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.pass4itsure.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

QUESTION 1

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.

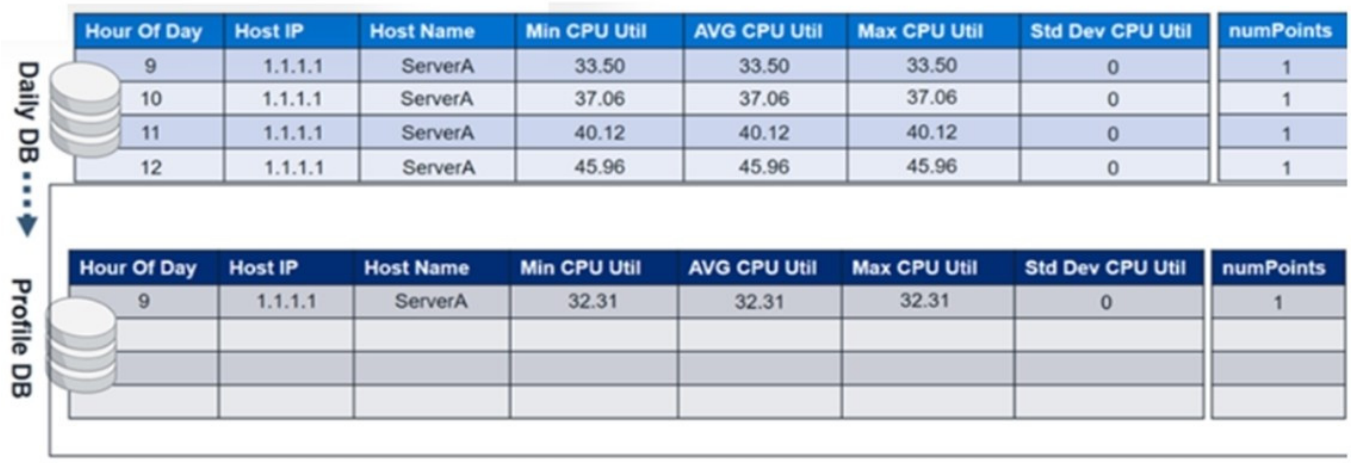
E. phRuleMaster wakes up to evaluate all the rule data in parallel, even/ 30 seconds

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 2

Refer to the exhibit. Click on the calculator button.



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:

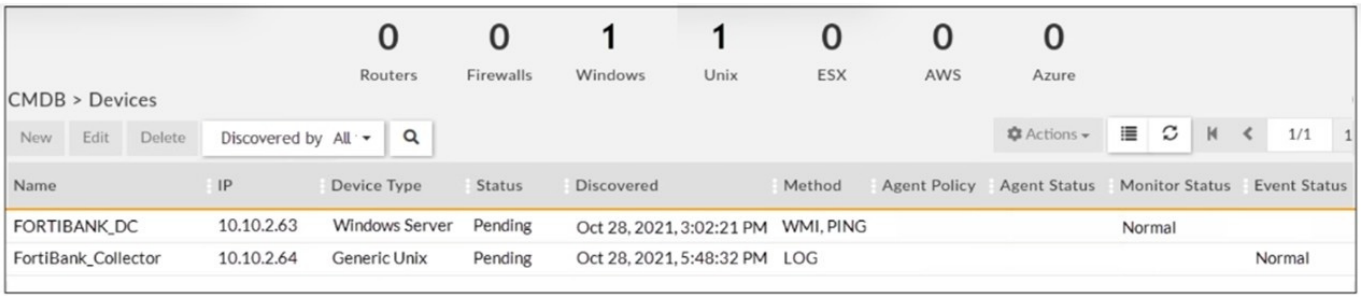
New value = (Old value + New value) / 2

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 3

Refer to the exhibit.



Why is the windows device still in the CMDB, even though the administrator uninstalled the windows agent?

