

Fortinet.FCP_FAZ_AN-7.4.v2024-11-15.q57

Exam Code:	FCP_FAZ_AN-7.4
Exam Name:	FCP - FortiAnalyzer 7.4 Analyst
Certification Provider:	Fortinet
Free Question Number:	57
Version:	v2024-11-15
# of views:	1787
# of Questions views:	570
https://www.freepdfdumps.com/Fortinet.FCP_FAZ_AN-7.4.v2024-11-15.q57.html	

NEW QUESTION: 1

For proper log correlation between the logging devices and FortiAnalyzer, FortiAnalyzer and all registered devices should:

- A. Use an NTP server
- B. Use host name resolution
- C. Use real-time forwarding
- D. Use DNS

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 2

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

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

Answer: A,D ([LEAVE A REPLY](#))

NEW QUESTION: 3

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

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

Answer: B,C ([LEAVE A REPLY](#))

NEW QUESTION: 4

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

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

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 5

Which FortiAnalyzer feature allows you to use a proactive approach when managing your network security?

- A. Threat hunting
- B. Incidents dashboards
- C. FortiView Monitor
- D. Outbreak alert services

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 6

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

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 7

What is required to authorize a FortiGate on FortiAnalyzer using Fabric authorization?

- A. A FortiGate ADOM
- B. A pre-shared key
- C. Valid FortiAnalyzer credentials
- D. The FortiGate serial number

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 8

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

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

- B. FortiAnalyzer is in an HA cluster.
- C. A separate license is required on FortiAnalyzer in order to register the FortiClient EMS device.
- D. ADOMs are not enabled on FortiAnalyzer.

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 9

What must you consider when using log fetching? (Choose two.)

- A. The archive logs retrieved from the server become archive logs in the client.
- B. The fetch client can retrieve logs from devices that are not added to its local Device Manager.
- C. You can use filters to include only logs from a single device.
- D. The fetching profile must include a user with the Super_User profile.

Answer: B,C ([LEAVE A REPLY](#))

NEW QUESTION: 10

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

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

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 11

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

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

Answer: C,D ([LEAVE A REPLY](#))

NEW QUESTION: 12

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

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

Answer: A,C ([LEAVE A REPLY](#))

NEW QUESTION: 13

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

Answer: A,C ([LEAVE A REPLY](#))

NEW QUESTION: 14

Which two elements are contained in a system backup created on FortiAnalyzer? (Choose two.)

- A. Report information
- B. Logs from registered devices
- C. System information
- D. Database snapshot

Answer: A,C ([LEAVE A REPLY](#))

NEW QUESTION: 15

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

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

Answer: A,B ([LEAVE A REPLY](#))

NEW QUESTION: 16

What can the CLI command # diagnose test application oftpd 3 help you to determine?

- A. What logs, if any, are reaching FortiAnalyzer
- B. What ADOMs are enabled and configured
- C. What devices and IP addresses are connecting to FortiAnalyzer
- D. What devices are registered and unregistered

Answer: ([SHOW ANSWER](#))

Valid FCP_FAZ_AN-7.4 Dumps shared by Actual4test.com for Helping Passing FCP_FAZ_AN-7.4 Exam! Actual4test.com now offer the **newest FCP_FAZ_AN-7.4 exam dumps**, the Actual4test.com FCP_FAZ_AN-7.4 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com FCP_FAZ_AN-7.4 dumps

with Test Engine here: https://www.actual4test.com/FCP_FAZ_AN-7.4_examcollection.html
(58 Q&As Dumps, **30%OFF** Special Discount: **Freepdfdumps**)

NEW QUESTION: 17

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

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

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 18

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

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

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 19

When is the execution of a playbook considered as failed?

- A. When at least one of the tasks fails
- B. When all the tasks fail
- C. When the playbook is disabled
- D. When the playbook is imported from another ADOM

Answer: ([SHOW ANSWER](#)**)**

NEW QUESTION: 20

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

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

Answer: C,D ([LEAVE A REPLY](#))

NEW QUESTION: 21

What database language does FortiAnalyzer use for logging and reporting?

- A. XML

- B. Java
- C. SQL
- D. XQuery

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 22

Which statement about sending notifications with incident updates is true?

- A. You must configure an output profile to send notifications by email.
- B. Notifications can be sent only when an incident is created or deleted.
- C. Each connector used can have different notification settings.
- D. Each incident can send notifications to a single external platform.

