Fortinet

Exam Questions NSE5_FAZ-6.4

Fortinet NSE 5 - FortiAnalyzer 6.4

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

> All examinations will be up to date.

* 24/7 Quality Support

> We will provide service round the clock.

* 100% Pass Rate

> Our guarantee that you will pass the exam.

* Unique Gurantee

> If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1
The admin administrator is failing to register a FortiClient EMS on the FortiAnalyzer device. What can be the reason for this failure?

A. FortiAnalyzer is in an HA cluster.
B. ADOM mode should be set to advanced, in order to register the FortiClient EMS device.
C. ADOMs are not enabled on FortiAnalyzer.
D. A separate license is required on FortiAnalyzer in order to register the FortiClient EMS device.

Answer: C

NEW QUESTION 2
In order for FortiAnalyzer to collect logs from a FortiGate device, what configuration is required? (Choose two.)

A. Remote logging must be enabled on FortiGate
B. Log encryption must be enabled
C. ADOMs must be enabled
D. FortiGate must be registered with FortiAnalyzer

Answer: AD

Explanation:
Pg 70: "after you add and register a FortiGate device with the FortiAnalyzer unit, you must also ensure that the FortiGate device is configured to send logs to the FortiAnalyzer unit."
https://docs.fortinet.com/uploaded/files/4614/FortiAnalyzer-5.4.6-Administration%20Guide.pdf
Pg 45: "ADOMs must be enabled to support the logging and reporting of NON-FORTIGATE devices, such as FortiCarrier, FortiClientEMS, FortiMail, FortiWeb, FortiCache, and FortiSandbox."

NEW QUESTION 3
What is the purpose of the following CLI command?

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

NEW QUESTION 4
Which two statements about log forwarding are true? (Choose two.)

A. Forwarded logs cannot be filtered to match specific criteria.
B. Logs are forwarded in real-time only.
C. The client retains a local copy of the logs after forwarding.
D. You can use aggregation mode only with another FortiAnalyzer.

Answer: CD

Explanation:
https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/420493/modes https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/621804/log-forwarding

NEW QUESTION 5
An administrator has moved FortiGate A from the root ADOM to ADOM1. However, the administrator is not able to generate reports for FortiGate A in ADOM1.
What should the administrator do to solve this issue?

A. Use the execute sql-local rebuild-db command to rebuild all ADOM databases.
B. Use the execute sql-local rebuild-adom ADOM1 command to rebuild the ADOM database.
C. Use the execute sql-report run ADOM1 command to run a report.
D. Use the execute sql-local rebuild-adom root command to rebuild the ADOM database.

Answer: B

NEW QUESTION 6
In Log View, you can use the Chart Builder feature to build a dataset and chart based on the filtered search results.
Similarly, which feature you can use for FortiView?

A. Export to Report Chart
B. Export to PDF
C. Export to Chart Builder
D. Export to Custom Chart

Answer: A

NEW QUESTION 7
Which two constraints can impact the amount of reserved disk space required by FortiAnalyzer? (Choose two.)

A. License type
B. Disk size
C. Total quota
D. RAID level

Answer: CD

Explanation:
https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/368682/disk-space-allocation

NEW QUESTION 8
Which log type does the FortiAnalyzer indicators of compromise feature use to identify infected hosts?

A. Antivirus logs
B. Web filter logs
C. IPS logs
D. Application control logs

Answer: B

NEW QUESTION 9
You've moved a registered logging device out of one ADOM and into a new ADOM. What happens when you rebuild the new ADOM database?

A. FortiAnalyzer resets the disk quota of the new ADOM to default.
B. FortiAnalyzer migrates archive logs to the new ADOM.
C. FortiAnalyzer migrates analytics logs to the new ADOM.
D. FortiAnalyzer removes logs from the old ADOM.

Answer: C

Explanation:
https://kb.fortinet.com/kb/documentLink.do?externalID=FD40383

NEW QUESTION 10
View the exhibit:

What does the 1000MB maximum for disk utilization refer to?

A. The disk quota for the FortiAnalyzer model
B. The disk quota for all devices in the ADOM
C. The disk quota for each device in the ADOM
D. The disk quota for the ADOM type

Answer: B

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

NEW QUESTION 10
Logs are being deleted from one of your ADOMs earlier that the configured setting for archiving in your data policy. What is the most likely problem?

A. The total disk space is insufficient and you need to add other disk.
B. CPU resources are too high.
C. The ADOM disk quota is set too low based on log rates.
D. Logs in that ADOM are being forwarded in real-time to another FortiAnalyzer device.

Answer: C

Explanation:
https://help.fortinet.com/fmgr/50hlp/56/5-6-1/FMG FAZ/1100_Storage/0017_Deleted%20device%20logs.htm
https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/87802/automatic-deletion

NEW QUESTION 14
What can you do on FortiAnalyzer to restrict administrative access from specific locations?

