=On%20FortiAnalyzer%2FFortiManager%20devices%20that,to%20exchanging%20the%20hard%20disk.
If a hard disk on a FortiAnalyzer unit fails, it must be replaced. On FortiAnalyzer devices that support hardware RAID, the hard disk can be replaced while the unit is still running – known as hot swapping.
On FortiAnalyzer units with software RAID, the device must be shutdown prior to exchanging the hard disk.
Reference: https://community.fortinet.com/t5/FortiAnalyzer/Technical-Note-How-to-swap-Hard-Disk-on-FortiAnalyzer/tap/194997?externalID=FD41397#:~:text=If%20a%20hard%20disk%20on,process%20known%20as%20hot%20swapping

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

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

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 16
FortiAnalyzer reports are dropping analytical data from 15 days ago, even though the data policy setting for analytics logs is 60 days.
What is the most likely problem?

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

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 17
Which log type does the FortiAnalyzer indicators of compromise feature use to identify infected hosts?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://help.fortinet.com/fa/faz50hlp/60/6-0-2/Content/
FortiAnalyzer_Admin_Guide/3600_FortiView/0200_Using_FortiView/1200_Compromised_hosts_pa ge.htm?
TocPath=FortiView%7CUsing%20FortiView%7C_____6

QUESTION 18
Which two settings must you configure on FortiAnalyzer to allow non-local administrators to authenticate to FortiAnalyzer with any user account in a single LDAP group? (Choose two.)

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

Correct Answer: AB
Section: (none)
Explanation

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

QUESTION 19
When you perform a system backup, what does the backup configuration contain? (Choose two.)

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

Correct Answer: BD
Section: (none)
Explanation

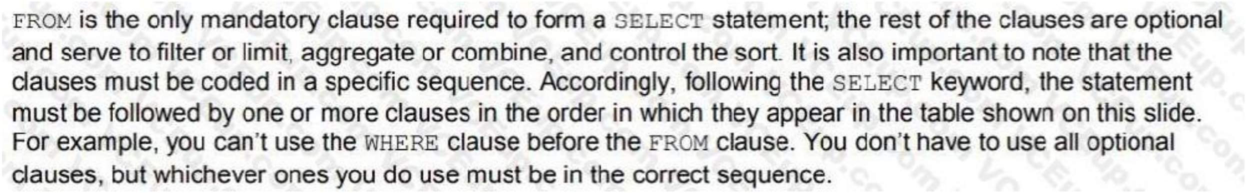
Explanation/Reference:
Explanation:
https://help.fortinet.com/fa/cli-olh/5-6-5/Content/Document/1400_execute/backup.htm
Reference: https://help.fortinet.com/fauth/5-2/Content/Admin%20Guides/5_2%20Admin%20Guide/300/301_Dashboard.htm

QUESTION 20
Which clause is considered mandatory in SELECT statements used by the FortiAnalyzer to generate reports?

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

Correct Answer: A
Section: (none)
Explanation

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



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

QUESTION 21
What is the purpose of a dataset query in FortiAnalyzer?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://docs2.fortinet.com/document/fortianalyzer/6.0.4/administrationguide/148744/creating-datasets

QUESTION 22
Logs are being deleted from one of the ADOMs earlier than the configured setting for archiving in the data policy.
What is the most likely problem?

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

Correct Answer: D
Section: (none)
Explanation

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

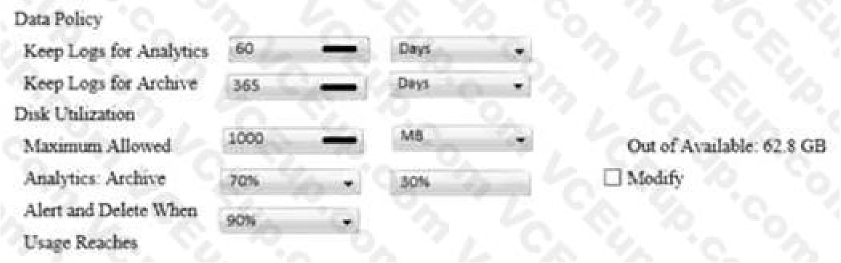
QUESTION 23
Which two constraints can impact the amount of reserved disk space required by FortiAnalyzer?
(Choose two.)

