Checkpoint156-587.by.Zodo.35q

Number: 156-587
Passing Score: 800
Time Limit: 120
File Version: 5.0

Exam Code: 156-587

Exam Name: Check Point Certified Troubleshooting Expert - R81.20

Exam A

QUESTION 1
User defined URLS and HTTPS inspection User defined URLs on the Security Gateway are stored in which database file?

A. https_urif.bin
B. urlf db.bin
C. urtf_https.bin
D. https_db.bin

Correct Answer: B
Section:

QUESTION 2
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. Multi-portal Daemon (MPD)
B. Mobile Access Daemon (MAD)
C. HTTPS Inspection Daemon (HID)
D. Connectra VPN Daemon (cvpnd)

Correct Answer: A
Section:
Explanation:
The Multi-portal Daemon (mpdaemon) is responsible for handling the clientless access connections in Mobile Access VPN. It listens on port 443 and redirects the traffic to the appropriate port of the process that handles the specific connection type, such as cvpnd for SSL Network Extender, MAD for Mobile Access Portal, or HID for HTTPS Inspection. The mpdaemon also performs authentication and authorization for the clientless access connections.
Reference: Check Point Processes and Daemons1, Mobile Access Blade Administration Guide
1: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk97638 :
https://sc1.checkpoint.com/documents/R81.10/WebAdminGuides/EN/CP_R81.10_Mobile_Access_AdminGuide/html_frameset.htm

QUESTION 3
What command is used to find out which port Multi-Portal has assigned to the Mobile Access Portal?

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

Correct Answer: A
Section:

QUESTION 4
How does Identity Collector connect to Windows Server?

A. ADQuery is needed for connection
B. LDAP connection
C. It uses a PDP demon to connect
D. via Windows API

Correct Answer: D
Section:

QUESTION 5
You run a free-command on a gateway and notice that the Swap column is not zero Choose the best answer

A. Utilization of ram is high and swap file had to be used
B. Swap file is used regularly because RAM memory is reserved for management traffic
C. Swap memory is used for heavy connections when RAM memory is full
D. Its ole Swap is used to increase performance

Correct Answer: A
Section:

QUESTION 6
You modified kernel parameters and after rebooting the gateway, a lot of production traffic gets dropped and the gateway acts strangely What should you do'?

A. Run command fw ctl set int fw1_kernel_all_disable=1
B. Restore fwkem.conf from backup and reboot the gateway
C. run fw unloadlocal to remove parameters from kernel
D. Remove all kernel parameters from fwkem.conf and reboot

Correct Answer: B
Section:
Explanation:
If you have modified kernel parameters (in fwkern.conf, for example) and the gateway starts dropping traffic or behaving abnormally after a reboot, the best practice is to restore the original or a known-good configuration from backup. Then, reboot again so that the gateway loads the last known stable settings.
Option A (fw ctl set int fw1_kernel_all_disable=1) is not a standard or documented method for ''undoing'' all kernel tweaks.
Option B (Restore fwkem.conf from backup and reboot the gateway) is the correct and straightforward approach.
Option C (fw unloadlocal) removes the local policy but does not revert custom kernel parameters that have already been loaded at boot.
Option D (Remove all kernel parameters from fwkem.conf and reboot) might help in some cases, but you risk losing other beneficial or necessary parameters if there were legitimate custom settings. Restoring from a known-good backup is safer and more precise.
Hence, the best answer: ''Restore fwkem.conf from backup and reboot the gateway.''
Check Point Troubleshooting Reference
sk98339 -- Working with fwkern.conf (kernel parameters) in Gaia OS.
sk92739 -- Advanced System Tuning in Gaia OS.
Check Point Gaia Administration Guide -- Section on kernel parameters and system tuning.
Check Point CLI Reference Guide -- Explanation of using fw ctl, fw unloadlocal, and relevant troubleshooting commands.

QUESTION 7
What process monitors terminates, and restarts critical Check Point processes as necessary?

