WINDOWS SERVER 2025 : SECURISER SON INFRASTRUCTURE

Public	Professionnels de l'administration systèmes et réseaux. Acteurs techniques des infrastructures IT. Responsables et techniciens en environnement systèmes et réseaux.
Durée	4 jours - 28 heures
Pré-requis	Avoir des connaissances de base en utilisation des systèmes d'exploitation en environnement réseau
Objectifs	Maîtriser les fonctionnalités avancées de sécurité de Windows Server 2025 : VBS, Credential Guard, Device Guard et OSConfig Sécuriser l'infrastructure Active Directory Domain Services et gérer les identités utilisateurs Mettre en place et administrer une infrastructure de certificats (PKI) avec Active Directory Certificate Services Protéger les données par le chiffrement : EFS, BitLocker et systèmes de fichiers NTFS / ReFS Configurer les mécanismes de contrôle d'accès et de délégation des droits dans Active Directory Sécuriser les accès réseau et distants : SMB over QUIC, VPN et Network Policy Server (RADIUS) Renforcer la sécurité des services critiques : DNS (DNSSEC), contrôleurs de domaine (RODC) et gestion des comptes privilégiés
Méthodes pédagogiques	Pour bien préparer la formation, le stagiaire remplit une évaluation de positionnement et fixe ses objectifs à travers un questionnaire. La formation est délivrée en présentiel ou distanciel (e-learning, classe virtuelle, présentiel et à distance). Le formateur alterne entre méthodes démonstratives, interrogatives et actives (via des travaux pratiques et/ou des mises en situation). La validation des acquis peut se faire via des études de cas, des quiz et/ou une certification. Cette formation est animée par un consultant-formateur dont les compétences techniques, professionnelles et pédagogiques ont été validées par des diplômes et/ou testées et approuvées par l'éditeur et/ou par Audit Conseil Formation.
Moyens techniques	1 poste de travail complet par personne De nombreux exercices d'application Mise en place d'ateliers pratiques Remise d'un support de cours Passage de certification(s) dans le cadre du CPF Remise d'une attestation de stage
Modalité d'évaluation des acquis	Evaluation des besoins et objectifs en pré et post formation Evaluation technique des connaissances en pré et post formation Evaluation générale du stage
Délai d'accès	L'inscription à cette formation est possible jusqu'à 5 jours ouvrés avant le début de la session
Accessibilité handicapés	Au centre d'affaires ELITE partenaire d'ACF à 20 m. Guide d'accessibilité à l'accueil.

1 - COMPRENDRE L'ARCHITECTURE DE WINDOWS SERVER 2025

- Comprendre les fonctionnalités de sécurité et les bonnes pratiques sous Windows Server 2025
- Identifier les étapes clés pour sécuriser un environnement Windows Server 2025
- Appréhender les évolutions du niveau fonctionnel de Active Directory Domain Services
- Mettre en œuvre la sécurité basée sur la virtualisation (VBS)
- Déployer et configurer Credential Guard et Device Guard
- Utiliser OSConfig (DSC nouvelle génération) pour automatiser et renforcer la configuration sécurisée
- Exploiter Windows Admin Center (version serveur native) pour l'administration sécurisée
- Configurer le contrôle d'accès dynamique des comptes utilisateurs
- Mettre en place un audit de sécurité à l'aide des outils dédiés

2 - COMPRENDRE LE FONCTIONNEMENT D'UNE AUTORITÉ DE CERTIFICATION ET D'UNE INFRASTRUCTURE PKI

- Comprendre le rôle des autorités de certification (CA) dans une infrastructure PKI
- Découvrir les nouveautés et améliorations de Active Directory Certificate Services sous Windows Server 2025
- Installer et mettre en œuvre une infrastructure PKI avec le rôle serveur de certificats
- Créer et gérer les certificats via les consoles MMC et Windows Admin Center (WAC)
- Créer et administrer des modèles de certificats adaptés aux besoins sous Windows Server 2025
- Mettre en place le rôle de répondeur en ligne (OCSP) et exploiter ses améliorations, notamment en environnement hybride
- Gérer les certificats de récupération (recovery certificates) et leur intégration dans l'infrastructure PKI

