CheckPoint.156-585.v2022-05-09.q49

Exam Code:	156-585
Exam Name:	Check Point Certified Troubleshooting Expert
Certification Provider:	CheckPoint
Free Question Number:	49
Version:	v2022-05-09
# of views:	1264
# of Questions views:	490
https://www.freeqas.com/qa/CheckPoint/156-585/CheckPoint.156-585.v2022-05-09.q49.html	

NEW QUESTION: 1
Your fwm constantly crashes and is restarted by the watchdog. You can't find any coredumps related to this process, so you need to check If coredumps are enabled at all How can you achieve that?
A. in dish run show core-dump status
B. in dish run set core-dump status
C. in expert mode run show core-dump status
D. in dish run show coredumb status
Answer: D (LEAVE A REPLY)

NEW QUESTION: 2
What is the main SecureXL database for tracking acceleration status of traffic?
A. cphwd_tmp1
B. cphwd_db
C. cphwd_dev_identity_table
D. cphwd_dev_conn_table
Answer: (SHOW ANSWER)

NEW QUESTION: 3
Which file is commonly associated with troubleshooting crashes on a system such as the Security Gateway?
A. core dump
B. CPMIL dump
C. tcpdump
D. fw monitor
Answer: A (LEAVE A REPLY)

NEW 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

Answer: (SHOW ANSWER)

Explanation

https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=

NEW 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 all the host name settings for the online application detection engine

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 the location information tor Application Control and/or URL Filtering entitlements

D. This file contains RAD proxy settings

Answer: B (LEAVE A REPLY)

NEW QUESTION: 6

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

A. grep SFWDIR/config/db/initial

B. grep cdm /config/db/coredump

C. grep cdm /config/db/initial

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

Answer: (SHOW ANSWER)

NEW QUESTION: 7

Which command(s) will turn off all vpn debug collection?

A. vpn debug off

B. fw ctl debug 0

C. vpn debug -a off

D. vpn debug off and vpn debug ikeoff

Answer: D (LEAVE A REPLY)

NEW QUESTION: 8

Check Point Access Control Daemons contains several daemons for Software Blades and features Which Daemon is usedfor Application & Control URL Filtering?

A. rad

B. cprad
C. pdpd
D. pepd
Answer: D (LEAVE A REPLY)

NEW QUESTION: 9
What command is usedtofind out which port Multi-Portal has assigned to the Mobile Access Portal?
A. mpclient getdata sslvpn
B. mpclient getdata mobi
C. netstat getdata sslvpn
D. netstat -nap | grep mobile
Answer: (SHOW ANSWER)

NEW QUESTION: 10
You need to run a kernel debug over a longer period of time as the problem occurs only once or twice a week. Therefore, you need to add a timestamp to the kernel debug and write the output to a file but you can't afford to fill up all the remaining disk space and you only have 10 GB free for saving the debugs. What is the correct syntax for this?
A. fw ctl kdebug -T -f -m 10 -s 1000000 > debugfilename
B. fw ctl debug -T -f -m 10 -s 1000000 -o debugfilename
C. fw ctl kdebug -T -f -m 10 -s 1000000 -o debugfilename
D. fw ctl kdebug -T -m 10 -s 1000000 -o debugfilename
Answer: B (LEAVE A REPLY)

NEW QUESTION: 11
When a User process or program suddenly crashes, a core dump is often used to examine the problem. Which command is used to enable the core-dumping via GAIA dish?
A. set core-dump enable
B. set core-dump total
C. set core-dump per_process
D. set user-dump enable
Answer: A (LEAVE A REPLY)

NEW QUESTION: 12
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
Answer: A (LEAVE A REPLY)

https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk62848&partition=Advanced&product=IPS

NEW QUESTION: 13
VPN issues may result from misconfiguration, communication failure, or incompatible default configurations between peers Which basic command syntax needs to be used for troubleshooting Site-to-Site VPN Issues?
A. vpn truncon debug
B. fw debug truncon
C. vpn debug truncon
D. cp debug truncon
Answer: (SHOW ANSWER)

NEW QUESTION: 14
Check Point Threat Prevention policies can contain multiple policy layers and each layer consists of its own Rule Base Which Threat Prevention daemon is used for Anti-virus?
A. in.msd
B. in.emaild.mta
C. in emaild
D. ctasd
Answer: C (LEAVE A REPLY)

