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.leads4pass.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

Why can collectors not be defined before the worker upload address is set on the supervisor?

A. Collectors can only upload data to a worker, and the supervisor is not a worker

B. To ensure that the service provider has deployed at least one worker along with a supervisor

C. Collectors receive the worker upload address during the registration process

D. To ensure that the service provider has deployed a NFS server

Correct Answer: C

Explanation: Collectors cannot be defined before the worker upload address is set on the supervisor because collectors receive the worker upload address during the registration process. The worker upload address is a list of IP addresses of worker nodes that can receive event data from collectors. The supervisor provides this list to collectors when they register with it, so that collectors can upload event data to any node in the list.

QUESTION 2

Which three statements about phRuleMaster are true? (Choose three.)

A. phRuleMaster queues up the data being received from the phRuleWorkers into buckets.

B. phRuleMaster is present on the supervisor and workers.

C. phRuleMaster is present on the supervisor only

D. phRuleMaster wakes up to evaluate all the rule data in series, every 30 seconds.

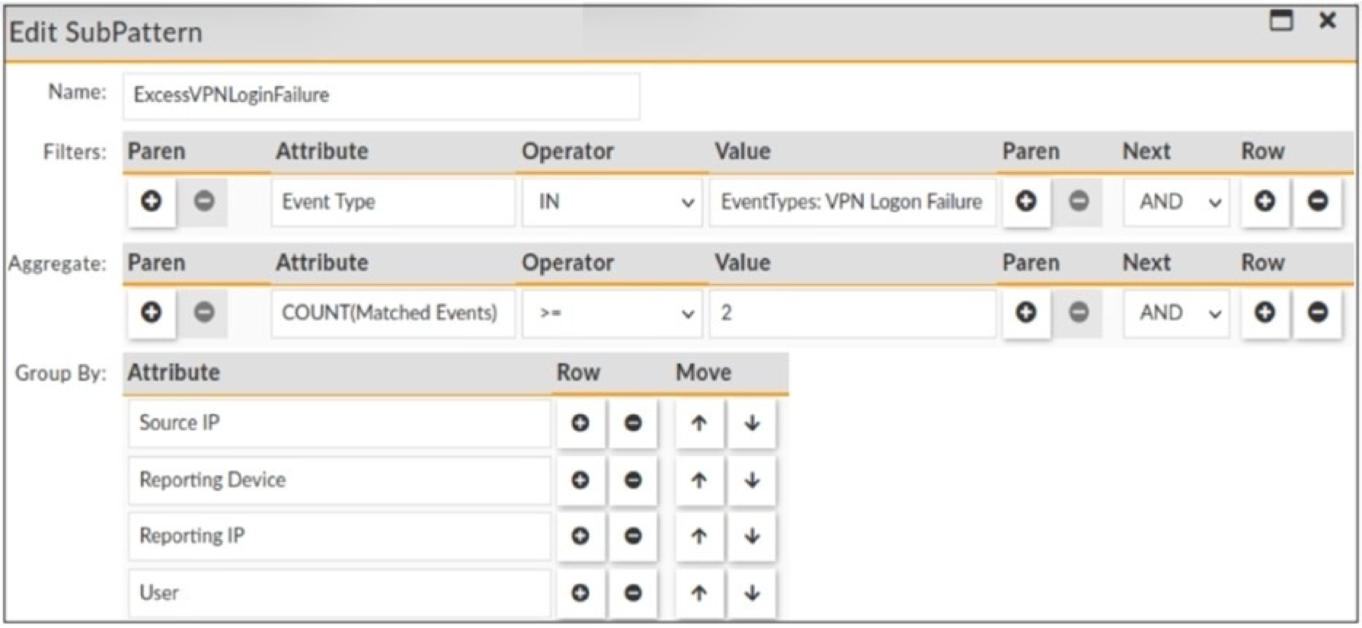
E. phRuleMaster wakes up to evaluate all the rule data in parallel, even/ 30 seconds

Correct Answer: ABE

Explanation: phRuleMaster is a process that performs rule evaluation and incident generation on FortiSIEM. phRuleMaster queues up the data being received from the phRuleWorkers into buckets based on time intervals, such as one minute, five minutes, or ten minutes. phRuleMaster is present on both the supervisor and workers nodes of a FortiSIEM cluster. phRuleMaster wakes up every 30 seconds to evaluate all the rule data in parallel using multiple threads.

QUESTION 3

Refer to the exhibit.



