Fortinet.FCP_FAZ_AN-7.6.v2026-08-07.q35

Exam Code:	FCP_FAZ_AN-7.6
Exam Name:	FCP - FortiAnalyzer 7.6 Analyst
Certification Provider:	Fortinet
Free Question Number:	35
Version:	v2026-08-07
# of views:	131
# of Questions views:	350
https://www.freepdfdumps.com/Fortinet.FCP_FAZ_AN-7.6.v2026-08-07.q35.html	

NEW QUESTION: 1
(You created a playbook on FortiAnalyzer that uses a FortiOS connector. When you configure FortiGate, which type of trigger must you use so that the actions in an automation stitch are available in the FortiOS connector? (Choose one answer)
A. FortiAnalyzer Event Handler
B. Incoming webhook
C. Fabric Connector event
D. IP ban
Answer: B (LEAVE A REPLY)
Exact Extract: Study Guide p.202: FortiOS connector actions require an Incoming Webhook Call trigger configured on FortiGate.
Technical Deep Dive: The correct answer is B. The FortiOS connector can appear once FortiGate is added to FortiAnalyzer, but FortiAnalyzer will not show the FortiOS automation actions until FortiGate has the proper automation rule. The trigger required is Incoming webhook/Incoming Webhook Call. A FortiAnalyzer Event Handler is a FortiAnalyzer-side event generator, not a FortiGate trigger for connector actions. Fabric Connector event and IP ban are not the trigger type required to expose FortiOS connector actions.

NEW QUESTION: 2
Why must you wait for several minutes before you run a playbook that you just created?
A. FortiAnalyzer needs that time to parse the new playbook.
B. FortiAnalyzer needs that time to debug the new playbook.
C. FortiAnalyzer needs that time to back up the current playbooks.
D. FortiAnalyzer needs that time to ensure there are no other playbooks running.
Answer: A (LEAVE A REPLY)
Exact Extract: Study Guide p.210: after creating a new playbook, FortiAnalyzer needs a few minutes to parse it.
Technical Deep Dive: The correct answer is A. FortiAnalyzer must parse the newly created playbook before it can execute reliably. Parsing checks the playbook definition and prepares it for execution by the automation engine. Option B is wrong because FortiAnalyzer is not automatically debugging the playbook; debugging happens after a failed or problematic run. Option C is unrelated to playbook creation. Option D is wrong because FortiAnalyzer can track multiple jobs; the wait is about playbook parsing, not waiting for all other playbooks to stop.

NEW QUESTION: 3
Which statement correctly describes one difference between templates and reports?
A. Reports support macros but templates do not
B. Templates can be cloned, but reports cannot be cloned.
C. Templates do not include advanced report settings, but reports do.
D. Reports can be moved between ADOMs but templates cannot.
Answer: C (LEAVE A REPLY)
Exact Extract: Study Guide p.172: templates include only Editor-tab details and do not include report settings or advanced settings.
Technical Deep Dive: The correct answer is C. Templates define the report layout: text, charts, and macros.
They do not carry report settings such as the report time range, selected devices, scheduling, filters, output profile, or advanced settings. Reports include those operational settings. Option A is wrong because templates can include macros. Option B is wrong because both reports and templates can be cloned. Option D is imprecise: reports/charts can be imported/exported between same-type ADOMs, while templates are not exported directly, but the tested difference is settings.

NEW QUESTION: 4
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.
Answer: (SHOW ANSWER)
Exact Extract: Study Guide p.173: macros represent dataset queries in abbreviated form, and macros are ADOM-specific.
Technical Deep Dive: The correct answer is C. FortiAnalyzer macros are not Excel-generation shortcuts and are not fixed templates. A macro is an abbreviated way to insert data extracted by a dataset query into a report without using a chart. Because reports, libraries, and related definitions are separated by ADOM, macros are ADOM-specific. Option A is wrong because custom macros can be created. Option B invents an Excel- specific behavior not described by the guide. Option D is too restrictive because macros are not limited only to FortiGate ADOMs.

