CheckPoint.156-587.v2025-09-01.q84

Exam Code:	156-587
Exam Name:	Check Point Certified Troubleshooting Expert - R81.20
Certification Provider:	CheckPoint
Free Question Number:	84
Version:	v2025-09-01
# of views:	105
# of Questions views:	840
https://www.freeqas.com/qa/CheckPoint/156-587/CheckPoint.156-587.v2025-09-01.q84.html	

NEW QUESTION: 1
John has renewed his NPTX License but he gets an error (contract for Anti-Bot expired). He wants to check the subscription status on the CLI of the gateway, what command can he use for this?
A. fwm lie print
B. fw monitor license status
C. cpstat antimalware-f subscription status
D. show license status

Answer: (SHOW ANSWER)
The correct command to check the subscription status on the CLI of the gateway is show license status. This command displays the current license information, such as the license type, expiration date, and subscription status for various blades, such as Anti-Bot, Anti-Virus, IPS, etc. The command also shows the contract status for each blade, such as valid, expired, or invalid. If John has renewed his NPTX license, but he gets an error that the contract for Anti-Bot expired, he can use this command to verify the contract status and the subscription status for the Anti-Bot blade.
The other commands are incorrect because:
A . fwm lie print is not a valid command. The correct command is fwm lic print, which displays the license information on the Security Management Server, not on the gateway. This command does not show the subscription status or the contract status for the blades.
B . fw monitor license status is not a valid command. The correct command is fw monitor, which is a tool for capturing network traffic on the gateway, not for checking the license status.
C . cpstat antimalware-f subscription status is not a valid command. The correct command is cpstat antimalware -f subscription_status, which displays the subscription status for the Anti-Virus blade, not for the Anti-Bot blade. This command does not show the contract status for the blade.
Reference:
How to check the contract status and expiration date of the Check Point products How to check the subscription status of the blades on the Security Gateway sk163417 - Check Point Software

NEW QUESTION: 2

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. psql_client postgres cpm
B. psql_client cpm postgres
C. mysql_client cpm postgres
D. mysql -u root
Answer: B (LEAVE A REPLY)

NEW QUESTION: 3
What Check Point process controls logging?
A. FWD
B. CPVVD
C. CPM
D. CPD
Answer: D (LEAVE A REPLY)
The CPD process controls logging on the Security Management Server or the Log Server. It is responsible for receiving logs from the Security Gateways, storing them in the log files, and forwarding them to the SmartLog and SmartEvent servers. It also handles the communication with the SmartConsole clients and the CPM process. The CPD process runs on the Security Management Server or the Log Server as part of the Management High Availability module.
Reference:
1: Check Point Processes and Daemons - CPD
2: Troubleshooting Check Point logging issues when Security Management Server / Log Server is not receiving logs from Security Gateway Troubleshooting Expert R81.1 (CCTE) Course Outline) - Module 9: Logging and Status Troubleshooting.

NEW QUESTION: 4
You want to fully investigate the VPN establishment, what will you do?
A. debug FWD because VPND Is child process
B. use kernel debug with fw ctl debug -m VPN all
C. vpn debug and use IKEview
D. use vpn tu command and use option 8 to start debug
Answer: (SHOW ANSWER)

NEW QUESTION: 5
When debugging is enabled on firewall kernel module using the fw ctl debug' command with required options, many debug messages are provided by the kernel that help the administrator to identify Issues. Which of the following is true about these debug messages generated by the kernel module?
A. Messages are written to SFWDIR
B. Messages are written to console and also /var/log/messages file
C. Messages are written to a buffer and collected using 'fw ctl kdebug
D. Messages are written to /etc/dmesg file
Answer: C (LEAVE A REPLY)

NEW QUESTION: 6
Which process is responsible for the generation of certificates?
A. dbsync
B. cpm
C. fwm
D. cpca
Answer: (SHOW ANSWER)
The cpca process is responsible for the generation of certificates on the Security Management Server or the Multi-Domain Security Management Server. It is the Check Point Internal Certificate Authority (ICA) that issues certificates for internal use, such as for VPN, HTTPS Inspection, SmartConsole, and Secure Internal Communication (SIC). The cpca process runs on the Security Management Server or the Multi-Domain Security Management Server as part of the Management High Availability module.
References:
* 1: Check Point Processes and Daemons - cpca
* 2: How to generate and install a 3rd party IPSec Certificate
* 3: Automate certificate management on your firewall to find threats in encrypted HTTPS sessions
* Troubleshooting Expert R81.1 (CCTE) Course Outline) - Module 10: Certificate Management Troubleshooting.

NEW QUESTION: 7
Which of the following inputs is suitable for debugging HTTPS inspection issues?
A. fw debug tls on TDERROR_ALL_ALL=5
B. fw ctl debug -m fw + conn drop cptls
C. vpn debug cptls on
D. fw diag debug tls enable
Answer: A (LEAVE A REPLY)
The input that is suitable for debugging HTTPS inspection issues is fw debug tls on TDERROR_ALL_ALL=5. This input will enable the TLS debug mode and set the debug level to 5, which is the highest level of verbosity. The fw debug command is used to control the debug features of the firewall modules, such as TLS, CPTLS, HTTP, etc. The tls option will enable the debug mode for the TLS module, which is responsible for handling the HTTPS inspection feature. The TDERROR_ALL_ALL environment variable will set the debug level to 5, which will generate the most detailed and comprehensive debug output. The debug output will be written to the $FWDIR/log/tls.elg file, which can be collected and analyzed with the TLSView tool1 to see the details of the HTTPS inspection process, such as certificate validation, SSL/TLS negotiation, encryption/decryption, etc. The other options are incorrect because:
fw ctl debug -m fw + conn drop cptls will enable the kernel debug mode for the firewall module, with the flags conn, drop, and cptls. The kernel debug mode will generate the kdebug.txt file in the $FWDIR/log directory, which contains information about the firewall traffic processing in the kernel. The kernel debug mode is useful for troubleshooting issues related to policy, NAT, routing, and inspection, but not for issues related to HTTPS inspection, which is handled by the TLS module in the user space2.
vpn debug cptls on will enable the IKE debug mode for the CPTLS module, which is a component of the VPN module. The IKE debug mode will generate the ike.elg and ikev2.xmll files in the $FWDIR/log directory, which contain information about the IKE negotiation, authentication, and key exchange between the VPN peers. The CPTLS module is responsible for handling the SSL/TLS encryption/decryption for the VPN traffic, but not for the HTTPS inspection traffic3.

