



Fortinet

Exam Questions FCP_FAZ_AD-7.4

FCP - FortiAnalyzer 7.4 Administrator

NEW QUESTION 1

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

- A. There is no need to do anything because the disk will self-recover.
- B. Run execute format disk to format and restart the FortiAnalyzer device.
- C. Perform a hot swap of the disk.
- D. Shut down FortiAnalyzer and replace the disk.

Answer: C

Explanation:

In a hardware RAID setup, FortiAnalyzer supports hot swapping, which allows you to replace a failed disk without shutting down the device. The RAID controller will automatically rebuild the array using the new disk, minimizing downtime and maintaining data integrity.

NEW QUESTION 2

Which process is responsible for enforcing the log file size?

- A. oftpd
- B. miglogd
- C. sqlplugind
- D. logfiled

Answer: D

Explanation:

The logfiled process is responsible for enforcing log file size and managing log rotation on FortiAnalyzer. It ensures that log files do not exceed the configured size limits and handles the creation and rotation of new log files when necessary.

NEW QUESTION 3

Which two parameters impact the amount of reserved disk space required by FortiAnalyzer? (Choose two.)

- A. Total quota
- B. License type
- C. RAID level
- D. Disk size

Answer: C

Explanation:

RAID level affects how much disk space is reserved for redundancy and fault tolerance. For example, RAID 1 mirrors data, meaning you need more space for redundancy, while RAID 5 or RAID 6 reserves space for parity.

Disk size directly influences the total available and reserved space since the larger the disk, the more space may need to be reserved for system functions, logs, and other operations.

The total quota and license type do not directly impact the reserved disk space, though they do influence other aspects of capacity and functionality.

NEW QUESTION 4

Which two statements about FortiAnalyzer operating modes are true? (Choose two.)

- A. When in collector mode, FortiAnalyzer offloads the log receiving task to the analyzer.
- B. When in analyzer mode, FortiAnalyzer supports event management and reporting features.
- C. For the collector, you should allocate most of the disk space to analytics logs.
- D. Analyzer mode is the default operating mode.

Answer: B

Explanation:

When in analyzer mode, FortiAnalyzer supports event management and reporting features.

In analyzer mode, FortiAnalyzer provides full support for log analysis, event management, and reporting capabilities.

Analyzer mode is the default operating mode.

By default, FortiAnalyzer operates in analyzer mode, which allows for log analysis and reporting. The other options are incorrect because:

In collector mode, the FortiAnalyzer primarily stores logs and forwards them to another FortiAnalyzer in analyzer mode, not the other way around.

In collector mode, most disk space is usually allocated to storage rather than analytics, as the logs are primarily stored for forwarding.

NEW QUESTION 5

Which three RAID configurations provide fault tolerance on FortiAnalyzer? (Choose three.)

- A. RAID0
- B. RAID 5
- C. RAID1
- D. RAID 6+0
- E. RAID 0+0

Answer: BCD

Explanation:

RAID 1 provides fault tolerance through disk mirroring.

RAID 5 provides fault tolerance by using distributed parity across multiple disks. RAID 6+0 combines striping with double parity, offering enhanced fault tolerance. RAID 0 and RAID 0+0 do not provide any fault tolerance, as they focus on performance through data striping but offer no redundancy.

NEW QUESTION 6
Refer to the exhibit.

Cluster Settings

Operation Mode

StandaloneHigh Availability

Preferred Role

SecondaryPrimary

Cluster Virtual IP

IP Address and Interface

IP Address

Interface

192.168.101.222

port1

Cluster Settings

Peer IP and Peer SN

Peer IP

Peer SN

10.0.1.210

FAZ-VM0000065040

Group Name

NSE6

Group ID

1

(1-255)

Password

.....

Heart Beat Interval

10

Seconds

Failover Threshold

30

Priority

120

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: A

Explanation:

Operation Mode: The mode is set to "High Availability" which indicates that this FortiAnalyzer is intended to be part of an HA cluster.

Preferred Role: The "Primary" role is selected, meaning this device is configured to act as the primary unit in the HA cluster. This is a crucial setting as it determines the device's behavior and responsibilities within the cluster.