NEW QUESTION: 5
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: (SHOW ANSWER)
Exact Extract: Study Guide p.188: diagnose sql status sqlreportd checks SQL query connections and hcache status for reports.
Technical Deep Dive: The correct answer is C. The sqlreportd diagnostic is a report troubleshooting command focused on SQL query connections and hcache status. It is useful when reports are slow because report generation depends heavily on hcache and SQL query execution. Option A is handled by scheduled report listing commands. Option B maps to diagnose sql process list. Option D maps more closely to sqlplugind insertion status, not sqlreportd.

NEW QUESTION: 6
(In a FortiAnalyzer Fabric deployment, which three modules from Fabric members are available for analysis on the supervisor? (Choose three answers))

A. Playbooks
B. Indicators
C. Logs
D. Events
E. Reports
Answer: (SHOW ANSWER)
Exact Extract: Study Guide p.25-p.26: the supervisor displays member logs, can aggregate report data, and shows events generated on members.
Technical Deep Dive: The correct answers are C, D, and E. FortiAnalyzer Fabric supervisor visibility includes logs collected on members, events generated by member event handlers, and reports that fetch and aggregate data from multiple members. Playbooks are not available as a supervisor-to-member execution module; the guide states supervisors cannot run automation playbooks on members. Indicators are not listed in the Fabric supervisor modules described for member analysis in the study guide.

NEW QUESTION: 7
Which two statements about local logs on FortiAnalyzer are true? (Choose two.)
A. They are not supported in FortiView.
B. You can view playbook logs for all ADOMs in the root ADOM.
C. Event logs show system-wide information, whereas application logs are ADOM-specific.
D. Event logs are available only in the root ADOM.
Answer: (SHOW ANSWER)
Exact Extract: Study Guide p.59: event logs show system-wide information; application logs are ADOM- specific, and non-root ADOMs show only application logs.
Technical Deep Dive: The correct answers are C and D. FortiAnalyzer local logs include system-wide event logs and ADOM-specific application logs. Because non-root ADOMs show only application logs, system event logs are effectively a root-ADOM visibility item. Option A is wrong because local audit logs are accessible in Log View under ADOMs. Option B overstates playbook visibility; playbook/application logs are ADOM-specific and should not be treated as all centralized in root for every ADOM.

NEW QUESTION: 8
Which log will generate an event with the status Contained?
A. An AV log with action=quarantine.
B. An IPS log with action=pass.
C. A WebFilter log with action=dropped.
D. An AppControl log with action=blocked.
Answer: A (LEAVE A REPLY)
Exact Extract: Study Guide p.82: Contained means the risk source is isolated; antivirus quarantine is the example.
Technical Deep Dive: The correct answer is A. An AV log with action=quarantine indicates the detected file or object has been isolated, so FortiAnalyzer classifies the event status as Contained. An IPS action=pass is Unhandled because the risk was not stopped. WebFilter dropped and AppControl blocked are enforcement outcomes, so they align with Mitigated rather than Contained. The distinction matters in SOC triage because Contained still deserves review, but the immediate source/object has already been isolated.

NEW QUESTION: 9
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 a 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: (SHOW ANSWER)
Exact Extract: Study Guide p.64-p.65: FortiView summarizes threats and can export FortiView information as a PDF file.
Technical Deep Dive: The correct answer is D. FortiView provides dashboard views such as Threats, where identified threats within a selected timeframe are summarized and organized for analysis. The guide also states FortiView information can be exported as a PDF. Log Browse and Log View are useful for searching individual logs, but they do not provide the same threat-summary dashboard workflow. Fabric View is for Security Fabric topology and inventory context, not top-threat investigation and PDF export.

NEW QUESTION: 10
As part of your analysis, you discover that an incident is a false positive.
You change the incident status to Closed: False Positive.
Which statement about your update is true?
A. The audit history log will be updated.
B. The corresponding event will be marked as mitigated.
C. The incident will be deleted.
D. The incident number will be changed
Answer: A (LEAVE A REPLY)
Exact Extract: Study Guide p.105-p.106: incident analysis includes audit history, and incident settings/status should be kept up to date.
Technical Deep Dive: The correct answer is A. When an analyst changes an incident status to Closed: False Positive, FortiAnalyzer records the action in the incident audit history. That preserves accountability and allows other analysts to see what changed and why. The corresponding event is not automatically reclassified as mitigated. The incident is not deleted just because it is closed. The incident number remains stable because it is the identifier used to track the case through its lifecycle.

