

# Windows Server: Managing and Supporting Active Directory Certificate Services



## WorkshopPLUS

### Public concerné :

*Pour assurer la haute qualité du transfert d'expertise attendue par les participants, le nombre de personnes est limité à 16, répondant aux critères suivants :*

- *Avoir au minimum 2 à 3 ans d'expérience dans l'administration d'Active Directory*
- *Dont le titre de poste est :*
  - *Administrateur Système*
  - *Architecte/Ingénieur Sécurité*
  - *Architecte/Ingénieur Active Directory*

*Les informations détaillées combinées à la haute qualité pratique à travers les ateliers, préparent les participants au mieux pour manager et supporter « Windows Server 2016 – ADCS »*

## Introduction

Le Workshop “Windows Server: Managing and Supporting Active Directory Certificate Services” offre aux participants la connaissance et les compétences pour comprendre, planifier, configurer, administrer, monitorer et supporter un Serveur Windows basé sur une Infrastructure de clefs publiques (PKI).

Au travers des différents modules et ateliers connexes abordés, ce workshop de 3 jours se concentre essentiellement sur les compétences et les objectifs alignés sur le chiffrement de données, les « PKI basics », la consultation et révocation de certificat, la sécurité et le support.

Le contenu de ce workshop a été créé dans l'optique de pouvoir délivrer les différents modules qui le compose indépendamment les uns des autres, permettant ainsi de pouvoir se concentrer sur une partie spécifique si besoin.

## Principales caractéristiques et avantages

Ce workshop est bénéfique pour les entreprises souhaitant développer leur compréhension du management et du support de « Windows Server 2016 PKI » visant à améliorer la santé opérationnelle des PKI en implémentant des opérations effectives, du support et des bonnes pratiques de management avec pour objectif une planification d'une migration vers « Windows Server 2016 PKI »

## Plus-values techniques

Après avoir suivi cette formation, vous serez en mesure de :

- Comprendre les bases du chiffrement de données et l'utilisation des techniques modernes de chiffrement de données dans les « Operating System » actuels.
- Comprendre les bases d'une infrastructure de clefs publiques (PKI).
- Appréhender la notion de certificat et de certificat Active Directory.
- Comprendre comment « revocation checking » et « chain building » fonctionnent.
- Comprendre les notions de sécurité et de support pour « PKI ».

## Programme

Cet atelier dure 3 jours. Les participants sont invités à respecter les horaires pour en tirer le bénéfice maximum. Un départ anticipé ou une arrivée tardive ne sont pas recommandés.

### **Matériels requis :**

*Dans le cas d'un Workshop ouvert, le matériel nécessaire sera fourni. Pour plus d'informations veuillez contacter votre TAM.*

**Module 01 : Introduction à « PKI »** - Ce module introduit les composants d'un « PKI » et présente les différents designs de topologies disponibles pour déployer une Autorité de Certification et une « PKI hierarchy », incluant les autorités de certification en ligne et hors-ligne.

**Module 02 : « Revocation » et « Chain building »** - Ce module décrit comment une « trust chain » est établie à l'intérieur d'une « PKI » et explique, en détails, les secrets du « revocation checking »

**Module 03 : Déployer une Tiers 2 « PKI Hierarchy »** - Ce module commencera par décrire les dessous d'un déploiement de « PKI », suivi par de multiples ateliers incluant le déploiement et la configuration d'une Autorité de Certification standard.

**Module 04 : Sécurité d'une Autorité de certification** : Pour garantir l'intégrité d'une « PKI », il est nécessaire de sécuriser la configuration et les opérations. Ce module expliquera à quoi prêter attention en priorité.

**Module 05 : Template de certificat et méthodes d' enrôlement** – Ce module explique et démontre l'utilisation correcte de templates de certificat dans l'« Active Directory Certificate Services » ainsi que les méthodes d' enrôlement disponibles. Ainsi cela permettra aux administrateurs de comprendre comment enrôler avec succès un certificat auprès de « Windows Server® 2016 Certification Authority ».

**Module 06 : Les bonnes pratiques « PKI Operations » et « Business Continuity »** - Ce module couvre les plans de continuité d'activités (PCA) et les plans de reprise d'activités (PRA) que chaque entreprise devrait avoir en place afin de rapidement se remettre d'un problème affectant « Active Directory Certificate Services in Windows Server 2016 ».