Cluster Virtual IP: A specific IP address (192.168.101.222) is assigned to be used by devices in the network to communicate with the cluster. This Virtual IP will be shared between the units in the cluster.

Cluster Settings: These include configurations for heartbeat interval, failover threshold, and priority which are crucial for maintaining cluster health and managing failover scenarios.

Given these points, the correct conclusion from the options provided is:

* C. This FortiAnalyzer will join the existing HA cluster as the primary.

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

NEW QUESTION 8

Which two methods can you use to restrict administrative access on FortiAnalyzer? (Choose two.)

- A. Configure trusted hosts.
- B. Limit access to specific virtual domains.
- C. Fabric connectors to external LDAP servers.
- D. Use administrator profiles.

Answer: AD

Explanation:

Configure trusted hosts.

Trusted hosts restrict administrative access to FortiAnalyzer by limiting the IP addresses or subnets from which administrators can log in.

Use administrator profiles.

Administrator profiles define roles and permissions, restricting what specific administrators can access and manage on FortiAnalyzer.

The other options are not applicable because:

Limiting access to specific virtual domains is not applicable to FortiAnalyzer, as virtual domains (VDOMs) are a concept used in FortiGate, not FortiAnalyzer.

Fabric connectors to external LDAP servers are used for authentication purposes but do not directly restrict administrative access based on roles or IP addresses.

NEW QUESTION 9

Which two statements regarding FortiAnalyzer log forwarding modes are true? (Choose two.)

- A. Both modes, forwarding and aggregation, support encryption of logs between devices.
- B. In aggregation mode, you can forward logs to syslog and CEF servers.
- C. Forwarding mode forwards logs in real time only to other FortiAnalyzer devices.
- D. Aggregation mode stores logs and content files and uploads them to another FortiAnalyzer device at a scheduled time.

Answer: AD

Explanation:

Both modes, forwarding and aggregation, support encryption of logs between devices.

Both forwarding and aggregation modes can use encryption to securely transfer logs between FortiAnalyzer devices.

Aggregation mode stores logs and content files and uploads them to another FortiAnalyzer device at a scheduled time.

In aggregation mode, logs are stored and then transferred to another FortiAnalyzer at a scheduled time, rather than in real-time. This mode is typically used when consolidating logs from multiple devices into a central FortiAnalyzer.

The other options are incorrect because:

Forwarding mode sends logs in real-time but not exclusively to other FortiAnalyzer devices; it can also send logs to external systems like syslog servers.

Aggregation mode is primarily for consolidating logs to another FortiAnalyzer and doesn't focus on forwarding logs to syslog or CEF servers.

NEW QUESTION 10

What does the disk status Degraded mean for RAID management?

- A. The hard drive is no longer being used by the RAID controller.
- B. One or more drives are missing from the FortiAnalyzer unit.
- C. The device is writing data to the disk to restore the volume to an optimal state.
- D. FortiAnalyzer determined that the parity data in the disk is not valid.

Answer: B

Explanation:

When the RAID status is Degraded, it typically indicates that one or more drives in the RAID array have failed or are missing, causing the RAID array to operate with reduced redundancy. In this state, the array is still functioning, but it's at risk because the fault tolerance provided by RAID is compromised.

NEW QUESTION 10

Which two statements about high availability (HA) on FortiAnalyzer are true? (Choose two.)

- A. FortiAnalyzer HA supports synchronization of logs as well as some system and configuration settings.
- B. FortiAnalyzer HA active-passive mode can function without VRRP.
- C. All devices in a FortiAnalyzer HA cluster must run in the same operation mode, either analyzer mode or collector mode.
- D. All devices in a FortiAnalyzer HA cluster must have the same available disk space.

Answer: A

Explanation:

The two correct statements about high availability (HA) on FortiAnalyzer are:

FortiAnalyzer HA supports synchronization of logs as well as some system and configuration settings.

FortiAnalyzer HA synchronizes both logs and certain system configuration settings between the units in the cluster to ensure consistent operation.

All devices in a FortiAnalyzer HA cluster must run in the same operation mode, either analyzer mode or collector mode.

In an HA cluster, all devices must be configured to operate in the same mode --- either analyzer mode or collector mode---to ensure consistency and proper functionality across the cluster.

