CheckPoint 156-582 CCTA Practice Questions

Shared by Whitley on 24-08-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

What does the FWD daemon instruct the gateway to do when communication issues between the gateway and SMS/Log Server occur?

Options:

A- It instructs the gateway to continue forwarding logs to SMS/Log Server and the logs will be stored in a holding queue for the server until communication is restored.
B- It instructs the gateway to stop logging until it can restore communication.
C- It instructs the gateway to store logs locally as it continues to try to restore communication.
D- It instructs the gateway to only log a specified number of logs as defined in the Security Policy.

Answer:

C

Explanation:

When there are communication issues between the Security Gateway and the Security Management Server (SMS)/Log Server, the FWD daemon directs the gateway to store logs locally. This ensures that logging continues without interruption, and the logs are queued until communication with the SMS/Log Server is re-established, preventing any loss of log data.

Question 2

Question Type: MultipleChoice

What file extension should be used with fw monitor to allow the output file to be imported and read in Wireshark?

Options:

A- .pea
B- .exe
C- .cap
D- .tgz

Answer:

C

Explanation:

The .cap file extension is commonly used for packet capture files that can be imported and analyzed in Wireshark. When using fw monitor, specifying the output file with a .cap extension ensures compatibility with Wireshark for detailed packet analysis. Other extensions like .exe and .tgz are not suitable for packet captures, and .pea is not a standard extension for this purpose.

Question 3

Question Type: MultipleChoice

When managing the disk space for locally stored logs, the Delete threshold for the gateway cannot be more than what percentage of the total disk space?

Options:

A- 10%
B- 75%
C- 50%
D- 25%

Answer:

B

Explanation:

The Delete threshold for managing locally stored logs on a Security Gateway should not exceed 75% of the total disk space. This threshold ensures that there is ample space for new logs while preventing the disk from becoming overly full, which could lead to system instability or loss of logging capabilities.

Question 4

Question Type: MultipleChoice

Which option best is the most significant impact of not having a valid Policy Management license installed on a management server?

Options:

A- Inability to make rule changes
B- Inability to install policies
C- Inability to review logs
D- Inability to log in to SmartConsole

Answer:

B

Explanation:

Without a valid Policy Management license installed on the management server, administrators are unable to install policies to the Security Gateways. This prevents the deployment of updated security rules and configurations, leaving the network potentially vulnerable to threats. Other functionalities like making rule changes or reviewing logs might still be accessible, but the core capability to enforce policies is compromised.

Question 5

Question Type: MultipleChoice

You want to collect diagnostics data to include with an SR (Service Request). What command or utility best meets your needs?

Options:

A- cpconfig
B- cpinfo
C- cpplic
D- contracts_mgmt

Answer:

B

Explanation:

The cpinfo command is designed to collect comprehensive diagnostic information from a Check Point gateway or management server. This data is essential when submitting a Service Request (SR) to Check Point Support, as it includes configuration details, logs, and system information. cpconfig is used for configuration, cpplic manages licenses, and contracts_mgmt handles contract management, none of which are specifically tailored for collecting diagnostic data for SRs.

P2P exams

Question 6

Question Type: MultipleChoice

After manipulating the rulebase and objects with SmartConsole the application crashes and closes immediately. To troubleshoot, you will need to review the crash report. In which directory on the host PC will you find this report?

Options:

A- <FW1 Directory>\data\crash_report
B- <SmartConsole Directory>\data\crash_report\
C- It instructs the gateway to continue forwarding logs to SMS/Log Server and the logs will be stored in a holding queue for the server until communication is restored.
D- <SmartConsole Directory>\crash_report\data\

P2P exams

Answer:

B

Explanation:

Crash reports for SmartConsole are typically located in the <SmartConsole Directory>\data\crash_report\ directory on the host PC. Reviewing these reports provides insights into why the application crashed, including error messages and stack traces, which are essential for diagnosing and resolving the underlying issues.

Question 7

Question Type: MultipleChoice

Check Point's self-service knowledge base of technical documents and tools covers everything from articles describing how to fix specific issues, understand error messages and to how to plan and perform product installation and upgrades. This knowledge base is called:

Options:

A- SupportCenterBase
B- SecureDocs
C- SupportDocs
D- SecureKnowledge

Answer:

D

Explanation:

Check Point's self-service knowledge base is known as SecureKnowledge. It provides a comprehensive repository of technical documents, guides, troubleshooting steps, and tools necessary for managing and resolving issues related to Check Point products. The other options listed are either incorrect or do not represent the official name of Check Point's knowledge base.

Question 8

Question Type: MultipleChoice

When accessing License Status In Smart Console, what information is available?

Options:

A- Blade Name, License Status, Expiration Date, Additional info
B- Expiration Date, Status, SKU, Signature Key
C- Blade Name, Expiration Date, Attached to, Status
D- License Status, Blade Name, Report available, Download

Answer:

C

Explanation:

In SmartConsole, when accessing the License Status, the following information is available:

Blade Name: Identifies the specific security blade the license pertains to.

Expiration Date: Indicates when the license will expire.

Attached to: Shows which device or component the license is attached to.

Status: Reflects the current state of the license (e.g., active, expired).

This information helps administrators monitor and manage their licenses effectively, ensuring that all security features remain operational.

Question 9

Question Type: MultipleChoice

Check Point provides tools & commands to help you identify issues about products and applications. Which Check Point command can help you display status and statistics information for various Check Point products and applications?

Options:

A- cpstat
B- CP-stat
C- CPview
D- fwstat

Answer:

A

Explanation:

The cpstat command is a versatile tool provided by Check Point to display status and statistics for various Check Point products and applications. It offers insights into system performance,

service statuses, and resource utilization, which are essential for diagnosing and resolving issues effectively.

Question 10

Question Type: MultipleChoice

How do you verify that Proxy ARP entries are loaded into the kernel?

Options:

A- fw ctl arp
B- show arp dynamic all
C- This information can be viewed in the logs, under NAT section of log, field: Proxy ARP entry
D- fw ctl get arp list all

Answer:

A

Explanation:

The fw ctl arp command is used to verify that Proxy ARP entries are loaded into the kernel. This command provides detailed information about the current ARP table, including any Proxy ARP entries that have been established for NAT configurations. Ensuring that these entries are present confirms that the system is correctly handling ARP requests for NATed addresses.

To Get Premium Files for 156-582 Visit

https://www.p2pexams.com/products/156-582

For More Free Questions Visit

https://www.p2pexams.com/checkpoint/pdf/156-582