NSE7_ADA-6.3 Q&As

Fortinet NSE 7 - Advanced Analytics 6.3

Pass Fortinet NSE7_ADA-6.3 Exam with 100% Guarantee

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

QUESTION 1

How can you invoke an integration policy on FortiSIEM rules?

A. Through Notification Policy settings

B. Through Incident Notification settings

C. Through remediation scripts

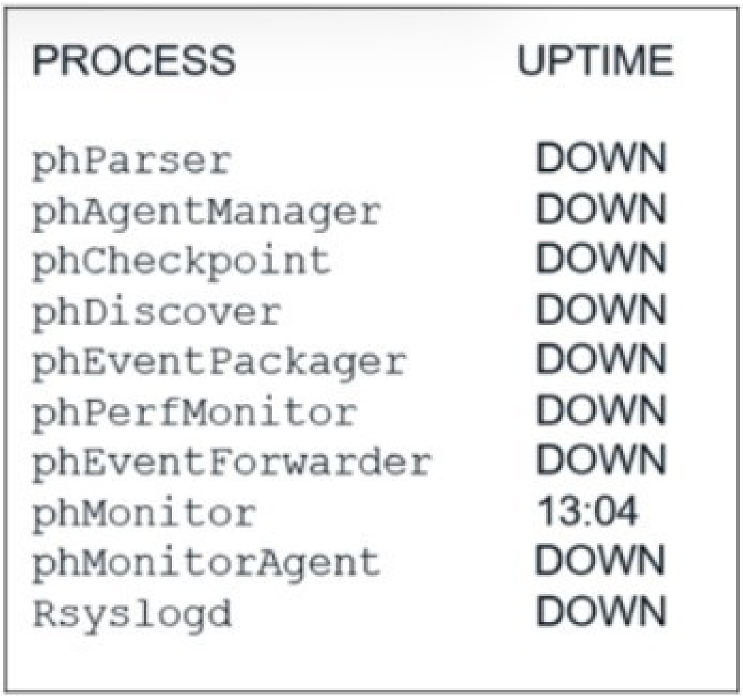
D. Through External Authentication settings

Correct Answer: A

Explanation: You can invoke an integration policy on FortiSIEM rules by configuring the Notification Policy settings. You can select an integration policy from the drop-down list and specify the conditions for triggering it. For example, you can invoke an integration policy when an incident is created, updated, or closed. References: Fortinet NSE 7 - Advanced Analytics 6.3 escription, page 9

QUESTION 2

Refer to the exhibit.



```
PROCESS                 UPTIME

phParser                DOWN
phAgentManager          DOWN
phCheckpoint            DOWN
phDiscover              DOWN
phEventPackager         DOWN
phPerfMonitor           DOWN
phEventForwarder        DOWN
phMonitor               13:04
phMonitorAgent          DOWN
Rsyslogd                DOWN
```

An administrator deploys a new collector for the first time, and notices that all the processes except the phMonitor are down. How can the administrator bring the processes up?

A. The administrator needs to run the command phtools --start all on the collector.

B. Rebooting the collector will bring up the processes.

C. The processes will come up after the collector is registered to the supervisor.

D. The collector was not deployed properly and must be redeployed.

Correct Answer: C

Explanation: The collector processes are dependent on the registration with the supervisor. The phMonitor process is responsible for registering the collector to the supervisor and monitoring the health of other processes. After the registration is successful, the phMonitor will start the other processes on the collector.

QUESTION 3

Which three statements about collector communication with the FortiSIEM cluster are true? (Choose three.)

A. The only communication between the collector and the supervisor is during the registration process.

B. Collectors communicate periodically with the supervisor node.

C. The supervisor periodically checks the health of the collector.

D. The supervisor does not initiate any connections to the collector node.

E. Collectors upload event data to any node in the worker upload list, but report their health directly to the supervisor node.

Correct Answer: BCE

Explanation: The statements about collector communication with the FortiSIEM cluster that are true are:

Collectors communicate periodically with the supervisor node. Collectors send heartbeat messages to the supervisor every 30 seconds to report their status and configuration.