A. CPM

B. FWD

C. CPWD

D. FWM

Correct Answer: C
Section:
Explanation:
CPWD (Check Point WatchDog) is the process that monitors, terminates (if necessary), and restarts critical Check Point processes (e.g., FWD, FWM, CPM) when they stop responding or crash.
CPM (Check Point Management process) is a process on the Management Server responsible for the web-based SmartConsole connections, policy installations, etc.
FWD (Firewall Daemon) handles logging and communication functions in the Security Gateway.
FWM (FireWall Management) is an older reference to the management process on the Management Server for older versions.
Therefore, the best answer is CPWD.
Check Point Troubleshooting Reference
sk97638: Check Point WatchDog (CPWD) process explanation and commands.
R81.20 Administration Guide -- Section on CoreXL, Daemons, and CPWD usage.
sk105217: Best Practices -- Explains system processes, how to monitor them, and how CPWD is utilized.

QUESTION 8
What is the best way to resolve an issue caused by a frozen process?

A. Power off the machine

B. Restart the process

C. Reboot the machine

D. Kill the process

Correct Answer: D
Section:
Explanation:
When a process is frozen (hung or unresponsive), the typical method to resolve it is to kill the process. On Check Point, you can use cpwd_admin kill -name <ProcessName> or a standard Linux kill -9 <PID> command if necessary. You then allow CPWD (the Check Point watchdog) to restart it, or manually restart it if needed.
Other options:
A . Power off the machine: This is too drastic and not recommended just for a single frozen process.
B . Restart the process: While this sounds viable, you typically must kill the frozen process first, then let WatchDog or an admin restart it.
C . Reboot the machine: Similar to powering off---too disruptive for just one stuck process.
Hence, the most direct and standard approach: ''Kill the process.''
Check Point Troubleshooting Reference
sk97638 -- Explanation of CPWD (Check Point WatchDog) and how to manage processes.
sk43807 -- How to gracefully stop or kill a Check Point process.
Check Point CLI Reference Guide -- Details on using cpwd_admin commands to kill or restart processes.

QUESTION 9
Which of the following file is commonly associated with troubleshooting crashes on a system such as the Security Gateway?

A. tcpdump

B. core dump

C. fw monitor

D. CPMIL dump

Correct Answer: B
Section:
Explanation:
When troubleshooting crashes on a Security Gateway (or any Linux-based system), the file type that is typically generated and used for in-depth analysis is a core dump.
A core dump captures the memory state of a process at the time it crashed and is critical for root-cause analysis.
Other options:
A . tcpdump: A packet capture file, not a crash-related file.
C . fw monitor: A Check Point packet capture tool, but not for crash debugging.
D . CPMIL dump: Not a common or standard crash dump reference in Check Point.

QUESTION 10
When a User Mode process suddenly crashes, it may create a core dump file. Which of the following information is available in the core dump and may be used to identify the root cause of the crash?
i. Program Counter
ii. Stack Pointer
iii. Memory management information
iv. Other Processor and OS flags / information

A. iii and iv only
B. i and ii only
C. i, ii, iii and iv
D. Only Iii

Correct Answer: C
Section:
Explanation:
A core dump file is essentially a snapshot of the process's memory at the time of the crash. This snapshot includes crucial information that can help diagnose the cause of the crash. Here's why all the options are relevant:
i. Program Counter: This register stores the address of the next instruction the CPU was supposed to execute. It pinpoints exactly where in the code the crash occurred.
ii. Stack Pointer: This register points to the top of the call stack, which shows the sequence of function calls that led to the crash. This helps trace the program's execution flow before the crash.
iii. Memory management information: This includes details about the process's memory allocations, which can reveal issues like memory leaks or invalid memory access attempts.
iv. Other Processor and OS flags/information: This encompasses various registers and system information that provide context about the state of the processor and operating system at the time of the crash.
By analyzing this information within the core dump, you can often identify the root cause of the crash, such as a segmentation fault, null pointer dereference, or stack overflow.
Check Point Troubleshooting
Reference:
While core dumps are a general concept in operating systems, Check Point's documentation touches upon them in the context of troubleshooting specific processes like fwd (firewall) or cpd (Check Point daemon). The fw ctl zdebug command, for example, can be used to trigger a core dump of the fwd process for debugging purposes.

