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:

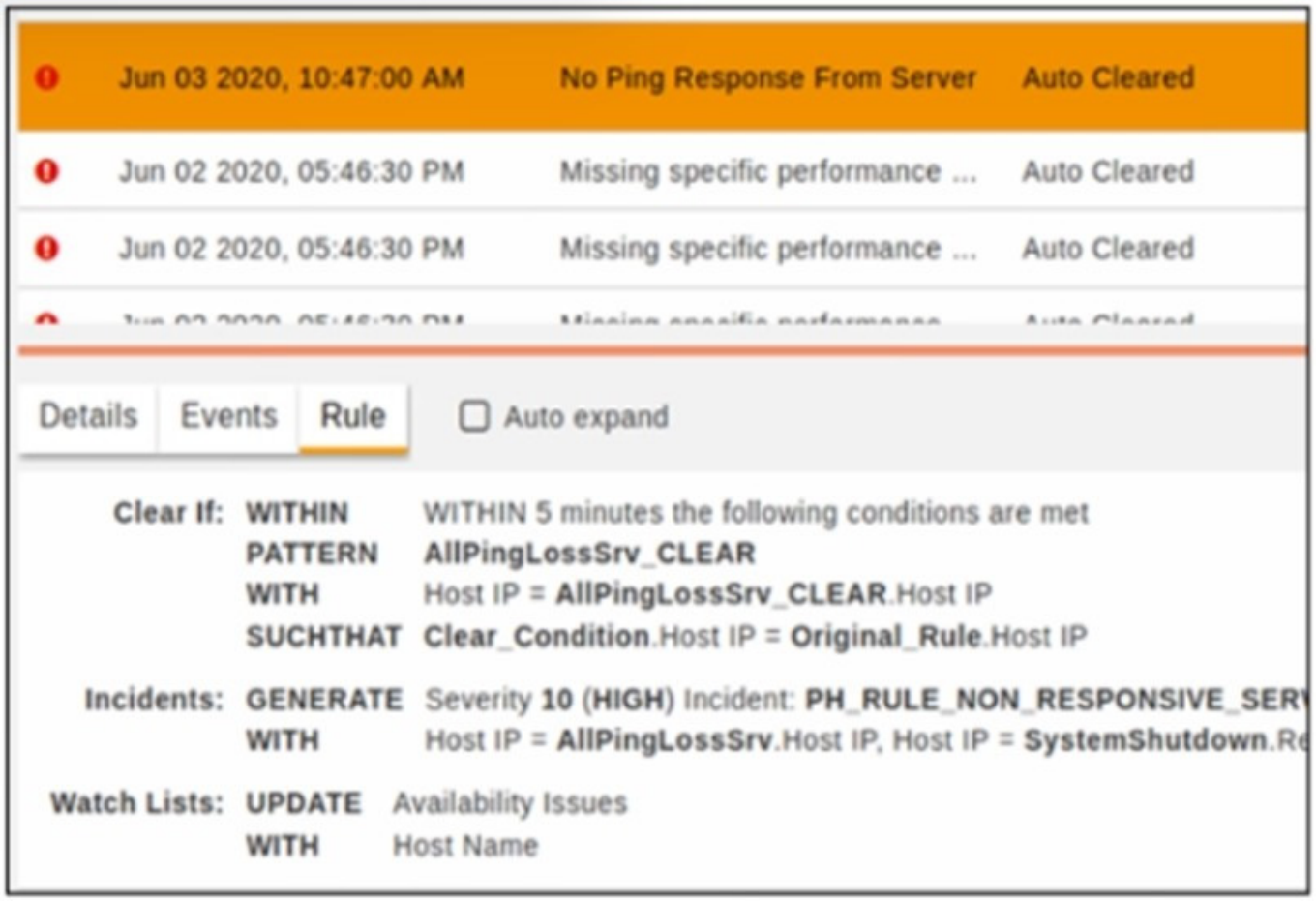
https://www.pass2lead.com/nse7_ada-6-3.html

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.



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 2

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 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

Refer to the exhibit.

An administrator wants to remediate the incident from FortiSIEM shown in the exhibit.

What option is available to the administrator?

