Question #1 *Topic 1*

Which statement about automation connectors on FortiAnalyzer is true?

A. An ADOM with the Fabric type comes with multiple connectors configured.

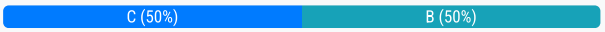
B. The local connector comes online once you have a playbook task referencing it.

C. The actions available with FortiOS connectors are determined by automation rules configured on FortiGate.

D. The playbook module must be enabled before external connectors are displayed.

Suggested Answer: *A*

Community vote distribution



l1996 1 week ago

Selected Answer: C

FortiAnalyzer 7.6.5 Administration Guide - Page 370: The actions available with FortiOS connectors are determined by automation rules configured on each
FortiGate.

upvoted 1 times

greyesz 2 weeks, 5 days ago

Selected Answer: B

Tengo una duda, no se si es A o B.

upvoted 1 times

Question #2 *Topic 1*

Which three modules does FortiAnalyzer automatically download content from with a valid SOC Automation service license? (Choose three.)

A. Report templates

B. Dashboards

C. Event handlers

D. Active Connectors

E. Playbooks

F. Incident templates

Suggested Answer: *CEF*

Currently there are no comments in this discussion, be the first to comment!

Question #3 *Topic 1*

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.)

A. This is a formatted view of the log.

B. This is a normalized log.

C. This log is in a raw log format.

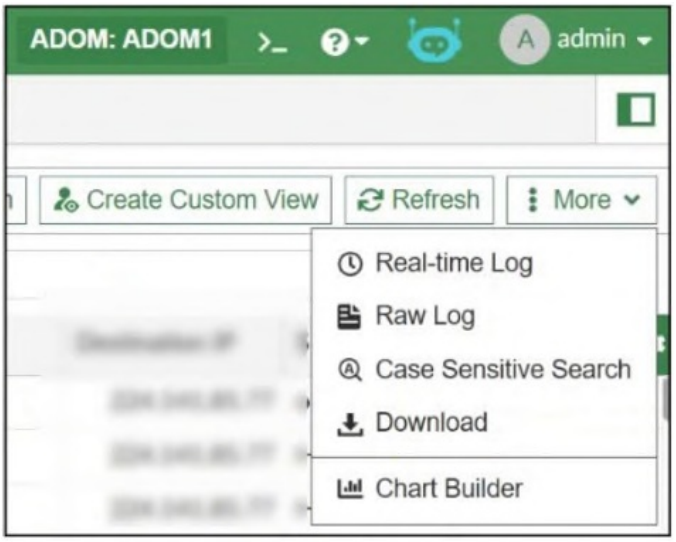
D. This is the original log that FortiAnalyzer received from FortiGate.

Suggested Answer: *CD*

Currently there are no comments in this discussion, be the first to comment!

Question #4 *Topic 1*

Refer to the exhibit.



What is the purpose of using the Chart Builder feature on FortiAnalyzer7?

A. To build a chart automatically based on the top 100 log entries

B. To add charts to generate reports directly in the current ADOM

C. To add a new chart under FortiView to be used in new reports

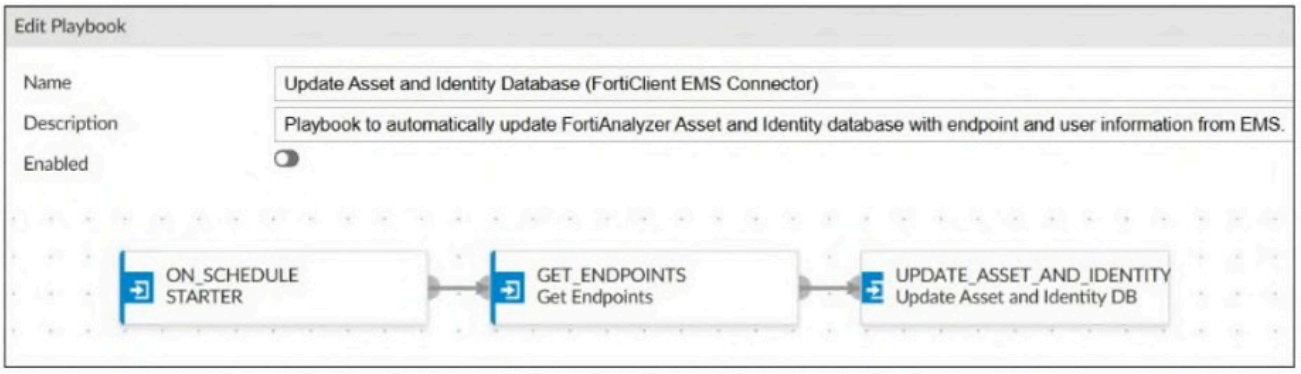
D. To build a dataset and chart based on the filtered search results

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #5 *Topic 1*

Refer to the exhibit.



