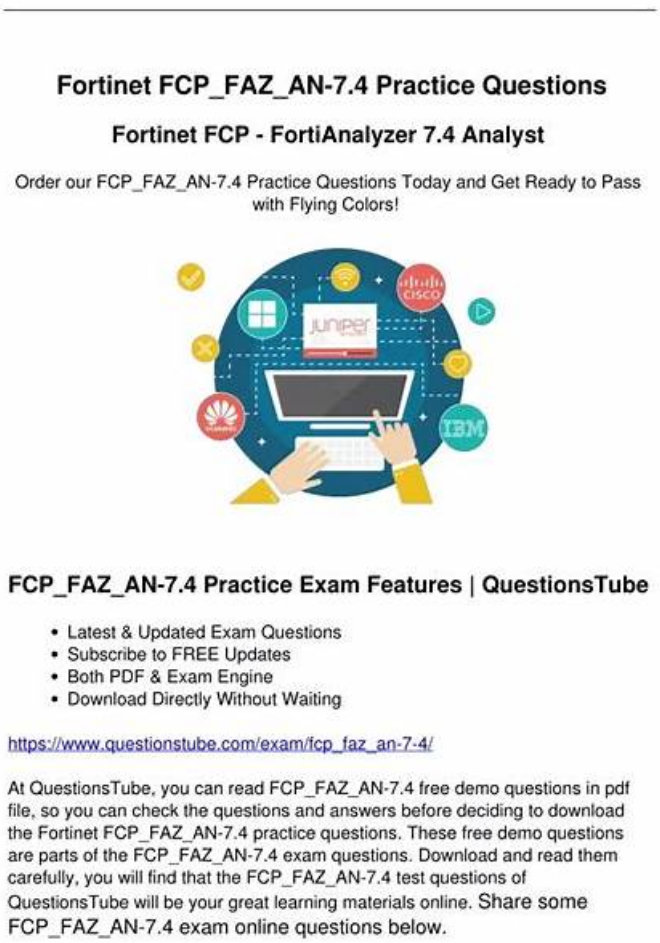
FCP_FAZ_AN-7.4 Exam Details - FCP_FAZ_AN-7.4 Official Practice Test



What's more, part of that Exam4Free FCP_FAZ_AN-7.4 dumps now are free: https://drive.google.com/open?id=1n6YvtsiwAHUrIpwRBKasn3AoErqHdE9v

Investing in a FCP - FortiAnalyzer 7.4 Analyst (FCP_FAZ_AN-7.4) certification is essential for professionals looking to advance their careers and stay competitive in the job market. With our actual Fortinet FCP_FAZ_AN-7.4 questions PDF, FCP_FAZ_AN-7.4 practice exams along with the support of our customer support team, you can be confident that you are getting the best possible FCP_FAZ_AN-7.4 Preparation material for the test. Download Real FCP_FAZ_AN-7.4 questions today and start your journey to success.

Fortinet FCP_FAZ_AN-7.4 Exam Syllabus Topics:

Topic	Details
Topic 1	• Features and Concepts: This section of the exam measures the skills of Fortinet Security Analysts and covers the fundamental concepts of FortiAnalyzer.
Topic 2	• Logging: Candidates will learn about logging mechanisms, log analysis, and gathering log statistics to effectively monitor security events and incidents.

Topic 3	• Reports: This section evaluates the skills of Fortinet Security Analysts in managing reports within FortiAnalyzer. Candidates will learn to create, troubleshoot, and optimize reports to ensure accurate data presentation and insights for security analysis.
Topic 4	• Playbooks: This domain measures the skills of Fortinet Network Analysts in creating and managing playbooks. Candidates will explain playbook components and develop workflows that automate responses to security incidents, improving operational efficiency in SOC environments.
Topic 5	• SOC Events and Incident Management: This domain targets Fortinet Network Analysts and focuses on managing security operations center (SOC) events. Candidates will explain SOC features on FortiAnalyzer, manage events and incidents, and understand the incident lifecycle to enhance incident response capabilities.

Pass Guaranteed Quiz 2026 Fortinet Latest FCP_FAZ_AN-7.4 Exam Details

Our experts update the FCP_FAZ_AN-7.4 training materials every day and provide the latest update timely to you. If you have the doubts or the questions about our product and the purchase procedures you can contact our online customer service personnel at any time. We provide the discounts to the old client and you can have a free download and tryout of our FCP_FAZ_AN-7.4 Test Question before your purchase. So there are many merits of our product. You can know the characteristics and the functions of our FCP_FAZ_AN-7.4 practice test by free demo before you purchase our FCP_FAZ_AN-7.4 exam questions.

Fortinet FCP - FortiAnalyzer 7.4 Analyst Sample Questions (Q16-Q21):

NEW QUESTION # 16
Which log will generate an event with the status Unhandled?

- A. An AppControl log with action=blocked.
- B. A WebFilter log will action=dropped.
- C. An IPS log with action=pass.
- D. An AV log with action=quarantine.

