DUMPSHQ

Free Questions for NSE6_FAZ-7.2 by dumpshq

Shared by Nash on 24-05-2024

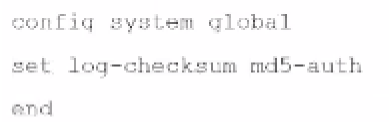
For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

An administrator has configured the following settings:



```
config system global
set log-checksum md5-auth
end
```

What is the purpose of executing these commands?

Options:

A- To record the hash value and authentication code of log files.

B- To encrypt log transfer between FortiAnalyzer and other devices.

C- To verify the integrity of the log files received.

D- To create the secure channel used by the OFTP process.

Answer:

C

Explanation:

The purpose of executing the provided CLI commands, which include setting the log-checksum to md5-auth, is to ensure the integrity of the log files. This setting is used to record the MD5 hash value of log files, which is a widely used cryptographic hash function that produces a 128-bit (16-byte) hash value. By using MD5 authentication, FortiAnalyzer ensures that the log files have not been altered or tampered with during transit, thereby verifying their integrity upon receipt. This is not related to encrypting log transfers, scheduling reports, or creating secure channels for OFTP (Over-the-FortiGate Protocol) processes.

Question 2

Question Type: MultipleChoice

What is true about FortiAnalyzer reports?

Options:

A- When you enable auto-cache, reports are scheduled by default.

B- Reports can be saved in a CSV format.

C- You require an output profile before reports are generated.

D- The reports from one ADOM are available for all ADOMs.

Answer:

C

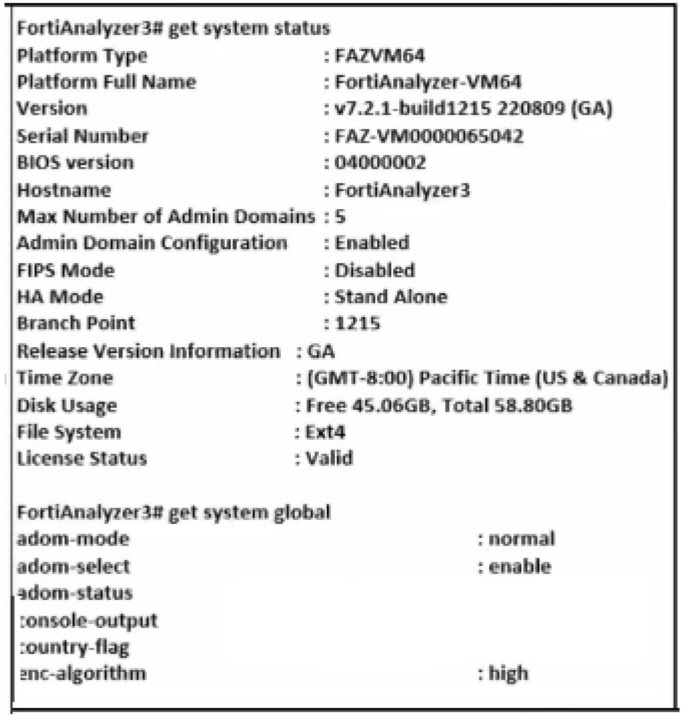
Explanation:

For FortiAnalyzer reports, an output profile must be configured before reports can be generated and sent to an external server or system. This output profile determines how the reports are distributed, whether by email, uploaded to a server, or any other supported method. The options such as auto-cache, saving reports in CSV format, or reports availability across different ADOMs are separate features/settings and not directly related to the requirement of having an output profile for report generation.

Question 3

Question Type: MultipleChoice

Refer to the exhibit.



```
FortiAnalyzer3# get system status
Platform Type                   : FAZVM64
Platform Full Name              : FortiAnalyzer-VM64
Version                         : v7.2.1-build1215 220809 (GA)
Serial Number                   : FAZ-VM0000065042
BIOS version                    : 04000002
Hostname                        : FortiAnalyzer3
Max Number of Admin Domains : 5
Admin Domain Configuration      : Enabled
FIPS Mode                       : Disabled
HA Mode                         : Stand Alone
Branch Point                    : 1215
Release Version Information  : GA
Time Zone                     : (GMT-8:00) Pacific Time (US & Canada)
Disk Usage                    : Free 45.06GB, Total 58.80GB
File System                   : Ext4
License Status                : Valid

FortiAnalyzer3# get system global
adom-mode                                         : normal
adom-select                                       : enable
adom-status
console-output
country-flag
enc-algorithm                                     : high
```

Based on the partial outputs displayed in the exhibit, which devices are ready to be configured as peers in an HA cluster?

