NSE7_ADA-6.3 Q&As

Fortinet NSE 7 - Advanced Analytics 6.3

Pass Fortinet NSE7_ADA-6.3 Exam with 100% Guarantee

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

https://www.certbus.com/nse7_ada-6-3.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

Refer to the exhibit.

```
psql -U phoenix phoenixdb
select cust_org_id, name, ip_addr, natural_id, collector_id from ph_sys_connector;

cust_org_id |      name      |  ip_addr   |              natural_id              | collector_id
------------+----------------+------------+--------------------------------------+-------------
    2000    | OrgA_Collector | 10.10.2.91 | 564DA6D2-1D90-1483-23F9-43F2AC4A3ABF |    1000
```

The exhibit shows the output of an SQL command that an administrator ran to view the natural_id value, after logging into the Postgres database. What does the natural_id value identify?

A. The supervisor

B. The worker

C. An agent

D. The collector

Correct Answer: D

Explanation: The natural_id value identifies the collector in the FortiSIEM system. The natural_id is a unique identifier that is assigned to each collector during the registration process with the supervisor. The natural_id is used to associate events and performance data with the collector that collected them.

QUESTION 2

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

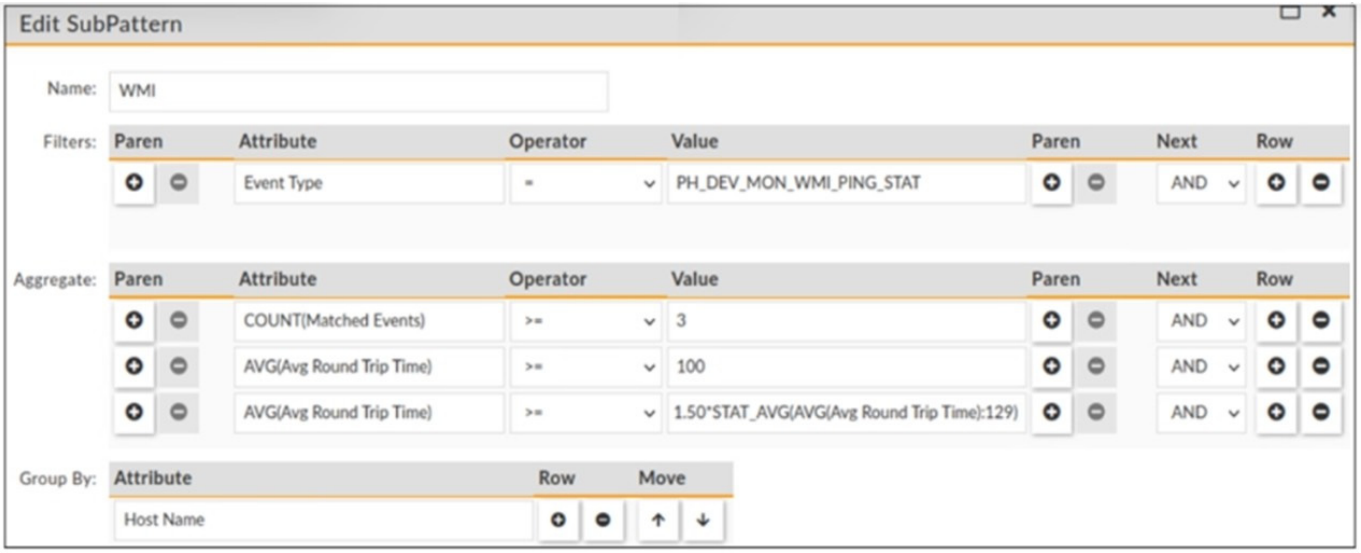
D. Tactic is a specific implementation of the technique

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.

QUESTION 3

Refer to the exhibit.



The window for this rule is 30 minutes. What is this rule tracking?

