

NSE6_FAZ-7.2 Dumps

Fortinet NSE 6 - FortiAnalyzer 7.2 Administrator

https://www.certleader.com/NSE6_FAZ-7.2-dumps.html



NEW QUESTION 1

An administrator has configured the following settings:

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

What is the purpose of executing these commands?

- 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.

NEW QUESTION 2

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 3

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.

NEW QUESTION 4

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 5

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 6

Which statement is true when you are upgrading the firmware on an HA cluster made up of three FortiAnalyzer devices?

- A. All FortiAnalyzer devices will be upgraded at the same time.
- B. Enabling uninterruptible-upgrade prevents normal operations from being interrupted during the upgrade.
- C. You can perform the firmware upgrade using only a console connection.
- D. First, upgrade the secondary devices, and then upgrade the primary device.

Answer: D

Explanation:

In an HA cluster, the firmware upgrade process involves upgrading the secondary devices first. This approach ensures that the primary device can continue to handle traffic and maintain the operational stability of the network while the secondary devices are being upgraded. Once the secondary devices have successfully upgraded their firmware and are operational, the primary device can then be upgraded. This method minimizes downtime and maintains network integrity during the upgrade process.

When upgrading firmware in a High Availability (HA) cluster of FortiAnalyzer units, the recommended practice is to first upgrade the secondary devices before upgrading the primary device. This approach ensures that the primary device, which coordinates the cluster's operations, remains functional for as long as possible, minimizing the impact on log collection and analysis. Once the secondary devices are successfully upgraded and operational, the primary device can be upgraded, ensuring a smooth transition and maintaining continuous operation of the cluster. References: FortiAnalyzer 7.2 Administrator Guide - "System Administration" and "High Availability" sections.

NEW QUESTION 7

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 8

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

- A. The traffic destination is another FortiGate 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. References: FortiAnalyzer 7.4.1 Administration Guide, "Fortinet Security Fabric" section.

NEW QUESTION 9

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 10

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 10

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 12

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 4dc.S.FGVH
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 32date =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>	<div><div></div>Remote-FortiGate</div>	FortiGate-VM64	<div><div></div>Real Time</div>	<div>0</div>

- 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 16

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your NSE6_FAZ-7.2 Exam with Our Prep Materials Via below:

https://www.certleader.com/NSE6_FAZ-7.2-dumps.html