fw diag debug tls enable is not a valid command and will not enable the TLS debug mode. The fw diag command is used to control the diagnostic features of the firewall, such as packet capture, core dump, etc. The debug option is not a valid option for the fw diag command, and the tls option is not a valid option for the debug option. Reference:
How to use the TLSView tool
How to debug the Firewall kernel (fw) module
How to debug VPN issues on Quantum Spark (SMB) Appliances
[fw diag - Check Point CLI Reference Card]

NEW QUESTION: 8
What is NOT a benefit of the 'fw ctl zdebug' command?
A. Automatically allocate a 1MB buffer
B. Collect debug messages from the kernel
C. Cannot be used to debug additional modules
D. Clean the buffer
Answer: C (LEAVE A REPLY)
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: 9
What are the four main database domains?
A. System. Global. Log. Event
B. Local, Global, User, VPN
C. System, User, Global. Log
D. System, User, Host, Network
Answer: (SHOW ANSWER)

NEW QUESTION: 10
What function receives the AD log event information?
A. FWD
B. CPD
C. PEP
D. ADLOG
Answer: (SHOW ANSWER)
The ADLOG function receives the AD log event information from the Domain Controllers. The ADLOG function is part of the Identity Awareness feature that enables the Security Gateway to identify users and machines in the network and enforce Access Control policy rules based on their identities. The ADLOG function uses the AD Query (ADQ) method to connect to the Active Directory Domain

Controllers using WMI and subscribe to receive Security Event logs that are generated when users perform login. The ADLOG function then extracts the user and machine information that maps to an IP address from the event logs and sends it to the PEP function, which enforces the policy based on the identity information.
References:
* 1: Identity Awareness AD Query - Check Point Software
* 2: Identity Logging - Frequently Asked Questions - Check Point Software
3: Support, Support Requests, Training ... - Check Point Software

NEW QUESTION: 11
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: B (LEAVE A REPLY)
https://support.checkpoint.com/results/sk/sk97638

NEW QUESTION: 12
You receive reports that Users cannot browse internet sites. You are using identity awareness with AD Query and Identity Collector in addition you have the Browser Based Authentication Enabled. What command can be used to debug the problem?
A. on the gateway: ad debug on
B. on the gateway: ad query debug on
C. on the management: ad query debug extended
D. on the gateway: pdp debug nac extended
Answer: D (LEAVE A REPLY)
Identity Awareness is a feature that enables the Security Gateway to identify users and groups behind IP addresses, and apply security policies based on their identity12. Identity Awareness uses different methods to acquire identities, such as AD Query, Identity Collector, and Browser-Based Authentication12. To debug Identity Awareness issues, you need to use the command pdp debug on the gateway, where pdp stands for Policy Decision Point, the component that handles the identity acquisition and enforcement13. The command pdp debug has different flags for different identity sources, such as adlog for AD Query, ic for Identity Collector, and nac for Browser-Based Authentication13. The flag extended enables more detailed debug output13. Therefore, the correct command to debug the problem of users not being able to browse internet sites with Identity Awareness using AD Query, Identity Collector, and Browser-Based Authentication is pdp debug nac extended on the gateway13. The other options are incorrect because they either use the wrong command (ad debug instead of pdp debug), the wrong flag (ad query instead of nac), or the wrong location (on the management instead of on the gateway). References:
* 1: CCTE Courseware, Module 9: Advanced Identity Awareness Troubleshooting, Slide 4
* 2: Check Point R81 Identity Awareness Administration Guide, Chapter 1: Introduction to Identity Awareness, Page 7
* 3: Check Point R81 Identity Awareness Administration Guide, Chapter 5: Troubleshooting Identity Awareness, Page 49

NEW QUESTION: 13

Which of these packet processing components stores Rule Base matching state-related information?
A. Observers
B. Classifiers
C. Manager
D. Handlers
Answer: A (LEAVE A REPLY)
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.
References = The information can be verified from the Terraform Registry documentation on Publishing Modules provided by HashiCorp Developer1.

NEW QUESTION: 14
You have just acquired new licenses for your Check Point security Gateway. You need to attach the new license.
What is the object in the Security Console where you can attach the license for a software blade?
A. Software Container
B. Security Blade
C. Hardware Blade
D. Software Blade
Answer: A (LEAVE A REPLY)

NEW QUESTION: 15
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: B (LEAVE A REPLY)
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: 16
For Identity Awareness, what is the PDP process?
A. Identity server
B. Log Sifter
C. Captive Portal Service
D. UserAuth Database
Answer: A (LEAVE A REPLY)
The PDP process is the Identity server, which is a component of the Identity Awareness blade on the Security Gateway. The PDP process is responsible for collecting and managing identity information from various sources, such as Active Directory, Identity Agents, Captive Portal, Terminal Servers, and RADIUS. The PDP process also communicates with the PEP process, which is the Policy Enforcement Point, to enforce identity-based policies on the traffic passing through the Security Gateway1. The other options, such as Log Sifter, Captive Portal Service, and UserAuth Database, are either not related to Identity Awareness or not processes, but rather files or services. Reference: 1: sk93046: Identity Awareness - How to Configure

NEW QUESTION: 17
You are seeing output from the previous kernel debug. What command should you use to avoid that?
A. fw ctl zdebug disable
B. fw ctl debug = 0
C. fw ctl debug 0
D. fw ctl clean buffer = 0
Answer: C (LEAVE A REPLY)

NEW QUESTION: 18
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. rflsop and rflstart
B. evstart and evstop
C. RFLstop and RFLstart
D. smartlog_server stop and smartlog_server restart
Answer: B (LEAVE A REPLY)

NEW QUESTION: 19
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
E. CPstat is not a valid command. The correct command is cpstat, which is case-sensitive.
Answer: B (LEAVE A REPLY)
The correct Check Point command to display status and statistics information for various Check Point products and applications is cpstat. This command provides a dynamic real-time view of the system, showing the information such as the number of connections, packets, drops, CPU usage, memory usage, disk space, license status, and blade status. The cpstat command can be customized by using various options and flags to specify the product, the interval, the fields, and the format of the output. For example, to display the status and statistics of the firewall module every 5 seconds, the command would be:
cpstat fw -f all -i 5
The other commands are incorrect because:
A: CPview is a Check Point tool that displays information about the system performance, such as the CPU, memory, disk, network, and firewall. It does not show information about other products and applications, such as VPN, Identity Awareness, Anti-Virus, etc.
C: fwstat is not a valid command. The correct command is fw ctl pstat, which displays information about the firewall kernel, such as the number of connections, packets, drops, memory, and synchronization. It does not show information about other products and applications, such as VPN, Identity Awareness, Anti-Virus, etc.
Reference:
cpstat - Check Point Software
CPView Utility
fw ctl pstat - Check Point Software
(CCTE) - Check Point Software

