Number: 156-586
Passing Score: 800
Time Limit: 120
File Version: 2.0

Exam Code: 156-586

Exam Name: Check Point Certified Troubleshooting Expert - R81

Exam A

QUESTION 1
Where do you enable log indexing on the SMS?

A. SMS object under 'Other'
B. SMS object under 'Advanced'
C. SMS object under 'Logs'
D. SMS object under 'General Properties'

Correct Answer: C
Section:

QUESTION 2
What is the correct syntax to turn a VPN debug on and create new empty debug files?

A. vpn debuq trunkon
B. vpn debug truncon
C. vpndebug trunc on
D. vpn kdebug on

Correct Answer: B
Section:

QUESTION 3
Which of the following file is commonly associated with troubleshooting crashes on a system such as the Security Gateway?

A. fw monitor
B. CPMIL dump
C. core dump
D. tcpdump

Correct Answer: C
Section:

QUESTION 4
What is the best way to resolve an issue caused by a frozen process?

A. Kill the process
B. Restart the process
C. Reboot the machine
D. Power off the machine

Correct Answer: C

Section:

QUESTION 5
What is the Security Gateway directory where an administrator can find vpn debug log files generated during Site-to-Site VPN troubleshooting?

A. /opt/CPsuiteR80/vpn/log/
B. $FWDIR/conf/
C. $FWDIR/log/
D. $CPDIR/conf/

Correct Answer: C
Section:

QUESTION 6
In Mobile Access VPN, clientless access is done using a web browser. The primary communication path for these browser based connections is a process that allows numerous processes to utilize port 443 and redirects traffic to a designated port of the respective process. Which daemon handles this?

A. Mobile Access Daemon (MAD)
B. Connectra VPN Daemon (cvpnd)
C. HTTPS Inspection Daemon (HID)
D. Multi-portal Daemon

Correct Answer: D
Section:

QUESTION 7
SmartEvent utilizes the Log Server, Correlation Unit and SmartEvent Server to aggregate logs and identify security events. The three main processes that govern these SmartEvent components are:

A. cpcu, cplog, cpse
B. eventiasv, eventiarp,eventiacu
C. cpsemd, cpsead, and DBSync
D. fwd, secu, sesrv

Correct Answer: C
Section:

QUESTION 8
Which of these packet processing components stores Rule Base matching state-related information?

A. Observers
B. Classifiers
C. Manager
D. Handlers

Correct Answer: D
Section:

QUESTION 9
That is the proper command for allowing the system to create core files?

A. $FWDIR/scripts/core-dump-enable.sh
B. # set core-dump enable # save config
C. > set core-dump enable > save config
D. service core-dump start

Correct Answer: C
Section:

QUESTION 10
What is correct about the Resource Advisor (RAD) service on the Security Gateways?

A. RAD functions completely in user space. The Pattern Matter (PM) module of the CMI looks up for URLs in the cache and if not found, contact the RAD process in user space to do online categorization
B. RAD is completely loaded as a kernel module that looks up URL in cache and if not found connects online for categorization. There is no user space involvement in this process
C. RAD is not a separate module, it is an integrated function of the W kernel module and does all operations in the kernel space
D. RAD has a kernel module that looks up the kernel cache, notifies client about hits and misses and forwards a-sync requests to RAD user space module which is responsible for online categorization

Correct Answer: D
Section:

QUESTION 11
Which of the following is contained in the System Domain of the Postgres database?

A. Trusted GUI clients
B. Configuration data of log servers
C. Saved queries for applications
D. User modified configurations such as network objects

Correct Answer: A
Section:

QUESTION 12
Where will the usermode core files located?

A. /var/log/dump/usermode
B. $CPDIR/var/log/dump/usermode
C. $FWDIR/var/log/dump/usermode
D. /var/suroot

Correct Answer: A
Section:

QUESTION 13
The Check Point Watch Daemon (CPWD) monitors critical Check Point processes, terminating them or restarting them as needed to maintain consistent, stable operating conditions. When checking the status/output of CPWD you are able to see some columns like APP, PID, STAT, START, etc. What is the column 'STAT' used for?

