Checkpoint

156-587

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

Killexams Complete pool of Questions and Answers of 156-587: Check Point Certified Troubleshooting Expert (CCTE) - R81.20 covers the below exam outline.

- *Identify and use Linux-based and Check Point commands and tools for system monitoring, file editing, and file viewing.*

- *Identify and use the appropriate troubleshooting and debug commands/tools to resolve advanced Management Server and API Server issues.*

- *Investigate and troubleshoot traffic or security-related issues using logs and events monitoring tools.*

- *Identify and use the appropriate troubleshooting and debug commands/tools to resolve advanced Security Gateway issues.*

- *Demonstrate an understanding of advanced troubleshooting tools and techniques for kernel debugging.*

- *Identify and use the appropriate troubleshooting and debug commands/tools to resolve advanced Access Control issues.*

- *Identify and use the appropriate troubleshooting and debug commands/tools to resolve advanced Identity Awareness issues.*

- *Identify and use the appropriate troubleshooting and debug commands/tools to resolve advanced Site-to-Site VPN Troubleshooting issues.*

- *Identify and use the appropriate troubleshooting and debug commands/tools to resolve advanced Client-to- Site VPN Troubleshooting issues.*

Below are sample questions. Full version contains complete set of Questions and Answers

Question: 805

How can you use the SmartLog to filter logs for a specific application traffic?

A. By filtering logs using the Application column
B. By filtering logs using the Source IP
C. By filtering logs using the Log Type
D. By using the Time Range filter

Answer: A

Explanation: The Application column in SmartLog allows you to filter logs specifically for traffic related to a particular application.

Question: 806

Which command is used to view the status of Check Point licenses on a Security Gateway?

A. cplic print
B. fw ctl pstat
C. cphaprob state
D. cpstat fw

Answer: A

Explanation: The command "cplic print" is used to view the status of Check

Point licenses on a Security Gateway. It displays information about the active licenses, license features, and expiration dates. Option B, "fw ctl pstat," displays the status of the firewall kernel and its various components. Option C, "cphaprob state," shows the state of the cluster members. Option D, "cpstat fw," retrieves firewall status information but does not specifically display license information.

Question: 807
If configuration changes are made on the Primary Management Server, how should they be replicated to the Secondary?

A. Manually configure the Secondary
B. Use the "cphaprob sync" command
C. The changes replicate automatically
D. Restart both servers

Answer: C

Explanation: In a properly configured HA environment, changes made on the Primary replicate automatically to the Secondary.

Question: 808
If you need to verify the configuration of the API Server, which command provides detailed information?

A. cpconfig
B. show api-config
C. api show config
D. cpstat api

Answer: C

Explanation: The api show config command gives a detailed view of the API Server's current configuration.

Question: 809

Which tool is used to troubleshoot VPN-related issues in Check Point firewalls?

A. vpn debug
B. fw ctl zdebug
C. tcpdump
D. sysconfig

Answer: A

Explanation: The tool used to troubleshoot VPN-related issues in Check Point firewalls is "vpn debug". Vpn debug is a command-line utility that enables debugging and logging of VPN-related events and messages. It provides detailed information about VPN negotiations, encryption algorithms, authentication failures, and other VPN-related issues, aiding in troubleshooting and resolving VPN connectivity problems.

Question: 810

When debugging Unified Policy matches, what does the 'match' keyword indicate in the debug output?

A. A rule has been bypassed
B. A connection was allowed
C. A rule has successfully matched a packet
D. A packet has been dropped

Answer: C

Explanation: The 'match' keyword in debug output indicates that a specific rule has successfully matched a packet, leading to further action based on that rule.

Question: 811
When is it appropriate to use the dbedit command?

A. To make changes to the running configuration
B. To directly edit the Management Database
C. To check the status of database connections
D. To restore a backup of the Management Server

Answer: B

Explanation: The dbedit command allows direct editing of the Management Database, which should be done with caution.

Question: 812
If you suspect a NAT issue, which command is best to verify the NAT configuration and its effects?

A. fw nat
B. fw tab -t nat -s
C. fw monitor
D. fw log

Answer: B

Explanation: The fw tab -t nat -s command displays statistics and configuration details about the NAT table, which is critical for troubleshooting NAT-related issues.

Question: 813
Which component of the Unified Policy helps in determining the decision path

for a traffic flow?

A. Security Gateway
B. Rule Base
C. Policy Layers
D. Threat Prevention

Answer: C

Explanation: Policy Layers are crucial in determining the decision path for traffic flows, as they dictate the order and criteria for rule evaluation.

Question: 814

Which command can be used to display the kernel routing table?

A. fw ctl route
B. fw tab -t routing
C. ip route show
D. netstat -r

Answer: C

Explanation: The command "ip route show" can be used to display the kernel routing table. It provides information about the network routes configured on the system, including the destination network, gateway, and interface.

Question: 815

Which command is used to display the current connections table in a Security Gateway?

A. fw tab -t connections

B. fw ctl conns
C. fw monitor -e "accept;"
D. fwaccel conns

Answer: A

Explanation: The command "fw tab -t connections" is used to display the current connections table in a Security Gateway. The connections table maintains information about the active connections passing through the gateway, including source and destination IP addresses, ports, and connection state. This command is useful for troubleshooting connection-related issues and monitoring the current connections on the gateway.

Question: 816
What does the output of vpn tu -s provide?

