FORTINET FCP_FSM_AN-7.2

Fortinet FortiSIEM Analyst Certification Questions & Answers

Exam Summary – Syllabus – Questions

FCP_FSM_AN-7.2

Fortinet Certified Professional - Security Operations

32 Questions Exam – Duration of 60 minutes

Table of Contents:

Know Your FCP_FSM_AN-7.2 Certification Well:

The FCP_FSM_AN-7.2 is best suitable for candidates who want to gain knowledge in the Fortinet Security Operations. Before you start your FCP_FSM_AN-7.2 preparation you may struggle to get all the crucial FortiSIEM Analyst materials like FCP_FSM_AN-7.2 syllabus, sample questions, study guide.

But don't worry the FCP_FSM_AN-7.2 PDF is here to help you prepare in a stress free manner.
The PDF is a combination of all your queries like-

- What is in the FCP_FSM_AN-7.2 syllabus?
- How many questions are there in the FCP_FSM_AN-7.2 exam?
- Which Practice test would help me to pass the FCP_FSM_AN-7.2 exam at the first attempt?

Passing the FCP_FSM_AN-7.2 exam makes you Fortinet Certified Professional - Security Operations. Having the FortiSIEM Analyst certification opens multiple opportunities for you. You can grab a new job, get a higher salary or simply get recognition within your current organization.

Fortinet FCP_FSM_AN-7.2 FortiSIEM Analyst Certification Details:

Exam Name	Fortinet FCP - FortiSIEM 7.2 Analyst
Exam Code	FCP_FSM_AN-7.2
Exam Price	$200 USD
Duration	60 minutes
Number of Questions	32
Passing Score	Pass / Fail
Recommended Training	**FortiSIEM Analyst**
Exam Registration	**PEARSON VUE**
Sample Questions	**Fortinet FCP_FSM_AN-7.2 Sample Questions**

Practice Exam	Fortinet Certified Professional - Security Operations Practice Test

FCP_FSM_AN-7.2 Syllabus:

Section	Objectives
Analytics	- Build queries from search results and events - Apply group by and data aggregation on search results - Perform CMDB and lookup table queries - Perform nested query lookups
Rules and subpatterns	- Identify various rule components - Utilize rule subpatterns, aggregation, and group by - Configure FortiSIEM analytics rules
Incidents, notifications, and remediation	- Manage incidents - Configure notification policies - Configure remediation options
Machine learning, UEBA, and ZTNA	- Configure machine learning configuration tasks - Integrate UEBA data into rules and dashboards - Describe how to integrate ZTNA into FortiSIEM operations

Fortinet FCP_FSM_AN-7.2 Sample Questions:

Question: 1

Which two attributes can you not select together in the Group By and Display Fields?

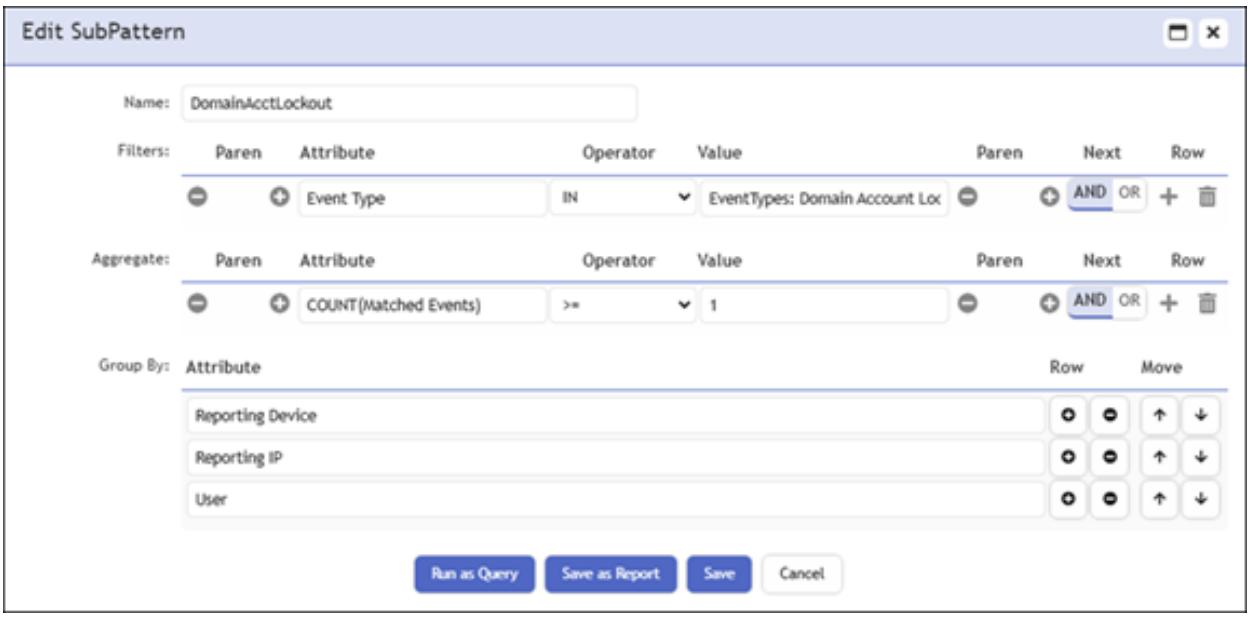
(Choose two.)

