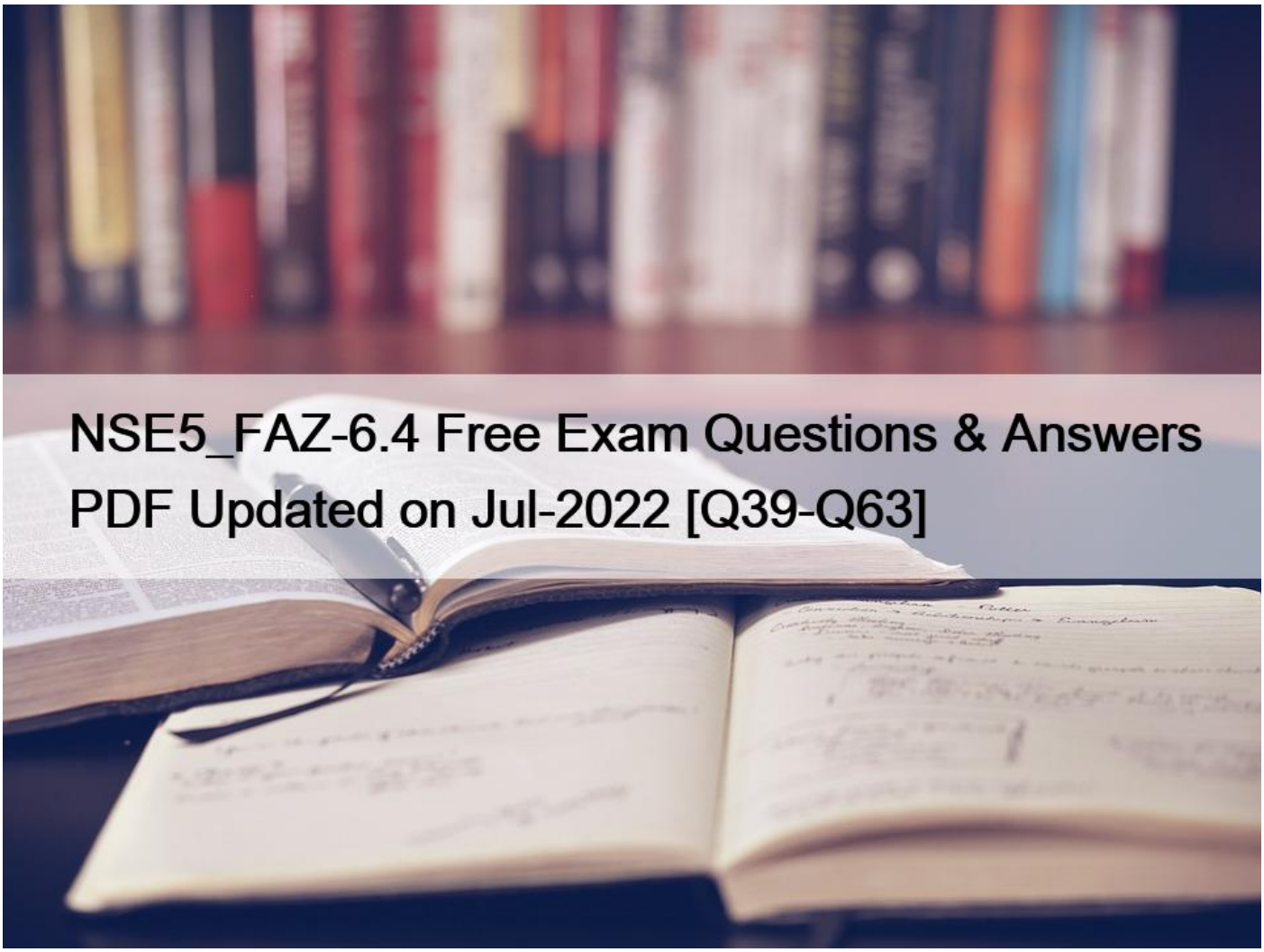
NSE5_FAZ-6.4 Free Exam Questions & Answers PDF Updated on Jul-2022 [Q39-Q63



NSE5_FAZ-6.4 Free Exam Questions and Answers PDF Updated on Jul-2022
Latest NSE5_FAZ-6.4 Exam Dumps Recently Updated 95 Questions

Fortinet NSE5_FAZ-6.4 Exam Syllabus Topics:

TopicDetailsTopic 1- Configure administrative domains (ADOMs)- Perform initial configurationTopic 2- Troubleshoot reports- Troubleshoot RAID- Protect log data- Logs and reportsTopic 3- Configure administrative access- Configure high availability (HA)Topic 4- Troubleshoot device communication issues- Device registration and communicationTopic 5- Troubleshoot and manage logs- Register devices in ADOMsTopic 6- Configure event handlers- System configuration

QUESTION 39

The admin administrator is failing to register a FortiClient EMS on the FortiAnalyzer device.

