Number: NSE7_ADA-6.3
Passing Score: 800
Time Limit: 120 min
File Version: 3.0

Exam Code: NSE7_ADA-6.3

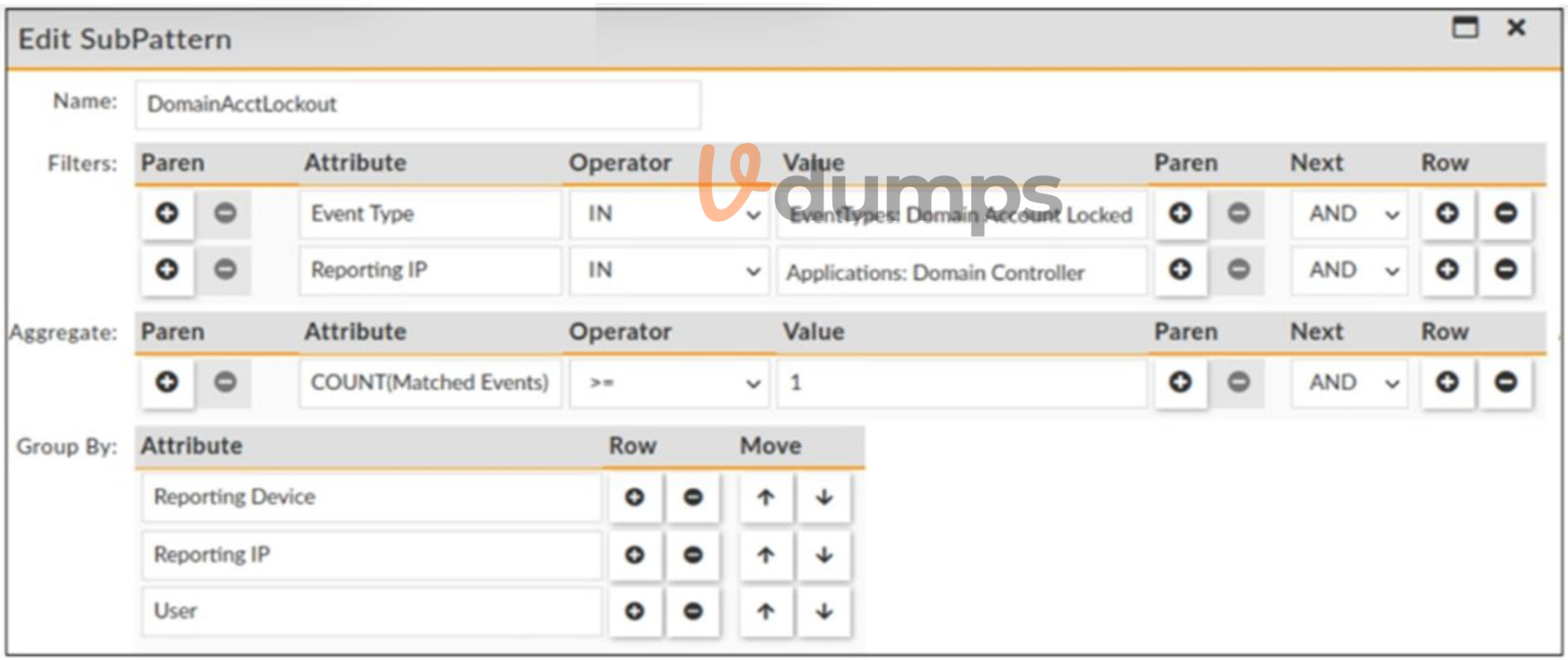
Exam Name: Fortinet NSE 7 - Advanced Analytics 6.3

Exam A

QUESTION 1
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.

Correct Answer: B, C
Section:
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 2
Refer to the exhibit.

