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.pass2lead.com/nse7_ada-6-3.html

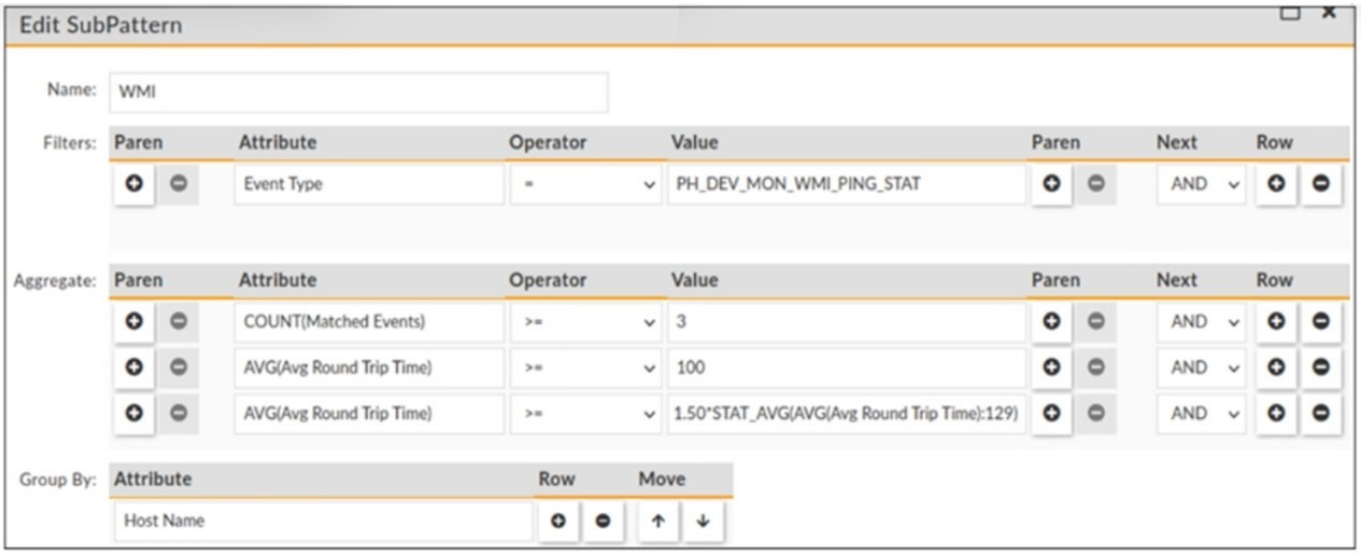
100% Passing Guarantee
100% Money Back Assurance

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.



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 2

Which statement about EPS bursting is true?

A. FortiSIEM will let you burst up to five times the licensed EPS once during a 24-hour period.

B. FortiSIEM must be provisioned with ten percent the licensed EPS to handle potential event surges.

C. FortiSIEM will let you burst up to five times the licensed EPS at any given time, provided it has accumulated enough unused EPS.

D. FortiSIEM will let you burst up to five times the licensed EPS at any given time, regardless of unused of EPS.

Correct Answer: C

Explanation: FortiSIEM allows EPS bursting to handle event spikes without dropping events or violating the license agreement. EPS bursting means that FortiSIEM will let you burst up to five times the licensed EPS at any given time, provided it has accumulated enough unused EPS from previous time intervals.

QUESTION 3

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

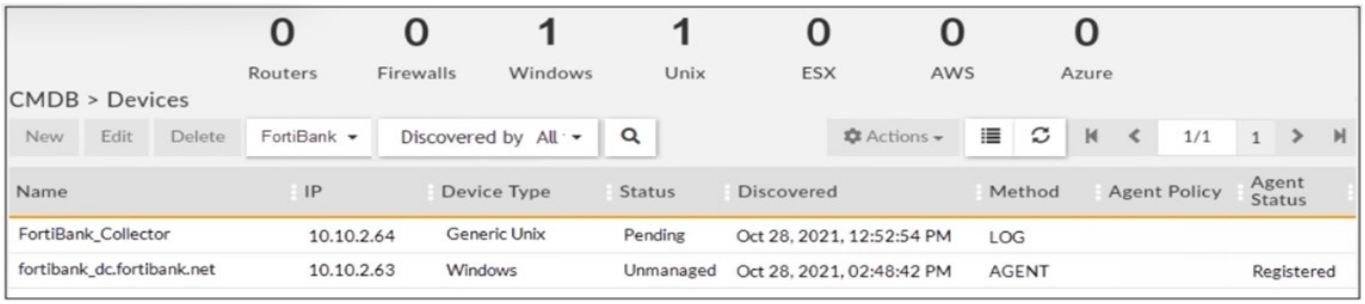
D. The collector

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 4

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 5

Why can collectors not be defined before the worker upload address is set on the supervisor?

A. Collectors can only upload data to a worker, and the supervisor is not a worker

B. To ensure that the service provider has deployed at least one worker along with a supervisor

C. Collectors receive the worker upload address during the registration process

D. To ensure that the service provider has deployed a NFS server

Correct Answer: C

Explanation: Collectors cannot be defined before the worker upload address is set on the supervisor because collectors receive the worker upload address during the registration process. The worker upload address is a list of IP addresses of worker nodes that can receive event data from collectors. The supervisor provides this list to collectors when they register with it, so that collectors can upload event data to any node in the list.