Fortinet

Exam Questions FCP_FAZ_AN-7.6

Fortinet NSE 5 - FortiAnalyzer 7.6 Analyst

NEW QUESTION 1
What is the purpose of playbook trigger variables?

A. To display statistics about the playbook runtime
B. To use information from the trigger to filter the action in a task
C. To provide the trigger information to make the playbook start running
D. To store the start the times of playbooks with On_Schedule triggers

Answer: B

NEW QUESTION 2
Which statement about sending notifications with incident updates is true?

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

Answer: A

NEW QUESTION 3
Which statement about sending notifications with incident update is true?

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

Answer: A

Explanation:
In FortiOS and FortiAnalyzer,incident notificationscan be sent to multiple external platforms, not limited to a single method such as email. Fortinet's security fabric and integration capabilities allow notifications to be
sent through various fabric connectors and third-party integrations. This flexibility is designed to ensure that incident updates reach relevant personnel or systems using preferred communication channels, such as email, Syslog, SNMP, or integration with SIEM platforms.
Let??s review each answer option for clarity:
* Option A: You can send notifications to multiple external platforms
* This is correct. Fortinet??s notification system is capable of sending updates to multiple platforms, thanks to its support for fabric connectors and external integrations. This includes options such as email, Syslog, SNMP, and others based on configured connectors.
* Option B: Notifications can be sent only by email
* This is incorrect. Although email is a common method, FortiOS and FortiAnalyzer support multiple notification methods through various connectors, allowing notifications to be directed to different platforms as per the organization??s setup.
* Option C: If you use multiple fabric connectors, all connectors must have the same settings
* This is incorrect. Each fabric connector can have its unique configuration, allowing different connectors to be tailored for specific notification and integration requirements.
* Option D: Notifications can be sent only when an incident is updated or deleted
* This is incorrect. Notifications can be sent upon the creation of incidents, as well as upon updates or deletion, depending on the configuration.
:According to FortiOS and FortiAnalyzer 7.4.1 documentation, notifications for incidents can be configured across various platforms by using multiple connectors, and they are not limited to email alone. This capability is part of the Fortinet Security Fabric, allowing for a broad range of integrations with external systems and platforms for effective incident response.

NEW QUESTION 4
An administrator on your team has configured multiple reports to run periodically. Management has an additional request that all new generated reports be sent to a company email inbox for accessibility. The mail server has already been configured on FortiAnalyzer.
Which item must configure on FortiAnalyzer so that emails are sent when the reports are generated?

A. Enable the option to email all repots under the mail server.
B. Add amailto:<emailaddress> option within the report layouts.
C. Enable email notification under the report calendar.
D. Enable an output profile on the reports.

Answer: D

Explanation:
To ensure that reports generated by FortiAnalyzer are automatically sent to an email inbox, you need to set up an output profile for the reports. Output profiles specify where and how reports should be delivered, including the option to send them via email.
* Option A - Enable the Option to Email All Reports Under the Mail Server:
* The mail server configuration allows FortiAnalyzer to send emails but does not automatically enable email distribution for reports. This setting alone does not specify which reports to send or to whom.
* Conclusion:Incorrect.
* Option B - Add a mailto:<email address> Option Within the Report Layouts:
* Adding an email address within the report layout is not a standard configuration option for report distribution. Report layouts define the format andcontent of the report but not its distribution method.
* Conclusion:Incorrect.
* Option C - Enable Email Notification Under the Report Calendar:
* The report calendar is used to schedule when reports are generated. While it triggers report generation at specific times, it does not handle email distribution. Emailing reports requires a configured output profile.
* Conclusion:Incorrect.

* Option D - Enable an Output Profile on the Reports:
* An output profile can be configured on FortiAnalyzer to define delivery options, including emailing the report to specified recipients. This setup ensures that every time a report is generated according to the schedule, it is automatically emailed to the configured address.
* Conclusion:Correct. Conclusion:
* Correct Answer D. Enable an output profile on the reports.
* Configuring an output profile is the correct way to set up automatic email distribution of generated reports in FortiAnalyzer.
References:
FortiAnalyzer 7.4.1 documentation on configuring output profiles and report distribution settings.

NEW QUESTION 5
Refer to the exhibit.

	Event	Event Status	Event Type	Severity
☐	56834764387462384.org (4)	Unhandled	Web Filter	Critical
☐	Web traffic to C&C from 10.0.1.200 detected	Unhandled	Web Filter	Critical

Which statement about the displayed event is correct? (Choose one answer))

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

Answer: D

Explanation:
Comprehensive and Detailed Explanation: From Exact Extract of knowledge of FortiAnalyzer 7.6 Study guide documents:
In the exhibit, theEvent Statusshown isUnhandled(Event Type: Web Filter; Severity: Critical). The FortiAnalyzer study guide definesUnhandledevents as events whose security risk has not been addressed and is therefore still active/open. Specifically, it states:??Unhandled: The security risk is considered open.??
This directly matches optionD.
The other options correspond to different statuses or actions:
* Isolated/Containedapplies when the risk source is isolated (statusContained), notUnhandled.
* Escalatedrefers to events moved/raised for further action (statusEscalated), notUnhandled.
* Whether an incident was created cannot be concluded solely from the status ??Unhandled?? in the exhibit; the study guide ties incident creation to incident management workflows rather than equating ??Unhandled?? with an incident being created.

NEW QUESTION 6
Which two statement regarding the outbreak detection service are true? (Choose two.)

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

Answer: BC

NEW QUESTION 7
What are two effects of enabling auto-cache in a FortiAnalyzer report? (Choose two.)

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

Answer: AC

Explanation:
Enablingauto-cachein FortiAnalyzer reports is designed to improve the efficiency and speed of report generation by leveraging cached data. Let??s analyze each option to determine which effects are correct.
* Option A - The Generation Time for Reports is Decreased:
* When auto-cache is enabled, FortiAnalyzer can use previously cached data instead of reprocessing all log datafrom scratch each time a report is generated. This results in faster report generation times, especially for recurring reports that use similar datasets.
* Conclusion:Correct.
* Option B - Hard-Cache Data is Automatically Updated When New Logs are Received:
* Enabling auto-cache does not immediately update the cache with every new log received. Instead, the cache is updated when reports are generated, based on the existing logs up to that point. Therefore, auto-cache does not constantly refresh with each incoming log, which would be inefficient.
* Conclusion:Incorrect.
* Option C - FortiAnalyzer Local Cache is Used to Store Generated Reports:
* Auto-cache utilizes FortiAnalyzer??s local cache to store data used in reports, reducing the need to retrieve and process logs repeatedly. This cached data can be reused for subsequent report generation, enhancing performance.
* Conclusion:Correct.
* Option D - The Size of Newly Generated Reports is Optimized to Conserve Disk Space:
* Auto-cache does not directly impact the size ofthe report files themselves. It focuses on performance optimization through cached data for faster access, but it does not compress or optimize the storage size of the generated report.
* Conclusion:Incorrect.Conclusion:
* Correct Answer A. The generation time for reports is decreasedandC. FortiAnalyzer local cache is used to store generated reports.
* Enabling auto-cache helps reduce report generation time by using locally cached data and optimizes report processing, though it does not impact report size or continuously update with each new log.