NEW QUESTION: 20
URL Filtering is an essential part of Web Security in the Gateway. For the Security Gateway to perform a URL lookup when a client makes a URL request, where is the sync-request forwarded from if a sync-request is required?
A. RAD User Space
B. RAD Kernel Space
C. URLF Online Service
D. URLF Kernel Client
Answer: C (LEAVE A REPLY)

NEW QUESTION: 21
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. Cpd daemon is unable to connect to the log server
C. Postgres database is down
D. The loqqed in administrator does not have permissions to run SmartEvent
Answer: (SHOW ANSWER)

NEW QUESTION: 22
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. smartlog_server restart
B. Run the commands on the SMS: smartlogstart and smartlogstop
C. smartlog debug on and smartlog debug off
D. cpmstop and cpmstart
Answer: B (LEAVE A REPLY)

NEW QUESTION: 23
URL Filtering is an essential part of Web Security in the Gateway. For the Security Gateway to perform a URL lookup when a client makes a URL request, where is the sync-request forwarded from if a sync-request is required?
A. RAD User Space
B. URLF Online Service
C. URLF Kernel Client
D. RAD Kernel Space
Answer: C (LEAVE A REPLY)
URL Filtering is an essential part of Web Security in the Gateway that allows the administrator to control the access to web sites based on the site categorization and reputation. For the Security Gateway to perform a URL lookup when a client makes a URL request, the following steps are involved12:
* The URLF Kernel Client is the component that intercepts the URL request from the client and extracts the URL information, such as the host name, the path, and the query parameters. The URLF Kernel Client then checks the local cache to see if the URL has been previously categorized. If the URL is found in the cache, the URLF Kernel Client returns the cached category to the Security Policy and enforces the relevant action. If the URL is not found in the cache, the URLF Kernel Client sends a sync- request to the URLF User Space.
* The URLF User Space is the component that handles the sync-request from the URLF Kernel Client and performs the URL lookup. The URLF User Space first checks the local database to see if the URL has been previously categorized. If the URL is found in the database, the URLF User Space returns the database category to the URLF Kernel Client. If the URL is not found in the database, the URLF User Space sends an async-request to the URLF Online Service.
* The URLF Online Service is the component that handles the async-request from the URLF User Space and performs the URL lookup. The URLF Online Service is a cloud-based service that provides the most updated and accurate URL categorization and reputation. The

URLF Online Service queries the Check Point cloud servers to get the category and reputation of the URL, and returns the result to the URLF User Space. The URLF Online Service also updates the local database and cache with the new URL information.
Therefore, the sync-request is forwarded from the URLF Kernel Client to the URLF User Space, if a sync- request is required.
References: Application Control Administration Guide1, (CCTE) - Check Point Software2
1: https://sc1.checkpoint.com/documents/R81.10/WebAdminGuides/EN/CP_R81.
10_ApplicationControl_AdminGuide/html_frameset.htm 2: https://www.checkpoint.com/downloads/training
/DOC-Training-Data-Sheet-CCTE-R81.10-V1.0.pdf

NEW QUESTION: 24
Check Point Access Control Daemons contains several daemons for Software Blades and features. Which Daemon is used for Application & Control URL Filtering?
A. rad
B. pepd
C. pdpd
D. cprad
Answer: A (LEAVE A REPLY)

NEW QUESTION: 25
Which of the following file is commonly associated with troubleshooting crashes on a system such as the Security Gateway?
A. tcpdump
B. CPMIL dump
C. core dump
D. fw monitor
Answer: C (LEAVE A REPLY)
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.

NEW QUESTION: 26
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 | debug on
C. pep debug idc on
D. pdp debug set IDP all all
Answer: (SHOW ANSWER)

NEW QUESTION: 27
What is the simplest and most efficient way to check all dropped packets in real time?
A. Smartlog
B. fw ctl zdebug + drop in expert mode
C. cat /dev/fw1/log in expert mode
D. tail -f $FWDIR/log/fw.log |grep drop in expert mode
Answer: B (LEAVE A REPLY)

NEW QUESTION: 28
What function receives the AD log event information?
A. PEP
B. FWD
C. ADLOG
D. CPD
Answer: C (LEAVE A REPLY)

NEW QUESTION: 29
What is correct about the Resource Advisor (RAD) service on the Security Gateways?
A. RAD is not a separate module, it is an integrated function of the kernel module and does all operations in the kernel space
B. 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
C. 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
D. 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
Answer: (SHOW ANSWER)

NEW QUESTION: 30
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 management at SNACPORTAL_ HOME/conf/httpd_ nac.conf
B. on the gateway at $CPNAC_ HOME/conf/httpd_ nac.conf
C. on the gateway at $NACPORTAL_ HOME/conf/httpd_ nac.conf
D. on the management at SCPNAC_ HOME/conf/httpd_ nac.conf
Answer: C (LEAVE A REPLY)

NEW QUESTION: 31
You receive reports that Users cannot browse internet sites. You are using identity awareness with AD Query and Identity Collector in addition you have the Browser Based Authentication Enabled.
What command can be used to debug the problem?

A. on the gateway: pdp debug nac extended
B. on the management: ad query debug extended
C. on the gateway: ad query debug on
D. on the gateway: ad debug on
Answer: A (LEAVE A REPLY)

NEW QUESTION: 32
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. mpclient getdata mobi
D. netstat getdata sslvpn
Answer: A (LEAVE A REPLY)

NEW QUESTION: 33
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. CMI Loader
B. cpas
C. Context Loader
D. PSL - Passive Signature Loader
Answer: (SHOW ANSWER)

NEW QUESTION: 34
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
Answer: A (LEAVE A REPLY)
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 References:
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.

NEW QUESTION: 35
What process monitors terminates, and restarts critical Check Point processes as necessary?
A. CPM
B. FWD
C. CPWD
D. FWM
Answer: C (LEAVE A REPLY)
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.

