156-587 Test Torrent - New 156-587 Test Cram

P.S. Free & New 156-587 dumps are available on Google Drive shared by It-Tests: https://drive.google.com/open?id=16jSw5S8jWfGJgEa3zLkfK_kEzfaKLMXf

Our website can offer you the latest CheckPoint pass guide and learning materials, which enable you pass 156-587 valid exam at your first attempt. Besides, there are 156-587 free braindumps that you can download to learn about our products. Once you decide to buy our test answers, you will be allowed to free update your 156-587 Top Dumps one-year.

CheckPoint 156-587 Exam Syllabus Topics:

Topic	Details
Topic 1	• Advanced Access Control Troubleshooting: This section of the exam measures the skills of Check Point System Administrators in demonstrating expertise in troubleshooting access control mechanisms. It involves understanding user permissions and resolving authentication issues.
Topic 2	• Advanced Firewall Kernel Debugging: This section of the exam measures the skills of Check Point Network Security Administrators and focuses on kernel-level debugging for firewalls. Candidates will learn how to analyze kernel logs and troubleshoot firewall-related issues at a deeper level.
Topic 3	• Introduction to Advanced Troubleshooting: This section of the exam measures the skills of Check Point Network Security Engineers and covers the foundational concepts of advanced troubleshooting techniques. It introduces candidates to various methodologies and approaches used to identify and resolve complex issues in network environments.
Topic 4	• Advanced Gateway Troubleshooting: This section of the exam measures the skills of Check Point Network Security Engineers and addresses troubleshooting techniques specific to gateways. It includes methods for diagnosing connectivity issues and optimizing gateway performance.
Topic 5	• Advanced Site-to-Site VPN Troubleshooting: This section of the exam measures the skills of Check Point System Administrators and covers troubleshooting site-to-site VPN connections.

Topic 6	- Advanced Client-to-Site VPN Troubleshooting: This section of the exam measures the skills of CheckPoint System Administrators and focuses on troubleshooting client-to-site VPN issues.
Topic 7	- Advanced Troubleshooting with Logs and Events: This section of the exam measures the skills of Check Point Security Administrators and covers the analysis of logs and events for troubleshooting. Candidates will learn how to interpret log data to identify issues and security threats effectively.

>> 156-587 Test Torrent <<

100% Pass CheckPoint - Accurate 156-587 - Check Point Certified Troubleshooting Expert - R81.20 Test Torrent

With our 156-587 practice test software, you can simply assess yourself by going through the 156-587 practice tests. We highly recommend going through the 156-587 answers multiple times so you can assess your preparation for the 156-587 exam. Make sure that you are preparing yourself for the 156-587 test with our practice test software as it will help you get a clear idea of the real 156-587 exam scenario. By passing the exams multiple times on practice test software, you will be able to pass the real 156-587 test in the first attempt.

CheckPoint Check Point Certified Troubleshooting Expert - R81.20 Sample Questions (Q108-Q113):

NEW QUESTION # 108
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. eventiasv, eventiarp,eventiacu
- B. fwd, secu, sesrv
- C. cpcu, cplog, cpse
- D. cpsemd, cpsead, and DBSync

Answer: A

Explanation:
SmartEvent is a unified security event management and analysis solution that collects and analyzes data from multiple sources to identify and respond to security threats. SmartEvent consists of three main components:
Log Server, Correlation Unit, and SmartEvent Server1. The three main processes that govern these SmartEvent components are:
* eventiasv: This process is responsible for indexing the logs received from the Log Server and storing them in the SmartEvent database. It also performs log consolidation and compression to optimize the disk space usage2.
* eventiarp: This process is responsible for running the predefined and custom correlation rules on the indexed logs and generating security events based on the rule criteria. It also sends notifications and triggers automatic responses for the security events3.
* eventiacu: This process is responsible for providing the web-based user interface for SmartEvent, which allows the administrators to view, analyze, and manage the security events. It also provides the SmartEvent API for external integration4. References: Check Point Processes and Daemons5, SmartEvent Administration Guide1
1: https://sc1.checkpoint.com/documents/R81.10/WebAdminGuides/EN/CP_R81.10_SmartEvent_AdminGuide/html_frameset.htm 2: https://sc1.checkpoint.com/documents/R81.10/WebAdminGuides/EN/CP_R81.10_SmartEvent_AdminGuide/Content/Topics-SmartEvent/SmartEvent-Components.htm#_Toc64167467 3: https://sc1.checkpoint.com/documents/R81.10/WebAdminGuides/EN/CP_R81.10_SmartEvent_AdminGuide/Content/Topics-SmartEvent/SmartEvent-Components.htm#_Toc64167468 4: https://sc1.checkpoint.com/documents/R81.10/WebAdminGuides/EN/CP_R81.10_SmartEvent_AdminGuide/Content/Topics-SmartEvent/SmartEvent-Components.htm#_Toc64167469 5: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk97638