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

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/368682/disk-spaceallocation

QUESTION 24
View the exhibit:



Data Policy
Keep Logs for Analytics 60 Days
Keep Logs for Archive 365 Days
Disk Utilization
Maximum Allowed 1000 MB Out of Available: 62.8 GB
Analytics: Archive 70% 30% □ Modify
Alert and Delete When Usage Reaches 90%

What does the 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

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 25
You've 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 archive logs to the new ADOM.
C. FortiAnalyzer migrates analytics logs to the new ADOM.
D. FortiAnalyzer removes logs from the old ADOM.

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 26
What happens when a log file saved on FortiAnalyzer disks reaches the size specified in the device log settings?

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

Correct Answer: B
Section: (none)

Explanation

Explanation/Reference:
Explanation:
Reference: https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/6d9f8fb5-6cf4-11e9-81a4-00505692583a/FortiAnalyzer-6.0.5-Administration-Guide.pdf
https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/355632/log-browse

QUESTION 27
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

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 28
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
https://docs.fortinet.com/document/fortianalyzer/6.2.0/administration-guide/651442/fetchermanagement

QUESTION 29
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

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 30
How are logs forwarded when FortiAnalyzer is using aggregation mode?

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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
https://www.fortinetguru.com/2020/07/log-forwarding-fortianalyzer-fortios-6-2-3/
https://docs.fortinet.com/document/fortianalyzer/6.2.0/administration-guide/420493/modes
Reference: https://docs.fortinet.com/document/fortianalyzer/6.2.0/cookbook/63238/what-is-thedifference-between-log-forward-and-log-aggregation-modes

QUESTION 31
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/717578/assigningadministrators-to-an-adom

QUESTION 32
In order for FortiAnalyzer to collect logs from a FortiGate device, what configuration is required?
(Choose two.)

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

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Pg 70: “after you add and register a FortiGate device with the FortiAnalyzer unit, you must also ensure that the FortiGate device is configured to send logs to the FortiAnalyzer unit.”
https://docs.fortinet.com/uploaded/files/4614/FortiAnalyzer-5.4.6-Administration%20Guide.pdfPg 45: “ADOMs must be enabled to support the logging and reporting of NON-FORTIGATE devices,such as FortiCarrier, FortiClientEMS, FortiMail, FortiWeb, FortiCache, and FortiSandbox.”

QUESTION 33
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

Correct Answer: A
Section: (none)

Explanation

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

QUESTION 34
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
https://docs.fortinet.com/document/fortianalyzer/6.2.0/cookbook/989203/building-charts-withchart-builder

QUESTION 35
In FortiAnalyzer's FormView, source and destination IP addresses from FortiGate devices are not resolving to a hostname. How can you resolve the source and destination IPs, without introducing any additional performance impact to FortiAnalyzer?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

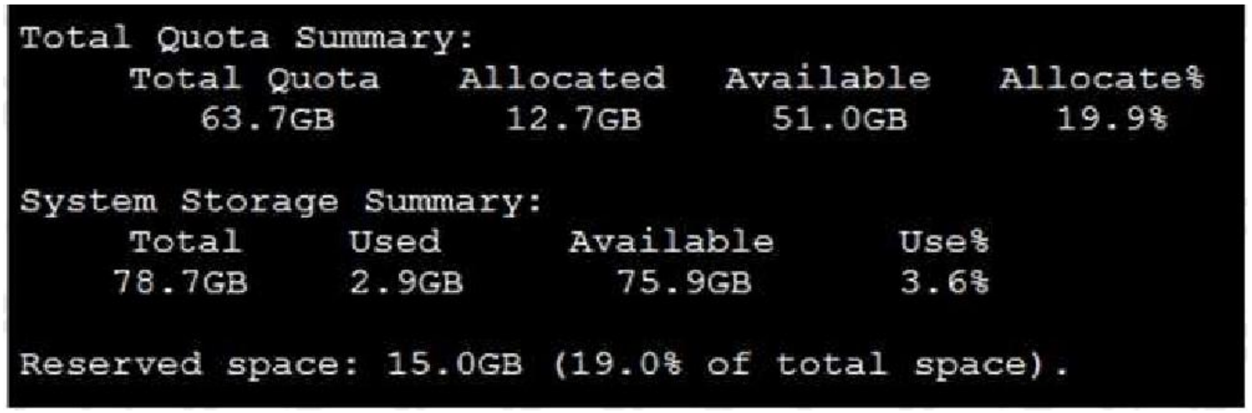
QUESTION 36
What must you configure on FortiAnalyzer to upload a FortiAnalyzer report to a supported external server?
(Choose two.)