A. Status of VPN tunnels
B. Security association details
C. VPN configuration details
D. Summary of VPN users

Answer: A

Explanation: The vpn tu -s command provides a summary status of all VPN tunnels, helping to quickly assess the state of connections.

Question: 817

Which command can you use to verify the connectivity between two Check Point gateways in a VPN tunnel?

A. fw monitor
B. ping

C. tcpdump
D. traceroute

Answer: B

Explanation: The "ping" command can be used to verify the connectivity between two Check Point gateways in a VPN tunnel. By sending ICMP echo request packets, you can check if the gateways can reach each other, which can be helpful in troubleshooting VPN connectivity issues.

Question: 818

Which tool can be used to troubleshoot and debug issues related to policy installation and rule matching in Check Point R81.20?

A. SmartView Monitor
B. SmartConsole
C. cpview
D. tcpdump

Answer: B

Explanation: SmartConsole is the tool that can be used to troubleshoot and debug issues related to policy installation and rule matching in Check Point R81.20. It provides a graphical user interface (GUI) for managing security policies, rulebases, and objects. It allows administrators to analyze policy installation logs, check rule matching, and diagnose policy-related issues.

Question: 819
What command can you use to verify the status of a VPN tunnel on a Check Point gateway?

A. vpn tu

B. fw ctl pstat
C. cphaprob state
D. vpn stat

Answer: A

Explanation: The vpn tu command provides detailed information about VPN tunnels, including their status and statistics.

Question: 820

Which of the following commands can be used to troubleshoot issues with Check Point Anti-Bot?

A. fw ctl pstat
B. cpstat fw
C. fw monitor -e "accept (anti_bot=1) ;"
D. fw tab -t connections -s

Answer: B, C

Explanation: The "cpstat fw" command provides information about the state of Check Point Anti-Bot. The "fw monitor -e 'accept (anti_bot=1) ;'" command can be used to capture and analyze traffic related to Anti-Bot.

Question: 821
If SmartConsole is unable to connect due to a network issue, which command can help diagnose the connectivity?

A. ping
B. telnet
C. traceroute
D. All of the above

Answer: D

Explanation: All these commands can help diagnose different aspects of network connectivity issues affecting SmartConsole.

Question: 822
You are troubleshooting a connectivity issue with a VPN tunnel. Which log file should you check first to diagnose the problem?

A. fw.log
B. vpn.log
C. user.log
D. cp.log

Answer: B

Explanation: The vpn.log file contains detailed information about VPN connections, making it the first log to check for tunnel-related issues.

Question: 823
In the context of troubleshooting, what does the fw ctl pstat command display?

A. The policy installation status.
B. The current CPU and memory usage of the firewall.
C. The connection table statistics.
D. The status of the VPN tunnels.

Answer: B

Explanation: The fw ctl pstat command provides information about the current CPU and memory usage of the firewall, which can help in diagnosing performance issues.

Question: 824

Which command is used to verify the connectivity between two Security Gateways in a cluster?

A. cphaprob state
B. fw ctl pstat
C. cphaprob -a if
D. fw ctl affinity -l

Answer: A

Explanation: The correct command to verify the connectivity between two Security Gateways in a cluster is "cphaprob state." This command displays the state of the cluster members and provides information about their connectivity status. Option B, "fw ctl pstat," displays the status of the firewall kernel and its various components but does not specifically verify connectivity between cluster members. Option C, "cphaprob -a if," shows the interface status of the cluster members but does not directly verify connectivity. Option D, "fw ctl affinity -l," displays the CPU affinity settings and is not used for verifying cluster connectivity.

Question: 825
In CPView, which section provides real-time data on CPU and memory usage?

A. System Resources
B. Traffic Statistics
C. Process Overview
D. Connection Status

Answer: A

Explanation: The "System Resources" section in CPView displays real-time data regarding CPU and memory usage.

Question: 826

Emily is troubleshooting a NAT-related issue on a Check Point firewall running R81.20. She wants to view the current NAT translation table entries. Which command should Emily use?

A. fw tab -t fwx_alloc
B. fw tab -t nat
C. fw ctl pstat
D. cpstat fw

Answer: B

Explanation: To view the current NAT translation table entries, Emily should use the "fw tab -t nat" command. This command displays the contents of the NAT table, which contains the active NAT translations performed by the firewall.

Question: 827

Which command is used to verify the synchronized state of the cluster members?

A. cphaprob state
B. fw ctl affinity -l
C. fw monitor -e "accept;"
D. cpwd_admin list

Answer: A

Explanation: The command "cphaprob state" is used to verify the synchronized state of the cluster members in a Check Point cluster. It displays the current state of each cluster member, indicating whether they are active, standby, or in a fault state. This command is useful for troubleshooting cluster-related issues and ensuring the proper functioning of the cluster.

Question: 828

Which command is used to reset the VPN client configuration on a remote machine?

A. vpn reset
B. vpn client reset
C. vpn client config
D. vpn config reset

Answer: B

Explanation: The vpn client reset command resets the VPN client configuration on the remote machine, which can resolve configuration-related issues.

Question: 829

Which command is used to display the status of the SecureXL device?

A. fwaccel stat
B. fw ctl affinity -l
C. fwaccel conns
D. fw tab -t connections

Answer: A

Explanation: The command "fwaccel stat" is used to display the status of the SecureXL device. It provides information about the current state of SecureXL, including whether it is enabled or disabled and the number of connections accelerated.