Options:

A- FortiAnalyzer1 and FortiAnalyzer3

B- FortiAnalyzer1 and FortiAnalyzer2

C- These devices cannot participate in the same cluster.

D- FortiAnalyzer2 and FortiAnalyzer3

Answer:

C

Explanation:

Based on the provided exhibit, which shows partial outputs of the system status and global settings for FortiAnalyzer devices, the devices cannot be configured as peers in an HA (High Availability) cluster. This is indicated by the HA Mode status being set to 'Stand Alone' for the displayed FortiAnalyzer device. For devices to be part of an HA cluster, they would need to have compatible HA configurations, and usually, they should not be in 'Stand Alone' mode. Additionally, the exhibit only shows information for one FortiAnalyzer, so it cannot be determined if there is another device ready to form an HA cluster with it.

Question 4

Question Type: **MultipleChoice**

Which two methods can you use to restrict administrative access on FortiAnalyzer? (Choose two.)

Options:

A- Use administrator profiles.

B- Configure trusted hosts.

C- Fabric connectors to external LDAP servers.

D- Limit access to specific virtual domains.

Answer:

A, B

Explanation:

To restrict administrative access on FortiAnalyzer, two effective methods are using administrator profiles and configuring trusted hosts. Administrator profiles allow for defining the level of access and permissions for different administrators, controlling what each administrator can see and do within the FortiAnalyzer unit. Configuring trusted hosts enhances security by limiting administrative access to specified IP addresses, ensuring that administrators can only connect from approved locations or networks, thus preventing unauthorized access from outside specified subnets or IP addresses. Reference: FortiAnalyzer 7.4.1 Administration Guide, 'Administrators' and 'Trusted hosts' sections.

Question 5

Question Type: **MultipleChoice**

A rogue administrator was accessing FortiAnalyzer without permission.

Where can you view the activities that the rogue administrator performed on FortiAnalyzer?

Options:

A- FortiView

B- Fabric View

C- Log View

D- System Settings

Answer:

A

Explanation:

To monitor the activities performed by any administrator, including a rogue one, on the FortiAnalyzer, you should use the FortiView feature. FortiView provides a comprehensive overview of the activities and events happening within the FortiAnalyzer environment, including administrator actions, making it the appropriate tool for tracking unauthorized or suspicious activities. Reference: FortiAnalyzer 7.4.1 Administration Guide, 'System Settings > Fabric Management' section.

Question 6

Question Type: **MultipleChoice**

Which two statements are true regarding fabric connectors? (Choose two.)

Options:

A- Using fabric connectors is more efficient than third-party polling information from the FortiAnalyzer API

B- Cloud-out connectors allow you to send real-time logs to public cloud accounts like Amazon S3.

C- Fabric connectors allow you to save storage costs and improve redundancy.

D- The storage connector service does not require a separate license to send logs to the cloud platform.

Answer:

A, D

Explanation:

Fabric connectors in FortiAnalyzer, such as security fabric connectors (e.g., FortiClient EMS, FortiMail, FortiCASB) and storage connectors (e.g., Amazon S3, Azure Blob Container, Google Cloud Storage), provide efficient integration and data sharing capabilities. Using fabric connectors for direct integration with FortiAnalyzer is more efficient and reliable than relying on third-party applications to poll information through the FortiAnalyzer API. Additionally, the ability to send logs to cloud storage platforms like Amazon S3, Azure Blob, and Google Cloud directly through storage connectors is a built-in feature that does not require an additional license, thus saving on storage costs and improving redundancy without incurring extra licensing fees. Reference: FortiAnalyzer 7.4.1 Administration Guide, 'Fabric Connectors' and 'Storage connectors' sections.

Question 7

Question Type: MultipleChoice

An administrator, fortinet, can view logs and perform device management tasks, such as adding and removing registered devices. However, administrator fortinet is not able to create a mail server that can be used to send alert emails.

What can be the problem?

Options:

A- ADOM mode is configured with Advanced mode.

B- fortinet is assigned the Standard_User administrative profile.

C- A trusted host is configured.

D- fortinet is assigned Restricted_User administrative profile.

Answer:

B

Explanation:

If the administrator 'fortinet' can view logs and perform device management tasks but cannot create a mail server for alert emails, it is likely due to the administrative profile assigned to them. The Standard_User administrative profile may restrict certain administrative functions, such as creating mail servers. To perform all administrative tasks, including creating mail servers, a higher privilege profile, such as Super_Admin, might be required. Reference: FortiAnalyzer 7.2 Administrator Guide, 'Mail Server' section.

20%
DISCOUNT