Exam Questions NSE5_FAZ-7.0

Fortinet NSE 5 - FortiAnalyzer 7.0

https://www.2passeasy.com/dumps/NSE5_FAZ-7.0/

NEW QUESTION 1
Which SQL query is in the correct order to query the database in the FortiAnslyzer?

A. SELECT devid FROM Slog GROOP BY devid WHERE * user' =* USERI'
B. SELECT devid WHERE 'u3er'='USERI' FROM $ log GROUP BY devid
C. SELECT devid FROM Slog- WHERE *user' =' USERI' GROUP BY devid
D. FROM Slog WHERE 'user* =' USERI' SELECT devid GROUP BY devid

Answer: C

Explanation:
FortiAnalyzer_7.0_Study_Guide-Online.pdf page 259: The main clauses FortiAnalyzer reports use are as follows:
•FROM
•WHERE
•GROUP BY
•ORDER BY
• LIMIT
• OFFSET
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.

NEW QUESTION 2
When working with FortiAnalyzer reports, what is the purpose of a dataset?

A. To provide the layout used for reports
B. To define the chart type to be used
C. To retrieve data from the database
D. To set the data included in templates

Answer: C

NEW QUESTION 3
Refer to the exhibit.
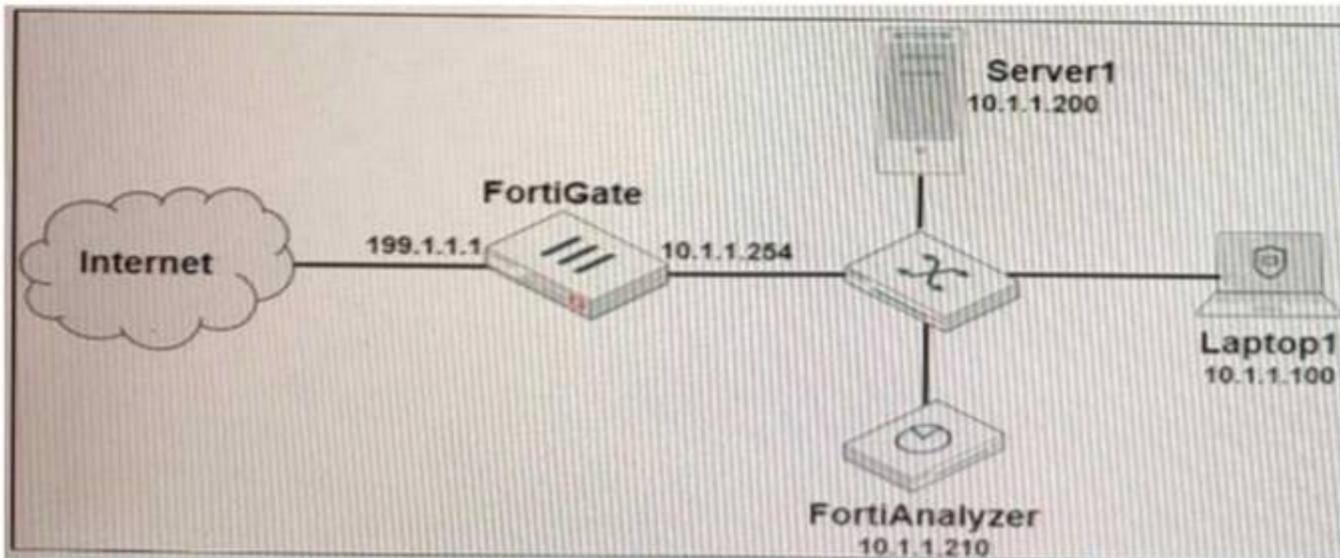
Laptopt is used by several administrators to manage FortiAnalyzer. You want to configure a generic text filter that matches all login attempts to the web interface generated by any user other than "admin" and coming from Laptop1:
Which filter will achieve the desired result?

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 4
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

NEW QUESTION 5

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 6
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

NEW QUESTION 7
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 8
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 FortiAnalyze
C. all stored logs are considered to be offline logs.
D. Logs that are indexed and stored in the SQL database.
E. Logs that are collected from offline devices after they boot up.

Answer: A

NEW QUESTION 9
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 10
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.

Answer: C

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

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 15
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 20
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: BD

Explanation:
Option B is correct because you must establish an IPsec tunnel ID and pre-shared key to secure the communication between FortiAnalyzer and FortiGate with IPsec12. The tunnel ID is a unique identifier for each tunnel and the pre-shared key is a secret passphrase that authenticates the peers.
Option D is correct because IPsec is only enabled through the CLI on FortiAnalyzer1. You cannot configure IPsec settings through the GUI on FortiAnalyzer.