NEW QUESTION: 36
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 (LEAVE A REPLY)
The Global Domain is one of the relational database domains in the Postgres database that stores the management configuration. The purpose of the Global Domain is to serve as the global database for Multi- Domain Security Management (MDSM) and contain the global objects and policies that are shared across all domains. The Global Domain also stores the global settings, such as the administrator roles, the LDAP servers, the IPS profiles, and the SmartEvent views. The Global Domain can be managed by the Global Domain Administrator or the Super User Administrator using the SmartConsole. The Global Domain can be backed up and restored using the mds_backup and mds_restore commands.
References:
* 1: Architecture and Processes - Check Point Software
* 2: Multi-Domain Security Management R81.10 Administration Guide
* 3: How to backup and restore Multi-Domain Security Management Server

NEW QUESTION: 37
The management configuration stored in the Postgres database is partitioned into several relational database domains. What is the purpose of the Global Domain?
A. This domain is used as the global database to back up the objects referencing the corresponding object attributes from the System Domain.
B. Global Domains is used by the IPS software blade to map the IDs to the corresponding countries according to the IpToCountry.csv file.
C. This domain is used as the global database for MDSM and contains global objects and policies.
D. This domain is used as the global database to track the changes made by multiple administrators on the same objects prior to publishing.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 38
You need to monitor traffic pre-inbound and before the VPN module in a Security Gateway. How would you achieve this using fw monitor?
A. fw monitor -p all
B. fw monitor -pi -vpn
C. fw monitor -pi +vpn
D. fw monitor -pi +vpn
Answer: B (LEAVE A REPLY)
The fw monitor command is a powerful troubleshooting tool in Check Point Gateways that captures packets at various points in the processing chain. The question asks how to capture traffic pre-inbound (before inbound processing, i.e., at the "i" inspection point) and before the VPN module (before VPN decryption or processing).
The fw monitor syntax allows specifying inspection points using options like -pi (pre-inbound) and module names (e.g., -vpn for the VPN module). The correct syntax to capture traffic before a specific module is -pi -<module>, where the module name is prefixed with a minus sign to indicate "before" the module.

Option A: Incorrect. fw monitor -p all captures packets at all inspection points in the chain, which includes pre-inbound, post-inbound, pre-outbound, and post-outbound points, as well as points around all modules. This is too broad and does not specifically target pre-inbound and before the VPN module.
Option B: Correct. fw monitor -pi -vpn captures packets at the pre-inbound inspection point ("i") and before the VPN module (-vpn). The -pi specifies the pre-inbound point, and -vpn ensures the capture occurs before VPN processing (e.g., decryption).
Option C: Incorrect. fw monitor -pi +vpn would capture packets at the pre-inbound point but after the VPN module (+vpn indicates after the module), which contradicts the requirement to capture before the VPN module.
Option D: Incorrect. This option is a duplicate of Option C in the provided question, likely a typographical error. Even if corrected, +vpn is incorrect for the same reason as Option C.
Reference:
The Check Point R81.20 Gaia Administration Guide explains the fw monitor command and its options, including how to specify inspection points and module positions. The CCTE R81.20 course includes hands-on labs for using fw monitor to troubleshoot packet flow, emphasizing precise inspection point selection.
For precise details, refer to:
Check Point R81.20 Gaia Administration Guide, section on "fw monitor" (available via Check Point Support Center).
CCTE R81.20 Courseware, which covers advanced packet capture techniques with fw monitor (available through authorized training partners).

NEW QUESTION: 39
How many packets are needed to establish IKEv1?
A. 5
B. Only three packets for main mode
C. 8
D. 6
Answer: (SHOW ANSWER)

NEW QUESTION: 40
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
Answer: A (LEAVE A REPLY)
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.

NEW QUESTION: 41
What information does the doctor-log script supply?
A. Current and daily average logging rates. Indexing status, Size
B. Repair options. Logging Rates, Logging Directories
C. Logging rates. Logging Directories, List of troubleshooting tips
D. Logging errors. Exceptions, Repair options
Answer: A (LEAVE A REPLY)

NEW QUESTION: 42
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 an asymmetric key on both sides
B. Produce a symmetric key on both sides
C. Symmetric keys based on pre-shared secret
D. Produce a pair of public and private keys
Answer: D (LEAVE A REPLY)

NEW QUESTION: 43
The two procedures available for debugging in the firewall kernel are
i. fw ctl zdebug
ii. fw ctl debug/kdebug
Choose the correct statement explaining the differences in the two
A. (i) is used to debug only issues related to dropping of traffic, however (ii) can be used for any firewall issue including NATing, clustering etc.
B. (i) is used to debug the access control policy only, however (ii) can be used to debug a unified policy
C. (i) is used on a Security Gateway, whereas (ii) is used on a Security Management Server

D. (i) is used for general debugging, has a small buffer and is a quick way to set kernel debug flags to getan output via command line whereas (ii) is useful when there is a need for detailed debugging and requires additional steps to set the buffer and get an output via command line

Answer: (SHOW ANSWER)

The correct statement explaining the differences between the two procedures for debugging in the firewall kernel is D. (i) is used for general debugging, has a small buffer and is a quick way to set kernel debug flags to get an output via command line whereas (ii) is useful when there is a need for detailed debugging and requires additional steps to set the buffer and get an output via command line.

The command fw ctl zdebug is a shortcut command that sets the kernel debug flags to a predefined value and prints the debug output to the standard output. It is useful for general debugging of common issues, such as traffic drops, NAT, VPN, or clustering. It has a small buffer size and does not require additional steps to start or stop the debugging. However, it has some limitations, such as it cannot be used with SecureXL, it cannot filter the output by chain modules, and it cannot save the output to a file12.

The command fw ctl debug is a command that allows the administrator to set the kernel debug flags to a custom value and specify the chain modules to debug. It is useful for detailed debugging of specific issues, such as policy installation, CoreXL, or Identity Awareness. It has a larger buffer size and can save the output to a file. However, it requires additional steps to start and stop the debugging, such as setting the buffer size, clearing the buffer, dumping the buffer, and resetting the debug flags12.

The command fw ctl kdebug is a command that is used in conjunction with fw ctl debug to dump the kernel debug buffer to the standard output or to a file. It is part of the procedure (ii) for detailed debugging in the firewall kernel12.

The other statements are not correct or relevant for explaining the differences between the two procedures for debugging in the firewall kernel. The command fw ctl zdebug can be used to debug more than just the access control policy, and the command fw ctl debug/kdebug can be used to debug more than just the unified policy. Both commands can be used on both the Security Gateway and the Security Management Server, depending on the issue to be debugged12.

References: Check Point Processes and Daemons3, (CCTE) - Check Point Software2

1: https://sc1.checkpoint.com/documents/R81.10/WebAdminGuides/EN/CP_R81.10_AdvancedTechnicalReferenceGuide/html_frameset.htm 2: https://www.checkpoint.com/downloads/training/DOC-Training-Data-Sheet-CCTE-R81.10-V1.0.pdf 3: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk97638

NEW QUESTION: 44

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

A. IKEview

B. vi on the cti

C. notepad++

D. any xml editor

Answer: (SHOW ANSWER)

IKE view is the most efficient way to read an IKEv2 debug. IKE view is a graphical user interface tool that enables you to analyze the IKEv2 debugs generated by the Security Gateway1. It can parse the debug files and display the information in a structured and readable format. It can also filter the debug messages based on various criteria, such as IP address, encryption domain, or IKEv2 state1. IKE view can help you to troubleshoot the IKEv2 issues and identify the root cause of the problems1. Reference: IKEView: VPN Debugging Tool - Check Point Software

NEW QUESTION: 45

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

Answer: (SHOW ANSWER)

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.

