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

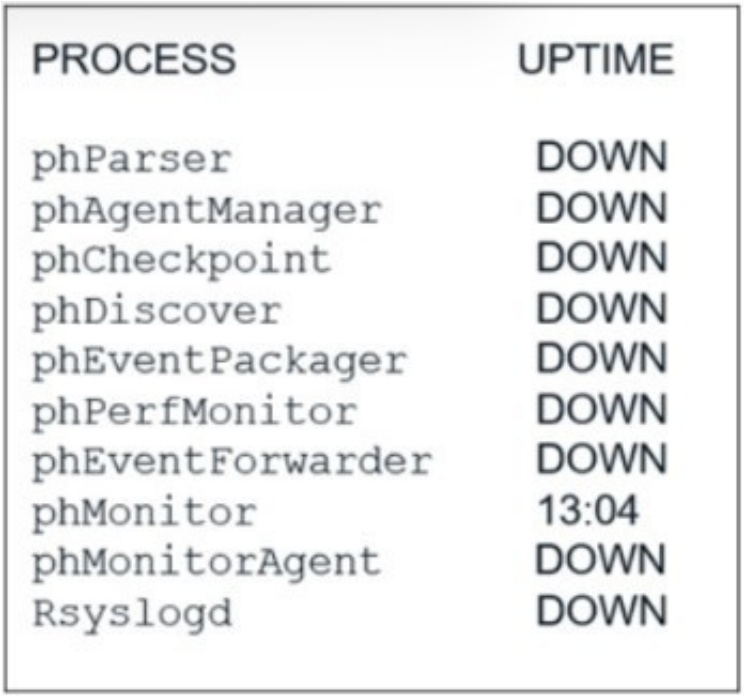
100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

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.

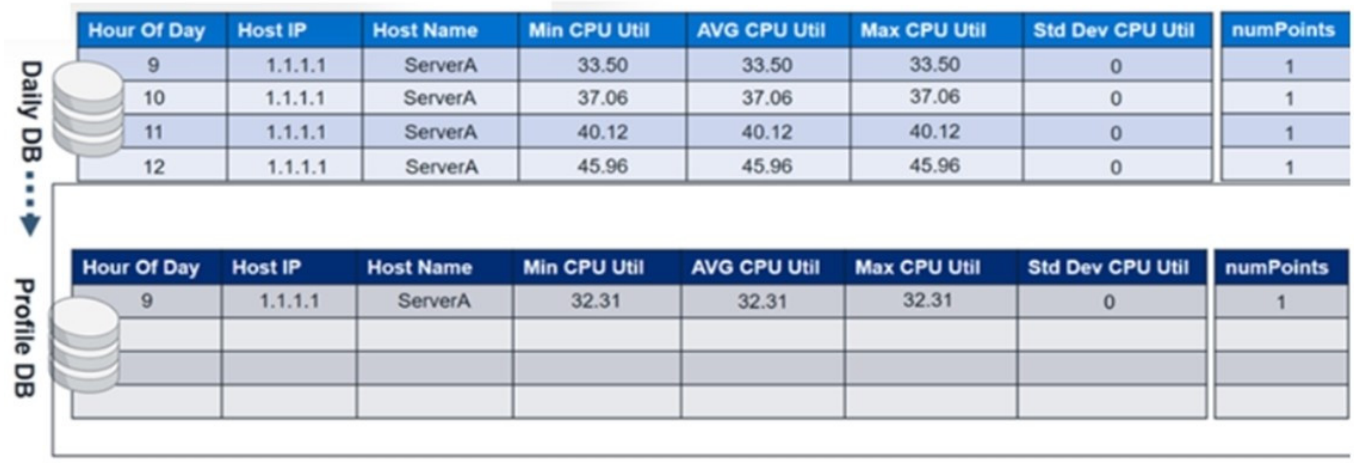
D. The collector was not deployed properly and must be redeployed.

Correct Answer: C

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 2

Refer to the exhibit. Click on the calculator button.



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

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 3

How can you empower SOC by deploying FortiSOAR? (Choose three.)

A. Aggregate logs from distributed systems

B. Collaborative knowledge sharing

C. Baseline user and traffic behavior

D. Reduce human error

E. Address analyst skills gap

Correct Answer: BDE

Explanation: You can empower SOC by deploying FortiSOAR in the following ways:

Collaborative knowledge sharing: FortiSOAR allows you to create and share playbooks, workflows, tasks, and notes among SOC analysts and teams. This enables faster and more consistent incident response and reduces duplication of

efforts.

Reduce human error: FortiSOAR automates repetitive and tedious tasks, such as data collection, enrichment, analysis, and remediation. This reduces the risk of human error and improves efficiency and accuracy. Address analyst skills gap:

FortiSOAR provides a graphical user interface for creating and executing playbooks and workflows without requiring coding skills. This lowers the barrier for entry-level analysts and helps them learn from best practices and expert knowledge.

References: Fortinet NSE 7 - Advanced Analytics 6.3 escription, page 19

QUESTION 4

How do customers connect to a shared multi-tenant instance on FortiSOAR?

A. The MSSP must provide secure network connectivity between the FortiSOAR manager node and the customer devices.

B. The MSSP must install a Secure Message Exchange node to connect to the customer\\'s shared multi-tenant instance.

C. The customer must install a tenant node to connect to the MSSP shared multi-tenant instance.

D. The MSSP must install an agent node on the customer\\'s network to connect to the customer\\'s shared multi-tenant instance.

Correct Answer: D

Explanation: To connect to a shared multi-tenant instance on FortiSOAR, the MSSP must install an agent node on the customer\\'s network. The agent node acts as a proxy between the customer\\'s devices and the FortiSOAR manager node. The agent node also performs data collection, enrichment, and normalization for the customer\\'s data sources. References: Fortinet NSE 7 - Advanced Analytics 6.3 escription, page 11

QUESTION 5

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.