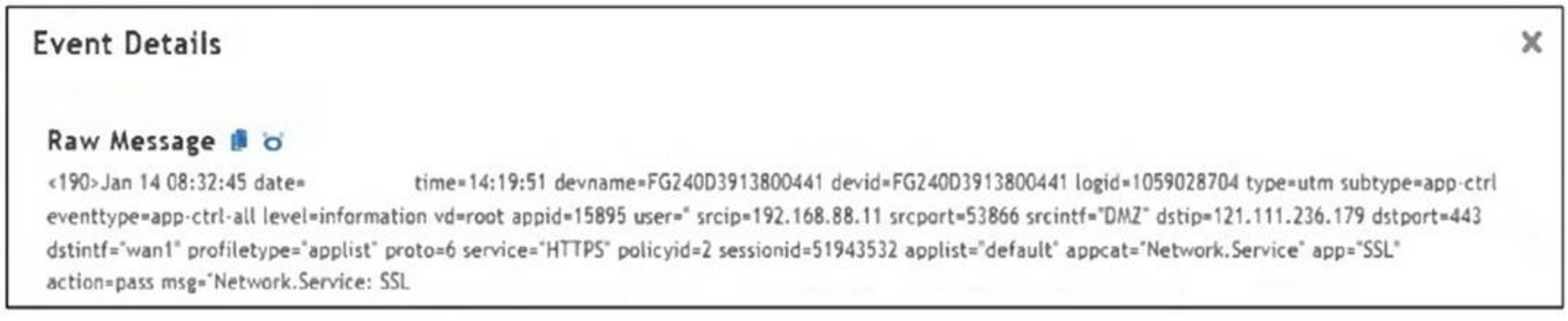
Fortinet

Exam Questions FCP_FSM_AN-7.2

FCP - FortiSIEM 7.2 Analyst

NEW QUESTION 1
Refer to the exhibit.

