

# HOT FCP\_FSM\_AN-7.2 Minimum Pass Score 100% Pass | Trustable Fortinet FCP - FortiSIEM 7.2 Analyst Premium Exam Pass for sure



BONUS!!! Download part of ExamcollectionPass FCP\_FSM\_AN-7.2 dumps for free: <https://drive.google.com/open?id=1bPN-wTtEd33gUfakBFfLdBdCO8GvXX7u>

If you buy ExamcollectionPass's Fortinet certification FCP\_FSM\_AN-7.2 exam practice questions and answers, you can not only pass Fortinet certification FCP\_FSM\_AN-7.2 exam, but also enjoy a year of free update service. If you fail your exam, ExamcollectionPass will full refund to you. You can free download part of practice questions and answers about Fortinet Certification FCP\_FSM\_AN-7.2 Exam as a try to test the reliability of ExamcollectionPass's products.

## Fortinet FCP\_FSM\_AN-7.2 Exam Syllabus Topics:

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

>> FCP\_FSM\_AN-7.2 Minimum Pass Score <<

## How Can You Avoid Wasting Your Money by Purchasing the Fortinet

## FCP\_FSM\_AN-7.2 Exam Questions?

"ExamcollectionPass" created a demo version for customer satisfaction so candidates can evaluate the FCP\_FSM\_AN-7.2 exam questions before purchasing. Also, "ExamcollectionPass" has made this Fortinet FCP\_FSM\_AN-7.2 practice exam material budget-friendly with many benefits that make it the best choice. Our team of experts who designed this FCP\_FSM\_AN-7.2 Exam Questions assures that whoever prepares with it adequately, there is no doubt of failure and they will pass the Fortinet CERTIFICATION EXAM on the first attempt. Purchase our "ExamcollectionPass" study material now and get free updates for up to 1 year.

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

#### NEW QUESTION # 27

Refer to the exhibit.



An analyst is trying to identify an issue using an expression based on the Expression Builder settings shown in the exhibit; however, the error message shown in the exhibit indicates that the expression is invalid.

What is the correct syntax to create an expression that generates a total count of matched events?

- A. COUNT(Matched Events)
- B. Matched Events COUNT()
- C. (COUNT) Matched Events
- D. Matched Events (COUNT)

**Answer: A**

Explanation:

The correct syntax is COUNT(Matched Events) - with proper capitalization and spacing - to generate a total count of matched events. The error in the exhibit likely stems from a formatting issue (e.g., lowercase count() or incorrect spacing), not the logical structure of the expression.

#### NEW QUESTION # 28

Refer to the exhibit.



The exhibit shows the configuration for a machine learning dataset using anomaly detection.

If the report generating the data being analyzed is run every hour, how long must the FortiSIEM device be up before a valid training set can be produced?

- A. 30 hours

- B. 24 hours
- **C. 10 hours**
- D. 3 hours

**Answer: C**

Explanation:

The Window parameter specifies the number of report intervals required to build a valid training set. Since the report runs every hour and the window is set to 10, FortiSIEM needs 10 data intervals (10 hours) of operation to collect sufficient data for training the anomaly detection model.

#### NEW QUESTION # 29

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

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

**Answer: B,D**

Explanation:

To allow FortiSIEM to apply tags to devices in FortiClient EMS, FortiEMS API credentials must be defined on FortiSIEM to enable communication with EMS, and FortiSIEM API credentials must be defined on FortiEMS to allow EMS to accept tagging instructions from FortiSIEM. This bidirectional API trust is essential for tag application.

#### 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)

nabass.com

The screenshot shows the FortiSIEM configuration interface. At the top, there is a checkbox labeled 'AVG(Received Bytes64)' which is checked. Below this, there is a section titled 'Field to Predict:' with a dropdown arrow. Under this section, there are four radio button options: 'AVG(CPU Util)' (which is selected), 'AVG(Memory Util)', 'AVG(Sent Bytes64)', and 'AVG(Received Bytes64)'. Below the 'Field to Predict' section, there is a section titled 'Train factor' with a dropdown arrow. Under this section, there is a slider control ranging from 0% to 100%, with a black slider knob positioned at approximately 30%. To the right of the slider, there is a text box containing the value '30'.

The configuration shown in the exhibit is incorrect.

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

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

**Answer: D**

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.

**Analytics**

Filter By: ☐ Event Keywords ☒ Event Attribute ☐ CMDB Attribute

| Paren | Attribute | Operator | Value                     | Paren | Next       | Row |
|-------|-----------|----------|---------------------------|-------|------------|-----|
| -     | Source IP | IN       | Group: Windows            | -     | + AND OR + | +   |
| -     | User      | IN       | Group: FortiSIEM Analysts | -     | + AND OR + | +   |

Time Range: ☐ Real-time ☒ Relative ☐ Absolute

Last

Trend Interval:

Result Limit:  K rows

What is the Group: FortiSIEM Analysts value referring to?