NEW QUESTION: 15
Which command do you need to execute to insert fw monitor after TCP streaming (out) in the outbound chain using absolute position? Given the chain was 1ffffe0, choose the correct answer.
A. fw monitor -po -0x1ffffe0
B. fw monitor -p0 ox1ffffe0
C. fw monitor -po 1ffffe0
D. fw monitor -p0 -ox1ffffe0
Answer: A (LEAVE A REPLY)
https://sc1.checkpoint.com/documents/R80.40/WebAdminGuides/EN/CP_R80.40_PerformanceTuning_AdminGuide/Content/Topics-PTG/CLI/fw-monitor.htm

NEW QUESTION: 16
Which one of the following is NOT considered a Solr core partition:
A. CPM_Gtobal_R
B. CPM_Global_A
C. CPM_0_Disabled
D. CPM_0_Revisions
Answer: A (LEAVE A REPLY)

NEW QUESTION: 17
When running a debug with fw monitor, which parameter will create a more verbose output?
A. -i
B. -d
C. -0
D. -i
Answer: B (LEAVE A REPLY)

NEW QUESTION: 18
Which command is most useful for debugging the fwaccel module?
A. fw zdebug
B. securexl debug
C. fw debug
D. fwaccel dbg
Answer: D (LEAVE A REPLY)

NEW QUESTION: 19
When a User process or program suddenly crashes, a core dump is often used to examine the problem. Which command is used to enable the core-dumping via GAIA dish?
A. set core-dump enable
B. set core-dump per_process
C. set user-dump enable
D. set core-dump total
Answer: D (LEAVE A REPLY)

NEW QUESTION: 20
What are four main database domains?
A. System, Global, Log, Event
B. System, User, Global, Log
C. Local, Global, User, VPN
D. System, User, Host, Network
Answer: B (LEAVE A REPLY)

NEW QUESTION: 21

URL Filtering is an essential part of Web Security in the Gateway. For the Security Gateway to perform a URL lookup when a client makes a URL request, where is the sync-request forwarded from if a sync-request is required"
A. URLF Kernel Client
B. URLF Online Service
C. RAD User Space
D. RAD Kernel Space
Answer: A (LEAVE A REPLY)

NEW QUESTION: 22
The management configuration stored in the Postgres database is partitioned into several relational database Domains, like - System, User, Global and Log Domains. The User Domain stores the network objects and security policies. Which of the following is stored in the Log Domain?
A. Active and past logs received from Gateways and Servers
B. Log Domain is not stored in Postgres database, it is part of Solr indexer only
C. Active Logs received from Security Gateways and Management Servers
D. Configuration data of Log Servers and saved queries for applications
Answer: (SHOW ANSWER)

NEW QUESTION: 23
Which is the correct "fw monitor" syntax for creating a capture file for loading it into WireShark?
A. fw monitor -e "accept<FILTER EXPRESSION>;" -o Output.cap
B. fw monitor -e "accept<FILTER EXPRESSION>;" >> Output.cap
C. This cannot be accomplished as it is not supported with R80.10
D. fw monitor -e "accept<FILTER EXPRESSION>;" -file Output.cap
Answer: (SHOW ANSWER)

NEW QUESTION: 24
Rules within the Threat Prevention policy use the Malware database and network objects. Which directory is used for the Malware database?
A. $FWDIR/log/install_manager_tmp/ANTIMALWARBlog?
B. $CPDIR/conf/install_manager_lmp/ANTIMALWARE/conf/
C. $FWDIR/conf/install_manager_tmp/ANTIMALWARE/conf/
D. $FWDIR/conf/install_firewall_imp/ANTIMALWARE/conf/
Answer: A (LEAVE A REPLY)

NEW QUESTION: 25
You need to run a kernel debug over a longer period of time as the problem occurs only once or twice a week. Therefore you need to add a timestamp to the kernel debug and write the output to a file What is the correct syntax for this?
A. fw ctl debug -T -f > filename.debug
B. fw ctl kdebug -T -f > filename.debug
C. fw ctl kdebug -T -f -o filename.debug

