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
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 2
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 3
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 4
Which statement is true when you areupgrading the firmware on an HA cluster made up of throe 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 thefirmware 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 5
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 6
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 commandslog-forwardandlog-forward-service.References:FortiAnalyzer 7.2 Administrator Guide, "Aggregation" and "CLI Commands for Aggregation Mode" sections.

NEW QUESTION 7
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 8
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 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/