The playbook shown in the exhibit requires fine-tuning. A task needs to be configured to run a report on the updated asset list that the FortiAnalyzer receives from the FortiClient EMS.

Which SOC role is responsible for making this change?

A. Threat hunter

B. SOC engineer

C. Security analyst

D. Incident responder

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #6 *Topic 1*

Which operation can you use SQL SELECT queries for?

A. To alter tables in the database

B. To purge log entries from the database

C. To insert new data into an existing table

D. To display the database schema

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #7 *Topic 1*

Refer to the exhibit.

What does the data point at 21:20 indicate?

A. FortiAnalyzer is indexing logs faster than logs are being received.

B. The sqlpugind daemon is behind in receiving logs by one log.

C. The fortilogd daemon is ahead in indexing by one log.

D. The log insert lag time is high.

Suggested Answer: *B*

Community vote distribution

A (100%)

victorgm83 6 days, 3 hours ago

Selected Answer: A

A mi me tienen que explicar porqué tienen puesta la B como correcta y cómo se supone que puede estar "un log" por detrás viendo una gráfica de logs por segundo... En mi opinión es la A

upvoted 1 times

Question #8 *Topic 1*

Which two parameters does FortiAnalyzer use to identify an indicator of compromise (IOC)? (Choose two.)

A. Application category

B. IP address

C. URL

D. Policy ID

Suggested Answer: *BC*

Currently there are no comments in this discussion, be the first to comment!

Question #9 *Topic 1*

Which statement describes archive logs on FortiAnalyzer?

A. Logs that are parsed and normalized by FortiAnalyzer and available in the log view

B. Logs received from other FortiAnalyzer devices

C. Logs compressed and saved in files with the .gz extension

D. Logs that are indexed and stored in the SQL database

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #10 *Topic 1*

An analyst needs to move reports between two ADOMs.
Which two statements are true? (Choose two.)

A. All charts and datasets associated with the report will be imported together.

B. The date and time will be appended to the original report name to avoid conflicts.

C. The ADOMs must be compatible types.

D. The reports must be converted into templates first.

Suggested Answer: *AC*

Currently there are no comments in this discussion, be the first to comment!

Question #11 *Topic 1*

After generating a report you notice that the information you were expecting to see is not included in that report. However, you confirm that the logs are there.
Which two actions must you perform? (Choose two.)

A. Test the dataset.

B. Check the time frame covered by the report.

C. Increase the report utilization quota.

D. Enable auto-cache.

Suggested Answer: *AB*

Currently there are no comments in this discussion, be the first to comment!

Question #12 *Topic 1*

When managing incidents on FortiAnalyzer, which fact must an analyst be aware of?

A. The status of the incident is always linked to the status of the attached event.

B. A playbook can be run from the Incidents page.

C. Incidents must be acknowledged before they can be analyzed.

D. Indicators found on the Incidents page can be enriched only from the Indicators page.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #13 *Topic 1*

You are trying to configure a task in the playbook editor to run a report. However, when you try to select the desired report you do not see it listed. What is the reason?

A. The report template needs to be switched to one that is available for playbooks.

B. You must create a trigger to run the report first.

C. The playbook is currently running and the report will be available after it is finished.

D. The report does not have auto-cache and extended log filtering enabled.

Suggested Answer: *A*

Community vote distribution

D (100%)

l1996 4 days, 20 hours ago

Selected Answer: D

FortiAnalyzer 7.6.5 Administration Guide - Page 214: Only reports with Auto Cache and Extended Log Filtering enabled can be run from an incident.

upvoted 1 times

Question #14 *Topic 1*

Which three types of indicators can FortiAnalyzer identify? (Choose three.)