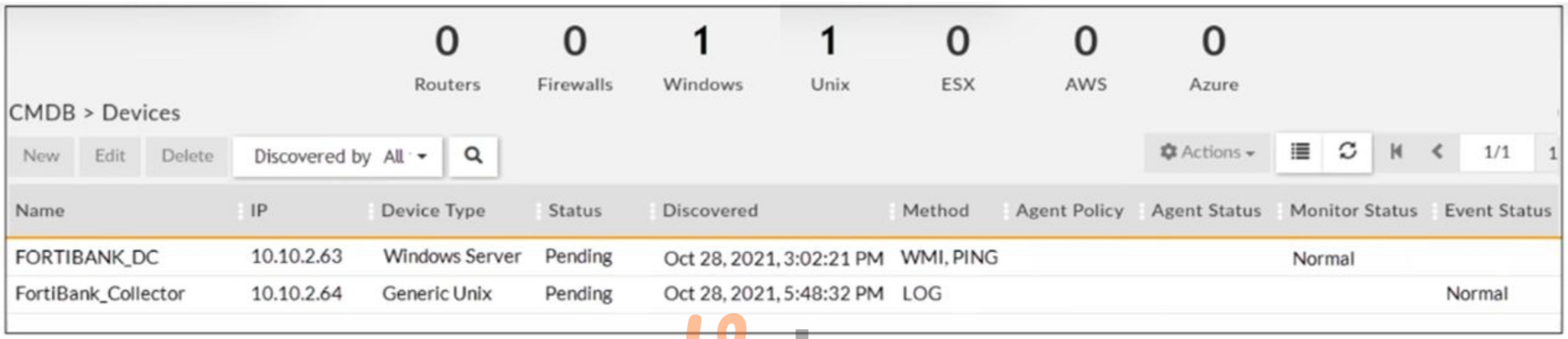


Which statement about the rule filters events shown in the exhibit is true?
A. The rule filters events with an event type that belong to the Domain Account Locked CMDB group or a reporting IP that belong to the Domain Controller applications group.
B. The rule filters events with an event type that belong 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
Section:
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.



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
Section:
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 4
Which syntax will register a collector to the supervisor?
A. phProvisionCollector --add
B. phProvisionCollector --add
C. phProvisionCollector --add
D. phProvisionCollector --add

Correct Answer: B
Section:
Explanation:
The syntax that will register a collector to the supervisor is phProvisionCollector --add <supervisor IP>. This command will initiate the registration process between the collector and the supervisor, and exchange certificates and configuration information. The <supervisor IP> parameter is the IP address of the supervisor node.

QUESTION 5
What is Tactic in the MITRE ATT&CK framework?
A. Tactic is how an attacker plans to execute the attack
B. Tactic is what an attacker hopes to achieve
C. Tactic is the tool that the attacker uses to compromise a system
D. Tactic is a specific implementation of the technique

Correct Answer: B
Section:
Explanation:
Tactic is what an attacker hopes to achieve in the MITRE ATT&CK framework. Tactic is a high-level category of adversary behavior that describes their objective or goal. For example, some tactics are Initial Access, Persistence, Lateral Movement, Exfiltration, etc. Each tactic consists of one or more techniques that describe how an attacker can accomplish that tactic.

QUESTION 6
Identify the processes associated with Machine Learning/AI on FortiSIEM. (Choose two.)
A. phFortiInsightAI
B. phReportMaster
C. phRuleMaster
D. phAnomaly
E. phRuleWorker

Correct Answer: A, D
Section:
Explanation:
The processes associated with Machine Learning/AI on FortiSIEM are phFortiInsightAI and phAnomaly. phFortiInsightAI is responsible for detecting anomalous user behavior using UEBA (User and Entity Behavior Analytics) techniques. phAnomaly is responsible for detecting anomalous network behavior using NTA (Network Traffic Analysis) techniques.

QUESTION 7
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: A, B, E
Section:
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 8
Which three processes are collector processes? (Choose three.)
A. phAgentManaqer
B. phParser
C. phRuleMaster
D. phReportM aster
E. phMonitorAgent

Correct Answer: B, C, E

Section:
Explanation:
The collector processes are responsible for receiving, parsing, normalizing, correlating, and monitoring events from various sources. The collector processes are phParser, phRuleMaster, and phMonitorAgent.