QUESTION 11
Where will the usermode core files located?

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

Correct Answer: D
Section:
Explanation:
Usermode core files are generated when a user mode process crashes. They are located in the $CPDIR/var/log/dump/usermode directory on the Security Gateway or Security Management server. The core files can be used to analyze the cause of the crash and troubleshoot the issue. The core files are named according to the process name, date, and time of the crash. For example, cpd_2023_02_03_16_40_55.core is a core file for the cpd process

that crashed on February 3, 2023 at 16:40:55

QUESTION 12
What is the function of the Core Dump Manager utility?

A. To determine which process is slowing down the system
B. To send crash information to an external analyzer
C. To limit the number of core dump files per process as well as the total amount of disk space used by core files
D. To generate a new core dump for analysis

Correct Answer: C
Section:
Explanation:
The Core Dump Manager (CDM) is a utility that helps manage core dump files on Check Point systems. Its main functions include:
Limiting file size and number: CDM can be configured to limit the size of individual core dump files and the total amount of disk space used for core dumps. This prevents core dumps from filling up valuable disk space.
Compression: CDM can compress core dump files to reduce their storage size. This is particularly helpful when dealing with large core dumps.
Process filtering: CDM allows you to specify which processes should be allowed to generate core dumps. This can help prevent unnecessary core dumps from being created.
Remote collection: CDM can be configured to send core dump files to a remote server for analysis. This is useful in environments where direct access to the system generating the core dump is limited.
By using CDM, you can effectively manage core dump files and ensure that they are not overwhelming your system's resources.

QUESTION 13
What is the proper command for allowing the system to create core files?

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

Correct Answer: C
Section:

QUESTION 14
When a user space process or program suddenly crashes, what type of file is created for analysis

A. core dump
B. kernel_memory_dump dbg
C. core analyzer
D. coredebug

Correct Answer: A
Section:
Explanation:
When a user space process crashes unexpectedly, the operating system often creates a core dump file. This file is a snapshot of the process's memory at the time of the crash, including information such as:
Program counter: This indicates where the program was executing when it crashed.
Stack pointer: This shows the function call stack, which can help trace the sequence of events leading to the crash.
Memory contents: This includes the values of variables and data structures used by the process.
Register values: This shows the state of the processor registers at the time of the crash.
Core dump files can be analyzed using debuggers like GDB to understand the cause of the crash.

Why other options are incorrect:
B . kernel_memory_dump dbg: This refers to a kernel memory dump, which is generated when the operating system kernel itself crashes.
C . core analyzer: This is a tool used to analyze core dump files, not the file itself.
D . coredebug: This is not a standard term for any type of crash dump file.
Check Point Troubleshooting
Reference:
Check Point's documentation mentions core dumps in the context of troubleshooting various processes, such as fwd (firewall) and cpd (Check Point daemon). You can find information on enabling core dumps and analyzing them in the Check Point administration guides and knowledge base articles.

QUESTION 15
You receive reports from multiple users that they cannot browse Upon further discovery you identify that Identity Awareness cannot identify the users properly and apply the configuredAccess Roles
What commands you can use to troubleshoot all identity collectors and identity providers from the command line?

