VCE & PDF
PassApply.com
https://www.passapply.com/nse5_faz-7-0.html

NSE5_FAZ-7.0^(Q&As)

Fortinet NSE 5 - FortiAnalyzer 7.0

Pass Fortinet NSE5_FAZ-7.0 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/nse5_faz-7-0.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Fortinet Official Exam Center

🗘 **Instant Download** After Purchase

🗘 **100% Money Back** Guarantee

🗘 **365 Days** Free Update

🗘 **800,000+** Satisfied Customers

QUESTION 1

What are offline logs on FortiAnalyzer?

A. Compressed logs, which are also known as archive logs, are considered to be offline logs.

B. When you restart FortiAnalyzer. all stored logs are considered to be offline logs.

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

D. Logs that are collected from offline devices after they boot up.

Correct Answer: A

Logs are received and saved in a log file on the FortiAnalyzer disks. Eventually, when the log file reaches a configured
size, or at a set schedule, it is rolled over by being renamed. These files (rolled or otherwise) are known as archive logs

and are considered offline so they don\\\'t offer immediate analytic support.

Combined, they count toward the archive quota and retention limits, and they are deleted based on the ADOM data
policy.

FortiAnalyzer_7.0_Study_Guide-Online page 140

Reference: https://help.fortinet.com/fa/faz50hlp/56/5-6-
6/Content/FortiAnalyzer_Admin_Guide/0300_Key_concepts/0600_Log_Storage/0400_Arch ive_analytics_logs.htm

QUESTION 2

Which statement correctly describes the management extensions available on FortiAnalyzer?

A. Management extensions do not require additional licenses.

B. Management extensions may require a minimum number of CPU cores to run.

C. Management extensions allow FortiAnalyzer to act as a FortiSIEM supervisor.

D. Management extensions require a dedicated VM for best performance.

Correct Answer: B

Events in FortiAnalyzer will be in one of four statuses. The current status will determine if more actions need to be taken
by the security team or not.

The possible statuses are:

Unhandled: The security event risk is not mitigated or contained, so it is considered open.

Contained: The risk source is isolated.

Mitigated: The security risk is mitigated by being blocked or dropped.

(Blank): Other scenarios.

FortiAnalyzer_7.0_Study_Guide-Online pag. 189.

QUESTION 3

You crested a playbook on FortiAnalyzer that uses a FortiOS connector

When configuring the FortiGate side, which type of trigger must be used so that the actions in an automation stitch are available in the FortiOS connector?

A. FortiAnalyzer Event Handler

B. Incoming webhook

C. FortiOS Event Log

D. Fabric Connector event

Correct Answer: B

"One possible scenario is shown on the slide:

1.

Traffic flows through the FortiGate

2.

FortiGate sends logs to FortiAnalyzer

3.

FortiAnalyzer detects some suspicious traffic and generates an event

4.

The event triggers the execution of a playbook in FortiAnalyzer, which sends a webhook call to FortiGate so that it runs an automation stitch

5.

FortiGate runs the automation stitch with the corrective or preventive actions"

QUESTION 4

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

A. Configure local DNS servers on FortiAnalyzer

B. Resolve IPs on FortiGate

C. Configure # set resolve-ip enable in the system FortiView settings

D. Resolve IPs on a per-ADOM basis to reduce delay on FortiView while IPs resolve

Correct Answer: B

QUESTION 5

How are logs forwarded when FortiAnalyzer is using aggregation mode?

A. Logs are forwarded as they are received and content files are uploaded at a scheduled time.

B. Logs and content files are stored and uploaded at a scheduled time.

C. Logs are forwarded as they are received.

D. Logs and content files are forwarded as they are received.

Correct Answer: B

https://www.fortinetguru.com/2020/07/log-forwarding-fortianalyzer-fortios-6-2-3/
https://docs.fortinet.com/document/fortianalyzer/6.2.0/administration-guide/420493/modes Reference:
https://docs.fortinet.com/document/fortianalyzer/6.2.0/cookbook/63238/what-is- the-difference-between-log-forward-and-log-aggregation-modes