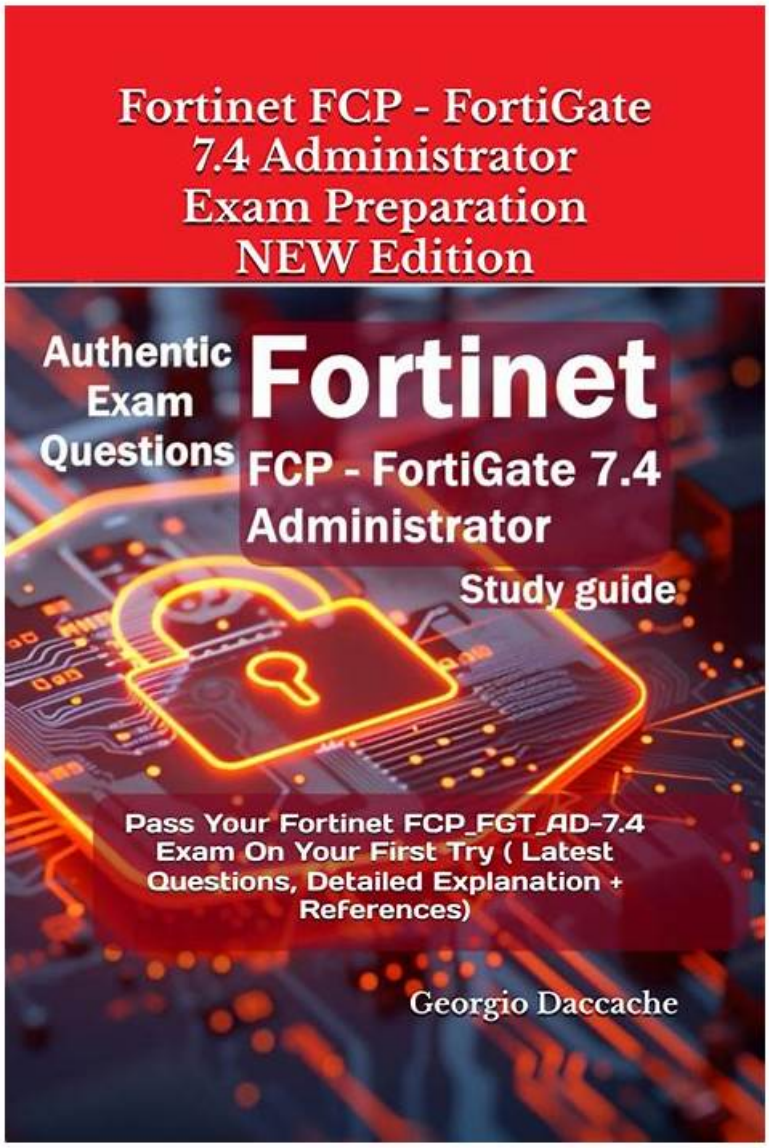
Fortinet FCP_FAZ_AN-7.4최고덤프공부 - FCP_FAZ_AN-7.4최신인증시험정보



ExamPassdump FCP_FAZ_AN-7.4 최신 PDF 버전 시험 문제집을 무료로 Google Drive에서 다운로드하세요: https://drive.google.com/open?id=130rIKsbN5L1AcN54Ls6O5CYd2k3ETPoO

ExamPassdump에는 IT인증시험의 최신Fortinet FCP_FAZ_AN-7.4학습가이드가 있습니다. ExamPassdump 는 여러분들이Fortinet FCP_FAZ_AN-7.4시험에서 패스하도록 도와드립니다. Fortinet FCP_FAZ_AN-7.4시험준비시간이 충분하지 않은 분은 덤프로 철저한 시험대비해보세요. 문제도 많지 않고 깔끔하게 문제와 답만으로 되어있어 가장 빠른 시간내에Fortinet FCP_FAZ_AN-7.4시험합격할수 있습니다.

Fortinet FCP_FAZ_AN-7.4 시험요강:

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

주제 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.
주제 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.
주제 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.

FCP_FAZ_AN-7.4최고덤프공부 덤프데모 다운받기

만약 아직도 우리를 선택할지에 대하여 망설이고 있다면. 우선은 우리 사이트에서 ExamPassdump가 제공하는 무료인 일부 문제와 답을 다운하여 체험해보시고 결정을 내리시길 바랍니다.그러면 우리의 덤프에 믿음이;갈 것이고, 우리 또한 우리의 문제와 답들은 무조건 100%통과 율로 아주 고득점으로Fortinet인증FCP_FAZ_AN-7.4험을 패스하실 수 있습니다,

