

# Réponses aux questions de cours

## Cours ACDI – SC084v4

### Chapitre 1

1. Est-ce que l'Edition WEB de Windows 2008 R2 est disponible en 32 bits ? 1 : Toutes les éditions de Windows 2008 R2 ne sont disponibles qu'en 64 bits ; l'édition Web ne fait pas exception.
2. Quelle sont les tailles mémoire minimale et maximale pour l'Edition standard de Windows 2008 R2 ? 2 : l'Edition standard de Windows 2008 R2 fonctionne avec une mémoire dont la taille minimale est 512 Mo de RAM ; cette édition peut gérer jusqu'à 32 Go de Ram.
3. Est-ce la présence d'une carte réseau est indispensable pour pouvoir installer Windows 2008 R2 ? 3 : La présence d'une carte réseau n'est pas indispensable pour pouvoir installer Windows 2008 R2 (par contre elle est indispensable pour pouvoir installer l'Active Directory).
4. Les outils d'Administration à distance des serveurs (2008 R2) font-ils partie des rôles ou des fonctionnalités ? 4 : Les outils d'Administration à distance des serveurs, qui ne peuvent s'installer que sur des serveurs, font partie des fonctionnalités. Le kit RSAT, disponible en téléchargement gratuit sur le site de Microsoft, permet de gérer des serveurs à distance à partir d'un poste de travail sous Windows 7.
5. Le serveur de noms DNS, qui est indispensable pour le fonctionnement de l'Active Directory, est un rôle. Qu'en est-il du serveur de noms Netbios (WINS) rôle ou fonctionnalité ? 5 : Le serveur de noms Netbios (WINS) fait partie des fonctionnalités.
6. A quel moment peut-on donner un nom à un serveur 2008 R2 : pendant l'installation ou dans la page des tâches initiales ? 6 : Le nom définitif d'un serveur exécutant Windows 2008 R2 est défini dans la page des tâches initiales ; pendant l'installation il a un nom provisoire déterminé aléatoirement.

### Chapitre 2

1. Quelle sont les 2 principales raisons de créer des unités d'organisation ? 1 : Les unités d'organisation permettent de déléguer certaines tâches (gestion des comptes d'utilisateurs, des groupes, ...) à des utilisateurs qui n'ont pas les privilèges « Administrateurs » ; elles permettent aussi d'appliquer des stratégies de groupe à des ensembles d'objets (utilisateurs, groupes, ...) afin de gérer la sécurité du système de façon centralisée.  
Une bonne organisation des unités d'organisation permet aussi d'avoir une meilleure visibilité de la gestion des objets pris en charge (Est-ce que l'entreprise a choisi une gestion centralisée ou décentralisée de son informatique ...)
2. Quelle est l'utilité des sites Active Directory ? 2 : Les sites Active Directory permettent de gérer le trafic de réplication (planification de la réplication Wan) et de gérer l'authentification des clients en privilégiant l'authentification sur le Lan plutôt qu'à travers d'un Wan..

