Fortinet Fortianalyzer 6.4 Practice Test (Sample)

Study Guide

BY EXAMZIFY

Everything you need from our exam experts!

Notice: Examzify makes every reasonable effort to obtain from reliable sources accurate, complete, and timely information about this product.

Questions

1. **What action does 'diagnose ha force-cfg-resync' perform?**

   A. **Force HA to load the latest firmware**

   B. **Force an HA configuration resynchronization**

   C. **Abort current HA operations**

   D. **Change the role of cluster devices**

2. **How many drives are required for RAID 50 to maintain fault tolerance against two drive failures?**

   A. **4 drives**

   B. **6 drives**

   C. **8 drives**

   D. **10 drives**

3. **What command is used to retrieve performance statistics on FortiAnalyzer?**

   A. **Get system performance**

   B. **Get sys status**

   C. **Get log performance**

   D. **Get performance metrics**

4. **In the log forwarding architecture, which component acts as the client?**

   A. **The server that receives logs**

   B. **The FAZ that forwards logs**

   C. **The clients generating logs**

   D. **The firewall**

5. **How can you change the ADOM mode in FortiAnalyzer using the GUI?**

   A. **System settings > advanced > advanced settings**

   B. **System settings > general > configurations**

   C. **Device settings > ADOM selection**

   D. **Administration > system settings**

6. What is required to resolve hostnames in logs on a FortiAnalyzer?

A. DNS server configured on FortiAnalyzer

B. Static IP settings applied

C. Manual hostname entry in logs

D. Local DNS cache adjustment

7. What information does the failed authentication section of Fortiview display?

A. Number of successful logins

B. Current system status

C. Source IP of login, login type, interface, and number of failed attempts

D. Administrator login history

8. What is one way to fine-tune a data set in FortiAnalyzer?

A. Add more columns

B. Setting a group, order by, and sort filter

C. Setting a limit on results

D. Setting the device and time frame

9. A macro in FortiAnalyzer primarily defines what?

A. The visual layout of a report

B. Which data is to be selected from a log

C. The export settings for a report

D. The scheduling of reports

10. What feature can you enable to boost report performance and reduce generation time?

A. Auto-cache

B. Manual refresh

C. Scheduled updates

D. Report compression

Answers

1. B
2. B
3. A
4. B
5. A
6. A
7. C
8. B
9. B
10. A

Explanations

1. What action does 'diagnose ha force-cfg-resync' perform?

A. Force HA to load the latest firmware

B. Force an HA configuration resynchronization

C. Abort current HA operations

D. Change the role of cluster devices

The action 'diagnose ha force-cfg-resync' triggers a forced resynchronization of the High Availability (HA) configuration on Fortinet devices. This means that the active unit in an HA cluster will push its configuration settings to the standby unit(s), ensuring that all units in the cluster have the same configuration. This is particularly useful in scenarios where the standby unit may have fallen out of sync with the active unit, whether due to manual changes or issues during previous synchronization processes. By executing this command, administrators can maintain consistency across their HA cluster, which is critical for reliable failover and load balancing capabilities. Such synchronization is integral for effective management of resources and minimizing downtime in case of hardware or software failures.

2. How many drives are required for RAID 50 to maintain fault tolerance against two drive failures?

A. 4 drives

B. 6 drives

C. 8 drives

D. 10 drives

RAID 50 is a nested RAID level that combines RAID 5 and RAID 0, providing both improved performance and fault tolerance. To understand how many drives are necessary to maintain fault tolerance against two drive failures in a RAID 50 configuration, it is important to know how RAID 5 works. RAID 5 requires a minimum of three drives, providing fault tolerance against a single drive failure. In a RAID 50 setup, multiple RAID 5 arrays are striped together to form a single logical unit. Each of these RAID 5 arrays can tolerate one drive failure. If you want RAID 50 to sustain two drive failures, it means you should have at least two RAID 5 arrays, each being able to lose one drive while remaining operational. Therefore, to ensure reliable fault tolerance, the minimum number of drives needed for two RAID 5 arrays (each requiring at least three drives) would be six. Thus, with two RAID 5 arrays, each consisting of three drives, you achieve both the required number of drives to support the necessary fault tolerance as well as a balanced configuration that maximizes both performance and redundancy. This is why the answer of six drives is correct.

