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 processlogfiledin 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,logfiledallows 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
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 3
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 lo the cluster first, and thenregistersthe 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 4
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 5
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 6
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 7
Which two settings must you configure on FortiAnalyzer to allow non-local administrators to authenticate on FortiAnalyzer with any user account in a single LDAP group? (Choose two.)

A. LDAP servers IP addresses added as trusted hosts
B. One or more remote LDAP servers
C. A local wildcard administrator account
D. An administrator group

Answer: BD

Explanation:
To allow non-local administrators to authenticate on FortiAnalyzer with any user account in a single LDAP group, you must configure one or more remote LDAP servers and an administrator group. First, you configure the LDAP server(s) by specifying the server name, IP, and other details such as the Common Name Identifier and Distinguished Name. Then, you add the LDAP server to a user group. Finally, you create an administrator account that uses this user group for authentication, allowing any user from the specified LDAP group to authenticate.References:FortiAnalyzer 7.2 Administrator Guide, "Configuring remote authentication for administrators using LDAP" section.

NEW QUESTION 8
Refer to the exhibit.
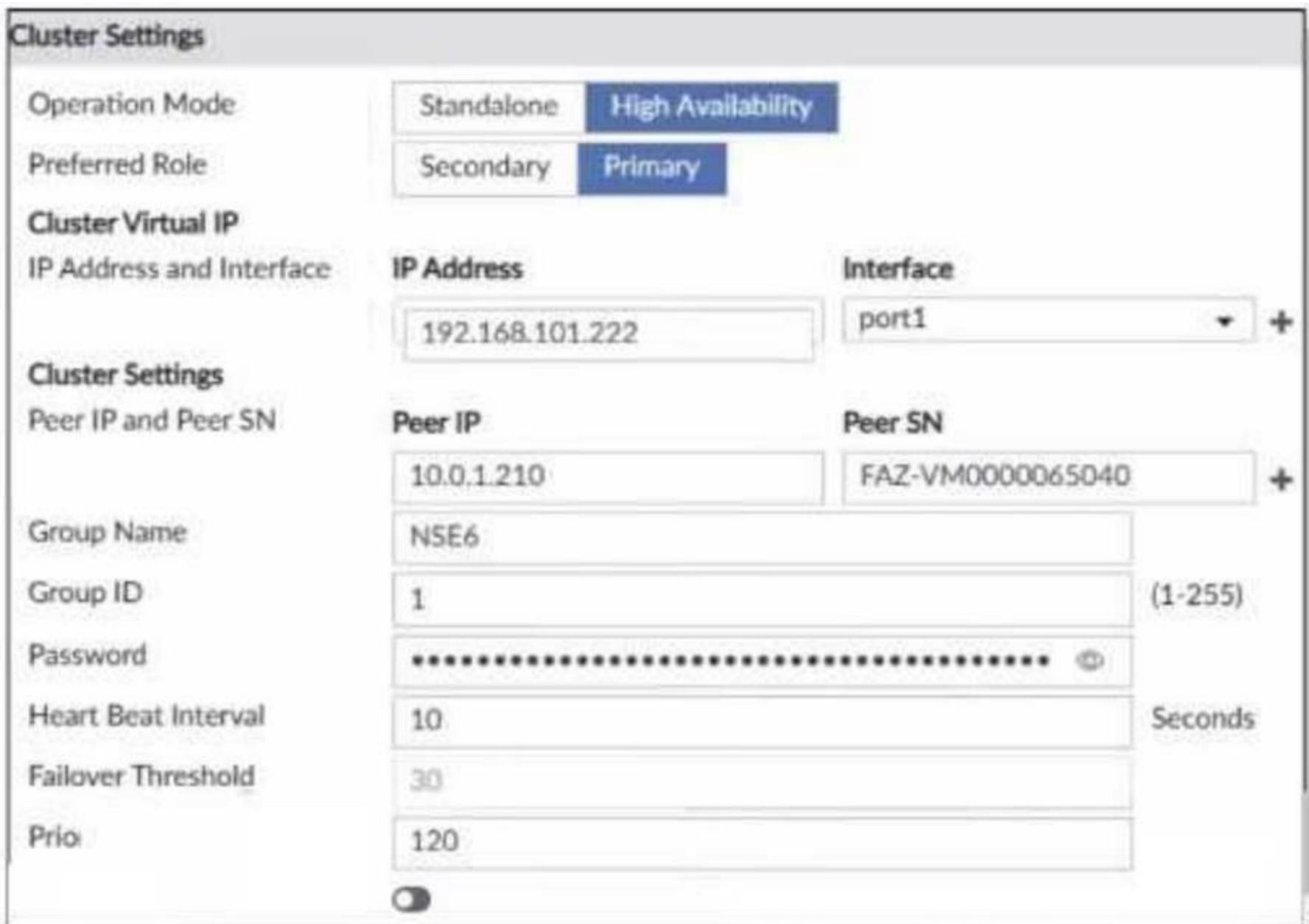
The image displays "he configuration of a FortiAnalyzer the administrator wants to join to an existing HA cluster.
What can you conclude from the configuration displayed?

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
What is true about a FortiAnalyzer Fabric?

A. Supervisors support HA.
B. Members events can be raised from the supervisor.
C. The supervisor and members cannot be in different time zones
D. The members send their logs to the supervisor.

Answer: D

Explanation:
In a FortiAnalyzer Fabric, the FortiAnalyzer can recognize a Security Fabric group of devices, and it supports the Security Fabric by storing and analyzing logs from these units as if they were from a single device. The members of the Security Fabric group send their logs to the FortiAnalyzer, which acts as a supervisor for log storage and analysis, providing a centralized point of visibility and control over the logs.References:FortiAnalyzer 7.4.1 Administration Guide, "Security Fabric" section.

NEW QUESTION 10
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 10
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 12
Which FortiAnalyzer command erases all device settings, images, databases, and logs on disk, but preserves The network configuration?

A. executefactory-reset
B. executeformat disk
C. executeformatlogdisk
D. executereset all-except—ip

Answer: A

Explanation:
The FortiAnalyzer commandexecute factory-resetis used to erase all device settings, images, databases, and logs on disk but preserves the current IP address and route information. This command effectively resets the FortiAnalyzer to its factory settings while maintaining its network configuration, allowing it to be quickly reconfigured with the same network settings.References:FortiAnalyzer 7.4.1 Administration Guide, "Reset Commands" section.

NEW QUESTION 15
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 17
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 19
......

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons 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](https://www.surepassexam.com/NSE6_FAZ-7.2-exam-dumps.html)