NSE5_FAZ-6.2^{Q&As}

Fortinet NSE 5 - FortiAnalyzer 6.2

Pass Fortinet NSE5_FAZ-6.2 Exam with 100% Guarantee

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

https://www.pass2lead.com/nse5_faz-6-2.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 purposes does the auto-cache setting on reports serve? (Choose two.)

A. To reduce report generation time

B. To automatically update the hcache when new logs arrive

C. To reduce the log insert lag rate

D. To provide diagnostics on report generation time

Correct Answer: AB

Reference: https://docs.fortinet.com/document/fortianalyzer/6.0.0/administration-guide/282280/enablingautocache

QUESTION 2

What must you configure on FortiAnalyzer to upload a FortiAnalyzer report to a supported external server? (Choose two.)

A. SFTP, FTP, or SCP server

B. Mail server

C. Output profile

D. Report scheduling

Correct Answer: AC

QUESTION 3

What FortiGate process caches logs when FortiAnalyzer is not reachable?

A. logfiled

B. sqlplugind

C. oftpd

D. miglogd

Correct Answer: D

Reference: https://forum.fortinet.com/tm.aspx?m=143106

![Pass2Lead](https://Pass2Lead.com)
QUESTION 4

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

Correct Answer: A

QUESTION 5

For which two SAML roles can the FortiAnalyzer be configured? (Choose two.)

A. Principal

B. Service provider

C. Identity collector

D. Identity provider

Correct Answer: BD

Reference: https://docs.fortinet.com/document/fortianalyzer/6.2.0/new-features/957811/samladminauthentication#:~:text=for%20the%20administrator.-,FortiAnalyzer%20can%20play%20the%20role%20of%20the%20identity%20provider%20(IdP,external%20identity%20provider%20is%20available

QUESTION 6

Which two settings must you configure on FortiAnalyzer to allow non-local administrators to authenticate to FortiAnalyzer with any user account in a single LDAP group? (Choose two.)

A. A local wildcard administrator account

B. A remote LDAP server

C. A trusted host profile that restricts access to the LDAP group

D. An administrator group

Correct Answer: AB

Reference: https://kb.fortinet.com/kb/documentLink.do?externalID=FD38567

![Pass2Lead](https://Pass2Lead.com)
QUESTION 7

View the exhibit:

```
Data Policy
  Keep Logs for Analytics    60      ——    Days         ▼
  Keep Logs for Archive      365     ——    Days         ▼
Disk Utilization
  Maximum Allowed            1000    ——    MB           ▼     Out of Available: 62.8 GB
  Analytics: Archive         70%     ▼     30%                ☐ Modify
  Alert and Delete When      90%     ▼
  Usage Reaches
```

What does the 1000MB maximum for disk utilization refer to?

A. The disk quota for the FortiAnalyzer model

B. The disk quota for all devices in the ADOM

C. The disk quota for each device in the ADOM

D. The disk quota for the ADOM type

Correct Answer: B

QUESTION 8

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

QUESTION 9

FortiAnalyzer centralizes which functions? (Choose three)

A. Network analysis

B. Graphical reporting

C. Content archiving / data mining

D. Vulnerability assessment

E. Security log analysis / forensics

Correct Answer: BCE

QUESTION 10

Logs are being deleted from one of the ADOMs earlier than the configured setting for archiving in the data policy.

What is the most likely problem?

A. CPU resources are too high

B. Logs in that ADOM are being forwarded, in real-time, to another FortiAnalyzer device

C. The total disk space is insufficient and you need to add other disk

D. The ADOM disk quota is set too low, based on log rates

Correct Answer: D

Reference: https://help.fortinet.com/fmgr/50hlp/56/5-6-1/FMG-FAZ/1100_Storage/0017_Deleted%20device
%20logs.htm

QUESTION 11

Which tabs do not appear when FortiAnalyzer is operating in Collector mode?

A. FortiView

B. Event Management

C. Device Manger

D. Reporting

Correct Answer: B

QUESTION 12

You have recently grouped multiple FortiGate devices into a single ADOM. System Settings > Storage Info shows the quota used.

What does the disk quota refer to?

A. The maximum disk utilization for each device in the ADOM

B. The maximum disk utilization for the FortiAnalyzer model

C. The maximum disk utilization for the ADOM type

D. The maximum disk utilization for all devices in the ADOM

Correct Answer: B

QUESTION 13

FortiAnalyzer reports are dropping analytical data from 15 days ago, even though the data policy setting for

analytics logs is 60 days.

What is the most likely problem?

A. Quota enforcement is acting on analytical data before a report is complete

B. Logs are rolling before the report is run

C. CPU resources are too high

D. Disk utilization for archive logs is set for 15 days

Correct Answer: A

Reference: https://forum.fortinet.com/tm.aspx?m=138806

QUESTION 14

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: B

Reference: https://docs.fortinet.com/document/fortianalyzer/6.0.2/cli-reference/551596/sql-local

QUESTION 15

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.

Correct Answer: BC

Latest NSE5_FAZ-6.2 Dumps   **NSE5_FAZ-6.2 PDF Dumps**   **NSE5_FAZ-6.2 Practice Test**