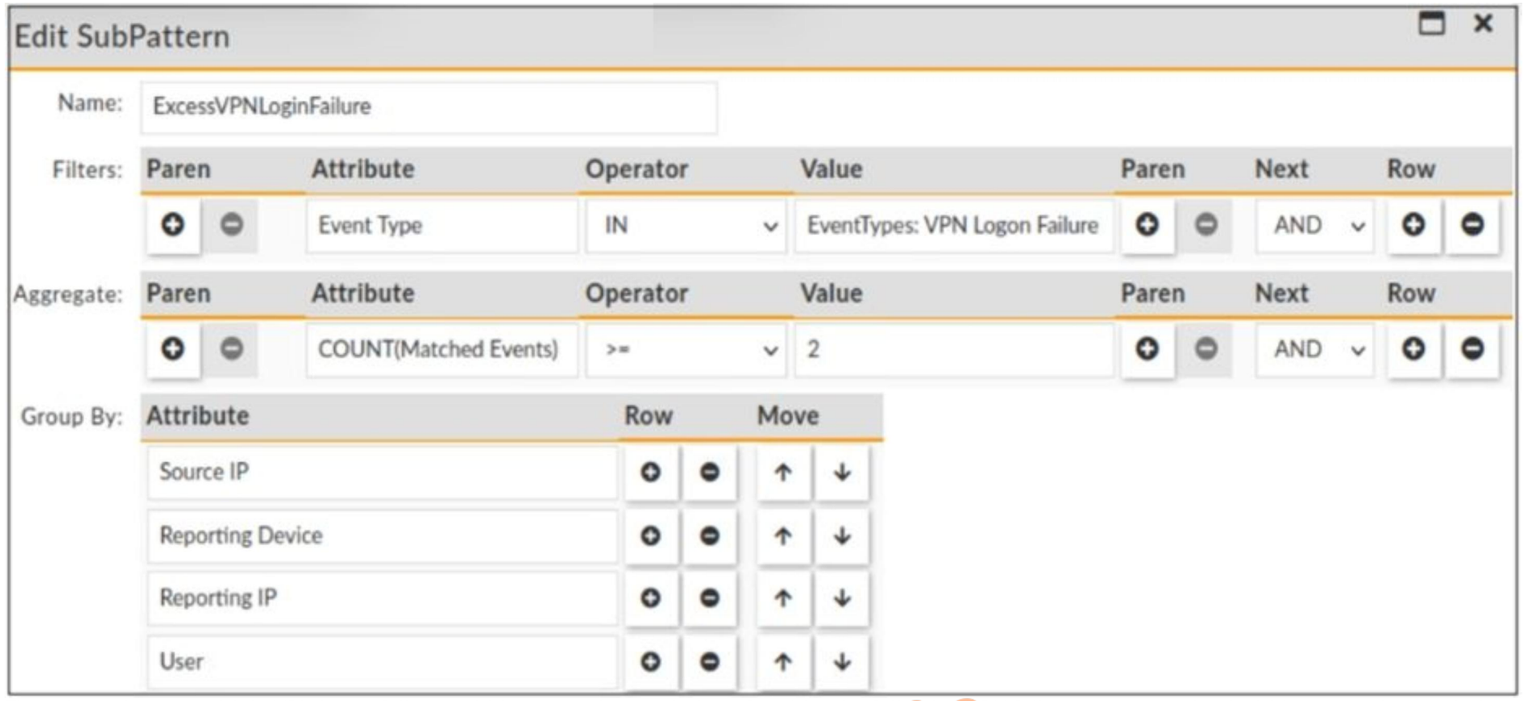
QUESTION 9
Which statement about EPS bursting is true?
A. FortiSIEM will let you burst up to five times the licensed EPS once during a 24-hour period.
B. FortiSIEM must be provisioned with ten percent the licensed EPS to handle potential event surges.
C. FortiSIEM will let you burst up to five times 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
Section:
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.

QUESTION 10
On which disk are the SQLite databases that are used for the baselining stored?
A. Disk1
B. Disk4
C. Disk2
D. Disk3

Correct Answer: D
Section:
Explanation:
The SQLite databases that are used for the baselining are stored on Disk3 of the FortiSIEM server. Disk3 is also used for storing raw event data and CMDB data.

