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

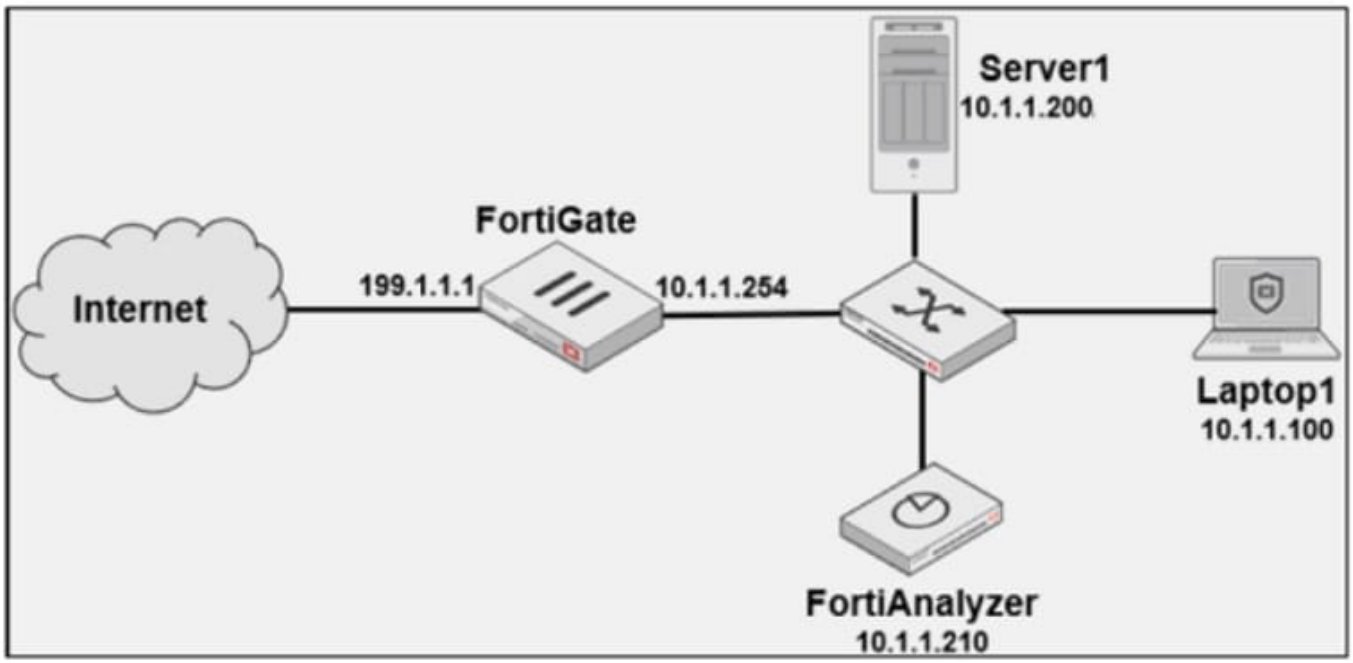
100% Passing Guarantee
100% Money Back Assurance

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

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 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

Which statement is true regarding Macros on FortiAnalyzer?

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.

Correct Answer: A

FortiAnalyzer 7.0 Study Guide online page no: 283 Reference: https://docs2.fortinet.com/document/fortianalyzer/6.2.3/administration- guide/617380/creating-macros

QUESTION 4

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. 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.

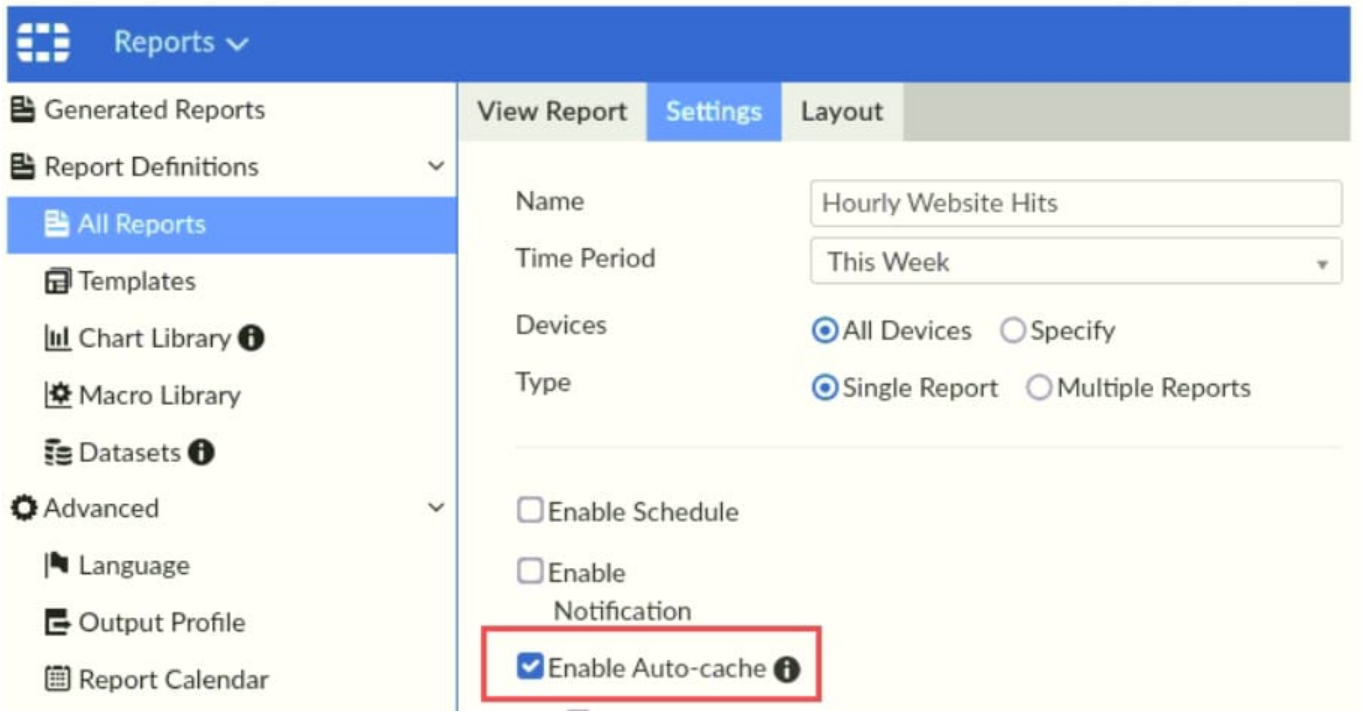
Correct Answer: AD

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 5

Refer to the exhibit.



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

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.

Correct Answer: CD