DUMPSBOSS.COM

Check Point Certified Troubleshooting Expert

Checkpoint 156-585

Version Demo

Total Demo Questions: 10

Total Premium Questions: 75

Buy Premium PDF

https://dumpsboss.com

support@dumpsboss.com

dumpsboss.com

QUESTION NO: 1

What process monitors, terminates, and restarts critical Check Point processes as necessary?

A. CPWD

B. CPM

C. FWD

D. FWM

ANSWER: A

QUESTION NO: 2

When debugging is enabled on firewall kernel module using the ‘fw ctl debug’ command with required options, many debug messages are provided by the kernel that help the administrator to identify issues. Which of the following is true about these debug messages generated by the kernel module?

A. Messages are written to a buffer and collected using ‘fw ctl kdebug’

B. Messages are written to console and also /var/log/messages file

C. Messages are written to /etc/dmesg file

D. Messages are written to $FWDIR/log/fw.elg

ANSWER: B

QUESTION NO: 3

Troubleshooting issues with Mobile Access requires the following:

A. Standard VPN debugs, packet captures, and debugs of ‘cvpnd’ process on Security Gateway

B. Standard VPN debugs and packet captures on Security Gateway, debugs of ‘cvpnd’ process on Security Management

C. ‘ma_vpnd’ process on Security Gateway

D. Debug logs of FWD captured with the command - ‘fw debug fwd on TDERROR_MOBILE_ACCESS=5’

ANSWER: A

QUESTION NO: 4

What is the best way to resolve an issue caused by a frozen process?

A. Reboot the machine

B. Restart the process

C. Kill the process

D. Power off the machine

ANSWER: B

QUESTION NO: 5

In Security Management High Availability, if the primary and secondary managements, running the same version of R80.x, are in a state of ‘Collision’, how can this be resolved?

A. Administrator should manually synchronize the servers using SmartConsole

B. The Collision state does not happen in R80.x as the synchronizing automatically on every publish action

C. Reset the SIC of the secondary management server

D. Run the command ‘fw send synch force’ on the primary server and ‘fw get sync quiet’ on the secondary server

ANSWER: A

QUESTION NO: 6

What are some measures you can take to prevent IPS false positives?

A. Exclude problematic services from being protected by IPS (sip, H.323, etc.)

B. Use IPS only in Detect mode

C. Use Recommended IPS profile

D. Capture packets, Update the IPS database, and Back up custom IPS files

ANSWER: A

QUESTION NO: 7

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

ANSWER: A

QUESTION NO: 8

Which one of the following is NOT considered a Solr core partition?

A. CPM_0_Revisions

B. CPM_Global_A

C. CPM_Global_R

D. CPM_0_Disabled

ANSWER: D

QUESTION NO: 9

Which process is responsible for the generation of certificates?

A. cpm

B. cpca

C. dbsync

D. fwm

ANSWER: B

QUESTION NO: 10

Check Point provides tools & commands to help you to identify issues about products and applications. Which Check Point command can help you to display status and statistics information for various Check Point products and applications?

A. cpstat

B. CPstat

C. CPview

D. fwstat

ANSWER: A