NSE5_FSM-5.2 Q&As

Fortinet NSE 5 - FortiSIEM 5.2

Pass Fortinet NSE5_FSM-5.2 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/nse5_fsm-5-2.html

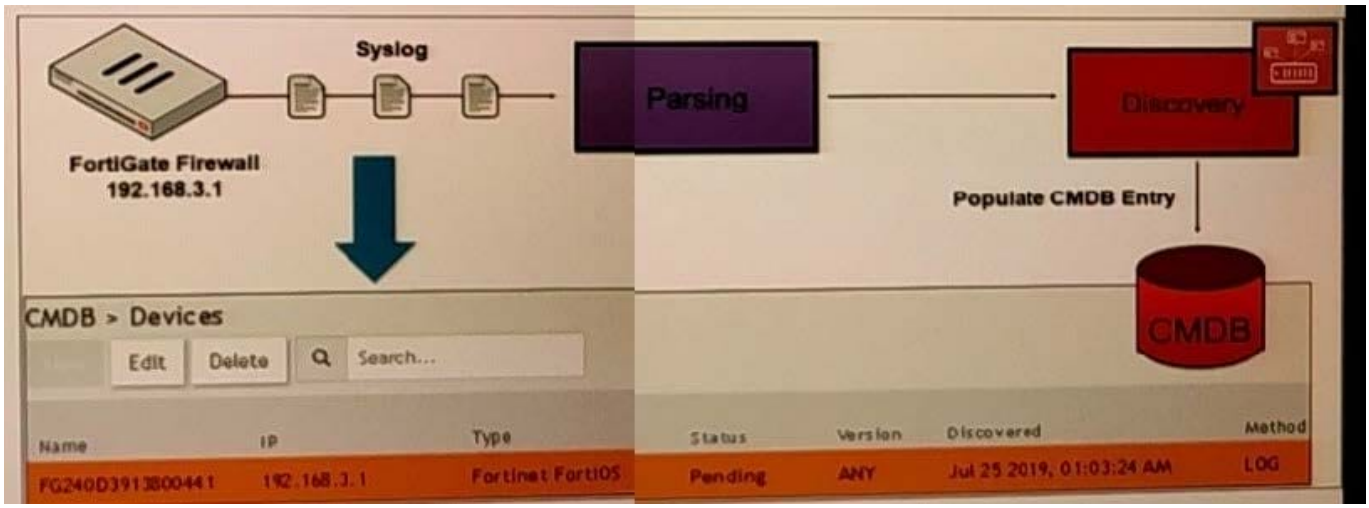
100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Fortinet Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Refer to the exhibit.



How was the FortiGate device discovered by FortiSIEM?