References:
FortiAnalyzer 7.4.1 documentation on report caching, auto-cache functionality, and report generation optimizations.

NEW QUESTION 8
Which two statements about playbook execution are true? (Choose two)

A. FortiAnalyzer will not commit changes made by a Failed playbook
B. The Playbook Monitor provides troubleshooting logs
C. You can run the default debugging playbook to investigate playbook errors.
D. Even I the playbook status is Failed, individual tasks may have succeeded.

Answer: AB

NEW QUESTION 9
Refer to the exhibit with partial output:

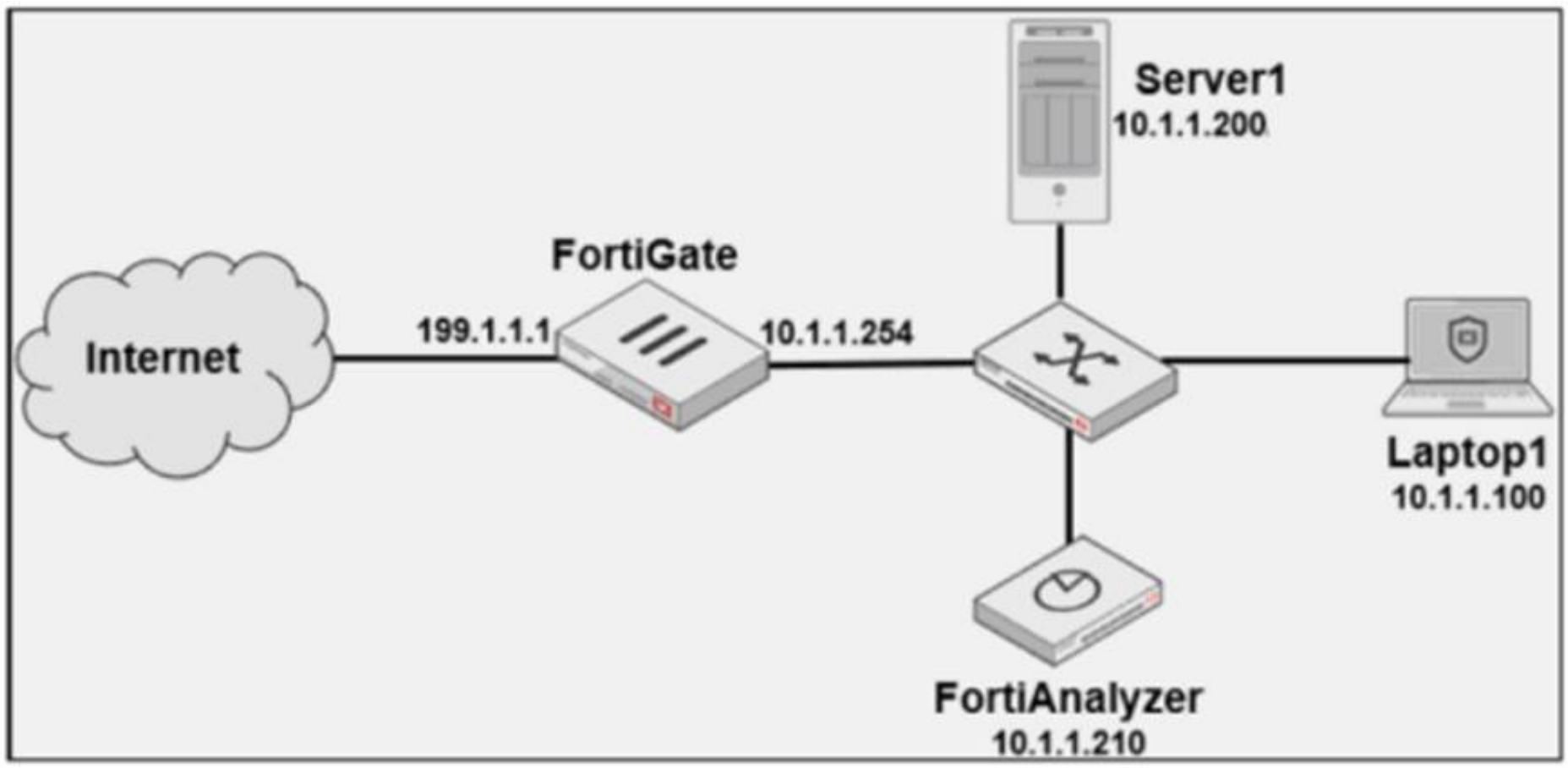
Your colleague exported a playbook and has sent it to you for review. You open the file in a text editor and observer the output as shown in the exhibit.
Which statement about the export is true?

A. The export data type is zipped.
B. The playbook is misconfigured.
C. The option to include the connector was not selected.
D. Your colleague put a password on the export.

Answer: A

Explanation:
In the exhibit, the data structure shows a checksum field and a data field with a long, seemingly encoded string. This format is indicative of a file that has been compressed or encoded for storage and transfer.
Export Data Type:
The data field is likely a base64-encoded string, which is commonly used to represent binary data in text format. Base64 encoding is often applied to data that has been compressed (zipped) for easier handling and transfer. The checksum field, with an MD5 hash, provides a way to verify the integrity of the data after decompression.
Option Analysis:
* A. The export data type is zipped: Correct. The compressed and encoded format of the data suggests that the export is in a zipped format, allowing for efficient storage and transfer.
* B. The playbook is misconfigured: There is no indication of misconfiguration in this exhibit. The presence of the checksum and data fields aligns with standard export practices.
* C. The option to include the connector was not selected: There is no evidence in the output to conclude that connectors are missing. Connectors are typically listed separately and would not directly affect the checksum and encoded data structure.
* D. Your colleague put a password on the export: There??s no indication of password protection in the exhibit. Password protection would likely alter the data structure, and there would be some mention of encryption.
Conclusion:
Correct Answer:A. The export data type is zipped.
This answer is consistent with the typical use of base64 encoding for compressed (zipped) data exports in FortiAnalyzer.
[References:, FortiAnalyzer 7.4.1 documentation on exporting playbooks and data compression methods.,]

NEW QUESTION 10
Exhibit.