NEW QUESTION 24
Which statement is true when you are upgrading the firmware on an HA cluster made up of two FortiAnalyzer devices?

A. First, upgrade the secondary device, and then upgrade the primary device.
B. Both FortiAnalyzer devices will be upgraded at the same time.
C. You can enable uninterruptible-upgrade so that the normal FortiAnalyzer operations are not interrupted while the cluster firmware upgrades.
D. You can perform the firmware upgrade using only a console connection.

Answer: A

Explanation:
FortiAnalyzer_7.0_Study_Guide-Online.pdf page 64: To upgrade FortiAnalyzer HA cluster firmware:
* 1. Log in to each secondary device.
* 2. Upgrade the firmware of all secondary devices.
* 3. Wait for the upgrades to complete and verify that all secondary devices joined the cluster.
* 4. Verify that logs on all secondary devices are synchronized with the primary device.
* 5. Upgrade the primary device.
https://docs.fortinet.com/document/fortianalyzer/7.2.0/upgrade-guide/262607/upgrading-fortianalyzer-firmware

NEW QUESTION 29
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

NEW QUESTION 30
Which clause is considered mandatory in SELECT statements used by the FortiAnalyzer to generate reports?

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

Answer: A

NEW QUESTION 33
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-a

NEW QUESTION 34

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.

Answer: B

NEW QUESTION 37

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

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

Answer: AC

Explanation:
A) FortiAnalyzer_7.0_Study_Guide-Online.pdf page 148: The log communication between devices can be protected by encryption, with the desired encryption level, using the commands shown on the slide. (You need to interpret this. "Real time" and "aggregation" is about the "moment" when Fortigate sends the logs. However, no matter the moment, Fortigate will upload logs encrypted or unencrypted based on previous / differente config).
C) FortiAnalyzer_7.0_Study_Guide-Online.pdf page 147: Aggregation: Logs and content files stored and uploaded at scheduled time.

NEW QUESTION 40

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

Answer: D

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"

NEW QUESTION 44

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 46

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 ADO
D. you can assign FortiGate VDOMs from a single FortiGate device to multiple FortiAnalyzer ADOMs.
E. Normal mode is the default ADOM mode.

Answer: CD

NEW QUESTION 50

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

Answer: A

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

NEW QUESTION 55
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 mod
D. FortiAnalyzer supports event management and reporting features.
E. 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

Answer: AD

NEW QUESTION 57
Which two statements are true regarding high availability (HA) on FortiAnalyzer? (Choose two.)

A. FortiAnalyzer HA can function without VRR
B. and VRRP is required only if you have more than two FortiAnalyzer devices in a cluster.
C. FortiAnalyzer HA supports synchronization of logs as well as some system and configuration settings.
D. All devices in a FortiAnalyzer HA cluster must run in the same operation mode: analyzer or collector.
E. FortiAnalyzer HA implementation is supported by many public cloud infrastructures such as AWS, Microsoft Azure, and Google Cloud.

Answer: BC

NEW QUESTION 61
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 66
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 69
Why run the command diagnose sql status sqlplugind?

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

Answer: C

NEW QUESTION 73
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.

Answer: A

NEW QUESTION 76
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 78
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