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

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Explanation:
https://docs.fortinet.com/document/fortianalyzer/6.0.2/administration-guide/598322/creatingoutput-profiles

QUESTION 37
View 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. 3.6% of the system storage is already being used.
B. Some space is reserved for system use, such as storage of compression files, upload files, and temporary report files
C. The oftpd process has not archived the logs yet
D. The logfiled process is just estimating the total quota

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/368682/disk-spaceallocation

QUESTION 38
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

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://docs.fortinet.com/document/fortianalyzer/6.0.0/administrationguide/282280/enabling-autocache

QUESTION 39
If you upgrade your FortiAnalyzer firmware, what report elements can be affected?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 40
How does FortiAnalyzer retrieve specific log data from the database?

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

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 41
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

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 42
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 43
What FortiGate process caches logs when FortiAnalyzer is not reachable?

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

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 44
FortiAnalyzer uses the Optimized Fabric Transfer Protocok (OFTP) over SSL for what purpose?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 45
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

Correct Answer: C
Section: (none)
Explanation

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

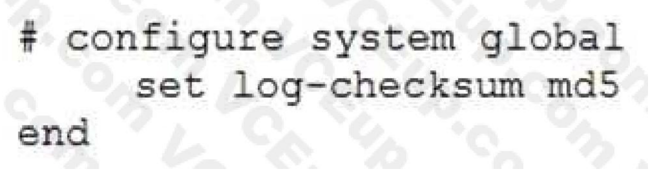
QUESTION 46
Logs are being deleted from one of your ADOMs earlier that the configured setting for archiving in your data policy. What is the most likely problem?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
https://help.fortinet.com/fmgr/50hlp/56/5-6-1/FMGFAZ/1100_Storage/0017_Deleted%20device%20logs.htm
https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/87802/automaticdeletion

QUESTION 47
What is the purpose of the following CLI command?



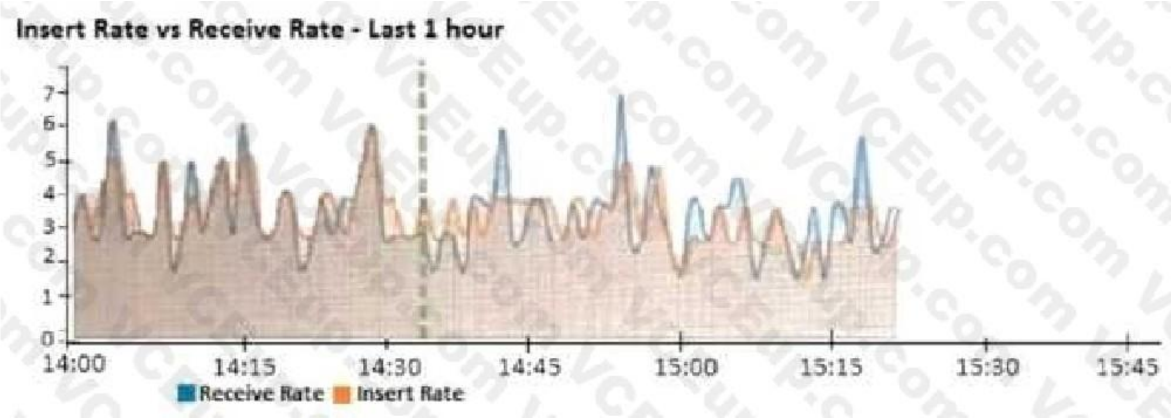
```
# configure system global
    set log-checksum md5
end
```

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

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 48
View the exhibit.



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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/47690/insert-rate-vsreceive-rate-widget

QUESTION 49
What remote authentication servers can you configure to validate your FortiAnalyzer administrator logons? (Choose three)

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

Correct Answer: ACE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 50
What statements are true regarding disk log quota? (Choose two)

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

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 51
What statements are true regarding FortiAnalyzer 's treatment of high availability (HA) dusters?
(Choose two)

A. FortiAnalyzer distinguishes different devices by their serial number.
B. FortiAnalyzer receives logs from d devices in a duster.
C. FortiAnalyzer receives bgs only from the primary device in the cluster.
D. FortiAnalyzer only needs to know (he serial number of the primary device in the cluster-it automaticaly discovers the other devices.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 52
What are the operating modes of FortiAnalyzer? (Choose two)

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

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 53
Which statements are correct regarding FortiAnalyzer reports? (Choose two)

A. FortiAnalyzer provides the ability to create custom reports.
B. FortiAnalyzer glows you to schedule reports to run.
C. FortiAnalyzer includes pre-defined reports only.
D. FortiAnalyzer allows reporting for FortiGate devices only.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 54
Which tabs do not appear when FortiAnalyzer is operating in Collector mode?

