



# Fortinet

## Exam Questions NSE6\_FAZ-7.2

Fortinet NSE 6 - FortiAnalyzer 7.2 Administrator

## About ExamBible

*[Your Partner of IT Exam](#)*

## Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

## Our Advances

### \* 99.9% Uptime

All examinations will be up to date.

### \* 24/7 Quality Support

We will provide service round the clock.

### \* 100% Pass Rate

Our guarantee that you will pass the exam.

### \* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

### NEW QUESTION 1

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 2

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 3

You finished registering a FortiGate device. After traffic starts to flow through FortiGate. you notice that only some of the logs expected are being received on FortiAnalyzer.

What could be the reason for the logs not arriving on FortiAnalyzer?

- A. FortiGate does not have logging configured correctly.
- B. This FortiGate model is not fully supported.
- C. This FortiGate is part of an HA cluster but it is the secondary device.
- D. FortiGate was added to the wrong ADOM type.

**Answer:** A

#### Explanation:

When only some of the expected logs from a FortiGate device are being received on FortiAnalyzer, it often indicates a configuration issue on the FortiGate side. Proper logging configuration on FortiGate involves specifying what types of logs to generate (e.g., traffic, event, security logs) and ensuring that these logs are directed to the FortiAnalyzer unit for storage and analysis. If the logging settings on FortiGate are not correctly configured, it could result in incomplete log data being sent to FortiAnalyzer. This might include missing logs for certain types of traffic or events that are not enabled for logging on the FortiGate device. Ensuring comprehensive logging is enabled and correctly directed to FortiAnalyzer is crucial for full visibility into network activities and for the effective analysis and reporting of security incidents and network performance.

### NEW 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 register 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. References: FortiAnalyzer 7.4.1 Administration Guide, sections mentioning HA cluster configuration and log forwarding.

### NEW QUESTION 5

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 6**

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 7**

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

- A. Request from the device
- B. Serial number
- C. Fabric Authorization
- D. Pre-shared key

**Answer:** BC

**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.

**NEW QUESTION 8**

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 9**

Refer to the exhibit.

Cluster Settings

Operation Mode

StandaloneHigh Availability

Preferred Role

SecondaryPrimary

Cluster Virtual IP

IP Address and Interface

IP Address

Interface

192.168.101.222

port1

Cluster Settings

Peer IP and Peer SN

Peer IP

Peer SN

10.0.1.210

FAZ-VM0000065040

Group Name

NSE6

Group ID

1

(1-255)

Password

.....

Heart Beat Interval

10

Seconds

Failover Threshold

30

Prio

120

The image displays "he configuration of a FortiAnalyzer the administrator wants to join to an existing HA cluster. What can you conclude from the configuration displayed?

- A. After joining to the cluster, this FortiAnalyzer will keep an updated log database.
- B. This FortiAnalyzer will trigger a failover after losing communication with its peers for 10 seconds.
- C. This FortiAnalyzer will join to the existing HA cluster as the primary.
- D. This FortiAnalyzer is configured to receive logs in its port1.

Answer: D

Explanation:

The configuration displayed in the exhibit indicates that the FortiAnalyzer is set up with a cluster virtual IP address of 192.168.101.222 assigned to interface port1. This setup is typically used for the FortiAnalyzer to receive logs on that interface when operating in a High Availability (HA) configuration. The exhibit does not provide enough information to conclude whether this FortiAnalyzer will be the primary unit in the HA cluster or the duration for the failover trigger; it only confirms the interface configuration for log reception. References: Based on the FortiAnalyzer 7.4.1 Administration Guide, the similar configurations for HA and log reception are discussed, which would be relevant for understanding the settings in FortiAnalyzer 7.2.

NEW QUESTION 10

Which two parameters impact the amount of reserved disk space required by FortiAnalyzer? (Choose two.)

- A. Disk size
- B. Total quota
- C. RAID level
- D. License type

Answer: AC

Explanation:

The amount of reserved disk space required by FortiAnalyzer is influenced by the disk size and the RAID level. The system reserves a portion of the disk space for system use and unexpected quota overflow, with the rest available for device allocation. The RAID level determines the disk size and the reserved disk quota level, with different RAID configurations leading to variations in the reserved space. References: FortiAnalyzer 7.2 Administrator Guide, "Disk Space Allocation" and "RAID Level Impact" sections.

NEW QUESTION 10

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 15**

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 16**

What are analytics logs on FortiAnalyzer?

- A. Logs that are compressed and saved to a log file
- B. Logs that roll over when the log file reaches a specific size
- C. Logs that are indexed and stored in the SQL
- D. Logs classified as type Traffic, or type Security

**Answer:** C

**Explanation:**

On FortiAnalyzer, analytics logs refer to the logs that have been processed, indexed, and then stored in the SQL database. This process allows for efficient data retrieval and analytics. Unlike basic log storage, which might involve simple compression and storage in a file system, analytics logs in FortiAnalyzer undergo an indexing process. This enables advanced features such as quick search, report generation, and detailed analysis, making it easier for administrators to gain insights into network activities and security incidents.

Reference:

FortiAnalyzer 7.2 Administrator Guide - "Log Management" and "Data Analytics" sections.

**NEW QUESTION 20**

Which items must you configure on FortiAnalyzer to send its reports to an external server?