3. What command is used to retrieve performance statistics on FortiAnalyzer?

A. Get system performance

B. Get sys status

C. Get log performance

D. Get performance metrics

The command used to retrieve performance statistics on FortiAnalyzer is "Get system performance." This command provides valuable insights into the operational efficiency of the FortiAnalyzer device, including details about CPU usage, memory status, and log processing capabilities. Monitoring these performance metrics is crucial for administrators to ensure that the system is functioning optimally and to identify any potential issues that may affect log management or overall performance. Understanding the context of system performance is essential for maintaining the reliability and effectiveness of the FortiAnalyzer, especially in environments with high traffic volume or extensive log generation. This command helps in assessing how well the device is handling its tasks and can inform necessary adjustments to system resources or configurations to enhance performance.

4. In the log forwarding architecture, which component acts as the client?

A. The server that receives logs

B. The FAZ that forwards logs

C. The clients generating logs

D. The firewall

In the context of log forwarding architecture, the component that acts as the client is the FortiAnalyzer (FAZ) that forwards logs. The FortiAnalyzer functions as a centralized logging and reporting system that collects logs from various Fortinet devices, such as firewalls, and stores them for analysis and management. When we consider the roles within the architecture, the FortiAnalyzer is responsible for requesting log data from the generating clients, such as firewalls or other security devices. It actively polls or receives these logs, acting in a client capacity as it communicates with the logging sources. The classification of the FAZ as the client is based on its function of initiating the log retrieval process, while other components like the server or clients generating logs have different roles in the overall architecture. The server, for instance, typically refers to a storage or processing entity that might aggregate or present the data after it has been collected. In contrast, the clients generating logs refer to the devices that produce logs but do not engage in the forwarding process themselves. Therefore, the position of the FortiAnalyzer as the log forwarder clearly identifies it as the client in this architecture.

5. How can you change the ADOM mode in FortiAnalyzer using the GUI?

A. System settings > advanced > advanced settings

B. System settings > general > configurations

C. Device settings > ADOM selection

D. Administration > system settings

The correct method to change the ADOM mode in FortiAnalyzer using the GUI is found within the System settings section. Specifically, navigating to advanced settings under System settings allows you to modify configurations related to the operation and behavior of the FortiAnalyzer, including the ADOM (Administrative Domain) mode. ADOMs in FortiAnalyzer are essential for managing different sets of logs and reports for various FortiGate devices or groups of devices. By accessing the advanced settings, users can effectively switch between different ADOM modes—such as requiring different configurations or settings that are vital for multi-tenancy or organizational change. The other options do not lead to the correct setting for changing the ADOM mode, as they either pertain to other general configurations or relate to specific device settings rather than the overarching system-level adjustments needed for managing ADOM configurations.

6. What is required to resolve hostnames in logs on a FortiAnalyzer?

A. DNS server configured on FortiAnalyzer

B. Static IP settings applied

C. Manual hostname entry in logs

D. Local DNS cache adjustment

To resolve hostnames in logs on a FortiAnalyzer, it is essential to have a DNS server configured. This configuration enables the FortiAnalyzer to translate IP addresses into human-readable names, facilitating easier identification of devices associated with those IPs in the log entries. Without a working DNS server, the FortiAnalyzer would only display IP addresses in the logs instead of the corresponding hostnames, which could hinder the analysis and monitoring of network events. The other options do not provide the necessary functionality for hostname resolution. Static IP settings would not resolve to hostnames as they are merely fixed addresses without the ability to resolve into names. Manually entering hostnames into logs could be cumbersome and impractical as it does not provide a dynamic solution. Lastly, while local DNS cache adjustments can help with efficiency, they do not replace the requirement for a proper DNS server configuration necessary for initial hostname resolution.

