

Check Point Certified Troubleshooting Expert R81.20

CCTE

Dieser Kurs vermittelt fortgeschrittene Troubleshooting-Fähigkeiten, um komplexere Probleme, die bei der Verwaltung Ihrer Check Point-Sicherheitsumgebung auftreten können, zu untersuchen und zu lösen. Dieser Kurs ist die ideale Ergänzung im Anschluss an die Zertifizierung zum CCSE.

Kursinhalt

- Introduction to Advanced Troubleshooting
- Advanced Management Server Troubleshooting
- Advanced Troubleshooting with Logs and Events
- Advanced Gateway Troubleshooting
- Advanced Firewall Kernel Debugging
- Advanced Access Control Troubleshooting
- Advanced Identity Awareness Troubleshooting
- Advanced Site-to-Site VPN Troubleshooting
- Advanced Client-to-Site VPN Troubleshooting

E-Book Sie erhalten die englischen Original-Unterlagen als Check Point e-Kit.

Zielgruppe

Dieser Kurs richtet sich an Sicherheitsexperten und Check Point-Reseller, die sich das notwendige Wissen aneignen möchten, um bei der Verwaltung ihrer Sicherheitsumgebungen fortgeschrittene Fähigkeiten zur Fehlerbehebung zu erlangen. Wer die Zertifizierung zum CCTE anstrebt, der sollte diesen Kurs besuchen.

Voraussetzungen

Die Teilnehmer sollten über das Wissen aus dem Kurs Check Point Certified Security Expert R81.20 – CCSE verfügen. Für das Ablegen der CCTE Zertifizierung wird eine bestehende oder abgelaufene CCSE Zertifizierung (R80 oder höher) vorausgesetzt.

Weiterhin sind Kenntnisse zu den Themen UNIX- und/oder Windows-Betriebssysteme, der Netzwerktechnik TCP/IP sowie der Check Point Sicherheitsprodukte hilfreich, um diesen Kurs erfolgreich abzuschließen.

Kursziel

- Linux- und Check Point-Befehle sowie -Werkzeuge zur Systemüberwachung, Dateibearbeitung und Dateianzeige identifizieren und verwenden.
- Identifizieren und Verwenden der entsprechenden Befehle/Tools zur Fehlersuche und Debug-Befehle/Tools zur Behebung von Problemen mit Management Server und API Server.
- Untersuchung und Fehlerbehebung von verkehrs- oder sicherheitsrelevanten Problemen mit Hilfe von Tools zur Überwachung von Protokollen und Ereignissen.
- Identifizierung und Verwendung geeigneter Befehle/Tools zur Fehlerbehebung und Debugging-Befehle/Tools zur Behebung fortgeschrittener Security Gateway-Probleme.
- Demonstration von Kenntnissen über fortgeschrittene Tools zur Fehlersuche und Techniken zur Kernel-Fehlersuche.
- Identifizierung und Verwendung geeigneter Fehlerbehebungs- und Debugging-Befehle/Tools zur Lösung fortgeschrittener Probleme bei der Zugriffskontrolle.
- Identifizieren und Anwenden der entsprechenden Fehlerbehebungs- und Debug-Befehle/Tools, um fortgeschrittene Identity Awareness Probleme zu beheben.
- Identifizierung und Verwendung geeigneter Fehlerbehebungs- und Debug-Befehle/Tools zur Lösung fortgeschrittener Probleme bei der Site-to-Site-VPN-Fehlerbehebung.
- Identifizierung und Verwendung der geeigneten Befehle/Tools zur Fehlerbehebung und Fehlersuche, um fortgeschrittene Probleme bei der Client-to-Site-VPN-Fehlerbehebung zu lösen.

Stand 25.04.2025

Dieser Kurs im Web



Alle tagesaktuellen Informationen und Möglichkeiten zur Bestellung finden Sie unter dem folgenden Link: www.experteach.de/go/CCTE

Vormerkung

Sie können auf unserer Website einen Platz kostenlos und unverbindlich für 7 Tage reservieren. Dies geht auch telefonisch unter 06074 4868-0.

Garantierte Kurstermine

Für Ihre Planungssicherheit bieten wir stets eine große Auswahl garantierter Kurstermine an.

Ihr Kurs maßgeschneidert

Diesen Kurs können wir für Ihr Projekt exakt an Ihre Anforderungen anpassen.

Training	Preise zzgl. MwSt.		
Termine in Deutschland	2 Tage	€ 1.995,-	
Termine in Österreich	2 Tage	€ 1.995,-	
Online Training	2 Tage	€ 1.995,-	
Termin/Kursort	Kursprache Deutsch		
03.07.-04.07.25	München	25.09.-26.09.25	Hamburg
03.07.-04.07.25	Online	25.09.-26.09.25	Online
07.08.-08.08.25	Frankfurt	04.12.-05.12.25	Online
07.08.-08.08.25	Online	04.12.-05.12.25	Wien

Check Point Certified Troubleshooting Expert R81.20

Check Point



EXPERTeach



Inhaltsverzeichnis

Check Point Certified Troubleshooting Expert R81.20 – CCTE

Übungen

Collect and read live and historical CPView data.
Troubleshoot CPM and SmartConsole login issues.
Restore a Management High Availability environment from a temporary Primary Down condition.
Troubleshoot SmartLog processes.
Collect and interpret user mode debugs.
Collect and interpret kernel debugs.
Debug Unified Policy Inspection in kernel to understand match process.
Debug the Identity Awareness user mode processes.
Collect and interpret Site-to-Site VPN Debugs.
Collect and interpret Remote Access VPN Debugs.

