Free Questions for NSE5_FAZ-7.2 by certsinside

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

Which two actions should an administrator take to view Compromised Hosts on FortiAnalyzer? (Choose two.)

Options:

A- Enable web filtering in firewall policies on FortiGate devices, and make sure these logs are sent to FortiAnalyzer.

B- Make sure all endpoints are reachable by FortiAnalyzer.

C- Enable device detection on an interface on the FortiGate devices that are connected to the FortiAnalyzer device.

D- Subscribe FortiAnalyzer to FortiGuard to keep its local threat database up to date.

Answer:

A, D

Explanation:

In order to configure IOC, you require the following:

* A one-year subscription to IOC. Note that FortiAnalyzer does include an evaluation license, but it is restrictive and only meant to give you an idea of how the feature works.

* A web filter services subscription on FortiGate device(s)

* Web filter policies on FortiGate device(s) that send traffic to FortiAnalyzer

Compromised Hosts or Indicators of Compromise service (IOC) is a licensed feature.

To view Compromised Hosts, you must turn on the UTM web filter of FortiGate devices and subscribe your FortiAnalyzer unit to FortiGuard to keep its local threat database synchronized with the FortiGuard threat database. See Subscribing FortiAnalyzer to FortiGuard.

Ref : https://docs.fortinet.com/document/fortianalyzer/6.4.0/administration-guide/137635/viewing-compromised-hosts

Question 2

Question Type: **MultipleChoice**

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

Which two statements are true regarding logs? (Choose two.)

Options:

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:

B, D

Question 3

Question Type: **MultipleChoice**

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

Options:

A- FortiAnalyzer HA can function without VRRP. and VRRP is required only if you have more than two FortiAnalyzer devices in a cluster.

B- FortiAnalyzer HA supports synchronization of logs as well as some system and configuration settings.

C- All devices in a FortiAnalyzer HA cluster must run in the same operation mode: analyzer or collector.

D- FortiAnalyzer HA implementation is supported by many public cloud infrastructures such as AWS, Microsoft Azure, and Google Cloud.

Answer:

B, C

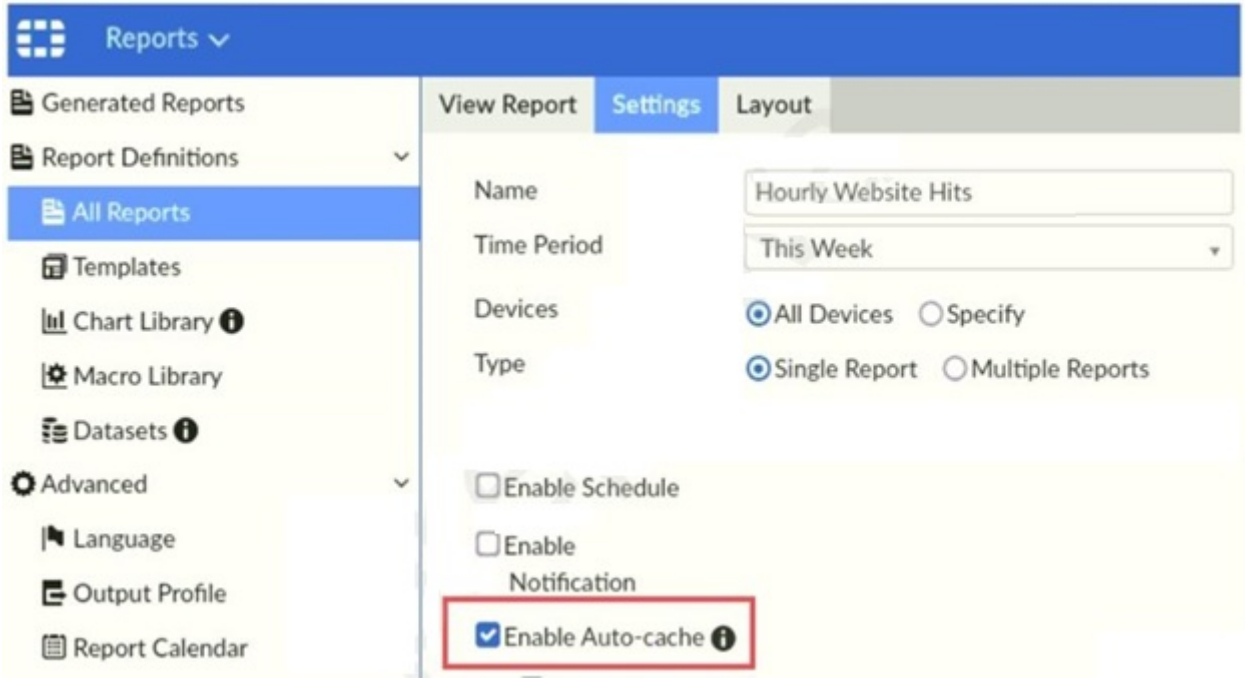
Explanation:

FortiAnalyzer HA implementation works only in networks where Virtual Router Redundancy Protocol (VRRP) is permitted. Therefore it may not be supported by some public cloud infrastructures.

Question 4

Question Type: MultipleChoice

Refer to the exhibit.



Which two statements are true regarding enabling auto-cache on FortiAnalyzer? (Choose two.)

Options:

A- Report size will be optimized to conserve disk space on FortiAnalyzer.

B- Reports will be cached in the memory.

C- This feature is automatically enabled for scheduled reports.

D- Enabling auto-cache reduces report generation time for reports that require a long time to assemble datasets.

Answer:

C, D

Explanation:

'Enable auto-cache in the report settings to boost the reporting performance and reduce report generation time. Scheduled reports have auto-cache enabled already.'

FortiAnalyzer_7.0_Study_Guide-Online page 306

Question 5

Question Type: MultipleChoice

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

What can be the reason for this failure?