NEW QUESTION: 46

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. cpstat

B. CPstat

C. CPview

D. fwstat

Answer: A (LEAVE A REPLY)

NEW QUESTION: 47

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. User, Active Directory and Access Role

D. Identity Awareness Blade on Security Gateway, User Database on Security Management Server and Active Directory
Answer: (SHOW ANSWER)

NEW QUESTION: 48
Captive Portal, PDP and PEP run in what space?
A. User
B. FWD
C. Kernel
D. CPM
Answer: (SHOW ANSWER)

NEW QUESTION: 49
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
Answer: (SHOW ANSWER)
When the free command on a Linux-based system (like a Check Point Gaia gateway) shows a non-zero value in the "Swap" column, it indicates that the system has utilized its swap space. Swap space is a portion of the hard disk designated to act as virtual RAM when the physical RAM is fully utilized.
The most direct and accurate explanation for swap usage is that the system's demand for Random Access Memory (RAM) exceeded the available physical RAM, forcing the operating system to move some less frequently used memory pages from RAM to the swap space on the disk. This frees up physical RAM for more active processes.
Let's analyze the options:
A . Utilization of ram is high and swap file had to be used: This is the correct and fundamental reason. Swap is used precisely because RAM utilization reached a point where the system needed more memory than was physically available.
B . Swap file is used regularly because RAM memory is reserved for management traffic: While Check Point gateways handle management traffic, operating systems do not typically use swap "regularly" due to a fixed reservation of RAM for such traffic in a way that would routinely force swapping under normal conditions. If management traffic is excessively high and consumes too much RAM, it would fall under the general case of high RAM utilization.
C . Swap memory is used for heavy connections when RAM memory is full: This describes a common cause for high RAM utilization on a firewall. Heavy connections can consume significant memory resources. When this consumption leads to RAM exhaustion, swap will indeed be used. However, option A is a more general and direct explanation of why swap is used, regardless of the specific cause of high RAM utilization. Option C is a specific scenario leading to the condition described in A.
D . Its ole Swap is used to increase performance: This statement is incorrect. Swapping to disk is significantly slower than accessing RAM. Therefore, swap usage generally indicates a performance bottleneck (or potential for one) rather than a performance enhancement. While virtual memory (which includes swap) allows a system to run more or larger applications than its physical RAM would normally allow, the act of swapping itself is detrimental to performance.

Conclusion: The best answer is A because it directly and accurately describes the immediate reason for swap usage: high RAM utilization necessitating the use of the swap file. Option C, while plausible as a cause of high RAM utilization, is a specific instance, whereas A is the overarching reason swap comes into play.
Reference (General Linux/System Administration Principles and supported by CCTE exam preparation materials): This understanding is based on fundamental principles of how operating systems manage memory and swap space. Check Point CCTE R81.20 exam preparation materials also affirm this understanding for similar questions. For instance, a question identical to this one appearing in CCTE exam preparation resources typically points to option A as the correct answer.

NEW QUESTION: 50
The Check Point Firewall Kernel is the core component of the Gaia operating system and an integral part of the traffic inspection process. There are two procedures available for debugging the firewall kernel. Which procedure/command is used for troubleshooting packet drops and other kernel activities while using minimal resources (1 MB buffer)?
A. fwk ell debug
B. fw ctl zdebug
C. fw debug ctl
D. fw ctl debug/kdebug
Answer: B (LEAVE A REPLY)

NEW QUESTION: 51
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 (LEAVE A REPLY)
The Global Domain is one of the relational database domains in the Postgres database that stores the management configuration. The purpose of the Global Domain is to serve as the global database for Multi-Domain Security Management (MDSM) and contain the global objects and policies that are shared across all domains. The Global Domain also stores the global settings, such as the administrator roles, the LDAP servers, the IPS profiles, and the SmartEvent views. The Global Domain can be managed by the Global Domain Administrator or the Super User Administrator using the SmartConsole. The Global Domain can be backed up and restored using the mds_backup and mds_restore commands.
Reference:
1: Architecture and Processes - Check Point Software
2: Multi-Domain Security Management R81.10 Administration Guide
3: How to backup and restore Multi-Domain Security Management Server

NEW QUESTION: 52

You found out that $FWDIR/log/fw.log is constantly growing in size at a Security Gateway, what is the reason?
A. The GW is logging locally
B. fw.log can grow when GW does not have space in logging directory
C. Its not a problem the gateways is logging connections and also sessions
D. TCP state logging is enabled
Answer: C (LEAVE A REPLY)

NEW QUESTION: 53
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
Answer: (SHOW ANSWER)
The correct answer is A. smartlogrestart and smartlogstart. These commands are used to restart the SmartLog service and start the SmartLog indexing process. They can be run on the Security Management Server or the Log Server to resolve issues with SmartLog not being active or failing to parse results from the server. The other commands are not valid or relevant for this purpose. References: Check Point Troubleshooting Expert (CCTE) R81.10 Course Data Sheet1, Check Point Troubleshooting Expert (CCTE) R81.10 Course Outline2, Check Point Troubleshooting Expert (CCTE) R81.10 Lab Manual3, sk175223 - SmartLog is not active or failed to parse results from server

NEW QUESTION: 54
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
Answer: D (LEAVE A REPLY)
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

NEW QUESTION: 55
What does CMI stand for in relation to the Access Control Policy?
A. Context Manipulation Interface
B. Context Management Infrastructure
C. Content Management Interface
D. Content Matching Infrastructure
Answer: (SHOW ANSWER)

CMI stands for Context Management Infrastructure, which is a component of the Access Control Policy that enables the Security Gateway to inspect traffic based on the context of the connection. Context includes information such as user identity, application, location, time, and device. CMI allows the Security Gateway to apply different security rules and actions based on the context of the traffic, and to dynamically update the context as it changes. CMI consists of three main elements: Unified Policy, Identity Awareness, and Content Awareness.

