NSE5_FAZ-7.0 Q&As

Fortinet NSE 5 - FortiAnalyzer 7.0

Pass Fortinet NSE5_FAZ-7.0 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/nse5_faz-7-0.html

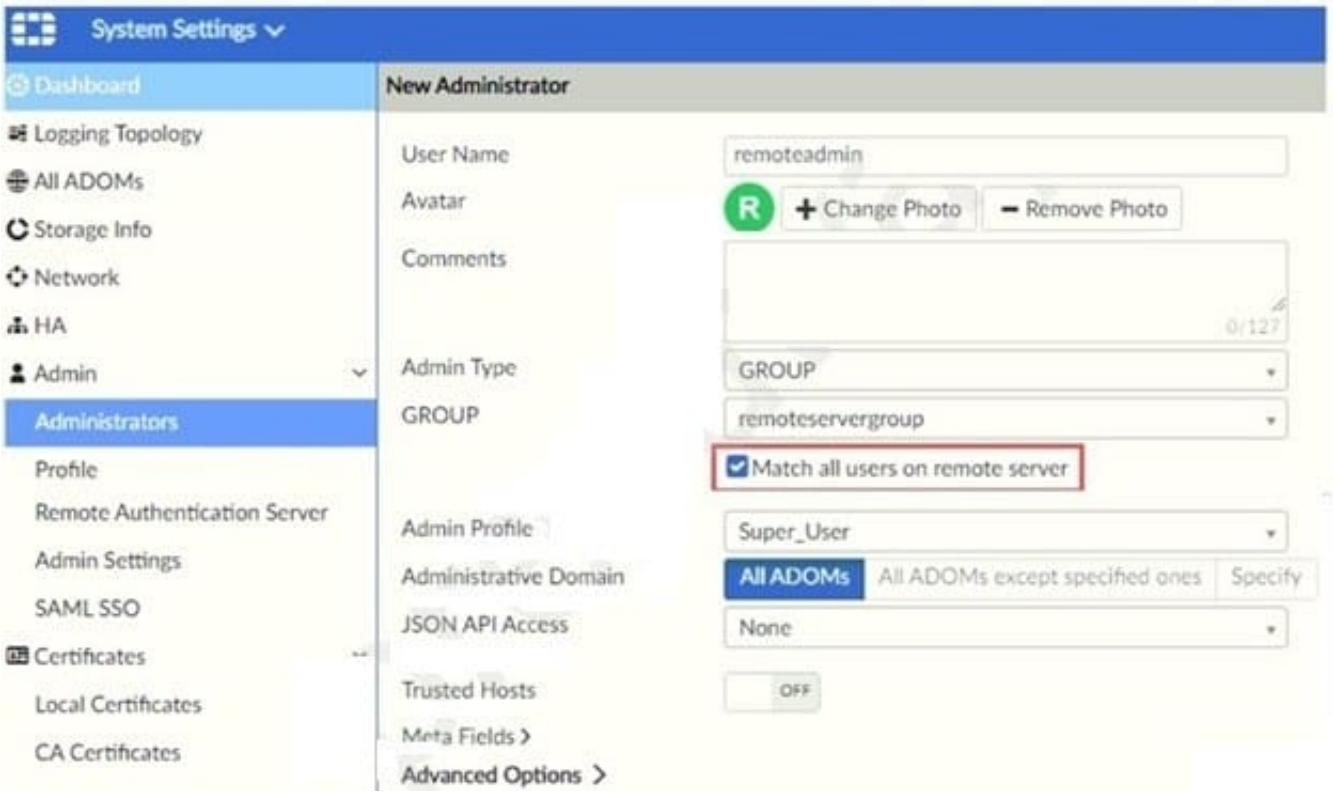
100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Fortinet Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

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.

Correct Answer: AB

Reference: https://docs.fortinet.com/document/fortimanager/7.0.1/administration- guide/858351/creating-administrators

QUESTION 2

Which two statement are true regardless initial Logs sync and Log Data Sync for Ha on FortiAnalyzer?

