# NSE7_ADA-6.3 Q&As

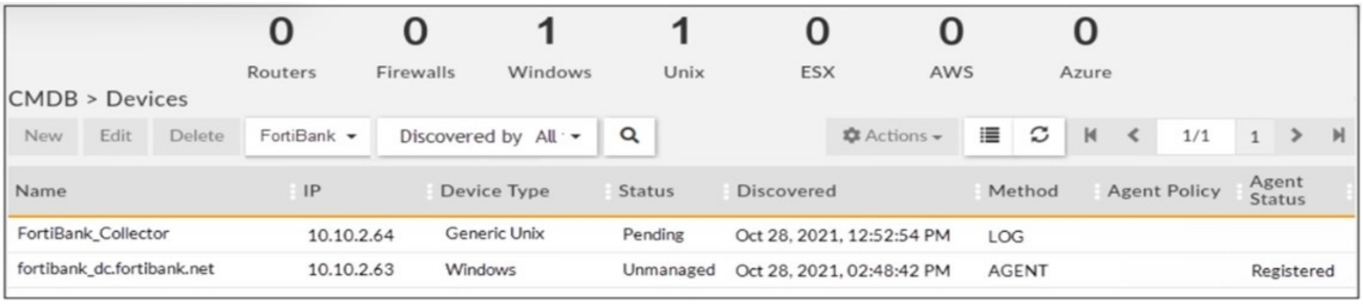
Fortinet NSE 7 - Advanced Analytics 6.3

## 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**

Refer to the exhibit.



| 0 | 0 | 1 | 1 | 0 | 0 | 0 |
|---|---|---|---|---|---|---|
| Routers | Firewalls | Windows | Unix | ESX | AWS | Azure |

CMDB > Devices

| Name | IP | Device Type | Status | Discovered | Method | Agent Policy | Agent Status |
|---|---|---|---|---|---|---|---|
| FortiBank_Collector | 10.10.2.64 | Generic Unix | Pending | Oct 28, 2021, 12:52:54 PM | LOG | | |
| fortibank_dc.fortibank.net | 10.10.2.63 | Windows | Unmanaged | Oct 28, 2021, 02:48:42 PM | AGENT | | Registered |

Is the Windows agent delivering event logs correctly?

A. The logs are buffered by the agent and will be sent once the status changes to managed.

B. The agent is registered and it is sending logs correctly.

C. The agent is not sending logs because it did not receive a monitoring template.

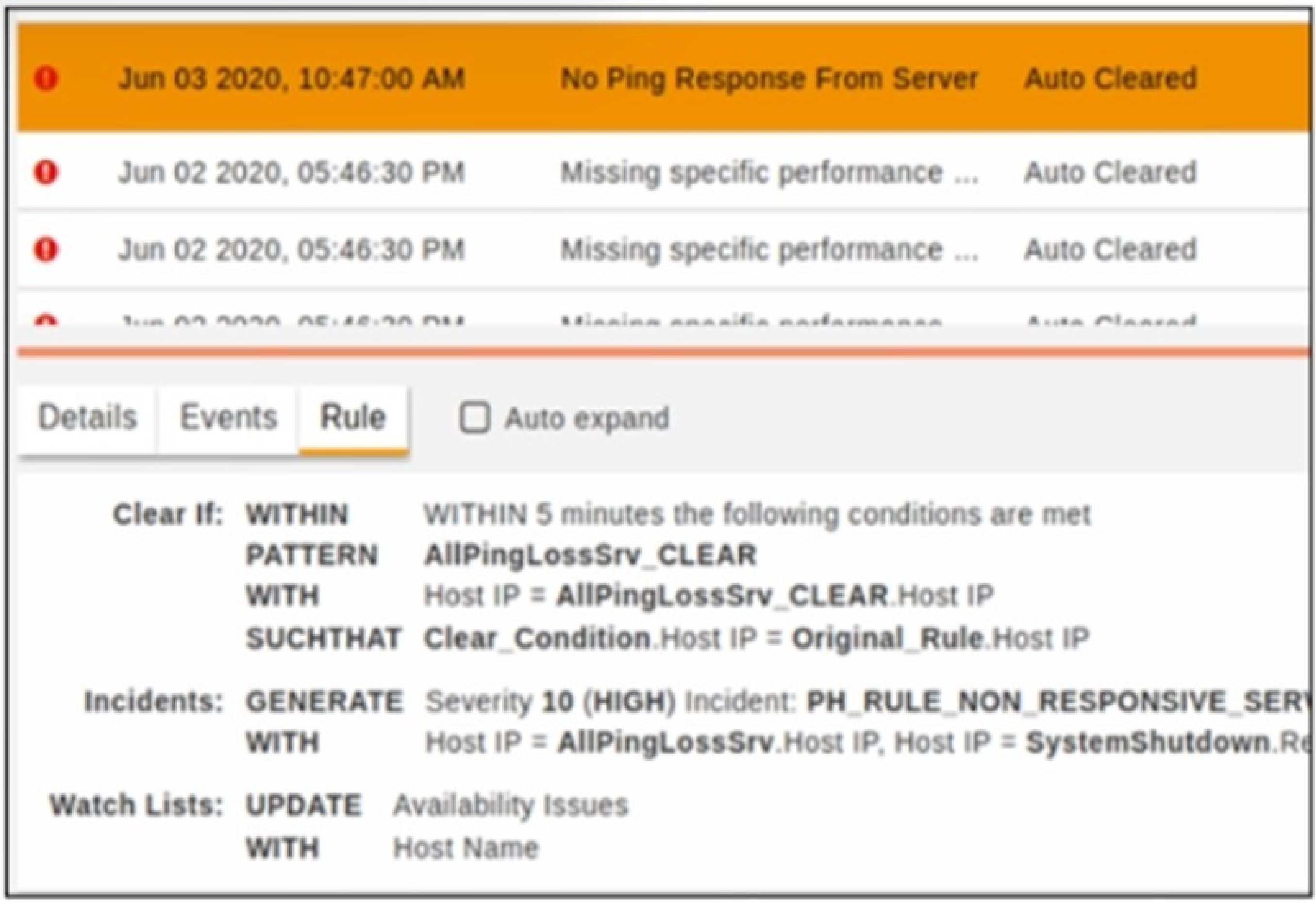
D. Because the agent is unmanaged. the logs are dropped silently by the supervisor.

Correct Answer: D

Explanation: The windows agent is not delivering event logs correctly because the agent is unmanaged, meaning it is not assigned to any organization or customer. The supervisor will drop the logs silently from unmanaged agents, as they are not associated with any valid license or CMDB.

**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**

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

A. phFortiInsightAI

B. phReportMaster

C. phRuleMaster

D. phAnomaly

E. phRuleWorker

Correct Answer: AD

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 4**

Which of the following are two Tactics in the MITRE ATTandCK framework? (Choose two.)

A. Root kit

B. Reconnaissance

C. Discovery

D. BITS Jobs

E. Phishing

Correct Answer: BC

Explanation: Reconnaissance and Discovery are two Tactics in the MITRE ATTandCK framework. Tactics are the high-level objectives of an adversary, such as initial access, persistence, lateral movement, etc. Reconnaissance is the tactic of gathering information about a target before launching an attack. Discovery is the tactic of exploring a compromised system or network to find information or assets of interest. References: Fortinet NSE 7 - Advanced Analytics 6.3 escription, page 21

**QUESTION 5**

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

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.