Laptop1 is used by several administrators to manage FotiAnalyzer. 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 and performed_on==????GUI(10.1.1.100)?? and user!=admin
B. Operation-login and performed_on==????GU (10.1.1.120)?? and user!=admin
C. Operation-login and srcip== 10.1.1.100 anddstip==10.1.1.1.210 and user==admin
D. Operation-login and dstip==10.1.1.210 and user!-admin

Answer: A

Explanation:
The objective is to create a filter that identifies all login attempts to the FortiAnalyzer web interface (GUI) coming fromLaptop1(IP 10.1.1.100) and excludes the admin user. This filter should match any user other than admin.
Filter Components Analysis:
Operation-login: This portion of the filter will target login actions specifically, which is correct for filtering login attempts.
performed_on=="GUI(10.1.1.100)': This indicates that the login attempt must occur on the GUI interface and originate from the specified IP, which matches Laptop1's IP address (10.1.1.100). This ensures that the filter only matches GUI logins from this specific device.
user!=admin: This part excludes logins by the admin user, meeting the requirement to capture only non-admin users.
Option Analysis:
Option A: Correctly specifies theOperation-login,performed_on=="GUI(10.1.1.100)', anduser!=admin. This setup effectively filters login attempts to the GUI from Laptop1, excluding the admin user.
Option B: Uses the incorrect IP 10.1.1.120 in the performed_on filter, which does not match Laptop1's IP (10.1.1.100).
Option C: This option includessrcip==10.1.1.100anddstip==10.1.1.210but incorrectly specifiesuser==admininstead ofuser!=admin, which does not match the requirement to exclude admin users.
Option D: This option does not specify theperformed_onfield to restrict it to the GUI and only includesdstip(destination IP) withoutsrcip. It also incorrectly uses user!-admin instead of the correct syntaxuser!=admin.
Conclusion:
Correct Answer:A. Operation-login and performed_on=="GUI(10.1.1.100)' and user!=admin
This filter precisely captures the required conditions: login attempts from Laptop1 to the GUI interface by any user except admin.
[References:, FortiAnalyzer 7.4.1 documentation on log filters, syntax for login operations, and GUI login tracking.,]

NEW QUESTION 10
Refer to the exhibit.

```
adom_oid=198 itime=2025-05-27 08:35:24 loguid=7509149554218893312 epid=3 euid=3 data_parsername=FortiGate Log Parser data_sourceid=FGVM02TM24013423
data_sourcename=HQ-NGFW-1 root data_sourcetype=FortiGate data_timestamp=1748334923 app_cat=unscanned app_name=NTP app_service=NTP dst_intf=port2(undefined)
dst_ip=208.91.112.63 dst_port=123 event_action=accept event_id=13 event_policy=3 event_ref=751261e0-ce9e-51ef-f12e-a382acaf16d6 event_severity=notice
event_subtype=forward event_type=traffic host_location=Reserved host_owner=fortinet.com net_proto=17 net_rcvdpkts=1 net_rcvbytes=76 net_sentbytes=76 net_sentpkts=1
net_sessionduration=180 net_sessionid=1357 src_intf=port6(undefined) src_ip=10.0.13.125 src_natip=100.65.0.101 src_natport=50403 src_port=50403 dstepid=101 dsteuid=3
dst_geo_country=United States event_creation_time=27800868 event_uuid=0000000013 src_geo_country=Reserved logflag=1 data_sourcedom=root dst_intf_role=undefined
event_policyid=3 event_policytype=policy src_intf_role=undefined itime_t=1748360124 _logMeta=undefined
```

Which two observations can you make after reviewing this log entry? (Choose two answers))

A. This is a normalized log.
B. This is a formatted view of the log.
C. This is the original log that FortiAnalyzer received from FortiGate.
D. This log is in a raw log format.

Answer: AD

Explanation:
Comprehensive and Detailed Explanation From Exact Extract of knowledge of FortiAnalyzer 7.6 Study guide documents:
The exhibit shows the log as a single-line key/value entry (not a columnar/table display), which aligns with FortiAnalyzer'sraw log formatview option. The study guide states:"You can toggle between viewing formatted and raw logs."This directly supports observationD.
At the same time, what you are viewing in FortiAnalyzer Log View isnormalizeddata (FortiAnalyzer parses and maps device logs into standardized fields for consistent searching and analysis). The study guide explicitly states:"The log view allows you to view all log types received by FortiAnalyzer in normalized log

format.??It also explains that FortiAnalyzer "uses predefined parsers to extract key fields from ingested logs and maps them to a consistent, standardized set of field names," then stores them as normalized logs in the SIEM database. This supports observationA.
Finally, the study guide clarifies that even when you switch to raw log format in FortiAnalyzer, you are still observing the normalized-field representation produced by FortiAnalyzer's parser/normalization process (rather than the untouched original device message). It notes that a FortiGate event log "has been normalized by FortiAnalyzer," and when you switch "to raw log format," you can observe the effect of normalization on common fields. This is whyCis not the best description for the exhibit.

NEW QUESTION 15
Exhibit.

Event	Event Status	Event Type	Severity
bujyqttatbsd.findhere.org (1)	Mitigated	Web Filter	Low
Web request to suspicious destination from 10.0.3.20 blocked	Mitigated	Web Filter	Low

Which statement about the event displayed is correct?

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

Answer: C

NEW QUESTION 19
Exhibit.

```
FAZ # diagnose fortilogd lograte
last 5 seconds: 70.0, last 30 seconds: 132.1, last 60 seconds: 133.3

FAZ # diagnose fortilogd msgrate
last 5 seconds: 1.4, last 30 seconds: 1.6, last 60 seconds: 1.6
```

What can you conclude about the output?

