

FCP_FAZ_AD-7.4 Valid Exam Fee & Valid FCP_FAZ_AD-7.4 Test Preparation



P.S. Free & New FCP_FAZ_AD-7.4 dumps are available on Google Drive shared by Exam4Free: <https://drive.google.com/open?id=1uF7oX4nDRqrUpLU38fH2a3SS3HCDVBcK>

Under the dominance of knowledge-based economy, we should keep pace with the changeable world and renew our knowledge in pursuit of a decent job and higher standard of life. In this circumstance, possessing a FCP_FAZ_AD-7.4 certification in your pocket can totally increase your competitive advantage in the labor market and make yourself distinguished from other job-seekers. Therefore our FCP_FAZ_AD-7.4 Study Guide can help you with dedication to realize your dream. And only after studying with our FCP_FAZ_AD-7.4 exam questions for 20 to 30 hours, you will be able to pass the FCP_FAZ_AD-7.4 exam.

To address the problems of FCP_FAZ_AD-7.4 exam candidates who are busy, Exam4Free has made the FCP_FAZ_AD-7.4 dumps PDF format of real FCP - FortiAnalyzer 7.4 Administrator (FCP_FAZ_AD-7.4) exam questions. This format's feature to run on all smart devices saves your time. Because of this, the portability of FCP_FAZ_AD-7.4 dumps PDF aids in your preparation regardless of place and time restrictions. The second advantageous feature of the FCP_FAZ_AD-7.4 Questions Pdf document is the ability to print FCP - FortiAnalyzer 7.4 Administrator (FCP_FAZ_AD-7.4) exam dumps to avoid eye strain due to the usage of smart devices.

>> FCP_FAZ_AD-7.4 Valid Exam Fee <<

Seeing FCP_FAZ_AD-7.4 Valid Exam Fee - Say Goodbye to FCP - FortiAnalyzer 7.4 Administrator

Our FCP_FAZ_AD-7.4 Study Materials include 3 versions: the PDF, PC and APP online. You can understand each version's merits and using method in detail before you decide to buy our FCP_FAZ_AD-7.4 study materials. For instance, PC version of our FCP_FAZ_AD-7.4 training quiz is suitable for the computers with the Windows system. It is a software application which can be installed and it stimulates the real exam's environment and atmosphere. It builds the users' confidence and can be practiced and learned at any time.

Fortinet FCP_FAZ_AD-7.4 Exam Syllabus Topics:

Topic	Details
Topic 1	<ul style="list-style-type: none">System Configuration: This section assesses the capabilities of network and security analysts in managing FortiAnalyzer systems. It includes tasks like performing initial configurations, setting up high-availability systems, and configuring RAID for storage.
Topic 2	<ul style="list-style-type: none">Administration: This section evaluates the ability of network and security analysts to configure administrative access and manage Administrative Domains (ADOMs). It covers tasks such as setting user permissions, managing backups, and disk quotas, and ensuring secure and efficient management of administrative privileges within FortiAnalyzer systems.

Topic 3	<ul style="list-style-type: none"> • Device Management: Here, Fortinet network and security analysts are evaluated on their ability to handle devices linked to FortiAnalyzer. This includes adding new devices, managing them efficiently, and troubleshooting communication issues.
Topic 4	<ul style="list-style-type: none"> • Logs and Reports Management: This part of the exam measures the candidate's ability to handle log data and generate reports using FortiAnalyzer. Network and security analysts must show proficiency in managing, analyzing, and reviewing logs to ensure effective system monitoring and auditing processes are in place.

Fortinet FCP - FortiAnalyzer 7.4 Administrator Sample Questions (Q118-Q123):

NEW QUESTION # 118

Which statement correctly describes RAID 10 (1+0) on FortiAnalyzer?

- A. A configuration with four disks, each with 2 TB of capacity, provides a total space of 2 TB.
- B. It uses striping to provide performance and fault tolerance.
- C. A configuration with four disks, each with 2 TB of capacity, provides a total space of 4 TB. B It combines mirroring striping and distributed parity to provide performance and fault tolerance

Answer: C

Explanation:

RAID 10 combines mirroring (RAID 1) and striping (RAID 0). In a RAID 10 setup with four disks, data is mirrored across two pairs of disks, and those pairs are striped for performance. This results in improved performance and fault tolerance, but the total usable storage is 50% of the total raw storage, meaning four 2 TB disks provide 4 TB of usable space.

