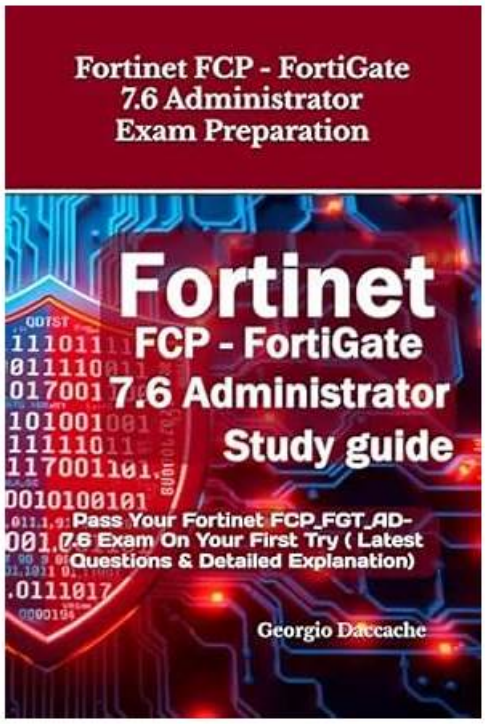
Ace Your Exam Preparation with Fortinet FCP_FAZ_AN-7.6 Exam Questions



P.S. Free & New FCP_FAZ_AN-7.6 dumps are available on Google Drive shared by TestInsides: https://drive.google.com/open?id=1p-iK8aTJOEZK_xlRjo5UvI6Jw4YJew49

The Fortinet FCP_FAZ_AN-7.6 certification exam is not only validate your skills but also prove your expertise. It can prove to your boss that he did not hire you in vain. The current IT industry needs a reliable source of Fortinet FCP_FAZ_AN-7.6 Certification Exam, TestInsides is a good choice. Select TestInsides FCP_FAZ_AN-7.6 exam material, so that you do not need yo waste your money and effort. And it will also allow you to have a better future.

Fortinet FCP_FAZ_AN-7.6 Exam Syllabus Topics:

Topic	Details
Topic 1	• Features and concepts: This domain covers FortiAnalyzer's integration with Security Fabric for log collection, the technical processes of log data flow, normalization and parsing, and the SOC features available for security monitoring and analysis.

Topic 2	• Reports: This domain explains the use of reports, charts, and datasets for presenting security intelligence, covers report configuration to meet organizational requirements, and includes troubleshooting report generation problems.
Topic 3	• Log Analysis: This domain focuses on examining and interpreting logs, events, and incidents, using FortiView dashboards and widgets for data visualization, and diagnosing report generation issues.
Topic 4	• SOC operation and automation: This domain addresses configuring events and event handlers, setting up incidents and indicators for threat tracking, configuring playbooks and fabric automation for orchestrated responses, and troubleshooting automation workflow issues.

FCP_FAZ_AN-7.6 Latest Braindumps Pdf, New FCP_FAZ_AN-7.6 Test Fee

Our FCP_FAZ_AN-7.6 exam torrent is compiled by experts and approved by experienced professionals and updated according to the development situation in the theory and the practice. Our FCP - FortiAnalyzer 7.6 Analyst guide torrent can simulate the exam and boosts the timing function. The language is easy to be understood and makes the learners have no learning obstacles. So our FCP_FAZ_AN-7.6 Exam Torrent can help you pass the exam with high possibility.

Fortinet FCP - FortiAnalyzer 7.6 Analyst Sample Questions (Q34-Q39):

NEW QUESTION # 34
Which two actions should an administrator take to vide Compromised Hosts on FortiAnalyzer?
(Choose two.)

- A. Make sure all endpoints are reachable by FortiAnalyzer.
- B. Subscribe FortiAnalyzer to FortiGuard to keep its local threat database up to date.
- C. Enable device detection on the FotiGate device that are sending logs to FortiAnalyzer.
- D. Enable web filtering in firewall policies on FortiGate devices, and make sure these logs are sent to fortiAnalyzer.

Answer: C,D

Explanation:
To view Compromised Hosts on FortiAnalyzer, certain configurations need to be in place on both FortiGate and FortiAnalyzer. Compromised Host data on FortiAnalyzer relies on log information from FortiGate to analyze threats and compromised activities effectively.
Option A: Enable device detection on the FortiGate devices that are sending logs to FortiAnalyzer Enabling device detection on FortiGate allows it to recognize and log devices within the network, sending critical information about hosts that could be compromised. This is essential because FortiAnalyzer relies on these logs to determine which hosts may be at risk based on suspicious activities observed by FortiGate. This setting enables FortiGate to provide device-level insights, which FortiAnalyzer uses to populate the Compromised Hosts view.
Option B: Enable web filtering in firewall policies on FortiGate devices, and make sure these logs are sent to FortiAnalyzer Web filtering is crucial in identifying potentially compromised hosts since it logs any access to malicious sites or blocked categories. FortiAnalyzer uses these web filter logs to detect suspicious or malicious web activity, which can indicate compromised hosts. By ensuring that FortiGate sends these web filtering logs to FortiAnalyzer, the administrator enables FortiAnalyzer to analyze and identify hosts engaging in risky behavior.