NEW QUESTION # 109
What are the four main database domains?

- A. System. Global. Log. Event
- B. System, User, Host, Network
- C. System, User, Global. Log
- D. Local, Global, User, VPN

Answer: C

Explanation:
The four main database domains are System, User, Global, and Log. Each domain contains different types of data and serves different purposes123. The System domain contains the configuration data of the Security Management Server (SMS), such as the SMS name, IP address, licensing, and installed products. The User domain contains the configuration data of the security policy, such as the objects, rules, services, and VPN communities. The Global domain contains the configuration data of the global policy, such as the global objects, rules, and services. The Log domain contains the log data of the security events, such as the source, destination, action, and time of each event123. Reference:
1: CCTE Courseware, Module 3: Management Database and Processes, Slide 4
2: Check Point R81 Security Management Administration Guide, Chapter 2: Security Management Server, Page 14
3: Check Point R81 Security Management Administration Guide, Chapter 2: Security Management Server, Page 15

NEW QUESTION # 110
What is NOT a benefit of the 'fw ctl zdebug' command?

- A. Cannot be used to debug additional modules
- B. Clean the buffer
- C. Automatically allocate a 1MB buffer
- D. Collect debug messages from the kernel

Answer: A

Explanation:
The fw ctl zdebug command is a powerful tool that can be used to collect debug messages from the kernel, clean the buffer, and automatically allocate a 1MB buffer. However, it cannot be used to debug additional modules, such as SecureXL, CoreXL, or VPN. For those modules, other commands or tools are needed, such as fwaccel dbg, fw ctl affinity, or vpn debug.
Reference:
2: "fw ctl zdebug" - Helpful Command Combinations
3: How to use " fw ctl zdebug" command
Troubleshooting Expert R81.1 (CCTE) Course Outline) - Module 4: Debugging Tools and Methods

NEW QUESTION # 111
User defined URLS and HTTPS Inspection User defined URLs on the Security Gateway are stored in which database file?

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

Answer: D

NEW QUESTION # 112
Which of the following commands can be used to see the list of processes monitored by the Watch Dog process?

- A. fw ctl get str watchdog
- B. cpstat fw -f watchdog
- C. ps -ef | grep watchd
- D. cpwd_admin list

Answer: D

Explanation:

To see the list of processes monitored by the WatchDog process (CPWD), you use the cpwd_admin list command.
Option A (cpstat fw -f watchdog): Shows firewall status and statistics for the "fw" context, not necessarily the list of monitored processes.
Option B (fw ctl get str watchdog): Not a valid parameter for retrieving the list of monitored processes; "fw ctl" deals with kernel parameters.
Option C (cpwd_admin list): Correct command that lists all processes monitored by CPWD, their status, and how many times they have been restarted.
Option D (ps -ef | grep watchd): This will list any running process that matches the string "watchd" but will not specifically detail which processes are being monitored by CPWD.
Therefore, the best answer is cpwd_admin list.
Check Point Troubleshooting Reference
sk97638: Explains Check Point WatchDog (CPWD) usage and the cpwd_admin utility.
R81.20 CLI Reference Guide: Describes common troubleshooting commands including cpwd_admin list.
Check Point Gaia Administration Guide: Provides instructions for monitoring system processes and verifying CPWD.

NEW QUESTION # 113

......