156-585 Q&As

Check Point Certified Troubleshooting Expert

Pass CheckPoint 156-585 Exam with 100% Guarantee

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

https://www.geekcert.com/156-585.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CheckPoint Official Exam Center

QUESTION 1

Which command can be run in Expert mode to verify the core dump settings?

A. grep cdm /config/db/coredump

B. grep cdm /config/db/initial

C. grep $FWDIR/config/db/initial

D. cat /etc/sysconfig/coredump/cdm.conf

Correct Answer: B

https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=andsolutionid=sk92764 [Expert@HostName]# grep cdm /config/db/initial

QUESTION 2

An administrator receives reports about issues with log indexing and text searching regarding an existing Management Server. In trying to find a solution she wants to check if the process responsible for this feature is running correctly. What is true about the related process?

A. fwm manages this database after initialization of the ICA

B. cpd needs to be restarted manual to show in the list

C. fwssd crashes can affect therefore not show in the list

D. solr is a child process of cpm

Correct Answer: D

QUESTION 3

Some users from your organization have been reporting some connection problems with CIFS since this morning

You suspect an IPS issue after an automatic IPS update last night. So you want to perform a packet capture on uppercase I only directly after the IPS chain module (position 4 in the chain) to check If the packets pass the IPS. What command do you need to run?

A. fw monitor -ml -pi 5 -e

B. fw monitor -pi 5 -e

C. tcpdump -eni any

D. fw monitor -pi asm

Correct Answer: C

QUESTION 4

James is using the same filter expression in fw monitor for CITRIX very often and instead of typing this all the time he wants to add it as a macro to the fw monitor definition file.

What\\'s the name and location of this file?

A. $FWDIR/lib/fwmonltor.def

B. $FWDIR/conf/fwmonltor.def

C. $FWDIR/lib/tcpip.def

D. $FWDIR/lib/fw.monitor

Correct Answer: A

QUESTION 5

What table does the command "fwaccel conns" pull information from?

A. fwxl_conns

B. SecureXLCon

C. cphwd_db

D. sxl_connections

Correct Answer: A