A. A sudden 50% increase in WMI response times over a 30-minute time window

B. A sudden 1.50 times increase in WMI response times over a 30-minute time window

C. A sudden 75% increase in WMI response times over a 30-minute time window

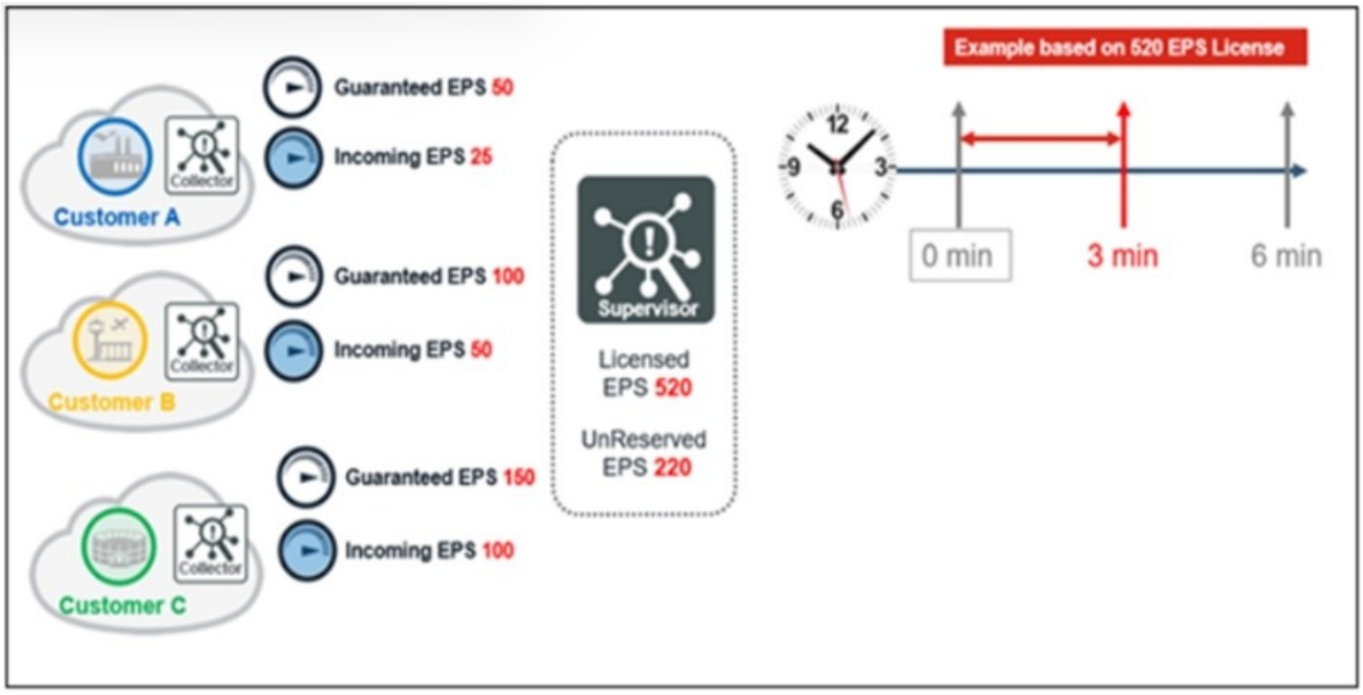
D. A sudden 150% increase in WMI response times over a 30-minute time window

Correct Answer: B

Explanation: The rule is tracking the WMI response times from Windows devices using a baseline calculation. The rule will trigger an incident if the current WMI response time is greater than or equal to 1.50 times the average WMI response time in the last 30 minutes.

QUESTION 4

Refer to the exhibit. Click on the calculator button.



Based on the information provided in the exhibit, calculate the unused events for the next three minutes for a 520 EPS license.

A. 72460

B. 73460

C. 74460

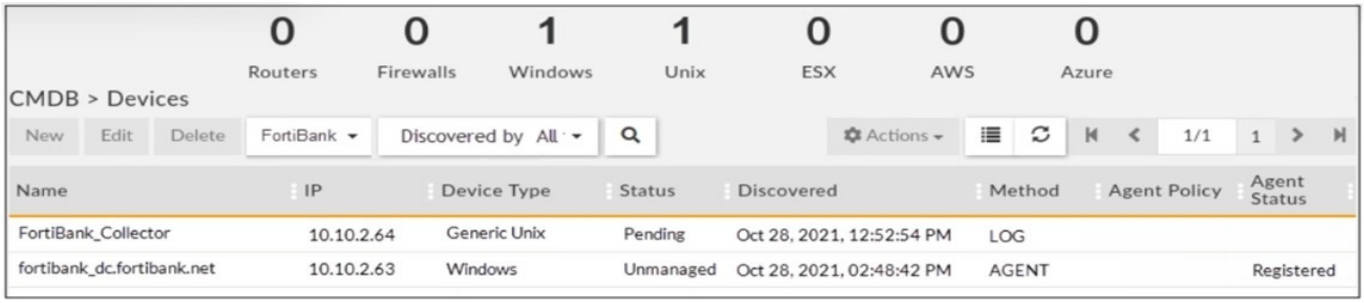
D. 71460

Correct Answer: B

Explanation: The unused events for the next three minutes for a 520 EPS license can be calculated by multiplying the licensed EPS by the time interval and subtracting the total number of events received in that interval. In this case, the calculation is: 520 x 180 - 27000 = 73460

QUESTION 5

Refer to the exhibit.