A. Quarantine IP FortiClient

B. Run the block MAC FortiOS.

C. Run the block IP FortiOS 5.4

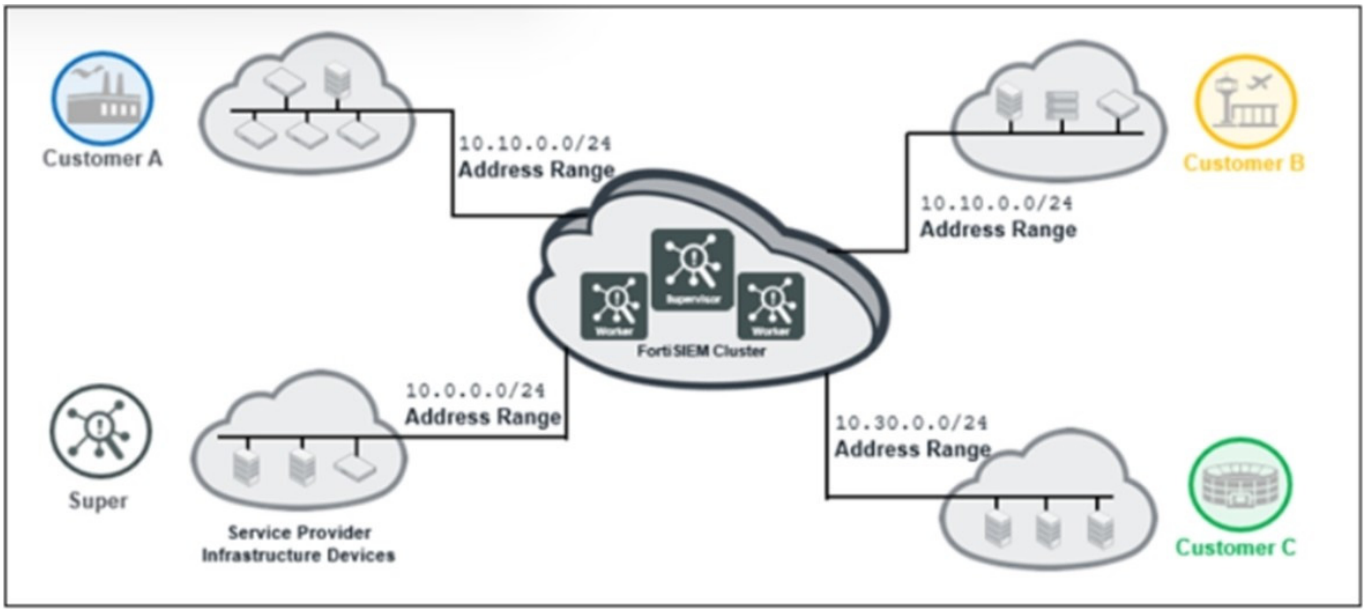
D. Run the block domain Windows DNS

Correct Answer: C

Explanation: The incident from FortiSIEM shown in the exhibit is a brute force attack on a FortiGate device. The remediation option available to the administrator is to run the block IP FortiOS 5.4 action, which will block the source IP address of the attacker on the FortiGate device using a firewall policy.

QUESTION 5

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 6

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.

