



ORGANISME DE FORMATION AUX TECHNOLOGIES ET METIERS DE L'INFORMATIQUE

Formation Windows 2022, sécuriser son infrastructure

N° ACTIVITÉ : 11 92 18558 92

TÉLÉPHONE : 01 85 77 07 07

E-MAIL : inscription@hubformation.com

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.

Référence	WSF
Durée	4 jours (28h)
Tarif	2 650 €HT

Objectifs

- | 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

- | Administrateurs et ingénieurs système

Prérequis

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

Programme de la formation

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.

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.

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.

SESSIONS PROGRAMMÉES

A DISTANCE (FRA)

le 22 septembre 2026

le 24 novembre 2026

PARIS

le 15 septembre 2026

le 17 novembre 2026

[VOIR TOUTES LES DATES](#)

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

Sécurisation de l'AD

- | Sécuriser l'AD : principes de base.
- | Nouveautés des services de certificats AD-CS.
- | RODC (Read Only Domain Controller) : scénarios 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.

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.

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)

Méthode pédagogique

Chaque participant travaille sur un poste informatique qui lui est dédié. Un support de cours lui est remis soit en début soit en fin de cours. La théorie est complétée par des cas pratiques ou exercices corrigés et discutés avec le formateur. Le formateur projette une présentation pour animer la formation et reste disponible pour répondre à toutes les questions.

Méthode d'évaluation

Tout au long de la formation, les exercices et mises en situation permettent de valider et contrôler les acquis du stagiaire. En fin de formation, le stagiaire complète un QCM d'auto-évaluation.

Suivre cette formation à distance

Voici les prérequis techniques pour pouvoir suivre le cours à distance :

- | Un ordinateur avec webcam, micro, haut-parleur et un navigateur (de préférence Chrome ou Firefox). Un casque n'est pas nécessaire suivant l'environnement.
- | Une connexion Internet de type ADSL ou supérieure. Attention, une connexion Internet ne permettant pas, par exemple, de recevoir la télévision par Internet, ne sera pas suffisante, cela engendrera des déconnexions intempestives du stagiaire et dérangera toute la classe.
- | Privilégier une connexion filaire plutôt que le Wifi.
- | Avoir accès au poste depuis lequel vous suivrez le cours à distance au moins 2 jours avant la formation pour effectuer les tests de connexion préalables.
- | Votre numéro de téléphone portable (pour l'envoi du mot de passe d'accès aux supports de cours et pour une messagerie instantanée autre que celle intégrée à la classe virtuelle).
- | Selon la formation, une configuration spécifique de votre machine peut être attendue, merci de nous contacter.
- | Pour les formations incluant le passage d'une certification la dernière journée, un voucher vous est fourni pour passer l'examen en ligne.
- | Pour les formations logiciel (Adobe, Microsoft Office...), il est nécessaire d'avoir le logiciel installé sur votre machine, nous ne fournissons pas de licence ou de version test.
- | Horaires identiques au présentiel.

Accessibilité



Les sessions de formation se déroulent sur des sites différents selon les villes ou les dates, merci de nous contacter pour

vérifier l'accessibilité aux personnes à mobilité réduite.
Pour tout besoin spécifique (vue, audition...), veuillez nous contacter au 01 85 77 07 07.