Fortinet.NSE5_FSM-5.2.v2022-06-28.q20

Exam Code:	NSE5_FSM-5.2
Exam Name:	Fortinet NSE 5 - FortiSIEM 5.2
Certification Provider:	Fortinet
Free Question Number:	20
Version:	v2022-06-28
# of views:	764
# of Questions views:	200
https://www.freeqas.com/qa/Fortinet/NSE5_FSM-5.2/Fortinet.NSE5_FSM-5.2.v2022-06-28.q20.html	

NEW QUESTION: 1
Which protocol is almost always required for the FortiSIEM GUI discovery process?
A. SNMP
B. WMI
C. Syslog
D. Telnet
Answer: A (LEAVE A REPLY)

NEW QUESTION: 2
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. The wrong option is selected in the Operator column

B. An invalid IP subnet is typed in the Value column
C. The wrong boolean operator is selected in the Next column
D. Parenthesis are missing
Answer: C (LEAVE A REPLY)

NEW QUESTION: 3
Which three ports can be used to send Syslogs to FortiSIEM? (Choose three.)
A. UDP 514
B. TCP 514
C. UDP9999
D. UDP 162
E. TCP 1470
Answer: (SHOW ANSWER)

NEW QUESTION: 4
If a performance rule is triggered repeatedly due to high CPU use. what occurs m the incident table?
A. The incident status changes to Repeated and the First Seen and Last Seen times are updated.
B. A new incident is created each time the rule is triggered, and the First Seen and Last Seen times are updated.
C. The Incident Count value increases, and the First Seen and Last Seen tomes update
D. A new incident is created based on the Rule Frequency value, and the First Seen and Last Seen times are updated
Answer: B (LEAVE A REPLY)

NEW QUESTION: 5
If an incident's status is Cleared, what does this mean?
A. The incident was cleared by an operator.
B. Two hours have passed since the incident occurred and the incident has not reoccurred.
C. A clear condition set on a rule was satisfied.
D. A security rule issue has been resolved.
Answer: C (LEAVE A REPLY)

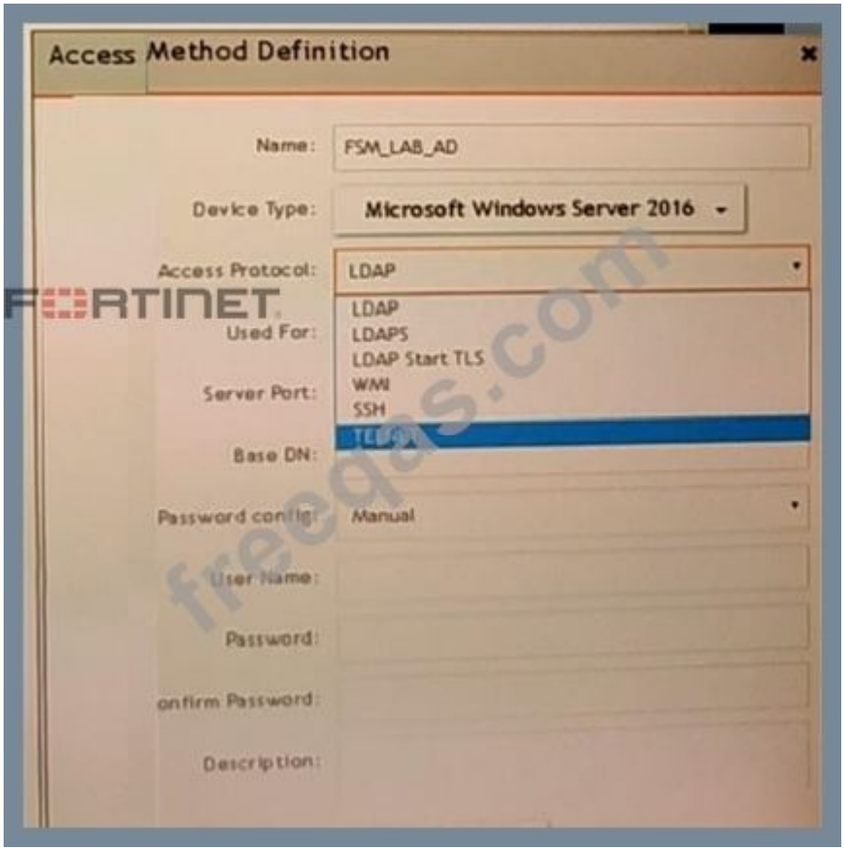
NEW QUESTION: 6
What is a prerequisite for a FortiSIEM supervisor with a worker deployment, using the proprietary flat file database?
A. The event database must be on a local disk
B. The \archive mount must be on a local disk
C. The event database must be on NFS
D. The CMDB database must be on NFS
Answer: C (LEAVE A REPLY)