NEW QUESTION # 35
Which statement describes archive logs on FortiAnalyzer?

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

Answer: A

Explanation:
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.

NEW QUESTION # 36
What happens when the indicator of compromise (IOC) engine on FortiAnalyzer finds web logs that match blacklisted IP addresses?

- A. A new infected entry is added for the corresponding endpoint under Compromised Hosts.
- B. FortiAnalyzer flags the associated host for further analysis.
- C. The detection engine classifies those logs as Suspicious.
- D. The endpoint is marked as Compromised and, optionally, can be put in quarantine.

Answer: A

NEW QUESTION # 37
Which two external servers can you configure to validate administrator logins? (Choose two.)

- A. RADIUS
- B. LDAP
- C. Syslog
- D. Only locally by FortiAnalyzer

Answer: A,B

NEW QUESTION # 38
Exhibit.
Laptop1 is used by several administrators to manage FotiAnalyzer. You want to configure a generic text filter that matches all login attempts to the web interface generated by any user other than admin", and coming from Laptop1.
Which filter will achieve the desired result?

- A. Operation-login and srcip== 10.1.1.100 and dstip==10.1.1.1.210 and user==admin
- B. Operation-login and performed_on=="GUI(10.1.1.100)' and user!=admin
- C. Operation-login and performed_on=="GU (10.1.1.120)' and user!=admin
- D. Operation-login and dstip==10.1.1.210 and user!-admin

Answer: B

Explanation:
The objective is to create a filter that identifies all login attempts to the FortiAnalyzer web interface (GUI) coming from Laptop1 (IP

10.1.1.100) and excludes the admin user. This filter should match any user other than admin.
* Filter Components Analysis:
* Operation-login: This portion of the filter will target login actions specifically, which is correct for filtering login attempts.
* performed_on=="GUI(10.1.1.100)': This indicates that the login attempt must occur on the GUI interface and originate from the specified IP, which matches Laptop1's IP address (10.1.1.100). This ensures that the filter only matches GUI logins from this specific device.
* user!=admin: This part excludes logins by the admin user, meeting the requirement to capture only non-admin users.
* Option Analysis:
* Option A: Correctly specifies the Operation-login, performed_on=="GUI(10.1.1.100)', and user!=admin. This setup effectively filters login attempts to the GUI from Laptop1, excluding the admin user.
* Option B: Uses the incorrect IP 10.1.1.120 in the performed_on filter, which does not match Laptop1's IP (10.1.1.100).
* Option C: This option includes srcip==10.1.1.100 and dstip==10.1.1.210 but incorrectly specifies user==admin instead of user!=admin, which does not match the requirement to exclude admin users.
* Option D: This option does not specify the performed_on field to restrict it to the GUI and only includes dstip (destination IP) without srcip. It also incorrectly uses user!-admin instead of the correct syntax user!=admin.
Conclusion:
* Correct Answer: A. Operation-login and performed_on=="GUI(10.1.1.100)' and user!=admin
* This filter precisely captures the required conditions: login attempts from Laptop1 to the GUI interface by any user except admin.
References:
FortiAnalyzer 7.4.1 documentation on log filters, syntax for login operations, and GUI login tracking.

NEW QUESTION # 39
.....

The staffs of FCP_FAZ_AN-7.6 training materials are all professionally trained. If you have encountered some problems in using our products, you can always seek our help. Our staff will guide you professionally. If you are experiencing a technical problem on the system, the staff at FCP_FAZ_AN-7.6 practice guide will also perform one-on-one services for you. We want to eliminate all unnecessary problems for you, and you can learn our FCP_FAZ_AN-7.6 Exam Questions without any problems. You may have enjoyed many services, but the professionalism of FCP_FAZ_AN-7.6 simulating exam will conquer you.

□FCP_FAZ_AN-7.6 Authentic Exam Questions

- Free PDF Fortinet - Unparalleled FCP_FAZ_AN-7.6 - FCP - FortiAnalyzer 7.6 Analyst Valid Test Materials □ Open【 www.validtorrent.com 】 enter ➠ FCP_FAZ_AN-7.6 □ and obtain a free download □FCP_FAZ_AN-7.6 Latest Test Labs
- www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, bbs.t-firefly.com, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, pastebin.com, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes

DOWNLOAD the newest TestInsides FCP_FAZ_AN-7.6 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1p-iK8aTJOEZK_xlRjo5UvI6Jw4YJew49