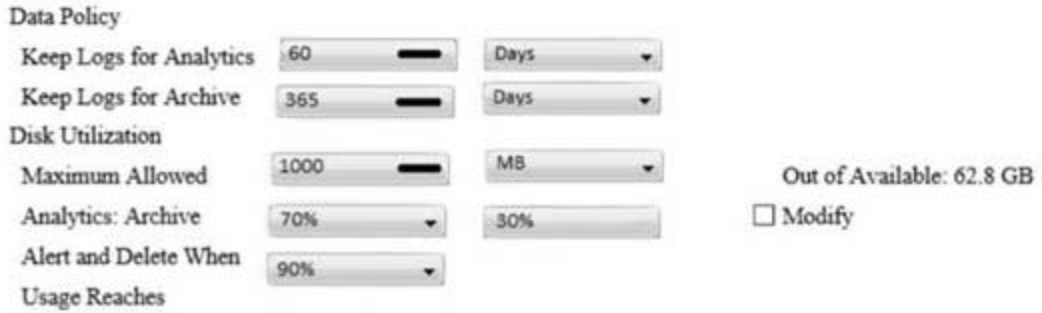
Actual exam question from Fortinet's NSE5_FAZ-6.0

Question #: 1

Topic #: 1

[All NSE5_FAZ-6.0 Questions]

View the exhibit:



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

Show Suggested Answer

Actual exam question from Fortinet's NSE5_FAZ-6.0

Question #: 2

Topic #: 1

[All NSE5_FAZ-6.0 Questions]

You've moved a registered logging device out of one ADOM and into a new ADOM. What happens when you rebuild the new ADOM database?

A. FortiAnalyzer resets the disk quota of the new ADOM to default.

B. FortiAnalyzer migrates archive logs to the new ADOM.

C. FortiAnalyzer migrates analytics logs to the new ADOM.

D. FortiAnalyzer removes logs from the old ADOM.

Show Suggested Answer

Actual exam question from Fortinet's NSE5_FAZ-6.0

Question #: 3

Topic #: 1

[All NSE5_FAZ-6.0 Questions]

What happens when a log file saved on FortiAnalyzer disks reaches the size specified in the device log settings?

A. The log file is stored as a raw log and is available for analytic support.

B. The log file rolls over and is archived.

C. The log file is purged from the database.

D. The log file is overwritten.

Show Suggested Answer

Actual exam question from Fortinet's NSE5_FAZ-6.0

Question #: 4

Topic #: 1

[All NSE5_FAZ-6.0 Questions]

What is the purpose of employing RAID with FortiAnalyzer?

A. To introduce redundancy to your log data

B. To provide data separation between ADOMs

C. To separate analytical and archive data

D. To back up your logs

Show Suggested Answer

Actual exam question from Fortinet's NSE5_FAZ-6.0

Question #: 5

Topic #: 1

[All NSE5_FAZ-6.0 Questions]

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

Show Suggested Answer

Actual exam question from Fortinet's NSE5_FAZ-6.0

Question #: 6

Topic #: 1

[All NSE5_FAZ-6.0 Questions]

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 <disk number> 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

Show Suggested Answer

Actual exam question from Fortinet's NSE5_FAZ-6.0

Question #: 7

Topic #: 1

[All NSE5_FAZ-6.0 Questions]

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.

Show Suggested Answer

Actual exam question from Fortinet's NSE5_FAZ-6.0

Question #: 8

Topic #: 1

[All NSE5_FAZ-6.0 Questions]

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

Show Suggested Answer

Actual exam question from Fortinet's NSE5_FAZ-6.0

Question #: 9

Topic #: 1

[All NSE5_FAZ-6.0 Questions]

In order for FortiAnalyzer to collect logs from a FortiGate device, what configuration is required? (Choose two.)

A. Remote logging must be enabled on FortiGate

B. Log encryption must be enabled

C. ADOMs must be enabled

D. FortiGate must be registered with FortiAnalyzer

Show Suggested Answer

Actual exam question from Fortinet's NSE5_FAZ-6.0

Question #: 10

Topic #: 1

[All NSE5_FAZ-6.0 Questions]

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

Show Suggested Answer

Actual exam question from Fortinet's NSE5_FAZ-6.0

Question #: 11

Topic #: 1

[All NSE5_FAZ-6.0 Questions]

What FortiView tool can you use to automatically build a dataset and chart based on a filtered search result?

A. Chart Builder

B. Export to Report Chart

C. Dataset Library

D. Custom View

Show Suggested Answer

Actual exam question from Fortinet's NSE5_FAZ-6.0

Question #: 12

Topic #: 1

[All NSE5_FAZ-6.0 Questions]

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

Show Suggested Answer

Actual exam question from Fortinet's NSE5_FAZ-6.0

Question #: 13

Topic #: 1

[All NSE5_FAZ-6.0 Questions]

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

Show Suggested Answer

Actual exam question from Fortinet's NSE5_FAZ-6.0

Question #: 14

Topic #: 1

[All NSE5_FAZ-6.0 Questions]

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

Show Suggested Answer

Actual exam question from Fortinet's NSE5_FAZ-6.0

Question #: 15

Topic #: 1

[All NSE5_FAZ-6.0 Questions]

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

Show Suggested Answer

Actual exam question from Fortinet's NSE5_FAZ-6.0

Question #: 16

Topic #: 1

[All NSE5_FAZ-6.0 Questions]

If you upgrade your FortiAnalyzer firmware, what report elements can be affected?

A. Output profiles

B. Report settings

C. Report scheduling

D. Custom datasets

Show Suggested Answer