NSE5_FAZ-7.0 Q&As

Fortinet NSE 5 - FortiAnalyzer 7.0

QUESTION 1

When you perform a system backup, what does the backup configuration contain? (Choose two.)

A. Generated reports

B. Device list

C. Authorized devices logs

D. System information

Correct Answer: BD

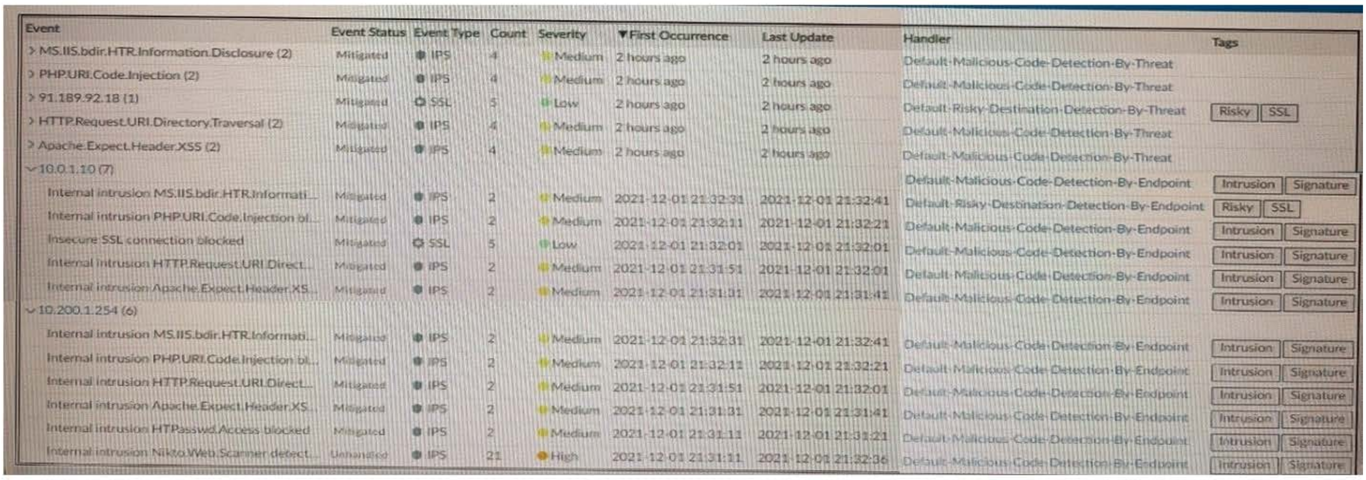
https://help.fortinet.com/fa/cli-olh/5-6- 5/Content/Document/1400_execute/backup.htm Reference: https://help.fortinet.com/fauth/5- 2/Content/Admin%20Guides/5_2%20Admin%20Guide/300/301_Dashboard.htm

QUESTION 2

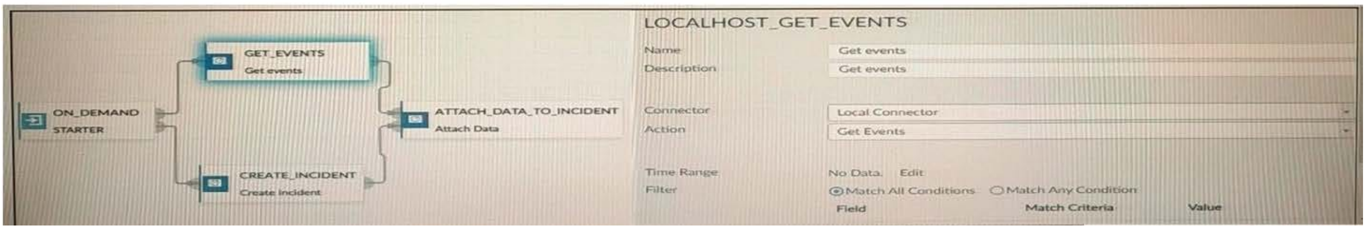
Refer to the exhibits.

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.



