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:

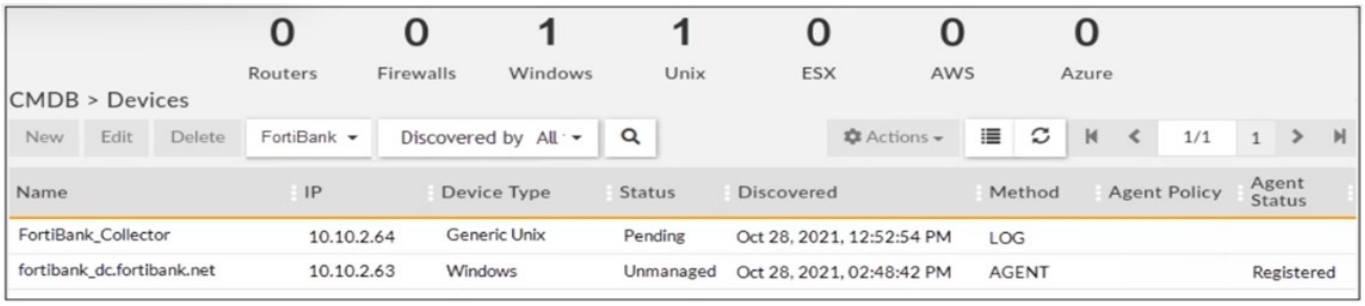
https://www.pass2lead.com/nse7_ada-6-3.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Fortinet Official Exam Center

QUESTION 1

Refer to the exhibit.



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

What is Tactic in the MITRE ATTandCK 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

Explanation: Tactic is what an attacker hopes to achieve in the MITRE ATTandCK 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 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

Which syntax will register a collector to the supervisor?

A. phProvisionCollector --add

B. phProvisionCollector --add

C. phProvisionCollector --add

D. phProvisionCollector --add

Correct Answer: B

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

QUESTION 5

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

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.