

Fortinet

Exam Questions NSE6_FAZ-7.2

Fortinet NSE 6 - FortiAnalyzer 7.2 Administrator



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 process logfiled in 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, logfiled allows 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

Which command can you use to find the IP addresses of the devices sending logs to FortiAnalyzer?

- A. diagnose debug application oftpd 8
- B. diagnose dvm adorn List
- C. diagnose test application miglogd 6
- D. diagnose test application oftpd 3

Answer: A

Explanation:

The command diagnose debug application oftpd 8 is 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 3

Which statement is true about ADOMs?

- A. When a FortiAnalyzer Fabric is implemented, the default ADOM mode is set to advanced.
- B. A fabric ADOM can include all the device types supported by FortiAnalyzer.
- C. You can change the ADOM mode only through the GUI.
- D. In normal mode, you cannot change the disk quota of the ADOM after its creation.

Answer: B

Explanation:

Regarding ADOMs (Administrative Domains) in FortiAnalyzer, a fabric ADOM is capable of including all device types that FortiAnalyzer supports. This is part of the flexibility offered by ADOMs to manage and report on logs from various devices within a Fortinet security fabric. ADOMs can be enabled to support non-FortiGate devices as well, and the root ADOM in Fabric ADOMs provides visibility into all Security Fabric devices. Additionally, it should be noted that in normal mode, you cannot assign different FortiGate VDOMs to different ADOMs, while in advanced mode, you can, which provides a more granular control over the log data from individual VDOMs. References: FortiAnalyzer 7.4.1 Administration Guide, "ADOMs" and "ADOM device modes" sections.

NEW QUESTION 4

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 5

Refer to the exhibit.

```
FortiAnalyzer3# get system status
Platform Type           : FAZVM64
Platform Full Name      : FortiAnalyzer-VM64
Version                 : v7.2.1-build1215 220809 (GA)
Serial Number           : FAZ-VM0000065042
BIOS version            : 04000002
Hostname                : FortiAnalyzer3
Max Number of Admin Domains : 5
Admin Domain Configuration : Enabled
FIPS Mode               : Disabled
HA Mode                 : Stand Alone
Branch Point            : 1215
Release Version Information : GA
Time Zone               : (GMT-8:00) Pacific Time (US & Canada)
Disk Usage              : Free 45.06GB, Total 58.80GB
File System              : Ext4
License Status           : Valid

FortiAnalyzer3# get system global
adom-mode                : normal
adom-select              : enable
adom-status
:console-output
:country-flag
enc-algorithm            : high
```

Based on the partial outputs displayed in the exhibit, which devices are ready to be configured as peers in an HA cluster?

- A. FortiAnalyzer1 and FortiAnalyzer3
- B. FortiAnalyzer1 and FortiAnalyzer2
- C. These devices cannot participate in the same cluster.
- D. FortiAnalyzer2 and FortiAnalyzer3

Answer: C

Explanation:
Based on the provided exhibit, which shows partial outputs of the system status and global settings for FortiAnalyzer devices, the devices cannot be configured as peers in an HA (High Availability) cluster. This is indicated by the HA Mode status being set to 'Stand Alone' for the displayed FortiAnalyzer device. For devices to be part of an HA cluster, they would need to have compatible HA configurations, and usually, they should not be in 'Stand Alone' mode. Additionally, the exhibit only shows information for one FortiAnalyzer, so it cannot be determined if there is another device ready to form an HA cluster with it.

NEW QUESTION 6

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 7

What is true about FortiAnalyzer reports?

- 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.

NEW QUESTION 8

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 9

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 10

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 10

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

Prio

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: 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 11

In a Fortinet Security Fabric, what can make an upstream FortiGate create traffic logs associated with sessions initiated on downstream FortiGate devices?

- A. The traffic destination is another FoitiGate in the fabric.
- B. Log redundancy is configured in the fabric.
- C. The upstream FortiGate is configured to do NAT.
- D. The downstream device cannot connect to FortiAnalyzer.

Answer: D

Explanation:

In a Fortinet Security Fabric, an upstream FortiGate may create traffic logs for sessions initiated on downstream FortiGate devices if the downstream device is unable to connect to FortiAnalyzer. This allows for continuity of logging and ensures that session logs are captured and stored even if the downstream device loses its connection to the log management system. References:FortiAnalyzer 7.4.1 Administration Guide, "Fortinet Security Fabric" section.

NEW QUESTION 14

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 18

What are analytics logs on FortiAnalyzer?

- 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.

NEW QUESTION 21

.....

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

NSE6_FAZ-7.2 Practice Exam Features:

- * NSE6_FAZ-7.2 Questions and Answers Updated Frequently
- * NSE6_FAZ-7.2 Practice Questions Verified by Expert Senior Certified Staff
- * NSE6_FAZ-7.2 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * NSE6_FAZ-7.2 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The NSE6_FAZ-7.2 Practice Test Here](#)