Exam Questions NSE5_FAZ-7.0

Fortinet NSE 5 - FortiAnalyzer 7.0

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

NEW QUESTION 1
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 2
What is the purpose of using prefilters when configuring event handlers?

A. They limit which logs are checked for matches by the other filters.
B. They can filter the logs before they are processed by FortiAnalyzer
C. They download new filters to be used in event handlers.
D. They are common filters applied simultaneously to all event handlers.

Answer: A

NEW QUESTION 3
Which item must you configure on FortiAnalyzer to email generated reports automatically?

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

Answer: A

NEW QUESTION 4
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

NEW QUESTION 5
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

Answer: B

NEW QUESTION 6
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 7
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

Answer: D

Explanation:
https://kb.fortinet.com/kb/documentLink.do?externalID=FD46446#:~:text=On%20FortiAnalyzer%2FFortiMana 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.

NEW QUESTION 8
How can you configure FortiAnalyzer to permit administrator logins from only specific locations?

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

Answer: C

Explanation:
https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/186508/trusted-hosts

NEW QUESTION 9
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 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
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. You enabled auto-cache with extended log filtering.
B. The logfiled service has not indexed all the expected logs.
C. The logs were overwritten by the data retention policy.
D. The time frame selected in the report is wrong.

Answer: BC

NEW QUESTION 15
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 19
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 22
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 24
What is the best approach to handle a hard disk failure on a FortiAnalyzer that supports hardware RAID?

A. Hot swap the disk.
B. There is no need to do anything because the disk will self-recover.
C. Run execute format disk to format and restart the FortiAnalyzer device.
D. Shut down FortiAnalyzer and replace the disk

Answer: A

Explanation:
https://help.fortinet.com/fa/faz50hlp/56/5-6-2/FMG-FAZ/0700_RAID/0800_Swapping%20Disks.htm#:~:text=If

NEW QUESTION 25
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 30
Which two statement are true regardless initial Logs sync and Log Data Sync for Ha on FortiAnalyzer?

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

Answer: CD

NEW QUESTION 31
Which statement describes a dataset in FortiAnalyzer?

A. They determine what data is retrieved from the databas
B. They provide the layout used for reports.
C. They are used to set the data included in template
D. They define the chart types to be used in report

Answer: A

NEW QUESTION 32
On FortiAnalyzer, what is a wildcard administrator account?

A. An account that permits access to members of an LDAP group
B. An account that allows guest access with read-only privileges
C. An account that requires two-factor authentication
D. An account that validates against any user account on a FortiAuthenticator

Answer: A

Explanation:
https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/747268/configuring-wildcard-admin-accounts

NEW QUESTION 33
Which tabs do not appear when FortiAnalyzer is operating in Collector mode?

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

Answer: B

NEW QUESTION 34
Refer to the exhibit.

The exhibit shows "remoteservergroup" is an authentication server group with LDAP and RADIUS servers. Which two statements express the significance of enabling "Match all users on remote server" when
configuring a new administrator? (Choose two.)

A. It creates a wildcard administrator using LDAP and RADIUS servers.
B. Administrator can log in to FortiAnalyzer using their credentials on remote servers LDAP and RADIUS.
C. Use remoteadmin from LDAP and RADIUS servers will be able to log in to FortiAnalyzer at anytime.
D. It allows administrators to use two-factor authentication.

Answer: AB

NEW QUESTION 36
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 40
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 43
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 45
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

Answer: C

NEW QUESTION 47
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 49
An administrator fortinet, is able to view logs and perform device management tasks, such as adding and removing registered devices. However, administrator fortinet is not able to create a mall server that can be used to send email.
What could be the problem?

A. Fortinet is assigned the Standard_ User administrator profile.
B. A trusted host is configured.
C. ADOM mode is configured with Advanced mode.
D. Fortinet is assigned the Restricted_ User administrator profile.