### Chapitre 3

1. Peut-on ouvrir une session en saisissant DOM1\Karen comme nom d'utilisateur sachant que DOM1 est un nom de domaine NETBIOS valable et que le compte Karen existe bien dans ce domaine AD DS ? 1 : La syntaxe DOM1\Karen est parfaitement valable pour demander l'authentification de l'utilisateur Karen. Le nom de domaine utilisé ici est un nom NetBIOS (et non DNS).
2. Peut-on ouvrir une session en saisissant cn=Karen, ou=itAdmins,DC=DOM1,DC=local comme nom d'utilisateur sachant que le compte de Karen existe bien dans l'unité d'organisation itAdmins et que DOM1.local est le nom DNS du domaine où réside ce compte ? 2 : Le nom « cn=Karen, ou=itAdmins,DC=DOM1,DC=local » est un nom LDAP tout à fait valable. Mais Windows ne supporte pas ces noms pour l'authentification des utilisateurs.
3. En reprenant le contexte de la question précédente, que faut-il faire afin que Karen puisse ouvrir une session avec la saisie de : Karen@simba.west sans que son compte change de domaine ? 3 : Pour que Karen puisse se connecter en saisissant « Karen@simba.west », il faut que le suffixe « simba.west » soit créé au niveau de la forêt et que ce suffixe soit associé à l'utilisateur Karen.
4. Si l'administrateur désactive le compte de la machine cliente utilisé par Karen, celle-ci ne pourra plus ouvrir de session en domaine à partir de cette machine. Elle pourra tout de même ouvrir une session locale à partir de cette machine et une session en domaine à partir d'une autre machine. 4 : Si l'administrateur désactive le compte de la machine cliente utilisé par Karen, celle-ci ne pourra plus ouvrir de session en domaine à partir de cette machine. Elle pourra tout de même ouvrir une session locale à partir de cette machine et une session en domaine à partir d'une autre machine.
5. Si l'administrateur désactive le compte de la machine cliente utilisée par Karen, est-ce que celle-ci pourra ouvrir une session en domaine à partir de sa machine ? Une session locale à partir de sa machine ? Une session en domaine à partir d'une autre machine ? 5 : Le mot de passe « MzbKxZZyGg » ne comprend que 2 catégories de caractères. L'Active Directory exige la présence d'au moins 3 catégories de caractères pour qu'un mot de passe soit considéré comme un mot de passe complexe.
5. Est-ce que MzbKxZZyGg est un mot de passe complexe pour l'Active Directory Services de domaines ?

## Chapitre 4

1. Est-ce que la protection contre les suppressions intempestives des unités d'organisation s'applique aux Administrateurs ?
2. Comment pouvez-vous supprimer la protection contre les suppressions intempestives des unités d'organisation ?
3. Lorsque vous créez une unité d'organisation, devez-vous déléguer le contrôle d'administration à des Administrateurs ou à des Utilisateurs ?
4. Quand vous créez une hiérarchie d'unités d'organisation, devez-vous reproduire fidèlement l'organigramme de l'entreprise ?
5. Comment supprimez-vous une délégation devenue inutile ?

- 1 : La protection contre les suppressions intempestives s'applique aussi aux Administrateurs.
- 2 : Pour supprimer la protection contre les suppressions intempestives des unités d'organisation il faut que l'affichage des fonctionnalités avancées soit sélectionné dans la console Utilisateurs et Ordinateurs Active Directory. Cette option sera alors visible dans l'onglet Objet. Naturellement la personne qui veut effectuer cette manipulation doit avoir les autorisations nécessaires.
- 3 : Les administrateurs possèdent par défaut toutes les permissions possibles sur l'Active Directory. Les délégations ne concernent que de simples utilisateurs.
- 4 : La reproduction servile de l'organigramme de l'entreprise n'est pas une bonne option. Le but principal est la gestion des ressources informatiques (posez-vous la question de la place d'une Direction Générale dans la gestion des ressources informatiques d'une entreprise).
- 5 : La délégation est un concept que Windows traduit par la mise en place de permissions. Windows est incapable de restituer les permissions mises en place sous forme de délégations. La suppression d'une délégation ne peut s'effectuer qu'en supprimant directement les permissions générées par Windows.

## Chapitre 5

1. Pourquoi devez vous préférer utiliser des groupes globaux plutôt que des groupes Domaines Locaux pour regrouper les utilisateurs d'un service Ventes dans une société qui utilise un réseau mono domaine ?
2. Vous voulez utiliser les groupes locaux d'un serveur membre afin de mettre en place une gestion décentralisée des permissions. Quels groupes pouvez-vous inclure dans un groupe local défini sur ce serveur ?
3. Pouvez-vous inclure dans le même groupe des comptes de machines et des comptes d'utilisateurs ?
4. Pouvez-vous expliquer la notion de groupe principal ?