a) Source IP
b) Raw Event Log
c) Destination IP
d) Event Reporting Time
e) Reporting IP

Answer: b, c

Question: 2

Refer to the exhibit.



Which section contains settings that determine which attribute associations are used to trigger an incident?

a) Name
b) Aggregate
c) Filters
d) Group By

Answer: d

Question: 3

Which two elements can you use to define how an automation policy activates?

(Choose two.)

a) Lookup table
b) Rules
c) Watchlist
d) Time range

Answer: b, d

Question: 4

When using user and entity behavior analytics (UEBA) on FortiSIEM, what must you use to dynamically supply a list of IP addresses to a FortiGate device for blocking purposes?

a) API Connection
b) SCP
c) Watchlists
d) Lookup tables

Answer: c

Question: 5

From which two sources can you import data to train FortiSIEM machine learning? (Choose two.)

a) Syslog archives
b) CSV files
c) FortiSIEM reports
d) SQL database

Answer: b, c

Question: 6

Where can an analyst configure rule notifications and automated remediation on FortiSIEM?

a) Notification policy
b) Response policies
c) Notification engine
d) Automation policy

Answer: d

Question: 7

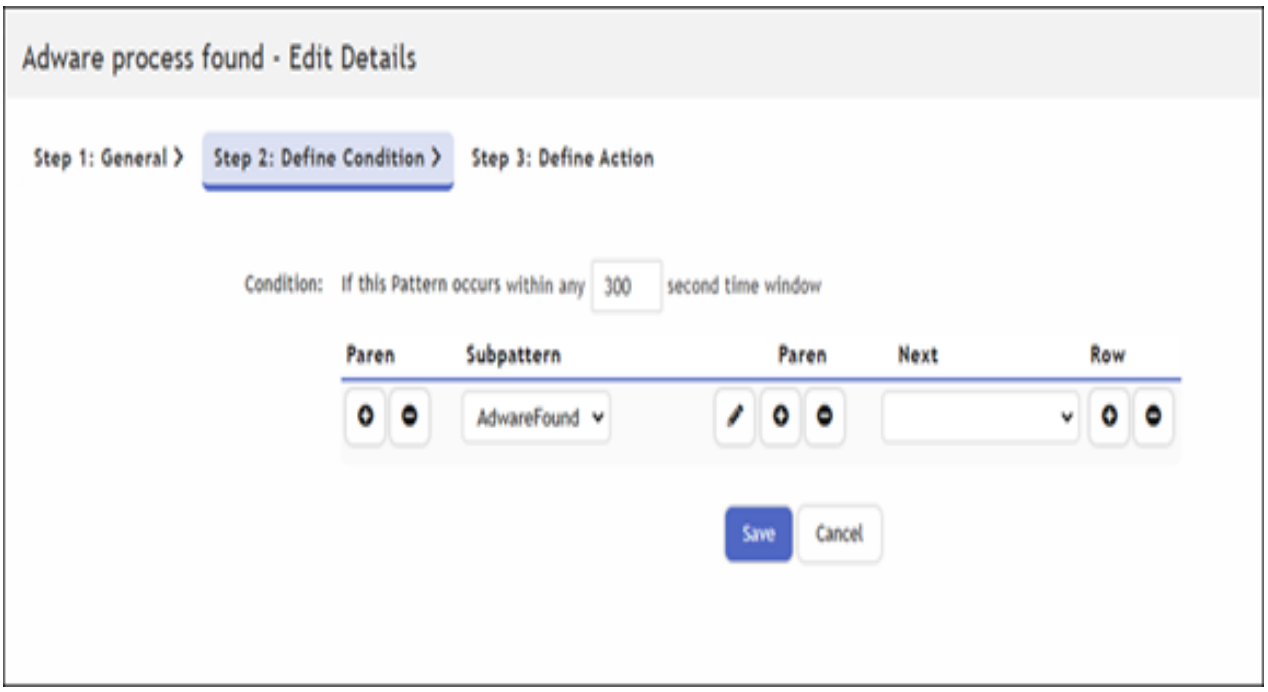
What must you configure to apply ZTNA tags from FortiSIEM to devices in FortiClient EMS?