NEW QUESTION: 11
Which statement about SQL SELECT queries is true?
A. They can be used to purge log entries from the database.
B. They must be followed immediately by a WHERE clause.
C. They can be used to display the database schema.
D. They are not used in macros.
Answer: C (LEAVE A REPLY)
Exact Extract: Study Guide p.159: SELECT * FROM $log can be used to obtain the schema for a selected log type.
Technical Deep Dive: The correct answer is C. FortiAnalyzer datasets use SQL SELECT queries not only to extract report data but also to reveal available columns for a log type. Running SELECT * FROM $log and testing the dataset shows the column headings available in the database schema. Option A is wrong because SELECT is read-only and does not purge data. Option B is wrong because WHERE is optional; FROM is the mandatory clause. Option D is wrong because macros represent dataset queries in abbreviated form, so SELECT logic is directly related to macros.

NEW QUESTION: 12
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 FortiAnalyzer Fabric?
A. FortiAnalyzer1 and FortiAnalyzer3
B. FortiAnalyzer1 and FortiAnalyzer2
C. FortiAnalyzer2 and FortiAnalyzer3
D. All devices listed can be members.
Answer: (SHOW ANSWER)
Exact Extract: Study Guide p.21: FortiAnalyzer Fabric operates with a supervisor and members; members send information to the supervisor for centralized monitoring.
Technical Deep Dive: The correct answer is D. The exhibit shows devices that meet the conditions to participate as FortiAnalyzer Fabric members, so all listed devices can be members. The key concept is that Fabric membership is about centralized monitoring visibility between FortiAnalyzer systems, not about forcing every member into HA or a single time zone. A member remains an operating FortiAnalyzer device and reports member information to the supervisor. The distractor pairs are too restrictive because they unnecessarily exclude devices that still satisfy the Fabric member role.

NEW QUESTION: 13
(How does FortiAnalyzer block indicators? (Choose one answer)
A. It uses an automation script to update FortiGate with the block list.
B. It uses a FortiManager connector to send the block list.
C. It uses a FortiClient EMS connector to send the block list.
D. It uses a webhook to allow FortiGate to send the block list.
Answer: B (LEAVE A REPLY)
Exact Extract: Study Guide p.98: blocking suspicious indicators requires an authorized FortiManager connector and updates a FortiManager External Resource list.
Technical Deep Dive: The correct answer is B. FortiAnalyzer does not directly push the block to FortiGate from the indicator page. It uses a FortiManager connector; the Block_indicator playbook periodically sends blocked indicators to FortiManager, where they are added to an External Resource list. FortiManager policies or threat feeds can then be used to push enforcement to FortiGate. Option A skips FortiManager, which is the documented control point. Options C and D use the wrong integration mechanism for indicator blocking.

NEW QUESTION: 14
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 (LEAVE A REPLY)
Exact Extract: Study Guide p.107: FortiAnalyzer can send incident notifications to external platforms using Fabric connectors; more than one connector can be added.
Technical Deep Dive: The correct answer is A. Incident update notifications are not restricted to email.
FortiAnalyzer can use configured Fabric connectors to notify external collaboration or response platforms, and each connector can be configured for the incident activities that should trigger a notification. Option B is too narrow because email is only one possible delivery model. Option C is wrong because multiple connectors do not have to share identical settings. Option D is wrong because notification triggers are configurable for different incident activities, not only update or delete events.