- A. CMDB user group
- B. Windows Active Directory user group
- C. FortiSIEM organization group
- D. LDAP user group

**Answer: A**

Explanation:

In FortiSIEM, the value Group: FortiSIEM Analysts under the User attribute refers to a CMDB user group. These groups are defined within FortiSIEM's CMDB and used to logically organize users for analytics, correlation rules, and reporting.

## NEW QUESTION # 32

.....

Are you feeling anxious about taking the FCP - FortiSIEM 7.2 Analyst (FCP\_FSM\_AN-7.2) exam? Our customizable practice test questions will help you overcome your anxiety and prepare for the actual exam. With each attempt, you will receive a score report that will help you identify and correct your mistakes before your final attempt. Our web-based practice exam creates a similar situation to the FCP\_FSM\_AN-7.2 Real Exam Questions, making it easier for you to pass. Purchase our FCP - FortiSIEM 7.2 Analyst (FCP\_FSM\_AN-7.2) practice test material today and say goodbye to exam anxiety!

**FCP\_FSM\_AN-7.2 Premium Exam:** [https://www.examcollectionpass.com/Fortinet/FCP\\_FSM\\_AN-7.2-practice-exam-dumps.html](https://www.examcollectionpass.com/Fortinet/FCP_FSM_AN-7.2-practice-exam-dumps.html)

- Test FCP\_FSM\_AN-7.2 Questions ☐ Latest FCP\_FSM\_AN-7.2 Mock Test ☐ Reliable FCP\_FSM\_AN-7.2 Test Price ☐ ☐ [www.troytecdumps.com](http://www.troytecdumps.com) ☐ is best website to obtain ☒ FCP\_FSM\_AN-7.2 ☒ ☐ for free download ☐ New FCP\_FSM\_AN-7.2 Test Tutorial
- Pdfvce FCP\_FSM\_AN-7.2 Exam Dumps Offers Exam Passing Money Back Guarantee ☐ Copy URL ☒ [www.pdfvce.com](http://www.pdfvce.com) ☐ ☒ open and search for ☐ FCP\_FSM\_AN-7.2 ☐ to download for free ☐ FCP\_FSM\_AN-7.2 New Dumps Book
- TOP FCP\_FSM\_AN-7.2 Minimum Pass Score - Fortinet FCP - FortiSIEM 7.2 Analyst - Trustable FCP\_FSM\_AN-7.2 Premium Exam ☐ Simply search for ☐ FCP\_FSM\_AN-7.2 ☐ for free download on ☐ [www.pass4test.com](http://www.pass4test.com) ☐ ☐ New FCP\_FSM\_AN-7.2 Test Tutorial
- Best Fortinet FCP\_FSM\_AN-7.2 Minimum Pass Score Help You Pass Your Fortinet FCP - FortiSIEM 7.2 Analyst Exam From The First Try ☐ Search for ☐ FCP\_FSM\_AN-7.2 ☐ and download it for free immediately on { [www.pdfvce.com](http://www.pdfvce.com) } ☐ New FCP\_FSM\_AN-7.2 Test Tutorial
- Test FCP\_FSM\_AN-7.2 Questions ☐ Updated FCP\_FSM\_AN-7.2 Dumps ☐ Download FCP\_FSM\_AN-7.2 Fee ☐ ☐ Copy URL ☐ [www.practicevce.com](http://www.practicevce.com) ☐ open and search for ☐ FCP\_FSM\_AN-7.2 ☐ to download for free ☐ Reliable FCP\_FSM\_AN-7.2 Test Price
- TOP FCP\_FSM\_AN-7.2 Minimum Pass Score - Fortinet FCP - FortiSIEM 7.2 Analyst - Trustable FCP\_FSM\_AN-7.2 Premium Exam ☐ Open ☐ [www.pdfvce.com](http://www.pdfvce.com) ☐ and search for ☒ FCP\_FSM\_AN-7.2 ☒ ☐ to download exam materials

Top FCP\_FSM\_AN-7.2 Minimum Pass Score 100% Pass | High-quality FCP\_FSM\_AN-7.2 Premium Exam: FCP - FortiSIEM 7.2 Analyst ☐ Search for ☐ FCP\_FSM\_AN-7.2 ☐ and download exam materials for free through [ [www.troytecdumps.com](http://www.troytecdumps.com)] ☐ Exam FCP\_FSM\_AN-7.2 Fees

- BTW, DOWNLOAD part of ExamcollectionPass FCP\_FSM\_AN-7.2 dumps from Cloud Storage: <https://drive.google.com/open?id=1bPN-wTtEd33gUfakBFfLdBdCO8GvXX7u>