a) Syslog connection to FortiSIEM from FortiGate firewalls
b) Syslog connection to FortiGate firewalls from FortiSIEM
c) API connection from FortiSIEM to FortiClient EMS
d) API connection from FortiClient EMS to FortiSIEM

Answer: c

Question: 8

Refer to the exhibit.



What does the Define Condition time field determine for this rule?

a) The time of day the rule will trigger.
b) How often the rule will evaluate the subpattern(s).
c) How often the rule will perform remediation.
d) The time period over which the rule evaluates events.

Answer: d

Question: 9

What are the five categories of incidents on FortiSIEM?

a) Performance, other, availability, security, and change
b) Devices, users, high risk, other, and low risk
c) Security, change, high risk, low risk, and other
d) Performance, other, devices, high risk, and low risk

Answer: a

Question: 10

What feature defines when an incident is created by FortiSIEM?

a) Rules
b) Cases
c) Analytics
d) CMDB

Answer: a

Study Guide to Crack Fortinet FCP_FSM_AN-7.2 Exam:

- Getting details of the FCP_FSM_AN-7.2 syllabus, is the first step of a study plan. This pdf is going to be of ultimate help. Completion of the syllabus is must to pass the FCP_FSM_AN-7.2 exam.
- Making a schedule is vital. A structured method of preparation leads to success.
- Joining the Fortinet provided training for FCP_FSM_AN-7.2 exam could be of much help. If there is specific training for the exam, you can discover it from the link above.
- Read from the FCP_FSM_AN-7.2 sample questions to gain your idea about the actual exam questions. In this PDF useful sample questions are provided to make your exam preparation easy.
- Practicing on FCP_FSM_AN-7.2 practice tests is must. Continuous practice will make you an expert in all syllabus areas.

Reliable Online Practice Test for FCP_FSM_AN-7.2 Certification

Make NWExam.com your best friend during your Fortinet FCP - FortiSIEM 7.2 Analystexam preparation. We provide authentic practice tests for the FCP_FSM_AN-7.2 exam. Experts design these online practice tests, so we can offer you an exclusive experience of taking the actual FCP_FSM_AN-7.2 exam. We guarantee you 100% success in your first exam attempt if you continue practicing regularly. Don't bother if you don't get 100% marks in initial practice exam attempts. Just utilize the result section to know your strengths and weaknesses and prepare according to that until you get 100% with our practice tests. Our evaluation makes you confident, and you can score high in the FCP_FSM_AN-7.2 exam.

Start Online practice of FCP_FSM_AN-7.2 Exam by visiting URL
https://www.nwexam.com/fortinet/fcp-fsm-7-2-fortinet-fcp-fortisiem-7-2-analyst