![Leads4Pass]

NSE5_FAZ-7.0^{Q&As}

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.leads4pass.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

Which statements are true of Administrative Domains (ADOMs) in FortiAnalyzer? (Choose two.)

A. ADOMs are enabled by default.

B. ADOMs constrain other administrator\\'s access privileges to a subset of devices in the device list.

C. Once enabled, the Device Manager, FortiView, Event Management, and Reports tab display per ADOM.

D. All administrators can create ADOMs--not just the admin administrator.

Correct Answer: BC

QUESTION 2

If you upgrade the FortiAnalyzer firmware, which report element can be affected?

A. Custom datasets

B. Report scheduling

C. Report settings

D. Output profiles

Correct Answer: A

https://docs.fortinet.com/document/fortianalyzer/6.2.5/upgrade- guide/669300/checking-reports

QUESTION 3

What is the best approach to handle a hard disk failure on a FortiAnalyzer that supports hardware RAID?

A. Hot swap the disk.

B. There is no need to do anything because the disk will self-recover.

C. Run execute format disk to format and restart the FortiAnalyzer device.

D. Shut down FortiAnalyzer and replace the disk
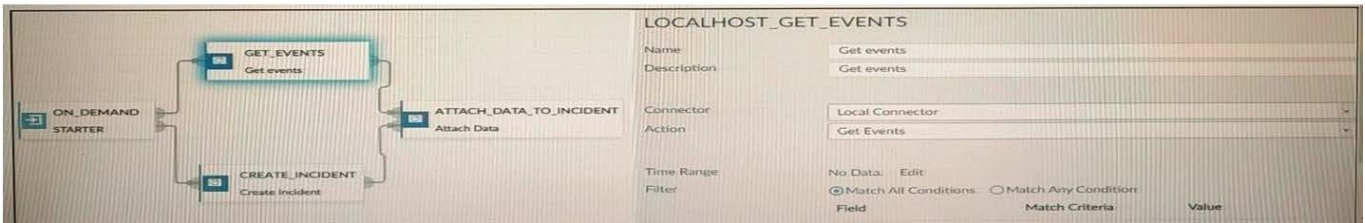
Correct Answer: A

Hardware RAID not software

QUESTION 4

Refer to the exhibits.

Page 306 of 7.0 study guide
Reference: https://help.fortinet.com/fa/faz50hlp/56/5-6-2/FMG- FAZ/2300_Reports/0025_Auto-cache.htm

QUESTION 18
Refer to the exhibits.

Page 306 of 7.0 study guide Reference: https://help.fortinet.com/fa/faz50hlp/56/5-6-2/FMG-FAZ/2300_Reports/0025_Auto-cache.htm

How many events will be added to the incident created after running this playbook?

A. Ten events will be added.

B. No events will be added.

C. Five events will be added.

D. Thirteen events will be added.

Correct Answer: C

QUESTION 5

Which two statements are true regarding FortiAnalyzer log forwarding? (Choose two.)

A. Both modes, forwarding and aggregation, support encryption of logs between devices.

B. In aggregation mode, you can forward logs to syslog and CEF servers as well.

C. Aggregation mode stores logs and content files and uploads them to another FortiAnalyzer device at a scheduled time.

D. Forwarding mode forwards logs in real time only to other FortiAnalyzer devices.

Correct Answer: AC

Aggregation mode is only supported between two FortiAnalyer devices, so B is wrong.

Forwarding is always in real time and does not ONLY forward to other FortiAnalyzer devices. It also forwards to Syslog/CEF. D is wrong. Answer is A and C.

Latest NSE5_FAZ-7.0 Dumps

NSE5_FAZ-7.0 PDF Dumps

NSE5_FAZ-7.0 VCE Dumps