# NSE7_ADA-6.3$^{\text{Q\&As}}$

Fortinet NSE 7 - Advanced Analytics 6.3

## Pass Fortinet NSE7_ADA-6.3 Exam with 100% Guarantee

**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.

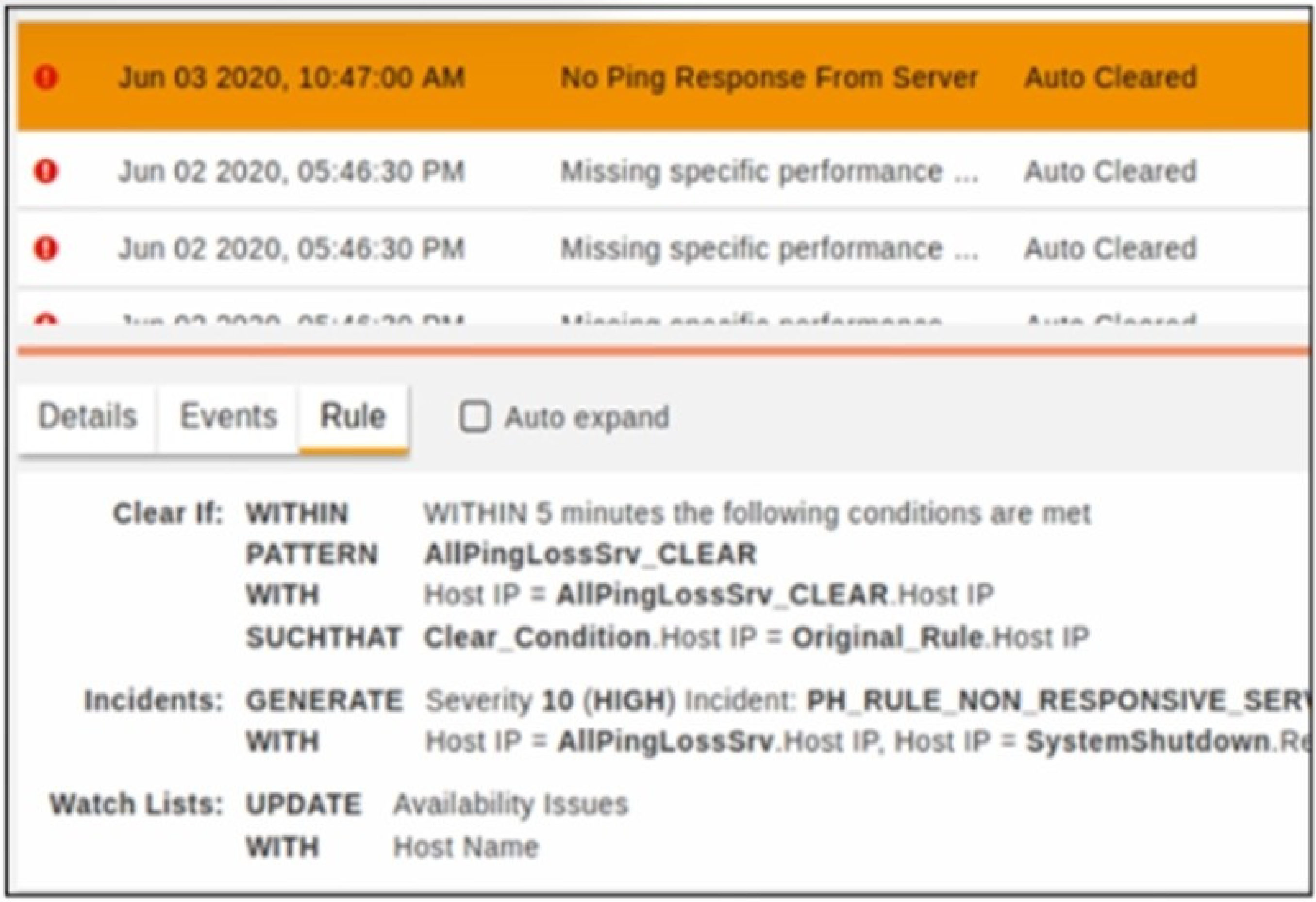
D. The device limit is defined for the whole system and is shared by every customer on a service provider edition.

