DAWAN

Plan de la formation

www.dawan.fr

Formation PKI Microsoft AD CS : déploiement, administration et sécurisation

Durée :	3 jours (21 heures)
Tarif inter-entreprises :	2 475,00 CHF HT (Présentiel) 1 980,00 CHF HT (Distanciel)
Public :	Administrateurs systèmes Windows et Active Directory, ingénieurs systèmes et réseaux, administrateurs sécurité et techniciens d'exploitation chargés de déployer ou de maintenir une infrastructure de certificats Microsoft.
Pré-requis :	Maîtriser l'administration de Windows Server et d'Active Directory Domain Services : utilisateurs, groupes, permissions, DNS et stratégies de groupe. Posséder de bonnes connaissances des réseaux TCP/IP et savoir exécuter des commandes PowerShell simples. Aucune expérience préalable d'AD CS n'est nécessaire.
Objectifs :	Comprendre une PKI et les certificats X.509 - Déployer une hiérarchie AD CS - Configurer les modèles et l'inscription automatique - Gérer le renouvellement et la révocation - Sécuriser et dépanner la PKI - Sauvegarder et restaurer une autorité de certification.
Méthode pédagogique :	Alternance d'apports théoriques, de démonstrations et de travaux pratiques sur un environnement virtualisé préparé. Construction progressive d'une PKI à deux niveaux, résolution d'incidents et restauration guidée. Évaluation des acquis au fil des ateliers et synthèse finale.
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.

Modalité 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 :	WIN103129-F
Note de satisfaction des participants :	Pas de données disponibles
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

Comprendre les certificats et les infrastructures PKI

Identifier les usages des certificats : authentification, chiffrement et signature
Comprendre les clés publiques et privées, les signatures et les chaînes de confiance
Lire un certificat X.509 : identité, période de validité, usages de clé, usages étendus et noms alternatifs
Distinguer autorités de certification, certificats d’autorité et certificats utilisateurs ou machines
Repérer les magasins de certificats Windows et les dépendances des applications

Atelier : analyser plusieurs certificats et reconstituer leur chaîne de confiance à partir d’un cas d’entreprise.

Préparer l’architecture d’une PKI Microsoft

Définir les besoins et les responsabilités d’administration
Distinguer les autorités autonomes et les autorités intégrées à Active Directory
Préparer une architecture à deux niveaux : autorité racine autonome hors ligne et autorité subordonnée d’entreprise

Choisir les noms, les paramètres cryptographiques et les durées de validité
Planifier les points de publication des certificats d'autorité et des listes de révocation : AIA et CDP
Préparer les comptes, les permissions et les prérequis des serveurs

Atelier : compléter le dossier de conception de la PKI du laboratoire et préparer son plan de publication.

Déployer une hiérarchie d'autorités AD CS

Installer et configurer le rôle AD CS sur Windows Server
Préparer la configuration de l'autorité racine et le fichier CAPolicy.inf
Installer l'autorité subordonnée d'entreprise et faire signer sa demande par la racine
Publier les certificats d'autorité et les listes de révocation
Distribuer la confiance et vérifier les chemins de publication
Contrôler le fonctionnement initial de la PKI et organiser le maintien hors ligne de la racine

Atelier : déployer une PKI à deux niveaux dans l'environnement préparé et valider la chaîne de certification.

Configurer les modèles et les droits d'inscription

Distinguer création d'un modèle dans Active Directory et publication sur une autorité
Dupliquer un modèle et adapter ses paramètres au besoin métier
Configurer les usages de clé, les usages étendus, l'identité du sujet et les noms alternatifs
Définir les durées de validité, les périodes de renouvellement et la protection des clés privées
Attribuer les droits de lecture, d'inscription et d'inscription automatique à des groupes ciblés
Identifier les risques liés aux permissions excessives et aux identités renseignées librement

Atelier : créer et publier des modèles pour les ordinateurs et un service Web, puis vérifier les droits avec des comptes autorisés et non autorisés.

Délivrer, déployer et renouveler les certificats

Effectuer une demande manuelle avec les outils Windows et traiter son émission
Configurer l'inscription automatique des machines par stratégie de groupe
Vérifier la distribution et le renouvellement des certificats

Déployer un certificat sur un service IIS et valider une connexion HTTPS
Gérer les formats d'échange et les précautions liées à l'exportation des clés privées

Atelier : automatiser la délivrance de certificats aux postes du domaine, sécuriser un site IIS et tester un scénario de renouvellement.

Gérer la révocation et la disponibilité des informations de validation

Comprendre les motifs de révocation et les conséquences pour les applications
Publier et contrôler les listes de révocation : CRL de base et principes des CRL différentielles
Vérifier l'accessibilité des points CDP et AIA
Comprendre les caches et les délais de prise en compte de la révocation
Présenter le rôle d'un répondeur OCSP et observer son fonctionnement dans un scénario préparé

Atelier : révoquer un certificat, publier une CRL et diagnostiquer les résultats de validation ; démonstration guidée d'une vérification OCSP.

Sécuriser les autorités et les processus de délivrance

Protéger les serveurs, les comptes d'administration et les clés des autorités
Séparer les responsabilités et appliquer le principe du moindre privilège
Limiter les services d'inscription aux besoins identifiés et examiner les protections des interfaces exposées
Contrôler les modèles présentant un risque d'usurpation d'identité
Comprendre les exigences de liaison forte entre certificats d'authentification et comptes Active Directory
Activer les traces utiles et organiser la revue des opérations sensibles

Atelier : examiner la configuration du laboratoire, corriger des permissions excessives et analyser un échec d'authentification par certificat à partir des journaux fournis.

Administrer et dépanner la PKI

Utiliser les consoles AD CS, Enterprise PKI, certutil et les commandes PowerShell adaptées
Consulter les demandes, les certificats délivrés et les événements d'inscription
Surveiller les échéances des certificats d'autorité et des listes de révocation
Diagnostiquer les erreurs de chaîne, de modèle, de permissions et de publication
Construire une procédure de vérification avant et après modification

Atelier : résoudre plusieurs incidents préparés concernant une inscription refusée, une chaîne non approuvée et un point de révocation inaccessible.

Sauvegarder et restaurer une autorité de certification

Identifier les éléments à préserver : base de l’autorité, clés privées, configuration et fichiers de publication
Sauvegarder la configuration du registre, le fichier CAPolicy.inf et la liste des modèles publiés
Distinguer les éléments propres à l’autorité des modèles et objets conservés dans Active Directory
Protéger et vérifier les sauvegardes
Réaliser une restauration guidée dans un environnement isolé et contrôler la reprise du service
Formaliser les opérations récurrentes et les points de surveillance

Atelier : sauvegarder l’autorité du laboratoire, réaliser sa restauration guidée sur un environnement isolé et compléter une fiche d’exploitation de la PKI.