Fortinet FCP_FSM_AN-7.2 Exam Price | New FCP_FSM_AN-7.2 Exam Experience

P.S. Free 2026 Fortinet FCP_FSM_AN-7.2 dumps are available on Google Drive shared by DumpsActual: https://drive.google.com/open?id=1Q1j-DDA9PVRq3o8cSHBb2FGdShgG8UtK

At DumpsActual, we strive hard to offer a comprehensive FCP - FortiSIEM 7.2 Analyst (FCP_FSM_AN-7.2) exam questions preparation material bundle pack. The product available at DumpsActual includes FCP - FortiSIEM 7.2 Analyst (FCP_FSM_AN-7.2) real dumps pdf and mock tests (desktop and web-based). Practice exams give an experience of taking the FCP - FortiSIEM 7.2 Analyst (FCP_FSM_AN-7.2) actual exam.

Fortinet FCP_FSM_AN-7.2 Exam Syllabus Topics:

Topic	Details
Topic 1	• Analytics: This section of the exam measures the skills of Security Analysts and covers the foundational techniques for building and refining queries. It focuses on creating searches from events, applying grouping and aggregation methods, and performing various lookup operations, including CMDB and nested queries to effectively analyze and correlate data.
Topic 2	• Incidents, notifications, and remediation: This section of the exam measures the skills of Incident Responders and encompasses the entire incident management lifecycle. This includes the skills required to manage and prioritize security incidents, configure policies for alert notifications, and set up automated remediation actions to contain and resolve threats.
Topic 3	• Rules and subpatterns: This section of the exam measures the skills of SOC Engineers and focuses on the construction and implementation of analytics rules. It involves identifying the different components that make up a rule, utilizing advanced features like subpatterns and aggregation, and practically configuring these rules within the FortiSIEM platform to detect security events.
Topic 4	• Machine learning, UEBA, and ZTNA: This section of the exam measures the skills of Advanced Security Architects and covers the integration of modern security technologies. It involves performing configuration tasks for machine learning models, incorporating UEBA (User and Entity Behavior Analytics) data into rules and dashboards for enhanced threat detection, and understanding how to integrate ZTNA (Zero Trust Network Access) principles into security operations.

>> Fortinet FCP_FSM_AN-7.2 Exam Price <<

New FCP_FSM_AN-7.2 Exam Experience, Pdf FCP_FSM_AN-7.2 Pass Leader

There is no denying that no exam is easy because it means a lot of consumption of time and effort. Especially for the upcoming FCP_FSM_AN-7.2 exam, although a large number of people to take the exam every year, only a part of them can pass. If you are also worried about the exam at this moment, please take a look at our FCP_FSM_AN-7.2 Study Materials, whose content is

carefully designed for the FCP_FSM_AN-7.2 exam, rich question bank and answer to enable you to master all the test knowledge in a short period of time.

Fortinet FCP - FortiSIEM 7.2 Analyst Sample Questions (Q11-Q16):