QUESTION 11
Refer to the exhibit.



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"
```

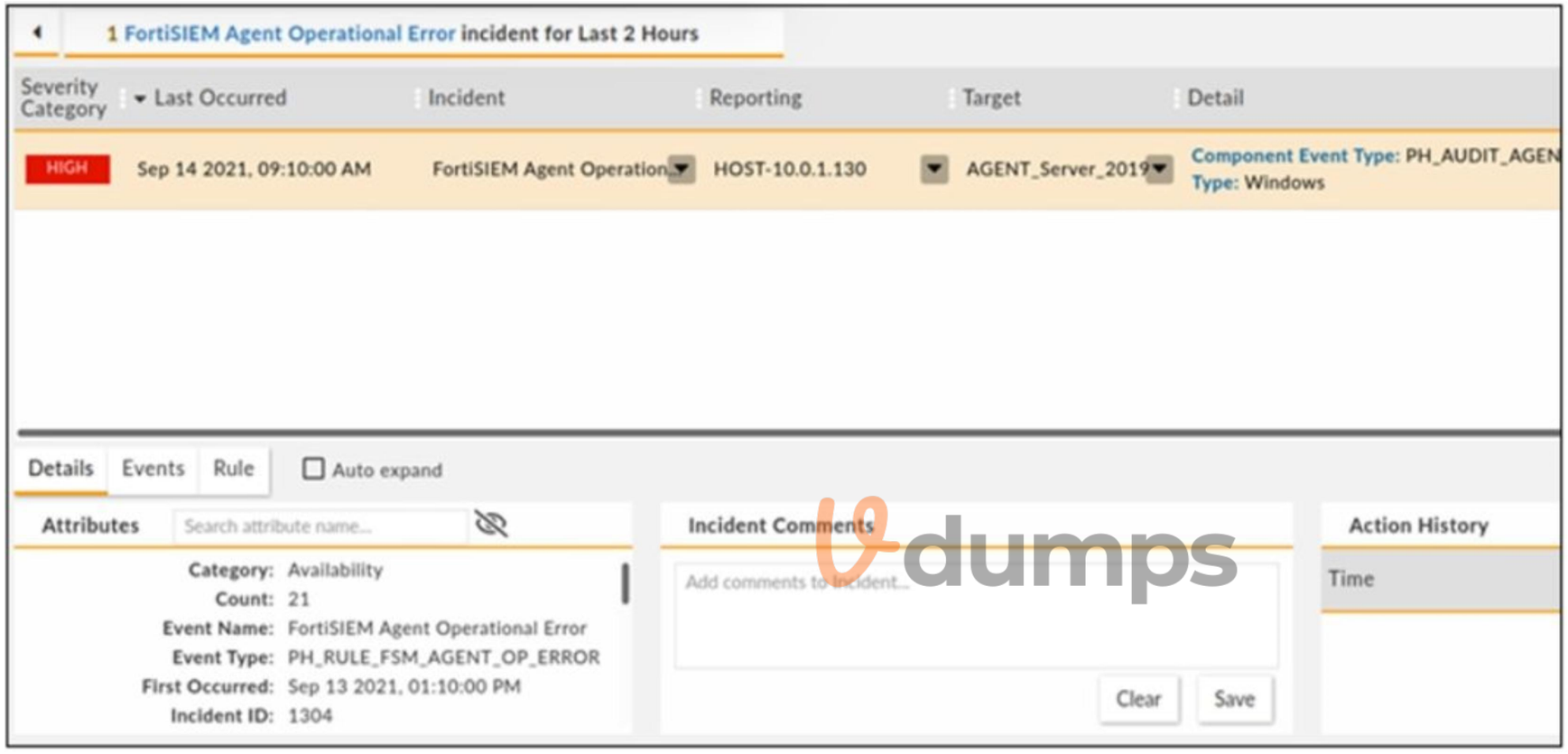
How many incidents are generated?

A. 1
B. 2
C. 0
D. 3

Correct Answer: B
Section:
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.

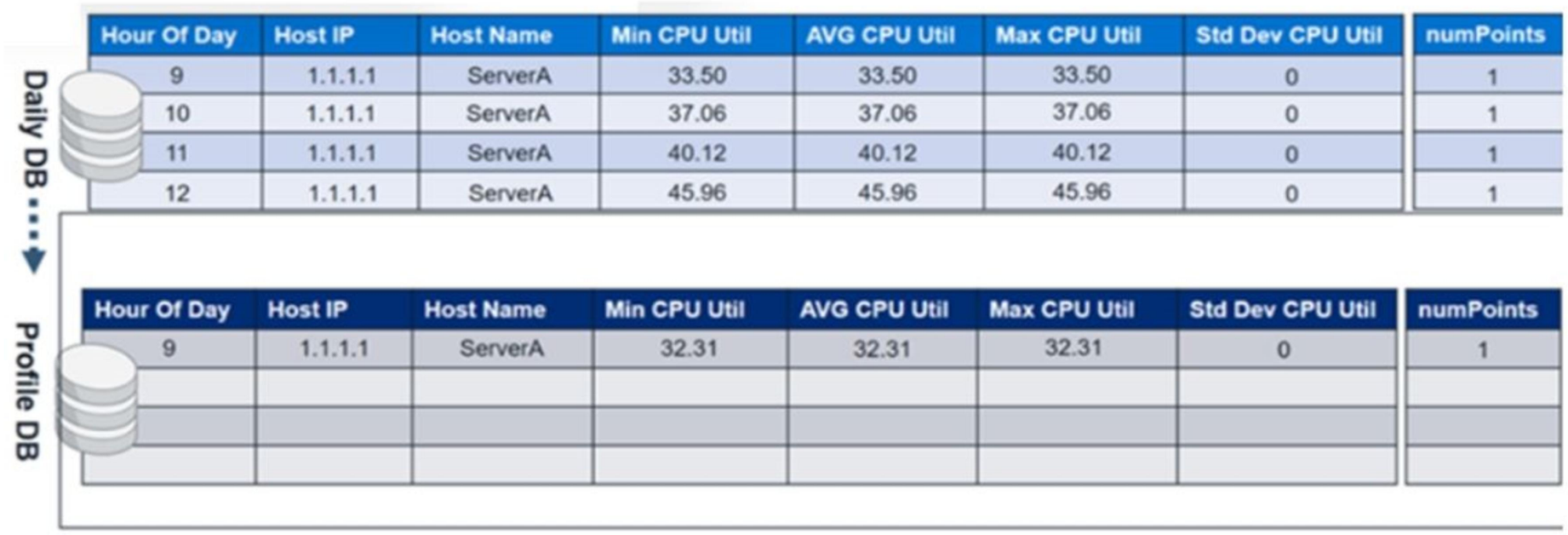
QUESTION 12
Refer to the exhibit.



How long has the UEBA agent been operationally down?
A. 21 Hours
B. 9 Hours
C. 20 Hours
D. 2 Hours

Correct Answer: A
Section:
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.

QUESTION 13
Refer to the exhibit. Click on the calculator button.



Hour Of Day	Host IP	Host Name	Min CPU Util	AVG CPU Util	Max CPU Util	Std Dev CPU Util	numPoints
9	1.1.1.1	ServerA	33.50	33.50	33.50	0	1
10	1.1.1.1	ServerA	37.06	37.06	37.06	0	1
11	1.1.1.1	ServerA	40.12	40.12	40.12	0	1
12	1.1.1.1	ServerA	45.96	45.96	45.96	0	1

Hour Of Day	Host IP	Host Name	Min CPU Util	AVG CPU Util	Max CPU Util	Std Dev CPU Util	numPoints
9	1.1.1.1	ServerA	32.31	32.31	32.31	0	1