A. on the gateway: pdp debug set IDC all IDP all
B. on the gateway: pdp debug set AD all and IDC all
C. on the management: pdp debug on IDC all
D. on the management: pdp debug set all

Correct Answer: A
Section:
Explanation:
To troubleshoot Identity Awareness issues related to user identification and Access Role application, you need to enable debugging for both Identity Collectors (IDC) and Identity Providers (IDP). The command pdp debug set IDC all IDP all on the gateway achieves this.
Here's why this is the correct answer and why the others are not:
A . on the gateway: pdp debug set IDC all IDP all: This correctly enables debugging for all Identity Collectors and Identity Providers, allowing you to see detailed logs and messages related to user identification and Access Role assignment. This helps pinpoint issues with user mapping, authentication, or authorization.
B . on the gateway: pdp debug set AD all and IDC all: This command only enables debugging for Active Directory (AD) as an Identity Provider and all Identity Collectors. It might miss issues related to other Identity Providers if they are in use.
C . on the management: pdp debug on IDC all: This command has two issues. First, it should be executed on the gateway, not the management server, as the gateway is responsible for user identification and policy enforcement. Second, it only enables debugging for Identity Collectors, not Identity Providers.
D . on the management: pdp debug set all: While this command might seem to enable debugging for everything, it's not specific enough for Identity Awareness troubleshooting. It might generate excessive logs unrelated to the issue and make it harder to find the relevant information.
Check Point Troubleshooting
Reference:
Check Point Identity Awareness Administration Guide: This guide provides detailed information about Identity Awareness components, configuration, and troubleshooting.
Check Point sk113963: This article explains how to troubleshoot Identity Awareness issues using debug commands and logs.
Check Point R81.20 Security Administration Guide: This guide covers general troubleshooting and debugging techniques, including the use of pdp debug commands.

QUESTION 16
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 clish?

A. set core-dump enable
B. set core-dump total
C. set user-dump enable
D. set core-dump per_process

Correct Answer: A
Section:
Explanation:

In Check Point Gaia, you can enable core dumping through the command line interface (clish) using the following command:
set core-dump enable
This command activates the core dump mechanism, allowing the system to generate core dump files when user processes crash. Remember to save the configuration after enabling core dumps with the command:
save config
Why other options are incorrect:
B . set core-dump total: This command is used to set the total disk space limit for core dump files, not to enable core dumping itself.
C . set user-dump enable: There is no such command in Gaia clish for enabling core dumps.
D . set core-dump per_process: This command sets the maximum number of core dump files allowed per process, but it doesn't enable core dumping.
Check Point Troubleshooting
Reference:
Check Point R81.20 Security Administration Guide: This guide provides comprehensive information about Gaia clish commands, including those related to system configuration and troubleshooting.
Check Point sk92764: This knowledge base article specifically addresses core dump management in Gaia, explaining how to enable and configure core dumps.
Enabling core dumps is a crucial step in troubleshooting process crashes as it provides valuable information for analysis and debugging.

QUESTION 17
The Unified Access Control policy eliminates the need to maintain policies for different access control features However, you need to start a general debug of the Unified Policy with all flags turned on Which of the following is the correct syntax?

A. fw ctl debug -m UP all
B. fw ctl debug -m UP + all flags
C. fw ctl kdebug -m UP all
D. fwm ctl debug -m UP all

Correct Answer: A
Section:

QUESTION 18
What function receives the AD log event information?

A. FWD
B. CPD
C. PEP
D. ADLOG

Correct Answer: D
Section:

QUESTION 19
You receive complains that Guest Users cannot login and use the Guest Network which is configured with Access Role of Guest Users. You need to verity the Captive Portal configuration. Where can you find the config file?

A. on the gateway at $NACPORTAL_ HOME/conf/httpd_ nac.conf
B. on the management at SCPNAC_ HOME/conf/httpd_ nac.conf
C. on the management at SNACPORTAL_ HOME/conf/httpd_ nac.conf
D. on the gateway at $CPNAC_ HOME/conf/httpd_ nac.conf

Correct Answer: A
Section:

QUESTION 20
What are the three main component of Identity Awareness?

A. Client, SMS and Secure Gateway
B. Identity Source Identity Server (POP) and Identity Enforcement (PEP)
C. Identity Awareness Blade on Security Gateway, User Database on Security Management Server and Active Directory
D. User, Active Directory and Access Role

Correct Answer: B
Section:

QUESTION 21
Captive Portal, PDP and PEP run in what space?

A. User
B. CPM
C. FWD
D. Kernel

Correct Answer: A
Section:

QUESTION 22
Which of these packet processing components stores Rule Base matching state-related information?