A. By default, Log Data Sync is disabled on all backup devise.

B. Log Data Sync provides real-time log synchronization to all backup devices.

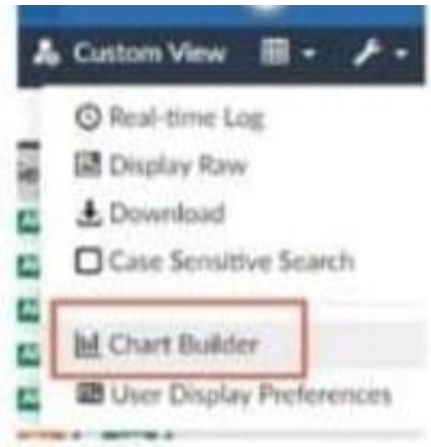
C. With initial Logs Sync, when you add a unit to an HA cluster, the primary device synchronizes its logs with the backup device.

D. When Logs Data Sync is turned on, the backup device will reboot and then rebuilt the log database with the synchronized logs.

Correct Answer: CD

QUESTION 3

Refer to the exhibit.



What is the purpose of using the Chart Builder feature on FortiAnalyzer?

A. In Log View, this feature allows you to build a dataset and chart automatically, based on the filtered search results.

B. In Log View, this feature allows you to build a chart and chart automatically, on the top 100 log entries.

C. This feature allows you to build a chart under FortiView.

D. You can add charts to generated reports using this feature.

Correct Answer: A

QUESTION 4

What is the best approach to handle a hard disk failure on a FortiAnalyzer that supports hardware RAID?

A. Hot swap the disk.

B. There is no need to do anything because the disk will self-recover.

C. Run execute format disk to format and restart the FortiAnalyzer device.

D. Shut down FortiAnalyzer and replace the disk

Correct Answer: A

Hardware RAID not software

QUESTION 5

How are logs forwarded when FortiAnalyzer is using aggregation mode?

A. Logs are forwarded as they are received and content files are uploaded at a scheduled time.

B. Logs and content files are stored and uploaded at a scheduled time.

C. Logs are forwarded as they are received.

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

Correct Answer: B

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 Reference:
https://docs.fortinet.com/document/fortianalyzer/6.2.0/cookbook/63238/what-is- the-difference-between-log-forward-and-log-aggregation-modes

QUESTION 6

For proper log correlation between the logging devices and FortiAnalyzer, FortiAnalyzer and all registered devices should:

A. Use DNS

B. Use host name resolution

C. Use real-time forwarding

D. Use an NTP server

Correct Answer: D

QUESTION 7

Which FortiAnalyzer feature allows you to retrieve the archived logs matching a specific timeframe from another FortiAnalyzer device?

