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
In the rules engine, which condition instructs FortiSIEM to summarize and count the matching evaluated data?

A. Time Window
B. Aggregation
C. Group By
D. Filters

Answer: B

NEW QUESTION 3
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 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
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 6
An administrator defines SMTP as a critical process on a Linux server. If the SMTP process is stopped, FortiSIEM would generate a critical event with which event type?

A. PH_DEV_MON_PROC_STOP
B. Postfix-Mail-Slop
C. Generic_SMTP_Process_Exit
D. PH_DEV_MON_SMTP_STOP

Answer: A

NEW QUESTION 7
Refer to the exhibit.

A FortiSIEM is continuously receiving syslog events from a FortiGate firewall The FortiSlfcM administrator is trying to search the raw event logs for the last two hours that contain the keyword tcp . However, the administrator is getting no results from the search.
Based on the selected filters shown in the exhibit, why are there no search results?

A. The keyword is case sensitive Instead of typing TCP in the Value fiel
B. the administrator should type tcp.
C. In the Time section, the administrator selected the Relative Last option, and in the drop-down lists, selected 2 and Hours as the lime period The time period should be 24 hours.
D. The administrator selected - in the Operator column That a the wrong operator.
E. The administrator selected AND in the Next drop-down lis
F. This is the wrong boolean operator.

Answer: C

NEW QUESTION 8
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 9
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 10
Which command displays the Linux agent status?

A. Service fsm-linux-agent status
B. Service Ao-linux-agent status
C. Service fortisiem-linux-agent status
D. Service linux-agent status

Answer: C

NEW QUESTION 10
If an incident’s status is Cleared, what does this mean?

A. Two hours have passed since the incident occurred and the incident has not reoccurred.
B. A clear condition set on a rule was satisfied.
C. A security rule issue has been resolved.
D. The incident was cleared by an operator.

Answer: B

NEW QUESTION 11
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 14
Refer to the exhibit.

Three events are collected over a 10-minutc time period from two servers Server A and Server B. Based on the settings being used for the rule subpattern. how many incidents will the servers generate?

A. Server A will not generate any incidents and Server B will not generate any incidents
B. Server A will generate one incident and Server B wifl generate one incident
C. Server A will generate one incident and Server B will not generate any incidents
D. Server B will generate one incident and Server A will not generate any incidents

Answer: A

NEW QUESTION 19
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 20
Which two export methods are available for FortiSIEM analytics results? (Choose two.)

A. CSV
B. PNG
C. HTML
D. PDF

Answer: AD

NEW QUESTION 22
Refer to the exhibit.

The FortiSIEM administrator is examining events for two devices to investigate an issue However, the administrator is not getting any results from their search. Based on the selected fillers shown in the exhibit, why is the search returning no results?

A. Parenthesis are missing
B. The wrong boolean operator is selected in the Next column
C. The wrong option is selected in the Operator column
D. An invalid IP subnet is typed in the Value column

Answer: B

NEW QUESTION 26
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 30
What protocol can be used to collect Windows event logs in an agentless method?

A. SSH
B. SNMP
C. WMI
D. SMTP

Answer: C

NEW QUESTION 33
Refer to the exhibit.

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

A. Eight results will be displayed
B. Four results will be displayed
C. Two results will be displayed

D. Unique attributes cannot be grouped

Answer: D

NEW QUESTION 37
If the reported packet loss is between 50% and 98%. which status is assigned to the device in the Availability column of summary dashboard?

A. Down status is assigned because of packet loss.
B. Up status is assigned because of received packets
C. Critical status is assigned because of reduction in number of packets received
D. Degraded status is assigned because of packet loss

Answer: D

NEW QUESTION 40
......