Answer: A

Explanation:
• Super_User, which, like in FortiGate, provides access to all device and system privileges.
• Standard_User, which provides read and write access to device privileges, but not system privileges.
• Restricted_User, which provides read access only to device privileges, but not system privileges. Access to the Management extensions is also removed.
• No_Permissions_User, which provides no system or device privileges. Can be used, for example, to temporarily remove access granted to existing admins.
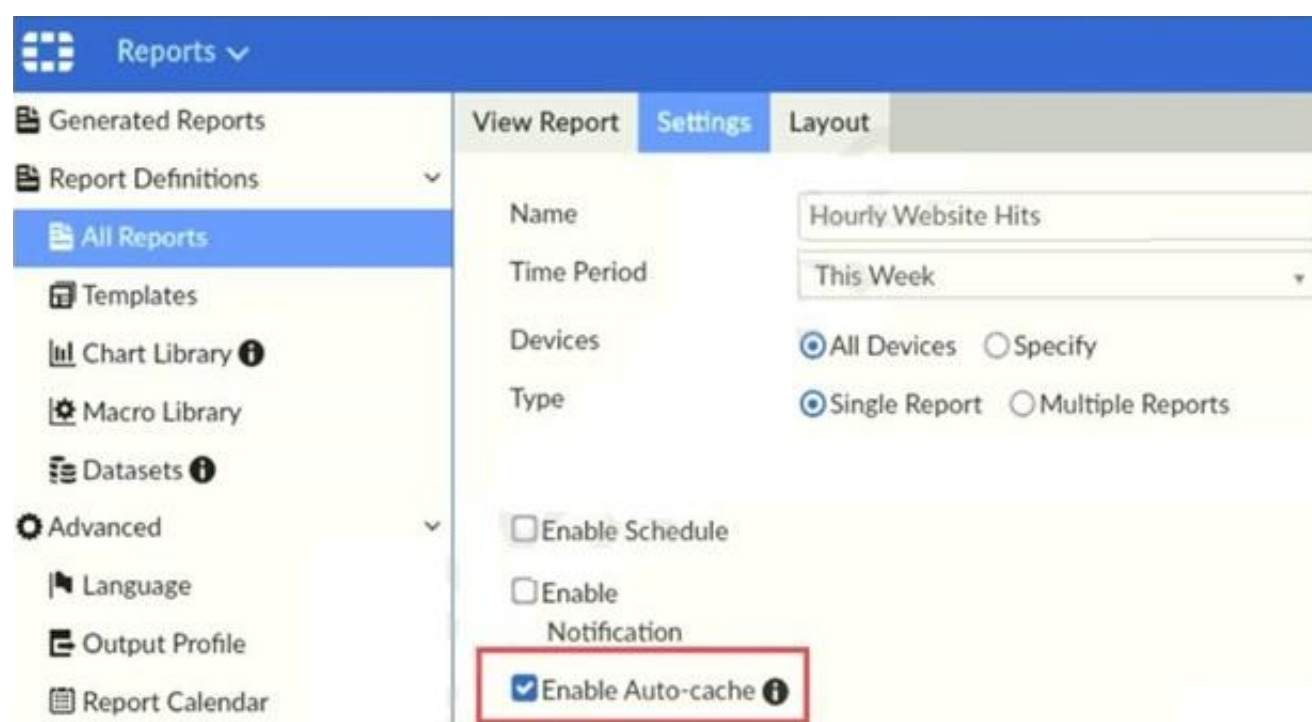FortiAnalyzer_7.0_Study_Guide-Online page 42

NEW QUESTION 53
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 54
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.
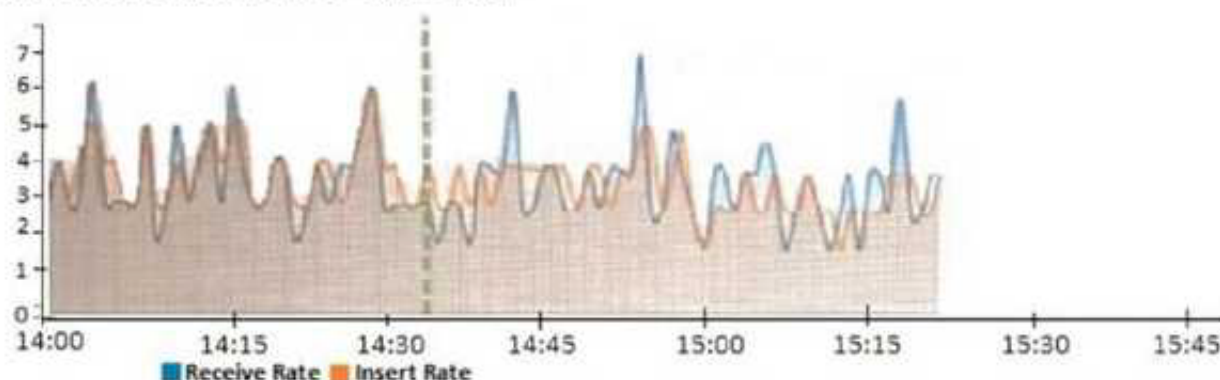
Answer: CD

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 58
View the exhibit.

