Vendor: Fortinet

Exam Code: NSE7_ADA-6.3

Exam Name: Fortinet NSE 7 - Advanced Analytics 6.3

Version: DEMO

QUESTION 1
Refer to the exhibit. An administrator deploys a new collector for the first time, and notices that all the processes except the phMonitor are down.

PROCESS	UPTIME
phParser	DOWN
phAgentManager	DOWN
phCheckpoint	DOWN
phDiscover	DOWN
phEventPackager	DOWN
phPerfMonitor	DOWN
phEventForwarder	DOWN
phMonitor	13:04
phMonitorAgent	DOWN
Rsyslogd	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
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 2
Which two statements about the maximum device limit on FortiSIEM are true? (Choose two.)

A. The device limit is defined per customer and every customer is assigned a fixed number of device limit by the service provider.
B. The device limit is only applicable to enterprise edition.
C. The device limit is based on the license type that was purchased from Fortinet.
D. The device limit is defined for the whole system and is shared by every customer on a service provider edition.

Answer: BC
Explanation:
The device limit is a feature of the enterprise edition of FortiSIEM that restricts the number of

devices that can be added to the system based on the license type. The device limit does not apply to the service provider edition, which allows unlimited devices per customer. The device limit is determined by the license type that was purchased from Fortinet, such as 100 devices, 500 devices, or unlimited devices.

QUESTION 3
What happens to UEBA events when a user is off-net?

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 4
Refer to the exhibit. 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.

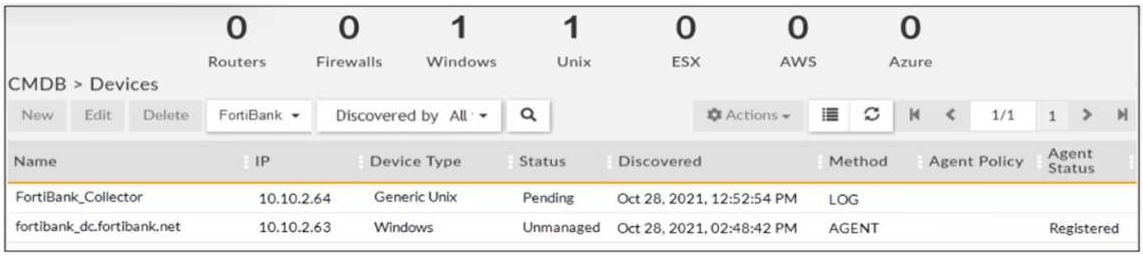
Event Receive Time	Event Type	Source IP	Destination IP	Reporting IP	User	Raw Event Log
08:49:01 02/02/2018	FortiGate-ssl-vpn-logon-failure	203.0.113.4	192.0.2.10	10.0.1.99	Admin	<189>date=2018-02-02…
08:49:24 02/02/2018	FortiGate-ssl-vpn-logon-failure	198.51.100.46	192.0.5.30	10.0.2.10	Tom	<189>date=2018-02-02…
08:50:31 02/02/2018	FortiGate-ssl-vpn-logon-failure	203.0.113.50	192.0.2.10	10.2.2.55	Jan	<189>date=2018-02-02…
08:50:45 02/02/2018	FortiGate-ssl-vpn-logon-failure	198.51.100.46	192.0.5.30	10.0.2.10	Tom	<189>date=2018-02-02…
08:52:59 02/02/2018	FortiGate-ssl-vpn-logon-failure	203.0.113.4	192.0.2.10	10.0.1.99	Admin	<189>date=2018-02-02…
08:55:09 02/02/2018	FortiGate-ssl-vpn-logon-failure	198.51.100.46	192.0.5.30	10.0.2.10	Tom	<189>date=2018-02-02…
08:52:59 02/02/2018	FortiGate-ssl-vpn-logon-failure	203.0.113.5	192.0.2.10	10.0.1.99	Admin	<189>date=2018-02-02…
08:52:59 02/02/2018	FortiGate-ssl-vpn-logon-failure	203.0.113.4	192.0.2.10	10.0.1.99	Sarah	<189>date=2018-02-02…
08:50:31 02/02/2018	FortiGate-ssl-vpn-logon-failure	203.0.113.50	192.0.2.10	10.2.2.55	Jan	<189>date=2018-02-02…

Which user would meet that condition?

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 5
Refer to the exhibit. Is the Windows agent delivering event logs correctly?



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 6
Refer to the exhibit. 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.

```
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
```

What does the natural_id value identify?

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.

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.lead2pass.com/all-products.html

10% Discount Coupon Code: **ASTR14**