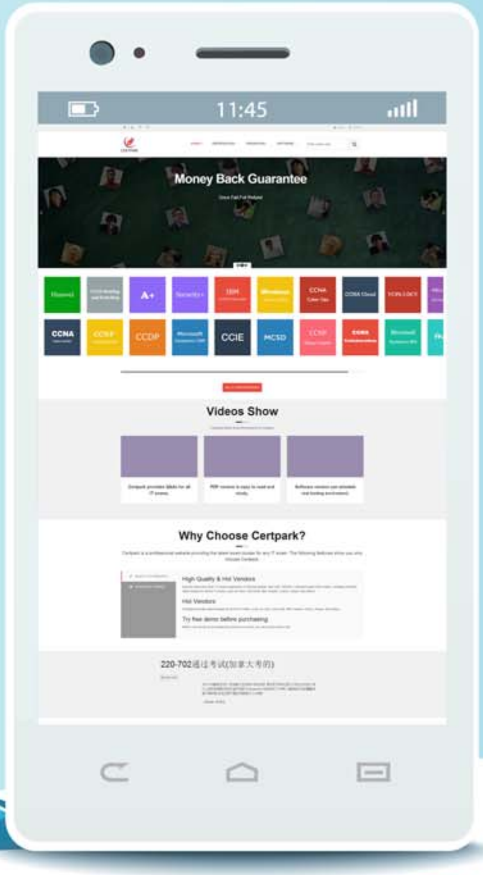
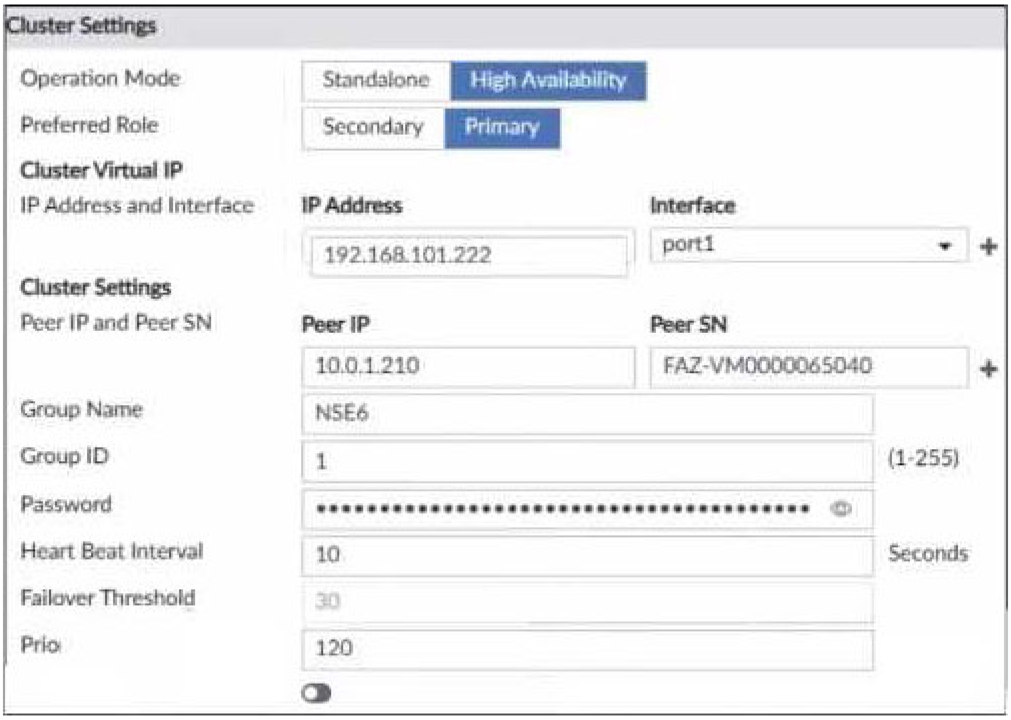

11:45
Money Back Guarantee
CCNA
CCNP
CCDP
CCIE
MCSD
Videos Show
Why Choose Certpark?
High Quality & Hot Vendors
Hot Vendors
Try free demo before purchasing
220-702通过考试(加拿大考的)

Exam : NSE6_FAZ-7.2

Title : Fortinet NSE 6 - FortiAnalyzer 7.2 Administrator

Version : DEMO

1.Refer to the exhibit.



Cluster Settings

Operation Mode: Standalone [✓ High Availability]

Preferred Role: Secondary [✓ Primary]

Cluster Virtual IP

IP Address and Interface: IP Address 192.168.101.222, Interface port1

Cluster Settings

Peer IP and Peer SN: Peer IP 10.0.1.210, Peer SN 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.

Reference: 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.

2.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

3.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.

4.Which statement is true when you are upgrading 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 the firmware 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.
Reference: FortiAnalyzer 7.2 Administrator Guide - "System Administration" and "High Availability" sections.

5.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.

Reference: FortiAnalyzer 7.2 Administrator Guide - "Hardware Maintenance" and "RAID Management" sections.