A. FortiView
B. Event Management
C. Device Manger
D. Reporting

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 55
FortiAnalyzer centralizes which functions? (Choose three)

A. Network analysis
B. Graphical reporting
C. Content archiving / data mining
D. Vulnerability assessment
E. Security log analysis / forensics

Correct Answer: BCE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 56
By default, what happens when a log file reaches its maximum file size?

A. FortiAnalyzer overwrites the log files.
B. FortiAnalyzer stops logging.
C. FortiAnalyzer rolls the active log by renaming the file.
D. FortiAnalyzer forwards logs to syslog.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 57
Which statements are true of Administrative Domains (ADOMs) in FortiAnalyzer? (Choose two.)

A. ADOMs are enabled by default.
B. ADOMs constrain other administrator’s access privileges to a subset of devices in the device list.
C. Once enabled, the Device Manager, FortiView, Event Management, and Reports tab display per ADOM.
D. All administrators can create ADOMs--not just the admin administrator.

Correct Answer: BC
Section: (none)

Explanation

Explanation/Reference:
Explanation:

QUESTION 58
Which statements are true regarding securing communications between FortiAnalyzer and FortiGate with SSL? (Choose two.)

A. SSL is the default setting.
B. SSL communications are auto-negotiated between the two devices.
C. SSL can send logs in real-time only.
D. SSL encryption levels are globally set on FortiAnalyzer.
E. FortiAnalyzer encryption level must be equal to, or higher than, FortiGate.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 59
What are two of the key features of FortiAnalyzer? (Choose two.)

A. Centralized log repository
B. Cloud-based management
C. Reports
D. Virtual domains (VDOMs)

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 60
What statements are true regarding the "store and upload" log transfer option between FortiAnalyzer and FortiGate? (Choose three.)

A. All FortiGates can send logs to FortiAnalyzer using the store and upload option.
B. Only FortiGate models with hard disks can send logs to FortiAnalyzer using the store and upload option.
C. Both secure communications methods (SSL and IPsec) allow the store and upload option.
D. Disk logging is enabled on the FortiGate through the CLI only.
E. Disk logging is enabled by default on the FortiGate.

Correct Answer: BCD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 61
Which statements are true regarding securing communications between FortiAnalyzer and FortiGate with IPsec? (Choose two.)

A. Must configure the FortiAnalyzer end of the tunnel only--the FortiGate end is auto-negotiated.
B. Must establish an IPsec tunnel ID and pre-shared key.
C. IPsec cannot be enabled if SSL is enabled as well.

D. IPsec is only enabled through the CLI on FortiAnalyzer.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 62
Which two statements about log forwarding are true? (Choose two.)

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.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
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/logforwarding

QUESTION 63
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 Forti Analyzer.
D. It resolves the destination IP address to a hostname in FortiView on FortiAnalyzer.

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 64
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.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://help.fortinet.com/fa/faz50hlp/56/5-6-1/FMGFAZ/
0800_ADOMs/0400_ADOM%20Device%20Modes.htm

QUESTION 65
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.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://docs.fortinet.com/document/fortianalyzer/6.2.0/cookbook/63238/what-is-thedifference-between-log-forward-and-log-aggregation-modes

QUESTION 66
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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://help.fortinet.com/fmgr/cli/5-6-1/FortiManager_CLI_Reference/700_execute/sqllocal+.htm

QUESTION 67
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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://docs2.fortinet.com/document/fortianalyzer/6.2.3/administrationguide/617380/creating-macros

QUESTION 68
Which two statements are true regarding FortiAnalyzer operating modes? (Choose two.)

