Formation PKI Mise en œuvre de services de certificats sous Windows Server 2016

Objectifs de la formation PKI Windows Server 2016

Les PKI (Public Key Infrastructure) du système d'exploitation Windows Serveur 2016 sont le fondement indispensable de la sécurité sous Windows 2016.

Cette formation vous permet d'en acquérir la maitrise, de l'implémentation à la gestion quotidienne, en passant par les cas d'utilisation pratique les plus fréquents.

Ce cours PKI Windows Server 2016 présente aussi les notions essentielles de la cryptographie, base de la PKI. La session est fortement orientée pratique et est illustrée de tous les cas les plus fréquents d'utilisation en entreprise.

À qui s'adresse cette formation ?

Public :

Ce stage PKI Windows Server 2016 s'adresse aux informaticiens, administrateurs systèmes et réseaux, spécialistes des architectures Microsoft, Ingénieurs systèmes souhaitant implémenter, gérer et dépanner une PKI Windows Serveur 2016.

Prérequis :

Pour suivre ce cours sur les PKI Windows Server 2016, il est demandé de posséder une expérience de base de la gestion de l'Active Directory, des réseaux et du système d'exploitation Microsoft Windows Serveur 2016.

Contenu du cours PKI Windows Server 2016

Cryptographie - Notions essentielles dans Windows Server 2016

Cryptage Symétrique
Cryptage Asymétrique
Structure des certificats
Combinaison des deux méthodes de cryptage
Les composantes d'une PKI d'entreprise

Autorité de certification sous Windows Server 2016

Type d'autorité de certification
Implémentation d'une autorité de certification d'entreprise

Demande manuelle de certificat

Inscription de certificats par MMC
Inscription de certificats par le navigateur Internet
Personnalisation de modèles de certificats

Déploiement automatique de certificats

Configuration des stratégies de groupe pour le déploiement automatique certificats
Mise à jour des modèles de certificats
Stockage des certificats dans l'Active Directory

Gestion de la révocation des certificats dans Windows Server 2016

Processus de révocation d'un certificat
Publication de la liste de révocation pour un accès externe

Serveur OCSP (Online Certificate Status Protocol)

Implémentation d'un serveur OCSP

Validation du répondeur en ligne OSCP

Archivage des certificats

Concept d'archivage et de récupération des certificats

Création des agents de récupération

Activation de l'archivage des certificats

Récupération de certificats archivés

Implémenter une architecture sécurisée (CA racine hors ligne)

Installer la CA racine hors ligne

Installer la CA émettrice secondaire en ligne Implémentation d'une autorité de certification secondaire

Valider le bon fonctionnement de l'architecture de PKI deux tiers

Application PKI - EFS (Encryptions File System)

Cryptage de fichiers

Ajout d'un menu contextuel pour le chiffrement

Tester l'accès aux fichiers cryptés

Partage de fichiers cryptés

Application PKI - Agent de récupération EFS

Génération des certificats d'agent de récupération

Modification de la stratégie

Récupération de fichiers cryptes

Exportation de certificat

Application PKI - Sécurisation de sites Web (SSL)

Fonctionnement de SSL

Inscription d'un certificat SSL

Liaison SSL

Test d'accès en SSL

Révocation de certificat SSL

Application PKI - Signature de code PowerShell

Certificat pour l'authentification et l'intégrité

Signature de code PowerShell

Révocation de certificat de signature de code

Application PKI – VPN (SSTP)

Implémenter un serveur VPN - SSTP

Valider la connexion au serveur

Révocation de certificat SSTP