- A. Report schedule
- B. Mail server
- C. Fabric connector
- D. Output profile

**Answer:** D

**Explanation:**

To send reports from FortiAnalyzer to an external server, you must configure the output profile. This involves specifying the method (FTP, SFTP, or SCP), server IP, username, password, and the directory where the report will be saved. Additionally, you have the option to delete the report after it has been uploaded to the server.

Reference: FortiAnalyzer 7.2 Administrator Guide, "Enable uploading of generated reports to a server" section.

**NEW QUESTION 22**

Refer to the exhibit.



Wireshark · Packet 5 · sniffer\_port3.1 (1).pcap

```
> Frame 5: 345 bytes on wire (2760 bits), 345 bytes captured (2760 bits)
> Ethernet II, Src: MS-NLB-PhysServer-09_0f:00:01:06 (02:09:0f:00:01:06),
> Internet Protocol Version 4, Src: 10.200.3.1, Dst: 10.200.1.210
> User Datagram Protocol, Src Port: 8678, Dst Port: 514
```

```
> [truncated]Syslog message: (unknown): \001\020\020\004\000\001\0
> Message: \001\020\020\004
```

0000	02 09 0f 00 02 06 02 09 0f 00 01 06 08 00 45 00	-----E-
0010	01 4b bb b3 00 00 3f 11 a4 8c 0a c8 03 01 0a c8	-K-...?-.....
0020	01 d2 21 e6 02 02 01 37 81 ea ec cf 20 60 01 10	..!-...7 .... *
0030	10 04 00 01 00 f7 00 fe 63 a1 53 9a 46 47 56 4d	.....c·S·FGVM
0040	30 31 30 30 30 30 30 36 35 30 33 36 52 65 6d 6f	01000006 5036Remo
0050	74 65 2d 46 6f 72 74 69 47 61 74 65 72 6f 6f 74	te-Forti Gateroot
0060	00 fe f1 14 64 61 74 65 3d 32 30 32 32 2d 31 32	...date =2022-12
0070	2d 31 39 20 74 69 6d 65 3d 32 32 3a 31 38 3a 30	-19 time =22:18:0
0080	32 20 65 76 65 6e 74 13 00 f1 29 31 36 37 31 35	2 event- ..)16715
0090	31 37 30 38 32 34 34 35 33 36 31 38 38 31 20 74	17082445 361881 t
00a0	7a 3d 22 2d 30 38 30 30 22 20 6c 6f 67 69 64 3d	z="-0800 " logid=
00b0	22 30 31 30 30 30 32 30 30 31 34 22 20 74 79 70	"0100020 014" typ
00c0	65 3d 22 42 00 52 22 20 73 75 62 10 00 f1 11 73	e="B·R" sub-...s
00d0	79 73 74 65 6d 22 20 6c 65 76 65 6c 3d 22 77 61	ystem" l evel="wa
00e0	72 6e 69 6e 67 22 20 76 64 3d 22 72 6f 6f 74 4b	rning" v d="rootK
00f0	00 f0 12 64 65 73 63 3d 22 54 65 73 74 22 20 75	...desc= "Test" u
0100	73 65 72 3d 22 61 64 6d 69 6e 22 20 61 63 74 69	ser="adm in" acti
0110	6f 6e 3d 22 6f 00 f0 0a 6e 22 20 73 74 61 74 75	on="o-... n" statu
0120	73 3d 22 73 75 63 63 65 73 73 22 20 6d 73 67 3d	s="succe ss" msg=
0130	22 32 00 11 20 31 00 00 97 00 f0 0e 67 65 64 20	"2- 1- ...ged
0140	69 6e 74 6f 20 74 68 65 20 66 77 20 2d 20 31 36	into the fw - 16
0150	37 31 35 31 37 30 38 32 22	71517082 "

Which image corresponds to the packet capture shown in the exhibit?

A)



B)



C)

Device Manager

Device Group

Edit

Delete

More

<div><input type="checkbox"/></div>	▲ Device Name	Platform	Logs	Average Log Rate(Logs/Sec)
<div><input type="checkbox"/></div>	Remote-FortiGate	FortiGate-VM64	<div><div></div>Real Time</div>	0

- A. Option A
- B. Option B
- C. Option A

Answer: D

Explanation:

The exhibit shows a packet capture with a syslog message containing a log event from a FortiGate device. This log event includes several details such as the date, time, and event message. The corresponding image that matches this packet capture would be the one which shows that the FortiGate device has logs being received in real-time, as indicated by the highlighted section in the packet capture where it mentions "real-time". Therefore, Option A is the correct answer because it shows logs with "Real Time" status for the FortiGate-VM64 device, indicating that this FortiAnalyzer is currently receiving real-time logs from the device, matching the activity in the packet capture.

Reference: Based on the provided exhibits and the real-time logging information, correlated with the knowledge from the FortiAnalyzer 7.2 Administrator documentation regarding log reception and device management.

NEW QUESTION 25

.....



## Relate Links

**100% Pass Your NSE6\_FAZ-7.2 Exam with Exambible Prep Materials**

[https://www.exambible.com/NSE6\\_FAZ-7.2-exam/](https://www.exambible.com/NSE6_FAZ-7.2-exam/)

## Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>