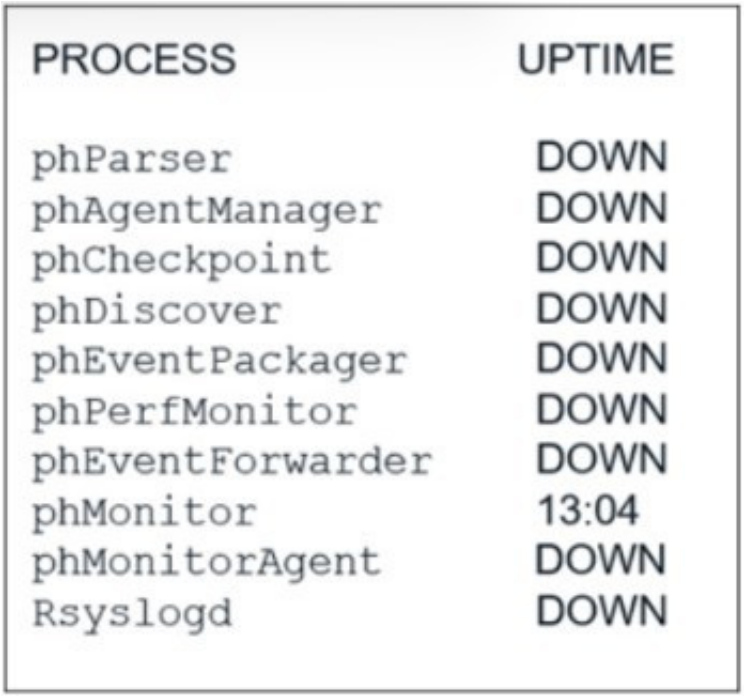
Correct Answer: BC

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 7

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.

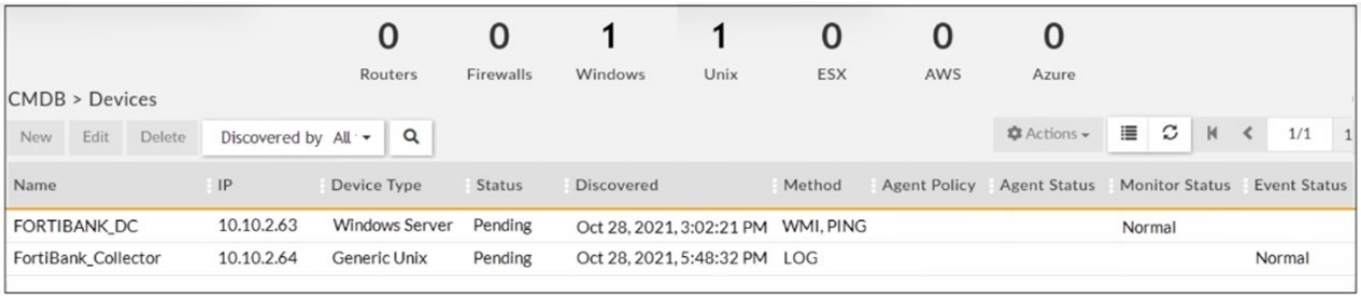
D. The collector was not deployed properly and must be redeployed.

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 8

Refer to the exhibit.



Why is the windows device still in the CMDB, even though the administrator uninstalled the windows agent?

A. The device was not uninstalled properly

B. The device must be deleted from backend of FortiSIEM

C. The device has performance jobs assigned

D. The device must be deleted manually from the CMDB

Correct Answer: D

Explanation: The windows device is still in the CMDB, even though the administrator uninstalled the windows agent, because the device must be deleted manually from the CMDB. Uninstalling the windows agent does not automatically remove the device from the CMDB, as there may be other sources of data for the device, such as SNMP or syslog. To delete the device from the CMDB, the administrator must go to CMDB > Devices > All Devices, select the device, and click Delete.

QUESTION 9

Which three processes are collector processes? (Choose three.)

A. phAgentManaqer

B. phParser

C. phRuleMaster

D. phReportM aster

E. phMonitorAgent

Correct Answer: BCE

Explanation: The collector processes are responsible for receiving, parsing, normalizing, correlating, and monitoring events from various sources. The collector processes are phParser, phRuleMaster, and phMonitorAgent.

QUESTION 10

Which three statements about collector communication with the FortiSIEM cluster are true? (Choose three.)

A. The only communication between the collector and the supervisor is during the registration process.

B. Collectors communicate periodically with the supervisor node.

C. The supervisor periodically checks the health of the collector.

D. The supervisor does not initiate any connections to the collector node.

E. Collectors upload event data to any node in the worker upload list, but report their health directly to the supervisor node.

Correct Answer: BCE

Explanation: The statements about collector communication with the FortiSIEM cluster that are true are:

Collectors communicate periodically with the supervisor node. Collectors send heartbeat messages to the supervisor every 30 seconds to report their status and configuration.

The supervisor periodically checks the health of the collector. The supervisor monitors the heartbeat messages from collectors and alerts if there is any issue with their connectivity or performance.

Collectors upload event data to any node in the worker upload list, but report their health directly to the supervisor node. Collectors use a round-robin algorithm to distribute event data among worker nodes in the worker upload list, which is

provided by the supervisor during registration. However, collectors only report their health and status to the supervisor node.