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.leads4pass.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

What is the purpose of output variables?

A. To store playbook execution statistics

B. To use the output of the previous task as the input of the current task

C. To display details of the connectors used by a playbook

D. To save all the task settings when a playbook is exported

Correct Answer: A

QUESTION 2

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

Correct Answer: D

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"

QUESTION 3

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

Correct Answer: A

Similar to the Chart Builder feature in Log View, you can export a chart from a FortiView. The chart export includes any filters you set on the FortiView. FortiAnalyzer_7.0_Study_Guide-Online pag. 292.

QUESTION 4

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

A. Log fetching allows the administrator to fetch analytics logs from another FortiAnalyzer for redundancy.

B. 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.

C. Log fetching can be done only on two FortiAnalyzer devices that are running the same firmware version.

D. 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.

Correct Answer: CD

Using FortiAnalyzer, you can enable log fetching. This allows FortiAnalyzer to fetch the archived logs of specified devices from another FortiAnalyzer, which you can then run queries or reports on for forensic analysis.

The FortiAnalyzer device that fetches logs operates as the fetch client, and the other FortiAnalyzer device that sends logs operates as the fetch server. Log fetching can happen only between two FortiAnalyzer devices, and both of them must be running the same firmware version. A FortiAnalyzer device can perform either the fetch server or client role, and it can perform two roles at the same time with different FortiAnalyzer devices at the other end. FortiAnalyzer_7.0_Study_Guide-Online pag. 168

QUESTION 5

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.

Correct Answer: CD

QUESTION 6

After you have moved a registered logging device out of one ADOM and into a new ADOM, what is the purpose of running the following CLI command? execute sql-local rebuild-adom

A. To reset the disk quota enforcement to default

B. To remove the analytics logs of the device from the old database

C. To migrate the archive logs to the new ADOM

D. To populate the new ADOM with analytical logs for the moved device, so you can run reports

Correct Answer: D

D is correct : From FortiAnalyzer study guide

QUESTION 7

Which statement correctly describes the management extensions available on FortiAnalyzer?

A. Management extensions do not require additional licenses.

B. Management extensions may require a minimum number of CPU cores to run.

C. Management extensions allow FortiAnalyzer to act as a FortiSIEM supervisor.

D. Management extensions require a dedicated VM for best performance.

Correct Answer: B

Events in FortiAnalyzer will be in one of four statuses. The current status will determine if more actions need to be taken by the security team or not.

The possible statuses are:

Unhandled: The security event risk is not mitigated or contained, so it is considered open.

Contained: The risk source is isolated.

Mitigated: The security risk is mitigated by being blocked or dropped.

(Blank): Other scenarios.

FortiAnalyzer_7.0_Study_Guide-Online pag. 189.

QUESTION 8

Which daemon is responsible for enforcing the log file size?

A. sqlplugind

B. logfiled

C. miglogd

D. ofrpd

Correct Answer: B

Disk quota enforcement is performed by different processes:

The logfiled process enforces the log file size and is also responsible for disk quota enforcement by monitoring the other processes.

FortiAnalyzer_7.0_Study_Guide-Online pag. 121

QUESTION 9

Why should you use an NTP server on FortiAnalyzer and all registered devices that log into FortiAnalyzer?

A. To properly correlate logs

B. To use real-time forwarding

C. To resolve host names

D. To improve DNS response times

Correct Answer: A

Study Guide 7.0 page 30: Synchronize the time on FortiAnalyzer and all Registered devices wit han NTP server for correct log correlation.

QUESTION 10

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.

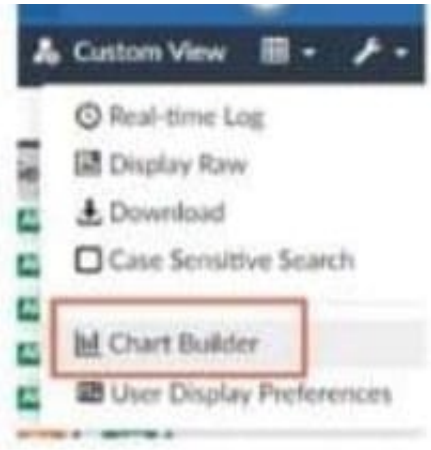
C. FortiAnalyzer includes pre-defined reports only.

D. FortiAnalyzer allows reporting for FortiGate devices only.

Correct Answer: AB

QUESTION 11

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.