D. fw ctl kdebug -T > filename.debug
Answer: A (LEAVE A REPLY)

NEW QUESTION: 26
If the cpsemd process of SmartEvent has crashed or is having trouble coming up. then it usually indicates that_____.
A. Postgres database ts down
B. Cpd daemon is unable to connect to the log server
C. The logged in administrator does not have permissions to run SmartEvent
D. The SmartEvent core on the Solr mdexer has been deleted
Answer: D (LEAVE A REPLY)

NEW QUESTION: 27
Which command can be run in Expert mode to verify the core dump settings?
A. grep cdm /config/db/coredump
B. grep $FWDIR/config/db/initial
C. grep cdm /config/db/initial
D. cat /etc/sysconfig/coredump/cdm.conf
Answer: B (LEAVE A REPLY)

NEW QUESTION: 28
Your users have some issues connecting Mobile Access VPN to the gateway. How can you debug the tunnel establishment?
A. run vpn debug truncon
B. in the file $CVPNDIR/conf/httpd.conf change the line loglevel .. To LogLevel debug and run cvpnrestart
C. in the file $VPNDIR/conf/httpd.conf the line Loglevel .. To LogLevel debug and run vpn restart
D. run fw ctl zdebug -m sslvpn all
Answer: B (LEAVE A REPLY)

NEW QUESTION: 29
What is connect about the Resource Advisor (RAD) service on the Security Gateways?
A. RAD functions completely in user space The Pattern Matter (PM) module ofthe CMI looks up for URLs in the cache and if not found, contact the RAD process inuser space to do online categorization
B. RAD is not a separate module, it is an integrated function of the 'fw1 kernel module and does all operations in the kernel space
C. RAD has a kernel module that looks up the kernel cache, notifies client about hits and misses andforwards a-sync requests to RADuser space module which is responsible for online categorization
D. RAD is completely loaded as a kernel module that looks up URL in cache and if not found connects online for categorization There isno user space involvement in this process
Answer: A (LEAVE A REPLY)

NEW QUESTION: 30
What does CMI stand for in relation to the Access Control Policy?
A. Content Management Interface

B. Content Matching Infrastructure
C. Context Manipulation Interface
D. Context Management Infrastructure
Answer: D (LEAVE A REPLY)

NEW QUESTION: 31
After kernel debug with "fw ctl debug" you received a huge amount of information It was saved in a very large file that is difficult to open and analyze with standard text editors Suggest a solution to solve this issue.
A. Use Check Point InfoView utility to analyze debug output
B. Reduce debug buffer to 1024KB and run debug for several times
C. Divide debug information into smaller files Use "fw ctl kdebug -f -o "filename" -m 25 - s "1024"
D. Use "fw ctl zdebug' because of 1024KB buffer size
Answer: B (LEAVE A REPLY)

NEW QUESTION: 32
What table does command "fwaccel conns" pull information from?
A. SecureXLCon
B. fwxl_conns
C. cphwd_db
D. sxl_connections
Answer: B (LEAVE A REPLY)

NEW QUESTION: 33
What components make up the Context Management Infrastructure?
A. CMI Loader and Pattern Matcher
B. CPX and FWM
C. CPMI and FW Loader
D. CPM and SOLR
Answer: A (LEAVE A REPLY)

NEW QUESTION: 34
VPN's allow traffic to pass through the Internet securely byencryptingthe traffic as it enters the VPN tunnel and then decrypting the exists. Which process is responsible for Mobile VPN connections?
A. vpnd

B. cvpnd
C. fwk
D. vpnk
Answer: D (LEAVE A REPLY)

NEW QUESTION: 35
What acceleration mode utilizes multi-core processing to assist with traffic processing?
A. Traffic Warping
B. CoreXL
C. HyperThreading
D. SecureXL
Answer: (SHOW ANSWER)

NEW QUESTION: 36
You are running R80.XX on an open server and you see a high CPU utilization on your 12 CPU cores You now want to enable Hyperthreading to get more cores to gain some performance. What is the correct way to achieve this?
A. just turn on HAT in the bios of the server and after it has booted enable it in cpconfig
B. in dish run set HAT on
C. Hyperthreading is not supported on open servers, on on Check Point Appliances
D. just turn on HAT in the bios of the server and boot it
Answer: B (LEAVE A REPLY)

NEW QUESTION: 37
If you run the command "fw monitor -e accept src=10.1.1.201 or src=172.21.101.10 or src=192.0.2.10;" from the cli sh What will be captured?
A. Only packet going to 192.0.2.10
B. fw monitor only works in expert mode so no packets will be captured
C. Packets from 10 1 1 201 going to 192.0 2.10
D. Packets destined to 172 21 101 10 from 10.1.1.101
Answer: A (LEAVE A REPLY)

NEW QUESTION: 38
Which of the following is contained in the System Domain of the Postgres database?
A. User modified configurations such as network objects
B. Saved queries for applications
C. Configuration data of log servers
D. Trusted GUI clients
Answer: (SHOW ANSWER)

NEW QUESTION: 39
How can you increase the ring buffer size to 1024 descriptors?