NEW QUESTION: 56
What is the kernel process for Content Awareness that collects the data from the contexts received from the CMI and decides if the file is matched by a data type?
A. dlpda
B. cntmgr
C. dlpu
D. cntawmod
Answer: D (LEAVE A REPLY)

NEW QUESTION: 57
Which Daemon should be debugged for HTTPS Inspection related issues?
A. VPND
B. WSTLSD
C. FWD
D. HTTPD
Answer: B (LEAVE A REPLY)

NEW QUESTION: 58
What version of Check Point can Security Gateways begin dynamically distributing Logs between log servers?
A. R81
B. R77
C. R30
D. R75
Answer: A (LEAVE A REPLY)

NEW QUESTION: 59
You run cpwd_admin list on a Security Gateway and notice that the CPM process is not listed. Select the best answer.
A. The output is different between Gateway and Management Server.
B. CPM is not running and can't be monitored by WatchDog.
C. If you want to monitor CPM, you have to manually add it to WatchDog.
D. CPM is not there because it has its own monitoring system. Only lower processes are monitored by WatchDog.
Answer: (SHOW ANSWER)
The cpwd_admin list command is used to display the status of processes monitored by the Check Point WatchDog Daemon (CPWD). The CPM (Check Point Management) process is a core process on the Security Management Server, responsible for management operations. However, on a Security Gateway, the CPM process is not typically present, as it is specific to management functions.

Option A: Correct. The output of cpwd_admin list differs between a Security Gateway and a Security Management Server. On a Security Gateway, processes like FWD, VPND, and PEP are monitored, but CPM is not present because it runs on the Management Server. Thus, CPM will not appear in the cpwd_admin list output on a Gateway.
Option B: Incorrect. While it's true that CPM is not running on the Security Gateway, the reason it's not listed is not because it "can't be monitored" by CPWD. On a Management Server, CPM is indeed monitored by CPWD, but this question pertains to a Gateway.
Option C: Incorrect. CPM is automatically monitored by CPWD on systems where it runs (e.g., Management Server). There is no need to manually add it to WatchDog's monitoring list.
Option D: Incorrect. CPM does not have its own separate monitoring system. On a Management Server, CPM is monitored by CPWD like other critical processes. The statement about "only lower processes" being monitored is inaccurate.
Reference:
The Check Point R81.20 Gaia Administration Guide explains the role of CPWD and the processes it monitors on different Check Point systems (Gateway vs. Management Server). The CCTE R81.20 course (as per and) emphasizes understanding the differences in process monitoring between Gateways and Management Servers, including the use of cpwd_admin commands for troubleshooting.https://edu.arrow.com/uk/training/course-detail/90175/Check-Point-Certified-Troubleshooting-Expert-%28CCTE%29-R81.20-%28includes-180-days%27-lab-access%29/False Reference:
The Check Point R81.20 Gaia Administration Guide explains the role of CPWD and the processes it monitors on different Check Point systems (Gateway vs. Management Server). The CCTE R81.20 course (as per and) emphasizes understanding the differences in process monitoring between Gateways and Management Servers, including the use of cpwd_admin commands for troubleshooting.https://edu.arrow.com/uk/training/course-detail/90175/Check-Point-Certified-Troubleshooting-Expert-%28CCTE%29-R81.20-%28includes-180-days%27-lab-access%29/False
https://www.koenig-solutions.com/ccte-r81-20-language-course
For precise details, refer to:
Check Point R81.20 Gaia Administration Guide, section on "CPWD and Process Monitoring" (available via Check Point Support Center).
CCTE R81.20 Courseware, which covers advanced troubleshooting of Security Gateway and Management Server processes (available through authorized training partners).

NEW QUESTION: 60
When dealing with monolithic operating systems such as Gaia, where are system calls initiated from to achieve a required system level function?
A. Slow Path
B. Kernel Mode
C. Medium Path
D. User Mode
Answer: D (LEAVE A REPLY)

NEW QUESTION: 61
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. HTTPS Inspection Daemon (HID)

B. Mobile Access Daemon (MAD)
C. Multi-portal Daemon
D. Connectra VPN Daemon (cvpnd)
Answer: (SHOW ANSWER)

NEW QUESTION: 62
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: (SHOW ANSWER)
The process responsible for log indexing and text searching is solr, which is a child process of cpm. The solr process is responsible for indexing the logs and providing the search engine for SmartLog and SmartConsole.
The solr process is started by the cpm process and can be monitored by the command cpwd_admin list. The solr process uses the PostgreSQL database to store the indexed data and the Lucene library to perform the text search. The solr process can be affected by various factors, such as the size and number of log files, the hardware resources, the network connectivity, and the configuration settings. If the solr process is not running correctly, the administrator may experience issues with log indexing and text searching, such as slow performance, missing logs, or incorrect results.

NEW QUESTION: 63
What is the proper command for allowing the system to create core files?
A. service core-dump start
B. # set core-dump enable
save config
C. SFWDIR/scripts/core-dump-enable.sh
D. set core-dump enable
>save config
Answer: D (LEAVE A REPLY)

NEW QUESTION: 64

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)

Answer: A (LEAVE A REPLY)

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

NEW QUESTION: 65

The FileApp parser in the Content Awareness engine does not extract text from which of the following file types?

A. Microsoft Office .docx files

B. PDF

C. Microsoft Office Powerpoint files

D. Microsoft Office Excel files

Answer: B (LEAVE A REPLY)

NEW QUESTION: 66

What is the simplest and most efficient way to check all dropped packets in real time?

A. tail -f $FWDIR/log/fw.log |grep drop in expert mode

B. cat /dev/fw1/log in expert mode

C. fw ctl zdebug + drop in expert mode

D. Smartlog

Answer: (SHOW ANSWER)

The simplest and most efficient way to check all dropped packets in real time is C. fw ctl zdebug + drop in expert mode. This command is a shortcut command that sets the kernel debug flags to a predefined value and prints the debug output to the standard output. It is useful for general debugging of common issues, such as traffic drops, NAT, VPN, or clustering. It has a small buffer size and does not require additional steps to start or stop the debugging. However, it has some limitations, such as it cannot be used with SecureXL, it cannot filter the output by chain modules, and it cannot save the output to a file12.
The other commands are not as simple or efficient as the fw ctl zdebug + drop command. The command tail -f $FWDIR/log/fw.log |grep drop in expert mode will only show the drops that are logged in the fw.log file, which may not include all the drops that occur in the kernel. The command cat /dev/fw1/log in expert mode will show the raw binary data of the kernel debug buffer, which is not human-readable and may contain irrelevant information. The command Smartlog will show the drops that are indexed and stored in the SmartEvent database, which may not be in real time and may depend on the log server performance12.