A. The message rate being lower that the log rate is normal.
B. Both messages and logs are almost finished indexing.
C. There are more traffic logs than event logs.
D. The output is ADOM specific

Answer: A

Explanation:
In this output, we see two diagnostic commands executed on a FortiAnalyzer device:
diagnose fortilogd lograte: This command shows the rate at which logs are being processed by the FortiAnalyzer in terms of log entries per second.
diagnose fortilogd msgrate: This command displays the message rate, or the rate at which individual messages are being processed.
The values provided in the exhibit output show:
Log rate (lograte): Consistently high, showing values such as 70.0, 132.1, and 133.3 logs per second over different time intervals.
Message rate (msgrate): Lower values, around 1.4 to 1.6 messages per second. Explanation
Interpretation of log rate vs. message rate: In FortiAnalyzer, the log rate typically refers to the rate of logs being stored or indexed, while the message rate refers to individual messages within these logs. Given that a single log entry can contain multiple messages, it's common to see a lower message rate relative to the log rate.
Understanding normal operation: In this case, the message rate being lower than the log rate is expected and typical behavior. This discrepancy can arise because each log entry may bundle multiple related messages, reducing the message rate relative to the log rate.
Conclusion
Correct Answer A. The message rate being lower than the log rate is normal.
This aligns with thenormal operational behavior of FortiAnalyzer in processing logs and messages.
There is no indication that both logs and messages are nearly finished indexing, as that would typically show diminishing rates toward zero, which is not the case here. Additionally, there's no information in this output about specific ADOMs or a comparison between traffic logs and event logs. Thus, options B, C, and D are incorrect.
[References:, FortiOS 7.4.1 and FortiAnalyzer 7.4.1 command guides for diagnose fortilogd lograte and diagnose fortilogd msgrate.,]

NEW QUESTION 21
You need to move reports between two ADOMs.
Which two statements are true? (Choose two.)
A. The ADOMs must be compatible types.
B. The date and time will be appended to the original report name to avoid conflicts.
C. All charts and datasets associated with the report will be imported together.
D. You need to convert the reports into templates first.

A.

Answer: AC

Explanation:
From Exact Extract of knowledge of FortiAnalyzer 7.6 Study guide documents:
FortiAnalyzer supports moving reporting content across ADOMs by importing/exporting reporting objects, but it enforces ADOM compatibility. The study guide states: "You can, however, import and export reports and charts ... into different ADOMs ..." and explicitly requires that "Both ADOMs must be of the same type." This directly validates statement A.
For report dependencies, the study guide clarifies how datasets are handled during transfer. While "You can't export templates and datasets," it also explains that

when you export a chart, "the associated dataset is exported with it, so when you import an exported chart, the associated dataset is imported as well." Since reports are composed of charts (and charts depend on datasets), moving a report between ADOMs entails moving its charts; when those charts are exported/imported, their datasets come with them. This supports statement C based on the documented chartdataset import/export behavior.
Statement D is not required because the study guide explicitly indicates you can "export and import reports" directly, and additionally notes that on import "you can save the layout of the report as a template" (optional, not a prerequisite).

NEW QUESTION 25
Which statement regarding macros on FortiAnalyzer is true?
A. Macros are predefined templates for reports and cannot be customized.
B. Macros are useful in generating excel log files automatically based on the report settings.
C. Macros are ADOM-specific and each ADOM type have unique macros relevant to that ADOM.
D. Macros are supported only on the FortiGate ADOMs.

A.

Answer: B

Explanation:
Macros in FortiAnalyzer are used to streamline reporting tasks by automating data extraction and report generation. Here's a breakdown of each option to determine the correct answer:
Option A - Macros are Predefined Templates for Reports and Cannot be Customized:
This statement is incorrect. Macros in FortiAnalyzer are not simply fixed templates; they allow for customization to tailor data extraction and reporting based on specific needs and configurations.
Conclusion: Incorrect.
Option B - Macros are Useful in Generating Excel Log Files Automatically Based on the Report Settings:
This statement is accurate. Macros in FortiAnalyzer can be configured to automate the generation of reports, including outputting log data to Excel format based on predefined report settings. This makes them especially useful for scheduled reporting and data analysis.
Conclusion: Correct.
Option C - Macros are ADOM-Specific and Each ADOM Type Has Unique Macros Relevant to that ADOM:
Macros are not limited to specific ADOMs, nor are they ADOM-specific. Macros can be applied across various ADOMs based on report configurations but are not inherently tied to or unique for each ADOM type.
Conclusion: Incorrect.
Option D - Macros are Supported Only on the FortiGate ADOMs:
This is not true. Macros in FortiAnalyzer are not restricted to FortiGate ADOMs; they can be utilized across different ADOMs that FortiAnalyzer manages.
Conclusion: Incorrect.Conclusion:
Correct Answer B. Macros are useful in generating excel log files automatically based on the report settings.
This answer correctly describes the functionality of macros in FortiAnalyzer, emphasizing their role in automating report generation, especially for Excel log files.
FortiAnalyzer 7.4.1 documentation on macros and report generation functionalities.

NEW QUESTION 26
Which statement about SQL SELECT queries is true?

A. They can be used to purge log entries from the database.
They must be followed immediately by a WHERE clause.
B. They can be used to display the database schema.
C. They are not used in macros.
D.

Answer: D

Explanation:
Option A - Purging Log Entries:
A SELECT query in SQL is used to retrieve data from a database and does not have the capability to delete or purge log entries. Purging logs typically requires a DELETE or TRUNCATE command.
Conclusion: Incorrect.
Option B - WHERE Clause Requirement:
In SQL, a SELECT query does not require a WHERE clause. The WHERE clause is optional and is used only when filtering results. A SELECT query can be executed without it, meaning this statement is false.
Conclusion: Incorrect.
Option C - Displaying Database Schema:
A SELECT query retrieves data from specified tables, but it is not used to display the structure or schema of the database. Commands like DESCRIBE, SHOW TABLES, or SHOW COLUMNS are typically used to view schema information.
Conclusion: Incorrect.
Option D - Usage in Macros:
FortiAnalyzer and similar systems often use macros for automated functions or specific query-based tasks. SELECT queries are typically not included in macros because macros focus on procedural or repetitive actions, rather than simple data retrieval.
Conclusion: Correct.
Conclusion:
Correct Answer D They are not used in macros.
This aligns with typical SQL usage and the specific functionalities of FortiAnalyzer.
Reference: FortiAnalyzer 7.4.1 documentation on SQL queries, database operations, and macro usage

NEW QUESTION 28
Which log will generate an event with the status Unhandled?

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

Answer: B

Explanation:
In FortiOS 7.4.1 and FortiAnalyzer 7.4.1, the "Unhandled" status in logs typically signifies that the FortiGate encountered a security event but did not take any specific action to block or alter it. This usually occurs in the context of Intrusion Prevention System (IPS) logs.
IPS logs with action=pass: When the IPS engine inspects traffic and determines that it does not match any known attack signatures or violate any configured policies, it assigns the action "pass". Since no action is taken to block or modify this traffic, the status is logged as "Unhandled."
Let's look at why the other options are incorrect:
An AV log with action=quarantine: Antivirus (AV) logs with the action "quarantine" indicate that a file was detected as malicious and moved to quarantine. This is a definitive action, so the status wouldn't be "Unhandled."
A WebFilter log will action=dropped: WebFilter logs with the action "dropped" indicate that web traffic was blocked according to the configured web filtering policies. Again, this is a specific action taken, not an "Unhandled" event.
An AppControl log with action=blocked: Application Control logs with the action "blocked" mean that an application was denied access based on the defined application control rules. This is also a clear action, not "Unhandled."

