



MS 2304 - Implémentation et administration de la sécurité au sein d'un réseau Microsoft Windows Server 2003 (=2823 US)

Objectif Ce cours décrit des solutions d'infrastructure essentiellement basées sur Microsoft Windows Server™ 2003. Il inclut aussi des éléments relatifs aux clients lorsque cela est nécessaire. Ce cours permet d'acquérir les connaissances fonctionnelles pour planifier et mettre en oeuvre une politique de sécurité. Equivalent au cours MS 2823 (US)

Pré requis Pour suivre ce stage, il est nécessaire suivi le cours Cours 2810 ou avoir les connaissances équivalentes ; une certaine expérience dans la mise en oeuvre d'un environnement Active Directory® Windows 2000 ou Windows Server 2003 ; avoir une première expérience avec des ressources d'entreprise comme des serveurs Web, FTP et Exchange, des ressources partagées et des services réseau comme DHCP, DNS et WINS.

Durée 5 jours

Contenu

Module 1 : Planification et configuration d'une stratégie d'authentification et d'autorisation

- déterminer la structure de groupe nécessaire pour un environnement à plusieurs domaines ou à plusieurs forêts
- créer des approbations dans un environnement Microsoft Windows Server 2003
- planifier, implémenter et gérer une stratégie d'autorisation et d'authentification dans une organisation à plusieurs forêts
- décrire les composants, outils et protocoles qui prennent en charge l'autorisation et l'authentification
- planifier et implémenter une stratégie d'autorisation et d'authentification dans une organisation à plusieurs forêts
- décrire les stratégies d'autorisation et d'authentification supplémentaires.

Module 2 : Installation, configuration et gestion des autorités de certification

- décrire une infrastructure à clé publique ;
- décrire les applications et les composants qui sont utilisés dans une infrastructure à clé publique ;
- installer une Autorité de certification ;
- créer et publier des points de distribution de la liste de révocation de certificats et de l'accès aux informations de l'Autorité ;
- sauvegarder et restaurer une Autorité de certification

Module 3 : Configuration, déploiement et gestion des certificats

- configurer des modèles de certificats dans un environnement PKI Microsoft Windows Server 2003 ;
- déployer, inscrire et révoquer des certificats dans un environnement PKI Windows Server 2003 ;
- décrire les applications et les composants qui sont utilisés dans une infrastructure à clé publique ;
- exporter, importer et archiver des certificats et des clés dans un environnement PKI Windows Server 2003

Module 4: Planification, implémentation et résolution des problèmes de certificats de cartes à puce

- comprendre les concepts et les applications de l'authentification multifactorielle ;
- planifier et implémenter une infrastructure de cartes à puce ;
- gérer et dépanner une infrastructure de cartes à puce

Module 5: Planification, implémentation et résolution des problèmes du système de fichiers EFS (Encrypting File System)

- décrire le système de fichiers EFS et expliquer son fonctionnement ;
- implémenter le système EFS dans un environnement Microsoft Windows XP autonome ;
- planifier et implémenter le système EFS dans un environnement de domaine qui utilise une infrastructure à clé publique (PKI) ;
- implémenter le partage de fichiers EFS ;
- résoudre les problèmes liés au système EFS

Module 6: Planification, configuration et déploiement d'une base sécurisée de serveurs membres

- décrire l'importance des bases de sécurité et des bases de serveurs membres ;
- planifier une base sécurisée de serveurs membres ;
- configurer des paramètres de sécurité supplémentaires ;
- déployer des modèles de sécurité

Module 7: Planification, configuration et implémentation de bases sécurisées pour les rôles des serveurs

- planifier et configurer une base sécurisée pour les contrôleurs de domaine ;
- planifier et configurer une base sécurisée pour les serveurs DNS (Domain Name System) ;
- planifier et configurer une base sécurisée pour les serveurs d'infrastructure ;
- planifier une base sécurisée pour les serveurs de fichiers et d'impression ;
- planifier et configurer une base sécurisée pour les serveurs IIS (Internet Information Services)



Module 8: Planification, configuration, implémentation et déploiement d'une base sécurisée d'ordinateurs clients

- planifier une base sécurisée d'ordinateurs clients ;
- configurer et déployer une base d'ordinateurs clients ;
- planifier et implémenter une stratégie de restriction logicielle sur les ordinateurs clients ;
- implémenter la sécurité sur les ordinateurs portables

Module 9: Planification et implémentation des services SUS (Software Update Services)

- décrire la nécessité de la gestion des mises à jour et les outils à leur disposition pour implémenter des stratégies de gestion des mises à jour ;
- planifier une stratégie de gestion des mises à jour ;
- implémenter une infrastructure SUS

Module 10: Planification, déploiement et résolution des problèmes liés à la sécurité des transmissions de données

- décrire les différentes méthodes de sécurisation des transmissions de données
- décrire l'objectif et le fonctionnement du protocole IPSec
- planifier la sécurité des transmissions de données
- implémenter des méthodes sécurisées de transmission de données
- résoudre les erreurs de transmission de données

Module 11: Planification et implémentation de la sécurité sur des réseaux sans fil

- décrire les composants et les fonctionnalités d'un réseau WLAN sécurisé et d'une infrastructure sans fil ;
- décrire l'authentification 802.1x et son fonctionnement ;
- planifier une infrastructure WLAN sécurisée ;
- implémenter une infrastructure WLAN sécurisée ;
- résoudre les problèmes liés aux composants et aux erreurs WLAN

Module 12: Planification et implémentation de la sécurité de périmètre à l'aide de ISA Server 2000

- décrire les avantages, les modes et les versions d'ISA Server ;
- installer ISA Server 2000 ;
- sécuriser un sous-réseau filtré avec ISA Server 2000 ;
- publier des serveurs

Module 13: Sécurisation de l'accès à distance

- décrire les différentes technologies utilisées pour l'accès à distance et les menaces associées à ce dernier ;
- planifier une stratégie d'accès à distance ;
- implémenter et configurer un serveur de réseau privé virtuel (VPN) ;
- déployer les composants du Contrôle de quarantaine pour l'accès réseau.