Date de publication : 24/02/2026

Formation : Windows 2025, sécuriser son infrastructure

Formation pratique - 4j - 28h00 - Réf. WSX
Prix : 2640 CHF H.T.

NEW

Objectifs pédagogiques

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

- Maîtriser les nouvelles fonctionnalités de sécurité de Windows Server 2025 (VBS, Credential Guard, Device Guard, OSConfig)
- Sécuriser l'infrastructure Active Directory 2025 et gérer les identités utilisateurs
- Mettre en place et administrer une infrastructure de gestion des certificats (PKI) avec AD CS
- Protéger les données par le chiffrement (EFS, BitLocker, NTFS/ReFS)
- Configurer les mécanismes de contrôle d'accès et de délégation des droits dans Active Directory
- Sécuriser les accès réseau et distants avec SMB over QUIC, VPN et NPS/RADIUS
- Renforcer la sécurité DNS et les contrôleurs de domaine (DNSSEC, RODC, comptes privilégiés)

Prérequis

Connaissances de base de l'utilisation des systèmes d'exploitation en réseau.

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

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

PARTICIPANTS

PRÉREQUIS

Connaissances de base de l'utilisation des systèmes d'exploitation en réseau.

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.

1 Architecture de Windows Serveur 2025

- Fonctionnalités de sécurité et bonnes pratiques pour Windows 2025.
- Les étapes clés pour sécuriser Windows Server 2025.
- Apport du nouveau niveau de fonctionnalité des services Active Directory.
- Sécurité basée sur la virtualisation (VBS).
- Mise en œuvre de Credential Guard, Device Guard.
- OSConfig sous Windows 2025 (DSC nouvelle génération).
- Windows Admin Center 2025 (version serveur natif).
- Le contrôle d'accès dynamique des comptes utilisateur.
- Mise en place d'un audit de sécurité via les outils spécifiques.

Travaux pratiques

Paramétrages et audit de base pour sécuriser un serveur Windows 2025.

2 Autorité de certification et architecture PKI

- Présentation et rôles des CA (autorités de certifications).
- Nouveautés et améliorations ADCS (Active Directory Certificate Services).
- Installation et mise en œuvre du rôle serveur de certificats (PKI).
- Création et gestion des certificats via les MMC et Windows Admin Center (WAC).
- Création et administration de modèles de certificats spécifiques Windows 2025.
- Le rôle répondeur en ligne. Amélioration OCSP (environnements hybrides).
- Les certificats de recouvrements et le rôle répondeur en ligne.

Travaux pratiques

Administration basique d'un serveur de certificats. Sécuriser les accès web avec HTTPS

3 Les services de fédération AD et Microsoft Entra ID

- Intérêt et mise en œuvre du rôle ADFS, quand ADFS reste pertinent en 2025.
- Gestion des certificats et création des relations de confiance.
- Entra ID et les fonctionnalités modernes (MFA, Conditional Access, Passwordless, Identity Protection).
- Installer le serveur WAP et la publication de l'ADFS vers l'extérieur.
- Le rôle de Web Application Proxy (WAP) version 2025.

Travaux pratiques

Mise en place des services de fédération AD, sécuriser l'AD. Installation et paramétrage du WAP.

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.

4 Gérer les identités

- Gestion de Credential Guard (protège les secrets » Kerberos/NTLM).
- LDAP signé et chiffré obligatoire.
- Attribuer des droits à des utilisateurs.
- Mettre en place la délégation utilisateur via l'active directory.
- Monitoring amélioré, les journaux enrichis : Kerberos, LDAP, réplication AD.
- Les nouveautés de 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.

5 Sécurisation de l'AD

- Nouveaux outils de diagnostic AD et améliorations , dcdiag, repadmin...
- Sécuriser l'AD : protection renforcée des comptes privilégiés isolation des processus LSASS.
- Nouveautés des services de certificats AD-CS "Le schéma 93" .
- RODC (Read Only Domain Controler) : scénarios de mise en œuvre et intérêt.
- Mise en œuvre 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 œuvre.

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 clés 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 SMB over QUIC, NPS 2025 et VPN

- Comparaison QUIC vs DirectAccess vs Always On VPN.
- Nouveautés VPN dans Windows Server 2025 (RRAS).
- Les serveurs NPS. Le durcissement du rôle NPS 2025.
- Composants d'une infrastructure RADIUS (802.1x).
- Always On VPN versus DirectAccess.
- VPN versus SMB over QUIC : lequel choisir?
- Le rôle de firewall dans Windows Server 2025 (qu'est-ce qui change ?).

Travaux pratiques

Mise en œuvre du SM over QUIC via Windows Admin Center, Always On VPN "Pourquoi c'est la solution moderne". Mise en place d'un serveur RADIUS 2025. Paramétrage avancé du firewall.

Dates et lieux

CLASSE À DISTANCE
2026 : 7 juil., 1 sep., 1 déc.