Edit SubPattern

Name: ExcessVPNLoginFailure

Filters:

Paren	Attribute	Operator	Value	Paren	Next	Row
⊕ ⊖	Event Type	IN	EventTypes: VPN Logon Failure	⊕ ⊖	AND	⊕ ⊖

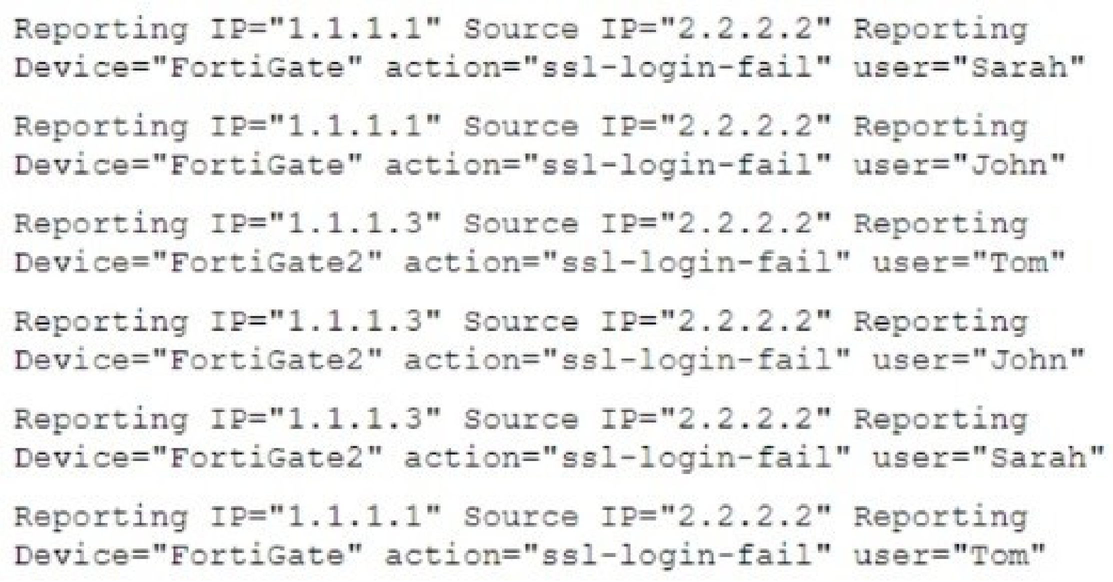
Aggregate:

Paren	Attribute	Operator	Value	Paren	Next	Row
⊕ ⊖	COUNT(Matched Events)	>=	2	⊕ ⊖	AND	⊕ ⊖

Group By:

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

The rule evaluates multiple VPN logon failures within a ten-minute window. Consider the following VPN failure events received within a ten-minute window:



```
Reporting IP="1.1.1.1" Source IP="2.2.2.2" Reporting
Device="FortiGate" action="ssl-login-fail" user="Sarah"

Reporting IP="1.1.1.1" Source IP="2.2.2.2" Reporting
Device="FortiGate" action="ssl-login-fail" user="John"

Reporting IP="1.1.1.3" Source IP="2.2.2.2" Reporting
Device="FortiGate2" action="ssl-login-fail" user="Tom"

Reporting IP="1.1.1.3" Source IP="2.2.2.2" Reporting
Device="FortiGate2" action="ssl-login-fail" user="John"

Reporting IP="1.1.1.3" Source IP="2.2.2.2" Reporting
Device="FortiGate2" action="ssl-login-fail" user="Sarah"

Reporting IP="1.1.1.1" Source IP="2.2.2.2" Reporting
Device="FortiGate" action="ssl-login-fail" user="Tom"
```

How many incidents are generated?

A. 1

B. 2

C. 0

D. 3

Correct Answer: B

Explanation: The rule evaluates multiple VPN logon failures within a ten-minute window. The rule will generate an incident if there are more than three VPN logon failures from the same source IP address within a ten-minute window.

Based

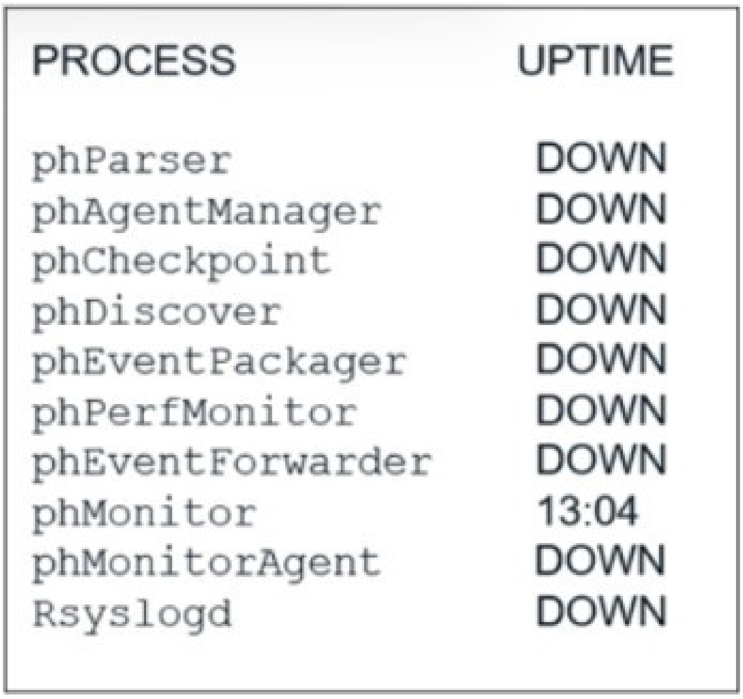
on the VPN failure events received within a ten-minute window, there are two incidents generated:

One incident for source IP address 10.10.10.10, which has four VPN logon failures at 09:01, 09:02, 09:03, and 09:04.