NEW QUESTION 29
Exhibit.

FortiAnalyzer partial configuration output

FortiAnalyzer1# get system status
Platform Type : FAZVM64-KVM
Platform Full Name : FortiAnalyzer-VM64-KVM
Version : v7.4.1-build2308 230831 (GA)
Serial Number : FAZ-VM0000065040
BIOS version : 04000002
Hostname : FortiAnalyzer1
Max Number of Admin Domains : 5
Admin Domain Configuration : Enabled
FIPS Mode : Disabled
HA Mode : Stand Alone
Branch Point : 2308
Release Version Information : GA
Time Zone : (GMT-8:00) Pacific Time (US & Canada)
Disk Usage : Free 43.60GB, Total 58.80GB
File System : Ext4
License Status : Valid

FortiAnalyzer1# get system global
adom-mode : normal
adom-select : enable
adom-status : enable
console-output : standard
country-flag : enable
enc-algorithm : high
ha-member-auto-grouping : enable
hostname : FortiAnalyzer1
log-checksum : md5
log-forward-cache-size : 5
log-mode : analyzer
longitude : (null)
max-aggregation-tasks : 0
max-running-reports : 1
oftp-ssl-protocol : tlsv1.2
ssl-low-encryption : disable
ssl-protocol : tlsv1.3 tlsv1.2
task-list-size : 2000
webservice-proto : tlsv1.3 tlsv1.2

FortiAnalyzer2# get system status
Platform Type : FAZVM64-KVM
Platform Full Name : FortiAnalyzer-VM64-KVM
Version : v7.4.1-build2308 230831 (GA)
Serial Number : FAZ-VM0000065041
BIOS version : 04000002
Hostname : FortiAnalyzer2
Max Number of Admin Domains : 5
Admin Domain Configuration : Enabled
FIPS Mode : Disabled
HA Mode : Stand Alone
Branch Point : 2308
Release Version Information : GA
Time Zone : (GMT-8:00) Pacific Time (US & Canada)
Disk Usage : Free 45.75GB, Total 58.80GB
File System : Ext4
License Status : Valid

FortiAnalyzer2# get system global
adom-mode : normal
adom-select : enable
adom-status : enable
console-output : standard
country-flag : enable
enc-algorithm : high
ha-member-auto-grouping : enable
hostname : FortiAnalyzer2
log-checksum : md5
log-forward-cache-size : 5
log-mode : analyzer
longitude : (null)
max-aggregation-tasks : 0
max-running-reports : 1
oftp-ssl-protocol : tlsv1.2
ssl-low-encryption : disable
ssl-protocol : tlsv1.3 tlsv1.2
task-list-size : 2000
webservice-proto : tlsv1.3 tlsv1.2

FortiAnalyzer3# get syste
Platform Type
Platform Full Name
Version : v7.4.1-build2308 230831 (GA)
Serial Number : FAZ-VM0000065042
BIOS version : 04000002
Hostname : FortiAnalyzer3
Max Number of Admin Domains : 5
Admin Domain Configuration : Enabled
FIPS Mode : Disabled
HA Mode : Stand Alone
Branch Point : 2308
Release Version Information : GA
Time Zone : (GMT-8:00) Pacific Time (US & Canada)
Disk Usage : Free 53.06GB, Total 79.80GB
File System : Ext4
License Status : Valid

FortiAnalyzer3# get system global
adom-mode : normal
adom-select : enable
adom-status : enable
console-output : standard
country-flag : enable
enc-algorithm : high
ha-member-auto-grouping : enable
hostname : FortiAnalyzer3
log-checksum : md5
log-forward-cache-size : 5
log-mode : analyzer
longitude : (null)
max-aggregation-tasks : 0
max-running-reports : 5
oftp-ssl-protocol : tlsv1.2
ssl-low-encryption : disable
ssl-protocol : tlsv1.3 tlsv1.2
task-list-size : 2000
webservice-proto : tlsv1.3 tlsv1.2

Based on the partial outputs displayed, which devices can be members of a FotiAnalyzer Fabric?

A. FortiAnalayzer1 and FortiAnalyzer3
B. FortiAnalyzer1 and FortiAnalyzer2
C. FortiAnalyzer2 and FortiAnalyzer3
D. All devices listed can be members.

Answer: D

Explanation:
In a FortiAnalyzer Fabric, devices can participate in a cluster or grouping if they meet specific compatibility criteria.
Based on the outputs provided, let's evaluate these criteria:
Version Compatibility:
All three devices, FortiAnalyzer1, FortiAnalyzer2, and FortiAnalyzer3, are running version v7.4.1-build0238, which is the same across the board. This version alignment is crucial because FortiAnalyzer Fabric requires that devices run compatible firmware versions for seamless communication and management.
Platform Type and Configuration:
All three devices are configured as Standalone in the HA mode, which allows them to operate independently but does not restrict their participation in a FortiAnalyzer Fabric. Each device is also on the FAZVM64-KVM platform type, ensuring hardware compatibility.
Global Settings:
Key settings such as adm-mode, adm-status, and adom-mode are consistent across all devices (adm-mode: normal, adm-status: enable, adom-mode: normal), which aligns with requirements for fabric integration and role assignment flexibility.
Each device also has the log-forward-cache-size set, which is relevant for forwarding logs within a fabric environment.
Based on the above analysis, all devices (FortiAnalyzer1, FortiAnalyzer2, and FortiAnalyzer3) meet the requirements to be part of a FortiAnalyzer Fabric.
Reference: FortiAnalyzer 7.4.1 documentation outlines that devices within a FortiAnalyzer Fabric should be on the same or compatible firmware versions and hardware platforms, and they must be configured for integration. Given that all devices match the version, platform, and mode criteria, they can all be part of the FortiAnalyzer Fabric.

NEW QUESTION 32
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 stich are available in the FortiOS connector?

