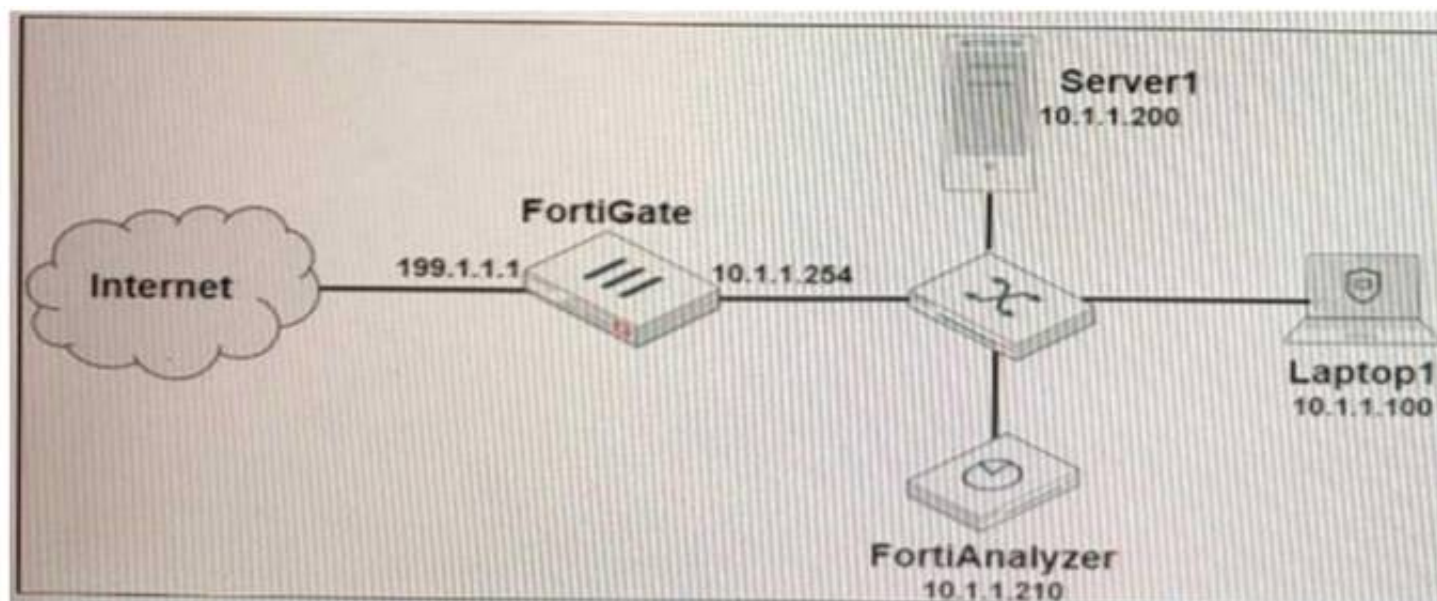# Fortinet

Exam Questions NSE5_FAZ-7.2

Fortinet NSE 5 - FortiAnalyzer 7.2

NEW QUESTION 1
Refer to the exhibit.

Laptopt is used by several administrators to manage FortiAnalyzer. You want to configure a generic text filter that matches all login attempts to the web interface generated by any user other than "admin" and coming from Laptop1:
Which filter will achieve the desired result?

A. operation-login & performed_on=="GUI(10.1.1.100)" & user!=admin
B. operation-login & srcip==10.1.1.100 & dstip==10.1.1.210 & user==admin
C. operation-login & dstip==10.1.1.210 & userl-admin
D. operation-login & performed_on=="GUI(10.1.1.210)' & user!=admin

Answer: A

Explanation:
On there the task was to create a filter for failed logins from any other location but the local computer: "Add the text performed_on!~10.0.1.10. This includes any attempts coming from devices with an IP address that is not the one configured on the Local-Client computer."

NEW QUESTION 2
What are two benefits of using fabric connectors? (Choose two.)

A. They allow FortiAnalyzer to send logs in real-time to public cloud accounts.
B. You do not need an additional license to send logs to the cloud platform.
C. Fabric connectors allow you to improve redundancy.
D. Using fabric connectors is more efficient than using third-party polling with API.

Answer: AC

NEW QUESTION 3
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

NEW QUESTION 4
What must you consider when using log fetching? (Choose two.)

