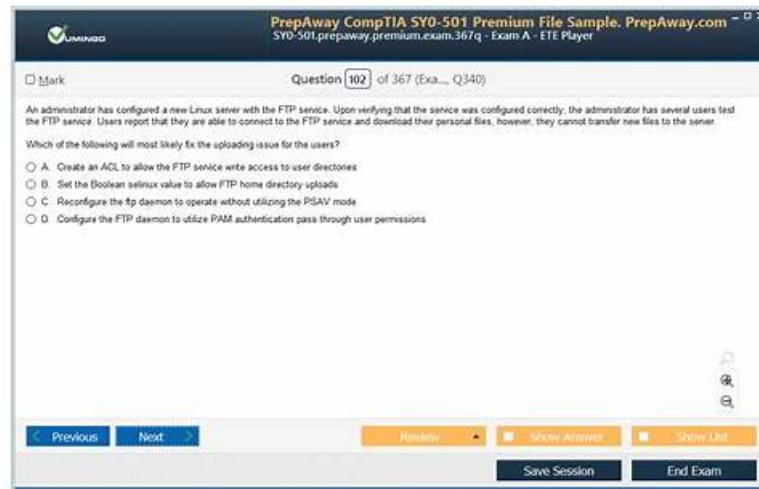


Reliable FCP_FSM_AN-7.2 Latest Practice Questions & Useful FCP_FSM_AN-7.2 Reliable Exam Cost & Correct Valid FCP_FSM_AN-7.2 Exam Tips



BTW, DOWNLOAD part of TorrentExam FCP_FSM_AN-7.2 dumps from Cloud Storage: <https://drive.google.com/open?id=1zQzI5Jv4byNZycoxTCoWFvbRHWAKtY>

Our FCP_FSM_AN-7.2 study materials are very popular in the international market and enjoy wide praise by the people in and outside the circle. We have shaped our FCP_FSM_AN-7.2 exam braindumps into a famous and top-ranking brand and we enjoy well-deserved reputation among the clients. Our FCP_FSM_AN-7.2 Training Questions boost many outstanding and superior advantages which other same kinds of products don't have. You won't regret if you buy them!

Fortinet FCP_FSM_AN-7.2 Exam Syllabus Topics:

Topic	Details
Topic 1	<ul style="list-style-type: none">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.
Topic 2	<ul style="list-style-type: none">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 3	<ul style="list-style-type: none">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 4	<ul style="list-style-type: none">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.

How I Prepared Fortinet FCP_FSM_AN-7.2 Exam Questions In One Week? [2026]

By seeing your goofs you can work on your show continually for the Fortinet FCP_FSM_AN-7.2 approach. You can give vast phony tests to make them ideal for Fortinet FCP_FSM_AN-7.2 and can check their past given exams. Fortinet FCP_FSM_AN-7.2 Dumps will give reliable free updates to our clients generally all the FCP - FortiSIEM 7.2 Analyst.

Fortinet FCP - FortiSIEM 7.2 Analyst Sample Questions (Q27-Q32):

NEW QUESTION # 27

What can you use to send data to FortiSIEM for user and entity behavior analytics (UEBA)?

- A. SSH
- B. SNMP
- C. FortiSIEM agent
- D. FortiSIEM worker

Answer: C

Explanation:

The FortiSIEM agent can be used to send detailed endpoint data such as user activity and process behavior to FortiSIEM, which is essential for performing User and Entity Behavior Analytics (UEBA).

NEW QUESTION # 28

Refer to the exhibit.

Automation Policy

Name
SOC Notification

Severity:
☒ Low
☒ Medium
☒ High

Rules:
ANY

Time Range:
ANY

Affected Items:
ANY

Affected Orgs:
ANY

Action:
☒ Send Email/SMS/Webhook to the target users.
☒ Run Remediation/Script.
☐ Invoke an Integration Policy. Run: no policy
☐ Create Case when an incident is created.
☐ Send SNMP message to the destination set in Admin > Settings > Analytics.
☐ Send XML file over HTTP(S) to the destination set in Admin > Settings > Analytics.
☐ Open Remedy ticket using the configuration set in Admin > Settings > Analytics.
☐ Invoke FortiAI and update Comments

Settings:
☒ Do not notify when an incident is cleared automatically.
☐ Do not notify when an incident is cleared manually.
☒ Do not notify when an incident is cleared by system.

Comments:

Save
Cancel

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. A notification is sent to the SOC manager dashboard.
- C. The remediation script is run.
- D. An email is sent to the SOC manager.

Answer: A

Explanation:

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.

NEW QUESTION # 29

Refer to the exhibit.

Group By and Display Fields Clear All Load Save

Attribute	Order	Display As	Row	Move
Event Receive Time	DESC ▼		+	-
Reporting IP	▼		+	-
Event Type	▼		+	-
Raw Event Log	▼		+	-
COUNT(Matched Events)	▼		+	-

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

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

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 # 30

Refer to the exhibit.

Machine Learning - Train Configuration

Run Mode: *Local*

Task: *Regression*

Algorithm: *DecisionTreeRegressor*


Fields to use for Prediction:

- ☐ AVG(CPU Util)
- ☒ AVG(Memory Util)
- ☒ AVG(Sent Bytes64)
- ☒ AVG(Received Bytes64)

Field to Predict:

- ☒ AVG(CPU Util)
- ☐ AVG(Memory Util)
- ☐ AVG(Sent Bytes64)
- ☐ AVG(Received Bytes64)

Train factor

0%  100%

The configuration shown in the exhibit is incorrect.