Answer: A

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


NEW QUESTION 81
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 82
Refer to the exhibit.
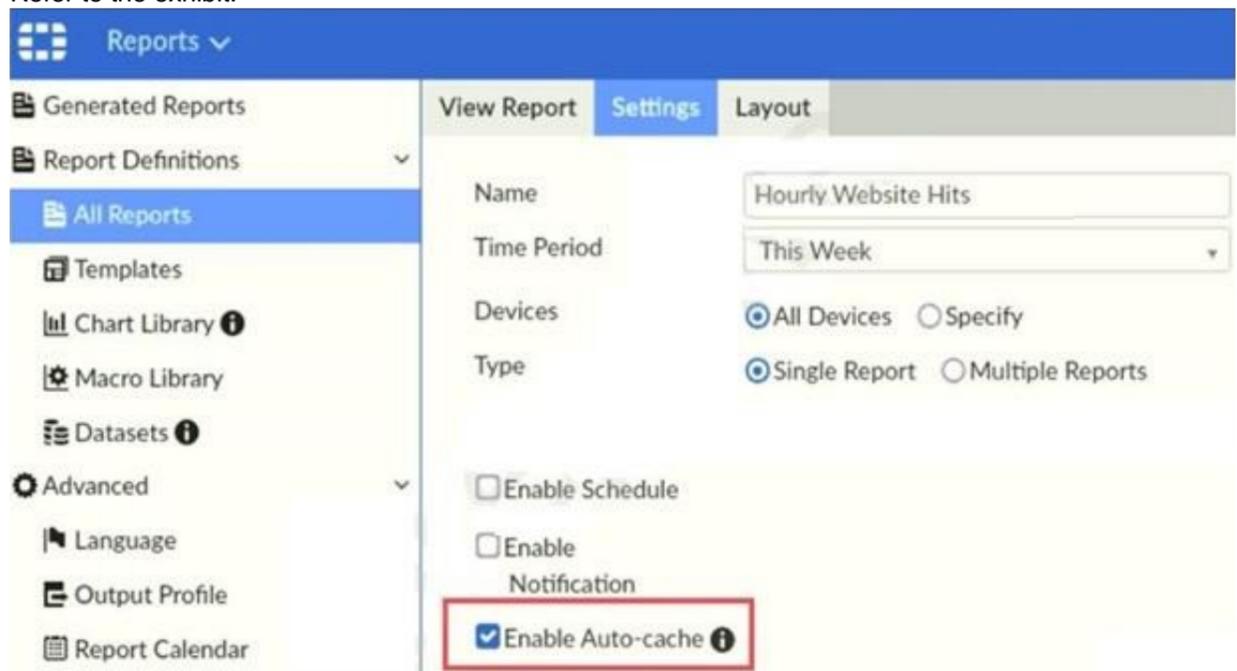
Which two statements are true regarding enabling auto-cache on FortiAnalyzer? (Choose two.)

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 83
Which daemon is responsible for enforcing raw log file size?

A. logfiled
B. oftpd

C. sqlplugind
D. miglogd

Answer: A

NEW QUESTION 88
View the exhibit.

Insert Rate vs Receive Rate - Last 1 hour
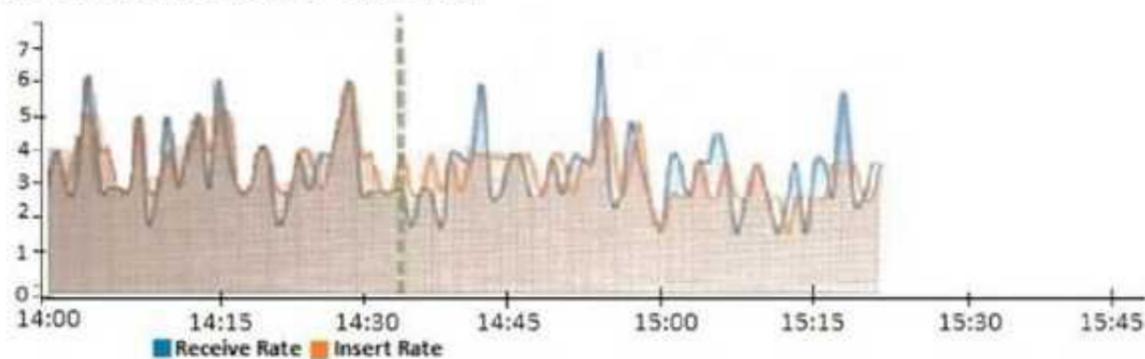
What does the data point at 14:35 tell you?

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.

Answer: B

Explanation:
https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/47690/insert-rate-vs-receive-rate-wi

NEW QUESTION 92
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

Answer: A

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/ta-

NEW QUESTION 94
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 96
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 98
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

Answer: AB

NEW QUESTION 103
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

NEW QUESTION 104
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

Answer: BD

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

NEW QUESTION 109
A playbook contains five tasks in total. An administrator runs the playbook and four out of five tasks finish successfully, but one task fails. What will be the status of the playbook after it is run?

A. Running
B. Failed
C. Upstream_failed
D. Success

Answer: B

NEW QUESTION 111
If you upgrade the FortiAnalyzer firmware, which report element can be affected?

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

Answer: A

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

NEW QUESTION 115
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

Answer: B

Explanation:

https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/368682/disk-space-allocation

NEW QUESTION 119
Which statement about the FortiSIEM management extension is correct?

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

Answer: A

NEW QUESTION 120
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.