A. Email address

B. Host name

C. Domain

D. URL

E. IP address

Suggested Answer: *CDE*

Currently there are no comments in this discussion, be the first to comment!

Question #15 *Topic 1*

Refer to the exhibit.

Log output

```
FAZ # diagnose log device
Device Name          Device ID            Used Space(logs / quarantine / content / IPS) Allocated Space  Used%
FGT-A                 FGVM010000077646      332.0KB( 332.0KB/    0.0KB/    0.0KB/    0.0KB) unlimited        n/a
FGT-B                 FGVM010000064692      600.7MB( 600.7MB/    0.0KB/    0.0KB/    0.0KB) unlimited        n/a
FGT-C                 FGVM010000065036        1.2MB(   1.2MB/    0.0KB/    0.0KB/    0.0KB) unlimited        n/a
Total: 3 log devices, used=602.3MB quota=unlimited


AdomName           AdomOID  Type                                    Logs                                                                  Database
                            [Retention   Quota      Used(    logs/quaranti/ content/     IPS) Used%]  [Retention   Quota      Used(  SiemDB/  hcache) Used%]
ADOM1              185      FSF   1000days   900.0MB  601.0MB( 601.0MB/    0.0KB/    0.0KB/    0.0KB) 66.8%    1000days     2.1GB    1.9GB(  67.9MB/  17.8KB) 92.4%
```

What can you conclude from this output?

A. The allocated disk quota to ADOM1 is 3 GB.

B. There is no disk quota allocated to quarantining files.

C. Archive logs are using more space than analytic logs.

D. ADOM1 has 300 MB of disk space remaining.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #16 *Topic 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?

A. Fabric Connector event

B. Incoming webhook

C. IP ban

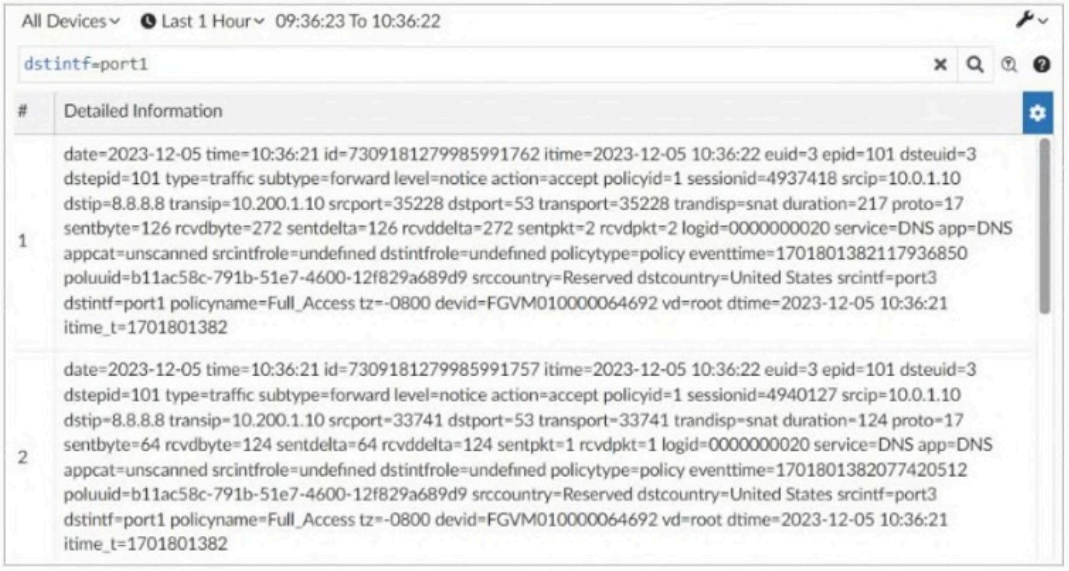
D. FortiAnalyzer Event Handler

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #17 *Topic 1*

Refer to the exhibit.



Which two conclusions can you make about these search results? (Choose two.)

A. The logs have been parsed by FortiGate log parser.

B. They were searched using text mode.

C. They are sortable by columns and customizable.

D. They can be downloaded to a CSV file.

Suggested Answer: *BD*

Currently there are no comments in this discussion, be the first to comment!