Event	Event Status	Event Type	Count	Severity	▼First Occurrence	Last Update	Handler	Tags
> MS.IIS.bdir.HTR.Information.Disclosure (2)	Mitigated	● IPS	4	Medium	2 hours ago	2 hours ago	Default-Malicious-Code-Detection-By-Threat	
> PHP.URI.Code.Injection (2)	Mitigated	● IPS	4	Medium	2 hours ago	2 hours ago	Default-Malicious-Code-Detection-By-Threat	
> 91.189.92.18 (1)	Mitigated	⚙ SSL	5	Low	2 hours ago	2 hours ago	Default-Risky-Destination-Detection-By-Threat	Risky SSL
> HTTP.Request.URI.Directory.Traversal (2)	Mitigated	● IPS	4	Medium	2 hours ago	2 hours ago	Default-Malicious-Code-Detection-By-Threat	
> Apache.Expect.Header.XSS (2)	Mitigated	● IPS	4	Medium	2 hours ago	2 hours ago	Default-Malicious-Code-Detection-By-Threat	
⌄10.0.1.10 (7)							Default-Malicious-Code-Detection-By-Endpoint	Intrusion Signature
Internal intrusion MS.IIS.bdir.HTR.Informati...	Mitigated	● IPS	2	Medium	2021-12-01 21:32:31	2021-12-01 21:32:41	Default-Risky-Destination-Detection-By-Endpoint	Risky SSL
Internal intrusion PHP.URI.Code.Injection bl...	Mitigated	● IPS	2	Medium	2021-12-01 21:32:11	2021-12-01 21:32:21	Default-Malicious-Code-Detection-By-Endpoint	Intrusion Signature
Insecure SSL connection blocked	Mitigated	⚙ SSL	5	Low	2021-12-01 21:32:01	2021-12-01 21:32:01	Default-Malicious-Code-Detection-By-Endpoint	Intrusion Signature
Internal intrusion HTTP.Request.URI.Direct...	Mitigated	● IPS	2	Medium	2021-12-01 21:31:51	2021-12-01 21:32:01	Default-Malicious-Code-Detection-By-Endpoint	Intrusion Signature
Internal intrusion Apache.Expect.Header.XS...	Mitigated	● IPS	2	Medium	2021-12-01 21:31:31	2021-12-01 21:31:41	Default-Malicious-Code-Detection-By-Endpoint	Intrusion Signature
⌄10.200.1.254 (6)								
Internal intrusion MS.IIS.bdir.HTR.Informati...	Mitigated	● IPS	2	Medium	2021-12-01 21:32:31	2021-12-01 21:32:41	Default-Malicious-Code-Detection-By-Endpoint	Intrusion Signature
Internal intrusion PHP.URI.Code.Injection bl...	Mitigated	● IPS	2	Medium	2021-12-01 21:32:11	2021-12-01 21:32:21	Default-Malicious-Code-Detection-By-Endpoint	Intrusion Signature
Internal intrusion HTTP.Request.URI.Direct...	Mitigated	● IPS	2	Medium	2021-12-01 21:31:51	2021-12-01 21:32:01	Default-Malicious-Code-Detection-By-Endpoint	Intrusion Signature
Internal intrusion Apache.Expect.Header.XS...	Mitigated	● IPS	2	Medium	2021-12-01 21:31:31	2021-12-01 21:31:41	Default-Malicious-Code-Detection-By-Endpoint	Intrusion Signature
Internal intrusion HTPasswd.Access blocked	Mitigated	● IPS	2	Medium	2021-12-01 21:31:11	2021-12-01 21:31:21	Default-Malicious-Code-Detection-By-Endpoint	Intrusion Signature
Internal intrusion Nikto.Web.Scanner detect...	Unhandled	● IPS	21	High	2021-12-01 21:31:11	2021-12-01 21:32:36	Default-Malicious-Code-Detection-By-Endpoint	Intrusion Signature



LOCALHOST_GET_EVENTS

Name: Get events
Description: Get events
Connector: Local Connector
Action: Get Events
Time Range: No Data. Edit
Filter: ● Match All Conditions ○ Match Any Condition

Field | Match Criteria | Value

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 3

Which two statements are true regarding FortiAnalyzer operating modes? (Choose two.)

A. By deploying different FortiAnalyzer devices in both modes, you can improve their overall performance.

B. When in collector mode. FortiAnalyzer collects logs from multiple devices and forwards these logs in the original binary format.

C. When in collector mode. FortiAnalyzer supports event management and reporting features.

D. By deploying different FortiAnalyzer devices with collector and analyzer mode in a network, you can improve the overall performance of log receiving, analysis, and reporting

E. Collector mode is the default operating mode.

Correct Answer: AB

FortiAnalyzer_7.0_Study_Guide-Online pag. 10

QUESTION 4

You\\'ve moved a registered logging device out of one ADOM and into a new ADOM. What happens when you rebuild the new ADOM database?

A. FortiAnalyzer resets the disk quota of the new ADOM to default.

B. FortiAnalyzer migrates archive logs to the new ADOM.

C. FortiAnalyzer migrates analytics logs to the new ADOM.

D. FortiAnalyzer removes logs from the old ADOM.

Correct Answer: C

When you move a device, only the archive logs (compressed logs) are migrated to the new ADOM. The analytics logs (indexed logs) stay in the old ADOM until you rebuild the database.
https://kb.fortinet.com/kb/documentLink.do?externalID=FD40383

QUESTION 5

Which SQL query is in the correct order to query the database in the FortiAnslyzer?

A. SELECT devid WHERE \\'user\\'=\\'USER1\\' FROM $log GROUP BY devid

B. FROM $log WHERE \\'user\\'=\\'USER1\\' SELECT devid GROUP BY devid

C. SELECT devid FROM $log WHERE \\'user\\'=\\'USER1\\' GROUP BY devid

D. SELECT devid FROM $log GROUP BY devid WHERE \\'user\\'=\\'USER1\\'

Correct Answer: C

Latest NSE5_FAZ-7.0 Dumps

NSE5_FAZ-7.0 Practice Test

NSE5_FAZ-7.0 Study Guide