更新する-便利なFCP_FSM_AN-7.2テスト内容試験-試験の準備方法FCP_FSM_AN-7.2日本語版サンプル

P.S. JPTestKingがGoogle Driveで共有している無料かつ新しいFCP_FSM_AN-7.2ダンプ：https://drive.google.com/open?id=1FX13CqmKx1nb34PaHmT2cB0Cx95AoAOA

JPTestKingのFCP_FSM_AN-7.2問題集の超低い価格に反して、 JPTestKingに提供される問題集は最高の品質を持っています。そして、もっと重要なのは、JPTestKingは質の高いサービスを提供します。望ましい問題集を支払うと、あなたはすぐにそれを得ることができます。JPTestKingのサイトはあなたが最も必要なもの、しかもあなたに最適な試験参考書を持っています。FCP_FSM_AN-7.2問題集を購入してから、また一年間の無料更新サービスを得ることもできます。一年以内に、あなたが持っている資料を更新したい限り、JPTestKingは最新バージョンのFCP_FSM_AN-7.2問題集を捧げます。JPTestKingはあなたに最大の利便性を与えるために全力を尽くしています。

Fortinet FCP_FSM_AN-7.2 Exam Overview:

Certification Vendor:	Fortinet
Exam Name:	FCP - FortiSIEM 7.2 Analyst
Exam Number:	FCP_FSM_AN-7.2
Available Languages:	English, Japanese
Passing Score:	Pass/Fail
Related Certifications:	Fortinet Certified Professional Security Operations

Exam Format:	Multiple Choice, Multiple Select, Scenario-based
Exam Price:	USD 200
Exam Duration:	60 minutes
Real Exam Qty:	30–35
Certificate Validity Period:	2 years
Recommended Training:	Fortinet Official Training: FortiSIEM 7.2 Analyst
Exam Registration:	Pearson VUE
Sample Questions:	Fortinet FCP_FSM_AN-7.2 Sample Questions
Exam Way:	Online proctored or onsite testing center
Pre Condition:	No mandatory prerequisites; recommended: basic SIEM knowledge, security fundamentals, hands-on FortiSIEM experience
Official Syllabus URL:	https://www.fortinet.com/training-certification/certifications/fcp-fortisiem-7-2-analyst

>> FCP_FSM_AN-7.2テスト内容 <<

検証するFCP_FSM_AN-7.2テスト内容 & 合格スムーズFCP_FSM_AN-7.2日本語版サンプル | 有難いFCP_FSM_AN-7.2的中関連問題

進歩を遂げ、FCP_FSM_AN-7.2トレーニング資料の証明書を取得することは、当然のことながら、最新の最も正確な知識を指揮する最も専門的な専門家によるものです。それが、FCP - FortiSIEM 7.2 Analyst試験準備が市場の大部分を占める理由です。それに、FCP_FSM_AN-7.2練習教材の利益を待つのではなく、支払い後すぐにダウンロードできるので、今すぐ成功への旅を始めましょう。