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 23

How are logs forwarded when FortiAnalyzer is using 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 and content files are stored and uploaded at a scheduled time.
- D. Logs are forwarded as they are received.

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 24

Why run the command `diagnose sql status sqlplugind`?

- A. To check what is the database log insertion status
- B. To list the current SQL processes running
- C. To display the SQL query connections and hcache status
- D. To view the current hcache size

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 25

How can you configure FortiAnalyzer to permit administrator logins from only specific locations?

- A. Use trusted hosts
- B. Use secure protocols
- C. Use static routes
- D. Use administrative profiles

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 26

How do you restrict an administrator's access to a subset of your organization's ADOMs?

- A. Configure trusted hosts
- B. Assign the ADOMs to the administrator's account

- C. Assign the default Super_User administrator profile
- D. Set the ADOM mode to Advanced

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 27

Which statement correctly describes the management extensions available on FortiAnalyzer?

- A. Management extensions may require a minimum number of CPU cores to run.
- B. Management extensions do not require additional licenses.
- C. Management extensions require a dedicated VM for best performance.
- D. Management extensions allow FortiAnalyzer to act as a FortiSIEM supervisor.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 28

After generating a report, you notice the information you were expecting to see is not included in it.

What are two possible reasons for this scenario? (Choose two.)

- A. The logs were overwritten by the data retention policy.
- B. You enabled auto-cache with extended log filtering.
- C. The time frame selected in the report is wrong.
- D. The logfiled service has not indexed all the expected logs.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 29

You created a playbook on FortiAnalyzer that uses a FortiOS connector. When configuring the FortiGate side, which type of trigger must be used so that the actions in an automation stitch are available in the FortiOS connector?

- A. Fabric Connector event
- B. FortiAnalyzer Event Handler
- C. Incoming webhook
- D. FortiOS Event Log

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 30

Which statement about the FortiSIEM management extension is correct?

- A. It can be installed as a dedicated VM.
- B. It requires a licensed FortiSIEM supervisor.
- C. Allows you to manage the entire life cycle of a threat or breach.
- D. Its use of the available disk space is capped at 50%.

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 31

Which statement is true about sending notifications with incident updates?

- A. Notifications can be sent only by email.
- B. You can send notifications to multiple external platforms.
- C. Notifications can be sent only when an incident is updated or deleted.
- D. If you use multiple fabric connectors, all connectors must have the same notification settings.

Answer: B ([LEAVE A REPLY](#))

Valid FCP_FAZ_AN-7.4 Dumps shared by Actual4test.com for Helping Passing FCP_FAZ_AN-7.4 Exam! Actual4test.com now offer the **newest FCP_FAZ_AN-7.4 exam dumps**, the Actual4test.com FCP_FAZ_AN-7.4 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com FCP_FAZ_AN-7.4 dumps with Test Engine here: https://www.actual4test.com/FCP_FAZ_AN-7.4_examcollection.html (58 Q&As Dumps, **30%OFF** Special Discount: **Freepdfdumps**)

NEW QUESTION: 32

Refer to the exhibit.



Event	Event Status	Event Type	Count	Severity
151.101.54.62 (1)				
Insecure SSL Connection blocked from 10.8.3.20	Mitigated	SSL	1	Low

Which statement is correct regarding the event displayed?

- A. An incident was created from this event.
- B. The security event risk is considered open.
- C. The security risk was blocked or dropped.
- D. The risk source is isolated.

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 33

If the primary FortiAnalyzer in an HA cluster fails, how is the new primary elected?

- A. The firmware version is checked first.
- B. The active port number is checked first.
- C. The configured IP address is checked first.
- D. The configured priority is checked first

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 34

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

- A. No need to do anything because the disk will self-recover.

- B. Shut down FortiAnalyzer and replace the disk.
- C. Hot swap the disk.
- D. Run execute format disk to format and restart the FortiAnalyzer device.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 35

Which item must you configure on FortiAnalyzer to email generated reports automatically?

- A. Report scheduling
- B. SFTP server
- C. SNMP server
- D. Output profile

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 36

Which two external servers can you configure to validate administrator logins? (Choose two.)

- A. RADIUS
- B. LDAP
- C. Only locally by FortiAnalyzer
- D. Syslog

Answer: A,B ([LEAVE A REPLY](#))

NEW QUESTION: 37

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

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

Answer: B,D ([LEAVE A REPLY](#))

NEW QUESTION: 38

What is the main purpose of deploying RAID with FortiAnalyzer?