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

Answer: BC

NEW QUESTION 5
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

Answer: AC

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

NEW QUESTION 6
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

Answer: AB

Explanation:
To prevent logs from being tampered with while in storage, you can add a log checksum using the config system global command. You can configure FortiAnalyzer to record a log file hash value, timestamp, and authentication code when the log is rolled and archived and when the log is uploaded (if that feature is enabled). This can also help against man-in-the-middle only for the transmission from FortiAnalyzer to an SSH File Transfer Protocol (SFTP) server during log upload. FortiAnalyzer_7.0_Study_Guide-Online page 149

NEW QUESTION 7
Refer to the exhibit.
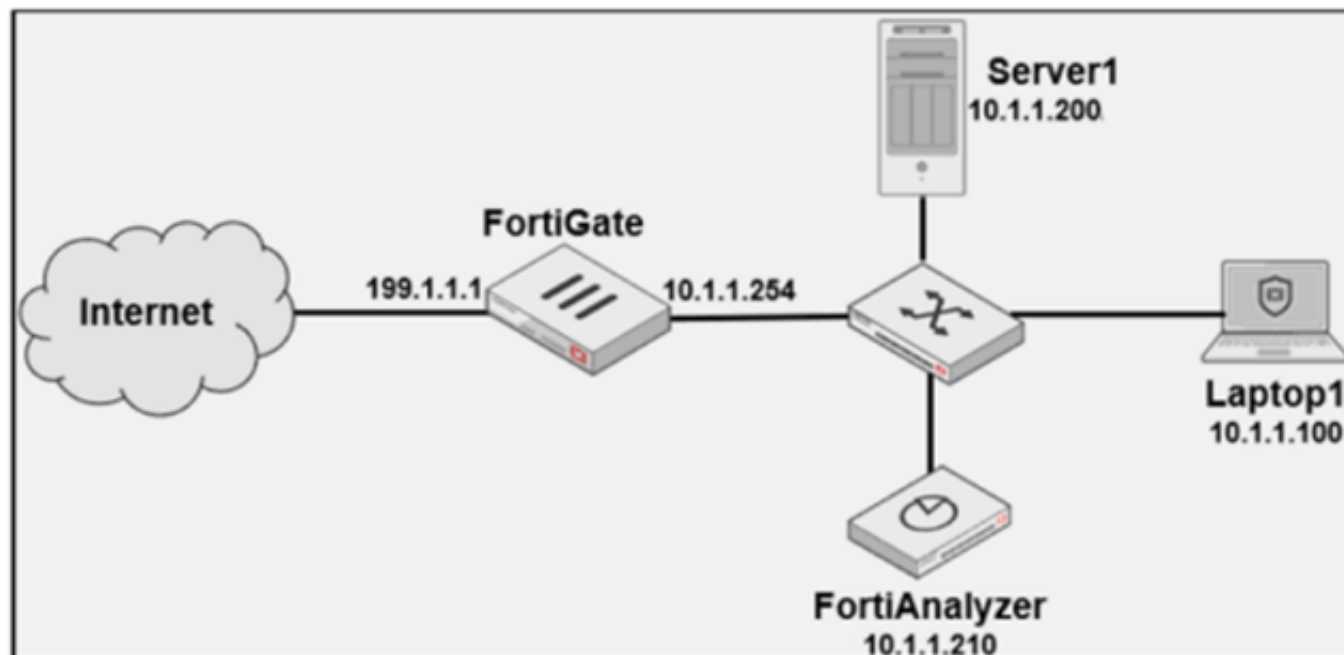
Laptop1 is used by several administrators to manage FortiAnalyzer. You want to configure a generic text filter that matches all login attempts to the web interface generated by any user other than "admin", and coming from Laptop1.
Which filter will achieve the desired result?

A. operation-login & dstip==10.1.1.210 & user!-admin
B. operation-login & srcip==10.1.1.100 & dstip==10.1.1.210 & user==admin
C. operation-login & performed_on=="GUI(10.1.1.210)" & user!=admin
D. operation-login & performed_on=="GUI(10.1.1.100)" & user!=admin

Answer: D

NEW QUESTION 8
An administrator has moved FortiGate A from the root ADOM to ADOM1. Which two statements are true regarding logs? (Choose two.)

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

Answer: BD

NEW QUESTION 9
Which statement about sending notifications with incident updates is true?

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

Answer: D

NEW QUESTION 10
Which statement describes online logs on FortiAnalyzer?