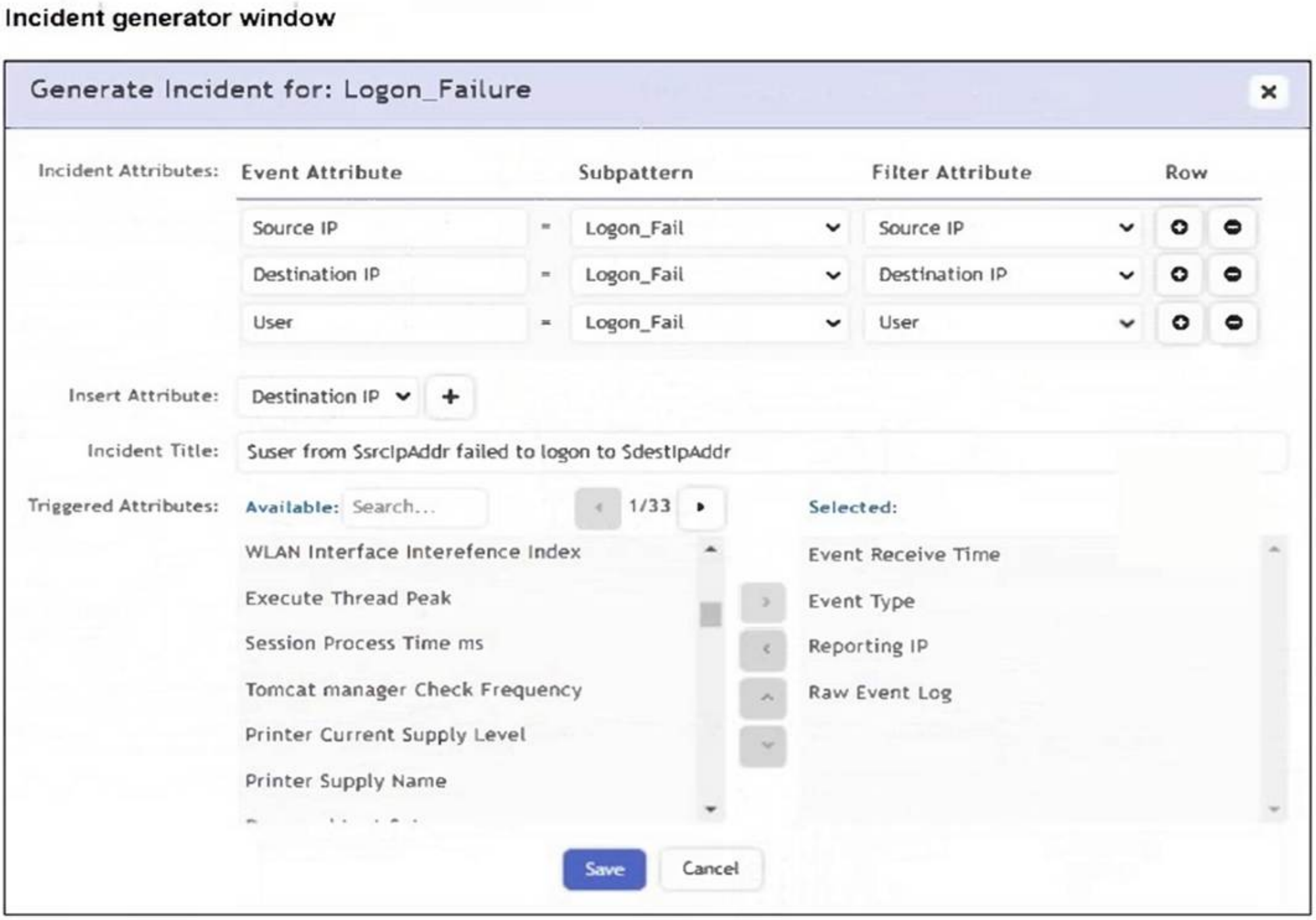


Which value would you expect the FortiSIEM parser to use to populate the Application Name field?

A. applist
B. Network.Service
C. SSL
D. wan1

Answer: C

NEW QUESTION 2
Refer to the exhibit.



An analyst is trying to generate an incident with a title that includes the Source IP, Destination IP, User, and Destination Host Name. They are unable to add a Destination Host Name as an incident attribute.
What must be changed to allow the analyst to select Destination Host Name as an attribute?

A. The Destination Host Name must be selected as a Triggered Attribute.
B. The Destination Host Name must be set as an aggregate item in a subpattern.
C. The Destination Host Name must be added as an Event type in the FortiSIEM.
D. The Destination IP Event Attribute must be removed.

