Windows 2019, sécuriser son infrastructure

Cours Pratique de 4 jours - 28h
Réf : WCH - Prix 2024 : 2 550CHF HT

Acquérez les connaissances nécessaires pour sécuriser votre environnement Windows Server 2019, mettre en œuvre les outils de sécurité qui y sont intégrés. Vous verrez comment sécuriser l'OS, l'Active Directory, créer une architecture PKI, protéger vos données et vos accès réseaux.

OBJECTIFS PÉDAGOGIQUES

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

Maitriser les paramètres de base pour sécuriser Windows Serveur 2019

Savoir gérer les certificats

Etre capable de sécuriser l'AD

Savoir protéger ses données

Protéger l'accès au réseau

LE PROGRAMME

dernière mise à jour : 06/2021

1) Architecture de Windows Serveur 2019

- Fonctionnalités de sécurité de Windows serveur 2019.
- Nouveautés des services de domaine AD. Credential Guard, Device Guard.
- Windows Admin Center (WAC). Insights système.
- Rôle de l'AD pour la sécurité, l'orientation cloud.
- Ouverture de session et authentification : NTLM et Kerberos.
- Contrôle d'accès dynamique des comptes utilisateur.
- Le firewall avancé de Windows 2019 Server.

Travaux pratiques : Paramétrages de base pour sécuriser un serveur Windows 2019.

2) Autorité de certification et architecture PKI

- Gestion des certificats et des clés privées. Architecture PKI à 2 niveaux.
- Le rôle de serveur de certificats.
- Gérer les certificats depuis la MMC.
- Le rôle répondeur en ligne.

Travaux pratiques : Administration de base d'un serveur de certificats. Sécuriser les accès Web avec HTTPS.

3) Les services de fédération AD

- Installer le rôle ADFS.
- Installer le serveur WAP. Importer des certificats.
- Créer des relations de confiance.

Travaux pratiques : Mise en place des services de fédération AD, Sécuriser l'AD. Installation et paramétrage du WAP.

4) Gérer les identités

- Attribuer des droits à des utilisateurs.
- Mettre en place la délégation utilisateur.

PARTICIPANTS

Administrateurs et ingénieurs systèmes.

PRÉREQUIS

Bonnes connaissances de TCP/IP, de l'administration de Windows Server 2019 et de l'Active Directory.

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.

- Installer et configurer LAPS. Mettre à jour le schéma AD.
Travaux pratiques : Mettre en place une politique de gestion des droits utilisateurs. Utiliser LAPS. Mettre en place la délégation utilisateur.

5) Sécurisation de l'AD
- Sécuriser l'AD : principes de base.
- Nouveautés des services de certificats AD-CS.
- RODC (Read Only Domain Controler) : intérêt et mise en œuvre.
- Protection par ACL (liste de contrôle d'accès).
Travaux pratiques : Sécuriser l'AD. Granularité des mots de passe. Installer et paramétrer un RODC.

6) Protection des données
- La sécurité NTFS, ReFS.
- Mise en place d'EFS.
- BitLocker : cryptage du disque et stockage de la clé de cryptage.
- Installer Microsoft BitLocker Administration and Monitoring.
- Configurer le client MBAM via les stratégies de groupe AD.
Travaux pratiques : Mise en place d'EFS. Récupérer des données avec un agent. Installer MBAM.

7) NPS, VPN et IP Sec
- VPN : principe du tunneling.
- Sécuriser l'accès au domaine avec IPSec.
- Les serveurs NPS. Composants d'une infrastructure RADIUS.
Travaux pratiques : Mise en œuvre d'IPSec. Paramétrage avancé du firewall. Mise en place d'un serveur RADIUS. Limiter l'accès au réseau pour les machines non conformes avec DHCP.

LES DATES

CLASSE À DISTANCE
2024 : 28 mai, 10 sept., 19 nov.