Answer: AD

NEW QUESTION 125
You crested 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. FortiAnalyzer Event Handler
B. Incoming webhook
C. FortiOS Event Log
D. Fabric Connector event

Answer: B

Explanation:
"One possible scenario is shown on the slide:
* 1. Traffic flows through the FortiGate
* 2. FortiGate sends logs to FortiAnalyzer
* 3. FortiAnalyzer detects some suspicious traffic and generates an event
* 4. The event triggers the execution of a playbook in FortiAnalyzer, which sends a webhook call to FortiGate so that it runs an automation stitch
* 5. FortiGate runs the automation stitch with the corrective or preventive actions" FortiAnalyzer_7.0_Study_Guide-Online page 228
In order to see the actions related to the FOS connector, you must enable an automation rule using the Incoming Webhook Call trigger on the FortiGate side.
FortiAnalyzer_7.0_Study Guide page no 233

NEW QUESTION 127
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.

Answer: B

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

NEW QUESTION 130
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

Answer: A

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

NEW QUESTION 131
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

Answer: BD

Explanation:
https://help.fortinet.com/fa/cli-olh/5-6-5/Content/Document/1400_execute/backup.htm

NEW QUESTION 134
Refer to the exhibit.

Which statement is correct regarding the event displayed?

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

Answer: A

Explanation:
Events in FortiAnalyzer will be in one of four statuses. The current status will determine if more actions need to be taken by the security team or not.
The possible statuses are:
Unhandled: The security event risk is not mitigated or contained, so it is considered open. Contained: The risk source is isolated.
Mitigated: The security risk is mitigated by being blocked or dropped. (Blank): Other scenarios.
FortiAnalyzer_7.0_Study_Guide-Online pag. 206

NEW QUESTION 137
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

Answer: AB

NEW QUESTION 142
Refer to the exhibit.
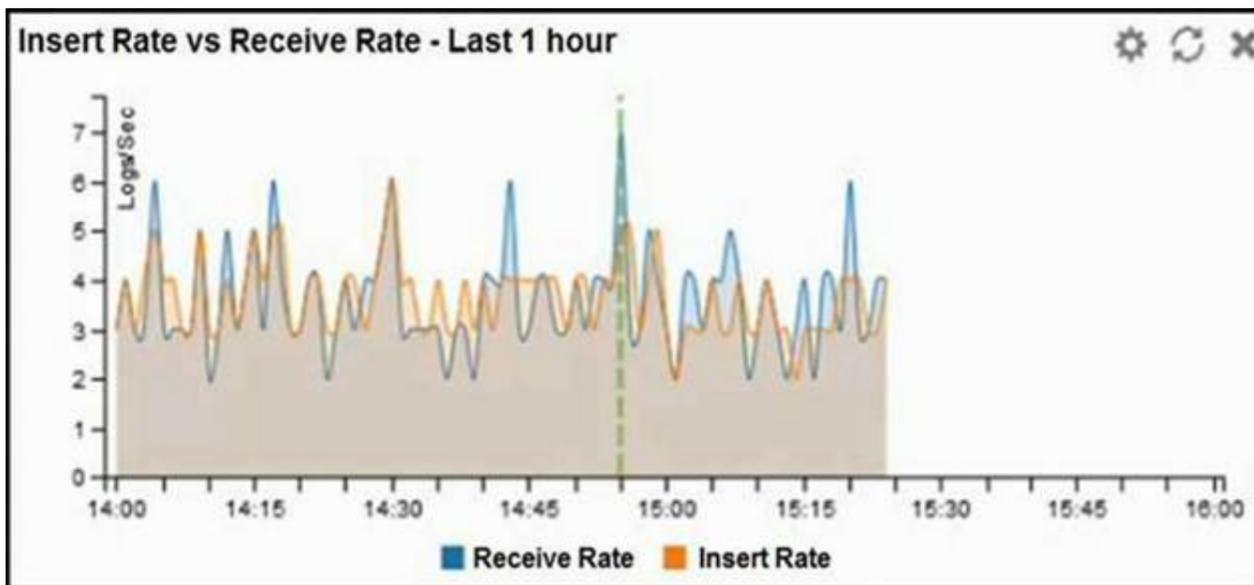
What does the data point at 14:55 tell you?

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 147
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

Answer: D

NEW QUESTION 148
Refer to the exhibit.
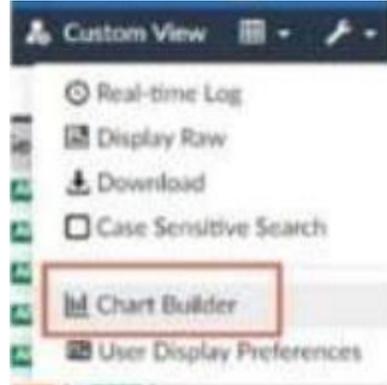
What is the purpose of using the Chart Builder feature on FortiAnalyzer?