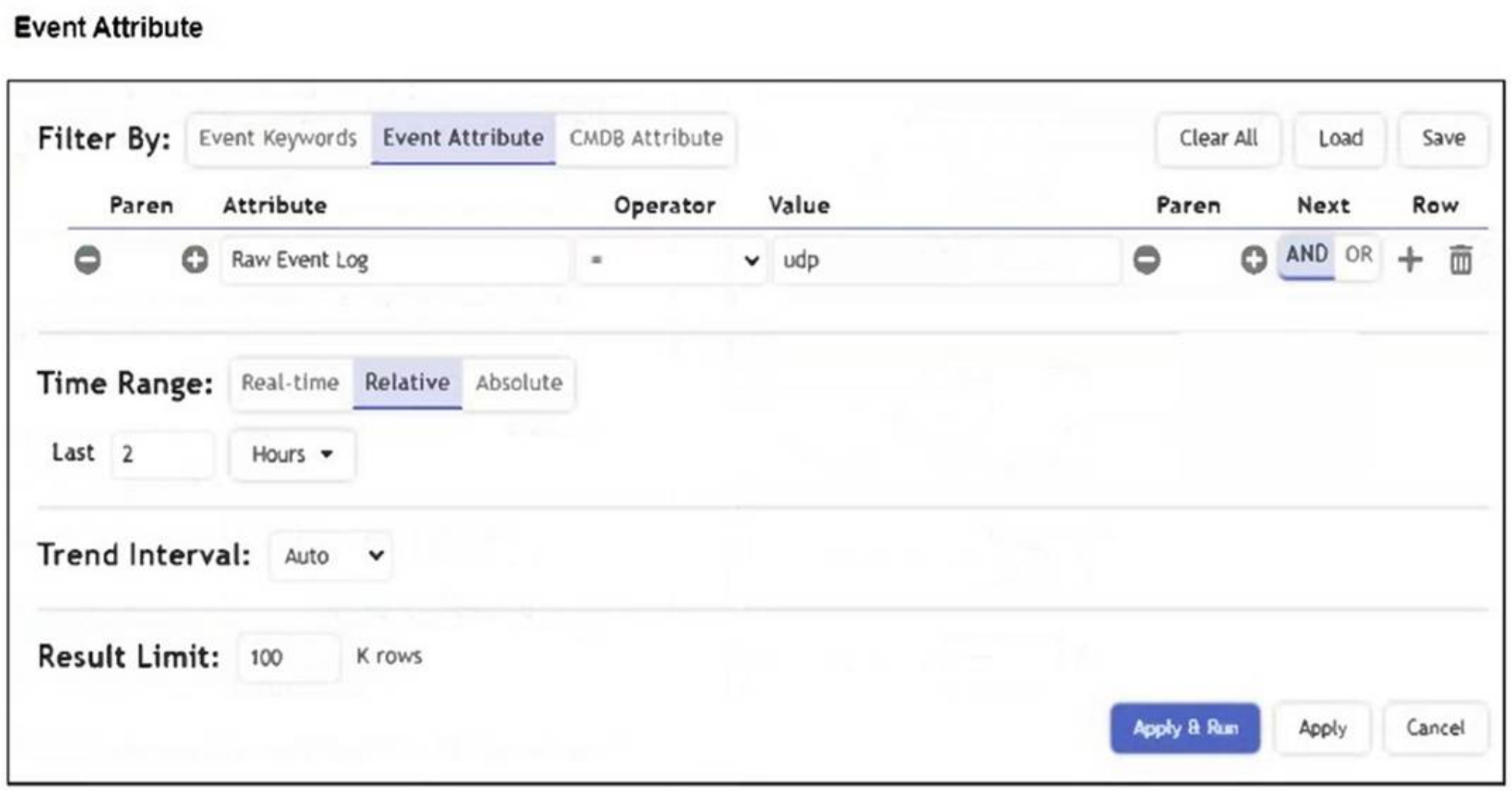
Answer: A

NEW QUESTION 3
Which statement about thresholds is true?

A. FortiSIEM uses fixed, hardcoded global and device thresholds for all performance metrics.
B. FortiSIEM uses only device thresholds for security metrics.
C. FortiSIEM uses global and per device thresholds for performance metrics.
D. FortiSIEM uses only global thresholds for performance metrics.

Answer: C

NEW QUESTION 4
Refer to the exhibit.



A FortiSIEM device is receiving syslog events from a FortiGate firewall. The FortiSIEM analyst is trying to search the raw event logs for the last two hours that contain the keyword "udp". However, they are getting no results from the search, which they know should be available. Based on the filter shown in the exhibit, why are there no search results?

A. The analyst selected AND in the Next colum
B. This is the wrong Boolean operator.
C. The Time Range value should be set to Real-Time.
D. The keyword is case sensitiv
E. Instead of typing udp in the Value field, the analyst should type UDP.
F. The analyst selected = in the Operator colum
G. That is the wrong operator.

