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 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
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
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 5
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 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 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 8
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 9

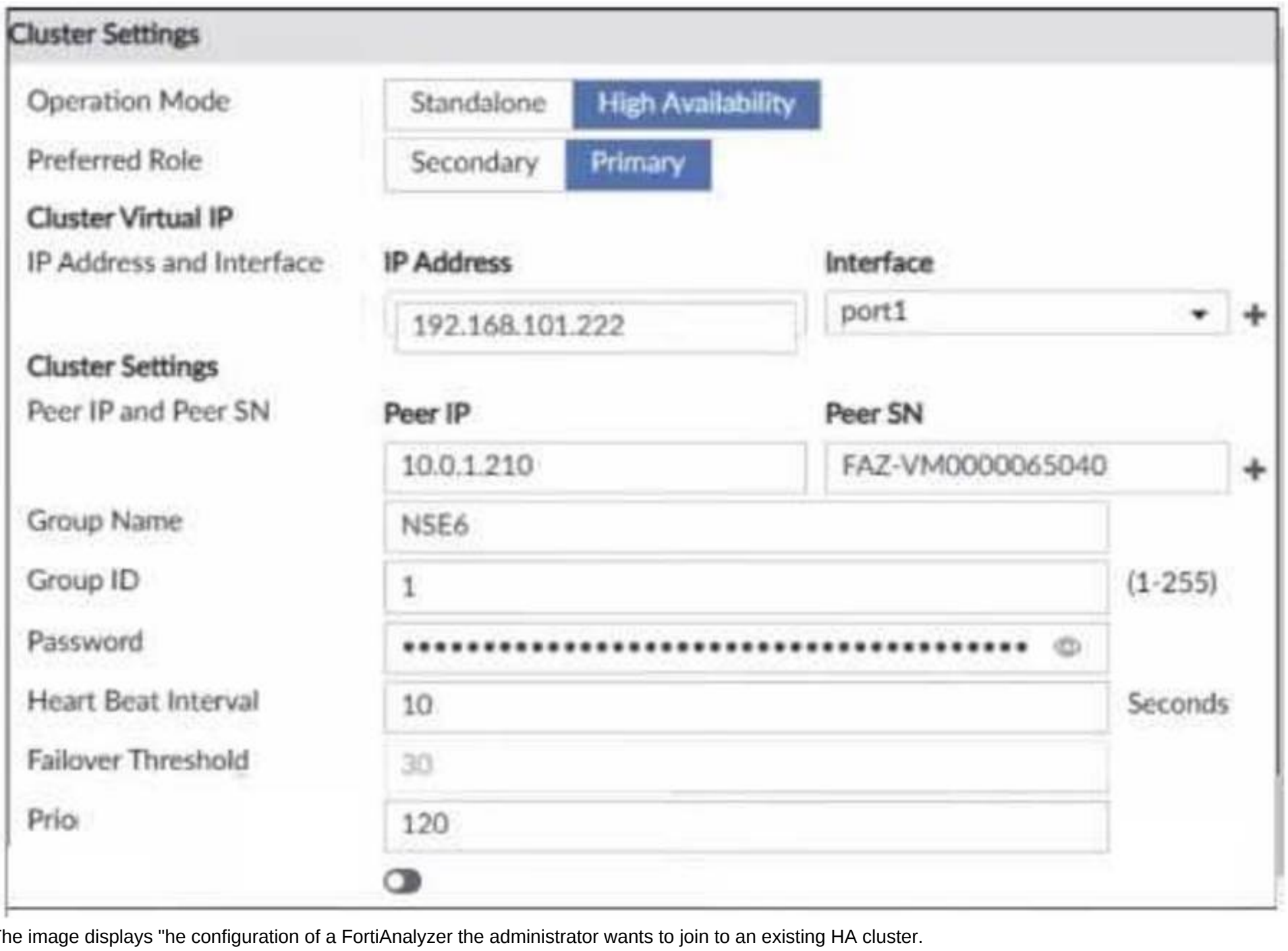
After you have moved a registered logging device out of one ADOM and into a new ADOM, you run the following command: execute sql-local rebuild-adom <new-ADOM-name>
What is the purpose of running this CLI command?

A. To reset the ADOM disk quota enforcement to its default value
B. To migrate the archive logs to the new ADOM
C. To populate the new ADOM with analytical logs for the moved device, so you can run reports
D. To remove the analytics logs of the device from the old database

Answer: C

Explanation:
When you move a registered logging device from one ADOM (Administrative Domain) to another in FortiAnalyzer, it's essential to ensure that the analytical logs for the moved device are available in the new ADOM to maintain continuity in reporting and log analysis. The commandexecute sql-local rebuild-adom < new-ADOM-name>is used specifically for this purpose. Running this command populates the new ADOM with the analytical logs of the moved device, enabling you to generate accurate and comprehensive reports based on the historical data of the device in its new ADOM context. This process ensures that the transition of devices between ADOMs does not lead to a loss of analytical insight or reporting capabilities for the device's traffic and events.

NEW QUESTION 10
Refer to the exhibit.



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
What is the best approach to handle a hard disk failure on a FortiAnalyzer that supports hardware RAID?

A. Shul down FortiAnalyzer and replace the disk.
B. Perform a hot swap of the disk.

C. Run execute format disk to format and restart the FortiAnalyzer device.
D. There is no need to do anything because the disk will self-recover.

Answer: B

Explanation:
In systems that support hardware RAID, hot swapping allows for the replacement of a failed disk without shutting down the system. This capability is crucial for maintaining uptime and ensuring data redundancy and availability, especially in critical environments. The RAID controller rebuilds the data on the new disk using redundancy data from the other disks in the array, ensuring no data loss and minimal impact on system performance.
In the context of a FortiAnalyzer unit equipped with hardware RAID support, the optimal approach to addressing a hard disk failure is to perform a hot swap of the disk. Hardware RAID configurations are designed to provide redundancy and fault tolerance, allowing for the replacement of a failed disk without the need to shut down the system. Hot swapping enables the administrator to replace the faulty disk with a new one while the system is still running, and the RAID controller will rebuild the data on the new disk, restoring the RAID array to its fully operational state.References:FortiAnalyzer 7.2 Administrator Guide - "Hardware Maintenance" and "RAID Management" sections.

NEW QUESTION 14
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 16
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 17
.....

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/