NSE7_ADA-6.3$^{\text{Q\&As}}$

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:

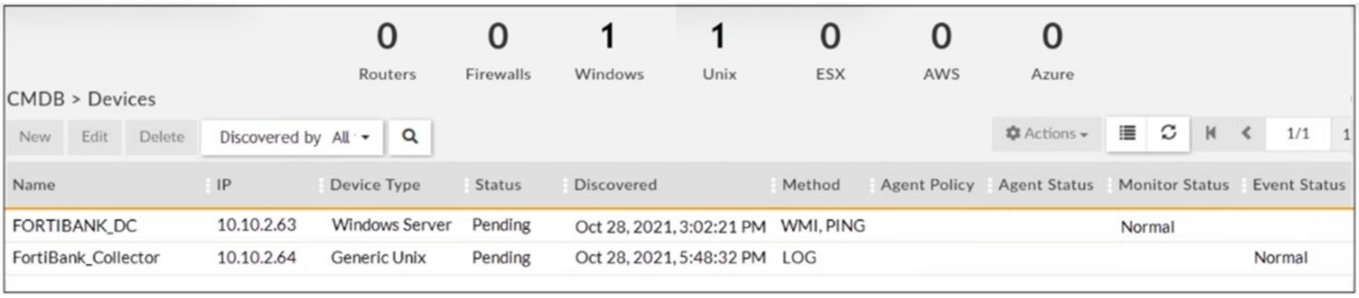
https://www.pass4itsure.com/nse7_ada-6-3.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Refer to the exhibit.



Name	IP	Device Type	Status	Discovered	Method	Agent Policy	Agent Status	Monitor Status	Event Status
FORTIBANK_DC	10.10.2.63	Windows Server	Pending	Oct 28, 2021, 3:02:21 PM	WMI, PING			Normal	
FortiBank_Collector	10.10.2.64	Generic Unix	Pending	Oct 28, 2021, 5:48:32 PM	LOG				Normal

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

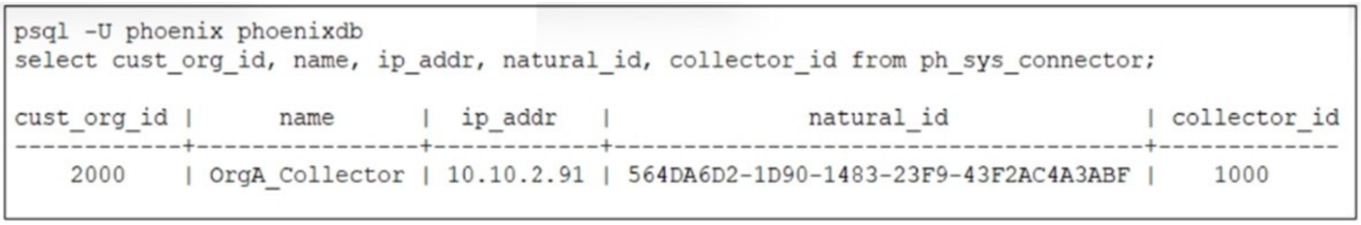
D. The device must be deleted manually from the CMDB

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 2

Refer to the exhibit.



```
psql -U phoenix phoenixdb
select cust_org_id, name, ip_addr, natural_id, collector_id from ph_sys_connector;

cust_org_id |       name       |  ip_addr    |              natural_id              | collector_id
------------+------------------+-------------+--------------------------------------+-------------
    2000    | OrgA_Collector   | 10.10.2.91  | 564DA6D2-1D90-1483-23F9-43F2AC4A3ABF |     1000
```

The exhibit shows the output of an SQL command that an administrator ran to view the natural_id value, after logging into the Postgres database. What does the natural_id value identify?

A. The supervisor

B. The worker

C. An agent

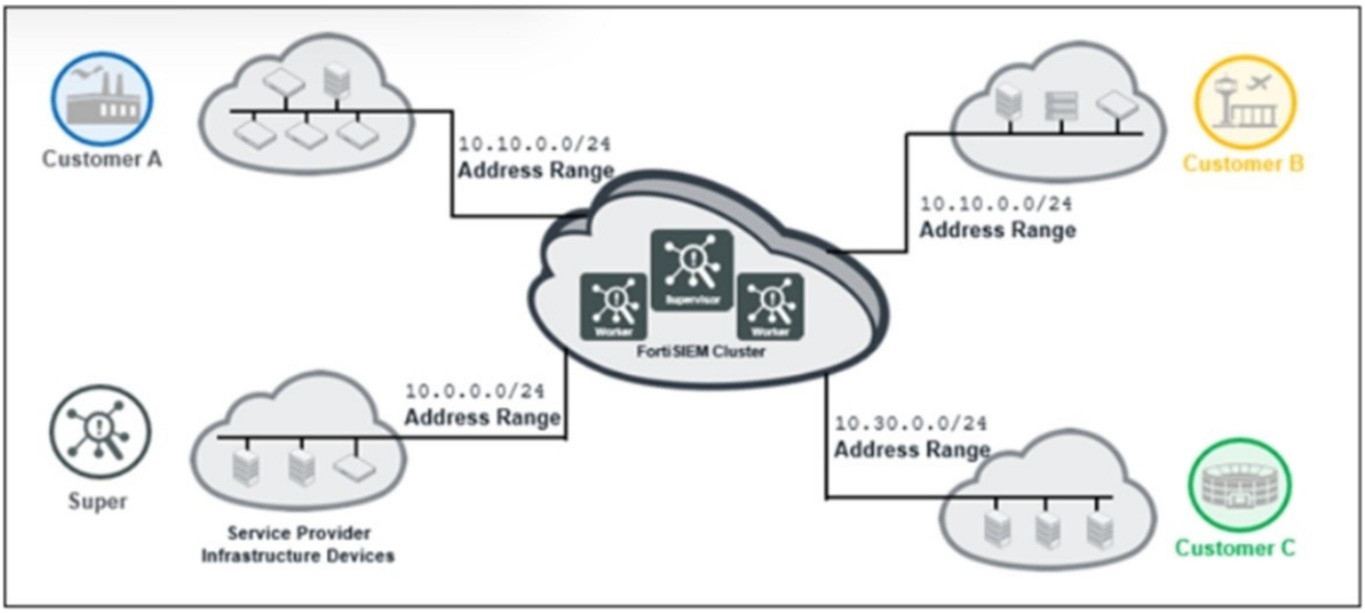
D. The collector

Correct Answer: D

Explanation: The natural_id value identifies the collector in the FortiSIEM system. The natural_id is a unique identifier that is assigned to each collector during the registration process with the supervisor. The natural_id is used to associate events and performance data with the collector that collected them.

QUESTION 3

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.

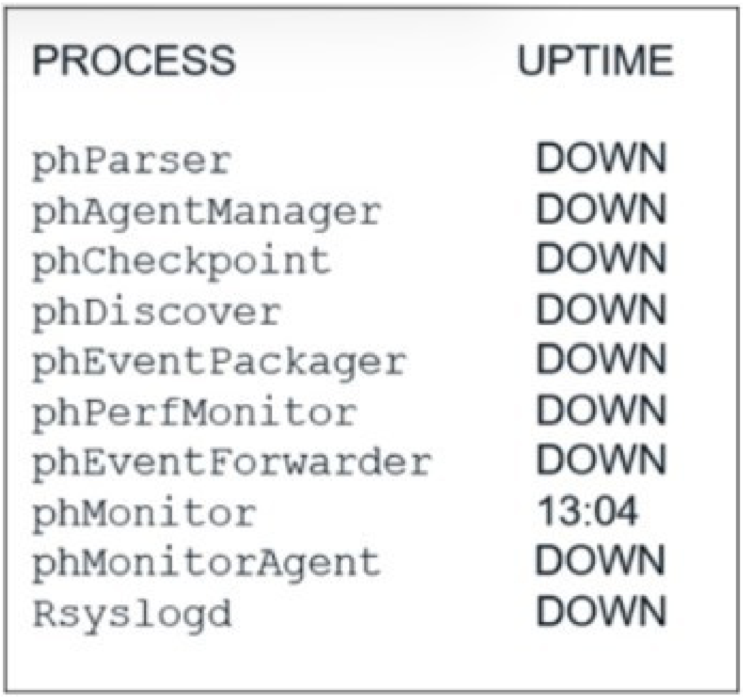
D. At least one collector must be deployed to collect logs from service provider infrastructure devices.

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.

QUESTION 4

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.

Correct Answer: C

Explanation: The collector processes are dependent on the registration with the supervisor. The phMonitor process is responsible for registering the collector to the supervisor and monitoring the health of other processes. After the registration is successful, the phMonitor will start the other processes on the collector.

QUESTION 5

From where does the rule engine load the baseline data values?

A. The profile report

B. The daily database

C. The profile database

D. The memory

Correct Answer: C

Explanation: The rule engine loads the baseline data values from the profile database. The profile database contains historical data that is used for baselining calculations, such as minimum, maximum, average, standard deviation, and percentile values for various metrics.