

# Fortinet

## Exam Questions NSE6\_FAZ-7.2

Fortinet NSE 6 - FortiAnalyzer 7.2 Administrator



#### NEW QUESTION 1

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

- A. logfiled
- B. sqlplugind
- C. miglogd
- D. oftpd

**Answer:** A

#### Explanation:

The processlogfiledin 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,logfiledallows 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.References:FortiOS 7.4.1 Administration Guide, "Log Buffering" and "Reliable Logging" sections.

#### NEW QUESTION 2

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

- A. diagnose debug applicationoftpd 8
- B. diagnose dvm adorn List
- C. diagnose teatapplication miglogd6
- D. diagnose bestapplicationoftpd 3

**Answer:** A

#### Explanation:

The commanddiagnose debug application oftpd 8is 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.References:FortiOS 7.4.1 Administration Guide, "Diagnostic commands" section.

#### NEW QUESTION 3

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

- A. When in collector mod
- B. FortiAnalyzer offloads the log receiving task to the analyzer.
- C. Analyzer mode is the default operating mode.
- D. For the collector, you should allocate most of the disk space to analytics logs.
- E. When in analyzer mod
- F. FortiAnalyzer supports event management and reporting features.

**Answer:** BD

#### 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.References:FortiAnalyzer 7.4.1 Administration Guide, "Operating modes" section.

#### NEW QUESTION 4

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.References:FortiAnalyzer 7.4.1 Administration Guide, "ADOMs" and "ADOM device modes" sections.

#### NEW QUESTION 5

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 lo the cluster first, and thenregistersthe 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. References: FortiAnalyzer 7.4.1 Administration Guide, sections mentioning HA cluster configuration and log forwarding.

**NEW QUESTION 6**

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. References: FortiAnalyzer 7.4.1 Administration Guide, "Scheduling automatic backups" section.

**NEW QUESTION 7**

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?

- 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.

#### NEW QUESTION 8

A rogue administrator was accessing FortiAnalyzer without permission.

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

- 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. References: FortiAnalyzer 7.4.1 Administration Guide, "System Settings > Fabric Management" section.

#### NEW QUESTION 9

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

- A. Use administrator profiles.
- B. Configure trusted hosts.
- C. Fabric connectors to external LDAP servers.
- D. Limit access to specific virtual domains.

**Answer:** AB

#### 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.

#### NEW QUESTION 10

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

- 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:** AD

#### 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.

#### NEW QUESTION 10

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. Reference: FortiAnalyzer 7.2 Administrator Guide, 'Mail Server' section.

#### NEW QUESTION 13

Which two settings must you configure on FortiAnalyzer to allow non-local administrators to authenticate on FortiAnalyzer with any user account in a single LDAP group? (Choose two.)

- A. LDAP servers IP addresses added as trusted hosts
- B. One or more remote LDAP servers
- C. A local wildcard administrator account
- D. An administrator group

**Answer:** BD

**Explanation:**

To allow non-local administrators to authenticate on FortiAnalyzer with any user account in a single LDAP group, you must configure one or more remote LDAP servers and an administrator group. First, you configure the LDAP server(s) by specifying the server name, IP, and other details such as the Common Name Identifier and Distinguished Name. Then, you add the LDAP server to a user group. Finally, you create an administrator account that uses this user group for authentication, allowing any user from the specified LDAP group to authenticate. References: FortiAnalyzer 7.2 Administrator Guide, "Configuring remote authentication for administrators using LDAP" section.

**NEW QUESTION 14**

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. References: FortiAnalyzer 7.4.1 Administration Guide, "Security Fabric" section.

**NEW QUESTION 15**

Which statement is true about using aggregation mode on FortiAnalyzer?

- A. Aggregation mode supports log filters.
- B. Aggregation mode can work with syslog servers.
- C. In aggregation mode, logs and content files are forwarded in real time.
- D. Aggregation mode can be configured only on the CLI.

**Answer:** B

**Explanation:**

In aggregation mode, FortiAnalyzer stores logs received from devices and forwards them at a specified time each day to avoid duplication. It is specifically designed to work between two FortiAnalyzer units and does not support syslog or CEF servers. Additionally, aggregation mode configurations are limited to CLI commands `log-forward` and `log-forward-service`. References: FortiAnalyzer 7.2 Administrator Guide, "Aggregation" and "CLI Commands for Aggregation Mode" sections.

**NEW QUESTION 20**

Which feature can you configure to add redundancy to FortiAnalyzer?

- A. Primary and secondary DNS
- B. VLAN interfaces
- C. IPv6 administrative access
- D. Link aggregation

**Answer:** D

**Explanation:**

Link aggregation is a method used to combine multiple network connections in parallel to increase throughput and provide redundancy in case one of the links fail. This feature is used in network appliances, including FortiAnalyzer, to add redundancy to the network connections, ensuring that there is a backup path for traffic if the primary path becomes unavailable. References: The FortiAnalyzer 7.4.1 Administration Guide explains the concept of link aggregation and its relevance to

**NEW QUESTION 21**

.....

## Thank You for Trying Our Product

### We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

### NSE6\_FAZ-7.2 Practice Exam Features:

- \* NSE6\_FAZ-7.2 Questions and Answers Updated Frequently
- \* NSE6\_FAZ-7.2 Practice Questions Verified by Expert Senior Certified Staff
- \* NSE6\_FAZ-7.2 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* NSE6\_FAZ-7.2 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The NSE6\\_FAZ-7.2 Practice Test Here](#)**