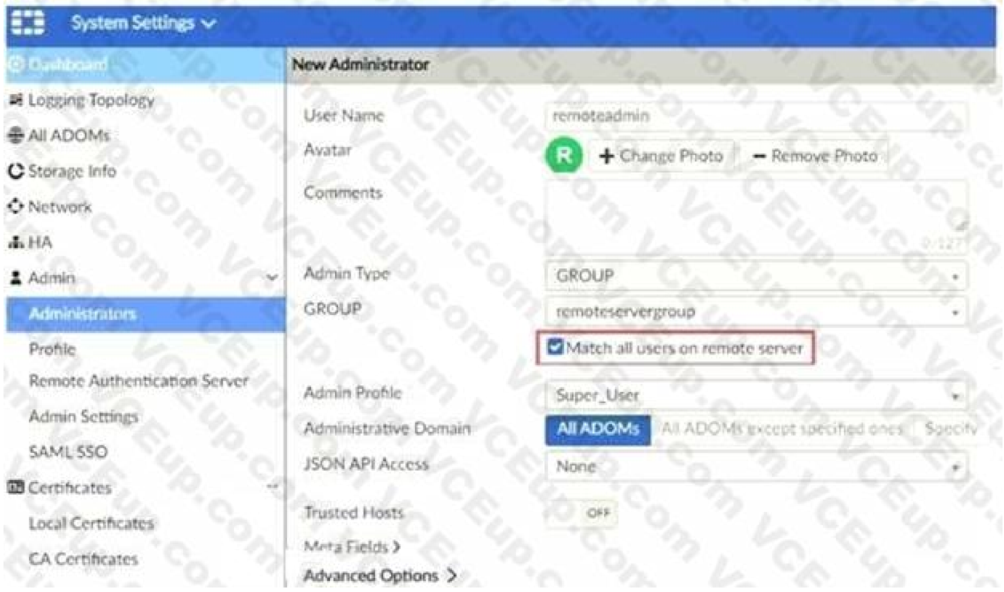
A. When in collector mode, FortiAnalyzer collects logs from multiple devices and forwards these logs in the original binary format.
B. Collector mode is the default operating mode.
C. When in collector mode. FortiAnalyzer supports event management and reporting features.
D. By deploying different FortiAnalyzer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

Correct Answer: AD
Section: (none)

Explanation

Explanation/Reference:
Explanation:
Reference: https://docs.fortinet.com/document/fortianalyzer/7.0.0/administrationguide/227478/collector-mode
https://docs.fortinet.com/document/fortianalyzer/7.0.0/administration-guide/312644/analyzercollector-collaboration

QUESTION 69
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 “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.)

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 anytime.
D. It allows administrators to use two-factor authentication.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://docs.fortinet.com/document/fortimanager/7.0.1/administrationguide/858351/creating-administrators

QUESTION 70
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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://docs.fortinet.com/document/fortimanager/6.4.1/administrationguide/792943/task-monitor

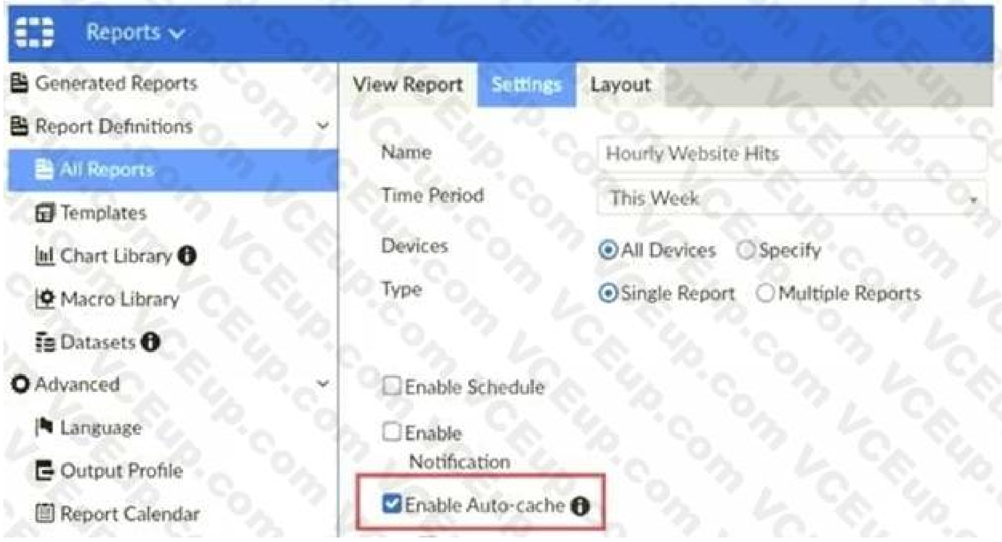
QUESTION 71
The admin administrator is failing to register a FortiClient EMS on the FortiAnalyzer device.
What can be the reason for this failure?

