VCEûp

Fortinet.Pre.NSE5_FSM-5.2.42q - DEMO

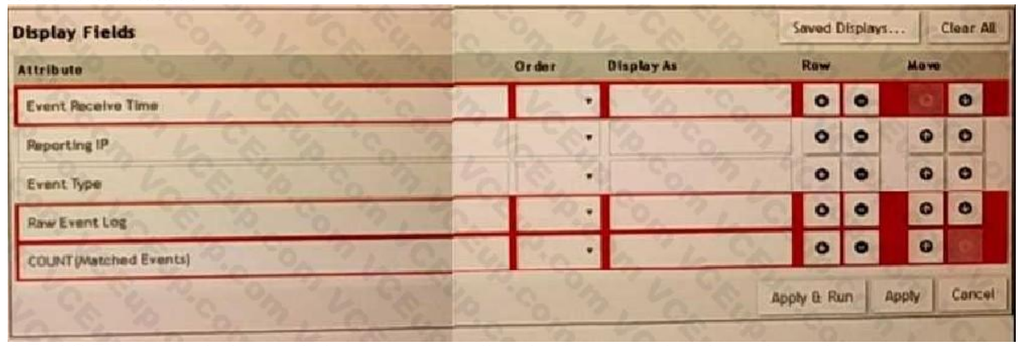
Number: NSE5_FSM-5.2
Passing Score: 800
Time Limit: 120 min
File Version: 1.0

Exam Code: NSE5_FSM-5.2
Exam Name: Fortinet NSE 5 - FortiSIEM 5.2
Website: https://VCEup.com/

VCEûp

VCEûp

QUESTION 1
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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
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. Seven results will be displayed.
B. There results will be displayed.
C. Unique attribute cannot be grouped.
D. Five results will be displayed.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

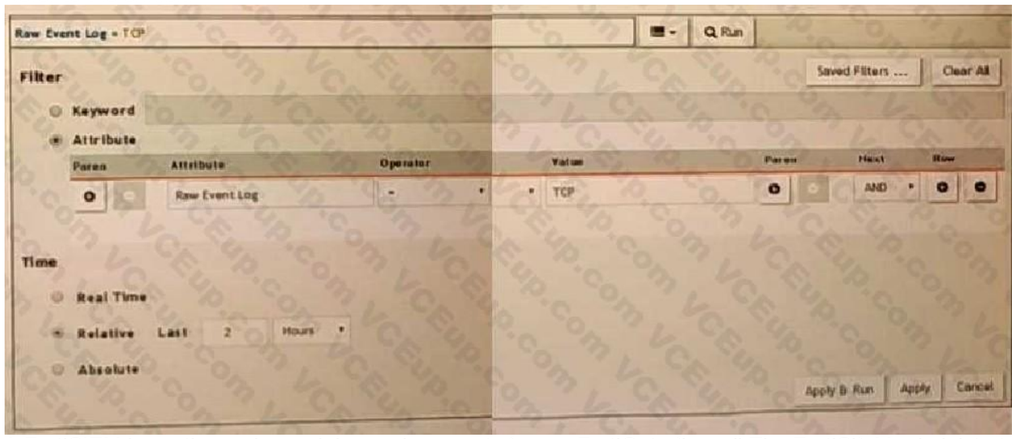
QUESTION 6
If an incident's status is Cleared, what does this mean?

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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
Refer to the exhibit.



A FortiSIEM is continuously receiving syslog events from a FortiGate firewall The FortiSIfcM 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 field. the administrator should type tcp.
B. 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.
C. The administrator selected - in the Operator column That a the wrong operator.
D. The administrator selected AND in the Next drop-down list. This is the wrong boolean operator.

Correct Answer: C
Section: (none)
Explanation

VCEûp

Explanation/Reference:

QUESTION 8
Which FortiSIEM components are capable of performing device discovery?

A. FortiSIEM Windows agent
B. Worker
C. FortiSIEM Linux agent
D. Collector

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
Refer to the exhibit.

An administrator is trying to identify an issue using an expression bated on the Expression Builder settings shown in the exhibit however, the error message shown in the exhibit indicates that the expression is invalid.
Which is the correct expression?

A. Matched Events COUNT()
B. Matched Events(COUNT)
C. COUNT(Matched Events)
D. (COUNT) Matched Events

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

VCEUp

QUESTION 11
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

Correct Answer: CDE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
In the advanced analytical rules engine in FortiSIEM, multiple subpatterms can be referenced using which three operation?(Choose three.)

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

Correct Answer: ABE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
Device discovery information is stored in which database?