NEW QUESTION: 15
When managing incidents on FortiAnalyzer, what must an analyst be aware of?
A. You can manually attach generated reports to incidents.
B. The status of the incident is always linked to the status of the attached event.
C. Severity incidents rated with the level High have an initial service-level agreement (SLA) response time of 1 hour.
D. Incidents must be acknowledged before they can be analyzed.
Answer: A (LEAVE A REPLY)
Exact Extract: Study Guide p.185: reports can be attached to incidents manually from an existing report, manually from an incident, or automatically through playbooks.
Technical Deep Dive: The correct answer is A. Incidents are containers for related security events, and attaching a report gives the analyst historical or contextual evidence in addition to real-time event data.

Option B is wrong because incident status is managed independently from attached event status. Option C is not a FortiAnalyzer default rule from the guide; SLA response times are organization-specific. Option D is wrong because incidents can be opened and analyzed directly; acknowledgment is not a prerequisite to analysis.

NEW QUESTION: 16
Which SQL query is in the correct order to query the database in the FortiAnalyzer?
A. SELECT devid FROM $log GROUP BY devid WHERE 'user',,' users1'
B. SELECT FROM $log WHERE devid 'user',, USER1' GROUP BY devid
C. SELCT devid WHERE 'user'-' USER1' FROM $log GROUP By devid
D. SELECT devid FROM $log WHERE 'user'=' GROUP BY devid
Answer: D (LEAVE A REPLY)
Exact Extract: Study Guide p.158: SELECT statements must follow clause order: SELECT, FROM, WHERE, GROUP BY, ORDER BY, LIMIT, OFFSET.
Technical Deep Dive: The correct answer is D because it is the only option that follows the expected SQL clause sequence closely enough: SELECT columns, FROM $log, WHERE condition, and GROUP BY. Even if the printed option appears to have a minor value/quotation issue, its clause order is the tested point. Option A places GROUP BY before WHERE, which is invalid. Option B lacks a proper selected column and malformed filtering syntax. Option C misspells SELECT and places WHERE before FROM, which breaks the required SQL structure.

NEW QUESTION: 17
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.
Answer: A,C (LEAVE A REPLY)
Exact Extract: Study Guide p.184: reports and charts can be imported/exported between same-type ADOMs; chart exports include associated datasets.
Technical Deep Dive: The correct answers are A and C. FortiAnalyzer requires the source and destination ADOMs to be the same type when moving reports or charts. Reports contain charts, and exported charts carry their associated datasets, so the reporting dependency comes across with the import workflow. Option B describes name-conflict behavior for playbook imports, not the report-moving requirement tested here. Option D is wrong because reports can be imported/exported directly; converting them to templates first is not required.

NEW QUESTION: 18
(An analyst is using FortiAI on FortiAnalyzer to simplify certain tasks but is worried about exceeding the monthly token limit. Which query will take the fewest FortiAI tokens? (Choose one answer)

A. Show logs for 192.168.1.10 (past week)
B. Show all logs from the past week
C. Can you show me all the log entries for the endpoint 192.168.1.10?
D. Show logs for 192.168.1.10
Answer: A (LEAVE A REPLY)
Exact Extract: Study Guide p.118: token usage includes prompt and response; more text and larger responses consume more tokens.
Technical Deep Dive: The correct answer is A. The best low-token prompt is concise and scoped: it specifies the endpoint and limits the response to the past week. Option C is verbose and asks for all log entries, increasing both input and output tokens. Option B asks for all logs for the past week without limiting to an endpoint, which can generate a large response. Option D is short, but it lacks a time window, so it can produce a broader and more token-heavy response than option A.

NEW QUESTION: 19
Which FortiAnalyzer feature allows you to use a proactive approach when managing your network security?
A. FortiView Monitor
B. Outbreak alert services
C. Incidents dashboard
D. Threat hunting
Answer: (SHOW ANSWER)
Exact Extract: Study Guide p.126: threat hunting is a proactive search for suspicious or risky network activity.
Technical Deep Dive: The correct answer is D. Threat hunting is FortiAnalyzer's proactive investigation workflow. Instead of waiting for an event handler or incident to tell the SOC what happened, the analyst begins with a hypothesis and searches logs for suspicious patterns. FortiView is valuable for visibility but is not, by itself, the named proactive method. Outbreak alerts notify about emerging threats, and the Incidents dashboard manages known incidents. Threat hunting is the feature that best matches proactive network- security management.