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

Answer: D

Explanation:
When using FortiAnalyzer to create playbooks that interact with FortiOS devices, an Incoming Webhook trigger is required on the FortiGate side to make the actions in an automation stitch accessible through the FortiOS connector. The incoming webhook trigger allows FortiAnalyzer to initiate actions on FortiGate by sending HTTP POST requests to specified endpoints, which in turn trigger automation stitches defined on the FortiGate.
Here's an analysis of each option:
Option A: FortiAnalyzer Event Handler
This is incorrect. The FortiAnalyzer Event Handler is used within FortiAnalyzer itself for handling log events and alerts, but it does not trigger automation stitches on FortiGate.
Option B: Fabric Connector event
This is incorrect. Fabric Connector events are related to Fortinet's Security Fabric integrations but are not specifically used to trigger FortiGate automation stitches from FortiAnalyzer.
Option C: FortiOS Event Log
This is incorrect. While FortiOS event logs can be used for monitoring, they are not designed to trigger automation stitches directly from FortiAnalyzer.
Option D: Incoming webhook
This is correct. The Incoming Webhook trigger on FortiGate enables it to receive requests from FortiAnalyzer, allowing playbooks to activate automation stitches defined on the FortiGate device. This method is commonly used to integrate actions from FortiAnalyzer to FortiGate via the FortiOS connector.
Reference: According to FortiOS and FortiAnalyzer documentation, when integrating FortiAnalyzer
playbooks with FortiGate automation stitches, the recommended trigger type on FortiGate is an Incoming Webhook, allowing FortiAnalyzer to interact with FortiGate??s automation framework through the FortiOS connector.

NEW QUESTION 37
Which statement describes archive logs on FortiAnalyzer?
A. Logs that are indexed and stored in the SQL database
B. Logs a FortiAnalyzer administrator can access in FortiView
C. Logs compressed and saved in files with the .gz extension
D. Logs previously collected from devices that are offline

Answer: C

Explanation:
In FortiAnalyzer, archive logs refer to logs that have been compressed and stored to save space. This process involves compressing the raw log files into the .gz format, which is a common compression format used in Fortinet systems for archived data. Archiving is essential in FortiAnalyzer to optimize storage and manage long-term retention of logs without impacting performance.
Let's examine each option for clarity:
Option A: Logs that are indexed and stored in the SQL database
This is incorrect. While some logs are indexed and stored in an SQL database for quick access and searchability, these are not classified as archive logs. Archived logs are typically moved out of the database and compressed.
Option B: Logs a FortiAnalyzer administrator can access in FortiView
This is incorrect because FortiView primarily accesses logs that are active and indexed, not archived logs. Archived logs are stored for long-term retention but are not readily available for immediate analysis in FortiView.
Option C: Logs compressed and saved in files with the .gz extension
This is correct. Archive logs on FortiAnalyzer are stored in compressed .gz files to reduce space usage. This archived format is used for logs that are no longer immediately needed in the SQL database but are retained for historical or compliance purposes.
Option D: Logs previously collected from devices that are offline
This is incorrect. Although archived logs may include data from devices that are no longer online, this is not a defining characteristic of archive logs.
Reference: FortiAnalyzer 7.4.1 documentation and configuration guides outline that archived logs are stored in compressed files with the .gz extension to conserve storage space, ensuring FortiAnalyzer can handle a larger volume of logs over extended periods?.

NEW QUESTION 41
Exhibit.

What is the analyst trying to create?

A. The analyst is trying to create a trigger variable to the used in the playbook.
B. The analyst is trying to create an output variable to be used in the playbook.
C. The analyst is trying to create a report in the playbook.
D. The analyst is trying to create a SOC report in the playbook.

Answer: B

Explanation:
In the exhibit, the playbook configuration shows the analyst working with the "Attach Data" action within a playbook. Here's a breakdown of key aspects:
Incident ID: This field is linked to the "Playbook Starter," which indicates that the playbook will attach data to an existing incident.
Attachment: The analyst is configuring an attachment by selecting Run_REPORT with a placeholder ID for report_uuid. This suggests that the report's UUID will dynamically populate as part of the playbook execution.
Analysis of Options:
Option A - Creating a Trigger Variable:
A trigger variable would typically be set up in the playbook starter or initiation configuration, not within the "Attach Data" action. The setup here does not indicate a trigger, as it's focusing on data attachment.
Conclusion: Incorrect.
Option B - Creating an Output Variable:
The field Attachment with a report_uuid placeholder suggests that the analyst is defining an output variable that will store the report data or ID, allowing it to be attached to the incident. This variable can then be referenced or passed within the playbook for further actions or reporting.
Conclusion: Correct.
Option C - Creating a Report in the Playbook:
While Run_REPORT is selected, it appears to be an attachment action rather than a report generation task. The purpose here is to attach an existing or dynamically generated report to an incident, not to create the report itself.
Conclusion: Incorrect.
Option D - Creating a SOC Report:
Similarly, this configuration is focused on attaching data, not specifically generating a SOC report.
SOC reports are generally predefined and generated outside the playbook.
Conclusion: Incorrect.
Conclusion:
Correct Answer B. The analyst is trying to create an output variable to be used in the playbook.
The setup allows the playbook to dynamically assign the report_uuid as an output variable, which can then be used in further actions within the playbook.
Reference: FortiAnalyzer 7.4.1 documentation on playbook configurations, output variables, and data attachment functionalities.

NEW QUESTION 42
As part of your analysis, you discover that a Medium severity level incident is fully remediated.
You change the incident status to Closed:Remediated.
Which statement about your update is true?

A. The incident can no longer be deleted.
B. The corresponding event will be marked as Mitigated.
C. The incident dashboard will be updated.
D. The incident severity will be lowered.

Answer: C

NEW QUESTION 43
Which statement about exporting items in Report Definitions is true?

A. Templates can be exported.
B. Template exports contain associated charts and datasets.
C. Chart exports contain associated datasets.
D. Datasets can be exported.

Answer: C

NEW QUESTION 48
What is the purpose of running the command diagnose sql status sqlreportd?

A. To view a list of scheduled reports
B. To list the current SQL processes running
C. To display the SQL query connections and hcache status
D. To identify the database log insertion status

Answer: C

Explanation:
The command diagnose sql statussqlreportd is used in FortiAnalyzer to obtain specific information about the SQL reporting process and caching status. Here??s what this command accomplishes and an analysis of each option:
Command Functionality:
sqlreportd is the FortiAnalyzer daemon responsible for managing SQL-based reporting processes.
The diagnose sql status sqlreportd command provides information on active SQL query connections and thehcache(historical cache) status, which helps in monitoring and troubleshooting SQL report generation.
Option Analysis:
Option A - To View a List of Scheduled Reports:
This option is incorrect because the command does not list scheduled reports. Instead, it focuses on SQL reporting processes and cache details.
Option B - To List the Current SQL Processes Running:
While the command may show active SQL connections, its primary focus is not a detailed list of all SQL processes but rather the connections and cache status for reporting.
Option C - To Display the SQL Query Connections and hcache Status:
This is correct. The command specifically provides information on SQL query connections related to the reporting process (sqlreportd) and displays thehcachestatus.
Option D - To Identify the Database Log Insertion Status:
This is incorrect. The command does not provide details on log insertion status. Log insertion status is typically monitored through different diagnostic commands focused on database processes and log handling.
Conclusion:
Correct Answer C. To display the SQL query connections and hcache status
This command is used to monitor SQL reporting activities and cache status, aiding in the analysis of report generation performance and connection health.
[References:, FortiAnalyzer 7.4.1 documentation on SQL diagnostic commands, particularly those related to reporting (sqlreportd) and caching mechanisms., ,]

NEW QUESTION 50
After generating a report, you notice the information you where expecting to see is not included in it. However, you confirm that the logs are there.
Which two actions should you perform? (Choose two.)