A. CMDB
B. Profile DB
C. Event DB
D. SVN DB

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
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

Correct Answer: A

VCEûp

Section: (none)
Explanation

Explanation/Reference:

QUESTION 15
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

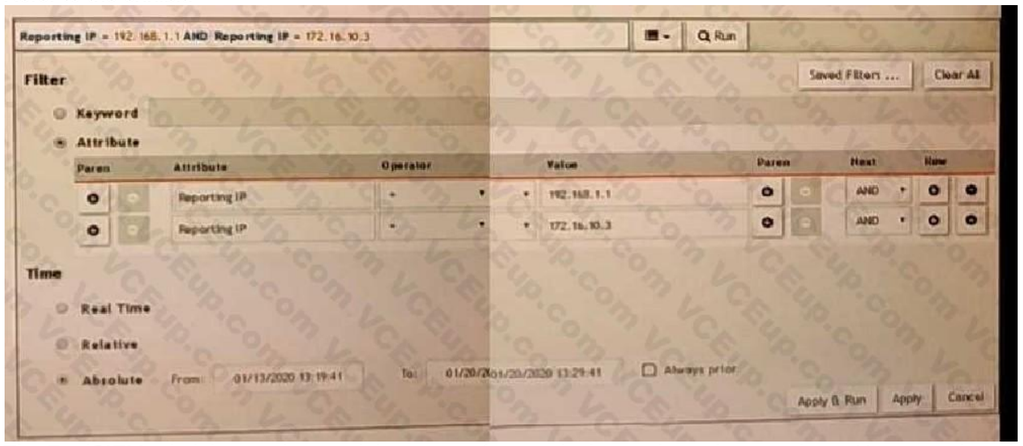
QUESTION 16
Which command displays the Linux agent status?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17
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

VCEUp

C. The wrong option is selected in the Operator column
D. An invalid IP subnet is typed in the Value column

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

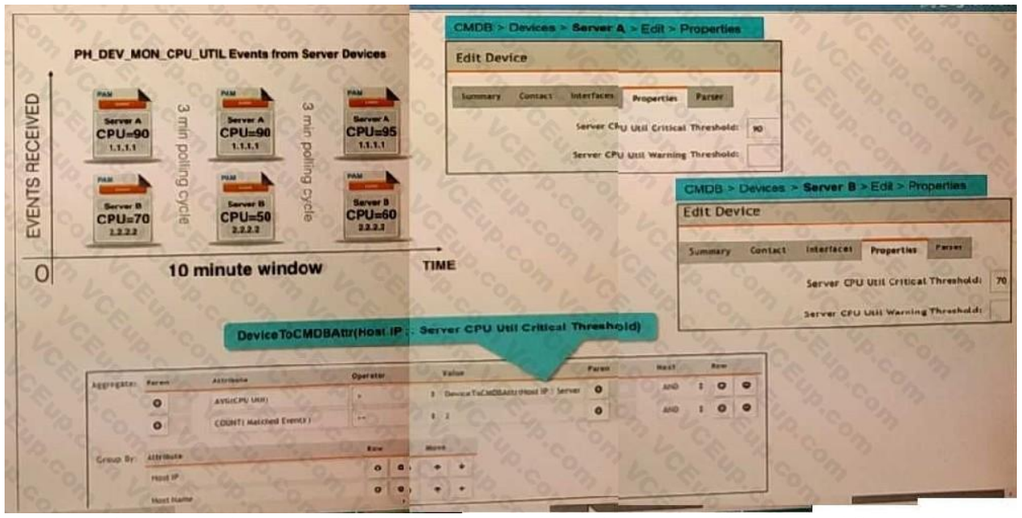
QUESTION 19
What are the four possible incident status values?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
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. Eight results will be displayed
B. Four results will be displayed
C. Two results will be displayed
D. Unique attributes cannot be grouped

Correct Answer: D
Section: (none)
Explanation

VCEUp

Explanation/Reference:

QUESTION 22
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, and data has been collected successfully
B. A yellow star indicates that a metric was applied during discovery, but data collection has not started
C. A yellow star indicates that a metric was applied during discovery, but FortiSIEM is unable to collect data.
D. A yellow star indicates that a metric was not applied during discovery and, therefore, FortiSEIM was unable to collect data.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
What are the four categories of incidents?

