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.leads4pass.com/nse7_ada-6-3.html

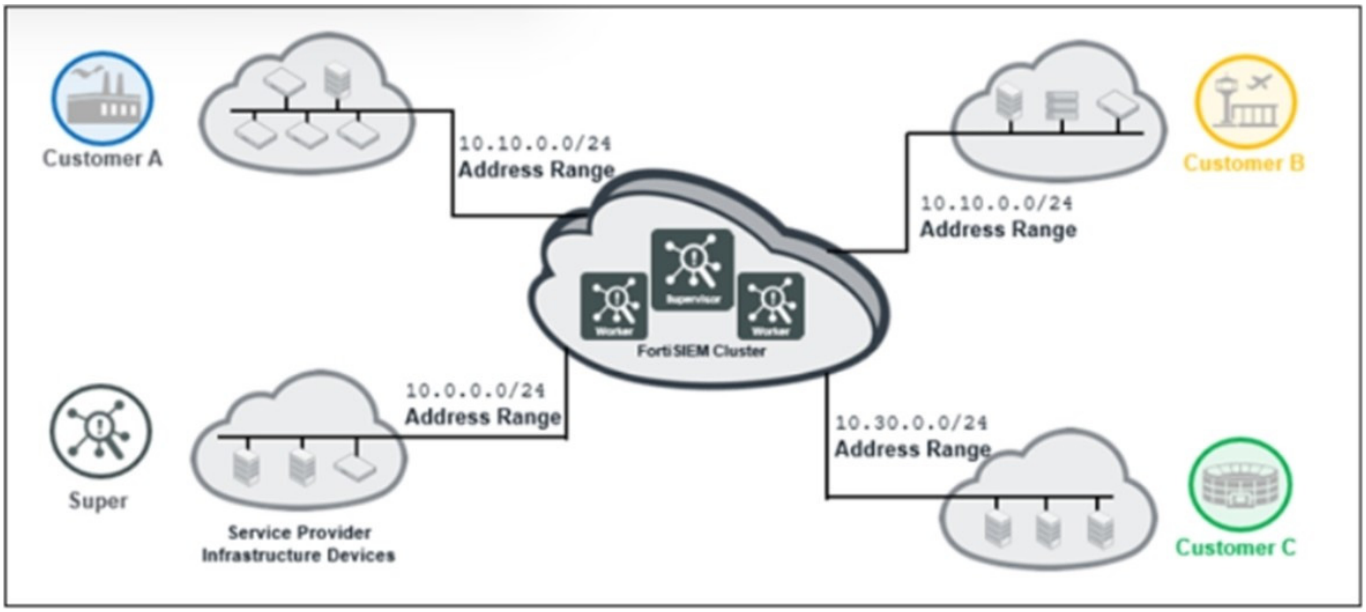
100% Passing Guarantee
100% Money Back Assurance

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.



The service provider deployed FortiSIEM without a collector and added three customers on the supervisor. What mistake did the administrator make?

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.

Correct 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 2

In the event of a WAN link failure between the collector and the supervisor, by default, what is the maximum number of event files stored on the collector?

A. 30.000

B. 10.000

C. 40.000

D. 20.000

Correct Answer: B

Explanation: By default, the maximum number of event files stored on the collector in the event of a WAN link failure between the collector and the supervisor is 10.000. This value can be changed in the collector.properties file by modifying the parameter max_event_files_to_store. References: Fortinet NSE 7 - Advanced Analytics 6.3 escription, page 13

QUESTION 3

How can you invoke an integration policy on FortiSIEM rules?

A. Through Notification Policy settings

B. Through Incident Notification settings

C. Through remediation scripts

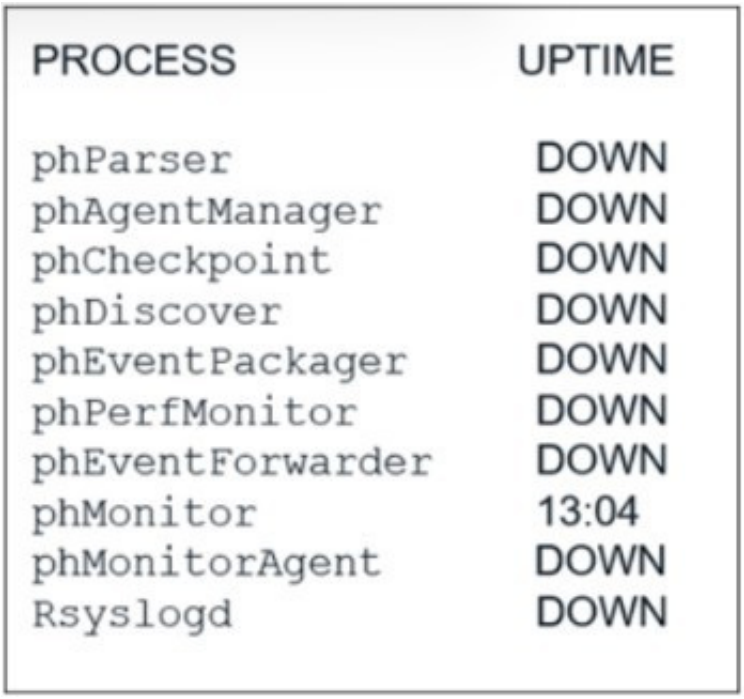
D. Through External Authentication settings

Correct Answer: A

Explanation: You can invoke an integration policy on FortiSIEM rules by configuring the Notification Policy settings. You can select an integration policy from the drop-down list and specify the conditions for triggering it. For example, you can invoke an integration policy when an incident is created, updated, or closed. References: Fortinet NSE 7 - Advanced Analytics 6.3 escription, page 9

QUESTION 4

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 5

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.