

KillTest

質量更高 服務更好



練習題

<https://www.killtest.net>

一年免費更新服務

Exam : **FCP_FAZ_AN-7.6**

Title : Fortinet NSE 5 -
FortiAnalyzer 7.6 Analyst

Version : DEMO

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.

Answer: C

2.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

Answer: ACE

3.Refer to the exhibit.

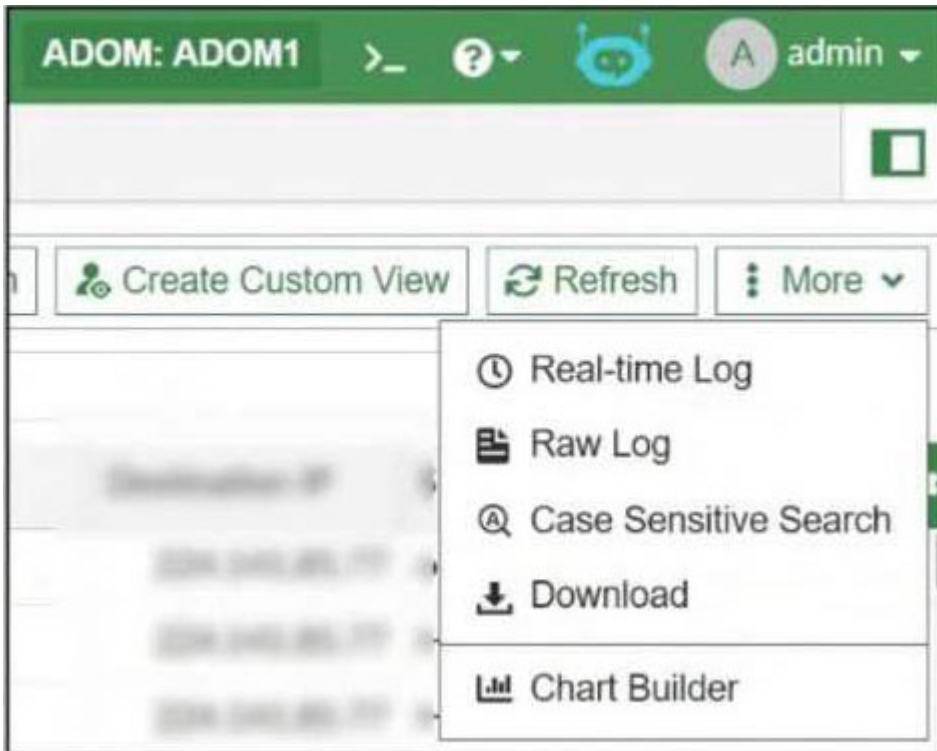
```
adom_oid=198 itime=2025-05-27 08:35:24 loguid=7509149554218893312 epid=3 euid=3 data_parsername=FortiGate Log Parser data_sourceid=FGVM02TM24013423
data_sourcename=HQ-NGFW-1 root_data_sourcetype=FortiGate data_timestamp=1748334923 app_cat=unscanned app_name=NTP app_service=NTP dst_intf=port2(undefined)
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 dststepid=101 dsteuid=3
dst_geo_country=United States event_creation_time=27800868 event_uuid=00000000013 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.

Answer: CD

4.Refer to the exhibit.

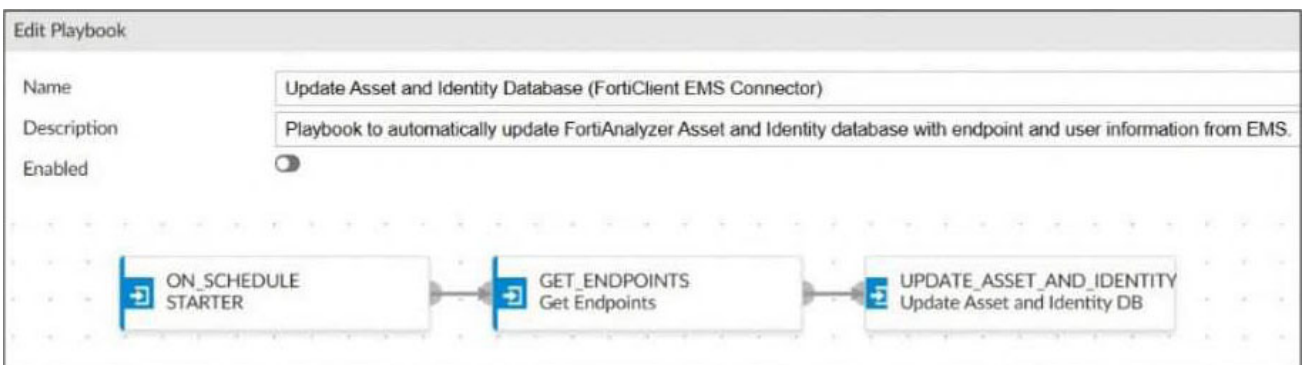


What is the purpose of using the Chart Builder feature on FortiAnalyzer?

- A. To build a chart automatically based on the top 100 log entries
- B. To add charts 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

Answer: D

5.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

Answer: B