NEW QUESTION: 20
What happens when the indicator of compromise (IOC) engine on FortiAnalyzer finds web logs that match blacklisted IP addresses?
A. FortiAnalyzer flags the associated host for further analysis.
B. A new infected entry is added for the corresponding endpoint under Compromised Hosts.
C. The detection engine classifies those logs as Suspicious.
D. The endpoint is marked as Compromised and, optionally, can be put in quarantine.
Answer: B (LEAVE A REPLY)
Exact Extract: Study Guide p.130-p.132: blacklisted IP or DGA matches produce an Infected verdict and appear under Compromised Hosts.
Technical Deep Dive: The correct answer is B. When IOC analysis finds web logs matching blacklisted IP addresses or domain-generation algorithm patterns, FortiAnalyzer treats that as a real breach and creates
/updates an infected compromised-host entry for the endpoint. Option A describes suspicious-list behavior, where FortiAnalyzer flags the host for further analysis. Option C is wrong because blacklisted matches are classified as Infected, not merely Suspicious. Option D overstates the automatic endpoint response; quarantine is a separate response action, not the IOC engine classification itself.

NEW QUESTION: 21
After generating a report, you notice the information you were 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: A,D (LEAVE A REPLY)
Exact Extract: Study Guide p.189: for missing report data, check the report time frame and test the dataset.
Technical Deep Dive: The correct answers are A and D. If the logs exist but the generated report lacks expected information, the first checks are whether the report time frame includes those logs and whether the dataset query returns the expected rows. Reports are only as accurate as their time filter and SQL dataset.
Disabling auto-cache is not the normal fix; cache improves performance and scheduled reports use it.
Increasing a quota does not correct a wrong time range or broken SQL query unless the report fails for resource reasons, which is not the scenario described.

NEW QUESTION: 22
Exhibit.

A FortiAnalyzer analyst is customizing a SQL query to use in a report.
Which SQL query should the analyst run to get the expected results?

A.
```
SELECT srcip AS "Source IP", dstport AS "Destination Port"
FROM $log
WHERE $filter AND srcip = '10.0.1.10'
ORDER BY dstport
GROUP by srcip, dstport DESC
```

B.
```
SELECT srcip AS "Source IP", dstport AS "Destination Port"
FROM $log
WHERE $filter AND Source IP != '10.0.1.10'
GROUP BY srcip, dstport
ORDER BY dstport DESC
```

C.
```
SELECT srcip AS "Source IP", dstport AS "Destination Port"
ORDER BY dstport DESC
GROUP BY srcip, dstport
FROM $log
WHERE $filter AND srcip = '10.0.1.10'
```

D.
```
SELECT srcip AS "Source IP", dstport AS "Destination Port"
FROM $log
WHERE $filter AND srcip = '10.0.1.10'
GROUP BY srcip, dstport
ORDER BY dstport DESC
```

Answer: A (LEAVE A REPLY)

Exact Extract: Study Guide p.157-p.158: report datasets use SQL SELECT queries, and clauses must be in the correct order.

Technical Deep Dive: The correct answer is A. The valid query must select the required fields, read from $log, apply the filter for the source IP, group the selected values, and order the output as expected. Option A follows the SQL structure FortiAnalyzer expects for report datasets. The incorrect options either reverse the filter logic, place clauses in the wrong order, or use malformed aliases/conditions. In FortiAnalyzer reporting, a syntactically correct dataset is mandatory because the chart receives only the data returned by that SQL SELECT query.

NEW QUESTION: 23

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 (LEAVE A REPLY)

Exact Extract: Study Guide p.211: output variables use the output from a preceding task as input to the current task.

Technical Deep Dive: The correct answer is B. The exhibit shows the analyst referencing output from an earlier task, such as a generated report identifier, so a later task can attach that result to an incident. That is an output variable. A trigger variable would pull values from the event or incident that started the

playbook. The analyst is not creating the report object itself, nor creating a SOC report definition; the report task has already produced data, and the current task is consuming that output dynamically.