The supervisor periodically checks the health of the collector. The supervisor monitors the heartbeat messages from collectors and alerts if there is any issue with their connectivity or performance.

Collectors upload event data to any node in the worker upload list, but report their health directly to the supervisor node. Collectors use a round-robin algorithm to distribute event data among worker nodes in the worker upload list, which is

provided by the supervisor during registration. However, collectors only report their health and status to the supervisor node.

QUESTION 4

Which syntax will register a collector to the supervisor?

A. phProvisionCollector --add

B. phProvisionCollector --add

C. phProvisionCollector --add

D. phProvisionCollector --add

Correct Answer: B

Explanation: The syntax that will register a collector to the supervisor is phProvisionCollector --add . This command will initiate the registration process between the collector and the supervisor, and exchange certificates and configuration information. The parameter is the IP address of the supervisor node.

QUESTION 5

In the event of a WAN link failure between the collector and the supervisor, by default, what is the maximum number of event files stored on the collector?

A. 30.000

B. 10.000

C. 40.000

D. 20.000

Correct Answer: B

Explanation: By default, the maximum number of event files stored on the collector in the event of a WAN link failure between the collector and the supervisor is 10.000. This value can be changed in the collector.properties file by modifying the parameter max_event_files_to_store. References: Fortinet NSE 7 - Advanced Analytics 6.3 escription, page 13

QUESTION 6

Identify the processes associated with Machine Learning/AI on FortiSIEM. (Choose two.)

A. phFortiInsightAI

B. phReportMaster

C. phRuleMaster

D. phAnomaly

E. phRuleWorker

Correct Answer: AD

Explanation: The processes associated with Machine Learning/AI on FortiSIEM are phFortiInsightAI and phAnomaly. phFortiInsightAI is responsible for detecting anomalous user behavior using UEBA (User and Entity Behavior Analytics) techniques. phAnomaly is responsible for detecting anomalous network behavior using NTA (Network Traffic Analysis) techniques.

QUESTION 7

On which disk are the SQLite databases that are used for the baselining stored?

A. Disk1

B. Disk4

C. Disk2

D. Disk3

Correct Answer: D

Explanation: The SQLite databases that are used for the baselining are stored on Disk3 of the FortiSIEM server. Disk3 is also used for storing raw event data and CMDB data.

QUESTION 8

What are the modes of Data Ingestion on FortiSOAR? (Choose three.)