A. Logs that reached a specific size and were rolled over
B. Logs that can be used to create reports
C. Logs that can be viewed using Log Browse
D. Logs that are saved to disk, compressed, and available in FortiView

Answer: C

NEW QUESTION 10
Which two statements are true regarding the outbreak detection service? (Choose two.)

A. New alerts are received by email.
B. Outbreak alerts are available on the root ADOM only.
C. An additional license is required.
D. It automatically downloads new event handlers and reports.

Answer: CD

NEW QUESTION 14
Which two methods are the most common methods to control and restrict administrative access on FortiAnalyzer? (Choose two.)

A. Virtual domains
B. Administrative access profiles
C. Trusted hosts
D. Security Fabric

Answer: BC

NEW QUESTION 16
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

Answer: B

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.

NEW QUESTION 19
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

Answer: AD

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.pdf
Pg 45: "ADOMs must be enabled to support the logging and reporting of NON-FORTIGATE devices, such as FortiCarrier, FortiClientEMS, FortiMail, FortiWeb, FortiCache, and FortiSandbox."

NEW QUESTION 23
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.

Answer: C

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

NEW QUESTION 28
Which two actions should an administrator take 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. Make sure all endpoints are reachable by FortiAnalyzer.
C. Enable device detection on an interface on the FortiGate devices that are connected to the FortiAnalyzer device.

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

Answer: AD

Explanation:
In order to configure IOC, you require the following:
• A one-year subscription to IOC. Note that FortiAnalyzer does include an evaluation license, but it is restrictive and only meant to give you an idea of how the feature works.
• A web filter services subscription on FortiGate device(s)
• Web filter policies on FortiGate device(s) that send traffic to FortiAnalyzer Compromised Hosts or Indicators of Compromise service (IOC) is a licensed feature.
To view Compromised Hosts, you must turn on the UTM web filter of FortiGate devices and subscribe your FortiAnalyzer unit to FortiGuard to keep its local threat database synchronized with the FortiGuard threat database. See Subscribing FortiAnalyzer to FortiGuard.
Ref :
https://docs.fortinet.com/document/fortianalyzer/6.4.0/administration-guide/137635/viewing-compromised-host

NEW QUESTION 31
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

NEW QUESTION 33
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

Answer: D

NEW QUESTION 37
How can you attach a report to an incident?

A. By attaching it to an event handler alert
B. By editing the settings of the desired report
C. From the properties of an existing incident
D. Saving it in JSON format, and then importing it

Answer: C

NEW QUESTION 38
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

Answer: D

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>

FortiAnalyzer_7.0_Study_Guide-Online.pdf page 128: Are the device analytics logs required for reports in the new ADOM? If so, rebuild the new ADOM database

NEW QUESTION 39
What happens when the IOC breach detection engine on FortiAnalyzer finds web logs that match a blocklisted IP address?

A. The endpoint is marked as Compromised an
B. optionally, can be put in quarantine.
C. FortiAnalyzer flags the associated host for further analysis.
D. A new Infected entry is added for the corresponding endpoint.
E. The detection engine classifies those logs as Suspicious

Answer: A

NEW QUESTION 44
What are the operating modes of FortiAnalyzer? (Choose two)

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

Answer: CD

NEW QUESTION 47
Which two statements are true regarding log fetching on FortiAnalyzer? (Choose two.)

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

Answer: BD

NEW QUESTION 51
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

Answer: A

Explanation:
https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/137bb60e-ff37-11e8-8524-f8bc1258b8

