CCSE, Check Point Certified Security Expert R81, préparation à la certification

Cours Pratique de 3 jours - 21h
Réf : CPW - Prix 2024 : 2 490CHF HT

Cette formation vous permettra d'acquérir l'ensemble des techniques et des méthodologies nécessaires au passage de l'examen pour l'obtention de la certification CCSE R81. Vous apprendrez à mettre en place des mécanismes avancés de clustering, de haute disponibilité et de qualité de service (QoS).

OBJECTIFS PÉDAGOGIQUES

À l'issue de la formation l'apprenant sera en mesure de :

Effectuer les mises à jour

Résoudre des problèmes d'accès utilisateur détectés lors de la mise en œuvre avec Identity Awareness

Mettre en œuvre un cluster en haute disponibilité et Load Sharing

Préparer l'examen officiel menant à la certification CCSE

CERTIFICATION

Pour passer l'examen de certification, il suffit de vous inscrire sur le site de Check Point. Vous pouvez ensuite passer l'examen directement en ligne ou dans un centre agréé. Il faudra posséder la certification CCSA.

LE PROGRAMME

dernière mise à jour : 09/2022

1) Gaia avancée & API

- Gaia en ligne de commandes.
- Présentation de l'API.
- Créer des objets et règles via l'API.

Travaux pratiques : Installation du SMS et des GWs en R81.
Utilisation de l'API pour créer des objets et règles de base.

2) Mise à niveau de Gaia

- Methodes de mise à niveau de Gaia.
- Mise à jour/niveau centralisé des passerelles.

Travaux pratiques : Methodes de mise à niveau de Gaia.
Mise à jour/niveau centralisé des passerelles.

3) Les processus Check Point

- Principaux processus Check Point.
- Commandes pour visualiser les processus Check Point.
- Les scripts et les « SmartTasks ».

Travaux pratiques : Configurer SmartTasks.

4) Installation de la politique de sécurité

- Processus d'installation de la politique de sécurité.
- Installation Accélérée.
- Policy Packages & Layers.
- Objets Dynamiques.

PARTICIPANTS

Technicien, administrateur et ingénieur système/réseaux/sécurité.

PRÉREQUIS

Bonnes connaissances de TCP/IP, de la sécurité des SI et des principales fonctions de Check Point ou avoir suivi le stage "CCSA, Check Point Certified Security Administrator R81" (Réf. CPQ).

COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum cinq à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

MODALITÉS D'ÉVALUATION

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques…
Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

MOYENS PÉDAGOGIQUES ET TECHNIQUES

• Les moyens pédagogiques et les méthodes d'enseignement utilisés sont principalement : aides audiovisuelles, documentation et support de cours, exercices pratiques d'application et corrigés des exercices pour les stages pratiques, études de cas ou présentation de cas réels pour les séminaires de formation.
• À l'issue de chaque stage ou séminaire, ORSYS fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques.
• Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le stagiaire a bien assisté à la totalité de la session.

MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Vous avez un besoin spécifique d'accessibilité ? Contactez Mme FOSSE, référente handicap, à l'adresse suivante psh-accueil@orsys.fr pour étudier au mieux votre demande et sa faisabilité.

- Updatable Objects.
Travaux pratiques : Vérification des fichiers d'installation.
Création des objets dynamiques.

5) Kernel operations & Traffic flow
- Circulation des paquets à l'intérieur de la passerelle.
- Chaînes de modules.
- L'outil « fw monitor ».
- Management Data Plane Separation (MDPS).
Travaux pratiques : Utilisation de l'outil « fw monitor ».

6) SecureXL & CoreXL
- L'accélération SecureXL et ses templates.
- Commandes de SecureXL.
- CoreXL et SND (Secure Network Distributor).
- CoreXL Affinity.
- Dynamic Balancing.
- Multi-Queue.
- Le CoreXL Dynamic Dispatcher.
- Priority Queues (PrioQ).

7) VPN IPSEC site to site
- L'architecture du VPN. Les bases du chiffrement.
- Introduction à IKE et IPSec.
- L'autorité de certification (CA). Le Domain-Based VPN.
- Mode Simplifié. Configuration des communautés VPN.
- Le routage VPN.
Travaux pratiques : VPN-IPSec Inter-sites (Shared Secret).
VPN-IPSec Inter-sites (Certificats).

8) Accès Distant
- Le VPN SSL et le VPN IPSec.
- Le Blade Mobile Access.
- Mobile Access du type : « Remote Access ».
- Mobile Access SSL : Clientless Applications & Native Applications. SSL Network Extender (SNX).
- Portail « Check Point Mobile ».
- Les clients VPN couche 3.
Travaux pratiques : Mise en place d´une connexion VPN de type « Remote Access » via le client « Check Point Mobile ».
Mise en place d´une connexion VPN de type « Mobile Access SSL ».

9) Logs & monitor
- Présentation de l'onglet Logs & Monitor.
- SmartEvent.
- Compliance.
- SmartEvent GUI Client.
- Suspicious Activity Monitoring (SAM).
Travaux pratiques : Configuration de SmartEvent.

10) Le clustering
- La redondance des firewalls.
- Le ClusterXL High Availability (Actif/Passif).
- Le ClusterXL Load Sharing.
- Load Sharing Multicast.
- Le ClusterXL High Availability (Actif/Actif).
- VMAC et les problématiques d'ARP.

- La haute disponibilité du Management Server.
Travaux pratiques : Mise en œuvre de ClusterXL en mode High Availability.

LES DATES

CLASSE À DISTANCE
2024 : 18 sept., 11 déc.