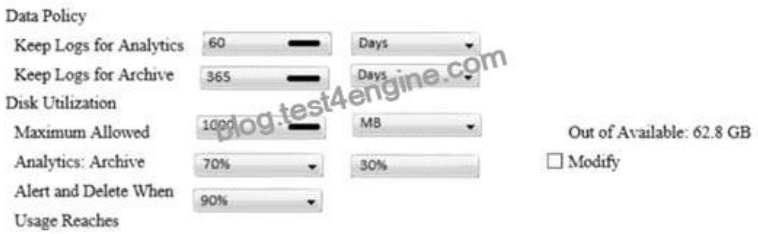
What can be the reason for this failure?
* FortiAnalyzer is in an HA cluster.
* ADOM mode should be set to advanced, in order to register the FortiClient EMS device.
* ADOMs are not enabled on FortiAnalyzer.
* A separate license is required on FortiAnalyzer in order to register the FortiClient EMS device.

QUESTION 40

What statements are true regarding the “store and upload” log transfer option between FortiAnalyzer and FortiGate? (Choose three.)
* All FortiGates can send logs to FortiAnalyzer using the store and upload option.
* Only FortiGate models with hard disks can send logs to FortiAnalyzer using the store and upload option.
* Both secure communications methods (SSL and IPsec) allow the store and upload option.
* Disk logging is enabled on the FortiGate through the CLI only.
* Disk logging is enabled by default on the FortiGate.

QUESTION 41

View the exhibit:



What does the 1000MB maximum for disk utilization refer to?
* The disk quota for the FortiAnalyzer model
* The disk quota for all devices in the ADOM
* The disk quota for each device in the ADOM
* The disk quota for the ADOM type

https://docs.fortinet.com/document/fortianalyzer/6.2.0/administration-guide/743670/configuring-log-storage-policy

QUESTION 42

Which statements are correct regarding FortiAnalyzer reports? (Choose two)
* FortiAnalyzer provides the ability to create custom reports.
* FortiAnalyzer glows you to schedule reports to run.
* FortiAnalyzer includes pre-defined reports only.
* FortiAnalyzer allows reporting for FortiGate devices only.

QUESTION 43

An administrator has moved FortiGate A from the root ADOM to ADOM1.

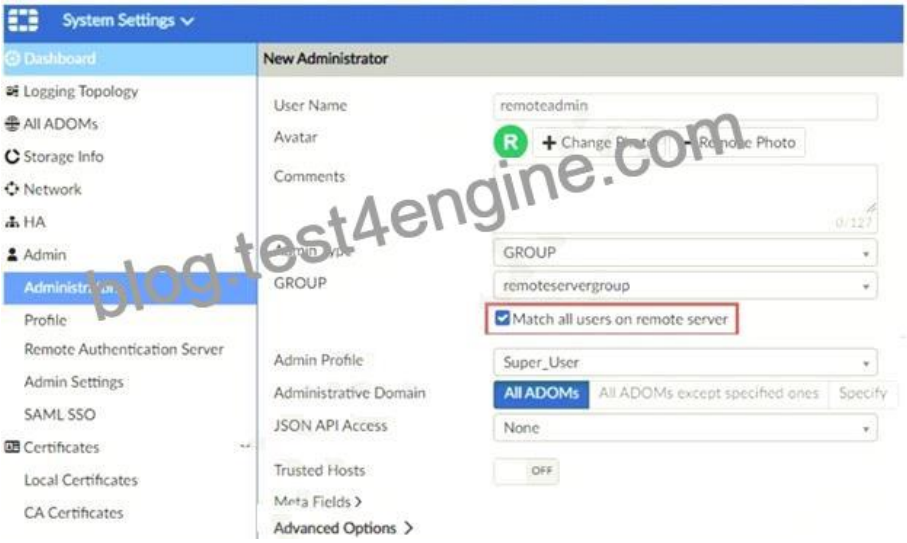
Which two statements are true regarding logs? (Choose two.)
* Analytics logs will be moved to ADOM1 from the root ADOM automatically.
* Archived logs will be moved to ADOM1 from the root ADOM automatically.
* Logs will be presented in both ADOMs immediately after the move.
* Analytics logs will be moved to ADOM1 from the root ADOM after you rebuild the ADOM1 SQL database.

QUESTION 44

What two things should an administrator do to view Compromised Hosts on FortiAnalyzer? (Choose two.)
* Enable web filtering in firewall policies on FortiGate devices, and make sure these logs are sent to FortiAnalyzer.
* Enable device detection on an interface on the FortiGate devices that are connected to the FortiAnalyzer.
* Subscribe FortiAnalyzer to FortiGuard to keep its local threat database up-to-date.
* Make sure all endpoints are reachable by FortiAnalyzer.

