

Fortinet

Exam Questions NSE6_FAZ-7.2

Fortinet NSE 6 - FortiAnalyzer 7.2 Administrator



NEW QUESTION 1

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 teatapplication miglogd6
- D. diagnose bestapplication 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 2

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 to the cluster first, and then register 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. References: FortiAnalyzer 7.4.1 Administration Guide, sections mentioning HA cluster configuration and log forwarding.

NEW QUESTION 3

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
: onsole-output
: ountry-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 4

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 the log-checksum to md5-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 5

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 6

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 7

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 8

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 9

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 10

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 FortiGate 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 10

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

- A. Shut 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 13

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 18

.....

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](#)