QUESTION 21
What FortiGate process caches logs when FortiAnalyzer is not reachable?

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

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

QUESTION 22
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

Answer: D

QUESTION 23
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.

Answer: AB

QUESTION 24
Which tabs do not appear when FortiAnalyzer is operating in Collector mode?

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

Answer: B

QUESTION 25
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

Answer: BCE

QUESTION 26
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.

Answer: C

QUESTION 27
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.

Answer: BC

QUESTION 28
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.

Answer: AD

QUESTION 29
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)

Answer: AC

QUESTION 30
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.

Answer: BCD

QUESTION 31
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.

Answer: C

QUESTION 32
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.

Answer: CD
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/log-forwarding

QUESTION 33
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

Answer: BC

QUESTION 34
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

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

QUESTION 35
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

Answer: C

QUESTION 36
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

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

QUESTION 37
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

Answer: B

QUESTION 38
For which two SAML roles can the FortiAnalyzer be configured? (Choose two.)

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

Answer: BD

QUESTION 39
Which two purposes does the auto cache setting on reports serve? (Choose two.)

A. It automatically updates the hcache when new logs arrive.
B. It provides diagnostics on report generation time.
C. It reduces the log insert lag rate.
D. It reduces report generation time.

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

QUESTION 40
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