The profile database contains CPU utilization values from day one. At midnight on the second day, the CPU utilization values from the daily database will be merged with the profile database.
In the profile database, in the Hour of Day column where 9 is the value, what will be the updated minimum, maximum, and average CPU utilization values?

A. Min CPU Util=32.31, Max CPU Ucil=33.50 and AVG CPU Util=33.50
B. Min CPU Util=32.31, Max CPU Ucil=33.50 and AVG CPU Util=32.67
C. Min CPU Util=32.31, Max CPU Ucil=32.31 and AVG CPU Util=32.31
D. Min CPU Util=33.50, Max CPU Ucil=33.50 and AVG CPU Util=33.50

Correct Answer: B
Section:
Explanation:
The profile database contains CPU utilization values from day one. At midnight on the second day, the CPU utilization values from the daily database will be merged with the profile database using a weighted average formula:
New value = (Old value x Old weight) + (New value x New weight) / (Old weight + New weight)
The weight is determined by the number of days in each database. In this case, the profile database has one day of data and the daily database has one day of data, so the weight is equal for both databases.
Therefore, the formula simplifies to:
New value = (Old value + New value) / 2
In the profile database, in the Hour of Day column where 9 is the value, the updated minimum, maximum, and average CPU utilization values are:
Min CPU Util = (32.31 + 32.31) / 2 = 32.31 Max CPU Util = (33.50 + 33.50) / 2 = 33.50 AVG CPU Util = (32.67 + 32.67) / 2 = 32.67

QUESTION 14
Refer to the exhibit.

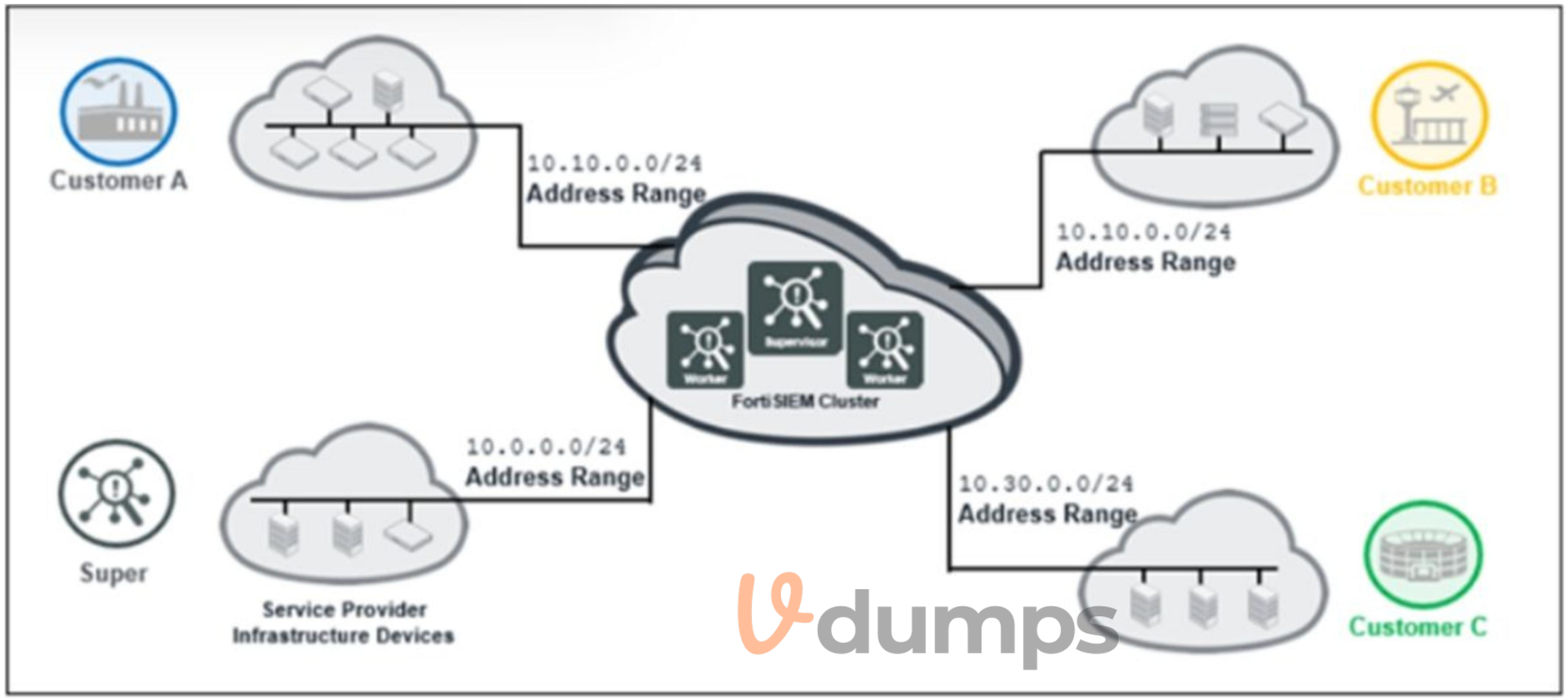
PROCESS	UPTIME
phParser	DOWN
phAgentManager	DOWN
phCheckpoint	DOWN
phDiscover	DOWN
phEventPackager	DOWN
phPerfMonitor	DOWN
phEventForwarder	DOWN
phMonitor	13:04
phMonitorAgent	DOWN
Rsyslogd	DOWN

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
Section:
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 15
Refer to the exhibit.

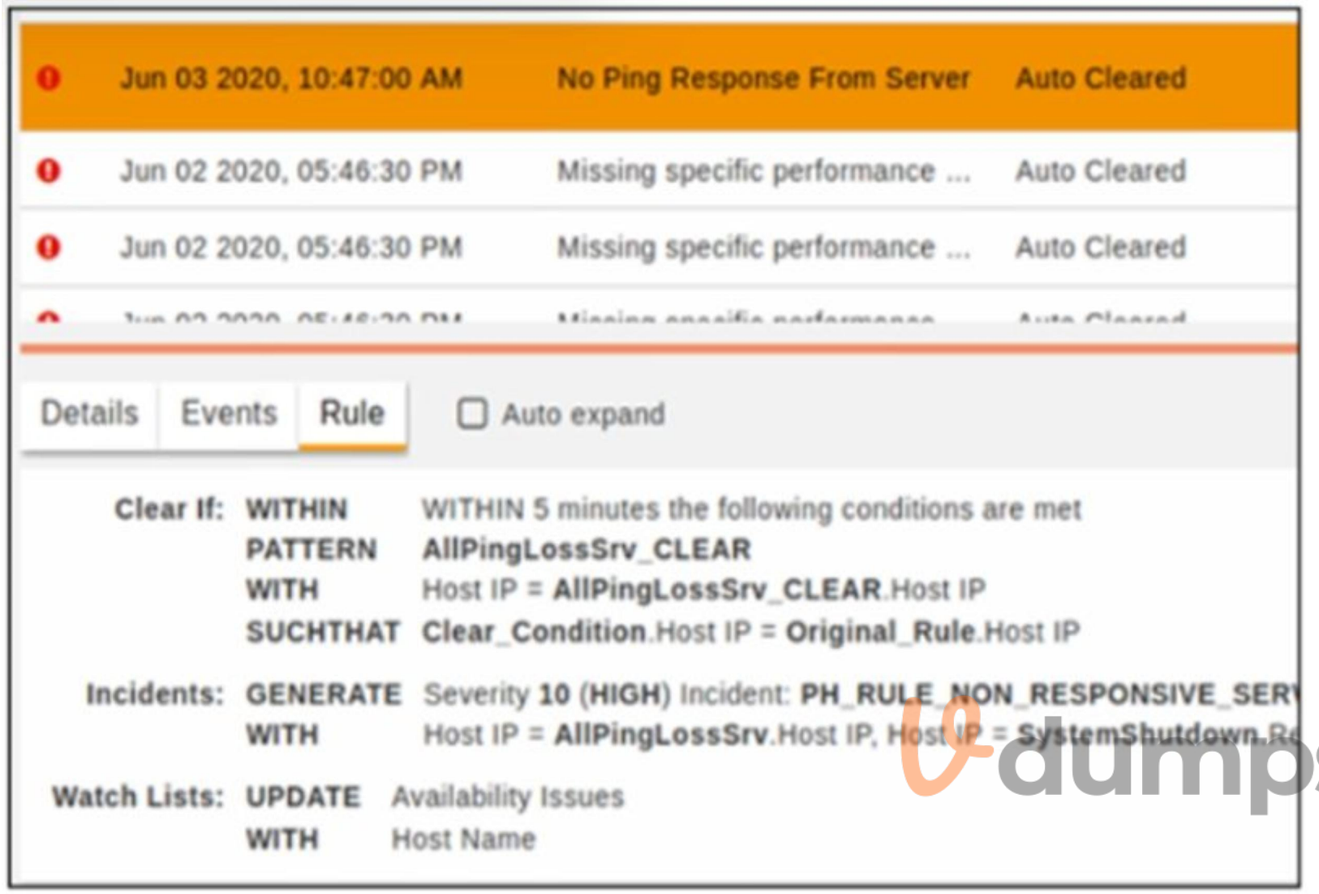


The service provider deployed FortiSIEM without a collector and added three customers on the supervisor.
What mistake did the administrator make?

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
Section:
