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:

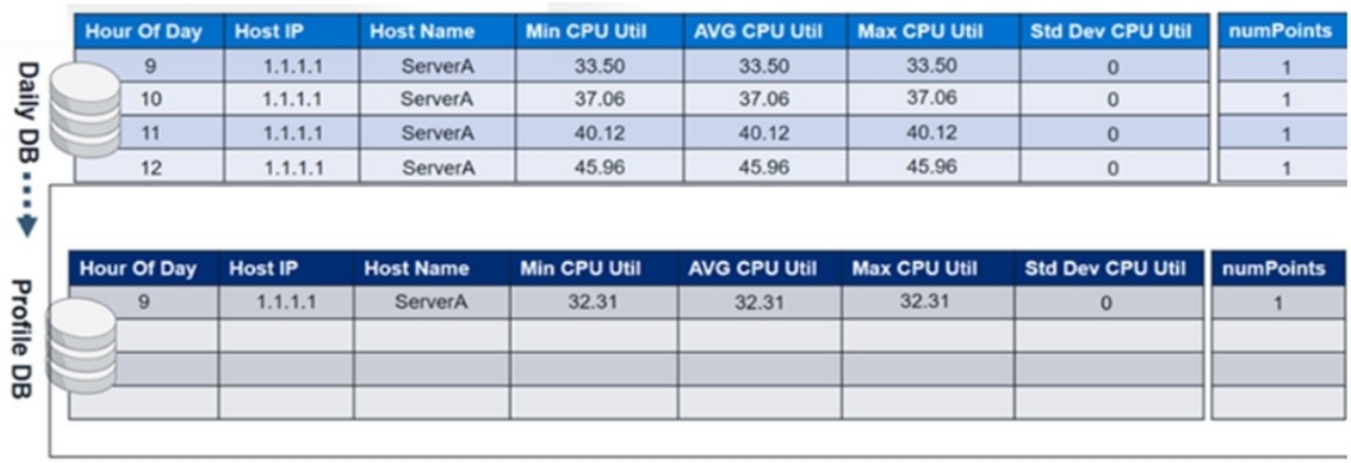
https://www.leads4pass.com/nse7_ada-6-3.html

100% Passing Guarantee
100% Money Back Assurance

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

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

In the event of a WAN link failure between the collector and the supervisor, by default, what is the maximum number of event files stored on the collector?

