



Vendor: Fortinet

Exam Code: NSE6_FAZ-7.2

Exam Name: Fortinet NSE 6 - FortiAnalyzer 7.2
Administrator

Version: DEMO

QUESTION 1

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?

- 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.

QUESTION 2

What is true about FortiAnalyzer reports?

- 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

What is true about a FortiAnalyzer Fabric?

- 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.

QUESTION 4

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

- A. Each cluster member sends its logs directly to FortiAnalyzer.
- B. You must add the device to 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.

QUESTION 5

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

- 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: AD

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.

QUESTION 6

Which statement is true about ADOMs?

- 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.

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

- ★ More than **99,900** Satisfied Customers Worldwide.
- ★ Average **99.9%** Success Rate.
- ★ **Free Update** to match latest and real exam scenarios.
- ★ **Instant Download** Access! No Setup required.
- ★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.
- ★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.
- ★ **100%** Guaranteed Success or **100%** Money Back Guarantee.
- ★ **Fast**, helpful support **24x7**.



View list of all certification exams: <http://www.lead2pass.com/all-products.html>



Microsoft



ORACLE



CITRIX



JUNIPER
NETWORKS



EMC²
where information lives

10% Discount Coupon Code: ASTR14