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 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 2
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 3
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 4
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 thelog-checksumtomd5-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 5
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 6
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 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
Which two statements are true regarding the log synchronization states for HA on FortiAnalyzer? (Choose two.)

A. Log Data Sync provides real-time log synchronization to all backup devices.
B. When Log Data Sync is turned on, the backup device reboots and then rebuilds the log database with the synchronized logs.
C. With Initial Logs Sync, when you add a unit to an HA cluster, the primary device synchronizes its logs with the backup device.
D. By defaul
E. Log Data Sync is disabled on all backup devices.

Answer: AC

Explanation:
For HA on FortiAnalyzer, Log Data Sync ensures real-time log synchronization among all cluster members, including backup devices. This feature is enabled by default. The Initial Logs Sync state is triggered when a new unit is added to an HA cluster, where the primary unit synchronizes its logs with the newly added unit. After the initial synchronization, the secondary unit reboots and rebuilds its log database with the synchronized logs.References:FortiAnalyzer 7.2 Administrator Guide, "Log synchronization" section.

NEW QUESTION 9
Which FortiAnalyzer command erases all device settings, images, databases, and logs on disk, but preserves The network configuration?

A. executefactory-reset
B. executeformat disk
C. executeformatlogdisk
D. executereset all-except—ip

Answer: A

Explanation:
The FortiAnalyzer commandexecute factory-resetis used to erase all device settings, images, databases, and logs on disk but preserves the current IP address and route information. This command effectively resets the FortiAnalyzer to its factory settings while maintaining its network configuration, allowing it to be quickly reconfigured with the same network settings.References:FortiAnalyzer 7.4.1 Administration Guide, "Reset Commands" section.

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 10
.....

Relate Links

100% Pass Your NSE6_FAZ-7.2 Exam with Exambible Prep Materials

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/