NEW QUESTION: 24
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 a 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. FortiView
B. Fabric View
C. Log View
D. Log Browse
Answer: A (LEAVE A REPLY)

NEW QUESTION: 25
Which two modules can be imported and exported between ADOMs on FortiAnalyzer? (Choose two.)
A. Templates
B. Reports
C. Charts
D. Datasets
Answer: B,C (LEAVE A REPLY)
Exact Extract: Study Guide p.184: reports and charts can be imported/exported; templates and datasets cannot be exported directly.
Technical Deep Dive: The correct answers are B and C. FortiAnalyzer allows reports and charts to be imported and exported between same-type ADOMs or FortiAnalyzer devices. The guide explicitly says templates and datasets cannot be exported directly. Datasets move only as dependencies of exported charts, not as standalone exportable modules. Therefore, reports and charts are the two modules that match the direct import/export capability described in the guide.

NEW QUESTION: 26
Refer to the exhibit.

SourceIP	DestIP	url
::ffff:10.0.11.50	::ffff:5.226.179.10	https://www.bet365.com/
::ffff:10.0.11.50	::ffff:5.226.179.10	http://www.bet365.com/
::ffff:10.0.11.50	::ffff:5.226.179.10	https://www.bet365.com/
::ffff:10.0.11.50	::ffff:104.18.35.228	https://www.betway.com/
::ffff:10.0.11.50	::ffff:104.18.35.228	https://betway.com/
::ffff:10.0.11.50	::ffff:104.18.35.228	https://www.betway.com/
::ffff:10.0.11.50	::ffff:172.64.152.28	https://us.betway.com/
::ffff:10.0.11.50	::ffff:172.64.152.28	https://us.betway.com/
::ffff:10.0.11.50	::ffff:104.18.35.228	https://gateway.betway.com/
::ffff:10.0.11.50	::ffff:104.18.35.228	https://gateway.betway.com/
::ffff:10.0.11.50	::ffff:142.251.167.121	https://sgtm.betway.com/
::ffff:10.0.11.50	::ffff:142.251.167.121	https://sgtm.betway.com/
::ffff:10.0.11.50	::ffff:142.251.167.121	https://sgtm.betway.com/
::ffff:10.0.11.50	::ffff:142.251.167.121	https://sgtm.betway.com/

An analyst is trying to create a dataset to pull all gambling websites that were visited by end users.
Which SQL query on FortiAnalyzer will give the result shown in the exhibit?

A. [Selected] select srcip as " SourceIP " , dstip as " DestIP " , url from $log where catdesc = ' Gambling '

B. select srcip as " SourceIPv6 " , dstip as " DestIPv6 " , url from $log where catdesc = ' Gambling '

C. select srcip as " SourceIP " , dstip as " DestIP " , url from $log where catdesc = ' Dating '

D. select srcip as " SourceIP " , dstip as " DestIP " , url from ' Gambling ' where catdesc = $log

Answer: A (LEAVE A REPLY)

Exact Extract: Study Guide p.157-p.159: datasets are SQL SELECT queries over $log, and WHERE filters narrow returned log rows.
Technical Deep Dive: The correct answer is A. The required dataset must select source IP, destination IP, and URL from $log, then filter web-filter logs where the category description equals Gambling. Option A uses the correct fields and catdesc filter. Option B incorrectly uses IPv6 aliases that do not match the expected output.
Option C filters Dating instead of Gambling. Option D reverses the table and filter logic by placing Gambling in the FROM position and $log in the WHERE expression, which is invalid for the intended dataset.

NEW QUESTION: 27

After generating a report, you notice the information you were expecting to see is not included in it. However, you confirm that the logs are there.

A. Check the time frame covered by the report.

B. Disable auto-cache.

C. Increase the report utilization quota.

D. Test the dataset

Answer: A,D (LEAVE A REPLY)

Exact Extract: Study Guide p.189: verify logs from the report time frame and test the dataset query when expected data is missing.
Technical Deep Dive: The correct answers are A and D. This duplicate scenario tests the same reporting troubleshooting logic. A report can be empty or incomplete even while the logs exist if the report uses a time window that excludes them or if the dataset filters them out. Testing the dataset proves whether the SQL query is actually retrieving the intended rows. Disabling auto-cache is a performance workaround only in very specific stale-cache investigations and is not the recommended first step. Report quota is not the issue when the report runs but contains the wrong data.

