



Vendor: Check Point

Exam Code: 156-587

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

Version: DEMO

QUESTION 1

What Check Point process controls logging?

- A. FWD
- B. CPVVD
- C. CPM
- D. CPD

Answer: A

Explanation:

FWD (Firewall Daemon) is the wrapper for the fw_full process and is responsible for logging. It is also responsible for logging and spawning child processes).

QUESTION 2

Which of the following daemons is used for Threat Extraction?

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

Answer: D

Explanation:

The scrubd daemon is responsible for the Check Point Threat Extraction process. It handles the sanitization of files by removing potentially malicious content or replacing the original file with a safe, scrubbed version.

QUESTION 3

If the cpsemd process of SmartEvent has crashed or is having trouble coming up, then it usually indicates that _____.

- A. The SmartEvent core on the Solr indexer has been deleted
- B. The logged in administrator does not have permissions to run SmartEvent
- C. Postgres database is down
- D. Cpd daemon is unable to connect to the log server

Answer: C

QUESTION 4

Your users are having trouble opening a Web page and you need to troubleshoot it. You open the Smart Console, and you get the following message when you navigate to the Logs and Monitor "SmartLog is not active or Failed to parse results from server". What is the first thing you can try to resolve it?

- A. Run the commands on the SMS: smartlogstart and smartlogstop
- B. smartlog debug on and smartlog debug off
- C. smartlog_server restart
- D. cpmstop and cpmstart

Answer: A

Explanation:

The error indicates the SmartLog indexing service on the Security Management Server (SMS) is not running or is stuck.

Restarting SmartLog with smartlogstop; smartlogstart on the SMS is the recommended initial action before trying deeper service or CPM restarts.

QUESTION 5

You do not see logs in the SMS. When you login on the SMS shell and run cpwd_admin list you notice that the RFL process is with status T. What command can you run to try to resolve it?

- A. RFLstop and RFLstart
- B. evstart and evstop
- C. smartlog_server stop and smartlog_server restart
- D. rflsop and rflstart

Answer: B

Explanation:

The RFL process is related to Eventia/SmartEvent log correlation on the Security Management Server, and a status of T in cpwd_admin list indicates it is terminated or not running correctly.

The recommended action in this scenario is to restart the SmartEvent services using the commands evstop and evstart on the SMS to bring RFL back to a healthy state.

QUESTION 6

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"

Answer: C

QUESTION 7

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

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

Answer: B

QUESTION 8

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

Answer: C

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.

QUESTION 9

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 per process
- C. set user-dump enable
- D. set core-dump total

Answer: A

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
```

QUESTION 10

The management configuration stored in the Postgres database is partitioned into several relational database domains. What is the purpose of the Global Domain?

- A. Global Domains is used by the IPS software blade to map the IDs to the corresponding countries according to the IpToCountry.csv file.
- B. This domain is used as the global database to back up the objects referencing the corresponding object attributes from the System Domain.
- C. This domain is used as the global database to track the changes made by multiple administrators on the same objects prior to publishing.
- D. This domain is used as the global database for MDSM and contains global objects and policies.

Answer: D

QUESTION 11

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

- A. IKE view
- B. vi on the cl

- C. any xml editor
- D. notepad++

Answer: A

Explanation:

<https://support.checkpoint.com/results/sk/sk30994>

QUESTION 12

Which of the following is a component of the Context Management Infrastructure used to collect signatures in user space from multiple sources, such as Application Control and IPS, and compiles them together into unified Pattern Matchers?

- A. PSL - Passive Signature Loader
- B. cpas
- C. Context Loader
- D. CMI Loader

Answer: D

Explanation:

Policy installation is handled by FW process.

During policy installation, the CMI Loader collects signatures from multiple sources (e.g. IPS, CTNT, APPI, ...) and compiles them together into unified Pattern Matchers (PM) (one for each context - such as URL, Host header, etc.).

QUESTION 13

User defined URLs and HTTPS Inspection User defined URLs on the Security Gateway are stored in which database file?

- A. https_db.bin
- B. urlf_https.bin
- C. https_urlf.bin
- D. urlf_db.bin

Answer: D

QUESTION 14

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

- A. CPWD
- B. CPM
- C. FWM
- D. FWD

Answer: A

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.

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

- ★ More than **99,900** Satisfied Customers Worldwide.
- ★ Average **99.9%** Success Rate.
- ★ **Free Update** to match latest and real exam scenarios.
- ★ **Instant Download** Access! No Setup required.
- ★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.
- ★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.
- ★ **100%** Guaranteed Success or **100%** Money Back Guarantee.
- ★ **Fast**, helpful support **24x7**.



View list of all certification exams: <http://www.lead2pass.com/all-products.html>



Microsoft



ORACLE



JUNIPER
NETWORKS



EMC²
where information lives

10% Discount Coupon Code: ASTR14