Free Questions for NSE6_FAZ-7.2 by actualtestdumps

Shared by Mckinney on 28-02-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which command can you use to find the IP addresses of the devices sending logs to FortiAnalyzer?

Options:

A- diagnose debug application oftpd 8

B- diagnose dvm adorn List

C- diagnose teat application miglogd 6

D- diagnose best application oftpd 3

Answer:

A

Explanation:

The command diagnose debug application oftpd 8 is used to obtain detailed debug output for the OFTP (Over the FortiGate Protocol) daemon on FortiAnalyzer. This protocol is responsible for the communication and log transfer between FortiGate devices and FortiAnalyzer. By using this debug level, administrators can find information including the IP addresses of devices that are sending logs to FortiAnalyzer. Reference: FortiOS 7.4.1 Administration Guide, 'Diagnostic commands' section.

Question 2

Question Type: **MultipleChoice**

Which two statements about FortiAnalyzer operating modes are true? (Choose two.)

Options:

A- When in collector mode. FortiAnalyzer offloads the log receiving task to the analyzer.

B- Analyzer mode is the default operating mode.

C- For the collector, you should allocate most of the disk space to analytics logs.

D- When in analyzer mode. FortiAnalyzer supports event management and reporting features.

Answer:

B, D

Explanation:

The default operating mode for FortiAnalyzer is analyzer mode. In this mode, FortiAnalyzer provides full functionality for event management and reporting features. This mode is intended for environments where comprehensive analysis and reporting are required. It allows FortiAnalyzer to collect, analyze, and store logs, as well as generate reports and manage events. Reference: FortiAnalyzer 7.4.1 Administration Guide, 'Operating modes' section.

Question 3

Question Type: **MultipleChoice**

In a Fortinet Security Fabric, what can make an upstream FortiGate create traffic logs associated with sessions initiated on downstream FortiGate devices?

Options:

A- The traffic destination is another FoitiGate in the fabric.

B- Log redundancy is configured in the fabric.

C- The upstream FortiGate is configured to do NAT.

D- The downstream device cannot connect to FortiAnalyzer.

Answer:

D

Explanation:

In a Fortinet Security Fabric, an upstream FortiGate may create traffic logs for sessions initiated on downstream FortiGate devices if the downstream device is unable to connect to FortiAnalyzer. This allows for continuity of logging and ensures that session logs are captured and stored even if the downstream device loses its connection to the log management system. Reference: FortiAnalyzer 7.4.1 Administration Guide, 'Fortinet Security Fabric' section.

Question 4

Question Type: MultipleChoice

Which two of the available registration methods place the device automatically in its assigned ADOM? (Choose two.)

Options:

A- Request from the device

B- Serial number

C- Fabric Authorization

D- Pre-shared key

Answer:

B, C

Explanation:

The registration methods that automatically place a device in its assigned ADOM are using the serial number and fabric authorization. When devices are added to FortiAnalyzer using these methods, they are automatically placed in the appropriate ADOM, which could be a default ADOM based on the device type or a predefined ADOM based on the serial number or fabric authorization. This simplifies the management of devices and their logs by organizing them into their respective ADOMs from the moment they are registered. Reference: FortiAnalyzer 7.4.1 Administration Guide, 'Default device type ADOMs' and 'Assigning devices to an ADOM' sections.

Question 5

Question Type: **MultipleChoice**

Which process caches logs on FortiGate when FortiAnalyzer is not readable?

Options:

A- logfiled

B- sqlplugind

C- miglogd

D- oftpd

Answer:

A

Explanation:

The process logfiled in FortiGate units with an SSD disk is responsible for buffering logs when FortiAnalyzer is unreachable. If the connection to FortiAnalyzer is lost and the memory log buffer is full, logfiled allows logs to be buffered on disk. These logs are then sent to FortiAnalyzer once the connection is restored. This reliable logging mechanism ensures that logs are not lost during periods when FortiAnalyzer is not reachable, thereby maintaining log integrity and continuity. Reference: FortiOS 7.4.1 Administration Guide, 'Log Buffering' and 'Reliable Logging' sections.

Question 6

Question Type: MultipleChoice

What is true about a FortiAnalyzer Fabric?