- A. To back up your logs
- B. To store data in chunks across multiple drives
- C. To make an identical copy of log data on two separate physical drives
- D. To provide redundancy of your log data

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 39

What is the purpose of employing RAID with FortiAnalyzer?

- A. To provide data separation between ADOMs

- B. To back up your logs
- C. To separate analytical and archive data
- D. To introduce redundancy to your log data

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 40

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

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 41

When generating reports on FortiAnalyzer, macros can be used to include additional data. Which two statements about macros are true? (Choose two.)

- A. Macros do not need to be associated with a chart
- B. Macros are supported in FortiGate ADOMs only
- C. Macros cannot be customized
- D. Macros are abbreviated dataset queries

Answer: A,D ([LEAVE A REPLY](#))

NEW QUESTION: 42

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

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 43

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

- A. Chart Builder
- B. Custom View
- C. Export to Report Chart (FortiView)
- D. Dataset Library

Answer: A,C ([LEAVE A REPLY](#))

NEW QUESTION: 44

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

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 45

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

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

Answer: B,C ([LEAVE A REPLY](#))

NEW QUESTION: 46

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

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

Answer: C,D,E ([LEAVE A REPLY](#))

Valid FCP_FAZ_AN-7.4 Dumps shared by Actual4test.com for Helping Passing FCP_FAZ_AN-7.4 Exam! Actual4test.com now offer the **newest FCP_FAZ_AN-7.4 exam dumps**, the Actual4test.com FCP_FAZ_AN-7.4 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com FCP_FAZ_AN-7.4 dumps with Test Engine here: https://www.actual4test.com/FCP_FAZ_AN-7.4_examcollection.html (58 Q&As Dumps, **30%OFF** Special Discount: **Freepdfdumps**)

NEW QUESTION: 47

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

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

Answer: B,D ([LEAVE A REPLY](#))

NEW QUESTION: 48

Which log will generate an event with the status Contained?

- A. An AppControl log with action=blocked.
- B. An IPS log with action=pass.
- C. A WebFilter log with action=dropped.
- D. An AV log with action=quarantine.

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 49

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

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

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 50

What does the disk status Degraded mean for RAID management?

- A. The hard drive is no longer being used by the RAID controller
- B. One or more drives are missing from the FortiAnalyzer unit. The drive is no longer available to the operating system.
- 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 FortiAnalyzer device is writing to all the hard drives on the device in order to make the array fault tolerant.

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 51

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

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 52

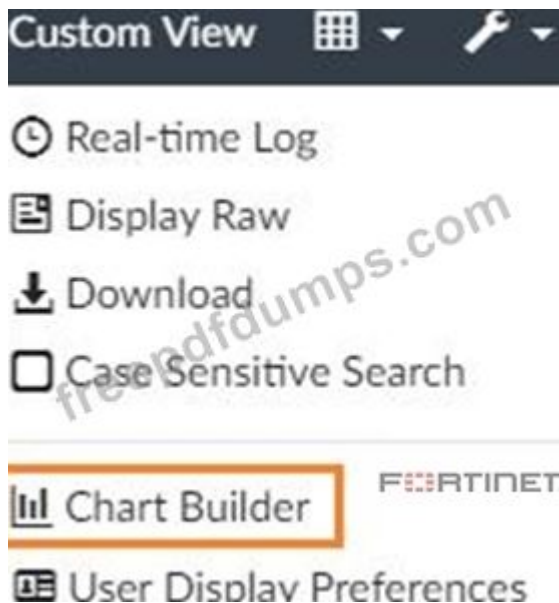
Which two statements about log forwarding are true? (Choose two.)

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

Answer: C,D ([LEAVE A REPLY](#))

NEW QUESTION: 53

Refer to the exhibit.



