



**Free Questions for [NSE7\\_ADA-6.3](#) by [go4braindumps](#)**

**Shared by [Alston](#) on [24-05-2024](#)**

**For More Free Questions and Preparation Resources**

**[Check the Links on Last Page](#)**

# Question 1

---

**Question Type:** MultipleChoice

---

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

## Options:

---

- 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

## 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

---

**Question Type:** MultipleChoice

---

Refer to the exhibit.

### Expression Builder

Expression:

Function:

Event Attribute:

CMDB Attribute:

If the Z-score for this rule is greater than or equal to three, what does this mean?

### Options:

---

- 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.

### Answer:

---

B

### 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.

## Question 3

---

**Question Type:** MultipleChoice

---

What is Tactic in the MITRE ATT&CK framework?

**Options:**

---

- 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

**Answer:**

---

B

**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 4

---

**Question Type:** MultipleChoice

---

Which syntax will register a collector to the supervisor?

### Options:

---

- A- phProvisionCollector --add
- B- phProvisionCollector --add
- C- phProvisionCollector --add
- D- phProvisionCollector --add

### Answer:

---

B

### 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

---

Question Type: MultipleChoice

---

Refer to the exhibit.

The screenshot shows the CMDB > Devices interface. At the top, there are seven summary cards for device types: Routers (0), Firewalls (0), Windows (1), Unix (1), ESX (0), AWS (0), and Azure (0). Below this is a navigation bar with buttons for 'New', 'Edit', 'Delete', a search box containing 'Discovered by All', and an 'Actions' menu. The main content is a table with the following data:

Name	IP	Device Type	Status	Discovered	Method	Agent Policy	Agent Status
FORTIBANK_DC	10.10.2.63	Windows Server	Pending	Oct 28, 2021, 3:02:21 PM	WMI, PING		
FortiBank_Collector	10.10.2.64	Generic Unix	Pending	Oct 28, 2021, 5:48:32 PM	LOG		

Why is the windows device still in the CMDB, even though the administrator uninstalled the windows agent?

Options:

---

- 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

**Answer:**

---

D

**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 6

---

**Question Type:** MultipleChoice

---

Refer to the exhibit.



## Edit SubPattern

Name:

Filters:

Paren	Attribute	Operator	Value	Paren	Ne
<input type="checkbox"/> <input type="checkbox"/>	Event Type	IN <input type="checkbox"/>	EventTypes: Domain Account Locked	<input type="checkbox"/> <input type="checkbox"/>	A
<input type="checkbox"/> <input type="checkbox"/>	Reporting IP	IN <input type="checkbox"/>	Applications: Domain Controller	<input type="checkbox"/> <input type="checkbox"/>	A

Aggregate:

Paren	Attribute	Operator	Value	Paren	Ne
<input type="checkbox"/> <input type="checkbox"/>	COUNT(Matched Events)	>= <input type="checkbox"/>	1	<input type="checkbox"/> <input type="checkbox"/>	A

Group By:

Attribute	Row		Move	
<input type="text" value="Reporting Device"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="text" value="Reporting IP"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="text" value="User"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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

### Options:

---

- 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 IP 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.

### 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 7

---

**Question Type:** MultipleChoice

---

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

### Options:

---

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

### Answer:

---

C

### 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 8

---

**Question Type:** MultipleChoice

---

Refer to the exhibit.

	Jun 03 2020, 10:47:00 AM	No Ping Response From Server	Auto Cleared
	Jun 02 2020, 05:46:30 PM	Missing specific performance ...	Auto Cleared
	Jun 02 2020, 05:46:30 PM	Missing specific performance ...	Auto Cleared
	Jun 02 2020, 05:46:30 PM	Missing specific performance ...	Auto Cleared

---

Details
Events
Rule
 Auto expand

**Clear If:** **WITHIN** WITHIN 5 minutes the following conditions are met

**PATTERN** AllPingLossSrv\_CLEAR

**WITH** Host IP = AllPingLossSrv\_CLEAR.Host IP

**SUCHTHAT** Clear\_Condition.Host IP = Original\_Rule.Host IP

**Incidents:** **GENERATE** Severity 10 (HIGH) Incident: PH\_RULE\_NON\_RESPONSIVE\_SERV

**WITH** Host IP = AllPingLossSrv.Host IP, Host IP = SystemShutdown.Re

**Watch Lists:** **UPDATE** Availability Issues

**WITH** Host Name

Why was this incident auto cleared?

