Free Questions for NSE6_FAZ-7.2

Shared by Beck on 04-10-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

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

What is the purpose of running this CLI command?

Options:

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 command execute 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.

Question 2

Question Type: **MultipleChoice**

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

Options:

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. Reference: FortiAnalyzer 7.2 Administrator Guide - 'Hardware Maintenance' and 'RAID Management' sections.

Question 3

Question Type: MultipleChoice

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

Options:

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. Reference: FortiAnalyzer 7.2 Administrator Guide - 'System Administration' and 'High Availability'

sections.

Question 4

Question Type: MultipleChoice

What are analytics logs on FortiAnalyzer?

Options:

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.

Question 5

Question Type: MultipleChoice

Which feature can you configure to add redundancy to FortiAnalyzer?

Options:

A- Primary and secondary DNS

B- VLAN interfaces

C- IPv6 administrative access

D- Link aggregation

Answer:

D

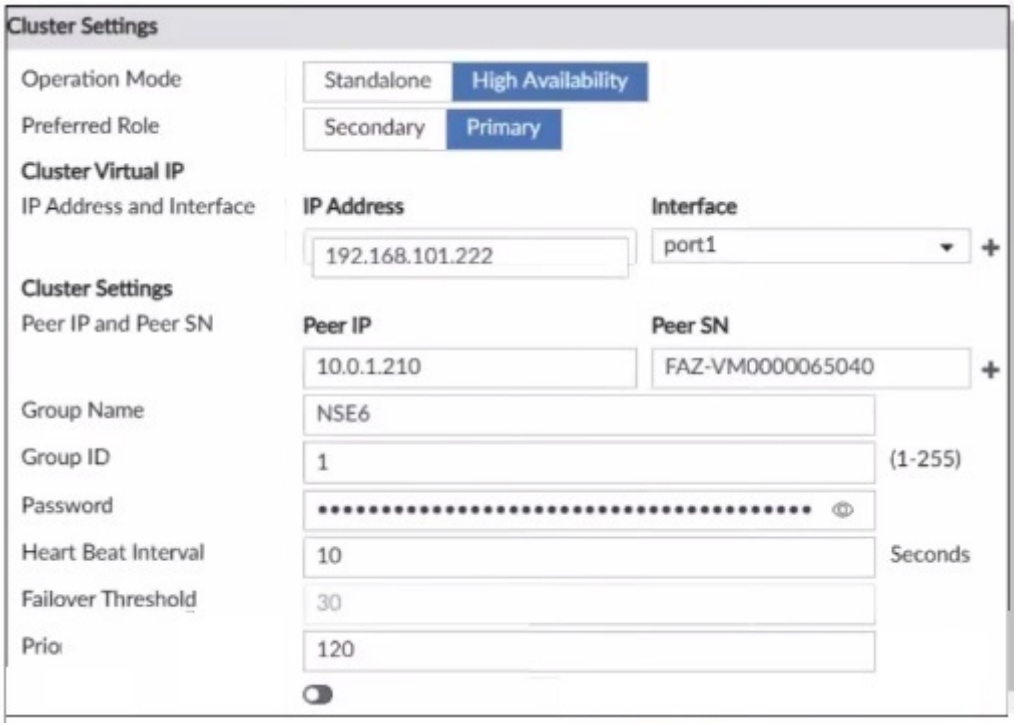
Explanation:

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. Reference: The FortiAnalyzer 7.4.1 Administration Guide explains the concept of link aggregation and its relevance to

Question 6

Question Type: MultipleChoice

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?

Options:

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. Reference: 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.

Question 7

Question Type: MultipleChoice

What is true about FortiAnalyzer reports?

Options:

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.

Question 8

Question Type: MultipleChoice

Which two statements are true regarding FortiAnalyzer system backups? (Choose two.)

Options:

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:

A, D

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. Reference: FortiAnalyzer 7.4.1 Administration Guide, 'Scheduling automatic backups' section.

Question 9

Question Type: MultipleChoice

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

Options:

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. Reference: FortiAnalyzer 7.2 Administrator Guide - 'System Administration' and 'High Availability' sections.

Question 10

Question Type: **MultipleChoice**

Which statement is true about the communication between FortiGate high availability (HA) clusters and FortiAnalyzer?

Options:

A- Each cluster member sends its logs directly to FortiAnalyzer.

B- You must add the device lo the cluster first, and then registers 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. Reference: FortiAnalyzer 7.4.1 Administration Guide, sections mentioning HA cluster configuration and log forwarding.