A. Check the time frame covered by the report.
B. Disable auto-cache.
C. Increase the report utilization quota.
D. Test the dataset

Answer: AD

Explanation:
When a generated report does not contain the expected information even though the logs are confirmed to be present, it typically indicates anissue with the report's configuration. There are a few common reasons this might happen:
Option A - Check the Time Frame Covered by the Report:
Reports are generated based on a specific time frame. If the report's time frame does not cover the period when the relevant logs were collected, those logs won??t appear in the report output. Verifying and adjusting the time frame is essential to ensure the report includes all relevant data.
Conclusion:Correct.
Option B - Disable Auto-Cache:
Auto-cache is designed to improve report generation speed by using cached data. Disabling auto-cache would typically only be relevant if the report is pulling outdated data from cache, but it doesn??t directly affect whether specific logs are included in a report.
Conclusion:Incorrect.
Option C - Increase the Report Utilization Quota:
The report utilization quota is related to the resource limits for generating reports. It does not directly influence whether certain data appears in a report. Increasing this quota would help only if there are resource issues preventing the report from completing, not if specific logs are missing from the report.
Conclusion:Incorrect.
Option D - Test the Dataset:
Datasets determine which logs and data fields are pulled into the report. If a dataset is configured incorrectly or does not include the required log fields, it could lead to missing information. Testing the dataset allows you to verify that it??s correctly configured and pulling the expected data.
Conclusion:Correct.
Conclusion:
Correct Answer:A. Check the time frame covered by the reportandD. Test the dataset.
These steps directly address the issues that could lead to missing information in a report when logs are available but not displayed.
[References:, FortiAnalyzer 7.4.1 documentation on report generation settings, time frames, and dataset configuration for accurate report results.,]

NEW QUESTION 54
Which statement about the FortiSIEM management extension is correct?

A. It allows you to manage the entire life cycle of a threat or breach.

B. It can be installed as a dedicated VM.
C. Its use of the available disk space is capped at 50%.
D. It requires a licensed FortiSIEM supervisor.

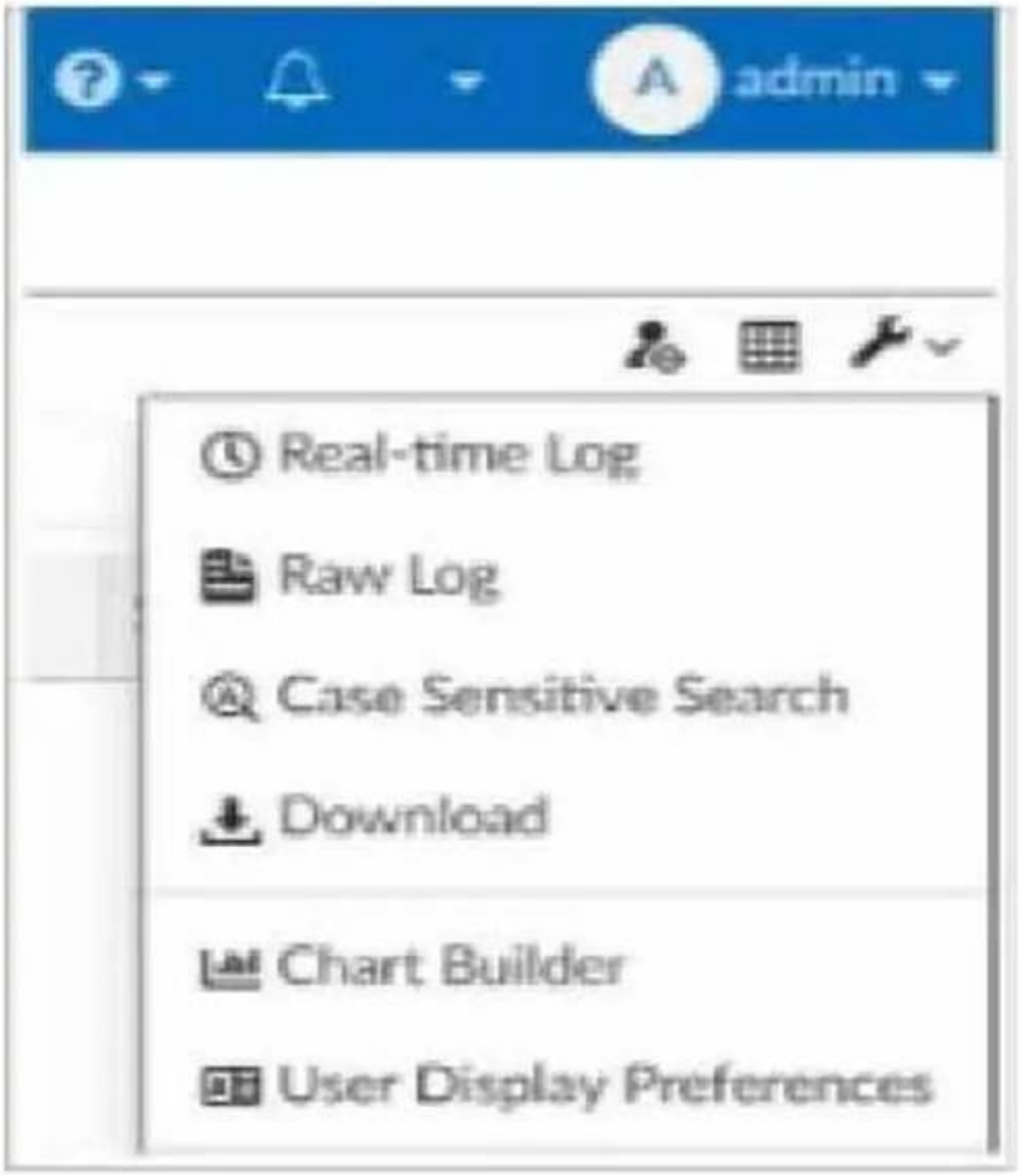
Answer: D

NEW QUESTION 55
You are tasked with finding logs corresponding to a suspected attack on your network.
You need to use an interface where all identified threats within timeframe are listed and organized. You also need to be able to quickly export the information to a PDF file.
Where can you go to accomplish this task?