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.

Answer: A

NEW QUESTION 153
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.

Answer: D

NEW QUESTION 158
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

Answer: B

Explanation:
https://docs.fortinet.com/document/fortianalyzer/6.2.0/administration-guide/743670/configuring-log-storage-pol

NEW QUESTION 162
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 163
Refer to the exhibit.
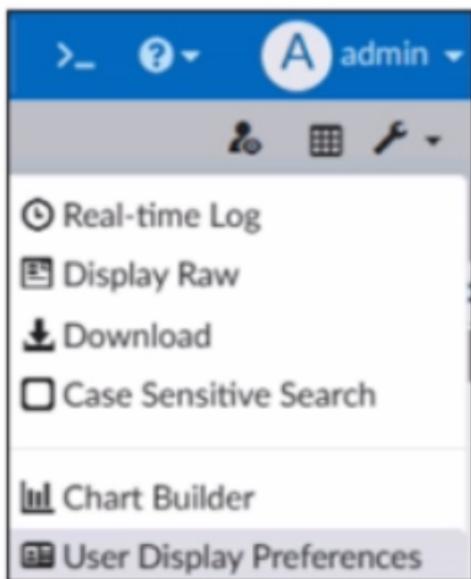
What is the purpose of using the Chart Builder feature on FortiAnalyzer?

A. To add a new chart under FortiView to be used in new reports
B. To build a dataset and chart automatically, based on the filtered search results
C. To add charts directly to generate reports in the current ADOM
D. To build a chart automatically based on the top 100 log entries

Answer: B

NEW QUESTION 166
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

Answer: A

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

NEW QUESTION 171
Which FortiAnalyzer feature allows you to use a proactive approach when managing your network security?

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

Answer: B

Explanation:
FortiAnalyzer_7.0_Study_Guide-Online.pdf page 217: Threat hunting consists in proactively searching for suspicious or potentially risky network activity in your environment. The proactive approach will help administrator find any threats that might have eluded detection by the current security solutions or configurations.