NEW QUESTION: 7
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. No RAW Event Log attribute is available for devices.
B. Unique attributes cannot be grouped.
C. The attribute COUNT(Matched event) is an invalid expression.
D. The Event Receive Time attribute is not available for logs.
Answer: (SHOW ANSWER)

NEW QUESTION: 8
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 Raw Logs
B. Event Received Proto Agents
C. External Event Receive Agents
D. External Event Receive Protocol
Answer: (SHOW ANSWER)

NEW QUESTION: 9
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. WMI

B. TELNET

C. LDAP start TLS

D. LDAPS

Answer: (SHOW ANSWER)

NEW QUESTION: 10

Which process converts Raw log data to structured data?

A. Data classification

B. Data enrichment

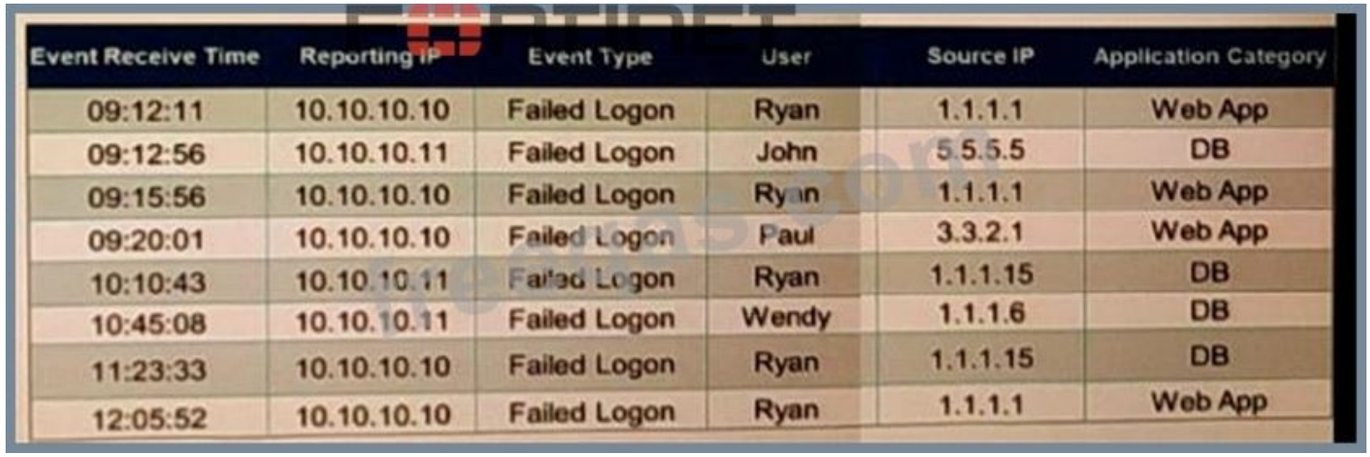
C. Data parsing

D. Data validation

Answer: (SHOW ANSWER)

NEW QUESTION: 11

Refer to the exhibit.