Is the Windows agent delivering event logs correctly?

A. The logs are buffered by the agent and will be sent once the status changes to managed.

B. The agent is registered and it is sending logs correctly.

C. The agent is not sending logs because it did not receive a monitoring template.

D. Because the agent is unmanaged. the logs are dropped silently by the supervisor.

Correct Answer: D

Explanation: The windows agent is not delivering event logs correctly because the agent is unmanaged, meaning it is not assigned to any organization or customer. The supervisor will drop the logs silently from unmanaged agents, as they are not associated with any valid license or CMDB.

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

Which two statements about the maximum device limit on FortiSIEM are true? (Choose two.)

A. The device limit is defined per customer and every customer is assigned a fixed number of device limit by the service provider.

B. The device limit is only applicable to enterprise edition.

C. The device limit is based on the license type that was purchased from Fortinet.

D. The device limit is defined for the whole system and is shared by every customer on a service provider edition.

Correct Answer: BC

Explanation: The device limit is a feature of the enterprise edition of FortiSIEM that restricts the number of devices that can be added to the system based on the license type. The device limit does not apply to the service provider edition, which allows unlimited devices per customer. The device limit is determined by the license type that was purchased

from Fortinet, such as 100 devices, 500 devices, or unlimited devices.

QUESTION 8

From where does the rule engine load the baseline data values?

A. The profile report

B. The daily database

C. The profile database

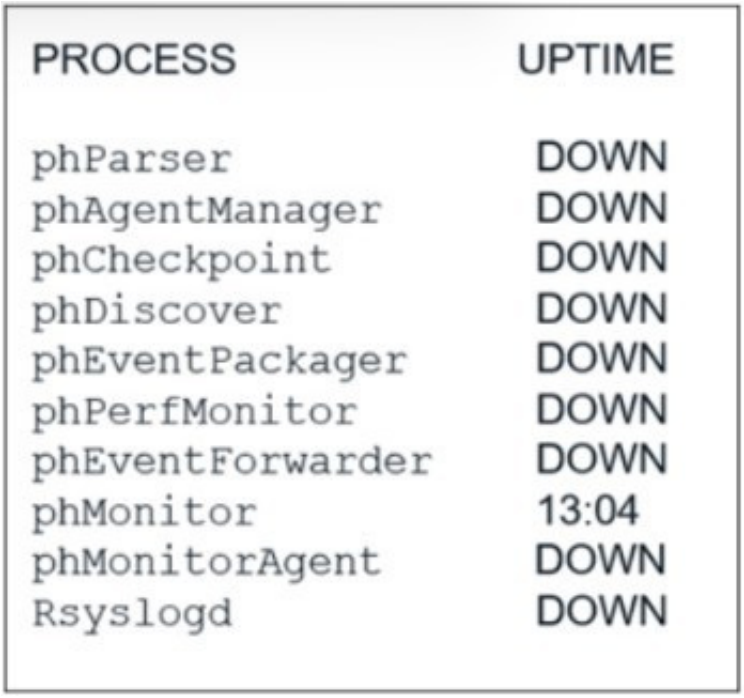
D. The memory

Correct Answer: C

Explanation: The rule engine loads the baseline data values from the profile database. The profile database contains historical data that is used for baselining calculations, such as minimum, maximum, average, standard deviation, and percentile values for various metrics.

QUESTION 9

Refer to the exhibit.



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 10

Which three processes are collector processes? (Choose three.)

A. phAgentManaqer

B. phParser

C. phRuleMaster

D. phReportM aster

E. phMonitorAgent

Correct Answer: BCE

Explanation: The collector processes are responsible for receiving, parsing, normalizing, correlating, and monitoring events from various sources. The collector processes are phParser, phRuleMaster, and phMonitorAgent.