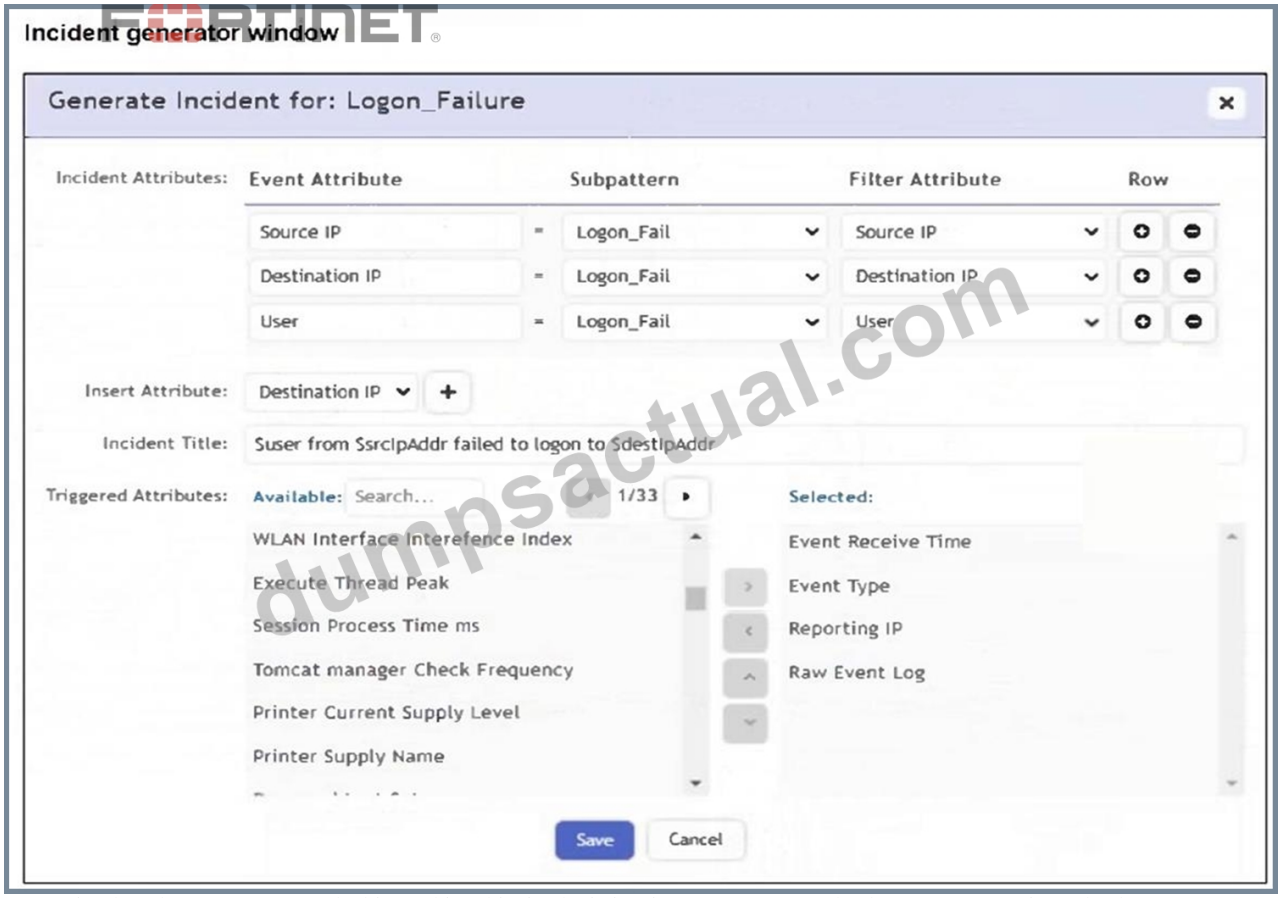
NEW QUESTION # 11
Which statement about thresholds is true?

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

Answer: C

Explanation:
FortiSIEM evaluates performance metrics against both global thresholds, which apply system-wide, and per-device thresholds, which can be customized for individual devices. This dual approach allows flexibility in monitoring while ensuring consistent baseline alerting.

NEW QUESTION # 12
Refer to the exhibit.