1:
https://sc1.checkpoint.com/documents/R81.10/WebAdminGuides/EN/CP_R81.10_AdvancedTechnicalReferenceGuide/html_frameset.htm
2: https://www.checkpoint.com/downloads/training/DOC-Training-Data-Sheet-CCTE-R81.10-V1.0.pdf The Check Point R81.20 Gaia Administration Guide describes fw ctl zdebug as a key troubleshooting tool for real-time packet analysis, particularly for drops. The CCTE R81.20 course emphasizes using fw ctl zdebug for kernel-level debugging, including monitoring dropped packets.
For precise details, refer to:
Check Point R81.20 Gaia Administration Guide, section on "fw ctl zdebug" (available via Check Point Support Center).
CCTE R81.20 Courseware, which covers advanced troubleshooting techniques for packet drops (available through authorized training partners).

NEW QUESTION: 67
John has renewed his NPTX License but he gets an error (contract for Anti-Bot expired). He wants to check the subscription status on the CLI of the gateway, what command can he use for this?
A. fwm lie print
B. cpstat antimalware-f subscription status
C. show license status
D. fw monitor license status
Answer: B (LEAVE A REPLY)

NEW QUESTION: 68
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
Answer: C (LEAVE A REPLY)
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.

NEW QUESTION: 69
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. Use Check Point InfoView utility to analyze debug output
B. Divide debug information into smaller files. Use "fw ctl kdebug -f -o "filename" -m 25 - s "1024"
C. Use "fw ctl zdebug" because of 1024KB buffer size
D. Reduce debug buffer to 1024KB and run debug for several times
Answer: (SHOW ANSWER)

NEW QUESTION: 70
User defined URLS and HTTPS Inspection User defined URLs on the Security Gateway are stored in which database file?
A. https_urlf.bin
B. urlf_https.bin
C. urlf_db.bin
D. https_db.bin
Answer: C (LEAVE A REPLY)

NEW QUESTION: 71
Which process is responsible for the generation of certificates?
A. dbsync
B. cpm
C. fwm
D. cpca
Answer: (SHOW ANSWER)
The cpca process is responsible for the generation of certificates on the Security Management Server or the Multi-Domain Security Management Server. It is the Check Point Internal Certificate Authority (ICA) that issues certificates for internal use, such as for VPN, HTTPS Inspection, SmartConsole, and Secure Internal Communication (SIC). The cpca process runs on the Security Management Server or the Multi-Domain Security Management Server as part of the Management High Availability module.
Reference:
1: Check Point Processes and Daemons - cpca
2: How to generate and install a 3rd party IPSec Certificate
3: Automate certificate management on your firewall to find threats in encrypted HTTPS sessions Troubleshooting Expert R81.1 (CCTE) Course Outline) - Module 10: Certificate Management Troubleshooting.

NEW QUESTION: 72
VPN issues may result from misconfiguration, communication failure, or incompatible default configurations between peers. Which basic command syntax needs to be used for troubleshooting Site-to-Site VPN issues?
A. cp debug truncon
B. fw debug truncon
C. vpn truncon debuq
D. vpn debug truncon
Answer: (SHOW ANSWER)

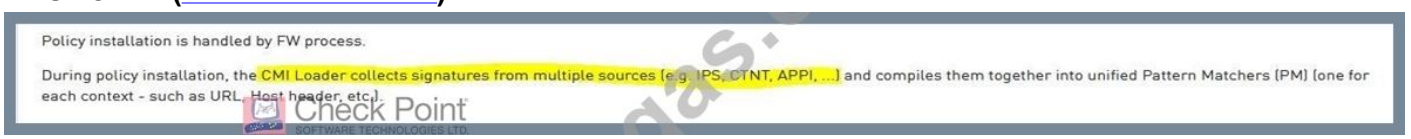
NEW QUESTION: 73
When a User Mode process suddenly crashes, it may create a core dump file. Which of the following information is available in the core dump and may be used to identify the root cause of the crash?
i. Program Counter
ii. Stack Pointer
iii. Memory management information
iv. Other Processor and OS flags / information
A. iii and iv only
B. i and ii only
C. i, ii, iii and iv
D. Only Iii
Answer: C (LEAVE A REPLY)
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 References:
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.

NEW QUESTION: 74
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
Answer: A (LEAVE A REPLY)
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.

NEW QUESTION: 75
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
Answer: B (LEAVE A REPLY)
The doctor-log script is a tool that provides information about the logging system and helps to identify and troubleshoot common issues. The script runs automatically every night and generates a report that contains the following information:
* Current and daily average logging rates: This shows how many logs are being generated and received by the log server per second. It can help to monitor the logging performance and identify any spikes or drops in the logging rate.
* Indexing status: This shows the status of the log indexing process, which enables faster and more efficient log searches. It can help to identify any issues with the indexing system, such as delays, failures, or errors.
* Size: This shows the size of the log files and the disk space used by the logging system. It can help to manage the disk space and plan for log rotation and backup.
The doctor-log script also provides some troubleshooting tips and repair options for common logging issues, such as corrupted log files, missing log indexes, or low disk space. The script can be run manually or scheduled to run at a specific time. The script output can be viewed in the SmartConsole or in the log server file system.
References: Check Point Troubleshooting Expert (CCTE) course, Module 2: Logs and Monitoring, Lesson 2.1: Logs and SmartEvent, Slide 19-21.

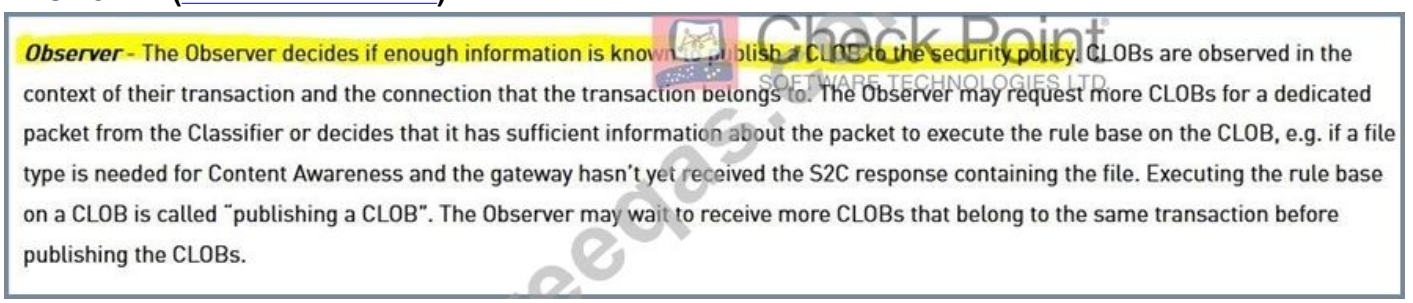
NEW QUESTION: 76
Which of the following is a component of the Context Management Infrastructure used to collect signatures in user space from multiple sources, such as Application Control and IPS, and compiles them together into unified Pattern Matchers?
A. PSL - Passive Signature Loader
B. cpas
C. Context Loader
D. CMI Loader
Answer: C (LEAVE A REPLY)