Event Receive Time	Reporting IP	Event Type	User	Source IP	Application Category
09:12:11	10.10.10.10	Failed Logon	Ryan	1.1.1.1	Web App
09:12:56	10.10.10.11	Failed Logon	John	5.5.5.5	DB
09:15:56	10.10.10.10	Failed Logon	Ryan	1.1.1.1	Web App
09:20:01	10.10.10.10	Failed Logon	Paul	3.3.2.1	Web App
10:10:43	10.10.10.11	Failed Logon	Ryan	1.1.1.15	DB
10:45:08	10.10.10.11	Failed Logon	Wendy	1.1.1.6	DB
11:23:33	10.10.10.10	Failed Logon	Ryan	1.1.1.15	DB
12:05:52	10.10.10.10	Failed Logon	Ryan	1.1.1.1	Web App

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

A. Unique attributes cannot be grouped

B. Four results will be displayed

C. Two results will be displayed

D. Eight results will be displayed

Answer: (SHOW ANSWER)

NEW QUESTION: 12

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. UI Access

C. Data Conditions

Answer: C (LEAVE A REPLY)

NEW QUESTION: 13

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 Raw Logs

B. External Event Receive Agents

C. External Event Receive Protocol

D. Event Received Proto Agents

Answer: C (LEAVE A REPLY)

NEW QUESTION: 14

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

A. 32GB RAM

B. 24GB RAM
C. 16GB RAM
D. 64GB RAM
Answer: B (LEAVE A REPLY)

NEW QUESTION: 15
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 generate one incident and Server B wifl generate one incident
B. Server A will not generate any incidents and Server B will not generate any incidents
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: (SHOW ANSWER)

NEW QUESTION: 16
Refer to the exhibit.

What do the yellow stars listed in the Monitor column indicate?

A. A yellow star indicates that a metric was applied during discovery, but FortiSIEM is unable to collect data.
B. A yellow star indicates that a metric was applied during discovery, and data has been collected successfully
C. A yellow star indicates that a metric was applied during discovery, but data collection has not started
D. A yellow star indicates that a metric was not applied during discovery and, therefore, FortiSEIM was unable to collect data.
Answer: (SHOW ANSWER)

NEW QUESTION: 17
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. No RAW Event Log attribute is available for devices.
B. The Event Receive Time attribute is not available for logs.
C. Unique attributes cannot be grouped.
D. The attribute COUNT(Matched event) is an invalid expression.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 18

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 B will generate one incident and Server A will not generate any incidents

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

Answer: (SHOW ANSWER)

NEW QUESTION: 19

Refer to the exhibit.

Event Receive Time	Reporting IP	Event Type	User	Source IP	Application Category
09:12:11	10.10.10.10	Failed Logon	Ryan	1.1.1.1	Web App
09:12:56	10.10.10.11	Failed Logon	John	5.5.5.5	DB
09:15:56	10.10.10.10	Failed Logon	Ryan	1.1.1.1	Web App
09:20:01	10.10.10.10	Failed Logon	Paul	3.3.2.1	Web App
10:10:43	10.10.10.11	Failed Logon	Ryan	1.1.1.15	DB
10:45:08	10.10.10.11	Failed Logon	Wendy	1.1.1.6	DB
11:23:33	10.10.10.10	Failed Logon	Ryan	1.1.1.15	DB
12:05:52	10.10.10.10	Failed Logon	Ryan	1.1.1.1	Web App

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

A. There results will be displayed.

B. Seven results will be displayed.

C. Unique attribute cannot be grouped.

D. Five results will be displayed.

Answer: (SHOW ANSWER)

NEW QUESTION: 20
Which command displays the Linux agent status?
A. Service fortisiem-linux-agent status
B. Service linux-agent status
C. Service fsm-linux-agent status
D. Service Ao-linux-agent status
Answer: A (LEAVE A REPLY)