NSE7_ADA-6.3 Q&As

Fortinet NSE 7 - Advanced Analytics 6.3

Pass Fortinet NSE7_ADA-6.3 Exam with 100% Guarantee

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

QUESTION 1

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

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.

Correct Answer: BCE

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.

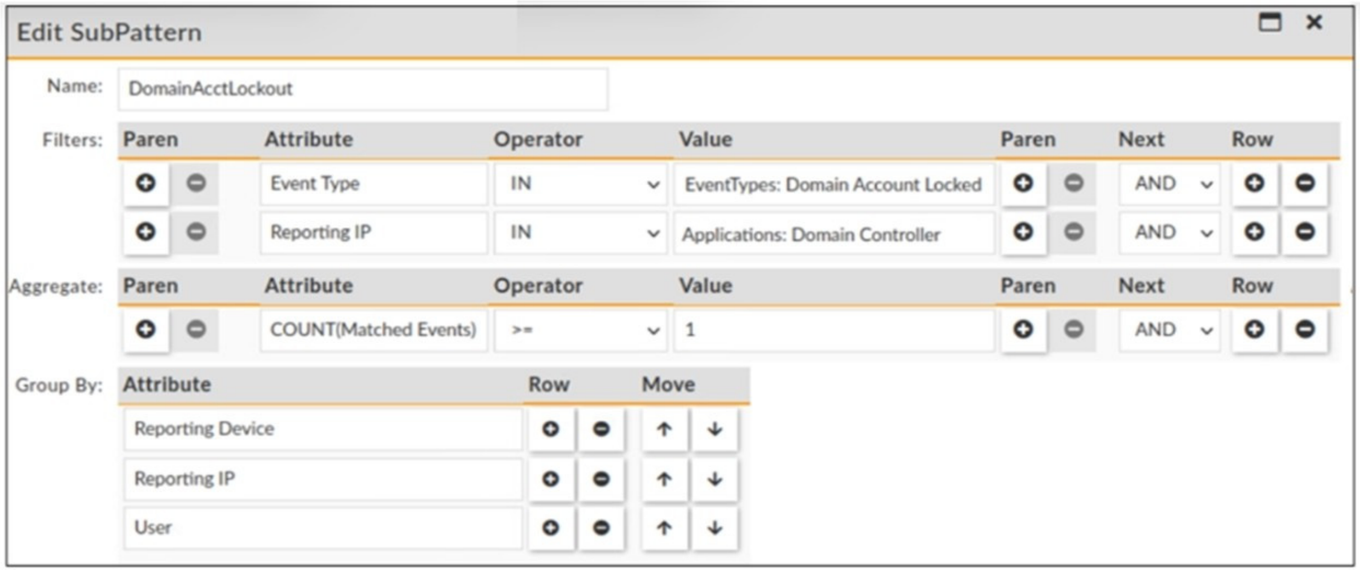
The supervisor periodically checks the health of the collector. The supervisor monitors the heartbeat messages from collectors and alerts if there is any issue with their connectivity or performance.

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 2

Refer to the exhibit.



Edit SubPattern

Name: DomainAcctLockout

Filters:

Paren	Attribute	Operator	Value	Paren	Next	Row
⊕ ⊖	Event Type	IN	EventTypes: Domain Account Locked	⊕ ⊖	AND	⊕ ⊖
⊕ ⊖	Reporting IP	IN	Applications: Domain Controller	⊕ ⊖	AND	⊕ ⊖

Aggregate:

Paren	Attribute	Operator	Value	Paren	Next	Row
⊕ ⊖	COUNT(Matched Events)	>=	1	⊕ ⊖	AND	⊕ ⊖

Group By:

Attribute	Row	Move
Reporting Device	⊕ ⊖	↑ ↓
Reporting IP	⊕ ⊖	↑ ↓
User	⊕ ⊖	↑ ↓

Which statement about the rule filters events shown in the exhibit is true?

A. The rule filters events with an event type that belong to the Domain Account Locked CMDB group or a reporting IP that belong to the Domain Controller applications group.

B. The rule filters events with an event type that belong to the Domain Account Locked CMDB group and a reporting |P that belong to the Domain Controller applications group.

C. The rule filters events with an event type that belong to the Domain Account Locked CMDB group and a user that belongs to the Domain Controller applications group.

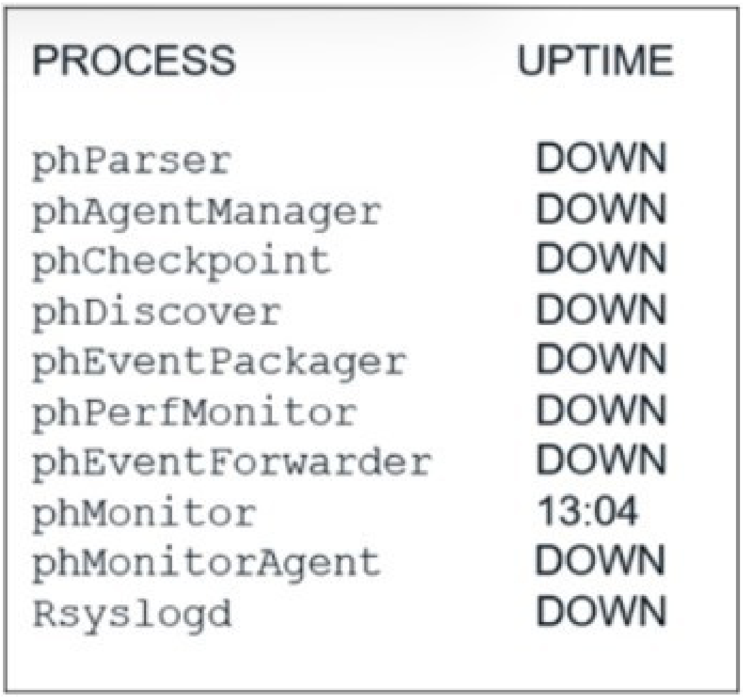
D. The rule filters events with an event type that equals Domain Account Locked and a reporting IP that equals Domain Controller applications.

Correct Answer: B

Explanation: The rule filters events with an event type that belong to the Domain Account Locked CMDB group and a reporting IP that belong to the Domain Controller applications group. This means that only events that have both criteria met will be processed by this rule. The event type and reporting IP are joined by an AND operator, which requires both conditions to be true.

QUESTION 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.

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 4

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

Correct 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

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.