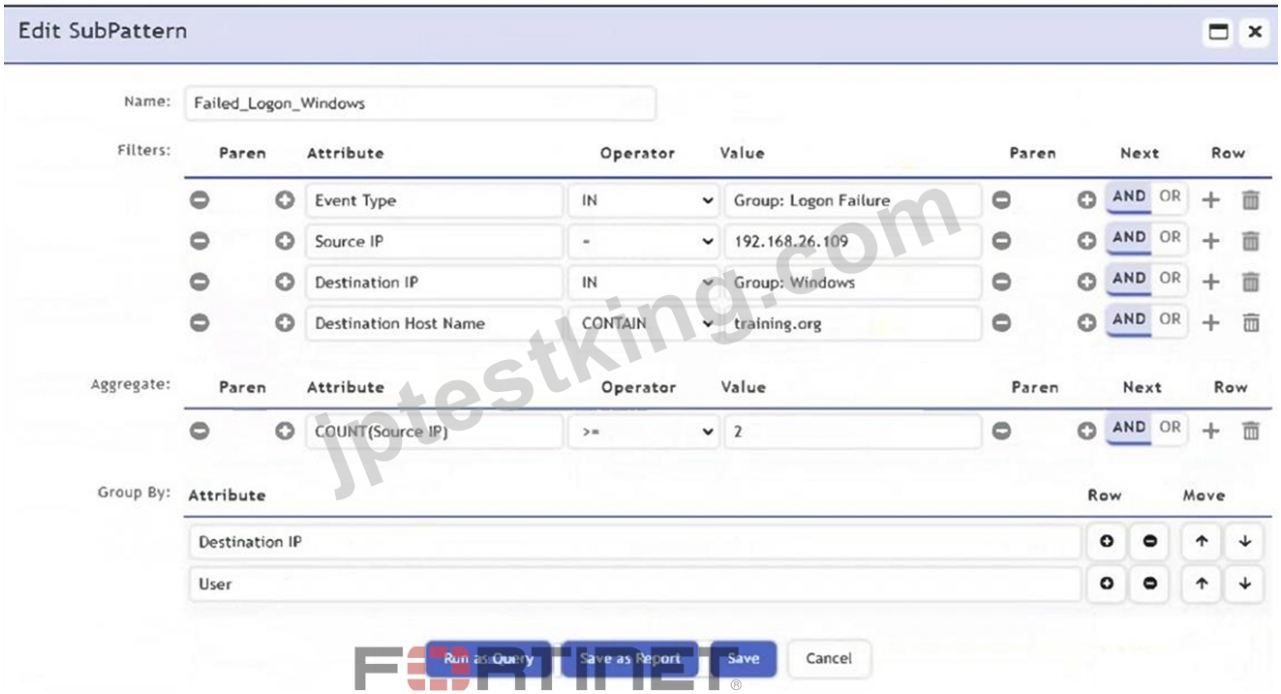
Fortinet FCP_FSM_AN-7.2 認定試験の出題範囲:

トピック	出題範囲
トピック 1	• 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.
トピック 2	• 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.
トピック 3	• 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.
トピック 4	• 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.

Fortinet FCP - FortiSIEM 7.2 Analyst 認定 FCP_FSM_AN-7.2 試験問題 (Q28-Q33):

質問 # 28
Refer to the exhibit.

SubPattern edit window



An analyst is troubleshooting the rule shown in the exhibit. It is not generating any incidents, but the filter parameters are generating events on the Analytics tab.
What is wrong with the rule conditions?

- A. The Destination Host Name value is not fully qualified.
- B. The Aggregate attribute is too restrictive.
- C. The Event Type refers to a CMDB lookup and should be an Event lookup.
- D. The Group By attributes restricts which events are counted.

正解：D

解説：
The Group By attributes - Destination IP and User - cause the aggregation (COUNT(Source IP) >= 2) to apply within each unique combination of those groupings. This restricts the count calculation and can prevent the rule from triggering incidents, even if matching events exist in the Analytics tab.

質問 # 29
What are the four incident status values on FortiSIEM?

- A. Active, cleared, cleared manually, false positive
- B. Active, auto closed, cleared manually, resolved
- C. Active, auto cleared, cleared manually, system cleared
- D. Active, closed, cleared, resolved

正解：C

解説：
FortiSIEM incidents can have four status values: Active, Auto Cleared, Cleared Manually, and System Cleared. These statuses track the lifecycle of an incident-from detection (Active) to resolution - whether it's cleared automatically by correlation logic or manually by an analyst.

質問 # 30
Refer to the exhibit.