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

Correct Answer: A
Section:
Explanation:
The Terraform Registry allows any user to publish and share modules. Published modules support versioning, automatically generate documentation, allow browsing version histories, show examples and READMEs, and more. Public modules are managed via Git and GitHub, and publishing a module takes only a few minutes. Once a module is published, releasing a new version of a module is as simple as pushing a properly formed Git tag1.
Reference = The information can be verified from the Terraform Registry documentation on Publishing Modules provided by HashiCorp Developer1.

QUESTION 23
What is the correct syntax to turn a VPN debug on and create new empty debug files'?

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

Correct Answer: B
Section:

QUESTION 24
What cli command is run on the GW to verify communication to the identity Collector?

A. pdp connections idc
B. pep connections idc
C. show idc connections
D. fwd connected

Correct Answer: A
Section:

QUESTION 25
You are using the identity Collector with identity Awareness in large environment. Users report that they cannot access resources on Internet You identify that the traffic is matching the cleanup rule Instead of the proper rule with Access Roles using the IDC How can you check if IDC is working?

A. pdp connections idc
B. ad query I debug on
C. pep debug idc on
D. pdp debug set IDP all

Correct Answer: A
Section:

QUESTION 26
For identity Awareness what is the PDP process?

A. Identity server
B. Captive Portal Service
C. User Auth Database
D. Log Sifter

Correct Answer: A
Section:

QUESTION 27
What command(s) will turn off all vpn debug collection?

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

Correct Answer: D
Section:

QUESTION 28
Like a Site-to-Site VPN between two Security Gateways, a Remote Access VPN relies on the Internet Key Exchange (IKE) what types of keys are generated by IKE during negotiation?

A. Produce a symmetric key on both sides
B. Produce an asymmetric key on both sides
C. Symmetric keys based on pre-shared secret
D. Produce a pair of public and private keys

Correct Answer: D
Section:

QUESTION 29
You were asked by security team to debug Mobile Access VPN. What processes will you debug?

A. HTTPD and CPVND
B. IKED
C. VPND and IKED
D. SNX daemon

Correct Answer: A
Section:

QUESTION 30
Which of the following daemons is used for Threat Extraction?

A. extractd
B. tedex
C. tex
D. scrubd

Correct Answer: A
Section:

QUESTION 31
What is the name of the VPN kernel process?

A. VPND
B. CVPND
C. FWK
D. VPNK

Correct Answer: C
Section:

QUESTION 32
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. Reduce debug buffer to 1024KB and run debug for several times
B. Use Check Point InfoView utility to analyze debug output

C. Use "fw ctl zdebug because of 1024KB buffer size

D. Divide debug information into smaller files. Use " fw ctl kdebug -f -o "filename -m 25 - s "1024"

Correct Answer: D
Section:

QUESTION 33
Troubleshooting issues with Mobile Access requires the following:

A. 'ma_vpnd' process on Security Gateway

B. Debug logs of FWD captured with the command - 'fw debug fwd on TDERROR_MOBILE_ACCESS=5'

C. Standard VPN debugs, packet captures and debugs of cvpnd1 process on Security Gateway

D. Standard VPN debugs and packet captures on Security Gateway, debugs of 'cvpnd' process on Security Management

Correct Answer: C
Section:

QUESTION 34
Your users have some issues connecting with Mobile Access VPN to your gateway. How can you debug the tunnel establishment?

A. run vpn debug truncon

B. in the file $VPNDIR/conf/httpd conf change the line Loglevel To LogLevel debug and run vpn restart

C. in the file SCVPNDIR/conf/httpd conf change the line Loglevel To LogLevel debug and run cvpnrestart

D. run fw ctl zdebug -m sslvpn all

Correct Answer: C
Section:

QUESTION 35
What is the most efficient way to read an IKEv2 Debug?

A. IKEview

B. vi on the cti

C. notepad++

D. any xml editor

Correct Answer: A
Section: