# 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 applicationoftpd 8
B. diagnose dvm adorn List
C. diagnose teatapplication miglogd6
D. diagnose bestapplicationoftpd 3

**Answer:** A

**Explanation:**
The commanddiagnose debug application oftpd 8is 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.

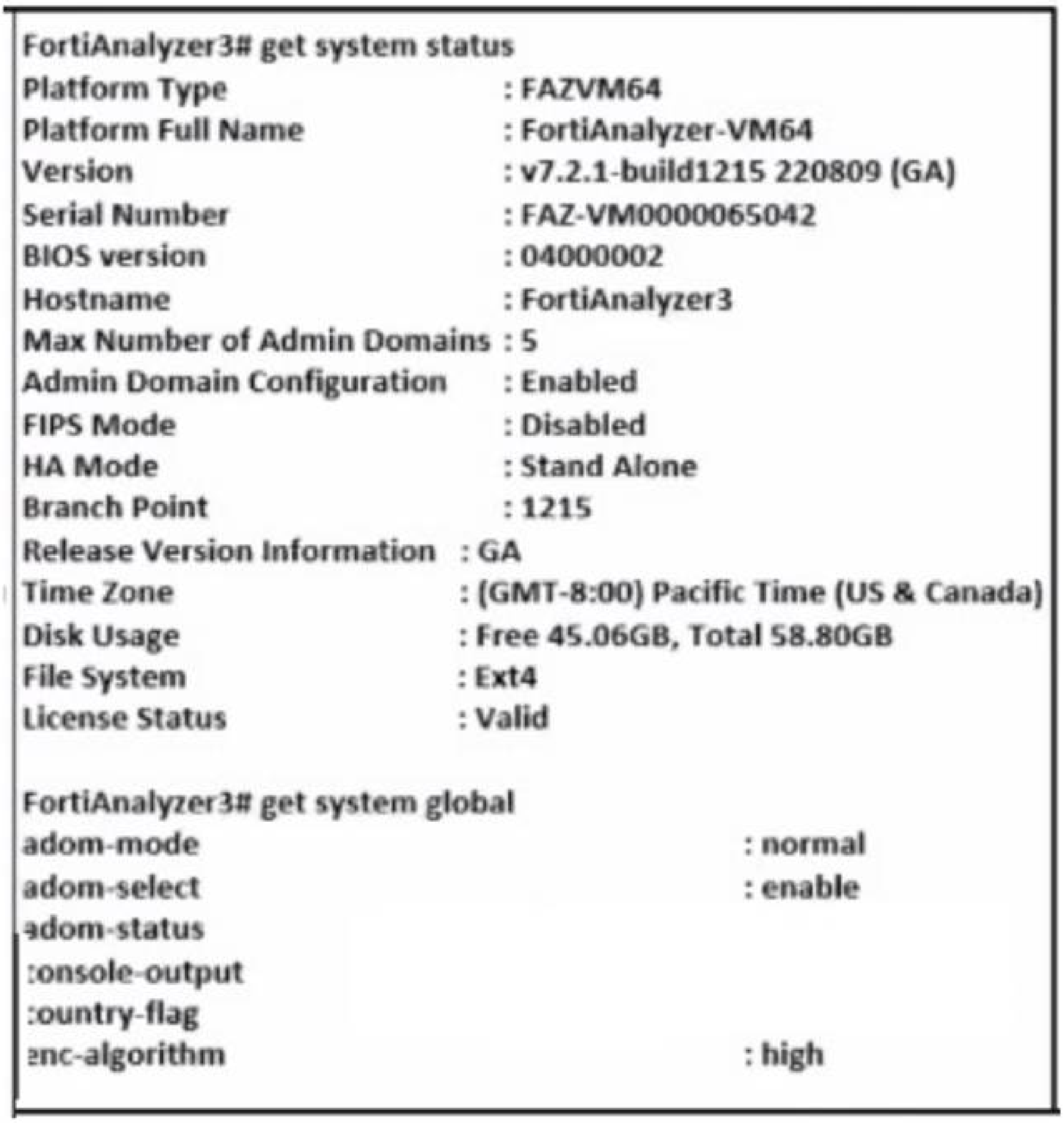
**NEW QUESTION 2**
Which two statements about FortiAnalyzer operating modes are true? (Choose two.)