7. What information does the failed authentication section of Fortiview display?

A. Number of successful logins

B. Current system status

C. Source IP of login, login type, interface, and number of failed attempts

D. Administrator login history

The failed authentication section of Fortiview provides critical details about unsuccessful login attempts, making it important for security monitoring and incident response. The information displayed includes the source IP address from which the login attempt originated, which helps identify potential malicious actors or unauthorized access attempts. It also indicates the login type, which shows what method was used for the authentication attempt, and the interface involved, giving insights into how attackers might be trying to gain access. Additionally, the section reports the number of failed attempts, which can be crucial for detecting brute force attacks or repeated login failure patterns over time. This comprehensive view aids security teams in analyzing and responding to authentication issues and potential threats effectively. Understanding this data is key to enhancing security policies and strategies within an organization.

8. What is one way to fine-tune a data set in FortiAnalyzer?

A. Add more columns

B. Setting a group, order by, and sort filter

C. Setting a limit on results

D. Setting the device and time frame

Fine-tuning a dataset in FortiAnalyzer enhances the relevance and clarity of the analysis you're conducting. One effective method to achieve this is by setting a group, order by, and sort filter. This approach allows you to organize the data according to specific attributes and criteria, making it easier to identify trends, anomalies, or important patterns within large sets of information. By grouping data, you can aggregate similar items together, which helps in a more coherent understanding of the relationships between different data points. Ordering the data based on specified fields facilitates a structured view, enabling users to see the most pertinent information at a glance. Moreover, applying sort filters lets you arrange the output in a way that highlights key aspects, such as sorting by the highest or lowest values, which can reveal insights that might otherwise go unnoticed. In contrast, while adding more columns, limiting results, or setting the device and time frame can also contribute to data analysis, they do not inherently provide the same level of fine-tuning that grouping, ordering, and sorting offer. These options may streamline results or define the dataset's boundaries, but they do not enhance the interpretative organization of the data itself as effectively as the chosen method.

9. A macro in FortiAnalyzer primarily defines what?

A. The visual layout of a report

B. Which data is to be selected from a log

C. The export settings for a report

D. The scheduling of reports

In FortiAnalyzer, a macro is utilized to define which data is to be selected from logs when generating reports. Macros act as placeholders or variables that can represent specific criteria or values, allowing for dynamic data selection based on user-defined parameters. This enables more customized reporting by allowing users to specify log fields or conditions that should be included in the report, ensuring that the data extracted is relevant to the analysis being performed. While the other options pertain to different aspects of report generation—like the visual layout, export settings, and scheduling—macros specifically focus on the data selection process, which is essential for tailoring reports according to the specific informational needs of the user or organization. By using macros effectively, users can streamline their reporting processes and enhance the clarity and relevance of the information presented in their reports.

10. What feature can you enable to boost report performance and reduce generation time?

A. Auto-cache

B. Manual refresh

C. Scheduled updates

D. Report compression

Enabling the auto-cache feature significantly enhances report performance and reduces the time it takes to generate reports. Auto-cache works by storing the frequently accessed data or report parameters in memory, so that subsequent requests can be served much faster. This eliminates the need to repeatedly process the same data or calculations for every report generation, leading to quicker results. In scenarios where reports are generated frequently or with similar parameters, auto-caching can be particularly beneficial, as it retrieves pre-computed results instead of starting from scratch each time. This effectively optimizes resource usage and speeds up report generation, making it a crucial feature for environments that rely heavily on timely data analysis and reporting. Other options, while potentially useful in different contexts, do not specifically address the need for enhanced performance in report generation as directly as auto-cache does.