One incident for source IP address 10.10.10.11, which has four VPN logon failures at 09:06, 09:07, 09:08, and 09:09.

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.

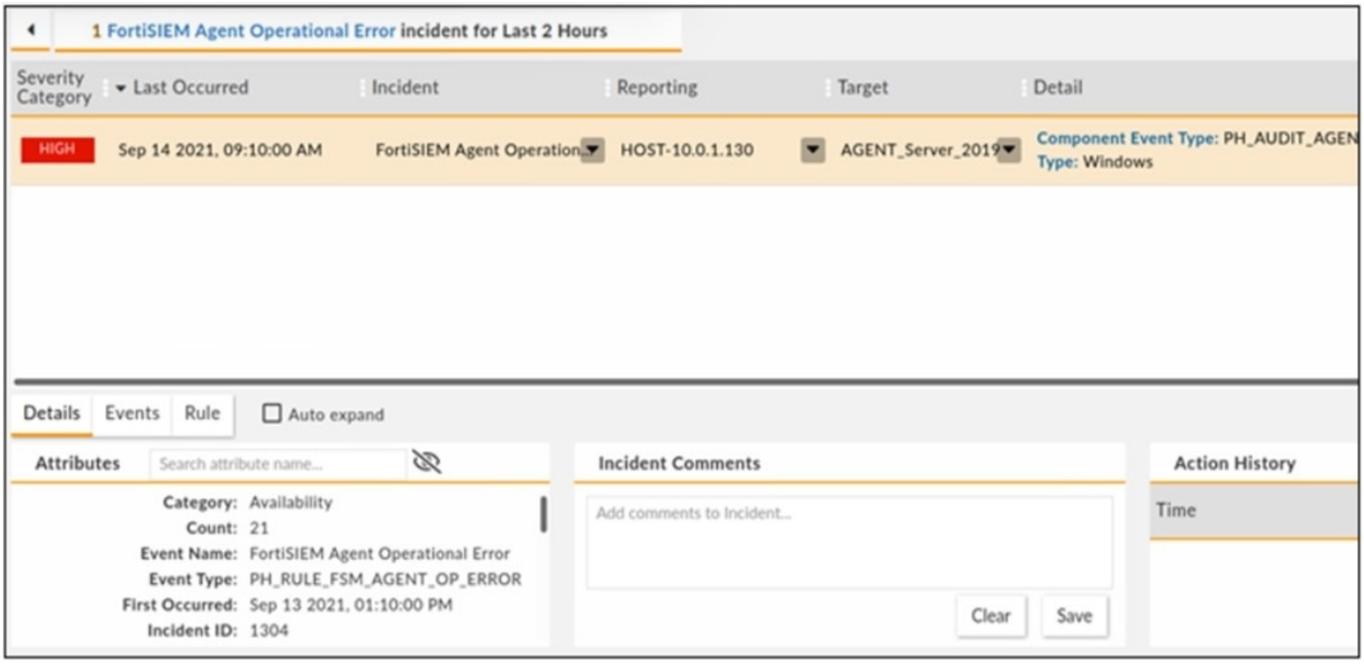
D. The collector was not deployed properly and must be redeployed.

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

Refer to the exhibit.



1 FortiSIEM Agent Operational Error incident for Last 2 Hours

Severity Category	Last Occurred	Incident	Reporting	Target	Detail
HIGH	Sep 14 2021, 09:10:00 AM	FortiSIEM Agent Operation	HOST-10.0.1.130	AGENT_Server_2019	Component Event Type: PH_AUDIT_AGEN Type: Windows

Category: Availability
Count: 21
Event Name: FortiSIEM Agent Operational Error
Event Type: PH_RULE_FSM_AGENT_OP_ERROR
First Occurred: Sep 13 2021, 01:10:00 PM
Incident ID: 1304

How long has the UEBA agent been operationally down?

A. 21 Hours

B. 9 Hours

C. 20 Hours

D. 2 Hours

Correct Answer: A

Explanation: The UEBA agent status shows that it has been operationally down for one day and three hours ago (1d3h). This means that it has been down for 24 hours plus three hours, which is equal to 21 hours.

NSE7_ADA-6.3 VCE Dumps

NSE7_ADA-6.3 Study Guide

NSE7_ADA-6.3 Braindumps