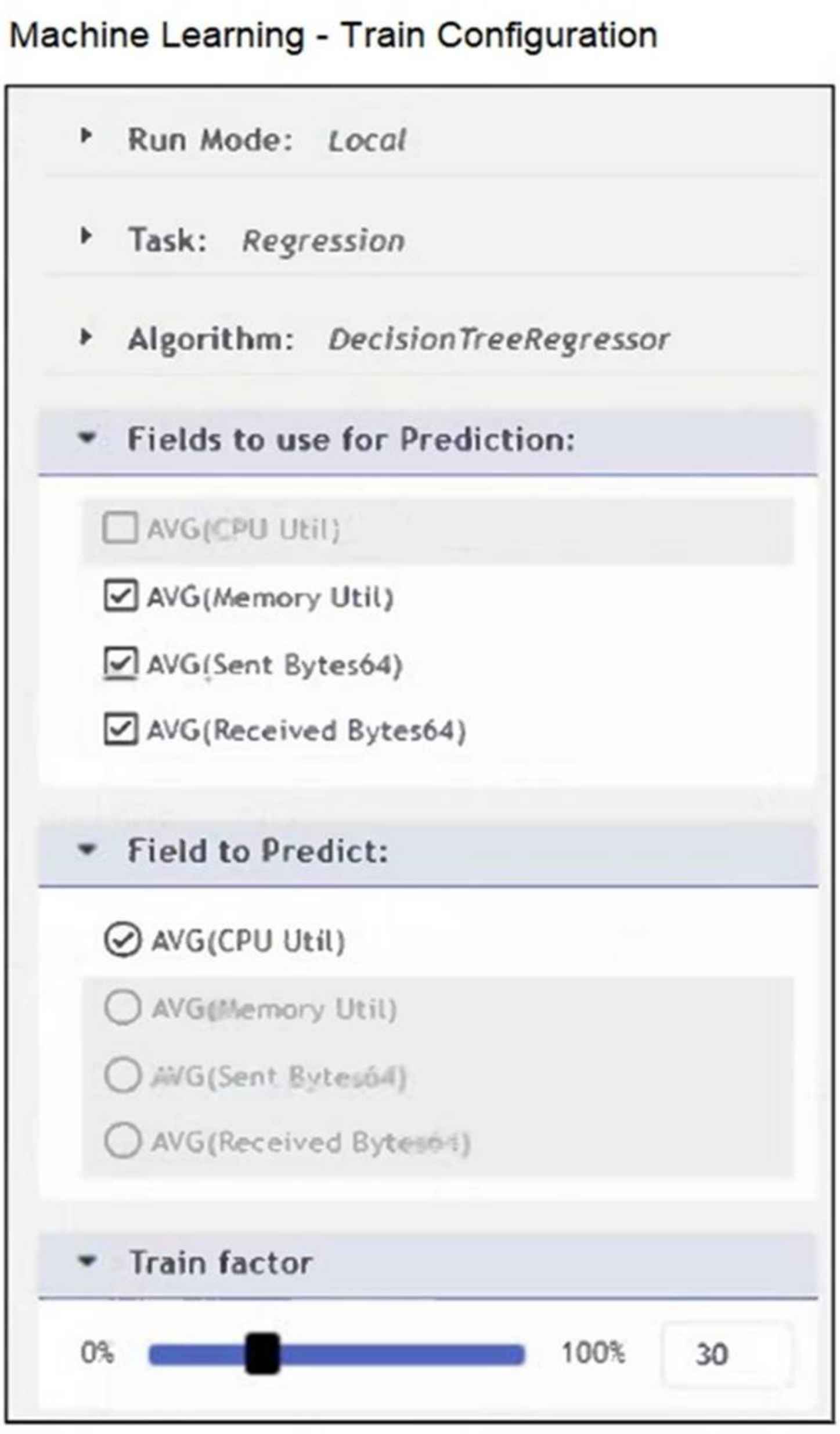
Answer: D

NEW QUESTION 5
Which analytics search can be used to apply a user and entity behavior analytics (UEBA) tag to an event for a failed login by the user JSmith?

A. User = smith
B. Username NOT END WITH jsmith
C. User IS jsmith
D. Username CONTAIN smit

Answer: D

NEW QUESTION 6
Refer to the exhibit.



The configuration shown in the exhibit is incorrect.
What must you change to allow this configuration to be successfully applied to FortiSIEM?

A. The Train factor must be 70% or greater.
B. Run Mode must be set to ML.
C. Only one AVG type field must be selected under Fields to use for Prediction.
D. The selection in Fields to use for Prediction and Field to Predict must match.

Answer: A

NEW QUESTION 7

How can you query the configuration management database (CMDB) in an analytics search?

A. Click Value > Select from CMDB.
B. On the CMDB tab, select an entry, and then click Create Search.
C. On the Admin tab, click CMDB Search.
D. Click Attribute > Select from CMDB.

Answer: A

NEW QUESTION 8
Which items are used to define a subpattern?

A. Filters, Aggregate, Group By definitions
B. Filters, Aggregate, Time Window definitions
C. Filters, Group By, Threshold definitions
D. Filters, Threshold, Time Window definitions

