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.leads4pass.com/nse7_ada-6-3.html

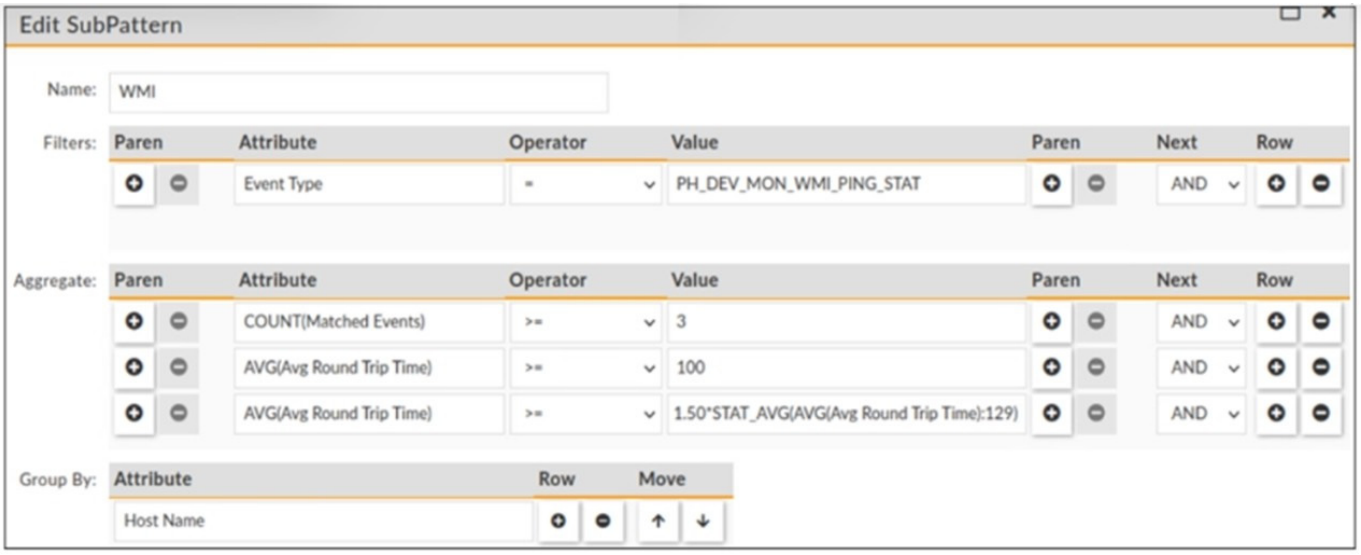
100% Passing Guarantee
100% Money Back Assurance

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 three statements about phRuleMaster are true? (Choose three.)

A. phRuleMaster queues up the data being received from the phRuleWorkers into buckets.

B. phRuleMaster is present on the supervisor and workers.

C. phRuleMaster is present on the supervisor only

D. phRuleMaster wakes up to evaluate all the rule data in series, every 30 seconds.

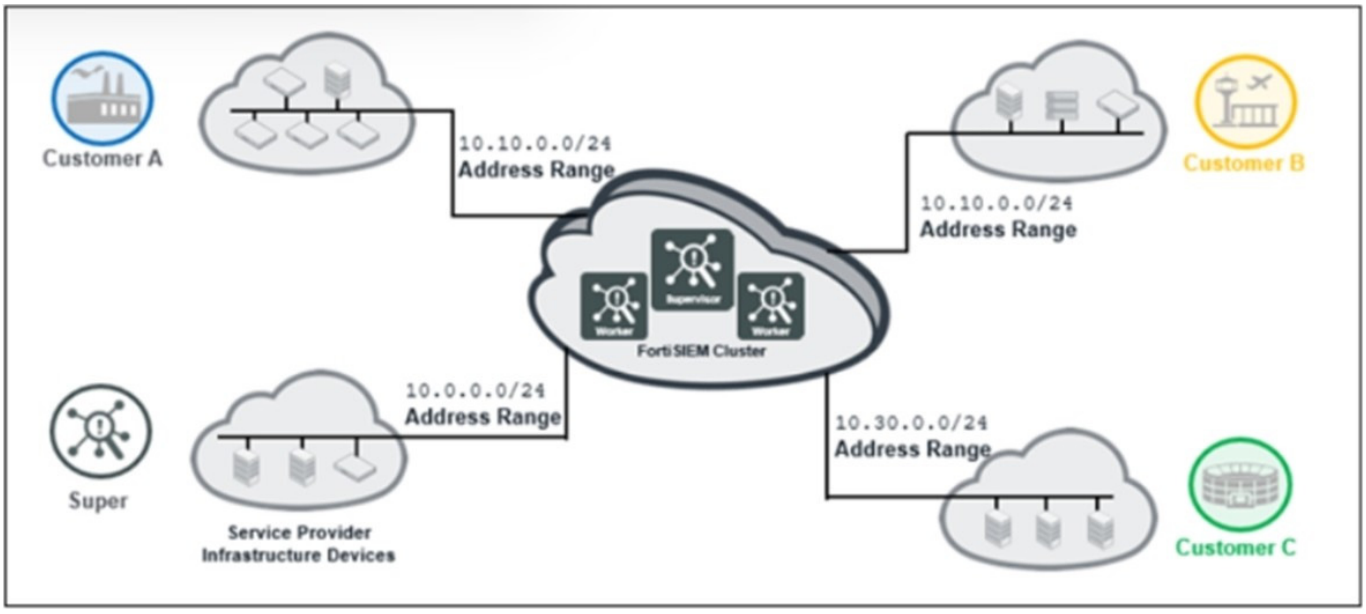
E. phRuleMaster wakes up to evaluate all the rule data in parallel, even/ 30 seconds