NEW QUESTION: 28

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: (SHOW ANSWER)
Exact Extract: Study Guide p.184: templates and datasets cannot be exported directly; chart exports include the associated dataset.
Technical Deep Dive: The correct answer is C. In Report Definitions, the export/import rule is specific:
reports and charts can be moved, templates and datasets cannot be exported directly. When a chart is exported, the dataset associated with that chart is included automatically, so importing the chart also imports the dataset. Option A is wrong because templates cannot be exported. Option B is wrong for the same reason.
Option D is wrong because datasets are not directly exportable as standalone objects.

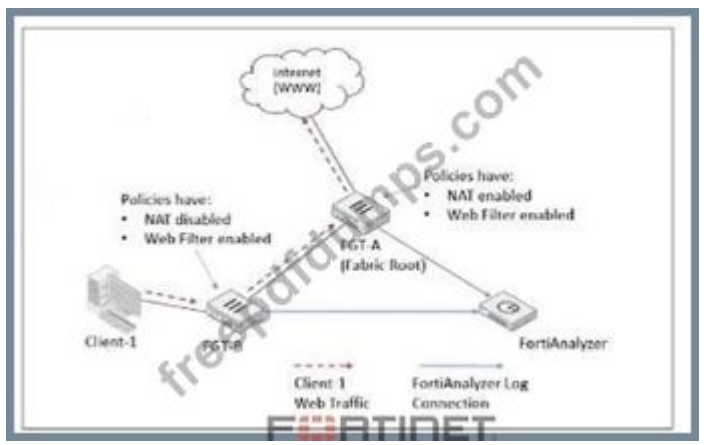
NEW QUESTION: 29
Which statement about the FortiSOAR management extension is correct?
A. It requires a FortiManager configured to manage FortiGate.
B. It runs as a docker container on FortiAnalyzer.
C. It requires a dedicated FortiSOAR device or VM.
D. It does not include a limited trial by default.
Answer: B (LEAVE A REPLY)
Exact Extract: Official Fortinet Administration Guide: Management Extension Applications are installed and run on FortiAnalyzer; CLI options include enabling the fortisoar container.
Technical Deep Dive: The correct answer is B. FortiSOAR MEA is a management extension application hosted by FortiAnalyzer, not a separate FortiSOAR appliance requirement for this question. FortiAnalyzer uses Docker-based MEA support, and FortiSOAR MEA is one of the supported extensions. Option A is wrong because FortiManager is not required just to run the FortiSOAR MEA. Option C describes a standalone FortiSOAR deployment, not the management extension. Option D is wrong because Fortinet documents FortiSOAR MEA trial licensing behavior for evaluation use.

NEW QUESTION: 30
Exhibit.
Laptop1 is used by several administrators to manage FortiAnalyzer. You want to configure a generic text filter that matches all login attempts to the web interface generated by any user other than admin", and coming from Laptop1.
Which filter will achieve the desired result?
A. Operation-login 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 and dstip==10.1.1.1.210 and user==admin
D. Operation-login and dstip==10.1.1.210 and user!-admin
Answer: A (LEAVE A REPLY)
Exact Extract: Study Guide p.83: generic text filters support field operators, including equality and inequality, for precise event-handler matching.
Technical Deep Dive: The correct answer is A. The required filter must match login operations to the GUI from Laptop1 and exclude the admin user. Option A includes the login operation, the correct GUI/IP value for Laptop1, and user!=admin. Option B uses the wrong IP address. Option C incorrectly matches

user==admin, which is the opposite of the requirement. Option D lacks the correct performed_on GUI condition and has malformed inequality syntax. For event-handler filters, small syntax or field mistakes change the result completely.

