

Sécuriser Windows Server® 2008 : Travaux pratiques - 4 jours

formation 964

- Vous apprendrez à**
- Utiliser les fonctionnalités de Windows Server 2008 pour sécuriser votre infrastructure
 - Déployer une infrastructure à clé publique Windows (PKI) comme fondation pour les services de sécurité
 - Améliorer les contrôles d'accès avec les stratégies multi-facteurs d'authentification
 - Mettre en place une méthode de chiffrement qui assure la récupération des données
 - Installer et configurer la protection d'accès réseau (Network Access Protection, NAP) pour exclure les ordinateurs non correctement protégés
 - Implémenter l'isolation de domaine pour réduire les risques réseaux pour les serveurs sensibles
- Objectif** Sécuriser l'infrastructure réseau est une priorité et un challenge technique pour la majorité des entreprises. Windows Server 2008 fournit des technologies puissantes et complexes pour réduire les risques réseaux et améliorer l'application des stratégies. Cette formation vous apporte les connaissances et l'expertise nécessaires pour implémenter correctement ces solutions.
- À qui s'adresse cette formation** Aux professionnels de l'informatique en charge de sécuriser une infrastructure réseau Windows. Une expérience du cours 960, "Windows Server 2008 : Introduction complète", ou une expérience pratique de configuration et administration de Windows Server 2003 est nécessaire.
- Travaux pratiques** Au cours de cette formation, vous acquerez l'expérience pratique pour planifier et mettre en œuvre une infrastructure réseau sécurisée. Ces exercices comprennent :
- Déploiement de serveurs de certificats pour fournir des autorités de séquestre et des clés d'agents de récupération
 - Mise en œuvre de stratégies d'authentification multi-facteurs
 - Restauration de données chiffrées avec les agents de récupération et les stratégies
 - Configuration de NAP pour la mise en quarantaine des ordinateurs non sécurisés
 - Réactivation des clients mis en quarantaine pour autoriser l'accès total au réseau
 - Mise en œuvre d'une solution d'isolation de domaine pour restreindre l'accès aux serveurs sensibles

Sécuriser Windows Server® 2008 : Travaux pratiques - 4 jours

formation 964

Infrastructure de sécurité d'entreprise Introduction des niveaux de sécurité

- Identification des fonctionnalités clés d'une infrastructure sécurisée
- Distinction entre sécurité d'entreprise et sécurité hôte

Évaluation des technologies de sécurité

- Mise en place des améliorations Windows Server 2008
- Utilisation des rôles Windows Server 2008

Création d'une infrastructure à clé publique

Les bases de PKI

- Identification des services de sécurité fournis par PKI
- Évaluation des avantages des services de certificats
- Implémentation du chiffrement avec clé publique

Gestion des certificats

- Création et réponse aux requêtes de certificats
- Contrôle de la création de certificats avec permissions
- Sécurisation des enregistrements Web avec HTTPS
- Révocation des clés compromises
- Publication d'une liste de révocation de certificats (CRL)

Stockage, archivage et récupération de clés

- Exportation des certificats et clés privés
- Déploiement de comptes d'agents de récupération de clés
- Maintenance des autorités de séquestre sécurisées
- Fourniture de stockage sécurisé pour clés privées

Authentification multi-facteurs

Étendre les solutions d'authentification

- Installation de domaines de support pour l'authentification multi-facteurs
- Tests Kerberos avec cartes à puces et biométrie

Authentification avec cartes à puces et jetons

- Configuration des enregistrements de stations avec cartes à puces
- Création des certificats utilisateurs sur cartes à puces
- Suspension de certificats sur des jetons déplacés

- Déploiement en domaine d'utilisateurs de cartes à puce et de stratégies d'ordinateurs

Authentification avec la biométrie

- Veille de la disponibilité des technologies de biométrie
- Déploiement de l'authentification biométrique dans l'entreprise
- Gestion des faux négatifs et réduction des faux positifs
- Contrôle des accès aux bases de données d'exemple
- Audit de l'enregistrement biométrique des utilisateurs

Déploiement d'un modèle de protection de données

Identification de solutions de confidentialité

- Spécification des informations requises de sécurité
- Analyse des technologies de protection de données
- Comparaison des solutions natives avec les besoins de l'entreprise

Déploiement d'EFS dans l'entreprise

- Utilisation des stratégies de groupe pour contrôler le chiffrement
- Assurer l'accès aux données avec les agents de récupération
- Récupération des clés perdues ou corrompues à partir des autorités de séquestre
- Sélection d'algorithmes de chiffrement approuvés dans des environnements réglementaires

Assurer la récupération des données avec BitLocker

- Analyse des besoins de l'entreprise
- Planification du déploiement de BitLocker dans l'entreprise
- Compenser les faiblesses d'EFS

Mise en œuvre de la protection d'accès réseau (Network Access Protection, NAP)

Maintenir l'intégrité du réseau avec NAP

- Intégrer les décisions basées NAP à la sécurité de l'entreprise
- Stratégies d'accès pour les clients gérés et non gérés
- Contrôle des accès à partir de machines internes et externes

Vérifier la conformité de la configuration du client

- Définition de stratégies de conformité client adéquates
- Authentification des requêtes NAP avec le System Health Validator (SHV)
- Remédier et assurer une conformité continue

Mise en place des restrictions d'accès réseau

- Configuration des composants serveur NAP
- Limiter l'accès réseau aux machines conformes avec DHCP et la mise en quarantaine des clients VPN

Isolation domaine et serveur

Isoler les serveurs critiques

- Protection de la propriété intellectuelle et de la vie privée
- Sécuriser les serveurs de données très critiques

Sécuriser l'accès au domaine avec IPsec

- Définition des besoins en segmentation
- Isolation de domaine avec l'AD et les stratégies de groupe
- Configuration des serveurs d'exceptions pour les ordinateurs non gérés
- Maximiser la sécurité tout en minimisant l'impact utilisateur