Options:

A- Supervisors support HA.

B- Members events can be raised from the supervisor.

C- The supervisor and members cannot be in different time zones

D- The members send their logs to the supervisor.

Answer:

D

Explanation:

In a FortiAnalyzer Fabric, the FortiAnalyzer can recognize a Security Fabric group of devices, and it supports the Security Fabric by storing and analyzing logs from these units as if they were from a single device. The members of the Security Fabric group send their logs to the FortiAnalyzer, which acts as a supervisor for log storage and analysis, providing a centralized point of visibility and control over the logs. Reference: FortiAnalyzer 7.4.1 Administration Guide, 'Security Fabric' section.

Question 7

Question Type: **MultipleChoice**

Which FortiAnalyzer command erases all device settings, images, databases, and logs on disk, but preserves The network configuration?

Options:

A- execute factory-reset

B- execute format disk

C- execute formatlogdisk

D- execute reset all-except---ip

Answer:

A

Explanation:

The FortiAnalyzer command execute factory-reset is used to erase all device settings, images, databases, and logs on disk but preserves the current IP address and route information. This command effectively resets the FortiAnalyzer to its factory settings while maintaining its network configuration, allowing it to be quickly reconfigured with the same network settings. Reference: FortiAnalyzer 7.4.1 Administration Guide, 'Reset Commands' section.

Question 8

Question Type: MultipleChoice

Which statement is true about ADOMs?

Options:

A- When a FortiAnalyzer Fabric is implemented, the default ADOM mode is set to advanced.

B- A fabric ADOM can include all the device types supported by FortiAnalyzer.

C- You can change the ADOM mode only through the GUI.

D- In normal mode, you cannot change the disk quota of the ADOM after its creation.

Answer:

B

Explanation:

Regarding ADOMs (Administrative Domains) in FortiAnalyzer, a fabric ADOM is capable of including all device types that FortiAnalyzer supports. This is part of the flexibility offered by ADOMs to manage and report on logs from various devices within a Fortinet security fabric. ADOMs can be enabled to support non-FortiGate devices as well, and the root ADOM in Fabric ADOMs provides visibility into all Security Fabric devices. Additionally, it should be noted that in normal mode, you cannot assign different FortiGate VDOMs to different ADOMs, while in advanced mode, you can, which provides a more granular control over the log data from individual VDOMs. Reference: FortiAnalyzer 7.4.1 Administration Guide, 'ADOMs' and 'ADOM device modes' sections.

Question 9

Question Type: MultipleChoice

Which two statements are true regarding FortiAnalyzer system backups? (Choose two.)

Options:

A- Existing reports can be included in the backup files.

B- The system reserves at least 5% to 20% disk space for backup files.

C- Scheduled system backups can be configured only from the CLI.

D- Backup files can be uploaded to SCP and SFTP servers.

Answer:

A, D

Explanation:

FortiAnalyzer allows for the inclusion of existing reports in the backup files, providing a comprehensive backup of configurations and data. Additionally, the backup files can be configured to be uploaded to SCP and SFTP servers, ensuring secure transfer and offsite storage of backup data. This can be configured both in the GUI and the CLI, providing flexibility in how backups are scheduled and managed. Reference: FortiAnalyzer 7.4.1 Administration Guide, 'Scheduling automatic backups' section.

Question 10

Question Type: MultipleChoice

Which statement is true about the communication between FortiGate high availability (HA) clusters and FortiAnalyzer?

Options:

A- Each cluster member sends its logs directly to FortiAnalyzer.

B- You must add the device lo the cluster first, and then registers the cluster with FortiAnalyzer.

C- FortiAnalyzer distinguishes each cluster member by its MAC address.

D- Only the primary device in the cluster communicates with FortiAnalyzer.

Answer:

D

Explanation:

In a FortiGate high availability (HA) cluster, only the primary device sends its logs to the FortiAnalyzer. This is to ensure that logs are not duplicated between the primary and secondary devices in the cluster. The configuration of the FortiAnalyzer server on the FortiGate is such that the HA primary device is set as the server that forwards the logs. Reference: FortiAnalyzer 7.4.1 Administration Guide, sections mentioning HA cluster configuration and log forwarding.

20%
DISCOUNT