Answer: A

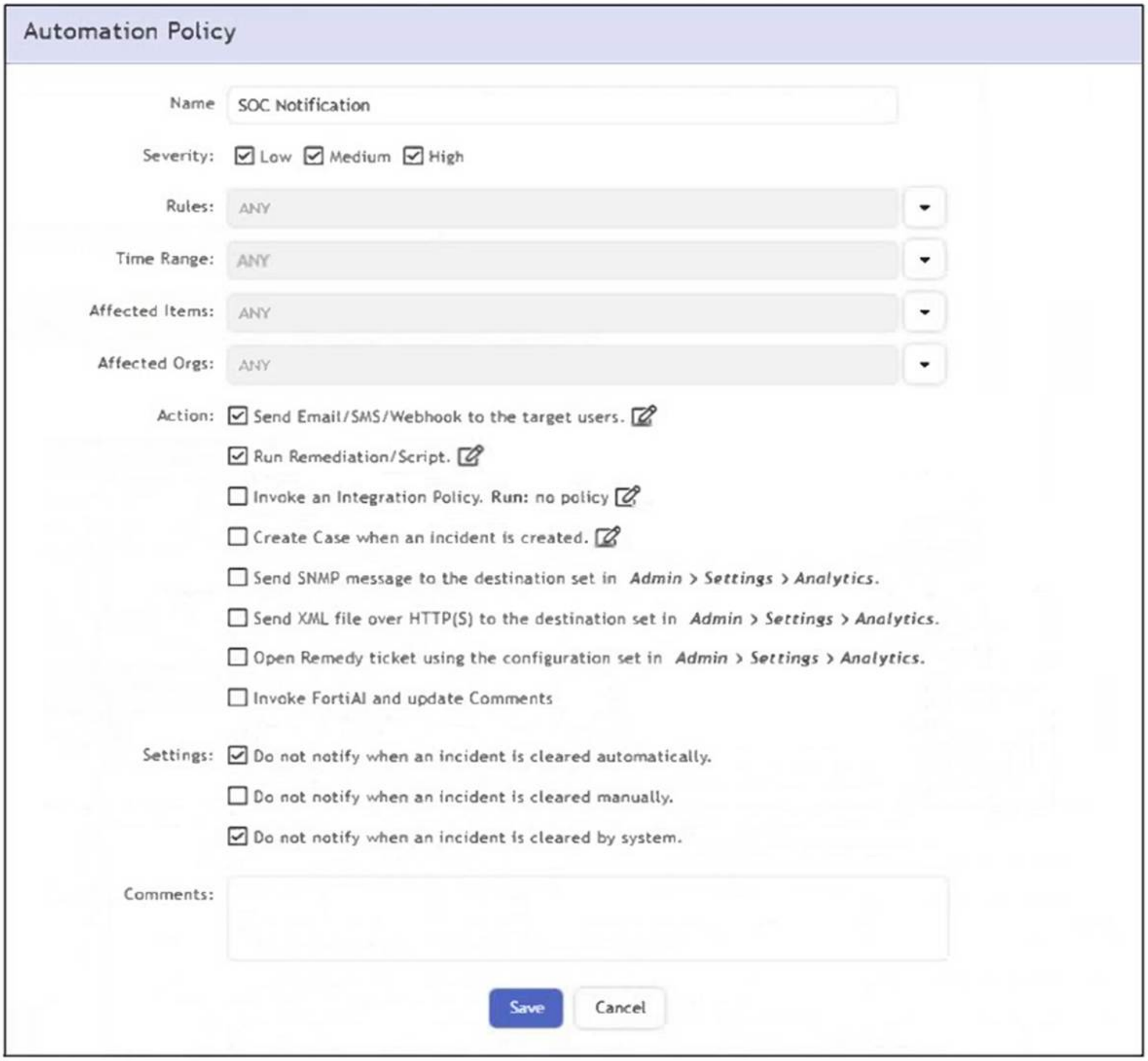
Explanation:
A subpattern in FortiSIEM is defined using Filters to match specific events, Aggregate conditions to apply statistical thresholds (e.g., COUNT), and Group By attributes to segment data for evaluation. These three components collectively determine how the subpattern functions.

NEW QUESTION 9
Which two settings must you configure to allow FortiSIEM to apply tags to devices in FortiClient EMS? (Choose two.)

A. FortiEMS API credentials defined on FortiSIEM
B. Remediation script configured
C. ZTNA tags defined on FortiSIEM
D. FortiSIEM API credentials defined on FortiEMS\

Answer: AC

NEW QUESTION 10
Refer to the exhibit.



What happens when an analyst clears an incident generated by a rule containing the automation policy shown in the exhibit?

A. No notification is sent.
B. An email is sent to the SOC manager.
C. The remediation script is run.
D. A notification is sent to the SOC manager dashboard.

Answer: B

NEW QUESTION 10
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

FCP_FSM_AN-7.2 Practice Exam Features:

* FCP_FSM_AN-7.2 Questions and Answers Updated Frequently

* FCP_FSM_AN-7.2 Practice Questions Verified by Expert Senior Certified Staff

* FCP_FSM_AN-7.2 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* FCP_FSM_AN-7.2 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year