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 60
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:

https://community.fortinet.com/t5/FortiAnalyzer/Technical-Note-How-to-swap-Hard-Disk-on-FortiAnalyzer/ta-

NEW QUESTION 61

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 62
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 64
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: A

NEW QUESTION 65
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 67
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 71
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 74
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 77
Which two elements are contained in a system backup created on FortiAnalyzer? (Choose two.)

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

Answer: AC

Explanation:
What does the System Configuration backup include?
System information, such as the device IP address and administrative user information. Device list, such as any devices you configured to allow log access.
Report information, such as any configured report settings, as well as all your custom report details. These are not the actual reports.
FortiAnalyzer_7.0_Study_Guide-Online pag. 29
FortiAnalyzer_7.0_Study_Guide-Online.pdf page 29: What does the System Configuration backup include?
• System information, such as the device IP address and administrative user information
• Device list, such as any devices you configured to allow log access
• Report information, such as any configured report settings, as well as all your custom report details. These are not the actual reports.

NEW QUESTION 82
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

NEW QUESTION 85
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 87
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 88
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 89
What are analytics logs on FortiAnalyzer?

A. Log type Traffic logs.
B. Logs that roll over when the log file reaches a specific size.
C. Logs that are indexed and stored in the SQL.
D. Raw logs that are compressed and saved to a log file.

Answer: C

NEW QUESTION 90
What is the purpose of output variables?

A. To store playbook execution statistics
B. To use the output of the previous task as the input of the current task
C. To display details of the connectors used by a playbook
D. To save all the task settings when a playbook is exported

Answer: B

Explanation:
FortiAnalyzer_7.0_Study_Guide-Online.pdf page 242: Output variables allow you to use the output from a preceding task as an input to the current task.
"Output variables allow you to use the output from a preceding task as an input to the current task." FortiAnalyzer_7.0_Study_Guide-Online page 242

NEW QUESTION 91
In Log View, you can use the Chart Builder feature to build a dataset and chart based on the filtered search results.
Similarly, which feature you can use for FortiView?

A. Export to Report Chart
B. Export to PDF
C. Export to Chart Builder
D. Export to Custom Chart

Answer: A

NEW QUESTION 95
In FortiAnalyzer's FormView, source and destination IP addresses from FortiGate devices are not resolving to a hostname. How can you resolve the source and destination IPs, without introducing any additional performance impact to FortiAnalyzer?

A. Configure local DNS servers on FortiAnalyzer
B. Resolve IPs on FortiGate
C. Configure # set resolve-ip enable in the system FortiView settings
D. Resolve IPs on a per-ADOM basis to reduce delay on FortiView while IPs resolve