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

**Answer:** BD

**Explanation:**
The default operating mode for FortiAnalyzer is analyzer mode. In this mode, FortiAnalyzer provides full functionality for event management and reporting features. This mode is intended for environments where comprehensive analysis and reporting are required. It allows FortiAnalyzer to collect, analyze, and store logs, as well as generate reports and manage events.References:FortiAnalyzer 7.4.1 Administration Guide, "Operating modes" section.

**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
```

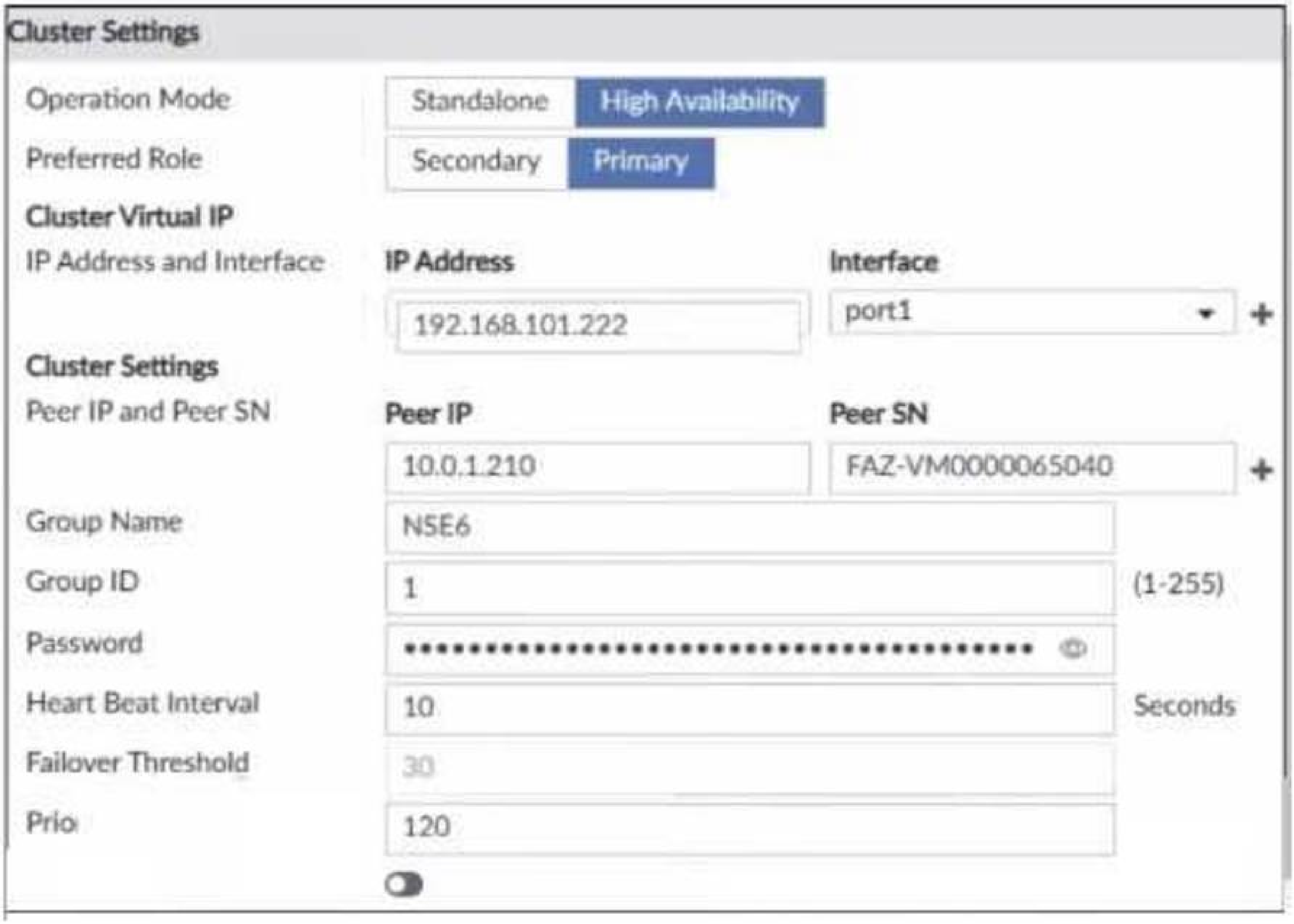
Based on the partial outputs displayed in the exhibit, which devices are ready to be configured as peers in an HA cluster?

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 havecompatible 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**
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.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 5**
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 6**
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 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.References:The FortiAnalyzer 7.4.1 Administration Guide explains the concept of link aggregation and its relevance to

**NEW QUESTION 8**
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 10**
......