The other options, such as VRRP, are not required for HA in FortiAnalyzer, and disk space can vary between nodes but may impact log storage capacity.

NEW QUESTION 11

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

- A. If devices were registered to FortiAnalyzer before forming a cluster, you can manually add them together
- B. FortiAnalyzer distinguishes each cluster member by the IP addresses in log message header
- C. If the HA primary device becomes unavailable, you must remove it from the HA cluster list on FortiAnalyzer
- D. The FortiGate HA cluster must be in active-passive mode in order to avoid conflict.

Answer: B

Explanation:

This allows FortiAnalyzer to correctly identify and process logs from different members of the HA cluster.

NEW QUESTION 16

Which statement correctly describes RAID 10 (1+0) on FortiAnalyzer?

- A. A configuration with four disks, each with 2 TB of capacity, provides a total space of 4 T
- B. 11 combines mirroring striping and distributed parity to provide performance and fault toleranc
- C. A configuration with four disks, each with 2 TB of capacity, provides a total space of 2 T
- D. It uses striping to provide performance and fault tolerance.

Answer: A

Explanation:

RAID 10 combines mirroring (RAID 1) and striping (RAID 0). In a RAID 10 setup with four disks, data is mirrored across two pairs of disks, and those pairs are striped for performance. This results in improved performance and fault tolerance, but the total usable storage is 50% of the total raw storage, meaning four 2 TB disks provide 4 TB of usable space.

NEW QUESTION 19

What is the recommended method of expanding disk space on a FortiAnalyzer VM?

- A. From the VM host manager, add an additional virtual disk and use the #execute lvm extendcommand to expand the storage.
- B. From the VM host manager, expand the size of the existing virtual disk.
- C. From the VM host manager, expand the size of the existing virtual disk and use the # executeformat disk command to reformat the disk.
- D. From the VM host manager, add an additional virtual disk and rebuild your RAID array.

Answer: A

Explanation:

Adding an Additional Virtual Disk:

From the VM host manager (such as VMware vSphere or Hyper-V), you can add a new virtual disk to the FortiAnalyzer VM.

Extending the Logical Volume:

After adding the new disk, use commands like #execute lvm extend within the FortiAnalyzer to extend the logical volume, making the additional storage available to the VM. This is particularly useful when you need to add more storage without disrupting existing data.

This approach is recommended when you need to ensure the FortiAnalyzer VM can handle more storage without reformatting or affecting existing data.

NEW QUESTION 21

Which statements are true of Administrative Domains (ADOMs) in FortiAnalyzer? (Choose two.)

- A. ADOMs are enabled by default.
- B. ADOMs constrain other administrator's access privileges to a subset of devices in the device list.
- C. Once enabled, the Device Manager, FortiView, Event Management, and Reports tab display per ADOM.
- D. All administrators can create ADOMs--not just the admin administrator.

Answer: BC

Explanation:

ADOMs constrain other administrators' access privileges to a subset of devices in the device list: ADOMs allow you to partition the FortiAnalyzer's management capabilities by restricting access to certain devices and logs based on the administrator's role. This segmentation helps in managing large deployments with different administrative needs.

Once enabled, the Device Manager, FortiView, Event Management, and Reports tab display per ADOM: When ADOMs are enabled, the FortiAnalyzer interface segments the Device Manager, FortiView, Event Management, and Reports tabs based on the selected ADOM. This allows administrators to work within their specific ADOM context.

ADOMs are enabled by default: This is incorrect because ADOMs are not enabled by default. They must be manually configured and enabled according to the organization's needs.

All administrators can create ADOMs--not just the admin administrator: This is not correct. Typically, creating and managing ADOMs requires administrative privileges, often restricted to the main admin or specific roles with sufficient permissions.

NEW QUESTION 22

Refer to the exhibit.

Event	Event Status	Event Type	Count	Severity
151.101.54.62 (1)				
Insecure SSL Connection blocked from 10.0.3.20	Mitigated	SSL	1	Low

Which statement is correct regarding the event displayed?

- A. An incident was created from this event.
- B. The security risk was blocked or dropped.
- C. The security event risk is considered open.
- D. The risk source is isolated.

