Check Point Certified Troubleshooting Expert

1. Which of these packet processing components stores Rule Base matching state-related information?

A. Observers

B. Classifiers

C. Manager

D. Handlers

Answer(s): D

---

2. 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

Answer(s): C

---

3. 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

Answer(s): D

---

4. 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

Answer(s): A

---

5. 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

Answer(s): A

---

6. 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

Answer(s): B

---

7. 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(s): D

---

8. When viewing data for CPMI objects in the Postgres database, what table column should be selected to query for the object instance?

A. CpmiHostCkp

B. fwset

C. CPM Global M

D. GuiDBedit

Answer(s): B

---

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

B. fwm manaqes this database after initialization of the 1CA

C. solr is a child process of cpm

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

Answer(s): C

---

10. 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

Answer(s): C

---

11. 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/

Answer(s): C

---

12. 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

Answer(s): D

---

13. 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

Answer(s): C

---

14. 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

Answer(s): A

---

15. 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

Answer(s): D

---

16. What is the name of the VPN kernel process?

A. FWK

B. VPND

C. CVPND

D. VPNK

Answer(s): C

---

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

A. R81

B. R77

C. R30

D. R75

Answer(s): A

---

18. 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

Answer(s): A

19. What is the port for the Log Collection on Security Management Server?

A. 253

B. 443

C. 18191

D. 257

Answer(s): D

20. 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

Answer(s): C