QUESTION 45

Refer to the exhibit.



The exhibit shows “remoteservergroup” is an authentication server group with LDAP and RADIUS servers.

Which two statements express the significance of enabling “Match all users on remote server” when configuring a new administrator? (Choose two.)
* It creates a wildcard administrator using LDAP and RADIUS servers.
* Administrator can log in to FortiAnalyzer using their credentials on remote servers LDAP and RADIUS.
* Use remoteadmin from LDAP and RADIUS servers will be able to log in to FortiAnalyzer at anytime.
* It allows administrators to use two-factor authentication.

QUESTION 46

How are logs forwarded when FortiAnalyzer is using aggregation mode?
* Logs are forwarded as they are received and content files are uploaded at a scheduled time.
* Logs and content files are stored and uploaded at a scheduled time.

* Logs are forwarded as they are received.
* Logs and content files are forwarded as they are received.

https://www.fortinetguru.com/2020/07/log-forwarding-fortianalyzer-fortios-6-2-3/

https://docs.fortinet.com/document/fortianalyzer/6.2.0/administration-guide/420493/modes

QUESTION 47

How do you restrict an administrator’s access to a subset of your organization’s ADOMs?
* Set the ADOM mode to Advanced
* Assign the ADOMs to the administrator’s account
* Configure trusted hosts
* Assign the default Super_User administrator profile

https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/717578/assigning-administrators-to-an-adom

QUESTION 48

What FortiView tool can you use to automatically build a dataset and chart based on a filtered search result?
* Chart Builder
* Export to Report Chart
* Dataset Library
* Custom View

https://docs.fortinet.com/document/fortianalyzer/6.2.0/cookbook/989203/building-charts-with-chart-builder

QUESTION 49

You need to upgrade your FortiAnalyzer firmware.

What happens to the logs being sent to FortiAnalyzer from FortiGate during the time FortiAnalyzer is temporarily unavailable?
* FortiAnalyzer uses log fetching to retrieve the logs when back online
* FortiGate uses the miglogd process to cache the logs
* The logfiled process stores logs in offline mode
* Logs are dropped

If FortiAnalyzer becomes unavailable to FortiGate for any reason, FortiGate uses its *miglogd* process to cache the logs. There is a maximum value to the cache size, and the miglogd process will drop cached logs. When the connection between the two devices is restored, the miglogd process begins to send the cached logs to FortiAnalyzer. Therefore, the FortiGate buffer will keeps logs long enough to sustain a reboot of your FortiAnalyzer (if you are upgrading the firmware, for example). But it is not intended for a lengthy FortiAnalyzer outage.

QUESTION 50

What can you do on FortiAnalyzer to restrict administrative access from specific locations?
* Configure trusted hosts for that administrator.
* Enable geo-location services on accessible interface.
* Configure two-factor authentication with a remote RADIUS server.
* Configure an ADOM for respective location.

QUESTION 51

Which two statements are true regarding log fetching on FortiAnalyzer? (Choose two.)
* A FortiAnalyzer device can perform either the fetch server or client role, and it can perform two roles at the same time with the same FortiAnalyzer devices at the other end.
* Log fetching can be done only on two FortiAnalyzer devices that are running the same firmware version.
* Log fetching allows the administrator to fetch analytics logs from another FortiAnalyzer for redundancy.
* Log fetching allows the administrator to run queries and reports against historical data by retrieving archived logs from one FortiAnalyzer device and sending them to another FortiAnalyzer device.

QUESTION 52

What are the operating modes of FortiAnalyzer? (Choose two)
* Standalone
* Manager
* Analyzer
* Collector

QUESTION 53

If you upgrade your FortiAnalyzer firmware, what report elements can be affected?
* Output profiles
* Report settings
* Report scheduling
* Custom datasets

QUESTION 54

Which two statements are true regarding log fetching on FortiAnalyzer? (Choose two.)
* A FortiAnalyzer device can perform either the fetch server or client role, and it can perform two roles at the same time with the same FortiAnalyzer devices at the other end.
* Log fetching can be done only on two FortiAnalyzer devices that are running the same firmware version.
* Log fetching allows the administrator to fetch analytics logs from another FortiAnalyzer for redundancy.
* Log fetching allows the administrator to run queries and reports against historical data by retrieving archived logs from one FortiAnalyzer device and sending them to another FortiAnalyzer device.