NEW QUESTION 52
Refer to the exhibit.
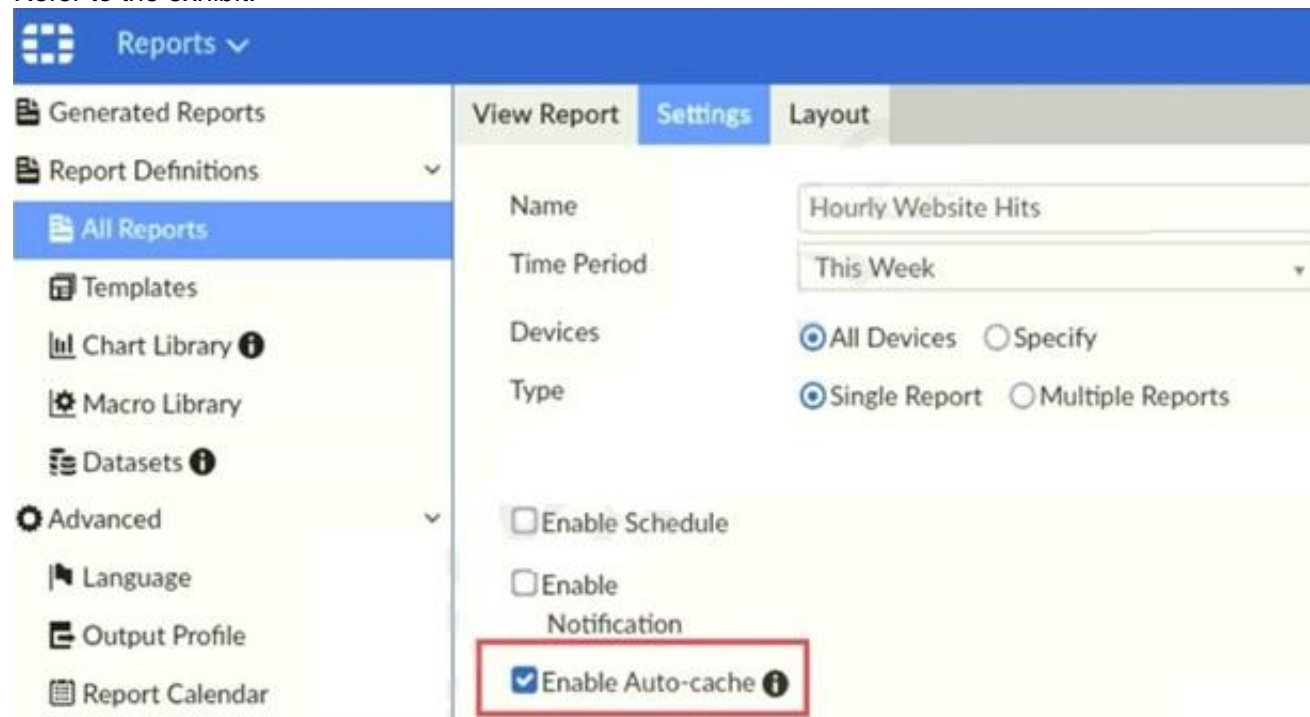
Which two statements are true regarding enabling auto-cache on FortiAnalyzer? (Choose two.)

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

Answer: CD

Explanation:
"Enable auto-cache in the report settings to boost the reporting performance and reduce report generation time. Scheduled reports have auto-cache enabled already."
FortiAnalyzer_7.0_Study_Guide-Online page 306

NEW QUESTION 54
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

Answer: A

Explanation:

~~When dealing with Fortinet Support because it allows for offline access to the database configuration~~

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

NEW QUESTION 58
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

Answer: C

NEW QUESTION 59
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.

Answer: AB

NEW QUESTION 64
What are two effects of enabling auto-cache in a FortiAnalyzer report? (Choose two.)

A. The size of newly generated reports is optimized to conserve disk space.
B. FortiAnalyzer local cache is used to store generated reports.
C. When new logs are received, the hard-cache data is updated automatically.
D. The generation time for reports is decreased.

Answer: CD

NEW QUESTION 69
An administrator has moved FortiGate A from the root ADOM to ADOM1. However, the administrator is not able to generate reports for FortiGate A in ADOM1.
What should the administrator do to solve this issue?

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

Answer: B

NEW QUESTION 70
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

Answer: D

NEW QUESTION 74
Which daemon is responsible for enforcing the log file size?

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

Answer: B

Explanation:
FortiAnalyzer_7.0_Study_Guide-Online.pdf page 121: The logfiled process enforces the log file size and is also responsible for disk quota enforcement by

monitoring the other processes.

NEW QUESTION 76
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.