NEW QUESTION # 119

You are using RAID with a FortiAnalyzer that supports software RAID, and one of the hard disks on FortiAnalyzer has failed. What is the recommended method to replace the disk?

- A. Perform a hot swap
- B. Shut down FortiAnalyzer and then replace the disk
- C. Downgrade your RAID level, replace the disk, and then upgrade your RAID level
- D. Clear all RAID alarms and replace the disk while FortiAnalyzer is still running

Answer: B

Explanation:

<https://community.fortinet.com/t5/FortiAnalyzer/Technical-Note-How-to-swap-Hard-Disk-on-FortiAnalyzer/ta-p/194997?externalID=FD41397#:~:text=If%20a%20hard%20disk%20on,process%20known%20as%20hot%20swapping>

NEW QUESTION # 120

Which two actions should an administrator take to view Compromised Hosts on FortiAnalyzer? (Choose two.)

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

Answer: A,B

Explanation:

In order to configure IOC, you require the following:

- * A one-year subscription to IOC. Note that FortiAnalyzer does include an evaluation license, but it is restrictive and only meant to give you an idea of how the feature works.
- * A web filter services subscription on FortiGate device(s)

* Web filter policies on FortiGate device(s) that send traffic to FortiAnalyzer Compromised Hosts or Indicators of Compromise service (IOC) is a licensed feature.

To view Compromised Hosts, you must turn on the UTM web filter of FortiGate devices and subscribe your FortiAnalyzer unit to FortiGuard to keep its local threat database synchronized with the FortiGuard threat database. See Subscribing FortiAnalyzer to FortiGuard.

Ref: <https://docs.fortinet.com/document/fortianalyzer/6.4.0/administration-guide/137635/viewing-compromised-hosts>

NEW QUESTION # 121

What are analytics logs on FortiAnalyzer?

- A. Logs that are indexed and stored in the SQL
- B. Logs that roll over when the log file reaches a specific size
- C. Logs classified as type Traffic, or type Security
- D. Logs that are compressed and saved to a log file

Answer: A

Explanation:

On FortiAnalyzer, analytics logs refer to the logs that have been processed, indexed, and then stored in the SQL database. This process allows for efficient data retrieval and analytics. Unlike basic log storage, which might involve simple compression and storage in a file system, analytics logs in FortiAnalyzer undergo an indexing process. This enables advanced features such as quick search, report generation, and detailed analysis, making it easier for administrators to gain insights into network activities and security incidents.

Reference: FortiAnalyzer 7.2 Administrator Guide - "Log Management" and "Data Analytics" sections.

NEW QUESTION # 122

Refer to the exhibit.

The screenshot shows the 'Cluster Settings' configuration page for a FortiAnalyzer. The 'Operation Mode' is set to 'High Availability'. The 'Preferred Role' is set to 'Primary'. The 'Cluster Virtual IP' section shows 'Interface' as 'port1' and 'IP Address' as '192.168.101.222'. The 'Cluster Settings' section shows 'Peer IP and Peer SN' with 'Peer IP' as '10.0.1.210' and 'Peer SN' as 'FAZ-VM0000065040'. Other settings include 'Group Name' as 'NSE5', 'Group ID' as '1', 'Password' as a masked field, 'Heart Beat Interval' as '10' seconds, 'Failover Threshold' as '30', and 'Priority' as '120'. A 'Log Data Sync' checkbox is at the bottom.

The image displays the configuration of a FortiAnalyzer the administrator wants to join to an existing HA cluster. What can you conclude from the configuration displayed?

- A. This FortiAnalyzer will join to the existing HA cluster as the primary.
- B. After joining to the cluster, this FortiAnalyzer will keep an updated log database.
- C. This FortiAnalyzer will trigger a failover after losing communication with its peers for 10 seconds.
- D. This FortiAnalyzer is configured to receive logs in its port1.

Answer: D

Explanation:

"If the preferred role is Primary, then this unit becomes the primary unit if it is configured first in a new HA cluster. If there is an

P.S. Free & New FCP_FAZ_AD-7.4 dumps are available on Google Drive shared by Exam4Free: <https://drive.google.com/open?id=1uF7oX4nDRqrUpLU38fh2a3SS3HCDVBcK>