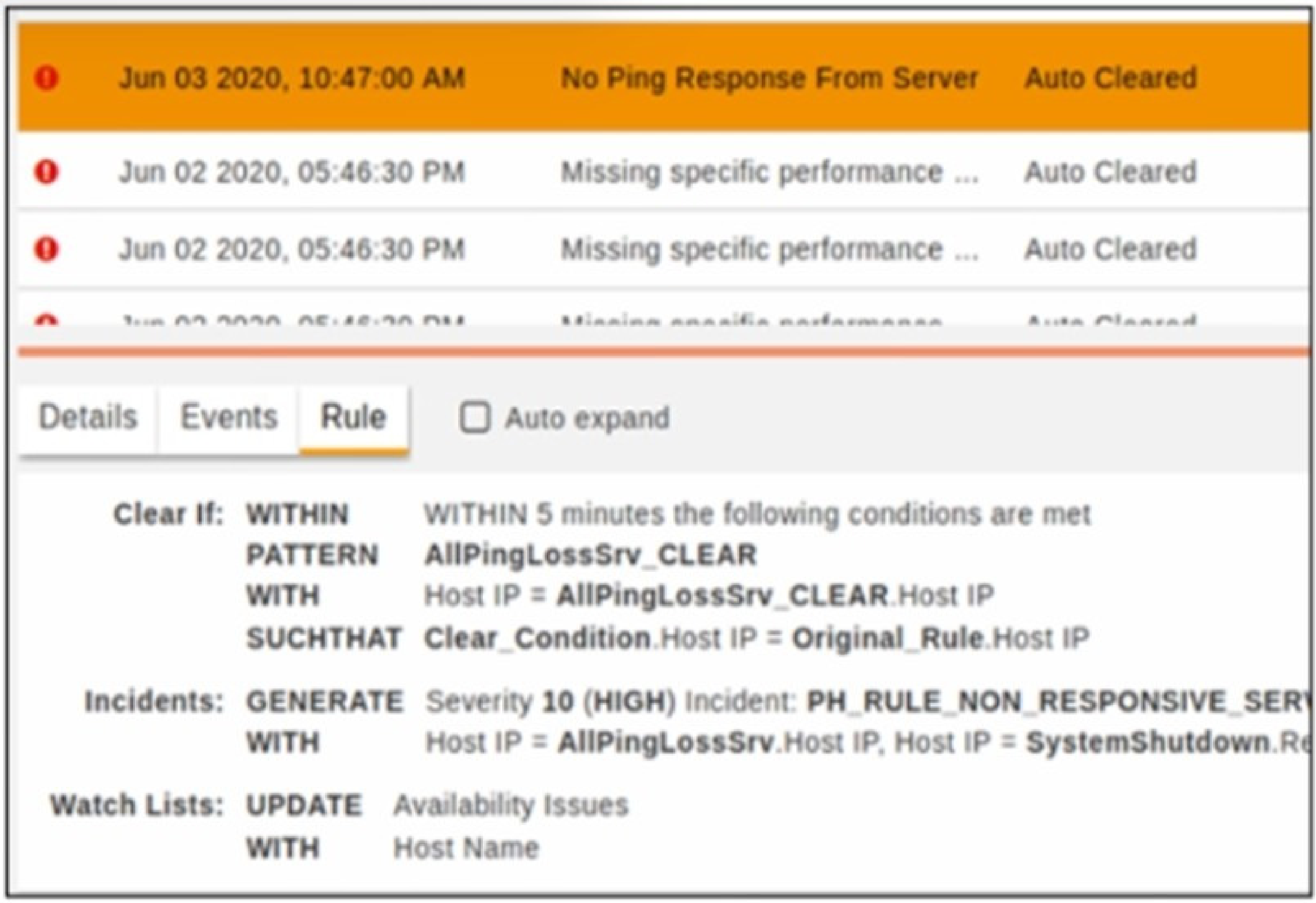
NSE7_ADA-6.3$^{Q\&As}$

Fortinet NSE 7 - Advanced Analytics 6.3

Pass Fortinet NSE7_ADA-6.3 Exam with 100% Guarantee

QUESTION 1

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 2

Why can collectors not be defined before the worker upload address is set on the supervisor?

A. Collectors can only upload data to a worker, and the supervisor is not a worker

B. To ensure that the service provider has deployed at least one worker along with a supervisor

C. Collectors receive the worker upload address during the registration process

D. To ensure that the service provider has deployed a NFS server

Correct Answer: C

Explanation: Collectors cannot be defined before the worker upload address is set on the supervisor because collectors receive the worker upload address during the registration process. The worker upload address is a list of IP addresses of worker nodes that can receive event data from collectors. The supervisor provides this list to collectors when they register with it, so that collectors can upload event data to any node in the list.

QUESTION 3

On which disk are the SQLite databases that are used for the baselining stored?

A. Disk1

B. Disk4

C. Disk2

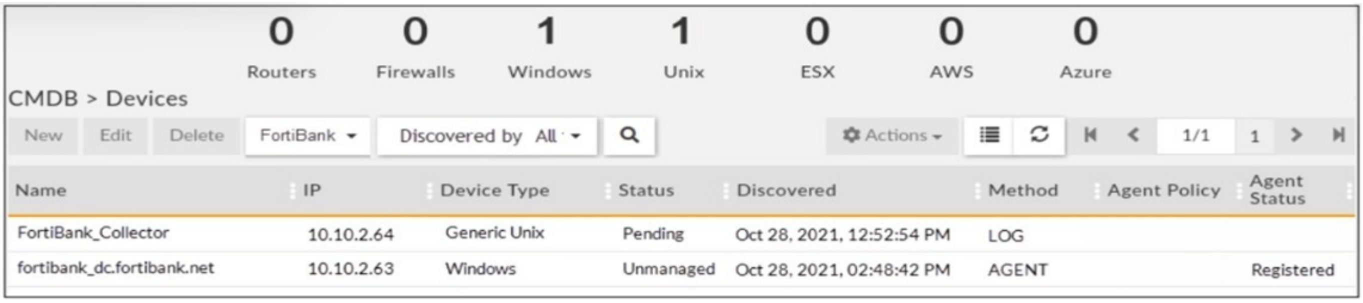
D. Disk3

Correct Answer: D

Explanation: The SQLite databases that are used for the baselining are stored on Disk3 of the FortiSIEM server. Disk3 is also used for storing raw event data and CMDB data.

QUESTION 4

Refer to the exhibit.



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 5

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