A. The device was not uninstalled properly

B. The device must be deleted from backend of FortiSIEM

C. The device has performance jobs assigned

D. The device must be deleted manually from the CMDB

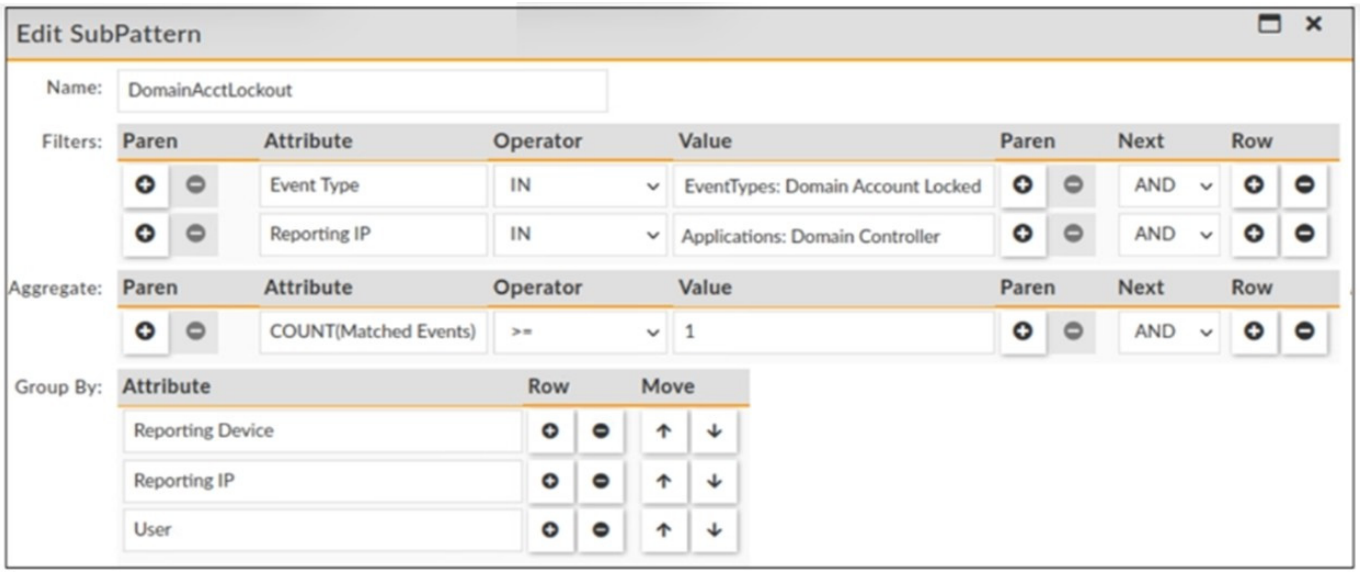
Correct Answer: D

Explanation: The windows device is still in the CMDB, even though the administrator uninstalled the windows agent, because the device must be deleted manually from the CMDB. Uninstalling the windows agent does not automatically

remove the device from the CMDB, as there may be other sources of data for the device, such as SNMP or syslog. To delete the device from the CMDB, the administrator must go to CMDB > Devices > All Devices, select the device, and click Delete.

QUESTION 4

Refer to the exhibit.



Which statement about the rule filters events shown in the exhibit is true?

A. The rule filters events with an event type that belong to the Domain Account Locked CMDB group or a reporting IP that belong to the Domain Controller applications group.

B. The rule filters events with an event type that belong to the Domain Account Locked CMDB group and a reporting |P that belong to the Domain Controller applications group.

C. The rule filters events with an event type that belong to the Domain Account Locked CMDB group and a user that belongs to the Domain Controller applications group.

D. The rule filters events with an event type that equals Domain Account Locked and a reporting IP that equals Domain Controller applications.

Correct Answer: B

Explanation: The rule filters events with an event type that belong to the Domain Account Locked CMDB group and a reporting IP that belong to the Domain Controller applications group. This means that only events that have both criteria met will be processed by this rule. The event type and reporting IP are joined by an AND operator, which requires both conditions to be true.

QUESTION 5

What is the disadvantage of automatic remediation?

A. It can make a disruptive change to a user, block access to an application, or disconnect critical systems from the

network.

B. It is equivalent to running an IPS in monitor-only mode -- watches but does not block.

C. External threats or attacks detected by FortiSIEM will need user interaction to take action on an already overworked SOC team.

D. Threat behaviors occurring during the night could take hours to respond to.

Correct Answer: A

Explanation: The disadvantage of automatic remediation is that it can make a disruptive change to a user, block access to an application, or disconnect critical systems from the network. Automatic remediation can have unintended consequences if not carefully planned and tested. Therefore, it is recommended to use manual or semi-automatic remediation for sensitive or critical systems. References: Fortinet NSE 7 - Advanced Analytics 6.3 escription, page 15