

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

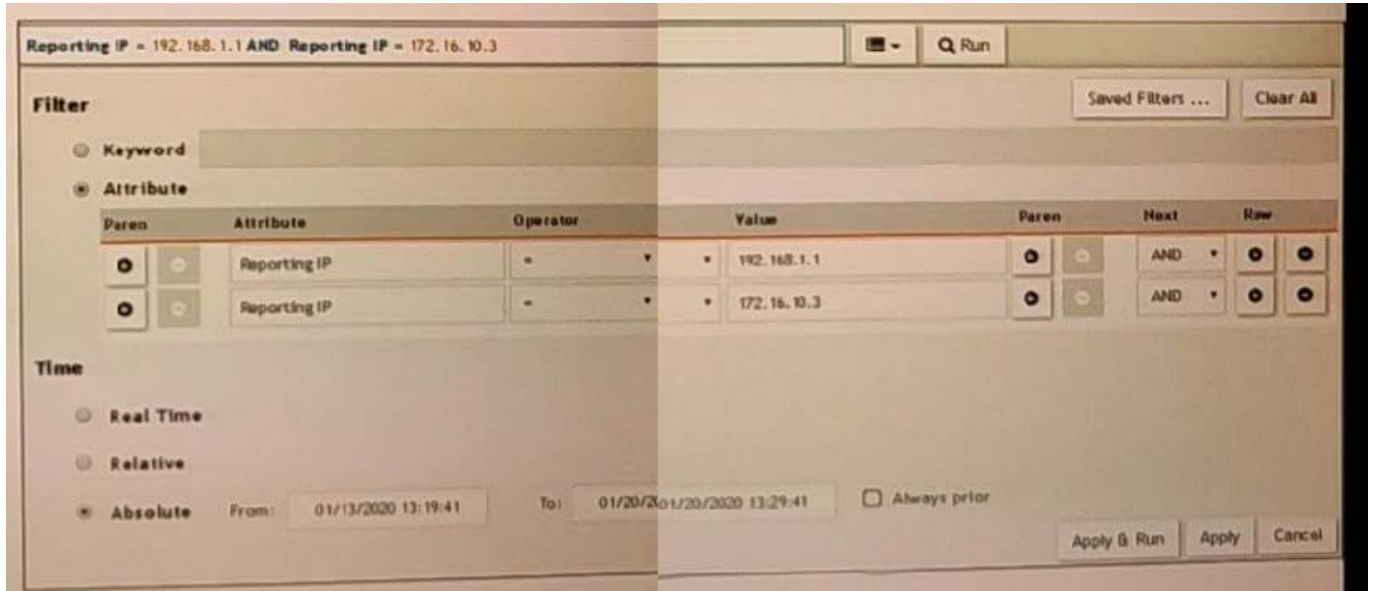
Following Questions and Answers are all new published by Fortinet Official Exam Center

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



QUESTION 1

Refer to the exhibit.



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 filters 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 2

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. Three results will be displayed.
- C. Unique attribute cannot be grouped.
- D. Five results will be displayed.

Correct Answer: D

QUESTION 3

Device discovery information is stored in which database?

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

Correct Answer: A

QUESTION 4

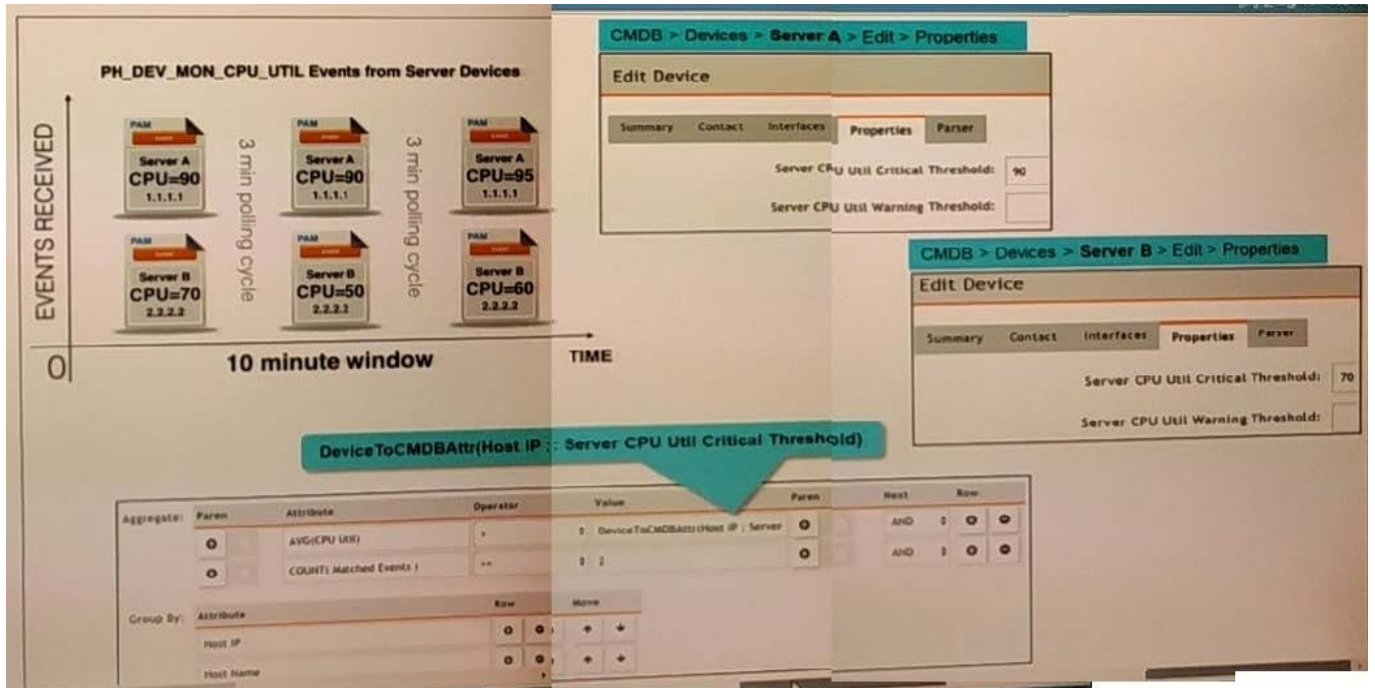
Which process converts Raw log data to structured data?

- A. Data enrichment
- B. Data classification
- C. Data parsing

D. Data validation
 Correct Answer: D

QUESTION 5

Refer to the exhibit.



Three events are collected over a 10-minute 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 will 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

[NSE5 FSM-5.2 PDF Dumps](#)

[NSE5 FSM-5.2 Practice Test](#)

[NSE5 FSM-5.2 Exam Questions](#)