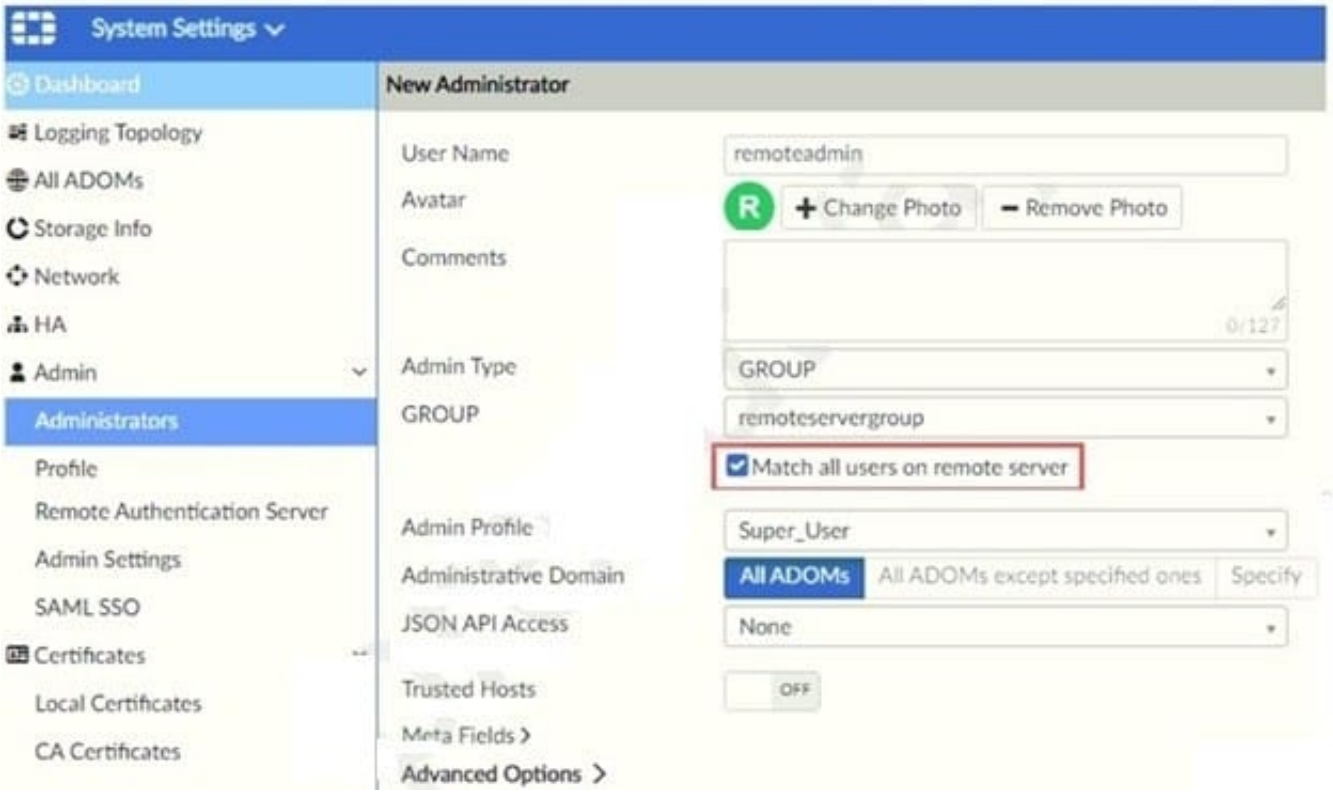
C. This feature allows you to build a chart under FortiView.

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

Correct Answer: A

QUESTION 12

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 13

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.

Correct Answer: A

Reference: https://docs.fortinet.com/document/fortigate/6.2.0/hardening-your- fortigate/582009/system-administrator-best-practices

QUESTION 14

What is Log Insert Lag Time on FortiAnalyzer?

A. The number of times in the logs where end users experienced slowness while accessing resources.

B. The amount of lag time that occurs when the administrator is rebuilding the ADOM database.

C. The amount of time that passes between the time a log was received and when it was indexed on FortiAnalyzer.

D. The amount of time FortiAnalyzer takes to receive logs from a registered device

Correct Answer: C

QUESTION 15

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

Correct Answer: A

page 27: synchronize the time on FortiAnalyzer and all registered devices with an NTP server for proper log correlation.