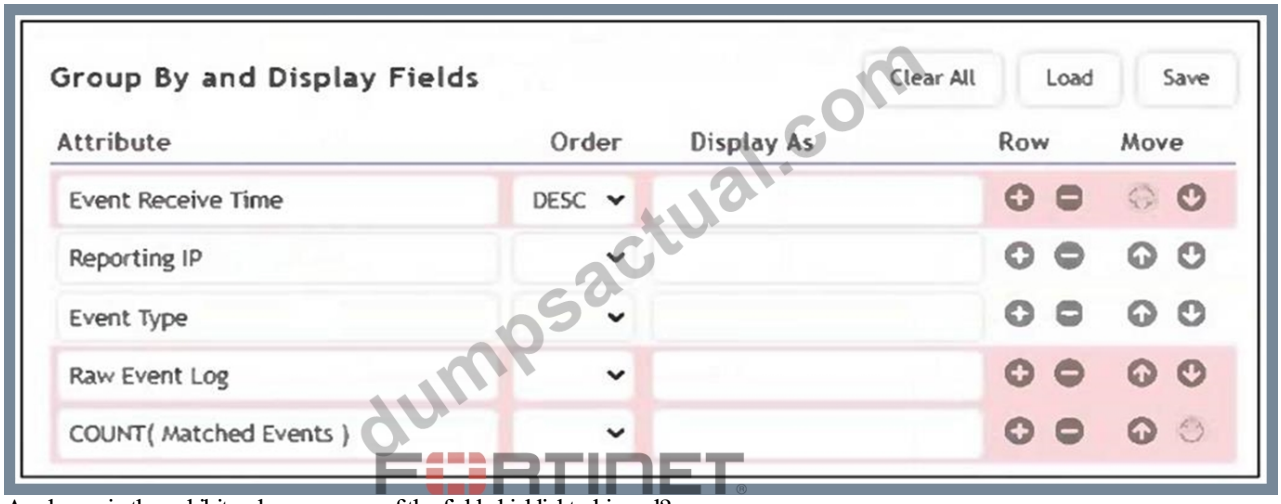
An analyst is trying to generate an incident with a title that includes the Source IP, Destination IP, User, and Destination Host Name. They are unable to add a Destination Host Name as an incident attribute.
What must be changed to allow the analyst to select Destination Host Name as an attribute?

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

Answer: B

Explanation:
For an attribute like Destination Host Name to be used in the incident title, it must first be included in the Triggered Attributes list. Only attributes listed there are available for substitution in the title template (e.g., $destIpAddr, $srcIpAddr).

NEW QUESTION # 13
Refer to the exhibit.



As shown in the exhibit, why are some of the fields highlighted in red?

- A. No RAW Event Log attribute information is available.
- B. Unique values cannot be grouped B.
- C. The Event Receive Time attribute is not available for logs.
- D. The attribute COUNT(Matched Events) is an invalid expression.

Answer: B

Explanation:
The fields are highlighted in red because unique values such as Event Receive Time and Raw Event Log cannot be used in group-by operations. Grouping requires aggregatable or consistent values across events, while these fields are unique to each event, making them incompatible for grouping.