A. 30.000

B. 10.000

C. 40.000

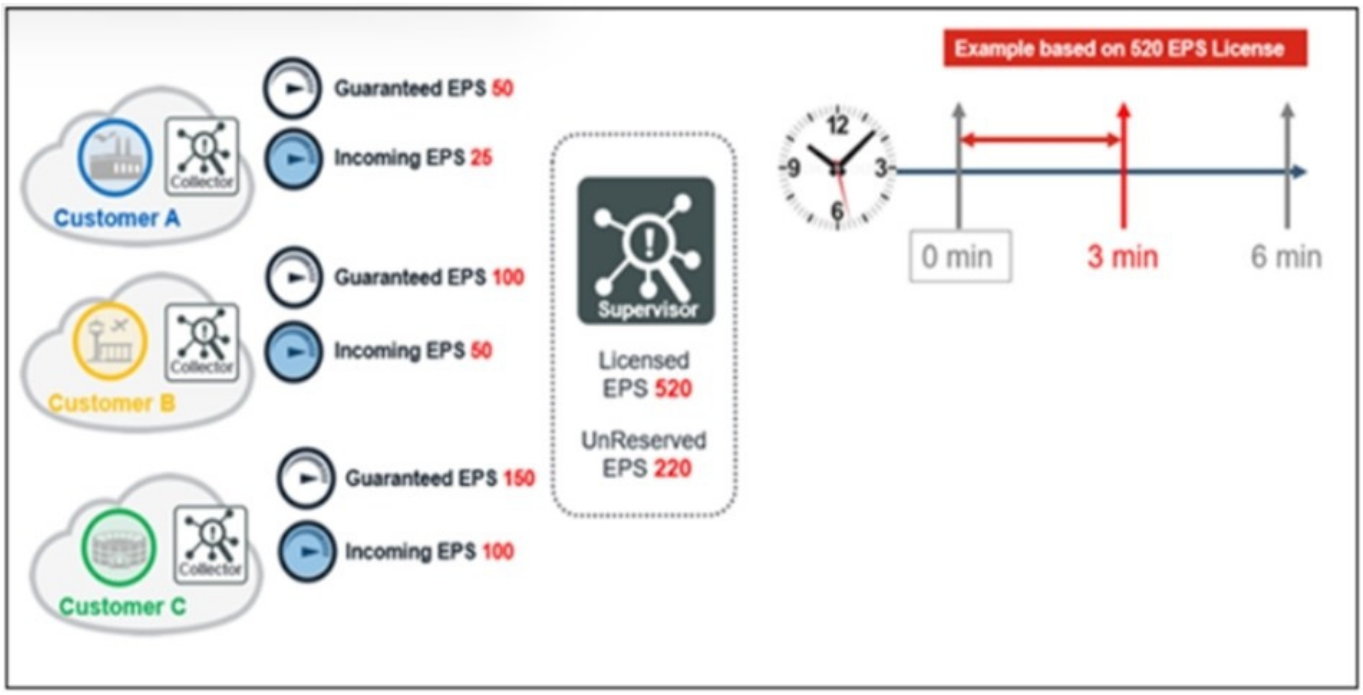
D. 20.000

Correct Answer: B

Explanation: By default, the maximum number of event files stored on the collector in the event of a WAN link failure between the collector and the supervisor is 10.000. This value can be changed in the collector.properties file by modifying the parameter max_event_files_to_store. References: Fortinet NSE 7 - Advanced Analytics 6.3 escription, page 13

QUESTION 3

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 4

What are the modes of Data Ingestion on FortiSOAR? (Choose three.)

A. Rule based

B. Notification based

C. App Push

D. Policy based

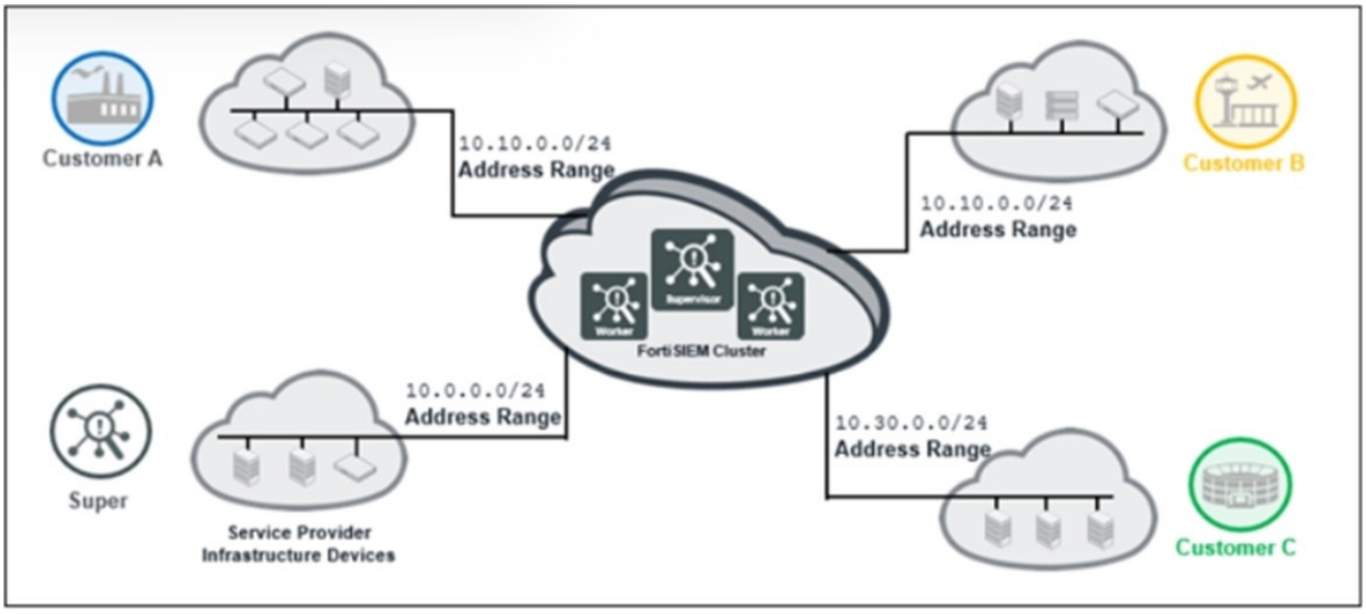
E. Schedule based

Correct Answer: BCE

Explanation: The modes of Data Ingestion on FortiSOAR are notification based, app push, and schedule based. Notification based mode allows FortiSOAR to receive data from external sources via webhooks or email notifications. App push mode allows FortiSOAR to receive data from external sources via API calls or scripts. Schedule based mode allows FortiSOAR to pull data from external sources at regular intervals using connectors. References: Fortinet NSE 7 - Advanced Analytics 6.3 escription, page 17

QUESTION 5

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.