A. Shows the Watch Dog name of the monitored process
B. Shows the status of the monitored process
C. Shows how many times the Watch Dog started the monitored process
D. Shows what monitoring method Watch Dog is using to track the process

Correct Answer: B
Section:

QUESTION 14
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

Correct Answer: D
Section:

QUESTION 15
During firewall kernel debug with fw ctl zdebug you received less information that expected. You noticed that a lot of messages were lost since the time the debug was started. What should you do to resolve this issue?

A. Increase debug buffer; Use fw ctl debug -buf 32768
B. Redirect debug output to file; Use fw ctl debug -o ./debug.elg
C. Redirect debug output to file; Use fw ctl zdebug -o ./debug.elg
D. Increase debug buffer; Use fw ctl zdebug -buf 32768

Correct Answer: A
Section:

QUESTION 16
Check Point Access Control Daemons contains several daemons for Software Blades and features. Which Daemon is used for Application & Control URL Filtering?

A. cprac
B. rad
C. pepd
D. pdpd

Correct Answer: D
Section:

QUESTION 17
What is the name of the VPN kernel process?

A. FWK
B. VPND

C. CVPND
D. VPNK

Correct Answer: C
Section:

QUESTION 18
What version of Check Point can Security Gateways begin dynamically distributing Logs between log servers?

A. R81
B. R77
C. R30
D. R75

Correct Answer: A
Section:

QUESTION 19
In some scenarios it is very helpful to use advanced Linux commands for troubleshooting purposes. Which command displays information about resource utilization for running processes and shows additional information for core utilization and memory?

A. top
B. vmstat
C. cptop
D. mpstat

Correct Answer: A
Section:

QUESTION 20
What is the port for the Log Collection on Security Management Server?

A. 253
B. 443
C. 18191
D. 257

Correct Answer: D
Section:

QUESTION 21
Troubleshooting issues with Mobile Access requires the following:

A. Standard VPN debugs and packet captures on Security Gateway, debugs of 'cvpnd' process on Security Management
B. Debug logs of FWD captured with the command - 'fw debug fwd on TDERROR_MOBILE_ACCESS=5'
C. 'ma_vpnd' process on Security Gateway
D. Standard VPN debugs, packet captures, and debugs of 'cvpnd' process on Security Gateway

Correct Answer: C
Section:

QUESTION 22
What command is used to find out which port Multi-Portal has assigned to the Mobile Access Portal?

A. mpclient getdata sslvpn
B. netstat getdata sslvpn
C. netstat -nap | grep mobile
D. mpclient getdata mobi

Correct Answer: A
Section:

QUESTION 23
What command(s) will turn off all vpn debug collection?

A. fw ctl debug 0
B. vpn debug -a off
C. vpn debug off
D. vpn debug off and vpn debug ikeoff

Correct Answer: D
Section:

QUESTION 24
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. CPview
B. cpstat
C. fwstat
D. CPstat

Correct Answer: B
Section:

QUESTION 25
The Check Point Firewall Kernel is the core component of the Gaia operating system and an integral part of traffic inspection process. There are two procedures available for debugging the firewall kernel. Which procedure/command is used for detailed troubleshooting and needs more resources?

A. fw debug/kdebug
B. fw ctl zdebug
C. fw debug/kdebug ctl
D. fw ctl debug/kdebug

Correct Answer: D

Section:

QUESTION 26
PostgreSQL is a powerful, open source relational database management system. Check Point offers a command for viewing the database to interact with Postgres interactive shell. Which command do you need to enter the PostgreSQL interactive shell?

A. mysql_client cpm postgres
B. mysql -u root
C. psql_client cpm postgres
D. psql_client postgres cpm

Correct Answer: C
Section:

QUESTION 27
What information does the doctor-log script supply?

A. Logging errors. Exceptions, Repair options
B. Current and daily average logging rates. Indexing status, Size
C. Logging rates. Logging Directories, List of troubleshooting tips
D. Repair options. Logging Rates, Logging Directories

Correct Answer: B
Section:

QUESTION 28
If SmartLog is not active or failed to parse results from server, what commands can be run to re-enable the service?

A. smartlogrestart and smartlogstart
B. smartlogstart and smartlogstop
C. smartloginit and smartlogstop
D. smartlogstart and smartlogsetup

Correct Answer: B
Section: