Free Questions for NSE7_ADA-6.3 by certsdeals

Shared by Bright on 25-07-2023

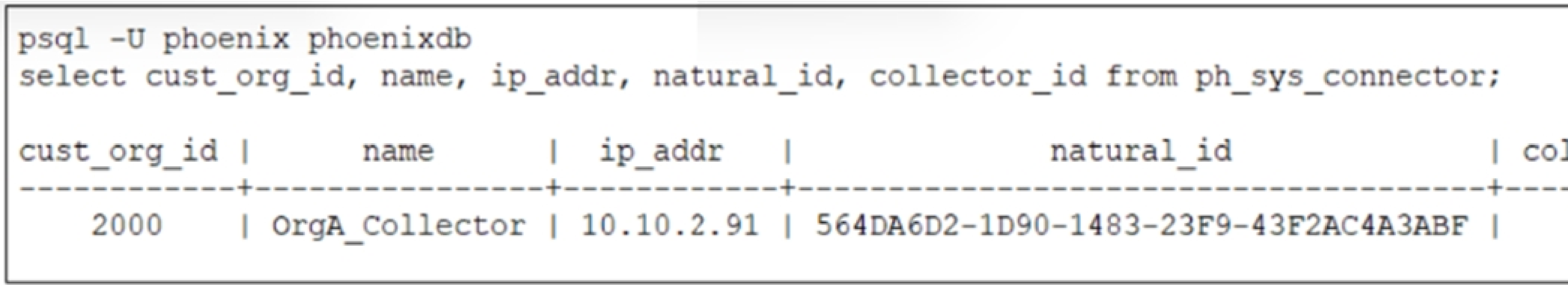
For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: **MultipleChoice**

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                | col
------------+------------------+-------------+------------------------------------------+----
    2000    | OrgA_Collector | 10.10.2.91 | 564DA6D2-1D90-1483-23F9-43F2AC4A3ABF |
```

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?

Options:

A- The supervisor

B- The worker

C- An agent

D- The collector

Answer:

D

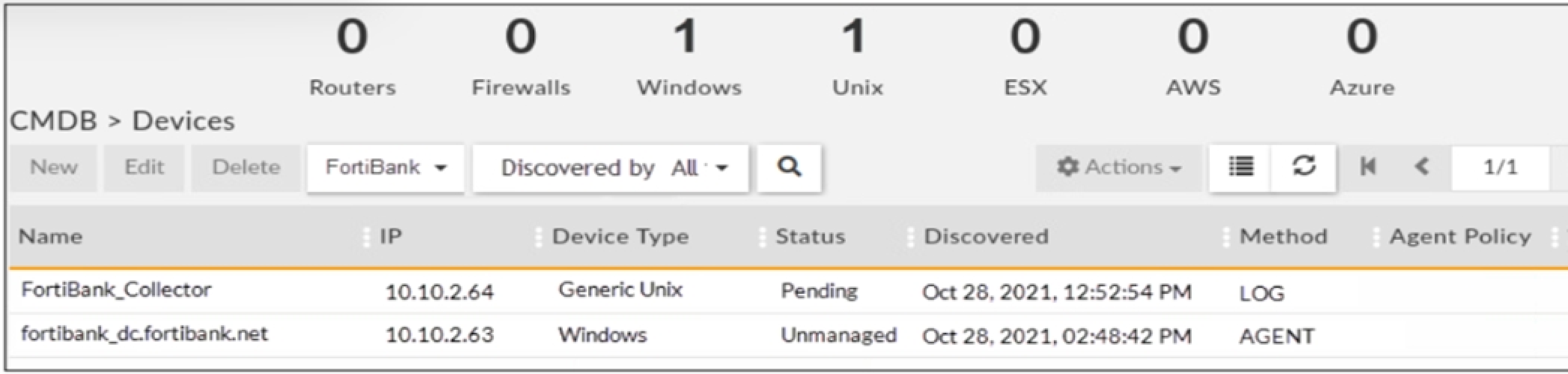
Explanation:

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 2

Question Type: MultipleChoice

Refer to the exhibit.



Name	IP	Device Type	Status	Discovered	Method	Agent Policy
FortiBank_Collector	10.10.2.64	Generic Unix	Pending	Oct 28, 2021, 12:52:54 PM	LOG	
fortibank_dc.fortibank.net	10.10.2.63	Windows	Unmanaged	Oct 28, 2021, 02:48:42 PM	AGENT	

Is the Windows agent delivering event logs correctly?

Options:

A- The logs are buffered by the agent and will be sent once the status changes to managed.

B- The agent is registered and it is sending logs correctly.

C- The agent is not sending logs because it did not receive a monitoring template.

D- Because the agent is unmanaged. the logs are dropped silently by the supervisor.

Answer:

D

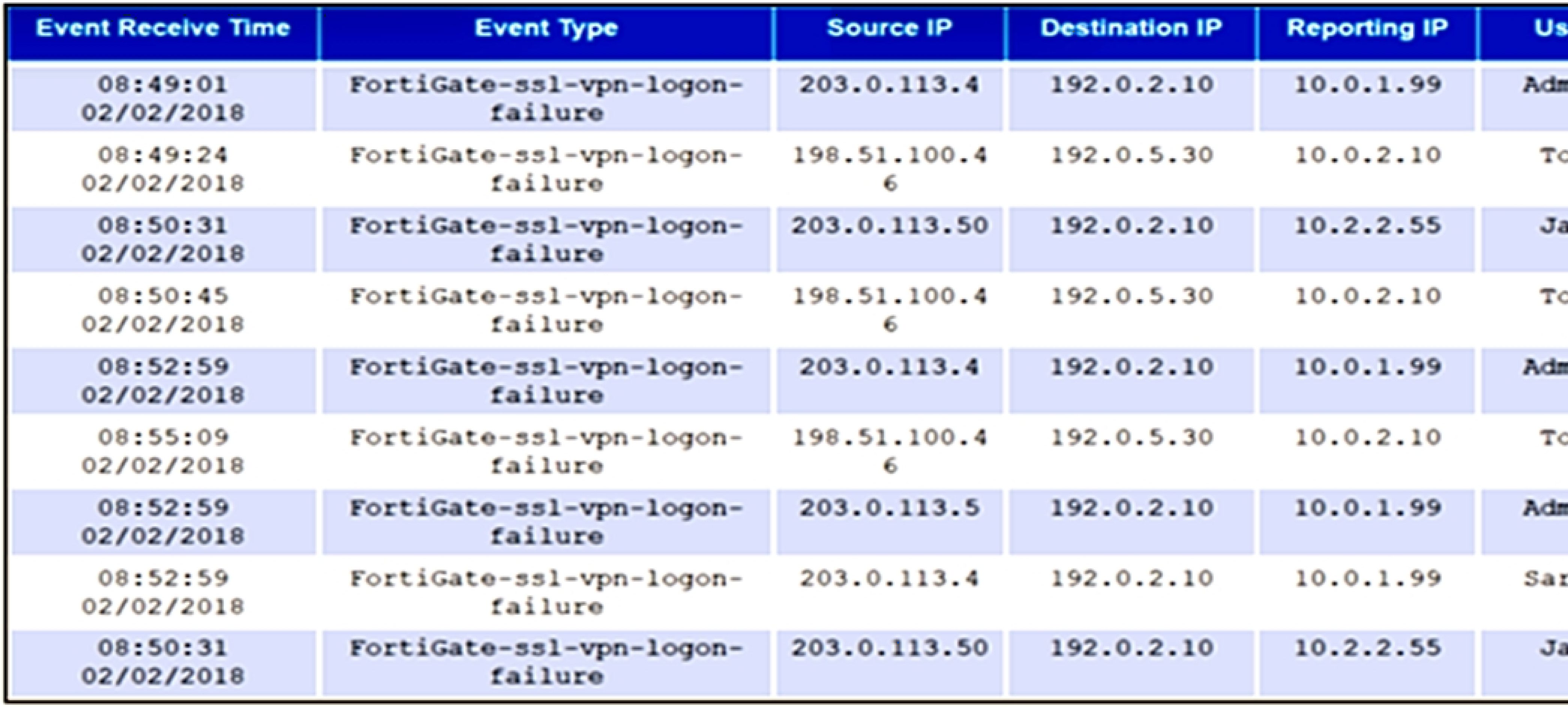
Explanation:

The windows agent is not delivering event logs correctly because the agent is unmanaged, meaning it is not assigned to any organization or customer. The supervisor will drop the logs silently from unmanaged agents, as they are not associated with any valid license or CMDB.

Question 3

Question Type: **MultipleChoice**

Refer to the exhibit.



Event Receive Time	Event Type	Source IP	Destination IP	Reporting IP	Us
08:49:01 02/02/2018	FortiGate-ssl-vpn-logon-failure	203.0.113.4	192.0.2.10	10.0.1.99	Adm
08:49:24 02/02/2018	FortiGate-ssl-vpn-logon-failure	198.51.100.46	192.0.5.30	10.0.2.10	To
08:50:31 02/02/2018	FortiGate-ssl-vpn-logon-failure	203.0.113.50	192.0.2.10	10.2.2.55	Ja
08:50:45 02/02/2018	FortiGate-ssl-vpn-logon-failure	198.51.100.46	192.0.5.30	10.0.2.10	To
08:52:59 02/02/2018	FortiGate-ssl-vpn-logon-failure	203.0.113.4	192.0.2.10	10.0.1.99	Adm
08:55:09 02/02/2018	FortiGate-ssl-vpn-logon-failure	198.51.100.46	192.0.5.30	10.0.2.10	To
08:52:59 02/02/2018	FortiGate-ssl-vpn-logon-failure	203.0.113.5	192.0.2.10	10.0.1.99	Adm
08:52:59 02/02/2018	FortiGate-ssl-vpn-logon-failure	203.0.113.4	192.0.2.10	10.0.1.99	Sar
08:50:31 02/02/2018	FortiGate-ssl-vpn-logon-failure	203.0.113.50	192.0.2.10	10.2.2.55	Ja

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?

Options:

A- Sarah

B- Jan

C- Tom

D- Admin

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 4

Question Type: **MultipleChoice**

What happens to UEBA events when a user is off-net?

Options:

A- The agent will upload the events to the Worker if it cannot upload them to a FortiSIEM collector

B- The agent will cache events locally if it cannot upload them to a FortiSIEM collector

C- The agent will upload the events to the Supervisor if it cannot upload them to a FortiSIEM collector

D- The agent will drop the events if it cannot upload them to a FortiSIEM collector

Answer:

B

Explanation:

When a user is off-net, meaning they are not connected to a network where a FortiSIEM collector is reachable, then UEBA events will be cached locally by the agent if it cannot upload them to a FortiSIEM collector. The agent will store up to 100 MB of events in a local database file and try to upload them when it detects a network change or every five minutes.

Question 5

Question Type: **MultipleChoice**

Which three statements about collector communication with the FortiSIEM cluster are true? (Choose three.)

Options:

A- The only communication between the collector and the supervisor is during the registration process.

B- Collectors communicate periodically with the supervisor node.

C- The supervisor periodically checks the health of the collector.

D- The supervisor does not initiate any connections to the collector node.

E- Collectors upload event data to any node in the worker upload list, but report their health directly to the supervisor node.

Answer:

B, C, E

Explanation:

The statements about collector communication with the FortiSIEM cluster that are true are:

Collectors communicate periodically with the supervisor node. Collectors send heartbeat messages to the supervisor every 30 seconds to report their status and configuration.

The supervisor periodically checks the health of the collector. The supervisor monitors the heartbeat messages from collectors and alerts if there is any issue with their connectivity or performance.

Collectors upload event data to any node in the worker upload list, but report their health directly to the supervisor node. Collectors use a round-robin algorithm to distribute event data among worker nodes in the worker upload list, which is provided by the supervisor during registration. However, collectors only report their health and status to the supervisor node.

Question 6

Question Type: **MultipleChoice**

Which three statements about collector communication with the FortiSIEM cluster are true? (Choose three.)

Options:

A- The only communication between the collector and the supervisor is during the registration process.

B- Collectors communicate periodically with the supervisor node.

C- The supervisor periodically checks the health of the collector.

D- The supervisor does not initiate any connections to the collector node.

E- Collectors upload event data to any node in the worker upload list, but report their health directly to the supervisor node.

Answer:

B, C, E

Explanation:

The statements about collector communication with the FortiSIEM cluster that are true are:

Collectors communicate periodically with the supervisor node. Collectors send heartbeat messages to the supervisor every 30 seconds to report their status and configuration.

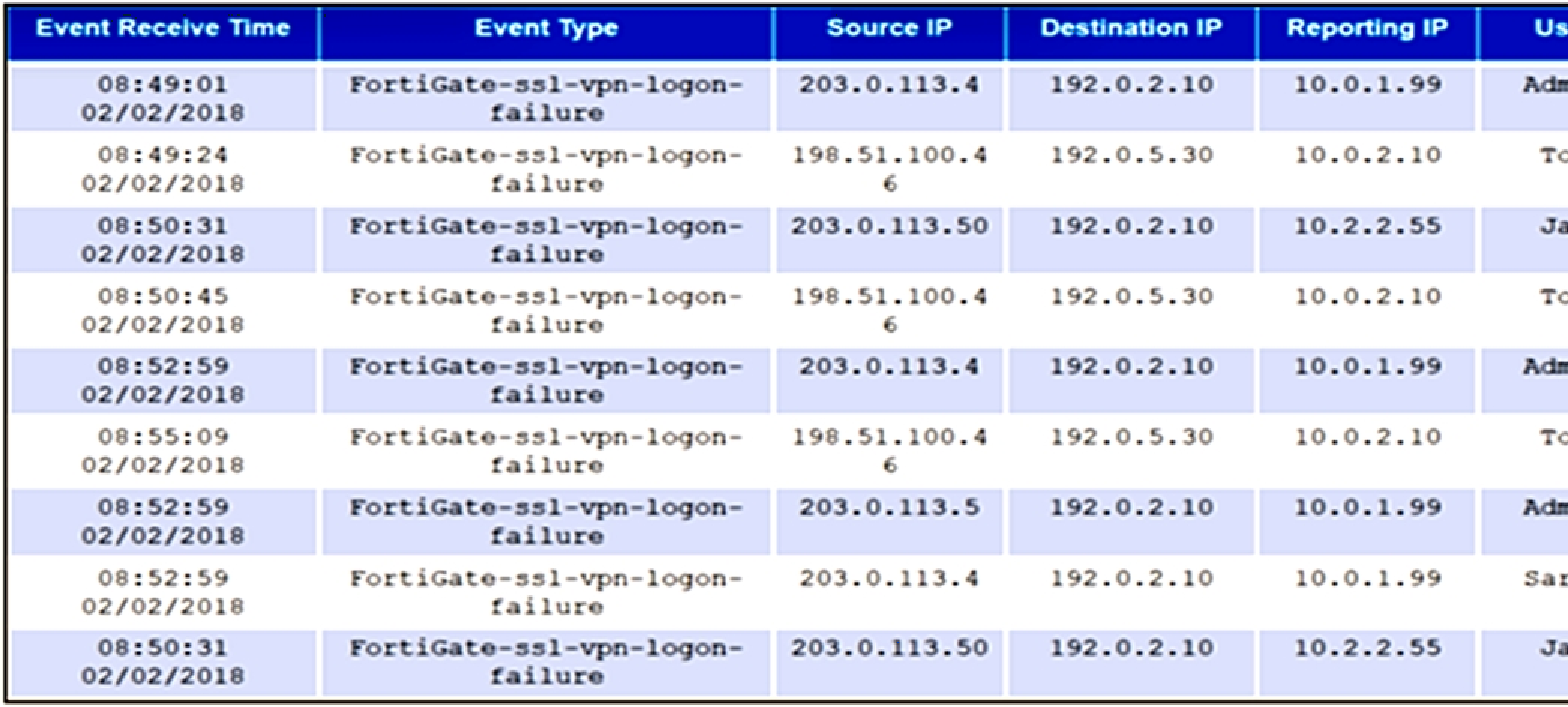
The supervisor periodically checks the health of the collector. The supervisor monitors the heartbeat messages from collectors and alerts if there is any issue with their connectivity or performance.

Collectors upload event data to any node in the worker upload list, but report their health directly to the supervisor node. Collectors use a round-robin algorithm to distribute event data among worker nodes in the worker upload list, which is provided by the supervisor during registration. However, collectors only report their health and status to the supervisor node.

Question 7

Question Type: MultipleChoice

Refer to the exhibit.



Event Receive Time	Event Type	Source IP	Destination IP	Reporting IP	Us
08:49:01 02/02/2018	FortiGate-ssl-vpn-logon-failure	203.0.113.4	192.0.2.10	10.0.1.99	Adm