A. Through GUI log discovery

B. Through syslog discovery

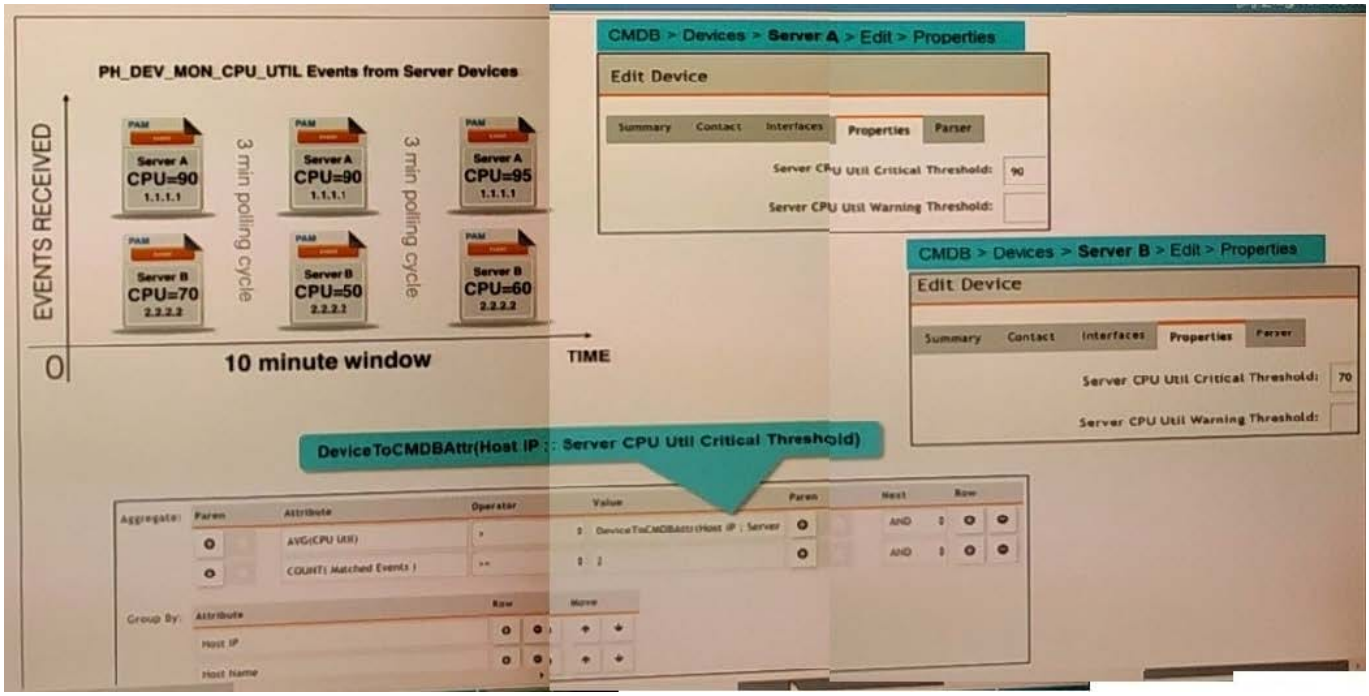
C. Using the pull events method

D. Through auto log discovery

Correct Answer: A

QUESTION 2

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

QUESTION 3

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: BDE

QUESTION 4

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

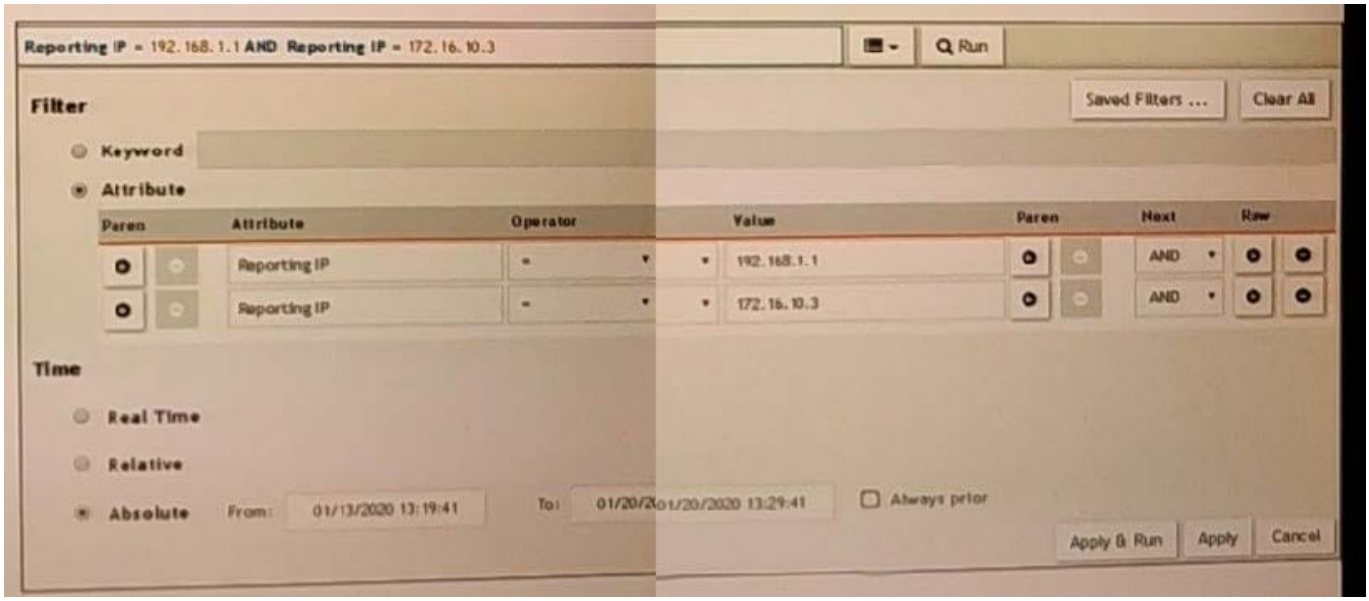
C. The Linux agent manager server must be installed.

D. Both the web server and the audit service must be installed on the Linux server being monitored

Correct Answer: D

QUESTION 5

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

Correct Answer: D

QUESTION 6

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

QUESTION 7

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

A. CSV

B. PNG

C. HTML

D. PDF

Correct Answer: AD

QUESTION 8

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.

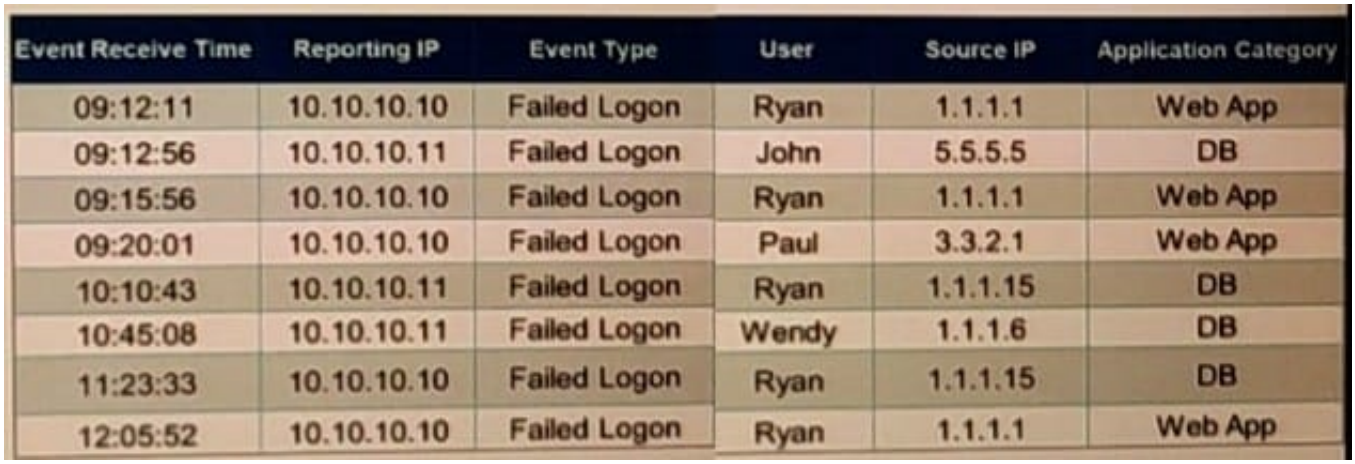
C. A new incident is created based on the Rule Frequency value, and the First Seen and Last Seen times are updated

D. The Incident Count value increases, and the First Seen and Last Seen tomes update

Correct Answer: A

QUESTION 9

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

QUESTION 10

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: D