QUESTION 55

Which daemon is responsible for enforcing raw log file size?
* logfiled
* oftpd
* sqlplugind
* miglogd

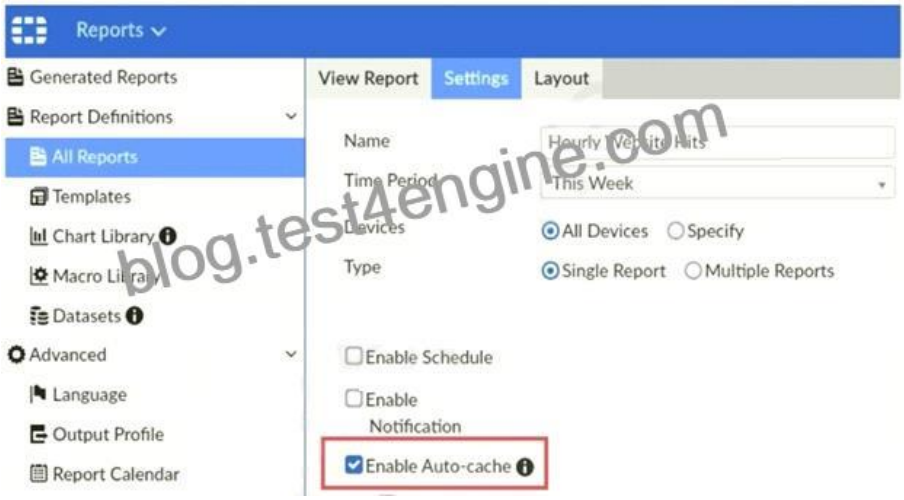
QUESTION 56

An administrator fortinet, is able to view logs and perform device management tasks, such as adding and removing registered devices. However, administrator fortinet is not able to create a mall server that can be used to send email.

What could be the problem?
* Fortinet is assigned the Standard_ User administrator profile.
* A trusted host is configured.
* ADOM mode is configured with Advanced mode.
* Fortinet is assigned the Restricted_ User administrator profile.

QUESTION 57

Refer to the exhibit.



Which two statements are true regarding enabling auto-cache on FortiAnalyzer? (Choose two.)
* Report size will be optimized to conserve disk space on FortiAnalyzer.
* Reports will be cached in the memory.
* This feature is automatically enabled for scheduled reports.
* Enabling auto-cache reduces report generation time for reports that require a long time to assemble datasets.

QUESTION 58

Which two statements are true regarding high availability (HA) on FortiAnalyzer? (Choose two.)
* FortiAnalyzer HA can function without VRRP. and VRRP is required only if you have more than two FortiAnalyzer devices in a cluster.
* FortiAnalyzer HA supports synchronization of logs as well as some system and configuration settings.
* All devices in a FortiAnalyzer HA cluster must run in the same operation mode: analyzer or collector.
* FortiAnalyzer HA implementation is supported by many public cloud infrastructures such as AWS, Microsoft Azure, and Google Cloud.

QUESTION 59

What is the purpose of the following CLI command?

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

* To add a log file checksum
* To add the MD’s hash value and authentication code
* To add a unique tag to each log to prove that it came from this FortiAnalyzer
* To encrypt log communications

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

QUESTION 60

Which two statements are true regarding FortiAnalyzer log forwarding? (Choose two.)
* In aggregation mode, you can forward logs to syslog and CEF servers as well.
* Forwarding mode forwards logs in real time only to other FortiAnalyzer devices.
* Aggregation mode stores logs and content files and uploads them to another FortiAnalyzer device at a scheduled time.
* Both modes, forwarding and aggregation, support encryption of logs between devices.

QUESTION 61

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?
* Click FortiView and generate a report for that administrator.
* Click Task Monitor and view the tasks performed by that administrator.
* Click Log View and generate a report for that administrator.
* View the tasks performed by the rogue administrator in Fabric View.

QUESTION 62

Which statements are true regarding securing communications between FortiAnalyzer and FortiGate with SSL? (Choose two.)
* SSL is the default setting.
* SSL communications are auto-negotiated between the two devices.
* SSL can send logs in real-time only.
* SSL encryption levels are globally set on FortiAnalyzer.
* FortiAnalyzer encryption level must be equal to, or higher than, FortiGate.

QUESTION 63

You have recently grouped multiple FortiGate devices into a single ADOM. System Settings > Storage Info shows the quota used.

What does the disk quota refer to?
* The maximum disk utilization for each device in the ADOM
* The maximum disk utilization for the FortiAnalyzer model
* The maximum disk utilization for the ADOM type
* The maximum disk utilization for all devices in the ADOM

Fortinet NSE5_FAZ-6.4 Real 2022 Braindumps Mock Exam Dumps:
https://www.test4engine.com/NSE5_FAZ-6.4_exam-latest-braindumps.html]