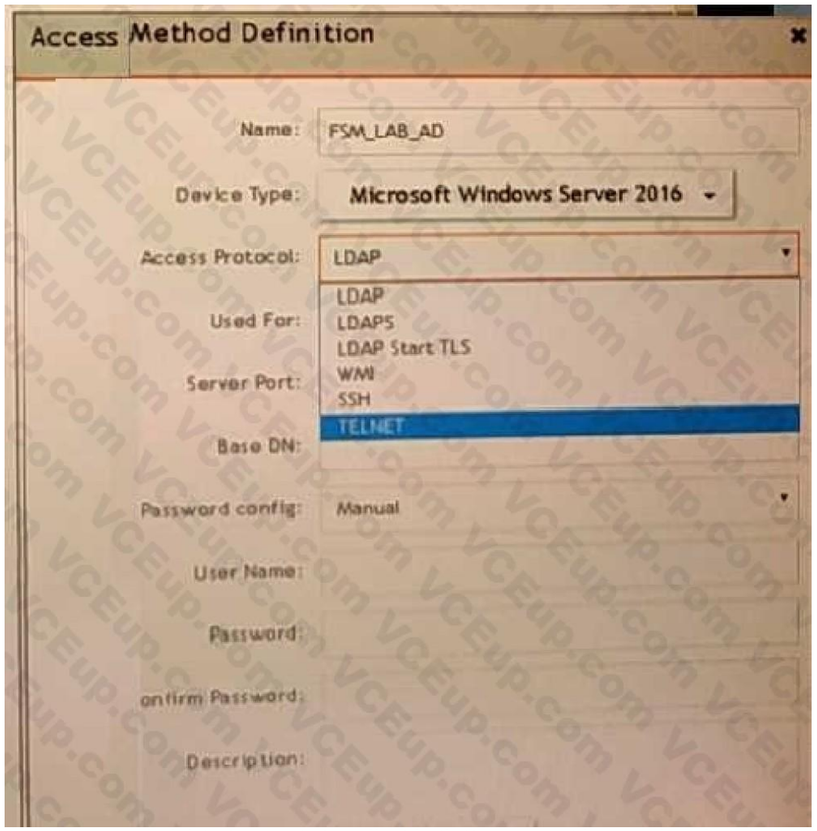
A. Devices, users, high risk, and low risk
B. Performance, availability, security, and change
C. Performance, devices, high risk, and low risk
D. Security, change, high risk, and low risk

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
Refer to the exhibit.

VCEûp



VCEûp

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
In FotiSIEM enterprise licensing mode, if the link between the collector and data center FortiSIEM cluster a down what happens?

A. The collector drops incoming events like syslog. but slops performance collection
B. The collector continues performance collection of devices, but stops receiving syslog
C. The collector buffers events
D. The collector processes stop, and events are dropped

Correct Answer: D
Section: (none)
Explanation

VCEUp

Explanation/Reference:

QUESTION 26
Which database is used for storing anomaly data, that is calculated for different parameters, such as traffic and device resource usage running averages, and standard deviation values?

A. Profile DB
B. Event DB
C. CMDB
D. SVN DB

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
Which process converts Raw log data to structured data?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
What is a prerequisite for FortiSIEM Linux agent installation?

A. The web server must be installed on the Linux server being monitored
B. The auditd service must be installed on the Linux server being monitored
C. The Linux agent manager server must be installed.
D. Both the web server and the audit service must be installed on the Linux server being monitored

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
If a performance rule is triggered repeatedly due to high CPU use. what occurs m the incident table?

A. A new incident is created each time the rule is triggered, and the First Seen and Last Seen times are updated.
B. The incident status changes to Repeated and the First Seen and Last Seen times are updated.
C. A new incident is created based on the Rule Frequency value, and the First Seen and Last Seen times are updated
D. The Incident Count value increases, and the First Seen and Last Seen tomes update

Correct Answer: A
Section: (none)
Explanation

VCEUp

Explanation/Reference:

QUESTION 30
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32
Which two export methods are available for FortiSIEM analytics results? (Choose two.)

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

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33
What are the minimum memory requirements for the FortiSIEM supervisor virtual appliance, when the proprietary flat file database is used?

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

Correct Answer: D

VCEûp

Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
To determine whether or not syslog is being received from a network device, which is the best command from the backend?

A. tcpdump
B. phDeviceTest
C. netcat
D. phSyslogRecorder

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35
Which protocol is almost always required for the FortiSIEM GUI discovery process?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 36
What is the best discovery scan option for a network environment where ping is disabled on all network devices?

A. Smartscan
B. Rangescan
C. CMDBscan
D. L2 scan

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 37
Which item is required to register a FortiSIEM appliance license?

A. Staticstorage
B. StaticMACaddress
C. StaticIPaddress
D. Static Hardware ID

VCEûp

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38
To determine SNMP discovery issues, which is the best command from the backend?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39
What operating system is FortiSIEM based on?

A. CentOS
B. MicrosoftWindows
C. RedHat
D. Ubuntu

VCEûp

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40
What protocol can be used to collect Windows event logs in an agentless method?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 41
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

VCEûp

D. Agent

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42
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. CMDBReportConditions
B. DataConditions
C. UI Access

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

VCEûp