DUMPSARENA

Fortinet NSE 5 - FortiAnalyzer 7.0

Fortinet NSE5_FAZ-7.0

Version Demo

Total Demo Questions: 10

Total Premium Questions: 114

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

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

ANSWER: A

Explanation:

- Synchronize the time on FortiAnalyzer and all registered devices with an NTP server for proper log correlation

QUESTION NO: 2

What is the recommended method of expanding disk space on a FortiAnalyzer VM?

A. From the VM host manager, add an additional virtual disk and use the #execute lvm extend command to expand the storage

B. From the VM host manager, expand the size of the existing virtual disk

C. From the VM host manager, expand the size of the existing virtual disk and use the # execute format disk command to reformat the disk

D. From the VM host manager, add an additional virtual disk and rebuild your RAID array

ANSWER: A

Explanation:

https://kb.fortinet.com/kb/documentLink.do?externalID=FD40848

QUESTION NO: 3

What can the CLI command # diagnose test application oftpd 3 help you to determine?

A. What devices and IP addresses are connecting to FortiAnalyzer

B. What logs, if any, are reaching FortiAnalyzer

C. What ADOMs are enabled and configured

D. What devices are registered and unregistered

ANSWER: A

Explanation:

https://docs.fortinet.com/document/fortianalyzer/6.2.5/cli-reference/395556/test#test_application

QUESTION NO: 4

Which two actions should an administrator take 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.

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 NO: 5

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

ANSWER: A

Explanation:

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

QUESTION NO: 6

Which statements are true regarding securing communications between FortiAnalyzer and FortiGate with IPsec? (Choose two.)

A. Must configure the FortiAnalyzer end of the tunnel only--the FortiGate end is auto-negotiated.

B. Must establish an IPsec tunnel ID and pre-shared key.

C. IPsec cannot be enabled if SSL is enabled as well.

D. IPsec is only enabled through the CLI on FortiAnalyzer.

ANSWER: B D

Explanation:

Option B is correct because you must establish an IPsec tunnel ID and pre-shared key to secure the communication between FortiAnalyzer and FortiGate with IPsec12. The tunnel ID is a unique identifier for each tunnel and the pre-shared key is a secret passphrase that authenticates the peers.

Option D is correct because IPsec is only enabled through the CLI on FortiAnalyzer1. You cannot configure IPsec settings through the GUI on FortiAnalyzer.

QUESTION NO: 7

In FortiAnalyzer's FormView, source and destination IP addresses from FortiGate devices are not resolving to

a hostname. How can you resolve the source and destination IPs, without introducing any additional

performance impact to FortiAnalyzer?

A. Configure local DNS servers on FortiAnalyzer

B. Resolve IPs on FortiGate

C. Configure # set resolve-ip enable in the system FortiView settings

D. Resolve IPs on a per-ADOM basis to reduce delay on FortiView while IPs resolve

ANSWER: B

QUESTION NO: 8

Which two elements are contained in a system backup created on FortiAnalyzer? (Choose two.)

A. System information

B. Logs from registered devices

C. Report information

D. Database snapshot

ANSWER: A C

Explanation:

What does the System Configuration backup include?

System information, such as the device IP address and administrative user information.

Device list, such as any devices you configured to allow log access.

Report information, such as any configured report settings, as well as all your custom report details. These are not the actual reports.

FortiAnalyzer_7.0_Study_Guide-Online pag. 29

FortiAnalyzer_7.0_Study_Guide-Online.pdf page 29: What does the System Configuration backup include?

• System information, such as the device IP address and administrative user information

• Device list, such as any devices you configured to allow log access

• Report information, such as any configured report settings, as well as all your custom report details. These are not the actual reports.

QUESTION NO: 9

Which two statements are true regarding fabric connectors? (Choose two.)

A. Configuring fabric connectors to send notification to ITSM platform upon incident creation Is more efficient than third-party information from the FortiAnalyzer API.

B. Fabric connectors allow to save storage costs and improve redundancy.

C. Storage connector service does not require a separate license to send logs to cloud platform.

D. Cloud-Out connections allow you to send real-time logs to pubic cloud accounts like Amazon S3, Azure Blob , and Google Cloud.

ANSWER: A D

QUESTION NO: 10

Which statements are true of Administrative Domains (ADOMs) in FortiAnalyzer? (Choose two.)

A. ADOMs are enabled by default.

B. ADOMs constrain other administrator's access privileges to a subset of devices in the device list.

C. Once enabled, the Device Manager, FortiView, Event Management, and Reports tab display per ADOM.

D. All administrators can create ADOMs--not just the admin administrator.

ANSWER: B C