Options:

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

Question 6

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

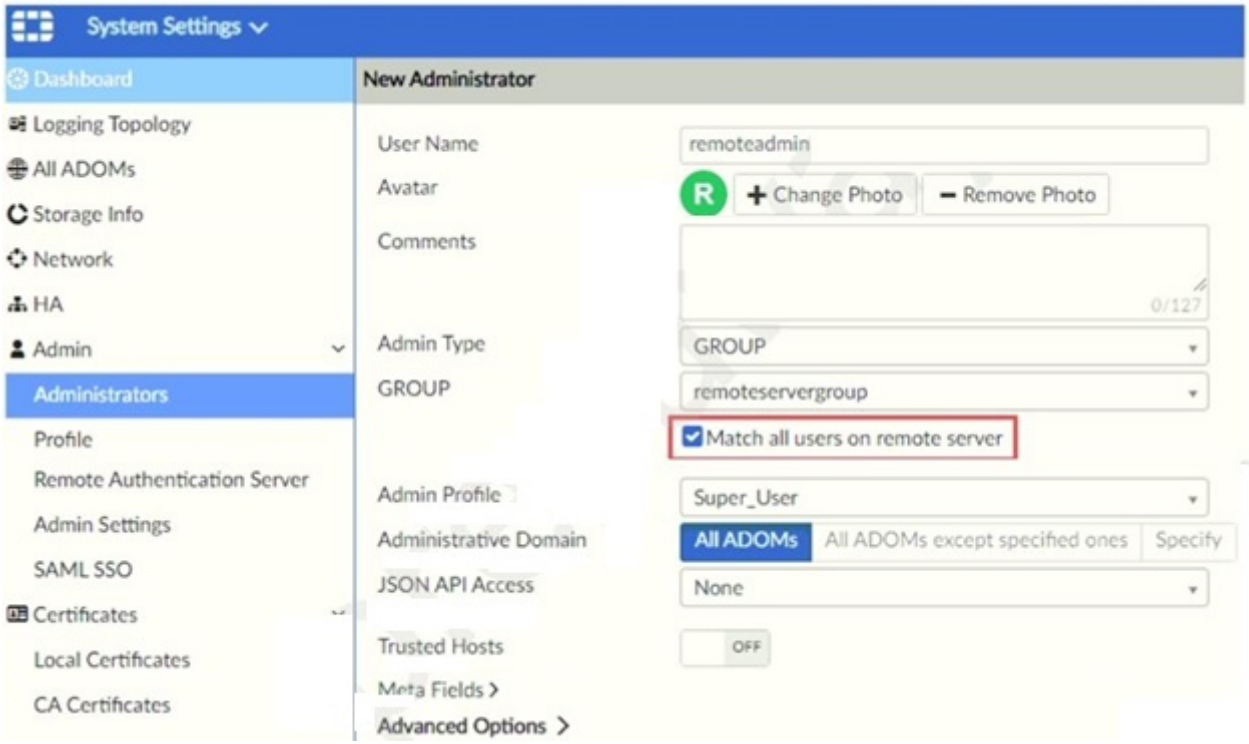
Explanation:

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

Question 7

Question Type: MultipleChoice

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.)

Options:

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:

A, B

Question 8

Question Type: **MultipleChoice**

Which two statements are true regarding FortiAnalyzer operating modes? (Choose two.)

Options:

A- When in collector mode, FortiAnalyzer collects logs from multiple devices and forwards these logs in the original binary format.

B- Collector mode is the default operating mode.

C- When in collector mode. FortiAnalyzer supports event management and reporting features.

D- By deploying different FortiAnalyzer devices with collector and analyzer mode in a network, you can improve the overall performance

of log receiving, analysis, and reporting

Answer:

A, D

Explanation:

https://docs.fortinet.com/document/fortianalyzer/7.0.0/administration-guide/312644/analyzer-collector-collaboration

Question 9

Question Type: MultipleChoice

Which statement is true regarding Macros on FortiAnalyzer?

Options:

A- Macros are ADOM specific and each ADOM will have unique macros relevant to that ADOM.

B- Macros are supported only on the FortiGate ADOM.

C- Macros are useful in generating excel log files automatically based on the reports settings.

D- Macros are predefined templates for reports and cannot be customized.

Answer:

A

Explanation:

FortiAnalyzer_7.0_Study_Guide-Online.pdf page 283: Note that macros are ADOM-specific and supported in FortiGate and FortiCarrier ADOMs only.

Question 10

Question Type: MultipleChoice

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?

Options:

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

Question 11

Question Type: MultipleChoice

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

Options:

A- Both modes, forwarding and aggregation, support encryption of logs between devices.

B- In aggregation mode, you can forward logs to syslog and CEF servers as well.

C- Aggregation mode stores logs and content files and uploads them to another FortiAnalyzer device at a scheduled time.

D- Forwarding mode forwards logs in real time only to other FortiAnalyzer devices.

Answer:

A, C

Explanation:

A) FortiAnalyzer_7.0_Study_Guide-Online.pdf page 148: The log communication between devices can be protected by encryption, with the desired encryption level, using the commands shown on the slide. (You need to interpret this. 'Real time' and 'aggregation' is about the 'moment' when Fortigate sends the logs. However, no matter the moment, Fortigate will upload logs encrypted or unencrypted based on previous / differente config).

C) FortiAnalyzer_7.0_Study_Guide-Online.pdf page 147: Aggregation: Logs and content files stored and uploaded at scheduled time.

To Get Premium Files for NSE5_FAZ-7.2 Visit

https://www.p2pexams.com/products/nse5_faz-7.2

For More Free Questions Visit

https://www.p2pexams.com/fortinet/pdf/nse5-faz-7.2