Answer: C

Explanation:
In FortiOS 7.4.1 and FortiAnalyzer 7.4.1, the "Unhandled" status in logs typically signifies that the FortiGate encountered a security event but did not take any specific action to block or alter it. This usually occurs in the context of Intrusion Prevention System (IPS) logs.
IPS logs with action=pass: When the IPS engine inspects traffic and determines that it does not match any known attack signatures or violate any configured policies, it assigns the action "pass". Since no action is taken to block or modify this traffic, the status is logged as "Unhandled." Let's look at why the other options are incorrect:
An AV log with action=quarantine: Antivirus (AV) logs with the action "quarantine" indicate that a file was detected as malicious and moved to quarantine. This is a definitive action, so the status wouldn't be "Unhandled." A WebFilter log will action=dropped: WebFilter logs with the action "dropped" indicate that web traffic was blocked according to the configured web filtering policies. Again, this is a specific action taken, not an "Unhandled" event.
An AppControl log with action=blocked: Application Control logs with the action "blocked" mean that an application was denied access based on the defined application control rules. This is also a clear action, not "Unhandled."

NEW QUESTION # 17
Which two statements about log forwarding are true? (Choose two.)

- A. Forwarded logs cannot be filtered to match specific criteria.
- B. Logs are forwarded in real-time only.
- C. You can use aggregation mode only with another FortiAnalyzer.
- D. The client retains a local copy of the logs after forwarding.

Answer: C,D

NEW QUESTION # 18
Which statement about the FortiSOAR management extension is correct?

- A. It requires a dedicated FortiSOAR device or VM.
- B. It runs as a docker container on FortiAnalyzer.
- C. It does not include a limited trial by default.
- D. It requires a FortiManager configured to manage FortiGate.

Answer: A

Explanation:
The FortiSOAR management extension is designed as an independent security orchestration, automation, and response (SOAR) solution that integrates with other Fortinet products but requires its own dedicated device or virtual machine (VM) environment. FortiSOAR is not natively integrated as a container or service within FortiAnalyzer or FortiManager, and it operates separately to manage complex security workflows and incident responses across various platforms.
Let's examine each option to determine the correct answer:
* Option A: It requires a FortiManager configured to manage FortiGate
* This is incorrect. FortiSOAR operates independently of FortiManager. While FortiSOAR can receive input or data from FortiGate (often managed by FortiManager), it does not require FortiManager to be part of its setup.
* Option B: It runs as a docker container on FortiAnalyzer
* This is incorrect. FortiSOAR does not run as a container within FortiAnalyzer. It requires its own dedicated environment, either as a physical device or a virtual machine, due to the resource requirements and specialized functions it performs.
* Option C: It requires a dedicated FortiSOAR device or VM
* This is correct. FortiSOAR is deployed as a standalone device or VM, which enables it to handle the intensive processing needed for orchestrating security operations, integrating with third-party tools, and automating responses across an organization's security infrastructure.
* Option D: It does not include a limited trial by default
* This is incorrect. FortiSOAR installations may come with trial options or demos in specific scenarios, especially for evaluation purposes. This depends on licensing and deployment policies.
References: The FortiSOAR platform, as outlined in Fortinet product documentation, is a standalone SOAR solution that requires a dedicated device or VM for deployment. It integrates with Fortinet's Security Fabric but operates separately from FortiAnalyzer, FortiManager, and FortiGate, focusing on advanced incident management and security automation.

NEW QUESTION # 19
Why must you wait for several minutes before you run a playbook that you just created?

- A. FortiAnalyzer needs that time to debug the new playbook.
- B. FortiAnalyzer needs that time to ensure there are no other playbooks running.
- C. FortiAnalyzer needs that time to back up the current playbooks.
- D. FortiAnalyzer needs that time to parse the new playbook.

Answer: D

Explanation:
When a new playbook is created on FortiAnalyzer, the system requires some time to parse and validate the playbook before it can be executed. Parsing involves checking the playbook's structure, ensuring that all syntax and logic are correct, and preparing the playbook for execution within FortiAnalyzer's automation engine. This initial parsing step is necessary for FortiAnalyzer to load the playbook into its operational environment correctly.
Here's why the other options are incorrect:
Option A: FortiAnalyzer needs that time to parse the new playbook
This is correct. The delay is due to the parsing and setup process required to prepare the new playbook for execution. FortiAnalyzer's automation engine checks for any issues or dependencies within the playbook, ensuring that it can run without errors.
Option B: FortiAnalyzer needs that time to debug the new playbook
This is incorrect. Debugging is not an automatic process that FortiAnalyzer undertakes after playbook creation. Debugging, if necessary, is a manual task performed by the administrator if there are issues with the playbook execution.
Option C: FortiAnalyzer needs that time to back up the current playbooks This is incorrect. FortiAnalyzer does not automatically back up playbooks every time a new one is created. Backups of configuration and playbooks are typically scheduled as part of

routine maintenance and are not triggered by playbook creation.
Option D: FortiAnalyzer needs that time to ensure there are no other playbooks running This is incorrect. FortiAnalyzer can manage multiple playbooks running simultaneously, so it does not require waiting for other playbooks to finish before initiating a new one. The waiting time specifically relates to the parsing process of the newly created playbook.

NEW QUESTION # 20
In order for FortiAnalyzer to collect logs from a FortiGate device, what configuration is required?
(Choose two.)

- A. Log encryption must be enabled
- B. Remote logging must be enabled on FortiGate
- C. FortiGate must be registered with FortiAnalyzer
- D. ADOMs must be enabled

Answer: B,C

NEW QUESTION # 21
.....

myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, ywhhg.com, kumu.io, Disposable vapes

2026 Latest Exam4Free FCP_FAZ_AN-7.4 PDF Dumps and FCP_FAZ_AN-7.4 Exam Engine Free Share: https://drive.google.com/open?id=1n6YvtsiwAHUrIpwRBKasn3AoErqHdE9v