A. Log upload

B. Indicators of Compromise

C. Log forwarding an aggregation mode

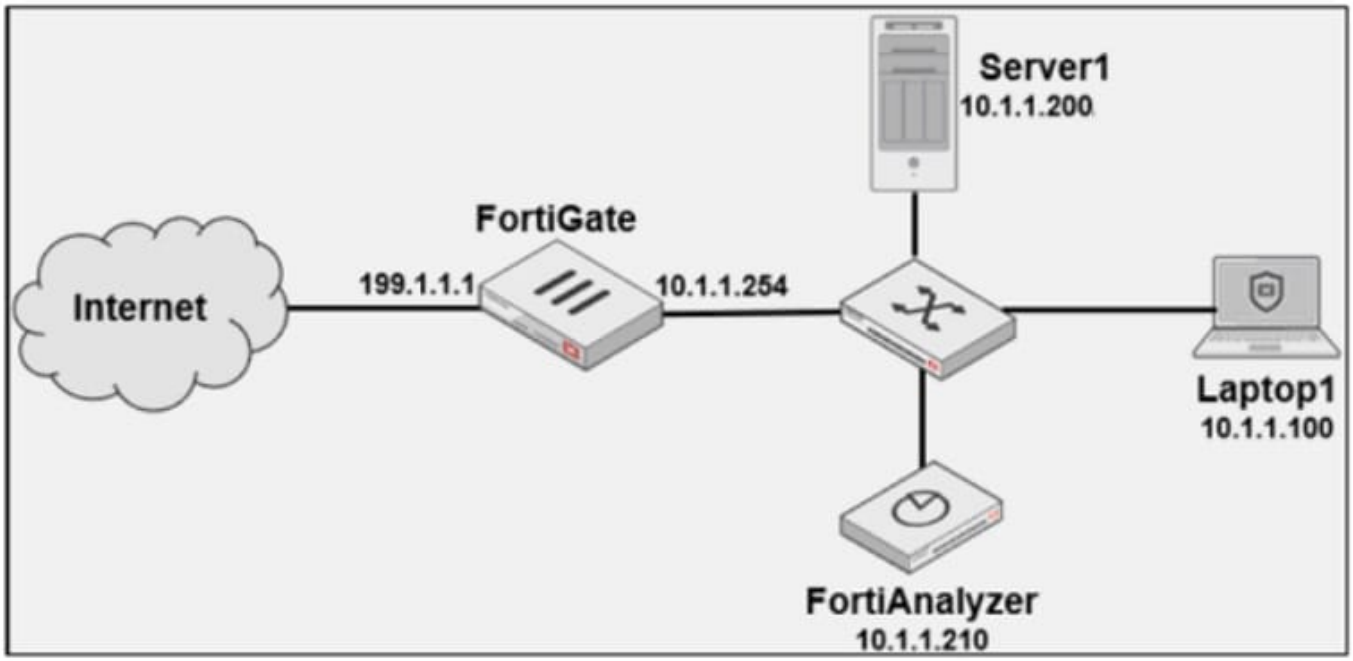
D. Log fetching

Correct Answer: D

https://docs.fortinet.com/document/fortianalyzer/6.2.0/administration- guide/651442/fetcher-management

QUESTION 8

Refer to the exhibit.



Laptopt is used by several administrators to manage FortiAnalyzer. You want to configure a generic text filter that matches all login attempts to the web interface generated by any user other than "admin" and coming from Laptop1: Which filter will achieve the desired result?

A. operation-login and performed_on=="GUI(10.1.1.100)" and user!=admin

B. operation-login and srcip==10.1.1.100 and dstip==10.1.1.210 and user==admin

C. operation-login and dstip==10.1.1.210 and userl-admin

D. operation-login and performed_on=="GUI(10.1.1.210)\\' and user!=admin

Correct Answer: D

QUESTION 9

View the exhibit.

```
Total Quota Summary:
     Total Quota    Allocated   Available   Allocate%
        63.7GB        12.7GB      51.0GB       19.9%

System Storage Summary:
     Total     Used      Available     Use%
    78.7GB     2.9GB       75.9GB      3.6%

Reserved space: 15.0GB (19.0% of total space).
```

Why is the total quota less than the total system storage?

A. 3.6% of the system storage is already being used.

B. Some space is reserved for system use, such as storage of compression files, upload files, and temporary report files

C. The oftpd process has not archived the logs yet

D. The logfiled process is just estimating the total quota

Correct Answer: B

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

QUESTION 10

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

A. A FortiGate ADOM

B. The FortiGate serial number

C. A pre-shared key

D. Valid FortiAnalyzer credentials

Correct Answer: D

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. FortiAnalyzer_7.0_Study_Guide-Online pag. 93

QUESTION 11

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

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.

Correct Answer: AC

Aggregation mode is only supported between two FortiAnalyer devices, so B is wrong.

Forwarding is always in real time and does not ONLY forward to other FortiAnalyzer devices. It also forwards to Syslog/CEF. D is wrong. Answer is A and C.

QUESTION 12

What is the purpose of the following CLI command?

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

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

Correct Answer: A

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

QUESTION 13

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.

Correct Answer: C

Reference: https://help.fortinet.com/fa/faz50hlp/56/5-6-2/FMG-

FAZ/0800_ADOMs/0015_FortiClient%20and%20ADOMs.htm

QUESTION 14

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

Correct Answer: B

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

QUESTION 15

You crested a playbook on FortiAnalyzer that uses a FortiOS connector

When configuring the FortiGate side, which type of trigger must be used so that the actions in an automation stitch are available in the FortiOS connector?

A. FortiAnalyzer Event Handler

B. Incoming webhook

C. FortiOS Event Log

D. Fabric Connector event

Correct Answer: B

"One possible scenario is shown on the slide:

1.

Traffic flows through the FortiGate

2.

FortiGate sends logs to FortiAnalyzer

3.

FortiAnalyzer detects some suspicious traffic and generates an event

4.

The event triggers the execution of a playbook in FortiAnalyzer, which sends a webhook call to FortiGate so that it runs

an automation stitch

5.

FortiGate runs the automation stitch with the corrective or preventive actions"