DAWAN

Plan de la formation

www.dawan.fr

Formation Windows Server 2016 : Sécuriser son infrastructure

Durée :	3 jours (21 heures)
Tarifs inter-entreprise :	2 225,00 CHF HT (standard) 1 780,00 CHF HT (remisé)
Public :	Administrateurs système
Pré-requis :	Connaissances en administration Windows Server 2016
Objectifs :	Connaître les outils permettant une meilleure gestion de la sécurité pour les OS Windows Server
Modalités pédagogiques, techniques et d'encadrement :	• Formation synchrone en présentiel et distanciel. • Méthodologie basée sur l'Active Learning : 75 % de pratique minimum. • Un PC par participant en présentiel, possibilité de mettre à disposition en bureau à distance un PC et l'environnement adéquat. • Un formateur expert.
Modalités d'évaluation :	• Définition des besoins et attentes des apprenants en amont de la formation. • Auto-positionnement à l'entrée et la sortie de la formation. • Suivi continu par les formateurs durant les ateliers pratiques. • Évaluation à chaud de l'adéquation au besoin professionnel des apprenants le dernier jour de formation.
Sanction :	Attestation de fin de formation mentionnant le résultat des acquis
Référence :	WIN100813-F
Note de satisfaction des participants:	4,82 / 5
Contacts :	commercial@dawan.fr - 09 72 37 73 73

Modalités d'accès :	Possibilité de faire un devis en ligne (www.dawan.fr, moncompteformation.gouv.fr, maformation.fr, etc.) ou en appelant au standard.
Délais d'accès :	Variable selon le type de financement.
Accessibilité :	Si vous êtes en situation de handicap, nous sommes en mesure de vous accueillir, n'hésitez pas à nous contacter à referenthandicap@dawan.fr, nous étudierons ensemble vos besoins

La sécurité du système d'exploitation Windows Server 2016

Option d'installation minimale et mode Core
Le contrôle des comptes utilisateur (UAC)
Le pare-feu Windows

Atelier : Paramétrages et réglages de base pour la sécurisation d'un serveur Windows 2016.

Correctifs sous Windows Server

Analyse de l'environnement : l'outil Hfnetchk
Scripts de gestion de correctif, déploiement

Atelier : Chaînage de correctifs, utilisation de MBSA.

Sécurisation de l'Active Directory

Principe de base pour la sécurité de l'AD
Protection des objets par les ACL
Les serveurs RODC : intérêt et mise en oeuvre

Atelier : Sécurisation de l'Active Directory. Granularité des mots de passe. Installation et paramétrage d'un RODC.

Cryptage, certificats et architecture PKI

Les bases de PKI
Gestion des certificats et des clés privées
Le rôle de serveur de certificats

Atelier : Mise en place d'un serveur de certificats. Administration de base

des certificats. Sécurisation des accès Web avec HTTPS.

L'authentification : la clé de la sécurité

Fonctionnement du protocole Kerberos
Kerberos avec les cartes à puces et la biométrie

Atelier : Tests du protocole Kerberos. Audit des accès.

La protection de données

Rappel sur les fondamentaux de la sécurité NTFS
Mise en place d'EFS. Limites d'EFS. BitLocker

Atelier : Mise en place d'EFS. Récupération de données avec un agent.

Contrôle d'accès dynamique : DAC

Principes et mise en place
Règles d'accès centralisées
Règles d'audit centrales

Atelier : Mise en place de contrôles d'accès dynamique sur un serveur de fichier Windows 2012 server

Etat désiré de configuration : DSC

Principes et installation
Configuration homogène de grappes de serveurs

Atelier : Installation d'un site web

Mise en place de la sécurité réseau

Sécurisation de l'accès au domaine avec IPsec
Configuration et administration du service RAS
Les VPN : principe du tunneling

Atelier : Mise en oeuvre d'IPSec sous Windows. Paramétrage avancé du firewall. Mise en place d'un serveur RAS et d'un serveur RADIUS sous Windows Server 2016.