Answer: B

Explanation:

The event status is "Mitigated", which indicates that the insecure SSL connection was successfully blocked or prevented. Events in FortiAnalyzer will be in one of four statuses. The current status will determine if more actions need to be taken by the security team or not. The possible statuses are: Unhandled: The security event risk is not mitigated or contained, so it is considered open. Contained: The risk source is isolated. Mitigated: The security risk is mitigated by being blocked or dropped.

NEW QUESTION 23

What are two potential advantages of deploying RAID on FortiAnalyzer? (Choose two.)

- A. It provides redundancy.
- B. It improves performance.
- C. It provides backups.
- D. It reduces system resource usage.

Answer: AB

Explanation:

Here are two potential advantages of deploying RAID on FortiAnalyzer: RAID configurations can mirror or stripe data across multiple disks. This redundancy helps ensure that even if one disk fails, the data remains accessible and recoverable. This is crucial for FortiAnalyzer as it stores security logs which are critical for analysis and forensic investigations. Certain RAID configurations, like RAID 0 (striping) can improve read performance by distributing data reads across multiple disks. This can be beneficial for FortiAnalyzer when performing faster searches or retrieving large log sets. Here's why the other options are not necessarily advantages: While RAID can improve data availability in case of disk failures, it's not a replacement for proper backups. Backups should be done regularly to a separate location to ensure data recovery in case of catastrophic events like hardware failures or ransomware attacks. RAID itself doesn't necessarily reduce system resource usage. In fact, some RAID configurations can introduce additional overhead for managing the redundant data.

NEW QUESTION 25

What are two of the key features of FortiAnalyzer? (Choose two.)

- A. Centralized log repository
- B. Cloud-based management
- C. Reports
- D. Virtual domains (VDOMs)

Answer: AC

Explanation:

FortiAnalyzer acts as a central repository for collecting and storing logs from multiple Fortinet devices. This centralized log management facilitates efficient analysis, search, and correlation of logs from across the network. FortiAnalyzer provides robust reporting capabilities, allowing users to generate detailed reports based on collected logs and data. These reports can include insights on security events, network performance, and compliance. Cloud-based management is not a primary feature of FortiAnalyzer, as it is typically an on-premises appliance, although it can integrate with cloud services. Virtual domains (VDOMs) are a feature of FortiGate devices, allowing them to be partitioned into multiple virtual domains for administrative and policy separation. FortiAnalyzer itself does not provide VDOMs.

NEW QUESTION 27

What FortiGate process caches logs when FortiAnalyzer is not reachable?

- A. logfiled
- B. sqlplugind
- C. oftpd
- D. miglogd

Answer: D

Explanation:

The miglogd process on FortiGate is responsible for caching logs when FortiAnalyzer is unreachable. It temporarily stores logs in memory and, if the memory buffer fills up, it starts storing logs on disk. Once the connection to FortiAnalyzer is restored, miglogd sends the cached logs to the FortiAnalyzer.

NEW QUESTION 28

How do you restrict an administrator's access to a subset of your organization's ADOMs?

- A. Set the ADOM mode to Advanced
- B. Assign the ADOMs to the administrator's account
- C. Configure trusted hosts
- D. Assign the default Super_User administrator profile

Answer: B

Explanation:

To restrict an administrator's access to a subset of your organization's ADOMs (Administrative Domains) in FortiAnalyzer, you need to assign the specific ADOMs to the administrator's account. Here's how this works:

Assign the ADOMs to the Administrator's Account (Option B):

In FortiAnalyzer, you can configure which ADOMs an administrator has access to by assigning them directly to the administrator's account. This allows you to control and limit the administrator's access to only the ADOMs they are authorized to manage or view.

NEW QUESTION 33

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

FCP_FAZ_AD-7.4 Practice Exam Features:

- * FCP_FAZ_AD-7.4 Questions and Answers Updated Frequently
- * FCP_FAZ_AD-7.4 Practice Questions Verified by Expert Senior Certified Staff
- * FCP_FAZ_AD-7.4 Most Realistic Questions that Guarantee you a Pass on Your First Try
- * FCP_FAZ_AD-7.4 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The FCP_FAZ_AD-7.4 Practice Test Here](#)