

Fortinet.Pre.NSE5_FAZ-7.0 .30q

Number: NSE5_FAZ-7.0
Passing Score: 800
Time Limit: 120 min



Exam Code: NSE5_FAZ-7.0
Exam Name: Fortinet NSE 5 - FortiAnalyzer 7.0
Website: <https://VCEup.com/>
Team-Support: <https://VCEplus.io/>



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

www.VCEplus.io

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

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

<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 get both source and destination, and it offloads the work from FortiAnalyzer. On FortiAnalyzer, this IP resolution 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

www.VCEplus.io

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 configuration, **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 keep 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>

www.VCEplus.io

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/](https://help.fortinet.com/fa/faz50hlp/60/6-0-2/Content/FortiAnalyzer_Admin_Guide/3600_FortiView/0200_Using_FortiView/1200_Compromised_hosts_page.htm?TocPath=FortiView%7CUsing%20FortiView%7C_____6)

[FortiAnalyzer_Admin_Guide/3600_FortiView/0200_Using_FortiView/1200_Compromised_hosts_page.htm?](https://help.fortinet.com/fa/faz50hlp/60/6-0-2/Content/FortiAnalyzer_Admin_Guide/3600_FortiView/0200_Using_FortiView/1200_Compromised_hosts_page.htm?TocPath=FortiView%7CUsing%20FortiView%7C_____6)

[TocPath=FortiView%7CUsing%20FortiView%7C_____6](https://help.fortinet.com/fa/faz50hlp/60/6-0-2/Content/FortiAnalyzer_Admin_Guide/3600_FortiView/0200_Using_FortiView/1200_Compromised_hosts_page.htm?TocPath=FortiView%7CUsing%20FortiView%7C_____6)

QUESTION 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

www.VCEplus.io

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

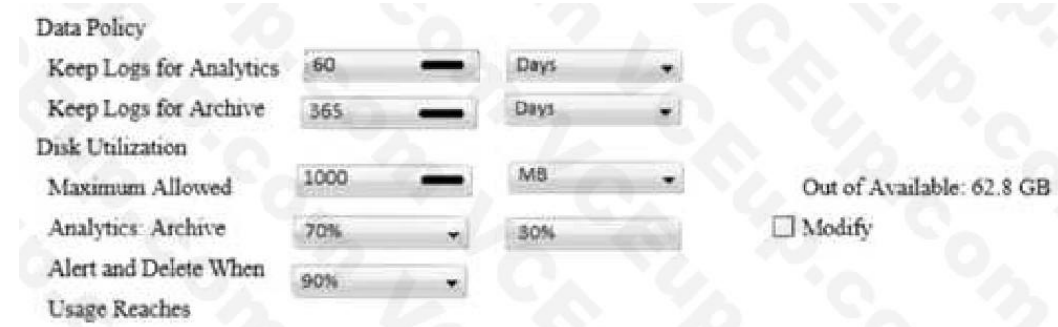
Explanation/Reference:

Explanation:

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

QUESTION 24

View the exhibit:



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.](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?

www.VCEplus.io

- 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-the-difference-between-log-forward-and-log-aggregation-modes>

www.VCEplus.io