

Déploiement et administration d'une infrastructure à clé publique

Infos Générales



Public visé : Ce cours s'adresse aux ingénieurs système responsables de la conception et de l'implémentation des solutions de sécurité



Objectifs : A la fin de ce cours les stagiaires sauront décrire l'infrastructure PKI et ses composants essentiels ; concevoir une hiérarchie d'Autorité de certification (AC) ; installer les services de certificats pour créer une hiérarchie AC ; configurer les modèles de certificats en créant, en publiant et en remplaçant des modèles de certificats ; inscrire des certificats ; implémenter l'archivage et la récupération de clé dans une infrastructure PKI ; configurer une approbation entre organisations ; déployer des cartes à puce dans un environnement Windows 2003 ; sécuriser un environnement Web par l'implémentation de SSL et l'authentification basée sur le certificat pour les applications Web.



Pré requis : connaissance pratique des technologies réseau et de services d'annuaires Windows 2003

infos pratiques

Référence

MS2821

Vos contacts

Christelle et Caroline

Certification

Pas de certification

Formateur

MCSE

Support

Microsoft Officiel

Durée



Repas



Café



Module 1 : Vue d'ensemble de l'infrastructure à clé publique

Module 2 : Conception d'une hiérarchie d'autorité de certification

Ce module explique comment démarrer la conception d'une infrastructure à clé publique en regroupant des données sous la forme de besoins d'entreprise et en planifiant une structure de hiérarchie de l'autorité de certification (AC).

Module 3 : Création d'une hiérarchie d'autorité de certification

Ce module explique comment installer les services de certificats pour créer une hiérarchie d'autorité de certification. Il explique également comment configurer l'autorité de certification.

Module 4 : Configuration des modèles de certificats

Ce module explique le mode de conception des modèles de certificats. Les stagiaires apprendront également à créer, publier et remplacer des modèles de certificats

Module 5 : Configuration de l'inscription de certificat

Ce module explique les différentes méthodes d'inscription de certificats et la manière de sélectionner la méthode adaptée à chaque situation

Module 6 : Configuration de l'archivage et de la récupération de clé

Ce module décrit le processus d'archivage et de récupération de clé. Les stagiaires apprendront également à configurer et à utiliser l'archivage et la récupération de clé

Module 7 : Gestion d'une infrastructure à clé publique

Ce module explique comment gérer une infrastructure PKI en gérant les certificats et les autorités de certification. Les stagiaires se prépareront également à une récupération après désastre en se familiarisant avec les étapes à appliquer pour assurer la récupération de leur infrastructure PKI en cas d'incident.

Module 8 : Configuration d'une approbation entre les organisations

Ce module aborde les hiérarchies PKI avancées et les différentes contraintes disponibles lors de l'établissement d'une approbation entre des hiérarchies AC. Une fois cette connaissance acquise, les stagiaires vont apprendre à configurer une approbation entre les organisations en configurant et en implémentant une subordination qualifiée

Module 9 : Déploiement des Smart Cards

Ce module explique comment déployer des cartes à puce.

Module 10 : Sécurisation du trafic Web avec SSL

Ce module explique comment sécuriser un environnement Web en implémentant la sécurité SSL et l'authentification basée sur le certificat pour les applications Web.

Module 11 : Configuration de la sécurité d'un système de messagerie

Ce module explique comment implémenter une messagerie sécurisée en développant Microsoft Exchange Server dans un environnement Windows .NET