A. Log Browse
B. Log View
C. Fabric View
D. FortiView

Answer: B

NEW QUESTION 56
Exhibit.

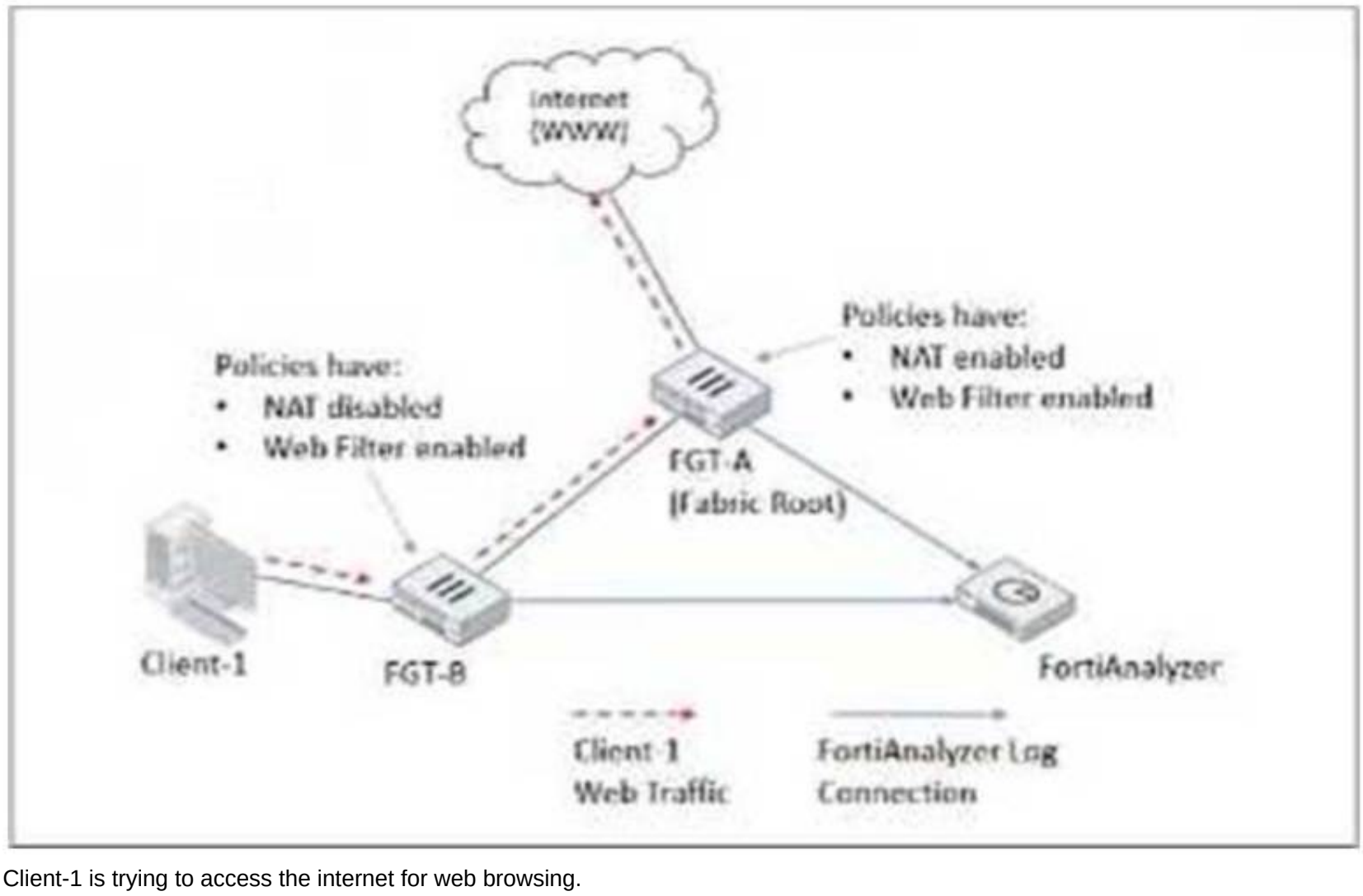


What is the purpose of using the Chart Builder feature On FortiAnalyzer?

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

Answer: D

NEW QUESTION 58
Refer to Exhibit:



Client-1 is trying to access the internet for web browsing.
All FortiGate devices in the topology are part of a Security Fabric with logging to FortiAnalyzer configured. All firewall policies have logging enabled. All web filter profiles are configured to log only violations.
Which statement about the logging behavior for this specific traffic flow is true?

A. Only FGT-B will create traffic logs.
B. FGT-B will see the MAC address of FGT-A as the destination and notifies FGT-A to log this flow.
C. FGT B will create traffic logs and will create web filter logs if it detects a violation.
D. Only FGT-A will create web filter logs if it detects a violation.

Answer: D

Explanation:
The study guide explains that in a Security Fabric,traffic logging is not duplicatedacross FortiGates for the same session:??Traffic logging for a session ?? is always carried out by the first FortiGate that handled it??and if a FortiGate receives traffic from a peer FortiGate MAC,"it does not generate a new traffic log for that session."
For UTM (web filtering) logs, the study guide states:"When configured, upstream devices complete UTM logging."
In the illustrated example, it further clarifies the role split:"All traffic from Client-1 is first received by FGT-B, which creates traffic logs for the initial session?? [then] forwarded to FGT-A?? [and]FGT-A ?? applies web filtering ?? and generates the relevant UTM logs as necessary."
Because web filter profiles are configured tolog only violations, web filter (UTM) logs will be generated only when a violation is detected—and per the study guide behavior, that UTM logging is done by theupstreamFortiGate (FGT-A). Therefore,only FGT-A will create web filter logs if it detects a violation(Option D)

NEW QUESTION 61
What two things should an administrator do to view Compromised Hosts on FortiAnalyzer? (Choose two.)

Enable web filtering in firewall policies on FortiGate devices, and make sure these logs are sent to FortiAnalyzer.
A. Enable device detection on an interface on the FortiGate devices that are connected to the FortiAnalyzer.
B. Subscribe FortiAnalyzer to FortiGuard to keep its local threat database up-to-date.
C. Make sure all endpoints are reachable by FortiAnalyzer.
D.

Answer: AC

NEW QUESTION 64
.....

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

FCP_FAZ_AN-7.6 Practice Exam Features:

* FCP_FAZ_AN-7.6 Questions and Answers Updated Frequently

* FCP_FAZ_AN-7.6 Practice Questions Verified by Expert Senior Certified Staff

* FCP_FAZ_AN-7.6 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* FCP_FAZ_AN-7.6 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year