A. Configure trusted hosts for that administrator.
B. Enable geo-location services on accessible interface.
C. Configure two-factor authentication with a remote RADIUS server.
D. Configure an ADOM for respective location.

Answer: A

NEW QUESTION 16
How do you restrict an administrator's access to a subset of your organization's ADOMs?

A. Set the ADOM mode to Advanced
B. Assign the ADOMs to the administrator's account
C. Configure trusted hosts
D. Assign the default Super_User administrator profile

Answer: B

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

NEW QUESTION 21
An administrator has configured the following settings: config system fortiview settings set resolve-ip enable end
What is the significance of executing this command?

A. Use this command only if the source IP addresses are not resolved on FortiGate.
B. It resolves the source and destination IP addresses to a hostname in FortiView on FortiAnalyzer.
C. You must configure local DNS servers on FortiGate for this command to resolve IP addresses on Forti Analyzer.
D. It resolves the destination IP address to a hostname in FortiView on FortiAnalyzer.

Answer: D

NEW QUESTION 25
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?

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

NEW QUESTION 28
What two things should an administrator do to view Compromised Hosts on FortiAnalyzer? (Choose two.)

A. Enable web filtering in firewall policies on FortiGate devices, and make sure these logs are sent to FortiAnalyzer.
B. Enable device detection on an interface on the FortiGate devices that are connected to the FortiAnalyzer.
C. Subscribe FortiAnalyzer to FortiGuard to keep its local threat database up-to-date.
D. Make sure all endpoints are reachable by FortiAnalyzer.

Answer: AC

NEW QUESTION 33
Which two methods can you use to send event notifications when an event occurs that matches a configured event handler? (Choose two.)

A. SMS
B. Email
C. SNMP
D. IM

Answer: BC

NEW QUESTION 34
What is the main purpose of using an NTP server on FortiAnalyzer and all of its registered devices?

A. Log correlation
B. Host name resolution
C. Log collection
D. Real-time forwarding

Answer: C

NEW QUESTION 36

In the FortiAnalyzer FortiView, source and destination IP addresses from FortiGate devices are not resolving to a hostname.
How can you resolve the source and destination IP addresses, without introducing any additional performance impact to FortiAnalyzer?

A. Resolve IP addresses on a per-ADOM basis to reduce delay on FortiView while IPs resolve
B. Configure # set resolve-ip enable in the system FortiView settings
C. Configure local DNS servers on FortiAnalyzer
D. Resolve IP addresses on FortiGate

Answer: D

Explanation:
https://packetplant.com/fortigate-and-fortianalyzer-resolve-source-and-destination-ip/
"As a best practice, it is recommended to resolve IPs on the FortiGate end. This is because you get both
source and destination, and it offloads the work from FortiAnalyzer. On FortiAnalyzer, this IP resolution does destination IPs only"

NEW QUESTION 40

What FortiView tool can you use to automatically build a dataset and chart based on a filtered search result?

A. Chart Builder
B. Export to Report Chart
C. Dataset Library
D. Custom View

Answer: A

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

NEW QUESTION 42

If you upgrade the FortiAnalyzer firmware, which report element can be affected?

A. Custom datasets
B. Report scheduling
C. Report settings
D. Output profiles

Answer: B

Explanation:
https://docs.fortinet.com/document/fortianalyzer/6.2.5/upgrade-guide/669300/checking-reports

NEW QUESTION 47

If a hard disk fails on a FortiAnalyzer that supports software RAID, what should you do to bring the FortiAnalyzer back to functioning normally, without losing data?

A. Hot swap the disk
B. Replace the disk and rebuild the RAID manually
C. Take no action if the RAID level supports a failed disk
D. Shut down FortiAnalyzer and replace the disk

Answer: D

Explanation:
 https://kb.fortinet.com/kb/documentLink.do?externalID=FD46446#:~:text=On%20FortiAnalyzer%2FFortiMana If a hard disk on a FortiAnalyzer unit fails, it must be replaced. On FortiAnalyzer devices that support
hardware RAID, the hard disk can be replaced while the unit is still running – known as hot swapping.
On FortiAnalyzer units with software RAID, the device must be shutdown prior to exchanging the hard disk.

NEW QUESTION 51

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.)

A. It creates a wildcard administrator using LDAP and RADIUS servers.
B. Administrator can log in to FortiAnalyzer using their credentials on remote servers LDAP and RADIUS.
C. Use remoteadmin from LDAP and RADIUS servers will be able to log in to FortiAnalyzer at anytime.
D. It allows administrators to use two-factor authentication.

Answer: BC

NEW QUESTION 55
What is the purpose of employing RAID with FortiAnalyzer?

