Question #1 *Topic 1*

On FortiAnalyzer, what is a wildcard administrator account?

A. An account that permits access to members of a LDAP group

B. An account that allows guest access with read-only privileges

C. An account that requires two-factor authentication

D. An account that validates against any user account on a FortiAuthenticator

Suggested Answer: *D*

Community vote distribution

A (100%)

mau_80 3 years ago

Selected Answer: A

A is the correct answer

upvoted 2 times

pratap105 3 years, 2 months ago

A is the correct answer

upvoted 1 times

Laflo 4 years ago

A is the correct one

upvoted 1 times

Question #2 *Topic 1*

Which FortiAnalyzer feature allows you to retrieve the archived logs matching a specific timeframe from another FortiAnalyzer device?

A. Log forwarding in aggregation mode

B. Log upload

C. Log fetching

D. Indicators of Compromise

Suggested Answer: *C*

mmelo 4 years, 2 months ago

C is correct

upvoted 1 times

Question #3 *Topic 1*

How does FortiAnalyzer retrieve specific log data from the database?

A. SQL FROM statement

B. SQL GET statement

C. SQL SELECT statement

D. SQL EXTRACT statement

Suggested Answer: *C*

mmelo 4 years, 2 months ago

C is correct

upvoted 1 times

Question #4 *Topic 1*

Logs are being deleted from one of your ADOMs earlier than the configured setting for archiving in your data policy. What is the most likely problem?

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

B. CPU resources are too high

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

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

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

mmelo 4 years, 2 months ago
C is correct
upvoted 1 times

Question #5 *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. Configure trusted hosts

C. Assign the ADOMs to the administrator's account

D. Assign the default Super_User administrator profile

Suggested Answer: *C*

mmelo 4 years, 2 months ago

C is correct

upvoted 1 times

Question #6 *Topic 1*

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

A. Chart Builder

B. Dataset Library

C. Custom View

D. Export to Report Chart

Suggested Answer: *A*

Community vote distribution

D (100%)

Christiandus 2 years ago

Selected Answer: D

D is correct

FortiAnalyzer_6.4 P222

upvoted 2 times

MEDO162 3 years, 8 months ago

D is correct

FortiAnalyzer_6.4 P222

upvoted 2 times

Oopy 3 years, 11 months ago

A is correct.

From FAZ6.4 Self Paced Training

A quick way to build a custom dataset and chart is to use the chart builder tool. This tool is located in Log View and allows you to build a dataset and chart automatically based on your filtered search results.

upvoted 1 times

Mr_Bello 3 years, 11 months ago

I think LogView and FortiView are two different tools. Keyword in question is "FortiView" which makes me believe D should be correct

upvoted 3 times

mmelo 4 years, 2 months ago

D is correct

upvoted 3 times

Question #7 *Topic 1*

FortiAnalyzer uses the Optimized Fabric Transfer Protocol (OFTP) over SSL for what purpose?

A. To prevent log modification during backup

B. To send an identical set of logs to a second logging server

C. To encrypt log communication between devices

D. To upload logs to a SFTP server

Suggested Answer: *C*

mmelo 4 years, 2 months ago

C is correct

upvoted 2 times

Question #8 *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 <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, add an additional disk and rebuild your RAID array

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

Suggested Answer: *A*
Reference:
http://kb.fortinet.com/kb/microsites/microsite.do?cmd=displayKC&docType=kc&externalId=FD40848

mmelo 4 years, 2 months ago
A is correct
upvoted 2 times

Question #9 *Topic 1*

What FortiGate process caches logs when FortiAnalyzer is not reachable?

A. oftpd

B. miglogd

C. sqlplugind

D. logfiled

Suggested Answer: *B*

mmelo 4 years, 2 months ago

B is correct

upvoted 2 times

Question #10 *Topic 1*

What is the purpose of the following CLI command?

```
# configure system global
     set log-checksum md5
   end
```

A. To add the MD5's hash value and authentication code

B. To encrypt log communications

C. To add a unique tag to each log to provide that it came from this FortiAnalyzer

D. To add a log file checksum

Suggested Answer: *A*

Community vote distribution

D (100%)

mmelo Highly Voted 4 years, 2 months ago

Correc is D.

set log-checksum md5 = record log file's MD5 hash value only.
set log-checksum md5-auth = record log file's MD5 hash value and authentication code
upvoted 6 times

Christiandus Most Recent 2 years ago

Selected Answer: D

Correct is D.

set log-checksum md5 = record log file's MD5 hash value only.
set log-checksum md5-auth = record log file's MD5 hash value and authentication code
upvoted 1 times

Question #11 *Topic 1*

In FortiAnalyzer's FortiView, 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 # set resolve-ip enable in the system FortiView settings

B. Resolve IPs on FortiGate

C. Configure local DNS servers on FortiAnalyzer

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

Suggested Answer: *A*

Community vote distribution

B (100%)

Christiandus 2 years ago

Selected Answer: B

B is correct

FortiAnalyzer 6.4 P157

upvoted 2 times

MEDO162 3 years, 8 months ago

B is correct

FortiAnalyzer 6.4 P157

upvoted 1 times

Kevin_Howard 3 years, 11 months ago

I believe that B is the correct answer. A would use resources.

upvoted 2 times

Sarwar 4 years ago

B is correct

upvoted 2 times

Question #12 *Topic 1*

What is the purpose of employing RAID with FortiAnalyzer?

A. To provide data separation between ADOMs

B. To separate analytical and archive data

C. To back up your logs

D. To introduce redundancy to your log data

Suggested Answer: *D*

mmelo 4 years, 2 months ago

Correct is D

upvoted 2 times