What must you change to allow this configuration to be successfully applied to FortiSIEM?

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

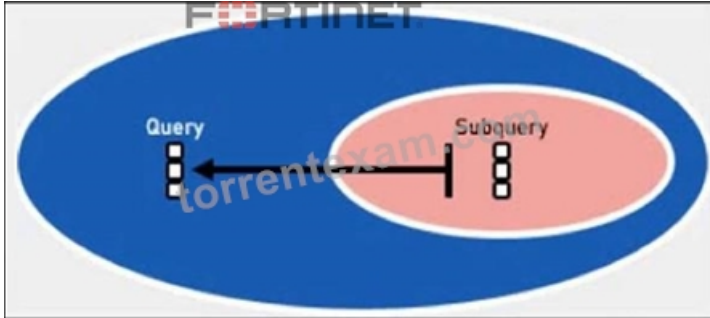
Answer: C

Explanation:

The Run Mode is set to Local, which is not valid for training machine learning models in FortiSIEM. To apply this configuration correctly, the Run Mode must be set to ML, which enables proper model training and prediction using selected fields.

NEW QUESTION # 31

Refer to the exhibit.



Which two lookup types can you reference as the subquery in a nested analytics query? (Choose two.)

- A. SNMP Query
- B. CMDB Query
- C. Event Query
- D. LDAP Query

Answer: A,C

Explanation:

In FortiSIEM nested analytics queries, you can reference both CMDB Queries and Event Queries as subqueries. These allow correlation between CMDB data and event data for advanced detection use cases.

NEW QUESTION # 32

.....

As an experienced exam dumps provider, our website offers you most reliable Fortinet real dumps and study guide. We offer customer with most comprehensive FCP_FSM_AN-7.2 exam pdf and the guarantee of high pass rate. The key of our success is to constantly provide the best quality FCP_FSM_AN-7.2 Dumps Torrent with the best customer service.

FCP_FSM_AN-7.2 Reliable Exam Cost: https://www.torrentexam.com/FCP_FSM_AN-7.2-exam-latest-torrent.html

- FCP_FSM_AN-7.2 Test Dumps.zip ☐ FCP_FSM_AN-7.2 Exam Online ☐ FCP_FSM_AN-7.2 Valid Study Materials ☐ Search for ☐ FCP_FSM_AN-7.2 ☐ and download it for free on ▶ www.pass4test.com ◀ website ☐ FCP_FSM_AN-7.2 Reliable Guide Files
- Valid free FCP_FSM_AN-7.2 exam answer collection - FCP_FSM_AN-7.2 real vce ☐ Copy URL ➡ www.pdfvce.com ☐ open and search for ➡ FCP_FSM_AN-7.2 ☐ to download for free ☐ FCP_FSM_AN-7.2 Test Dumps.zip
- First-grade Fortinet FCP_FSM_AN-7.2 Latest Practice Questions and Realistic FCP_FSM_AN-7.2 Reliable Exam Cost ☐ Easily obtain free download of ▶ FCP_FSM_AN-7.2 ◀ by searching on 《 www.vce4dumps.com 》 ☐ FCP_FSM_AN-7.2 Exam Online
- Real Fortinet FCP_FSM_AN-7.2 Dumps PDF - Achieve Success In Exam ☐ Enter ✓ www.pdfvce.com ☐ ✓ ☐ and search for ➡ FCP_FSM_AN-7.2 ⇐ to download for free ☐ FCP_FSM_AN-7.2 Reliable Exam Cost
- FCP_FSM_AN-7.2 Exam Online ☐ FCP_FSM_AN-7.2 Sample Questions Answers ☐ FCP_FSM_AN-7.2 Reliable Guide Files ☐ Download ▶ FCP_FSM_AN-7.2 ◀ for free by simply entering { www.dumpsmaterials.com } website ☐ 100% FCP_FSM_AN-7.2 Correct Answers
- Valid free FCP_FSM_AN-7.2 exam answer collection - FCP_FSM_AN-7.2 real vce ☐ Download (FCP_FSM_AN-7.2) for free by simply searching on ➡ www.pdfvce.com ☐ ☐ FCP_FSM_AN-7.2 Sample Questions Answers
- FCP_FSM_AN-7.2 New Braindumps Questions ☐ FCP_FSM_AN-7.2 Latest Exam Format ☐ New FCP_FSM_AN-7.2 Exam Questions ☐ The page for free download of 《 FCP_FSM_AN-7.2 》 on ➡ www.practicevce.com ☐ will open immediately ☐ FCP_FSM_AN-7.2 Reliable Exam Cost

- 2026 Latest TorrentExam FCP_FSM_AN-7.2 PDF Dumps and FCP_FSM_AN-7.2 Exam Engine Free Share:
<https://drive.google.com/open?id=1LzQz5Jv4byNZiycoxTCoWFvbRHWAKtY>

2026 Latest TorrentExam FCP_FSM_AN-7.2 PDF Dumps and FCP_FSM_AN-7.2 Exam Engine Free Share:
<https://drive.google.com/open?id=1LzQz5Jv4byNZiycoxTCoWFvbRHWAKtY>