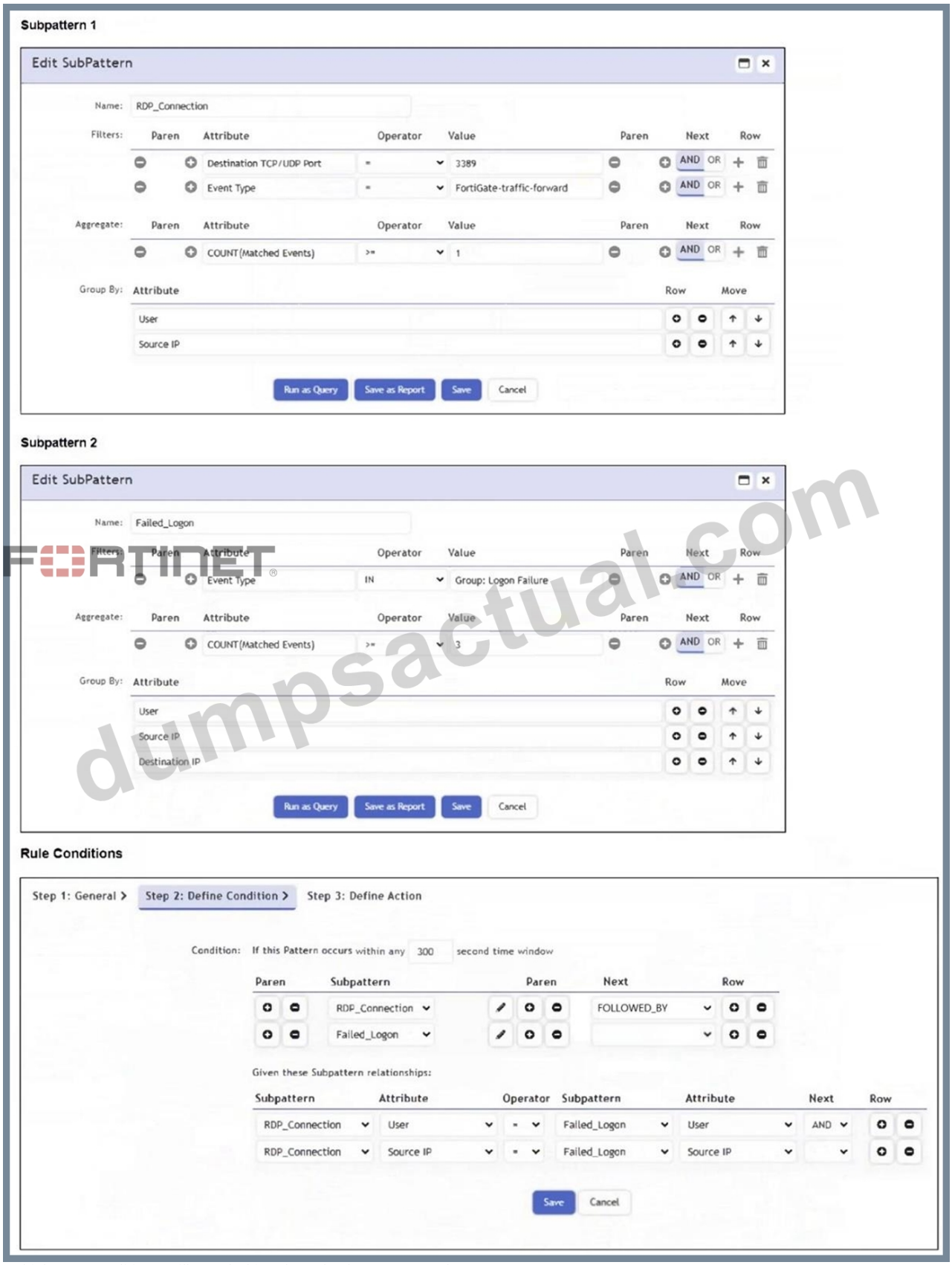
NEW QUESTION # 14
Which information can FortiSIEM retrieve from FortiClient EMS through an API connection?

- A. FortiSIEM license
- B. ZTNA tags
- C. Host login credentials
- D. Host software versions

Answer: B

Explanation:
FortiSIEM can retrieve ZTNA tags from FortiClient EMS through an API connection, enabling dynamic user and device classification for policy enforcement and incident response.

NEW QUESTION # 15
Refer to the exhibit.



Which two conditions will match this rule and subpatterns? (Choose two.)

- A. A user connects to the wrong IP address for an RDP session five times.
- B. A user using RDP over SSL VPN fails to log in to an application five times.
- C. A user fails twice to log in when connecting through RDP.
- D. A user runs a brute force password cracker against an RDP server.

Answer: B,D

Explanation:
The user initiates an RDP session (Subpattern 1) and then fails to log in multiple times (Subpattern 2 with COUNT(Matched Events) >= 3) - both from the same Source IP and User within 300 seconds.
The brute force attempts typically involve a successful RDP connection followed by multiple failed logins, satisfying the sequence and grouping conditions in the rule.

NEW QUESTION # 16
.....

We learned that a majority of the candidates for the exam are office workers or students who are occupied with a lot of things, and do not have plenty of time to prepare for the FCP_FSM_AN-7.2 exam. So we have tried to improve the quality of our training materials for all our worth. Now, I am proud to tell you that our training materials are definitely the best choice for those who have been yearning for success but without enough time to put into it. There are only key points in our FCP_FSM_AN-7.2 Training Materials. That is to say, you can pass the FCP_FSM_AN-7.2 exam as well as getting the related certification only with the minimum of time and efforts under the guidance of our training materials.