NEW QUESTION: 77
Which of the following inputs is suitable for debugging HTTPS inspection issues?
A. fw debug tls on TDERROR_ALL_ALL=5
B. fw ctl debug -m fw + conn drop cptls
C. vpn debug cptls on
D. fw diag debug tls enable
Answer: (SHOW ANSWER)
The input that is suitable for debugging HTTPS inspection issues is fw debug tls on TDERROR_ALL_ALL=5. This input will enable the TLS debug mode and set the debug level to 5, which is the highest level of verbosity. The fw debug command is used to control the debug features of the firewall modules, such as TLS, CPTLS, HTTP, etc. The tls option will enable the debug mode for the TLS module, which is responsible for handling the HTTPS inspection feature. The TDERROR_ALL_ALL environment variable will set the debug level to 5, which will generate the most detailed and comprehensive debug output. The debug output will be written to the $FWDIR/log/tls.elg file, which can be collected and analyzed with the TLSView tool1 to see the details of the HTTPS inspection process, such as certificate validation, SSL
/TLS negotiation, encryption/decryption, etc. The other options are incorrect because:
* fw ctl debug -m fw + conn drop cptls will enable the kernel debug mode for the firewall module, with the flags conn, drop, and cptls. The kernel debug mode will generate the kdebug.txt file in the $FWDIR
/log directory, which contains information about the firewall traffic processing in the kernel. The kernel debug mode is useful for troubleshooting issues related to policy, NAT, routing, and inspection, but not for issues related to HTTPS inspection, which is handled by the TLS module in the user space2.

* vpn debug cptls on will enable the IKE debug mode for the CPTLS module, which is a component of the VPN module. The IKE debug mode will generate the ike.elg and ikev2.xmll files in the $FWDIR
/log directory, which contain information about the IKE negotiation, authentication, and key exchange between the VPN peers. The CPTLS module is responsible for handling the SSL/TLS encryption
/decryption for the VPN traffic, but not for the HTTPS inspection traffic3.
* fw diag debug tls enable is not a valid command and will not enable the TLS debug mode. The fw diag command is used to control the diagnostic features of the firewall, such as packet capture, core dump, etc. The debug option is not a valid option for the fw diag command, and the tls option is not a valid option for the debug option. References:
* How to use the TLSView tool
* How to debug the Firewall kernel (fw) module
* How to debug VPN issues on Quantum Spark (SMB) Appliances
* [fw diag - Check Point CLI Reference Card]

NEW QUESTION: 78
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
Answer: D (LEAVE A REPLY)
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

NEW QUESTION: 79
In Check Point's Packet Processing Infrastructure, what is the role of Observers?
A. They store Rule Base matching state related information
B. Observers monitor the state of Check Point gateways and report it to the security manager
C. Observers attach object IDs to traffic
D. Observers decide whether or not to publish a CLOB to the Security Policy
Answer: D (LEAVE A REPLY)


NEW QUESTION: 80
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
Answer: B (LEAVE A REPLY)
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.

NEW QUESTION: 81
If SmartLog is not active or failed to parse results from server, what commands can be run to re- enable the service?
A. smartloginit and smartlogstop
B. smartlogstart and smartlogstop
C. smartlogrestart and smartlogstart
D. smartlogstart and smartlogsetup
Answer: C (LEAVE A REPLY)

NEW QUESTION: 82
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. i and ii only
B. Only iii
C. iii and iv only
D. i, ii, iii and iv
Answer: (SHOW ANSWER)

NEW QUESTION: 83
VPNs allow traffic to pass through the Internet securely by encrypting the traffic as it enters the VPN tunnel and decrypting the traffic as it exits. Which process is responsible for Mobile VPN connections?
A. cvpnd
B. fwk
C. vpnd
D. vpnk

E. vpnk: This refers to VPN kernel-level operations and modules (e.g., handling the actual encryption/decryption of traffic processed by IPsec SAs). It is not the user-space daemon that manages Mobile VPN sessions and policies.
Answer: A (LEAVE A REPLY)
Therefore, cvpnd is the specific process dedicated to managing Mobile VPN connections within the Check Point architecture.
Reference (based on official Check Point documentation naming and functionality):
Check Point R81.20 CLI Reference Guide (details for cvpnd_admin).
Check Point R81.20 Administration Guides (sections discussing Mobile Access architecture and daemons).
Commonly known Check Point process lists available in CCTE study materials.
Explanation:
The Check Point process responsible for Mobile VPN connections, particularly those associated with the Mobile Access Software Blade (which includes SSL VPN and clientless access), is cvpnd (Connectra VPN Daemon).
Exact Extracts and Supporting Information:
Check Point CLI Reference Guide (for cvpnd_admin):
"cvpnd_admin. Description. Changes the behavior of the Mobile Access cvpnd process." This command utility directly interacts with cvpnd for Mobile Access functionalities.
Check Point Daemon Lists (e.g., from "tech :: stuff - Checkpoint Daemons and Processes Explained" or similar CCTE R81.20 documentation):
Under the "Mobile Access Blade" section, CVPND is typically listed as:"CVPND - Connectra VPN Daemon. Main daemon for the Mobile Access Software Blade." It's also often noted that the cpwd_admin list command (Check Point WatchDog) shows this process as "CVPND".
Commands like cvpnstart and cvpnstop are used to manage this daemon.
Exam Preparation Materials (e.g., ExamTopics for 156-586):
A question directly asking "Which process is responsible for Mobile VPN connections?" with options including cvpnd, vpnk, fwk, and vpnd, typically indicates cvpnd as the correct answer.
Explanation of other options:
B : fwk: This is a general suffix often related to firewall worker processes or kernel modules, not a specific high-level daemon for Mobile VPN.
C : vpnd: This is the main VPN daemon, primarily responsible for site-to-site IPsec VPNs and some traditional IPsec remote access clients. While it handles VPN functions, cvpnd is specialized for Mobile Access.

NEW QUESTION: 84
What tool would you run to diagnose logging and indexing?
A. run doctor-log.sh
B. cpstat mg -f log_server
C. run diagnostic view
D. run cpm_doctor.sh
Answer: A (LEAVE A REPLY)