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 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.

QUESTION 2

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

A. Rule based

B. Notification based

C. App Push

D. Policy based

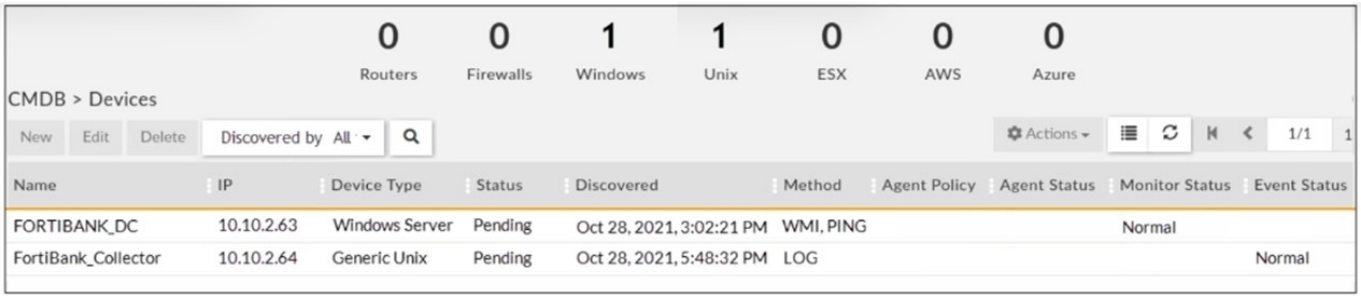
E. Schedule based

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 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

Which syntax will register a collector to the supervisor?

A. phProvisionCollector --add

B. phProvisionCollector --add

C. phProvisionCollector --add

D. phProvisionCollector --add

Correct Answer: B

Explanation: The syntax that will register a collector to the supervisor is phProvisionCollector --add . This command will initiate the registration process between the collector and the supervisor, and exchange certificates and configuration information. The parameter is the IP address of the supervisor node.

QUESTION 5

Which statement about EPS bursting is true?

A. FortiSIEM will let you burst up to five times the licensed EPS once during a 24-hour period.

B. FortiSIEM must be provisioned with ten percent the licensed EPS to handle potential event surges.

C. FortiSIEM will let you burst up to five times the licensed EPS at any given time, provided it has accumulated enough unused EPS.

D. FortiSIEM will let you burst up to five times the licensed EPS at any given time, regardless of unused of EPS.

Correct Answer: C

Explanation: FortiSIEM allows EPS bursting to handle event spikes without dropping events or violating the license agreement. EPS bursting means that FortiSIEM will let you burst up to five times the licensed EPS at any given time, provided it has accumulated enough unused EPS from previous time intervals.