### Options:

---

- 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

### Answer:

---

D

### 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.

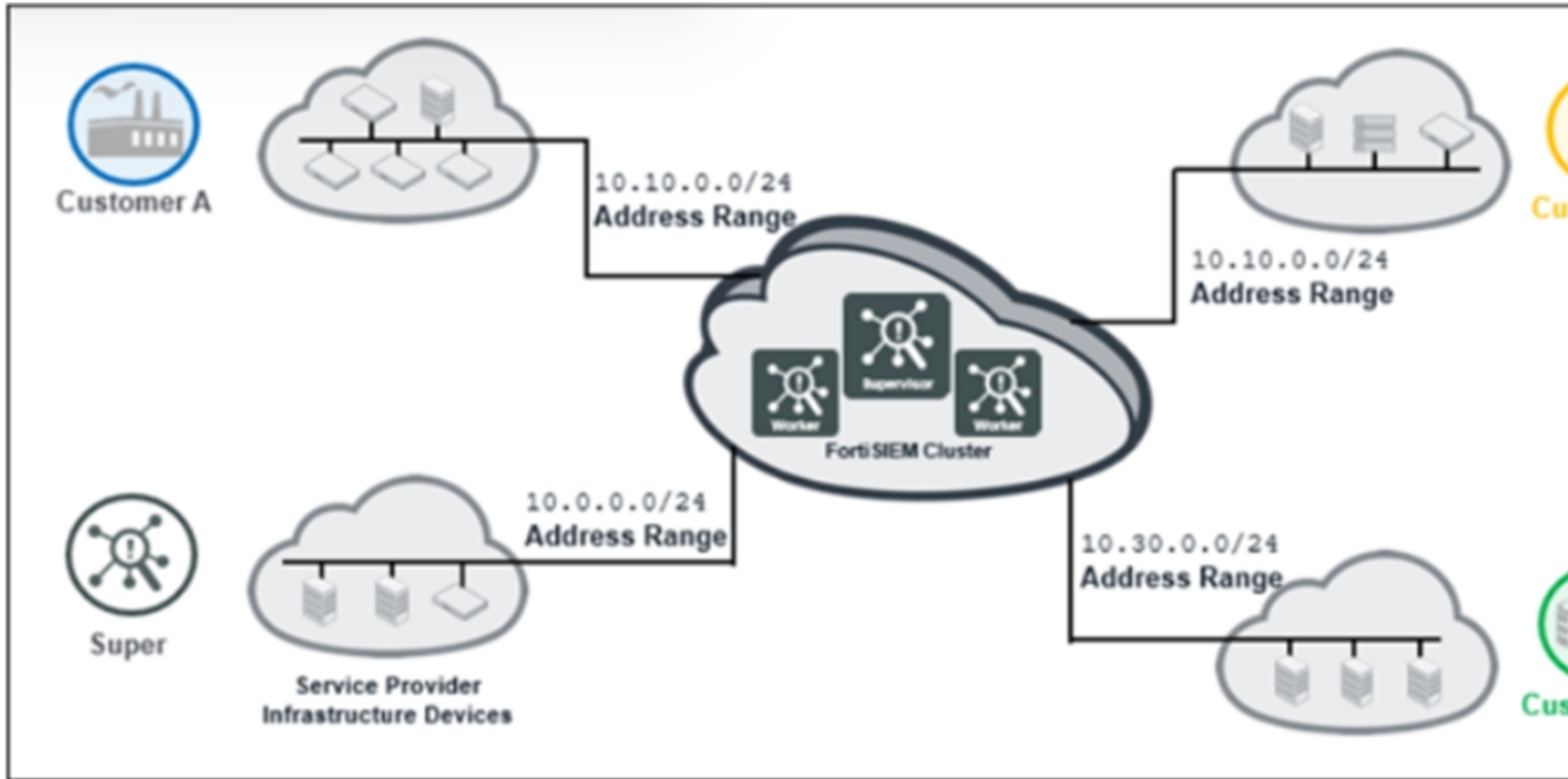
## Question 9

---

**Question Type:** MultipleChoice

---

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?

**Options:**

---

- 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.

**Answer:**

---

A

**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 10

---



**Question Type: MultipleChoice**

---

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

**Options:**

---

- 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, every 30 seconds

**Answer:**

---

A, B, E

**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 11

---

**Question Type:** MultipleChoice

---

Identify the processes associated with Machine Learning/AI on FortiSIEM. (Choose two.)

### Options:

---

- A- phFortilInsightAI
- B- phReportMaster
- C- phRuleMaster
- D- phAnomaly
- E- phRuleWorker

### Answer:

---

A, D

### **Explanation:**

---

The processes associated with Machine Learning/AI on FortiSIEM are phFortilnsightAI and phAnomaly. phFortilnsightAI 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 12**

---

### **Question Type: MultipleChoice**

---

Which two statements about the maximum device limit on FortiSIEM are true? (Choose two.)

### **Options:**

---

- 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:**

---

B, C

**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.

**To Get Premium Files for NSE7\_ADA-6.3 Visit**

[https://www.p2pexams.com/products/nse7\\_ada-6.3](https://www.p2pexams.com/products/nse7_ada-6.3)

**For More Free Questions Visit**

<https://www.p2pexams.com/fortinet/pdf/nse7-ada-6.3>