- 1 : L'utilisation des groupes globaux permettra de passer facilement d'une gestion centralisée des permissions à une gestion décentralisée des permissions. Rappelez-vous qu'il est possible d'inclure un groupe global (groupe de comptes) dans un groupe domaine local (groupe de permissions) mais pas l'inverse.
- 2 : On peut inclure seulement des groupes globaux de l'Active Directory dans un groupe local d'un serveur membre.
- 3 : Il est tout à fait possible d'inclure des comptes machines et des comptes d'utilisateurs dans un même groupe (à condition de pouvoir expliquer pourquoi).
- 4 : Les groupes principaux sont par les applications POSIX et l'authentification Linux ; dans les précédentes versions des systèmes ils étaient aussi utilisés par le serveur de fichier Macintosh (qui n'existe plus). Le groupe principal d'un utilisateur doit être un groupe global de sécurité..

## Chapitre 6

1. Quel est le rôle des listes DACL dans la sécurité de l'accès aux ressources; est ce que ces listes sont uniquement accessibles dans un environnement AD DS ?
2. Quelle sont les différences entre le partage et le partage avancé ?
3. Comment faire pour forcer les « utilisateurs » à n'utiliser que le partage avancé ?

- 1 : Les listes DACL contiennent les permissions associées à des ressources (NTFS, Active Directory, registre, imprimantes). Elles sont utilisées pour contrôler les demandes d'accès à ces ressources. Comme le système de fichiers NTFS est disponible sur toutes les machines fonctionnant sur une version récente de Windows, ces listes ne sont l'apanage exclusif de l'Active Directory
- 2 : Le Partage avancé permet de gérer toutes les options du partage de dossiers mais il ne gère pas les permissions NTFS. Le partage utilise un assistant qui gère (assez grossièrement) les permissions de partage et les permissions NTFS de façon à ce que les permissions soient en accord entre elles. Rappelez-vous que les permissions NTFS s'appliquent à tous les accès (locaux et réseau) tandis que les permissions de partage ne s'appliquent qu'aux accès réseau.
- 3 : Au moyen des stratégies de groupe ou des options de l'explorateur Windows, il est possible de désactiver l'assistant de partage des dossiers (non recommandé par Microsoft).

## Chapitre 7 (facultatif)

1. Lorsqu'un poste de travail est incorporé dans un domaine Active Directory, est-ce que la stratégie locale de cette machine s'applique toujours ?  
2. Pour un objet lien, quelle est la différence entre Appliqué et Activé ?

3. Vous essayez d'utiliser l'assistant Résultat de stratégie de groupe pour obtenir la configuration d'un poste sous Windows Vista SP1 mais la machine ne répond pas. Le réseau n'étant pas en cause (la commande ping répond), quelle est la cause la plus probable de cette absence de réponse ?

- 1 : Lorsqu'un poste de travail intègre un domaine Active Directory, sa stratégie locale s'applique toujours mais les stratégies de groupe sont prioritaires. Un paramètre défini dans la stratégie locale d'une machine ne s'appliquera que si ce même paramètre n'est défini dans aucune stratégie de groupe applicable à cette machine.
- 2 : Un lien caractérisé par l'option « activé » permettra l'application « normale » d'une stratégie de groupe sur l'objet lié (Unité d'organisation principalement). Un lien caractérisé par l'option « appliqué » imposera l'application de la stratégie sur l'objet lié en faisant abstraction des priorités : on parle alors d'une application « de force » qui ne devrait être utilisée que pour les options de sécurité.
- 3 : L'assistant « résultat de stratégie de groupe » a besoin d'accéder à la machine dont il doit analyser le comportement. Pour cette machine, il s'agit de trafic réseau entrant non sollicité qui, par défaut, sera bloqué par le pare-feu. Pour obtenir une réponse, il sera donc nécessaire de configurer ou de désactiver temporairement le pare-feu.

XXXXXXXXXX