NEW QUESTION: 31
What is the purpose of using data selectors when configuring event handlers?
A. They filter the types of logs that FortiAnalyzer can accept from registered devices.
B. They download new filters can be used in event handlers.
C. They apply their filter criteria to the entire event handler so that you don't have to configure the same criteria in the individual rules.
D. They are common filters that can be applied simultaneously to all event handlers.
Answer: C (LEAVE A REPLY)
Exact Extract: Study Guide p.78 and p.81: a data selector is a common filter applied before every rule in the event handler.
Technical Deep Dive: The correct answer is C. Data selectors prevent analysts from repeating the same filtering logic in each event-handler rule. They narrow the data evaluated by the handler using device, subnet, and log-field criteria before individual rules are processed. Option A is wrong because data selectors do not control what FortiAnalyzer accepts from registered devices. Option B is invented; they do not download filters. Option D is too broad because a data selector is applied to selected handlers, not automatically to all event handlers at the same time.

NEW QUESTION: 32
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 (LEAVE A REPLY)
Exact Extract: Study Guide p.19-p.20: the first FortiGate creates the traffic log, while upstream devices complete UTM logging.
Technical Deep Dive: The correct answer is D. Client traffic first reaches the access-layer FortiGate, which creates the initial traffic log. The upstream FortiGate applies the web filter profile; therefore, if the session violates the web filtering policy, the upstream FortiGate generates the web filter UTM log. Because the web filter profile is configured to log only violations, no web filter log appears unless a violation occurs. Options A and C incorrectly place web filter logging on FGT-B. Option B misstates how Security Fabric logging avoids duplicate logs; FortiGates do not notify peers to log the flow.

NEW QUESTION: 33
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 reports under the mail server.
B. Add a mailto: < email address > option within the report layouts.
C. Enable email notification under the report calendar.
D. Enable an output profile on the reports.
Answer: D (LEAVE A REPLY)
Exact Extract: Study Guide p.181: output profiles specify report format and whether to email or upload generated reports.
Technical Deep Dive: The correct answer is D. The mail server being configured only gives FortiAnalyzer the ability to send email. To send generated reports automatically, the report must use an output profile that defines the delivery method and recipients or upload target. Option A is not a report-level distribution setting.
Option B confuses report layout content with report delivery. Option C is wrong because the report calendar shows scheduled report status; scheduling and distribution are configured in the report settings and output profile.

NEW QUESTION: 34
Which statement about automation connectors in FortiAnalyzer is true?
A. An ADOM with the Fabric type comes with multiple connectors configured.
B. The local connector becomes available after you configured any external connector.
C. The local connector becomes available after you connectors are displayed.
D. The actions available with FortiOS connectors are determined by automation rules configured on FortiGate.
Answer: D (LEAVE A REPLY)
Exact Extract: Study Guide p.202-p.203: FortiOS connector actions require automation rules configured on FortiGate.
Technical Deep Dive: The correct answer is D. FortiAnalyzer lists the FortiOS connector after FortiGate is added, but the available actions depend on FortiGate automation configuration. Specifically, the FortiGate side must have automation rules using the Incoming Webhook Call trigger before actions become available to the connector. Option A is wrong because Fabric ADOMs do not automatically come with multiple usable external connectors. Options B and C misunderstand the local connector, which is available by default for local FortiAnalyzer actions.

NEW QUESTION: 35
You find that as part of your role as an analyst, you frequently search log View using the same parameters.
Instead of defining your search filters repeatedly, what can you do to save time?
A. Configure a custom dashboard.

B. Configure a custom view.
C. Configure a data selector.
D. Configure a macro and apply it to device groups.
Answer: B (LEAVE A REPLY)
Exact Extract: Study Guide p.54: custom views save search filters, device, and time period for repeated Log View searches.
Technical Deep Dive: The correct answer is B. A custom view is designed for exactly this use case: an analyst repeatedly searches Log View with the same filters and wants to avoid rebuilding them every time. A custom dashboard shows widgets and summary data but does not preserve a Log View search workflow. A data selector is used mainly as a reusable filter for event handlers and related features. A macro is for report data extraction, not for reusing interactive log-search parameters.