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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://help.fortinet.com/fa/faz50hlp/56/5-6-2/FMGFAZ/0800_ADOMs/0015_FortiClient%20and%20ADOMs.htm

QUESTION 72
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.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://help.fortinet.com/fa/faz50hlp/56/5-6-2/FMG-FAZ/2300_Reports/0025_Autocache.htm

QUESTION 73
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.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://help.fortinet.com/fa/faz50hlp/60/6-0-2/Content/FMGFAZ/4600_HA/0000_HA.htm?TocPath=High%20Availability%7C_____0

QUESTION 74
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.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://community.fortinet.com/t5/Fortinet-Forum/FW-Migration-between-ADOMs/mp/32683?m=158008

QUESTION 75
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.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://docs.fortinet.com/document/fortianalyzer/6.4.0/administrationguide/137635/viewing-compromised-hosts

QUESTION 76
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://community.fortinet.com/t5/FortiAnalyzer/Creating-a-Custom-report-from-FortiView-Export-to-Report-Chart/ta-p/190154?externalID=FD40483

QUESTION 77
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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://docs.fortinet.com/document/fortigate/6.2.0/hardening-yourfortigate/582009/system-administrator-best-practices

QUESTION 78
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 mall server that can be used to send email.
What could be the problem?

A. Fortinet is assigned the Standard_ User administrator profile.
B. A trusted host is configured.
C. ADOM mode is configured with Advanced mode.
D. Fortinet is assigned the Restricted_ User administrator profile.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 79
Which two statements express the advantages of grouping similar reports? (Choose two.)

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

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 80
What are analytics logs on FortiAnalyzer?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

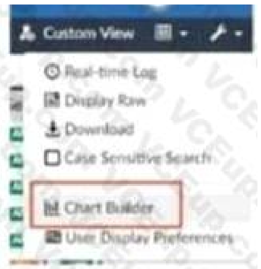
QUESTION 81
What is Log Insert Lag Time on FortiAnalyzer?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 82
Refer to the exhibit.



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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 83
Which two statement are true regardless initial Logs sync and Log Data Sync for Ha on FortiAnalyzer?

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

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 84
Which two statements are true regarding fabric connectors? (Choose two.)

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

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 85
What does the disk status Degraded mean for RAID management?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

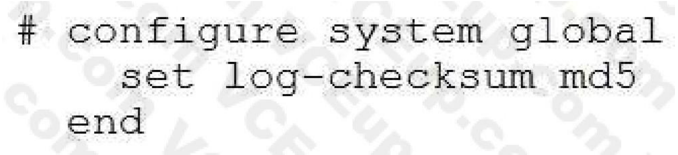
QUESTION 86
Which two methods can you use to send event notifications when an event occurs that matches a configured event handler? (Choose two.)

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

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Explanation:
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
Reference: https://help.fortinet.com/fa/faz50hlp/60/6-0-
2/Content/FortiAnalyzer_Admin_Guide/1800_Events/0200_Event_handlers/0600_Create_event_ha ndlers.htm

QUESTION 87
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

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 88
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 89
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

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
Explanation:
https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/448471/creating-asecurity-fabric-adom

QUESTION 90
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://help.fortinet.com/fa/faz50hlp/56/5-6-2/FMGFAZ/2300_Reports/0010_Predefined_reports.htm#:~:text=FortiAnalyzer%20includes%20a%20number% 20of,create%20and%2For%20build%20reports.&text=A%20template% 20populates%20the%20Layou t,that% 20is%20to%20be%20created.
https://help.fortinet.com/fa/faz50hlp/56/5-6-2/FMGFAZ/2300_Reports/0010_Predefined_reports.htm
Reference: https://docs2.fortinet.com/document/fortianalyzer/6.0.8/administrationguide/618245/predefined-reports-templates-charts-and-macros

QUESTION 91
For which two SAML roles can the FortiAnalyzer be configured? (Choose two.)

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

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://docs.fortinet.com/document/fortianalyzer/6.2.0/new-features/957811/samladminauthentication#:~:text=for%20the%20administrator.-,FortiAnalyzer%20can%20play%20the%20role%20of%20the%20identity%20provider%20(IdP,external%20identity%20provider%20is%20available.
https://docs.fortinet.com/document/fortianalyzer/6.2.0/administration-guide/981386/saml-adminauthentication

QUESTION 92
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.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference:
https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/384416/how-autocache-works
https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/86926/enabling-autocache

QUESTION 93
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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://help.fortinet.com/fa/faz50hlp/56/5-6-6/Content/FortiAnalyzer_Admin_Guide/0300_Key_concepts/0600_Log_Storage/0400_Archive_anal ytics_logs.htm

QUESTION 94
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.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://docs.fortinet.com/document/fortianalyzer/7.0.1/administrationguide/651442/fetcher-management