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

Rules within the Threat Prevention policy use the Malware database and network objects. Which directory is used for the Malware database?

A. $FWDIR/conf/install_manager_tmp/ANTIMALWARE/conf/

B. $CPDIR/conf/install_manager_lmp/ANTIMALWARE/conf/

C. $FWDIR/conf/install_firewall_imp/ANTIMALWARE/conf/

D. $FWDIR/log/install_manager_tmp/ANTIMALWARBlog?

Correct Answer: A

QUESTION 2

If IPS protections that prevent SecureXL from accelerating traffic, such as Network Quota, Fingerprint Scrambling. TTL Masking etc, have to be used, what is a recommended practice to enhance the performance of the gateway?

A. Use the IPS exception mechanism

B. Disable all such protections

C. Disable SecureXL and use CoreXL

D. Upgrade the hardware to include more Cores and Memory

Correct Answer: A

For protections that prevent SecureXL from accelerating traffic , use the IPS exception mechanism. This mechanism allows SecureXL to accelerate connections that match exception rules. For example, the Network Quota protection does not disable SecureXL templates on connections that match the protection\\'s exception rules.

QUESTION 3

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

A. CPM_0_Revisions

B. CPM_Global_A

C. CPM_Gtobal_R

D. CPM_0_Disabled

Correct Answer: D

CPM_0_Active - Contains SMC_User Damain, system domain information from both public data and private session CPM_0_Revision - contains revision and public data CPM_Global_A - Contains CP_Data log, APPI, IPS, global domain information for both public data and private session CPM_Global_R - Contail Global revision and pubic data

CPM_0_Log - Contains Log data Solr has 2 of these cores CPM_Global_M - contains statuses of SmarView New revision are transfer from active core to revision core once a day at midnight

Reference: http://dkcheckpoint.blogspot.com/2019/12/check-point-certified-security-master.html

QUESTION 4

You have configured IPS Bypass Under Load function with additional kernel parameters ids_tolerance_no_stress=15 and ids_tolerance_stress-15 For configuration you used the *fw ctl set\\' command After reboot you noticed that these parameters returned to their default values

What do you need to do to make this configuration work immediately and stay permanent?

A. Set these parameters again with "fw ctl set" and edit appropriate parameters in $FWDIR/boot/modules/ fwkern.conf

B. Use script $FWDIR/bin IpsSetBypass.sh to set these parameters

C. Set these parameters again with "fw ctl set" and save configuration with "save config"

D. Edit appropriate parameters in $FWDIR/boot/modules/fwkern.conf

Correct Answer: A

To set the desired value for this kernel parameter permanently:

For Gaia / SecurePlatform OS:

[Expert@HostName]# touch $FWDIR/boot/modules/fwkern.conf

https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=andsolutionid=sk62848

QUESTION 5

RAD is initiated when Application Control and URL Filtering blades are active on the Security Gateway What is the purpose of the following RAD configuration file SFWDIR/conf/rad_settings.C?

A. This file contains the location information tor Application Control and/or URL Filtering entitlements

B. This file contains the information on how the Security Gateway reaches the Security Managers RAD service for Application Control and URL Filtering

C. This file contains RAD proxy settings

D. This file contains all the host name settings for the online application detection engine

Correct Answer: B