Answer: B

NEW QUESTION 97
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 100
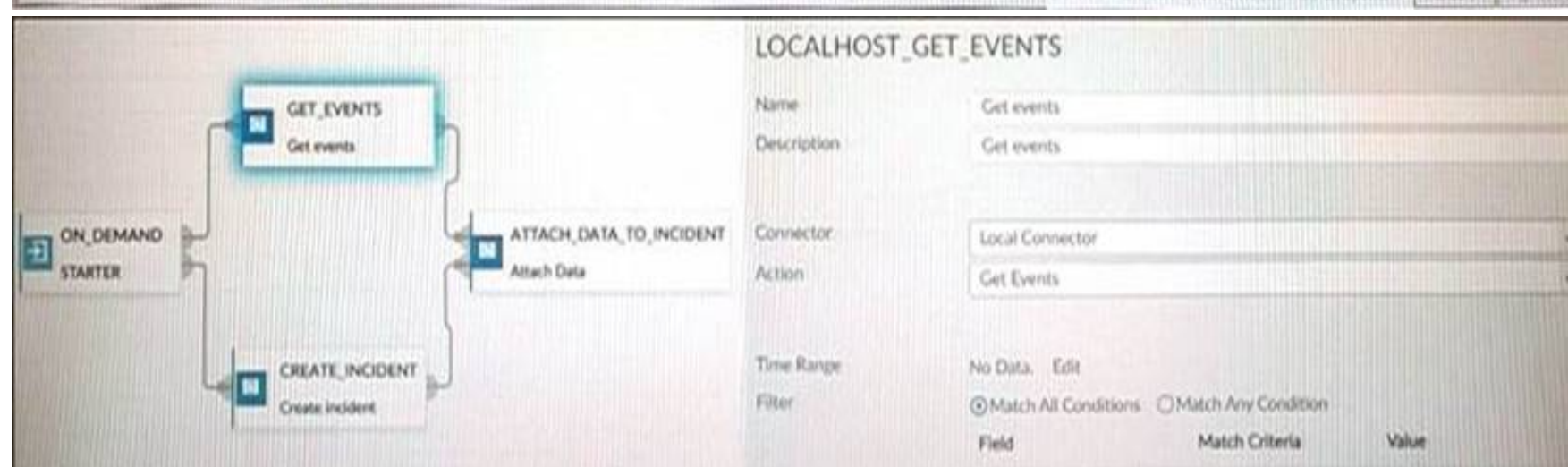If you upgrade your FortiAnalyzer firmware, what report elements can be affected?

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

Answer: D

NEW QUESTION 105
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 109
Which log will generate an event with the status Contained?

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

Answer: C

NEW QUESTION 114
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 119
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
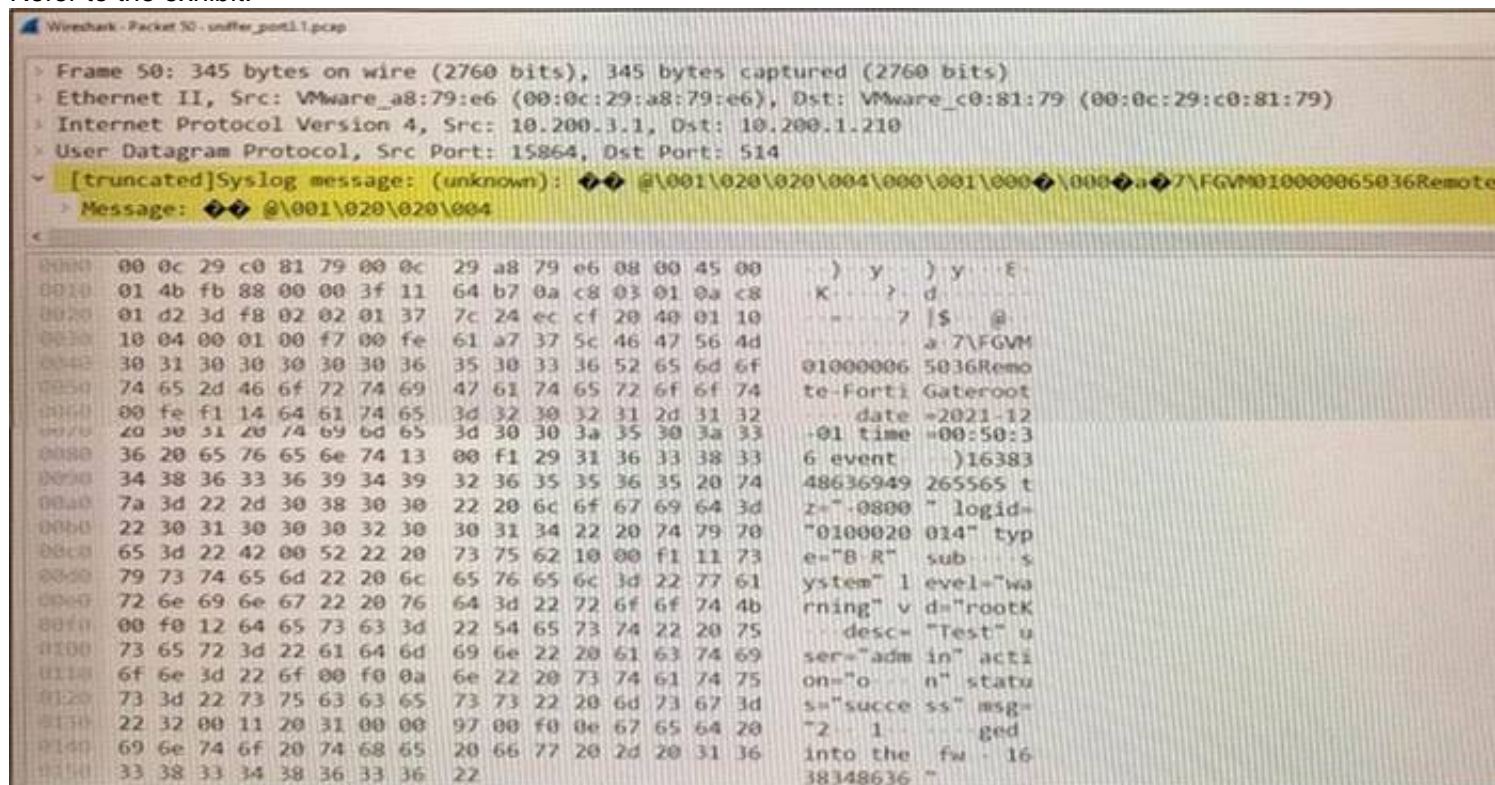
Answer: D