Correct Answer: ABE

Explanation: phRuleMaster is a process that performs rule evaluation and incident generation on FortiSIEM. phRuleMaster queues up the data being received from the phRuleWorkers into buckets based on time intervals, such as one minute, five minutes, or ten minutes. phRuleMaster is present on both the supervisor and workers nodes of a FortiSIEM cluster. phRuleMaster wakes up every 30 seconds to evaluate all the rule data in parallel using multiple threads.

QUESTION 3

Refer to the exhibit.



The service provider deployed FortiSIEM without a collector and added three customers on the supervisor. What mistake did the administrator make?

A. Customer A and customer B have overlapping IP addresses.

B. Collectors must be deployed on all customer premises before they are added to organizations on the supervisor.

C. The number of workers on the FortiSIEM cluster must match the number of customers added.

D. At least one collector must be deployed to collect logs from service provider infrastructure devices.

Correct Answer: A

Explanation: The mistake that the administrator made is that customer A and customer B have overlapping IP addresses. This will cause confusion and errors in event collection and correlation, as well as CMDB discovery and classification. To avoid this problem, each customer should have a unique IP address range or use NAT to translate their IP addresses.

QUESTION 4

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

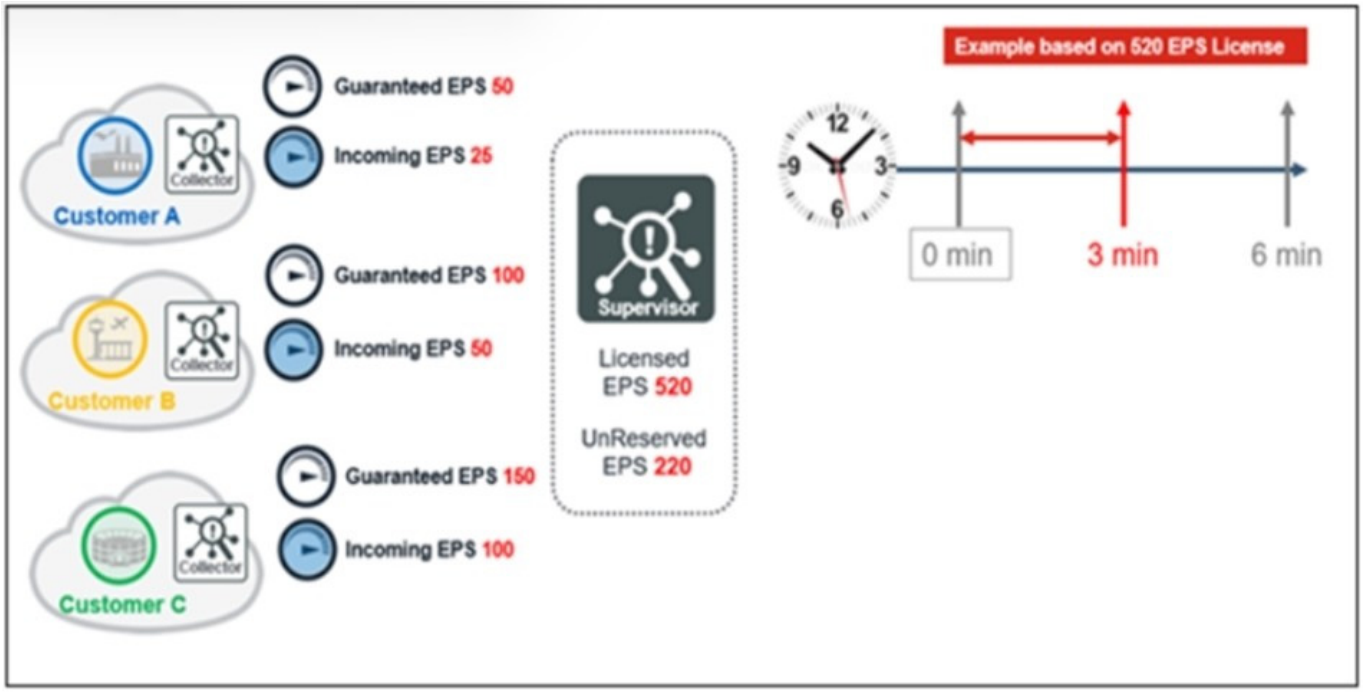
D. To ensure that the service provider has deployed a NFS server

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.

QUESTION 5

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