3 - COMPRENDRE LES SERVICES DE FÉDÉRATION AVEC ACTIVE DIRECTORY FEDERATION SERVICES ET MICROSOFT ENTRA ID

- Comprendre les cas d'usage et la pertinence de Active Directory Federation Services en 2025
- Mettre en œuvre une infrastructure de fédération d'identités avec AD FS
- Gérer les certificats et configurer les relations de confiance dans un environnement fédéré
- Découvrir les fonctionnalités avancées de Microsoft Entra ID : MFA, Conditional Access, Passwordless et Identity Protection
- Installer et configurer Web Application Proxy (WAP) pour publier les services AD FS vers l'extérieur
- Comprendre le rôle et les évolutions du Web Application Proxy (version 2025)

4 - GÉRER LES IDENTITÉS SOUS WINDOWS SERVER 2025

- Mettre en œuvre Credential Guard pour protéger les secrets d'authentification (Kerberos / NTLM)
- Sécuriser les communications LDAP en imposant la signature et le chiffrement
- Attribuer et gérer les droits des utilisateurs dans un environnement Active Directory Domain Services
- Mettre en place la délégation des droits via Active Directory
- Exploiter les capacités de supervision avancée : journaux enrichis (Kerberos, LDAP, réplication AD)
- Découvrir et configurer les nouveautés de Windows LAPS ainsi que les stratégies de groupe (GPO) associées

5 - SÉCURISER UN ENVIRONNEMENT ACTIVE DIRECTORY DOMAIN SERVICES

- Exploiter les outils de diagnostic d'Active Directory : dcdiag, repadmin et leurs améliorations
- Renforcer la sécurité de Active Directory Domain Services : protection des comptes à privilèges et isolation du processus LSASS
- Découvrir les évolutions de Active Directory Certificate Services, notamment le schéma 93
- Mettre en œuvre un contrôleur de domaine en lecture seule (RODC) : cas d'usage et bénéfices
- Sécuriser les services DNS avec DNSSEC et la protection des zones
- Utiliser Active Directory Administrative Center (ADAC) pour l'administration centralisée
- Mettre en place des stratégies de mot de passe fines (PSO) pour gérer la granularité des mots de passe

6 - PROTÉGER LES DONNÉES SOUS WINDOWS SERVER 2025

- Sécuriser les systèmes de fichiers NTFS et ReFS
- Mettre en œuvre le chiffrement des fichiers avec EFS et gérer les certificats de récupération
- Déployer BitLocker pour le chiffrement des disques
- Centraliser la gestion des clés de chiffrement dans Active Directory Domain Services via les stratégies de groupe (GPO)

7 - SÉCURISER LES ACCÈS RÉSEAU AVEC SMB OVER QUIC, NETWORK POLICY SERVER ET VPN SOUS WINDOWS SERVER 2025

- Comparer les solutions d'accès distant : QUIC, DirectAccess et Always On VPN
- Découvrir les nouveautés VPN sous Windows Server 2025 via le rôle RRAS
- Comprendre le fonctionnement des serveurs Network Policy Server (NPS) et le durcissement du rôle en 2025
- Identifier les composants d'une infrastructure RADIUS (802.1X)
- Comparer les approches Always On VPN et DirectAccess : cas d'usage, avantages et limites
- Analyser les différences entre VPN et SMB over QUIC afin de choisir la solution adaptée
- Comprendre le rôle et les évolutions du pare-feu sous Windows Server 2025

NOUS CONTACTER

Siège social
16, ALLÉE FRANÇOIS VILLON
38130 ÉCHIROLLES

Téléphone
04 76 23 20 50 - 06 81 73 19 35

Suivez-nous sur les réseaux sociaux, rejoignez la communauté !

ACF Audit Conseil Formation

@ACF_Formation

Dernière mise à jour : 17/04/2026

PROFIL Formateur : Les formateurs sont recrutés selon plusieurs critères :
Expérience, pédagogie, dynamisme et prévoyance.