NEW QUESTION 176
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 178
Refer to the exhibit.
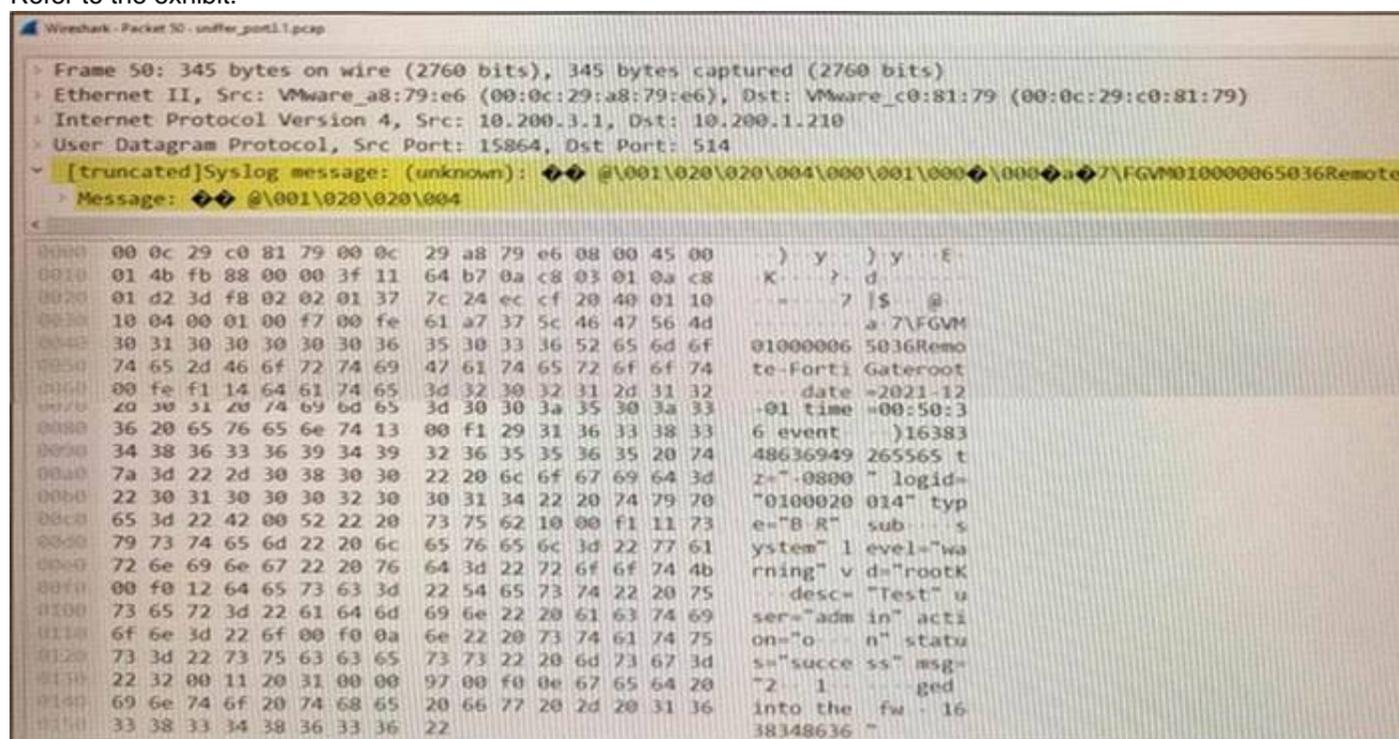
Which image corresponds to the packet capture shown in the exhibit?
A)
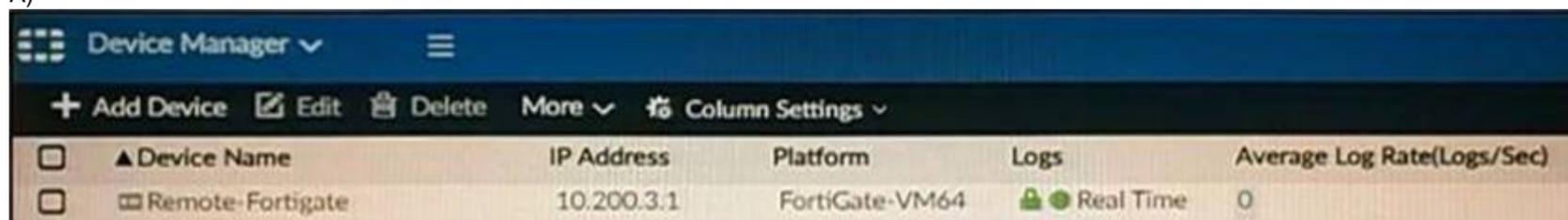
B)
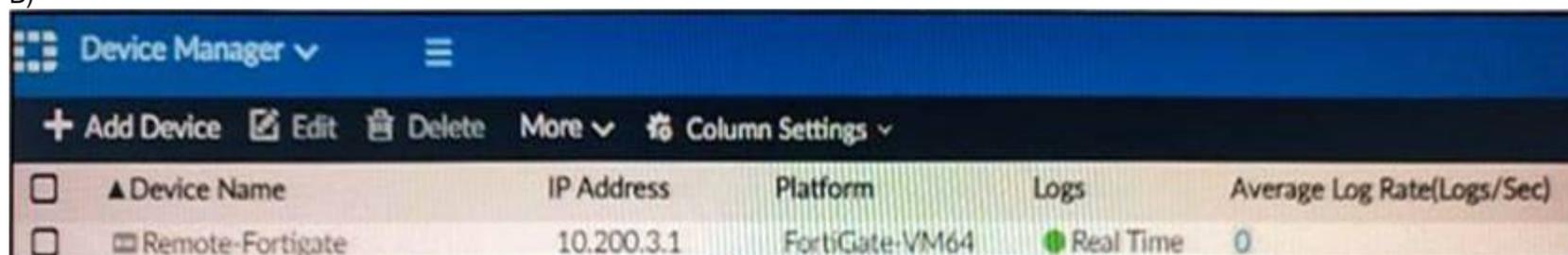
C)

D)

A. Option A
B. Option B
C. Option C
D. Option D

Answer: C

NEW QUESTION 181
......

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual NSE5_FAZ-7.0 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the NSE5_FAZ-7.0 Product From:

https://www.2passeasy.com/dumps/NSE5_FAZ-7.0/

Money Back Guarantee

NSE5_FAZ-7.0 Practice Exam Features:

* NSE5_FAZ-7.0 Questions and Answers Updated Frequently

* NSE5_FAZ-7.0 Practice Questions Verified by Expert Senior Certified Staff

* NSE5_FAZ-7.0 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* NSE5_FAZ-7.0 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year