A. Rule based

B. Notification based

C. App Push

D. Policy based

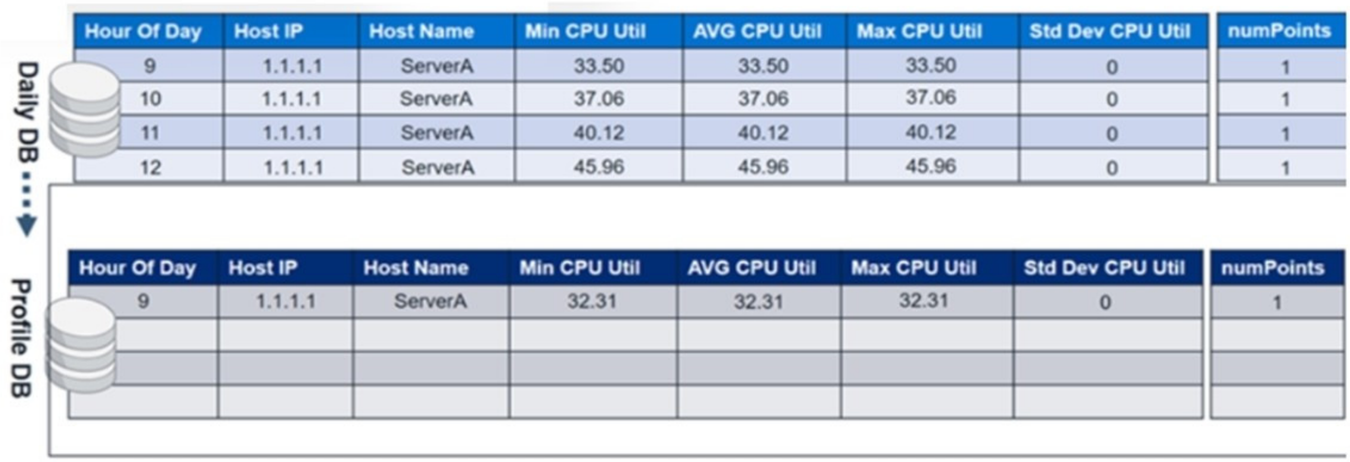
E. Schedule based

Correct Answer: BCE

Explanation: The modes of Data Ingestion on FortiSOAR are notification based, app push, and schedule based. Notification based mode allows FortiSOAR to receive data from external sources via webhooks or email notifications. App push mode allows FortiSOAR to receive data from external sources via API calls or scripts. Schedule based mode allows FortiSOAR to pull data from external sources at regular intervals using connectors. References: Fortinet NSE 7 - Advanced Analytics 6.3 escription, page 17

QUESTION 9

Refer to the exhibit. Click on the calculator button.


Daily DB
Profile DB

Hour Of Day	Host IP	Host Name	Min CPU Util	AVG CPU Util	Max CPU Util	Std Dev CPU Util	numPoints
9	1.1.1.1	ServerA	33.50	33.50	33.50	0	1
10	1.1.1.1	ServerA	37.06	37.06	37.06	0	1
11	1.1.1.1	ServerA	40.12	40.12	40.12	0	1
12	1.1.1.1	ServerA	45.96	45.96	45.96	0	1

Hour Of Day	Host IP	Host Name	Min CPU Util	AVG CPU Util	Max CPU Util	Std Dev CPU Util	numPoints
9	1.1.1.1	ServerA	32.31	32.31	32.31	0	1

The profile database contains CPU utilization values from day one. At midnight on the second day, the CPU utilization values from the daily database will be merged with the profile database.

In the profile database, in the Hour of Day column where 9 is the value, what will be the updated minimum, maximum, and average CPU utilization values?

A. Min CPU Util=32.31, Max CPU Ucil=33.50 and AVG CPU Util=33.50

B. Min CPU Util=32.31, Max CPU Ucil=33.50 and AVG CPU Util=32.67

C. Min CPU Util=32.31, Max CPU Ucil=32.31 and AVG CPU Util=32.31

D. Min CPU Util=33.50, Max CPU Ucil=33.50 and AVG CPU Util=33.50

Correct Answer: B

Explanation: The profile database contains CPU utilization values from day one. At midnight on the second day, the CPU utilization values from the daily database will be merged with the profile database using a weighted average formula:

New value = (Old value x Old weight) + (New value x New weight) / (Old weight + New weight)

The weight is determined by the number of days in each database. In this case, the profile database has one day of data and the daily database has one day of data, so the weight is equal for both databases. Therefore, the formula simplifies

to:

New value = (Old value + New value) / 2

In the profile database, in the Hour of Day column where 9 is the value, the updated minimum, maximum, and average CPU utilization values are:

Min CPU Util = (32.31 + 32.31) / 2 = 32.31 Max CPU Util = (33.50 + 33.50) / 2 = 33.50 AVG CPU Util = (32.67 + 32.67) / 2 = 32.67

QUESTION 10

What is Tactic in the MITRE ATTandCK framework?

A. Tactic is how an attacker plans to execute the attack

B. Tactic is what an attacker hopes to achieve

C. Tactic is the tool that the attacker uses to compromise a system

D. Tactic is a specific implementation of the technique

Correct Answer: B

Explanation: Tactic is what an attacker hopes to achieve in the MITRE ATTandCK framework. Tactic is a high-level category of adversary behavior that describes their objective or goal. For example, some tactics are Initial Access, Persistence, Lateral Movement, Exfiltration, etc. Each tactic consists of one or more techniques that describe how an attacker can accomplish that tactic.