EXAMTOPICS

-Expert Verified, Online, **Free**.



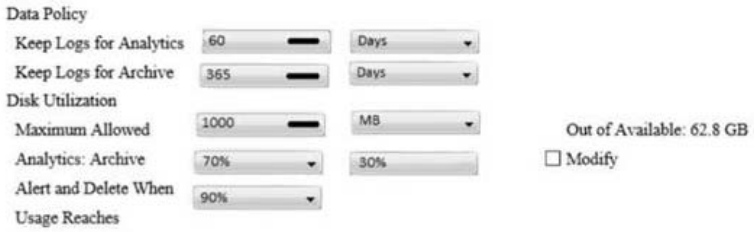
CERTIFICATION TEST

-CertificationTest.net - Cheap & Quality Resources With Best Support

Question #1 *Topic 1*

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

Suggested Answer: *B*

HasanAhmed Highly Voted 6 years, 2 months ago

B is the Right Answer

upvoted 6 times

mmelo Most Recent 5 years, 9 months ago

B is correct

upvoted 1 times

freakydummy 5 years, 11 months ago

B is correct

upvoted 1 times

Question #2 *Topic 1*

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.

Suggested Answer: *C*

geek1992 Highly Voted 6 years, 1 month ago

no c is correct sorry

upvoted 6 times

ohmaxx Most Recent 4 years, 6 months ago

C is correct

upvoted 1 times

mau_80 4 years, 7 months ago

Selected Answer: C

C: When you move a device, only the archive logs (compressed logs) are migrated to the new ADOM. The analytics logs (indexed logs) stay in the old ADOM until you rebuild the database.

upvoted 2 times

yadavarya97 4 years, 11 months ago

Page 118 , FAZ study guide

upvoted 1 times

ami376 5 years, 4 months ago

C is correct

upvoted 1 times

Morm0n 5 years, 6 months ago

think before you type here misleading information. It's option C, since you are are doing the rebuild, the analytics logs will move to the new ADOM.

upvoted 1 times

Sarwar 5 years, 6 months ago

Sorry B is correct

upvoted 1 times

Sarwar 5 years, 6 months ago

C is correct as per the study guide page 111

upvoted 2 times

d8tr 5 years, 10 months ago

B is correct per Lab Demo. Analytics would need to be migrated manually, archived files are automatic

upvoted 1 times

killbots Highly Voted 5 years, 10 months ago

C is correct when you rebuild(manual process) the database the device's analytics are migrated. The analytics logs (indexed logs) stay in the old ADOM until you rebuild the database. studyguide page 111

upvoted 5 times

freakydummy 5 years, 11 months ago

C is correct

upvoted 2 times

mai340 6 years ago

C is correct

upvoted 2 times

geek1992 6 years, 1 month ago

B not C

upvoted 1 times

Question #3 *Topic 1*

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.

Suggested Answer: *B*

certchris Most Recent 5 years, 2 months ago

B is correct page 123, study guide

upvoted 1 times

Dee244 5 years, 5 months ago

B is correct https://help.fortinet.com/fa/faz50hlp/56/5-6-1/FMG-FAZ/1100_Storage/0010_Log%20and%20file%20workflow.htm

upvoted 1 times

killbots 5 years, 10 months ago

Agreed Correct answer is B

upvoted 2 times

freakydummy 5 years, 11 months ago

B is correct

upvoted 3 times

Question #4 *Topic 1*

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

Suggested Answer: *A*

mmelo Most Recent 5 years, 9 months ago

A is correct. To introduce redundancy to your log data

upvoted 2 times

freakydummy 5 years, 11 months ago

A is correct

upvoted 2 times

Question #5 *Topic 1*

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

Suggested Answer: *D*

Sil_ Most Recent 3 years, 12 months ago

The correct is D.

upvoted 1 times

certchris 5 years, 2 months ago

D is correct page 146, study guide

upvoted 2 times

freakydummy 5 years, 11 months ago

D is correct

upvoted 3 times

Question #6 *Topic 1*

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

Suggested Answer: *A*

freakydummy Highly Voted 5 years, 11 months ago

A is correct

upvoted 5 times

Question #7 *Topic 1*

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.

Suggested Answer: *B*

certchris Most Recent 5 years, 2 months ago

B is correct page 130, study guide

upvoted 1 times

ami376 5 years, 4 months ago

Answer B https://www.fortinetguru.com/2020/07/log-forwarding-fortianalyzer-fortios-6-2-3/

upvoted 1 times

freakydummy 5 years, 11 months ago

B is correct

upvoted 3 times

Question #8 *Topic 1*

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

Suggested Answer: *B*

freakydummy Most Recent 5 years, 11 months ago

B is correct

upvoted 4 times

Question #9 *Topic 1*

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

Suggested Answer: *A, D*

freakydummy Highly Voted 5 years, 11 months ago

A and D are correct

upvoted 5 times

Thomas_2020 Most Recent 2 years, 7 months ago

Selected Answer: AD

A&D, are correct

upvoted 1 times

Brightm 5 years, 8 months ago

A and D are correct

upvoted 3 times

Question #10 *Topic 1*

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

Suggested Answer: *A*

mmelo Highly Voted 5 years, 9 months ago

A is correct.

Device and ADOM Status Check

diagnose test application oftpd 3 # Devices and IPs are connecting to FortiAnalyzer diagnose test application oftpd 8 # Receiving logs in FortiAnalyzre diagnose dvm adom list # ADOMs are enabled and configured diagnose dvm device list # Devices or VDOMs are currently registed and unregistered

upvoted 8 times

Thomas_2020 Most Recent 2 years, 7 months ago

A is Correct, but diagnose test application oftpd 8 # Receiving logs in FortiAnalyzre --> Not IS: diagnose DEBUG application oftpd 8 , is debug not test

upvoted 1 times

hbiyoudi 4 years, 8 months ago

A is correct https://help.fortinet.com/fmgr/cli/5-6-2/Document/1600_diagnose/test+.htm#test_application_..189

upvoted 1 times

freakydummy 5 years, 11 months ago

A is correct

upvoted 4 times