A. To introduce redundancy to your log data
B. To provide data separation between ADOMs
C. To separate analytical and archive data
D. To back up your logs

Answer: A

Explanation:
https://en.wikipedia.org/wiki/RAID#:~:text=RAID%20(%22Redundant%20Array%20of%20Inexpensive,%2C%

NEW QUESTION 58
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?

A. FortiAnalyzer uses log fetching to retrieve the logs when back online
B. FortiGate uses the miglogd process to cache the logs
C. The logfiled process stores logs in offline mode
D. Logs are dropped

Answer: B

Explanation:

NEW QUESTION 63
What statements are true regarding disk log quota? (Choose two)

A. The FortiAnalyzer stops logging once the disk log quota is met.
B. The FortiAnalyzer automatically sets the disk log quota based on the device.
C. The FortiAnalyzer can overwrite the oldest logs or stop logging once the disk log quota is met.
D. The FortiAnalyzer disk log quota is configurable, but has a minimum o 100mb a maximum based on the reserved system space.

Answer: CD

NEW QUESTION 65
Which two statements are true regarding high availability (HA) on FortiAnalyzer? (Choose two.)

A. FortiAnalyzer HA can function without VRR
B. and VRRP is required only if you have more than two FortiAnalyzer devices in a cluster.
C. FortiAnalyzer HA supports synchronization of logs as well as some system and configuration settings.
D. All devices in a FortiAnalyzer HA cluster must run in the same operation mode: analyzer or collector.
E. FortiAnalyzer HA implementation is supported by many public cloud infrastructures such as AWS, Microsoft Azure, and Google Cloud.

Answer: BC

NEW QUESTION 66
How does FortiAnalyzer retrieve specific log data from the database?

A. SQL FROM statement
B. SQL GET statement
C. SQL SELECT statement
D. SQL EXTRACT statement

Answer: A

Explanation:
https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/137bb60e-ff37-11e8-8524-f8bc1258b8

NEW QUESTION 68
What are the operating modes of FortiAnalyzer? (Choose two)

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

Answer: CD

NEW QUESTION 73
What are offline logs on FortiAnalyzer?

A. Compressed logs, which are also known as archive logs, are considered to be offline logs.
B. When you restart FortiAnalyze
C. all stored logs are considered to be offline logs.
D. Logs that are indexed and stored in the SQL database.
E. Logs that are collected from offline devices after they boot up.

Answer: A

NEW QUESTION 76
Which daemon is responsible for enforcing raw log file size?

A. logfiled
B. oftpd
C. sqlplugind
D. miglogd

Answer: A

NEW QUESTION 79
Which statements are correct regarding FortiAnalyzer reports? (Choose two)

A. FortiAnalyzer provides the ability to create custom reports.
B. FortiAnalyzer glows you to schedule reports to run.
C. FortiAnalyzer includes pre-defined reports only.
D. FortiAnalyzer allows reporting for FortiGate devices only.

Answer: AB

NEW QUESTION 82
An administrator has moved FortiGate A from the root ADOM to ADOM1. Which two statements are true regarding logs? (Choose two.)

A. Analytics logs will be moved to ADOM1 from the root ADOM automatically.
B. Archived logs will be moved to ADOM1 from the root ADOM automatically.
C. Logs will be presented in both ADOMs immediately after the move.
D. Analytics logs will be moved to ADOM1 from the root ADOM after you rebuild the ADOM1 SQL database.

Answer: BC

NEW QUESTION 85
Which two statements are true regarding FortiAnalyzer log forwarding? (Choose two.)

A. In aggregation mode, you can forward logs to syslog and CEF servers as well.
B. Forwarding mode forwards logs in real time only to other FortiAnalyzer devices.
C. Aggregation mode stores logs and content files and uploads them to another FortiAnalyzer device at a scheduled time.
D. Both modes, forwarding and aggregation, support encryption of logs between devices.

Answer: CD

NEW QUESTION 87
What must you configure on FortiAnalyzer to upload a FortiAnalyzer report to a supported external server? (Choose two.)

A. SFTP, FTP, or SCP server
B. Mail server
C. Output profile
D. Report scheduling

Answer: AC

Explanation:
https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/6d9f8fb5-6cf4-11e9-81a4-0050569258 page 119
There is an option for "uploading reports to server" under configuring the output profile. The available options are: SFTP, FTP and SCP. You have to be careful on the question itself. The question tells you to "upload reports to a server (external server). Which means, a server has been configured already in this case prior to enabling the "upload reports to server".

NEW QUESTION 90

Relate Links

100% Pass Your NSE5_FAZ-6.4 Exam with Exambible Prep Materials

https://www.exambible.com/NSE5_FAZ-6.4-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/

100% Pass Your NSE5_FAZ-6.4 Exam with Exambible Prep Materials

https://www.exambible.com/NSE5_FAZ-6.4-exam/