Correct Answer: 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 2**

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
```

```
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_SER
              WITH        Host IP = AllPingLossSrv.Host IP, Host IP = SystemShutdown.Re

Watch Lists:  UPDATE    Availability Issues
              WITH      Host Name
```

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

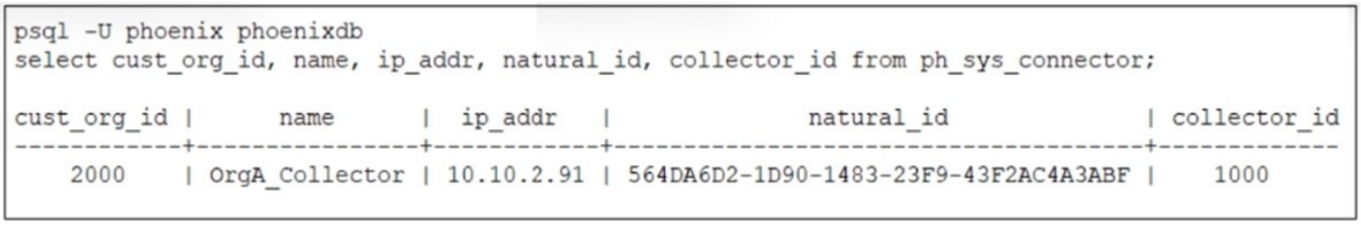
D. Within five minutes, the packet loss percentage dropped to a level where the host IP of the original rule matches the host IP of the clear condition pattern

Correct Answer: D

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 3**

Refer to the exhibit.



```
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
```

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. What does the natural_id value identify?

A. The supervisor

B. The worker

C. An agent

D. The collector

Correct 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.

**QUESTION 4**

What is the disadvantage of automatic remediation?

A. It can make a disruptive change to a user, block access to an application, or disconnect critical systems from the network.

B. It is equivalent to running an IPS in monitor-only mode -- watches but does not block.

C. External threats or attacks detected by FortiSIEM will need user interaction to take action on an already overworked SOC team.

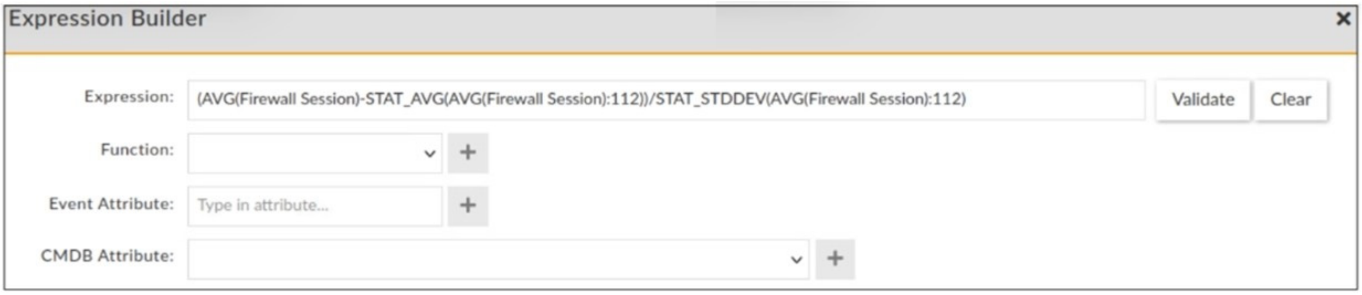
D. Threat behaviors occurring during the night could take hours to respond to.

Correct Answer: A

Explanation: The disadvantage of automatic remediation is that it can make a disruptive change to a user, block access to an application, or disconnect critical systems from the network. Automatic remediation can have unintended consequences if not carefully planned and tested. Therefore, it is recommended to use manual or semi-automatic remediation for sensitive or critical systems. References: Fortinet NSE 7 - Advanced Analytics 6.3 escription, page 15

**QUESTION 5**

Refer to the exhibit.



Expression Builder

Expression: (AVG(Firewall Session)-STAT_AVG(AVG(Firewall Session):112))/STAT_STDDEV(AVG(Firewall Session):112)

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

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.