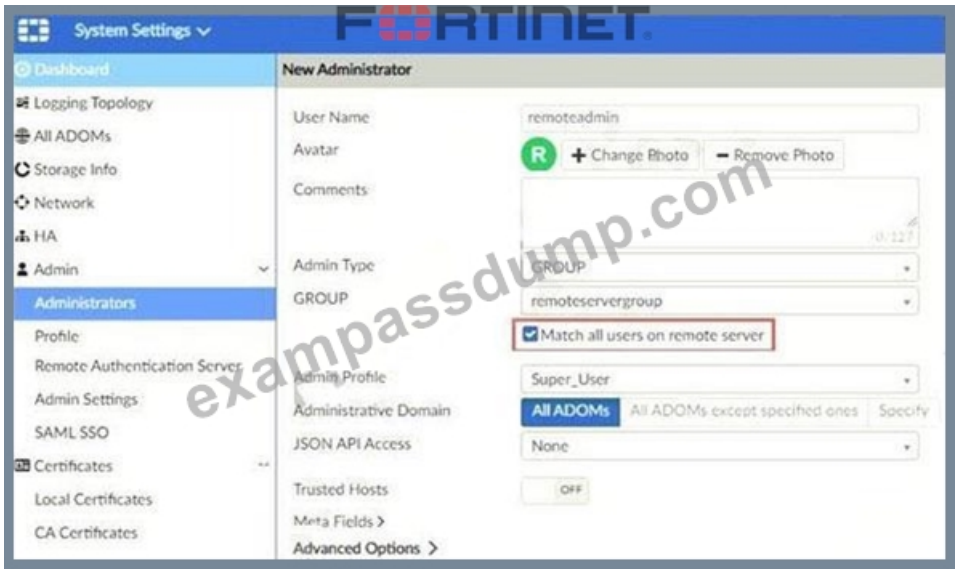
최신 FCP in Security Operations FCP_FAZ_AN-7.4 무료샘플문제 (Q52-Q57):

질문 # 52
An administrator has configured the following settings:
config system global
set log-checksum md5-auth
end
What is the significance of executing this command?

- A. This command records passwords in log files and encrypts them.
- B. This command encrypts log transfer between FortiAnalyzer and other devices
- C. This command records the log file MD5 hash value.
- D. This command records the log file MD5 hash value and authentication code.

정답：D

질문 # 53
Refer to the exhibit.



The exhibit shows "remoteservergroup" is an authentication server group with LDAP and RADIUS servers.
Which two statements express the significance of enabling "Match all users on remote server" when configuring a new administrator? (Choose two.)

- A. Use remoteadmin from LDAP and RADIUS servers will be able to log in to FortiAnalyzer at anytime.
- B. Administrator can log in to FortiAnalyzer using their credentials on remote servers LDAP and RADIUS.
- C. It creates a wildcard administrator using LDAP and RADIUS servers.
- D. It allows administrators to use two-factor authentication.

정답： B,C

질문 # 54
Which statement about sending notifications with incident updates is true?

- A. Each connector used can have different notification settings.
- B. Each incident can send notifications to a single external platform.
- C. Notifications can be sent only when an incident is created or deleted.
- D. You must configure an output profile to send notifications by email.

정답： A

질문 # 55
Which statement describes archive logs on FortiAnalyzer?

- A. Logs a FortiAnalyzer administrator can access in FortiView
- B. Logs that are indexed and stored in the SQL database
- C. Logs compressed and saved in files with the .gz extension
- D. Logs previously collected from devices that are offline

정답： C

설명:
In FortiAnalyzer, archive logs refer to logs that have been compressed and stored to save space. This process involves compressing the raw log files into the .gz format, which is a common compression format used in Fortinet systems for archived data. Archiving is essential in FortiAnalyzer to optimize storage and manage long-term retention of logs without impacting performance.
Let's examine each option for clarity:
* Option A: Logs that are indexed and stored in the SQL database
* This is incorrect. While some logs are indexed and stored in an SQL database for quick access and searchability, these are not classified as archive logs. Archived logs are typically moved out of the database and compressed.
* Option B: Logs a FortiAnalyzer administrator can access in FortiView
* This is incorrect because FortiView primarily accesses logs that are active and indexed, not archived logs. Archived logs are

stored for long-term retention but are not readily available for immediate analysis in FortiView.
* Option C: Logs compressed and saved in files with the .gz extension
* This is correct. Archive logs on FortiAnalyzer are stored in compressed .gz files to reduce space usage. This archived format is used for logs that are no longer immediately needed in the SQL database but are retained for historical or compliance purposes.
* Option D: Logs previously collected from devices that are offline
* This is incorrect. Although archived logs may include data from devices that are no longer online, this is not a defining characteristic of archive logs.
* FortiAnalyzer 7.4.1 documentation and configuration guides outline that archived logs are stored in compressed files with the .gz extension to conserve storage space, ensuring FortiAnalyzer can handle a larger volume of logs over extended periods.

질문 # 56
What is required to authorize a FortiGate on FortiAnalyzer using Fabric authorization?

- A. A FortiGate ADOM
- B. A pre-shared key
- C. The FortiGate serial number
- D. Valid FortiAnalyzer credentials

정답：D

질문 # 57
.....