Exam Questions NSE5_FSM-5.2

Fortinet NSE 5 - FortiSIEM 5.2

https://www.2passeasy.com/dumps/NSE5_FSM-5.2/

NEW QUESTION 1
A FortiSIEM administrator wants to restrict a network administrator to running searches for only firewall devices. Under role management, which option does the FortiSIEM administrator need to configure to achieve this scenario?

A. CMDB Report Conditions
B. Data Conditions
C. UI Access

Answer: B

NEW QUESTION 2
Which item is required to register a FortiSIEM appliance license?

A. Static storage
B. Static MAC address
C. Static IP address
D. Static Hardware ID

Answer: D

NEW QUESTION 3
Refer to the exhibit.

How was the FortiGate device discovered by FortiSIEM?

A. Through GUI log discovery
B. Through syslog discovery
C. Using the pull events method
D. Through auto log discovery

Answer: A

NEW QUESTION 4
Which protocol is almost always required for the FortiSIEM GUI discovery process?

A. SNMP
B. WMI
C. Syslog
D. Telnet

Answer: A

NEW QUESTION 5
Which three ports can be used to send Syslogs to FortiSIEM? (Choose three.)

A. UDP9999
B. UDP 162
C. TCP 514
D. UDP 514
E. TCP 1470

Answer: CDE

NEW QUESTION 6
What are the minimum memory requirements for the FortiSIEM supervisor virtual appliance, when the proprietary flat file database is used?

A. 16GB RAM
B. 32GB RAM
C. 64GB RAM
D. 24GB RAM

Answer: D

NEW QUESTION 7
A FortiSIEM supervisor at headquarters is struggling to keep up with an increase of EPS (Events Per Second) being reported across the enterprise. What components should an administrator consider deploying to assist the supervisor with processing data?

A. Supervisor
B. Worker
C. Collector
D. Agent

Answer: B

NEW QUESTION 8
What operating system is FortiSIEM based on?

A. Cent OS
B. Microsoft Windows
C. RedHat
D. Ubuntu

Answer: A

NEW QUESTION 9
Which FortiSIEM components can do performance availability and performance monitoring?

A. Supervisor, worker, and collector
B. Supervisor and workers only
C. Supervisor only
D. Collectors only

Answer: A

NEW QUESTION 10
What is a prerequisite for a FortiSIEM supervisor with a worker deployment, using the proprietary flat file database?

A. The CMDB database must be on NFS
B. The event database must be on NFS
C. The event database must be on a local disk
D. The \archive mount must be on a local disk

Answer: B

NEW QUESTION 10
Which process converts Raw log data to structured data?

A. Data enrichment
B. Data classification
C. Data parsing
D. Data validation

Answer: C

NEW QUESTION 15
In the advanced analytical rules engine in FortiSIEM, multiple subpatterns can be referenced using which three operation?(Choose three.)

A. ELSE
B. NOT
C. FOLLOWED_BY
D. OR
E. AND

Answer: ABE

NEW QUESTION 19
Refer to the exhibit.

A FortiSIEM administrator wants to collect both SIEM event logs and performance and availability metrics (PAM) events from a Microsoft Windows server Which protocol should the administrator select in the Access Protocol drop-down list so that FortiSIEM will collect both SIEM and PAM events?

A. TELNET
B. WMI
C. LDAPS
D. LDAP start TLS

Answer: A

NEW QUESTION 23
Refer to the exhibit.

If events are grouped by Reporting IP, Event Type, and user attributes in FortiSIEM, how ,many results will be displayed?

A. Seven results will be displayed.
B. There results will be displayed.
C. Unique attribute cannot be grouped.
D. Five results will be displayed.

Answer: D

NEW QUESTION 28
To determine SNMP discovery issues, which is the best command from the backend?

A. snmpwalk
B. phSNMPTest
C. snmptest
D. ssh

Answer: A

NEW QUESTION 33
An administrator wants to search for events received from Linux and Windows agents.
Which attribute should the administrator use in search filters, to view events received from agents only.

A. External Event Receive Protocol
B. Event Received Proto Agents
C. External Event Receive Raw Logs
D. External Event Receive Agents

Answer: A

NEW QUESTION 37
Refer to the exhibit.

A FortiSIEM administrator wants to group some attributes for a report, but is not able to do so successfully.
As shown in the exhibit, why are some of the fields highlighted in red?

A. The Event Receive Time attribute is not available for logs.
B. The attribute COUNT(Matched event) is an invalid expression.

C. Unique attributes cannot be grouped.
D. No RAW Event Log attribute is available for devices.

Answer: C

NEW QUESTION 41
Which discovery scan type is prone to miss a device, if the device is quiet and the entry foe that device is not present in the ARP table of adjacent devices?

A. CMDB scan
B. L2 scan
C. Range scan
D. Smart scan

Answer: D

NEW QUESTION 44
What are the four possible incident status values?

A. Active, dosed, cleared, open
B. Active, cleared, cleared manually, system cleared
C. Active, closed, manual, resolved
D. Active, auto cleared, manual, false positive

Answer: C

NEW QUESTION 49
What is the best discovery scan option for a network environment where ping is disabled on all network devices?

A. Smart scan
B. Range scan
C. CMDB scan
D. L2 scan

Answer: A

NEW QUESTION 53
Which two FortiSIEM components work together to provide real-time event correlation?

A. Collector and Windows agent
B. Supervisor and worker
C. Worker and collector
D. Supervisor and collector

Answer: D

NEW QUESTION 57
......