A. dbedit>modify properties firewall_properties rx_ringsize 1024
B. fw ctl int rx_ringsize 1024
C. echo rx_ringsize=1024>>/etc/sysconfig/sysctl.conf
D. set interface eth0 rx-ringsize 1024
Answer: (SHOW ANSWER)

NEW QUESTION: 40
What is the benefit of running "vpn debug trunc over "vpn debug on"?
A. "vpn debug trunc*truncates the capture hence the output contains minimal capture
B. No advantage one over the other
C. "vpn debug trunc" purges ike.elg and vpnd elg and creates limestarnp while starting ike debug and vpn debug
D. "vpn debug trunc* provides verbose capture
Answer: C (LEAVE A REPLY)

NEW QUESTION: 41
Which situation triggers an IPS bypass under load on a 24-core Check Point appliance?
A. all CPU core most be above the threshold for more than 10 seconds
B. a single CPU core must be above the threshold for more than 10 seconds, but is must be the same core during this time
C. the average cpu utilization over all cores must be above the threshold for 1 second
D. any of the CPU cores is above the threshold for more than 10 seconds
Answer: (SHOW ANSWER)

NEW QUESTION: 42
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 $FWDIR/log/fw.elg
B. Messages are written to /etc/dmesg file
C. Messages are written to console and also /var/log/messages file
D. Messages are written to a buffer and collected using 'fw ctl kdebug'
Answer: C (LEAVE A REPLY)

NEW QUESTION: 43
Which process is responsible for the generation of certificates?
A. fwm
B. cpm
C. dbsync
D. cpca
Answer: D (LEAVE A REPLY)

NEW QUESTION: 44

The two procedures available for debugging in the firewall kernel are
i fw ctl zdebug
ii fw ctl debug/kdebug
Choose the correct statement explaining the differences in the two
A. (i) is used to debug only issues related to dropping of traffic, however (n) can be used for any firewall issue including NATing, clustering etc.
B. (i) Is used for general debugging, has a small buffer and is a quick way to set kernel debug flags to get an output via command line whereas (11) is useful when there is a need for detailed debugging and requires additional steps to set the buffer and get an output via command line
C. (i) is used to debug the access control policy only, however (n) can be used to debug a unified policy
D. (i) is used on a Security Gateway, whereas (11) is used on a Security Management Server
Answer: A (LEAVE A REPLY)

NEW QUESTION: 45
What process is responsible for sending and receiving logs in the management server?
A. CPD
B. CPM
C. FWM
D. FWD
Answer: (SHOW ANSWER)

NEW QUESTION: 46
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. CPview
C. CPstat
D. fwstat
Answer: (SHOW ANSWER)

NEW QUESTION: 47
To check the current status of hyper-threading, which command would you execute in expert mode?
A. cat /proc/smt_stat
B. cat /proc/hypert_status

C. cat /proc/smt_status
D. cat /proc/hypert_stat
Answer: C (LEAVE A REPLY)

NEW QUESTION: 48
You are running R80.XX on an open server and you see a high CPU utilization on your 12 CPU cores You now want to enable Hyperthreading to get more cores to gain some performance. What is the correct way to achieve this?
A. just turn on HAT in the bios of the server and boot it
B. just turn on HAT in the bios of the server and after it has booted enable it in cpconfig
C. in dish run set HAT on
D. Hyperthreading is not supported on open servers, on on Check Point Appliances
Answer: D (LEAVE A REPLY)

NEW QUESTION: 49
What are the main components of Check Point's Security Management architecture?
A. Management server Log server, Gateway server. Security server
B. Management server, Security Gateway. Multi-Domain Server, SmartEvent Server
C. Management server management database, log server, automation server
D. Management Server. Log Server. LDAP Server, Web Server
Answer: B (LEAVE A REPLY)