EndExam

QUESTION & ANSWER

Accurate study guides, High passing rate!

1 / 4

Exam   :   FCSS_ADA_AR-6.7

Title   :   FCSS—Advanced Analytics 6.7 Architect

Version   :   DEMO

1.Refer to the exhibit.

	Hour Of Day	Host IP	Host Name	Min CPU Util	AVG CPU Util	Max CPU Util	Std Dev CPU Util	numPoints
Daily DB	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
Profile DB	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 Util=33.50 and AVG CPU Util=33.50
B. Min CPU Util=32.31, Max CPU Util=33.50 and AVG CPU Util=32.67
C. Min CPU Util=32.31, Max CPU Util=32.31 and AVG CPU Util=32.31
D. Min CPU Util=33.50, Max CPU Util=33.50 and AVG CPU Util=33.50
Answer: B

2.What is the primary purpose of remediation in FortiSIEM?
A. To add new users to the network?
B. To address and resolve detected security incidents?
C. To upgrade the FortiSIEM software?
D. To change the visual theme of the FortiSIEM interface?
Answer: B

3.Refer to the exhibit.

```
PROCESS                  UPTIME

phParser                 DOWN
phAgentManager           DOWN
phCheckpoint             DOWN
phDiscover               DOWN
phEventPackager          DOWN
phPerfMonitor            DOWN
phEventForwarder         DOWN
phMonitor                13:04
phMonitorAgent           DOWN
Rsyslogd                 DOWN
```

An administrator deploys a new collector for the first time, and notices that all the processes except the phMonitor are down.

How can the administrator bring the processes up?

A. The administrator needs to run the command phtools --start all on the collector.

B. Rebooting the collector will bring up the processes.

C. The processes will come up after the collector is registered to the supervisor.

D. The collector was not deployed properly and must be redeployed.

Answer: C

4.Refer to the exhibit.

●	Jun 03 2020, 10:47:00 AM	No Ping Response From Server	Auto Cleared
●	Jun 02 2020, 05:46:30 PM	Missing specific performance ...	Auto Cleared
●	Jun 02 2020, 05:46:30 PM	Missing specific performance ...	Auto Cleared
●	Jun 02 2020, 05:46:30 PM	Missing specific performance ...	Auto Cleared

Details   Events   Rule   ☐ Auto expand

Clear If: WITHIN   WITHIN 5 minutes the following conditions are met
           PATTERN   AllPingLossSrv_CLEAR
           WITH   Host IP = AllPingLossSrv_CLEAR.Host IP
           SUCHTHAT   Clear_Condition.Host IP = Original_Rule.Host IP

Incidents: GENERATE   Severity 10 (HIGH) Incident: PH_RULE_NON_RESPONSIVE_SER\
           WITH   Host IP = AllPingLossSrv.Host IP, Host IP = SystemShutdown.R\

Watch Lists: UPDATE   Availability Issues
             WITH   Host Name

Why was this incident auto cleared?

A. Within five minutes the packet loss percentage dropped to a level where the reporting IP is the same as the host IP

B. The original rule did not trigger within five minutes

C. Within five minutes, the packet loss percentage dropped to a level where the reporting IP is same as the source IP

D. Within five minutes, the packet loss percentage dropped to a level where the host IP of the original rule matches the host IP of the clear condition pattern

Answer: D

5.Which are key considerations when installing FortiSIEM agents on diverse operating systems?

A. Verifying proper communication between the agent and the collector.

B. Ensuring ample storage space on the device.

C. Checking system compatibility and prerequisites.

D. Validating the latest version of the web browser.

Answer: AC