# Free Questions for NSE5_FAZ-7.2

## Shared by Floyd on 15-04-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

# Question 1

Question Type: MultipleChoice

What are two advantages of setting up fabric ADOM? (Choose two.)

## Options:

A- It can be used for fast data processing and log correlation
B- It can be used to facilitate communication between devices in same Security Fabric
C- It can include all Fortinet devices that are part of the same Security Fabric
D- It can include only FortiGate devices that are part of the same Security Fabric

## Answer:

A, C

## Explanation:

https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/448471/creating-a-security-fabric-adom

# Question 2

Question Type: MultipleChoice

Refer to the exhibit.

```
FortiAnalyzer1# get system status
Platform Type                : FAZVM64-KVM
Platform Full Name           : FortiAnalyzer-VM64-KVM
Version                      : v7.2.1-build1215 220809 (GA)
Serial Number                : FAZ-VM0000065040
BIOS version                 : 04000002
Hostname                     : FortiAnalyzer1
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 43.60GB, Total 58.80GB
File System                  : Ext4
License Status               : Valid

FortiAnalyzer1# get system global
adom-mode                    : normal
adom-select                  : enable
adom-status                  : enable
console-output               : standard
country-flag                 : enable
enc-algorithm                : high
ha-member-auto-grouping      : enable
hostname                     : FortiAnalyzer2
log-checksum                 : md5
log-forward-cache-size       : 5
log-mode                     : analyzer
longitude                    : (null)
max-aggregation-tasks        : 0
max-running-reports          : 1
oftp-ssl-protocol            : tlsv1.2
ssl-low-encryption           : disable
ssl-protocol                 : tlsv1.3 tlsv1.2
task-list-size               : 2000
webservice-proto             : tlsv1.3 tlsv1.2
```

```
FortiAnalyzer3# get system status
Platform Type                : FAZVM64-KVM
Platform Full Name           : FortiAnalyzer-VM64-KVM
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 12.98GB, Total 79.80GB
File System                  : Ext4
License Status               : Valid

FortiAnalyzer3# get system global
adom-mode                    : normal
adom-select                  : enable
adom-status                  : enable
console-output               : standard
country-flag                 : enable
enc-algorithm                : high
ha-member-auto-grouping      : enable
hostname                     : FortiAnalyzer3
log-checksum                 : md5
log-forward-cache-size       : 5
log-mode                     : analyzer
longitude                    : (null)
max-aggregation-tasks        : 0
max-running-reports          : 5
oftp-ssl-protocol            : tlsv1.2
ssl-low-encryption           : disable
ssl-protocol                 : tlsv1.3 tlsv1.2
task-list-size               : 2000
webservice-proto             : tlsv1.3 tlsv1.2
```

Based on the partial outputs displayed, which devices can be members of a FortiAnalyzer Fabric?

## Options:

A- FortiAnalyzerl and FortiAnalyzer3
B- FortiAnalyzer1 and FortiAnalyzer2
C- All devices listed can be members
D- FortiAnalyzer2 and FortiAnalyzer3

## Answer:

C

# Question 3

Question Type: MultipleChoice

Which log will generate an event with the status Contained?

### Options:

A- An IPS log with action=pass.
B- A WebFilter log with action=dropped.
C- An AV log with action=quarantine.
D- An AppControl log with action=blocked.

### Answer:

C

## Question 4

Question Type: MultipleChoice

Which daemon is responsible for enforcing the log file size?

### Options:

A- sqlplugind
B- logfiled
C- miglogd
D- ofrpd

### Answer:

B

### Explanation:

FortiAnalyzer_7.0_Study_Guide-Online.pdf page 121: The logfiled process enforces the log file size and is also responsible for disk quota enforcement by monitoring the other processes.

## Question 5

Question Type: MultipleChoice

What are two benefits of using fabric connectors? (Choose two.)

### Options:

A- They allow FortiAnalyzer to send logs in real-time to public cloud accounts.
B- You do not need an additional license to send logs to the cloud platform.
C- Fabric connectors allow you to improve redundancy.
D- Using fabric connectors is more efficient than using third-party polling with API.

### Answer:

A, C

## Question 6

Question Type: MultipleChoice

What is the purpose of the following CLI command?

```
# configure system global
     set log-checksum md5
end
```

### Options:

A- To add a log file checksum
B- To add the MD's hash value and authentication code
C- To add a unique tag to each log to prove that it came from this FortiAnalyzer
D- To encrypt log communications

### Answer:

A

### Explanation:

https://docs2.fortinet.com/document/fortianalyzer/6.0.3/cli-reference/849211/global

## Question 7

Question Type: MultipleChoice

What is required to authorize a FortiGate on FortiAnalyzer using Fabric authorization?

## Options:

A- A FortiGate ADOM
B- The FortiGate serial number
C- A pre-shared key
D- Valid FortiAnalyzer credentials

## Answer:

D

## Explanation:

FortiAnalyzer_7.0_Study_Guide-Online.pdf page 93: The fourth method uses the Fortinet Security Fabric authorization process. This method requires that both FortiGate and FortiAnalyzer are running version 7.0.1 or higher. It is also required that the FortiGate administrator has valid credentials to log in on FortiAnalyzer and complete the registration.

https://docs.fortinet.com/document/fortianalyzer/7.2.1/administration-guide/13897/adding-a-fortigate-using-security-fabric-authorization

# Question 8

Question Type: MultipleChoice

Which statement about the FortiSOAR management extension is correct?

## Options:

A- It requires a FortiManager configured to manage FortiGate
B- It requires a dedicated FortiSOAR device or VM.
C- It does not include a limited trial by default.
D- It runs as a docker container on FortiAnalyzer

## Answer:

D

# Question 9

Question Type: MultipleChoice

A rogue administrator was accessing FortiAnalyzer without permission, and you are tasked to see what activity was performed by that rogue administrator on FortiAnalyzer.

What can you do on FortiAnalyzer to accomplish this?

## Options:

A- Click FortiView and generate a report for that administrator.
B- Click Task Monitor and view the tasks performed by that administrator.
C- Click Log View and generate a report for that administrator.
D- View the tasks performed by the rogue administrator in Fabric View.

## Answer:

B

## Explanation:

FortiAnalyzer_7.0_Study_Guide-Online.pdf page 54: View the tasks FortiAnalyzer administrators have performed, including progress and status.

# Question 10

Question Type: MultipleChoice

By default, what happens when a log file reaches its maximum file size?

## Options:

A- FortiAnalyzer overwrites the log files.
B- FortiAnalyzer stops logging.
C- FortiAnalyzer rolls the active log by renaming the file.
D- FortiAnalyzer forwards logs to syslog.

## Answer:

C

# Question 11

Question Type: MultipleChoice

What are the operating modes of FortiAnalyzer? (Choose two)



## Options:

A- Standalone
B- Manager
C- Analyzer
D- Collector

## Answer:

C, D