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 16
Refer to the exhibit.



Why was this incident auto cleared?

A. Within five minutes the packet loss percentage dropped to a level where the reporting IP is the same as the host IP
B. The original rule did not trigger within five minutes
C. Within five minutes, the packet loss percentage dropped to a level where the reporting IP is same as the source IP
D. Within five minutes, the packet loss percentage dropped to a level where the host IP of the original rule matches the host IP of the clear condition pattern

Correct Answer: D
Section:
Explanation:
The incident was auto cleared because within five minutes, the packet loss percentage dropped to a level where the host IP of the original rule matches the host IP of the clear condition pattern. The clear condition pattern specifies that if there is an event with a packet loss percentage less than or equal to 10% and a host IP that matches any host IP in this incident, then clear this incident.

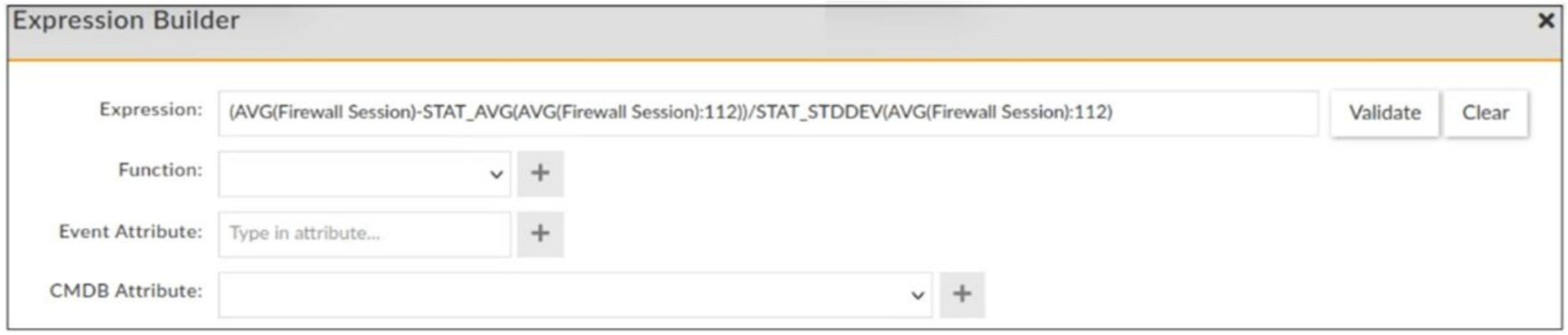
QUESTION 17
From where does the rule engine load the baseline data values?

A. The profile report
B. The daily database
C. The profile database
D. The memory

Correct Answer: C

Section:
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.

QUESTION 18
Refer to the exhibit.



If the Z-score for this rule is greater than or equal to three, what does this mean?
A. The rate of firewall connection is optimum.
B. The rate of firewall connection is above the historical average value.
C. The rate of firewall connection is above the current average value.
D. The rate of firewall connection is below historical average value.

Correct Answer: B
Section:
Explanation:
If the Z-score for this rule is greater than or equal to three, it means that the rate of firewall connection is above the historical average value. The Z-score is a measure of how many standard deviations a value is away from the mean of a distribution. A Z-score of three or more indicates that the value is significantly higher than the mean, which implies an anomaly or deviation from normal behavior.