Event Attribute

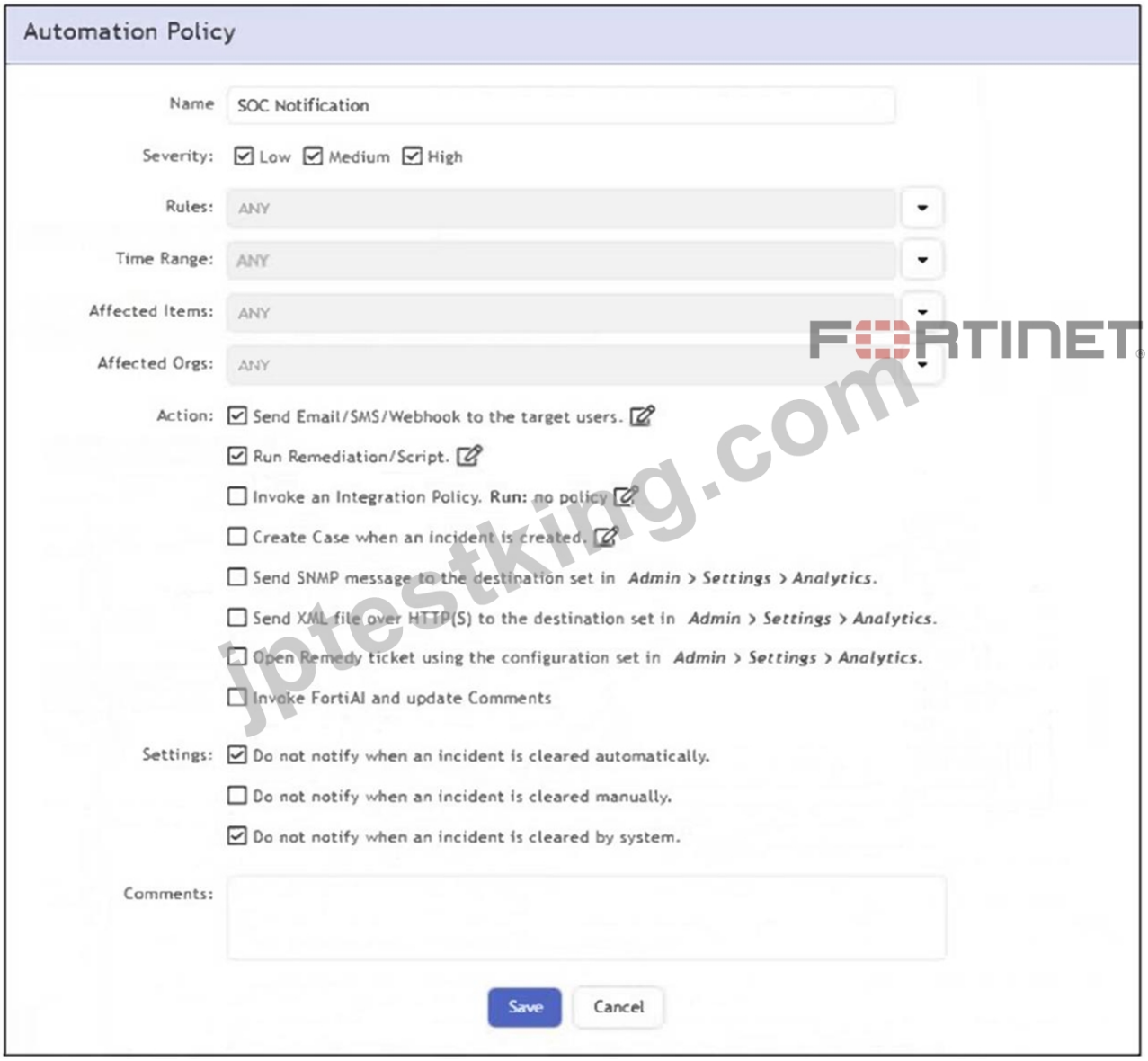
A FortiSIEM device is receiving syslog events from a FortiGate firewall. The FortiSIEM analyst is trying to search the raw event logs for the last two hours that contain the keyword "udp". However, they are getting no results from the search, which they know should be available. Based on the filter shown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

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

正解：C

解説：
The operator is set to "=", which performs an exact match on the entire raw event log, not a substring search. To find logs that contain the keyword "udp", the analyst should use the CONTAIN operator instead. This will return all logs where "udp" appears anywhere in the raw log message.

質問 # 31
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. A notification is sent to the SOC manager dashboard.
- D. The remediation script is run.

正解：A

解説：
The automation policy has the option "Do not notify when an incident is cleared manually" enabled. Therefore, when an analyst manually clears an incident, no notification or automation action is triggered.

質問 # 32
Refer to the exhibit. What does the Define Condition time field determine for this rule?

- A. How often the rule will evaluate the subpattern(s).
- B. The time of day the rule will trigger.
- C. The time period over which the rule evaluates events.
- D. How often the rule will perform remediation.

正解：C

質問 # 33
.....