Answer: D

NEW QUESTION 81
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

NEW QUESTION 84
Refer to the exhibit.
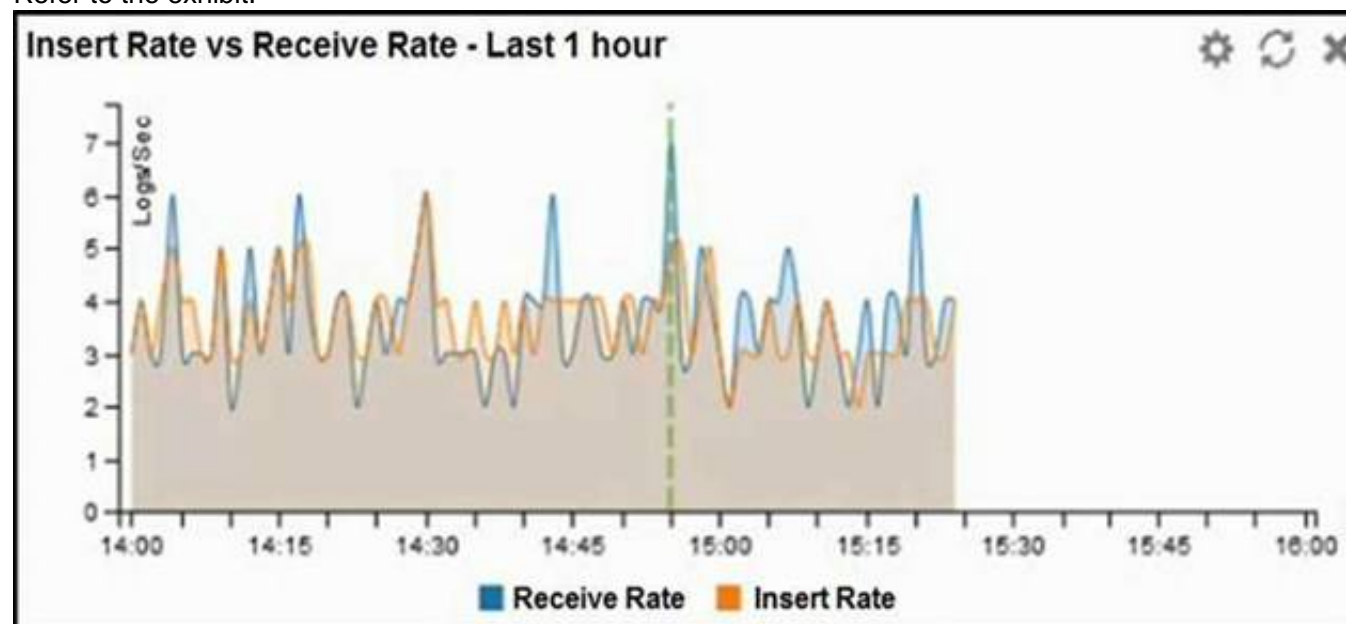
What does the data point at 14:55 tell you?

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

Answer: D

NEW QUESTION 87
What does the disk status Degraded mean for RAID management?

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

Answer: D

NEW QUESTION 88
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

Answer: AB

NEW QUESTION 90
If you upgrade your FortiAnalyzer firmware, what report elements can be affected?

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

Answer: D

NEW QUESTION 91
Refer to the exhibits.

How many events will be added to the incident created after running this playbook?

A. Ten events will be added.
B. No events will be added.
C. Five events will be added.
D. Thirteen events will be added.

Answer: A

NEW QUESTION 95
Why must you wait for several minutes before you run a playbook that you just created?

A. FortiAnalyzer needs that time to parse the new playbook.
B. FortiAnalyzer needs that time to back up the current playbooks.
C. FortiAnalyzer needs that time to ensure there are no other playbooks running.
D. FortiAnalyzer needs that time to debug the new playbook.

Answer: A

NEW QUESTION 99
If the primary FortiAnalyzer in an HA cluster fails, how is the new primary elected?

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

Answer: D

Explanation:
In the case of a primary device failure, FortiAnalyzer HA uses the following rules to select a new primary:
• All cluster devices are assigned a priority from 80 to 120. The default priority is 100. If the primary device becomes unavailable, the device with the highest priority is selected as the new primary device. For example, a device with a priority of 110 is selected over a device with a priority of 100.

• If multiple devices have the same priority, the device whose primary IP address has the greatest value is selected as the new primary device. For example, 123.45.67.124 is selected over 123.45.67.123.
• If a new device with a higher priority or a greater value IP address joins the cluster, the new device does not replace (or pre-empt) the current primary device automatically.
FortiAnalyzer_7.0_Study_Guide-Online page 62

NEW QUESTION 103
......

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

NSE5_FAZ-7.2 Practice Exam Features:

* NSE5_FAZ-7.2 Questions and Answers Updated Frequently

* NSE5_FAZ-7.2 Practice Questions Verified by Expert Senior Certified Staff

* NSE5_FAZ-7.2 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* NSE5_FAZ-7.2 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
Order The NSE5_FAZ-7.2 Practice Test Here