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
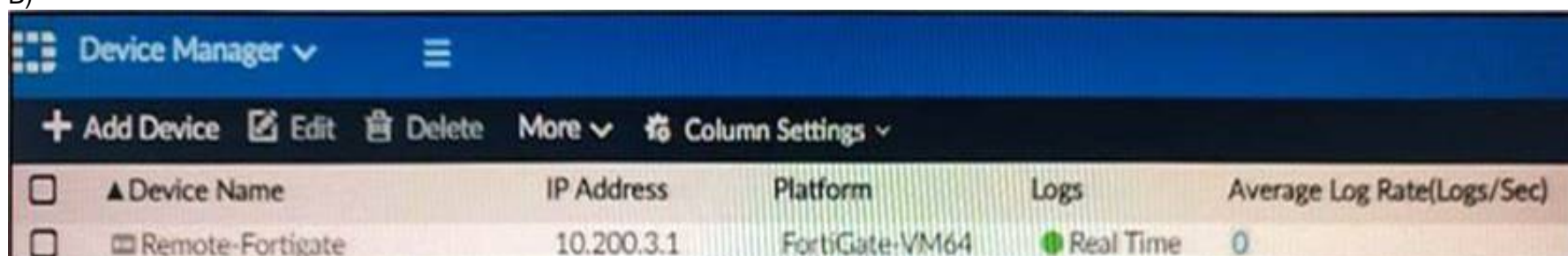
NEW QUESTION 121
Refer to the exhibit.

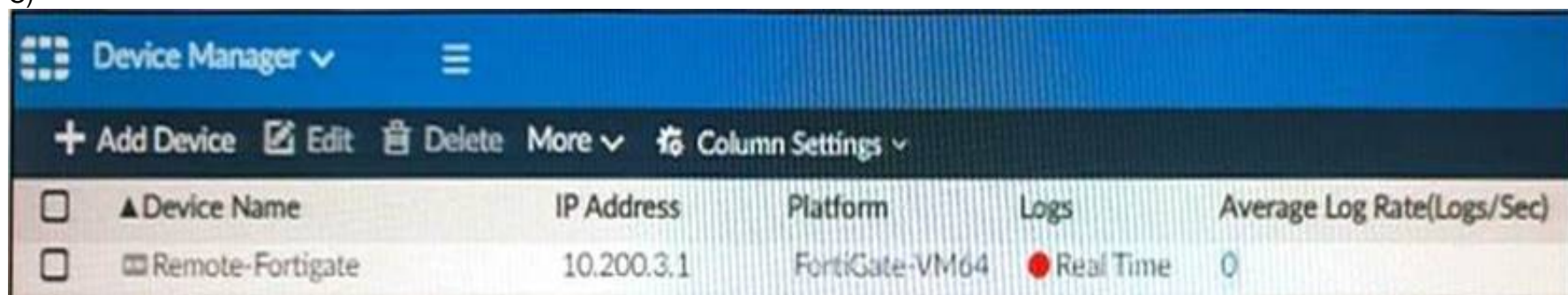Which image corresponds to the packet capture shown in the exhibit?

A)

B)

C)

D)

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

Answer: C

NEW QUESTION 125
......

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