08:49:24 02/02/2018	FortiGate-ssl-vpn-logon-failure	198.51.100.46	192.0.5.30	10.0.2.10	To
08:50:31 02/02/2018	FortiGate-ssl-vpn-logon-failure	203.0.113.50	192.0.2.10	10.2.2.55	Ja
08:50:45 02/02/2018	FortiGate-ssl-vpn-logon-failure	198.51.100.46	192.0.5.30	10.0.2.10	To
08:52:59 02/02/2018	FortiGate-ssl-vpn-logon-failure	203.0.113.4	192.0.2.10	10.0.1.99	Adm
08:55:09 02/02/2018	FortiGate-ssl-vpn-logon-failure	198.51.100.46	192.0.5.30	10.0.2.10	To
08:52:59 02/02/2018	FortiGate-ssl-vpn-logon-failure	203.0.113.5	192.0.2.10	10.0.1.99	Adm
08:52:59 02/02/2018	FortiGate-ssl-vpn-logon-failure	203.0.113.4	192.0.2.10	10.0.1.99	Sar
08:50:31 02/02/2018	FortiGate-ssl-vpn-logon-failure	203.0.113.50	192.0.2.10	10.2.2.55	Ja

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?

Options:

A- Sarah

B- Jan

C- Tom

D- Admin

Answer:

C

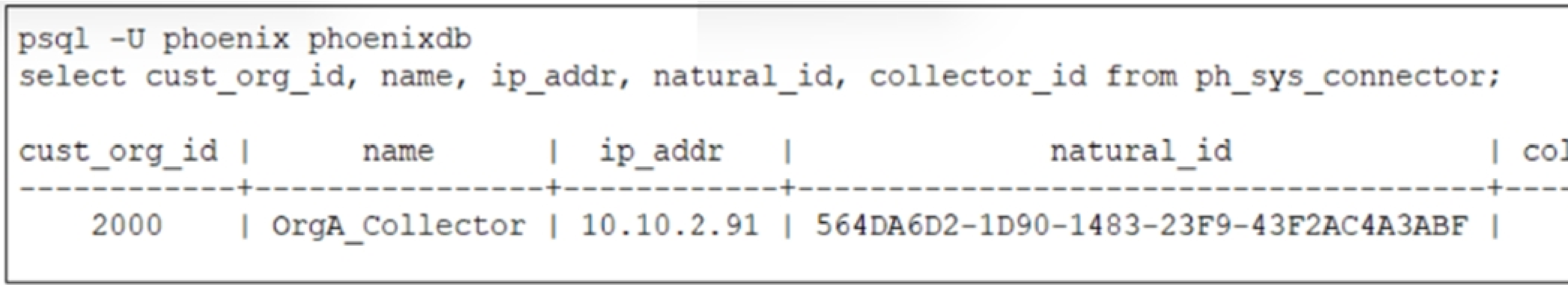
Explanation:

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 8

Question Type: **MultipleChoice**

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               | col
------------+------------------+-------------+---------------------------------------+----
    2000    | OrgA_Collector | 10.10.2.91 | 564DA6D2-1D90-1483-23F9-43F2AC4A3ABF |
```

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?

Options:

A- The supervisor

B- The worker

C- An agent

D- The collector

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 9

Question Type: MultipleChoice

What happens to UEBA events when a user is off-net?

Options:

A- The agent will upload the events to the Worker if it cannot upload them to a FortiSIEM collector

B- The agent will cache events locally if it cannot upload them to a FortiSIEM collector

C- The agent will upload the events to the Supervisor if it cannot upload them to a FortiSIEM collector

D- The agent will drop the events if it cannot upload them to a FortiSIEM collector

Answer:

B

Explanation:

When a user is off-net, meaning they are not connected to a network where a FortiSIEM collector is reachable, then UEBA events will be cached locally by the agent if it cannot upload them to a FortiSIEM collector. The agent will store up to 100 MB of events in a local database file and try to upload them when it detects a network change or every five minutes.

20%
DISCOUNT