Date de publication : 15/01/2025

Formation : Windows 2022, sécuriser son infrastructure

Formation pratique - 4j - 28h00 - Réf. WSF
Prix : 2260 € H.T.

★★★★★ 5 / 5

Sécurisez votre infrastructure Windows Server 2022 avec cette formation technique et complète ! Maîtrisez les technologies de protection avancées, du Credential Guard aux certificats PKI. Apprenez à verrouiller vos identités, chiffrer vos données et sécuriser vos accès réseau.

Objectifs pédagogiques

À l'issue de la formation, le participant sera en mesure de :

- Maîtriser les nouvelles fonctionnalités de sécurité de Windows Server 2022 (Credential Guard, Device Guard, VBS)
- Sécuriser l'infrastructure Active Directory et gérer les identités utilisateurs
- Mettre en place et administrer une infrastructure de gestion des certificats (PKI)
- Protéger les données par le chiffrement (EFS, BitLocker) et la gestion des systèmes de fichiers
- Configurer les mécanismes de contrôle d'accès et de délégation des droits
- Sécuriser les accès réseau avec des technologies comme VPN, IPSec et RADIUS
- Mettre en place des mécanismes de protection DNS et des contrôleurs de domaine sécurisés

Public concerné

Administrateurs et ingénieurs systèmes.

Prérequis

Bonnes connaissances de TCP/IP, de l'administration de Windows Server 2019/2022 et de l'Active Directory.

Vérifiez que vous avez les prérequis nécessaires pour profiter pleinement de cette formation en faisant ce test.

PARTICIPANTS

Administrateurs et ingénieurs systèmes.

PRÉREQUIS

Bonnes connaissances de TCP/IP, de l'administration de Windows Server 2019/2022 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.

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.

Programme de la formation

1 Architecture de Windows Serveur 2022

- Fonctionnalités de sécurité et bonnes pratiques pour Windows 2022.
- Nouveautés des services de domaine AD, Credential Guard, Device Guard.
- Serveur Secured-core, Racine de confiance matérielle.
- Sécurité basée sur la virtualisation (VBS).
- Windows Admin Center pour gérer Windows Server 2022.
- Contrôle d'accès dynamique des comptes utilisateur.
- Mettre en place un audit de sécurité via les outils spécifiques.

Travaux pratiques

Paramétrages et audit de base pour sécuriser un serveur Windows 2022.

2 Autorité de certification et architecture PKI

- Présentation et rôles des CA (Autorités de certifications).
- Installation et mise en oeuvre du rôle Serveur de Certificats (PKI).
- Création et administration de modèles spécifiques de certificats.
- Gérer les certificats depuis WAC et les consoles MMC.
- Les certificats de recouvrements et 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

- Intérêt et mise en oeuvre du rôle ADFS.
- Gestion des certificats et Création des relations de confiance.
- Installer le serveur WAP. Importer des certificats adéquates.

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 via l'active directory
- Installer et configurer Windows LAPS et les GPO associées

Travaux pratiques

Mettre en place une politique de gestion des droits utilisateurs. Utiliser Windows LAPS. Mettre en place la délégation utilisateur.

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 formations pratiques, études de cas ou présentation de cas réels pour les séminaires de formation.
• À l'issue de chaque formation 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 participant 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

Pour toute question ou besoin relatif à l'accessibilité, vous pouvez joindre notre équipe PSH par e-mail à l'adresse psh-accueil@orsys.fr.

5 Sécurisation de l'AD

- Sécuriser l'AD : principes de base.
- Nouveautés des services de certificats AD-CS.
- RODC (Read Only Domain Controler) : scenarios de mise en oeuvre et intérêt.
- Mise en oeuvre du DNS SEC. Protection de zone DNS.
- Rôles et intérêts de l'ADAC (centre d'administration active directory).
- PSO pour la granularité des mots de passe intérêt et mise en oeuvre.

Travaux pratiques
Sécuriser l'AD. Granularité des mots de passe. Installer et paramétrer un RODC.

6 Protection des données

- La sécurité des systèmes de fichier NTFS et ReFS.
- Mise en place d'EFS et gestion des certificats de recouvrements.
- BitLocker : cryptage du disque et stockage de la clé de chiffrement.
- Centralisation des clefs dans l'AD via les stratégies de groupe.

Travaux pratiques
Mise en place du chiffrement. Récupération des données avec l'agent et les certificats associés.

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 (802.1x)

Travaux pratiques
Mise en oeuvre 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.

Dates et lieux

CLASSE À DISTANCE
2026 : 9 juin, 22 sep., 24 nov.

PARIS LA DÉFENSE
2026 : 2 juin, 15 sep., 17 nov.