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

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

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 54

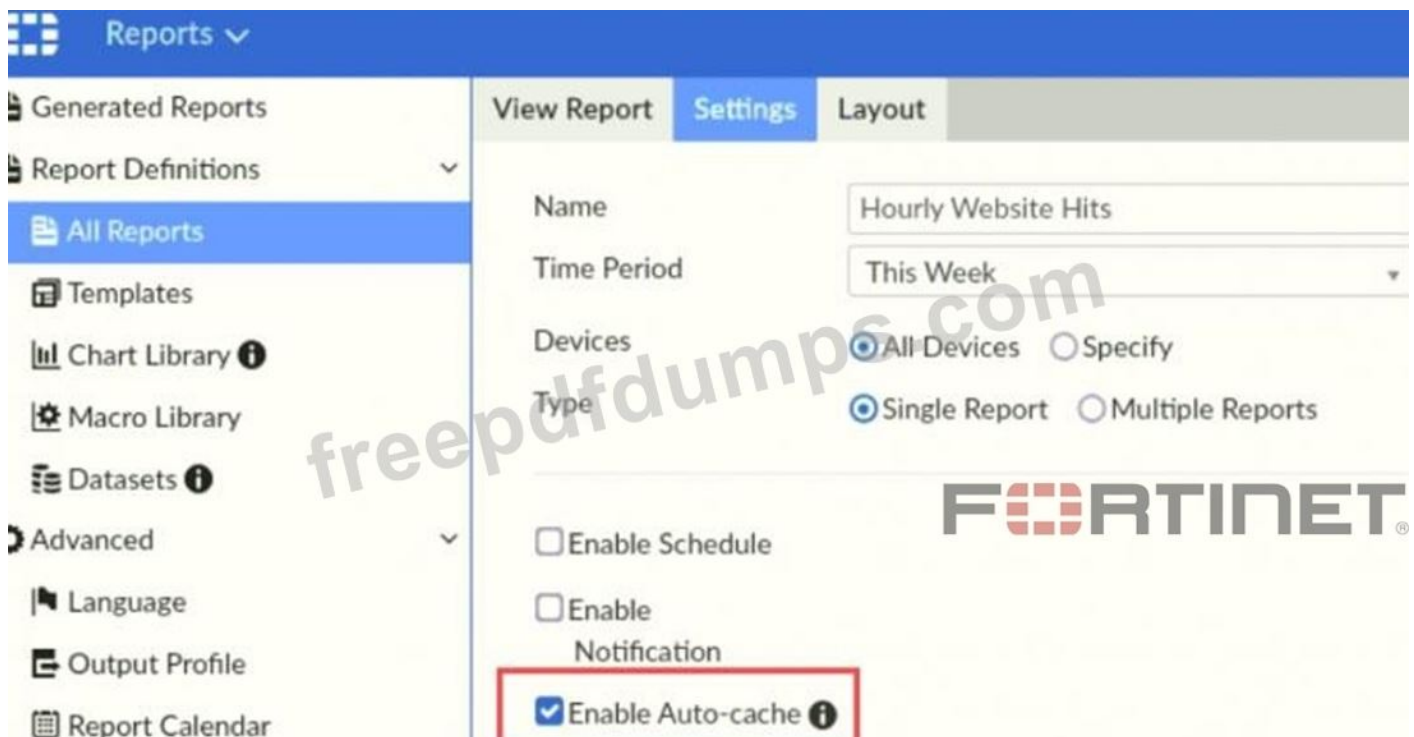
By default, what happens when a log file reaches its maximum file size?

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

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 55

Refer to the exhibit.



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. This feature is automatically enabled for scheduled reports.
- C. Reports will be cached in the memory.
- D. Enabling auto-cache reduces report generation time for reports that require a long time to assemble datasets.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 56

Which statement is true when you are upgrading the firmware on an HA cluster made up of two FortiAnalyzer devices?

- A. You can perform the firmware upgrade using only a console connection.
- B. First, upgrade the secondary device, and then upgrade the primary device.
- C. Both FortiAnalyzer devices will be upgraded at the same time.

D. You can enable uninterruptible-upgrade so that the normal FortiAnalyzer operations are not interrupted while the cluster firmware upgrades.

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 57

Which statement is true regarding Macros on FortiAnalyzer?

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

Answer: B ([LEAVE A REPLY](#))

Valid FCP_FAZ_AN-7.4 Dumps shared by Actual4test.com for Helping Passing FCP_FAZ_AN-7.4 Exam! Actual4test.com now offer the **newest FCP_FAZ_AN-7.4 exam dumps**, the Actual4test.com FCP_FAZ_AN-7.4 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com FCP_FAZ_AN-7.4 dumps with Test Engine here: https://www.actual4test.com/FCP_FAZ_AN-7.4_examcollection.html (58 Q&As Dumps, **30%OFF** Special Discount: **Freepdfdumps**)