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:

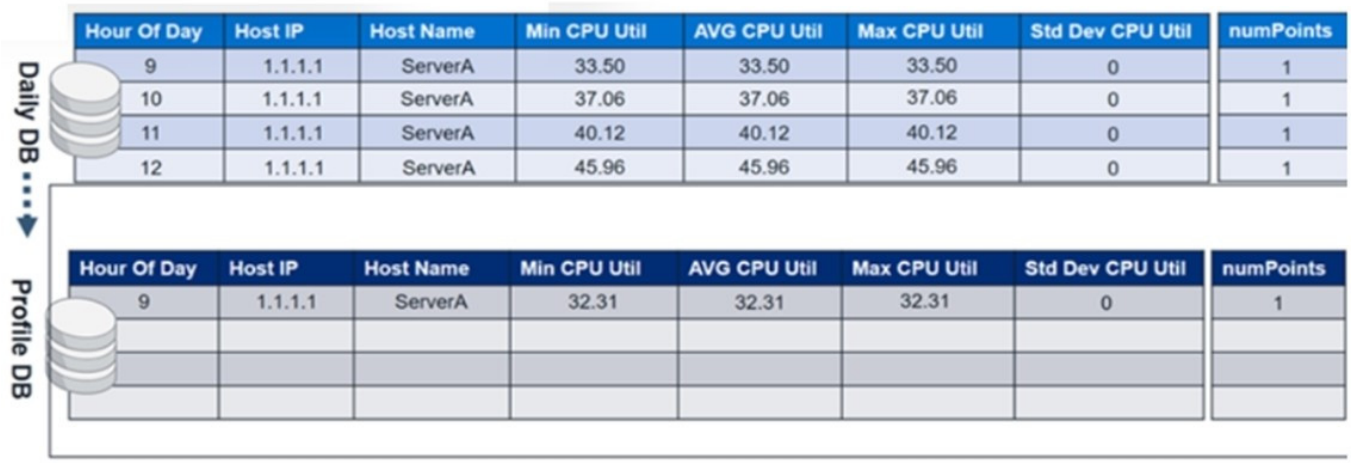
https://www.geekcert.com/nse7_ada-6-3.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Refer to the exhibit. Click on the calculator button.



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 2

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 3

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 4

Refer to the exhibit.

Event Receive Time	Event Type	Source IP	Destination IP	Reporting IP	User	Raw Event Log
08:49:01 02/02/2018	FortiGate-ssl-vpn-logon-failure	203.0.113.4	192.0.2.10	10.0.1.99	Admin	<189>date=2018-02-02…
08:49:24 02/02/2018	FortiGate-ssl-vpn-logon-failure	198.51.100.46	192.0.5.30	10.0.2.10	Tom	<189>date=2018-02-02…
08:50:31 02/02/2018	FortiGate-ssl-vpn-logon-failure	203.0.113.50	192.0.2.10	10.2.2.55	Jan	<189>date=2018-02-02…
08:50:45 02/02/2018	FortiGate-ssl-vpn-logon-failure	198.51.100.46	192.0.5.30	10.0.2.10	Tom	<189>date=2018-02-02…
08:52:59 02/02/2018	FortiGate-ssl-vpn-logon-failure	203.0.113.4	192.0.2.10	10.0.1.99	Admin	<189>date=2018-02-02…
08:55:09 02/02/2018	FortiGate-ssl-vpn-logon-failure	198.51.100.46	192.0.5.30	10.0.2.10	Tom	<189>date=2018-02-02…
08:52:59 02/02/2018	FortiGate-ssl-vpn-logon-failure	203.0.113.5	192.0.2.10	10.0.1.99	Admin	<189>date=2018-02-02…
08:52:59 02/02/2018	FortiGate-ssl-vpn-logon-failure	203.0.113.4	192.0.2.10	10.0.1.99	Sarah	<189>date=2018-02-02…
08:50:31 02/02/2018	FortiGate-ssl-vpn-logon-failure	203.0.113.50	192.0.2.10	10.2.2.55	Jan	<189>date=2018-02-02…

An administrator runs an analytic search for all FortiGate SSL VPN logon failures. The results are grouped by source IP, reporting IP, and user. The administrator wants to restrict the results to only those rows where the COUNT >= 3. Which user would meet that condition?

A. Sarah

B. Jan

C. Tom

D. Admin

Correct Answer: C

Explanation: The user who would meet that condition is Tom. Tom has four rows in the results where the COUNT is greater than or equal to three, meaning he had at least three SSL VPN logon failures from the same source IP and reporting IP. The other users have either less than three rows or less than three COUNT in each row.

QUESTION 5

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.

NSE7_ADA-6.3 Study Guide | NSE7_ADA-6.3 Exam Questions | NSE7_ADA-6.3 Braindumps