A. Rôle du service d'annuaire dans l'entreprise

Le service d'annuaire est l'un des composants les plus importants d'un système d'information, et ce, quelle que soit sa taille. Il offre des services centraux capables de fédérer les multiples éléments qui composent le système d'information lui-même. Par exemple, imaginez qu'un utilisateur recherche un élément du réseau sans pour autant en connaître le nom ou l'endroit ! De prime abord, le problème semble insoluble alors que finalement il n'en est rien. En fait, l'utilisateur pourra résoudre lui-même ce problème en initiant une recherche vers le système d'annuaire sur la base d'un ou de plusieurs attributs qu'il connaît. De cette manière, il est par exemple possible à notre utilisateur de localiser une imprimante couleurs supportant l'impression recto verso, l'agrafage et ce, à un emplacement géographique particulier. Au travers de ce premier exemple, nous pouvons maintenant introduire les fondements de l'annuaire Active Directory. L'annuaire Active Directory doit offrir les moyens de stocker toutes les informations qui caractérisent l'ensemble des objets pouvant exister dans le réseau de l'entreprise ainsi que disposer des services capables de rendre ces informations globalement utilisables par les utilisateurs, et ce, en fonction de leurs droits et privilèges. Par voie de conséquence, les services de domaine Active Directory de Windows Server offrent les services ci-dessous :

- La possibilité de publier à l'échelle de l'entreprise des services indispensables au bon fonctionnement de celle-ci. Les services à caractères globaux pourront trouver leur place au sein d'un service d'annuaire offrant de telles possibilités de publication et de sélection. Par exemple, il pourrait s'agir pour une application s'exécutant sur le poste de travail, de localiser le serveur de messagerie instantanée le plus proche et le plus disponible. Pour reprendre l'exemple précédent, il pourrait aussi s'agir d'un poste de travail devant sélectionner une autorité de certification capable de délivrer un certificat permettant d'accéder à un site ou une application particulièrement sécurisée.
- Ils pourront, si nécessaire, jouer le rôle de colonne vertébrale pour l'ensemble des services de sécurité du réseau de l'entreprise. De cette manière, les administrateurs pourront s'appuyer sur un modèle de gestion globale de la sécurité, lequel permettra de garantir plus facilement un haut niveau de sécurité des accès et une meilleure confidentialité des données sensibles. Par exemple, ce pourrait être le cas de la distribution automatique de certificats numériques pour signer un message électronique ou aussi prendre en charge l'authentification des utilisateurs sur présentation d'une carte à puce ou via la vérification de l'empreinte digitale ou pourquoi pas aussi de l'iris. Il pourra aussi s'agir de distribuer les listes de contrôle d'accès à un firewall en fonction de l'authentification d'un utilisateur sur une connexion VPN. De cette manière, les services de domaine Active Directory permettent ou ne permettent pas à un utilisateur distant d'accéder à certaines ressources du réseau privé en contrôlant dynamiquement les règles contenues dans un firewall.
- L'annuaire est globalement distribué. Cette fonctionnalité permet à l'ensemble des utilisateurs du réseau de s'appuyer sur l'ensemble des services de sécurité, des services applicatifs et des services de recherche de l'Active Directory. Évidemment, les services globaux doivent être globalement accessibles ! Il ne saurait en être autrement, surtout s'il s'agit des contrôles d'accès et du bon fonctionnement d'applications critiques telles que la messagerie ou les services de collaboration. Il est clair que ces exigences nécessiteront une adoption généralisée des technologies indispensables à l'implémentation de celles-ci.

- L'annuaire doit disposer de fonctions naturelles qui lui permettent de résister aux défaillances. La réplication de l'annuaire Active Directory sur chaque site géographique important permettra à l'annuaire de jouer son rôle central. Par exemple, la disparition d'un contrôleur de domaine sur un site géographique donné doit être solutionnée sans nécessiter d'intervention humaine.
- Les services de domaine Active Directory apportent avec eux la technologie de partitionnement qui permet de s'appuyer sur un espace de stockage distribué à l'échelle de l'entreprise. De cette manière, l'annuaire Active Directory est capable de gérer des millions d'objets et permet aux utilisateurs d'y accéder quel que soit leur emplacement ou même celui des ressources. Ce rôle central donnera au service d'annuaire Active Directory un caractère particulièrement stratégique et critique qu'il conviendra de considérer au plus tôt.

B. Positionnement et innovations de Windows Server 2008 R2

1. Version majeure de Windows Server

Windows Server 2008 R2 a été conçu comme une version majeure pour fournir aux entreprises une plate-forme plus productive pour la virtualisation, alimenter les applications et protéger des réseaux. Les plus grosses évolutions et avancées permettent de fournir une plate-forme sécurisée facile à gérer, du simple serveur de groupe de travail aux plus grands centres de données.

2. Évolutions en matière de sécurité

La sécurité a également été améliorée grâce à la protection des accès réseaux (NAP, *Network Access Protection*), des nouveaux contrôleurs de domaine en lecture seule (RODC, *Read Only Domain Controller*) et à la nouvelle version des services et infrastructure à clé publique (AD CS, *Active Directory Certificate Services*). Les services de gestion des droits numériques RMS (AD RMS, *Active Directory Rights Management Services*) permettent aussi une gestion des informations critiques et données confidentielles au sein et en dehors de l'entreprise. La présence des fonctions de renforcement des services Windows, du nouveau pare-feu Windows bidirectionnel et des fonctions cryptographiques CNG (*Crypto Next Generation*) sont aussi des points essentiels.

3. Accès aux applications et mobilité

Les utilisateurs mobiles ne sont pas en reste puisqu'il est désormais possible d'exécuter des programmes de n'importe quel emplacement distant grâce à RemoteApp et les fonctions de Remote Desktop Gateway. Windows Server 2008 R2 permet aussi aux équipes de déploiement de progresser grâce aux Services de déploiement Windows (*Windows Deployment Services*).

4. Virtualisation des serveurs

Enfin, les progrès accomplis dans l'intégration des technologies virtuelles au matériel permet à Hyper-V de virtualiser des charges de travail beaucoup plus exigeantes que les versions précédentes et avec une plus grande flexibilité. L'architecture est basée sur un hyperviseur 64 bits à faible surcharge spécialisé pour les processeurs 64 bits Intel VT-x AMD-V. Windows Server 2008 R2 et Hyper-V prennent en charge la gestion des configurations de type multinoyaux. Chaque machine virtuelle (VM) peut recevoir un maximum de quatre processeurs logiques pour virtualiser des charges de travail intensives qui profitent du traitement en parallèle des noyaux des VM multiprocesseurs. Le système hôte 64 bits prend en charge les systèmes d'exploitation invités en mode 64 bits pour assurer un accès rapide aux grandes zones mémoires des VM invitées. Hyper-V supporte aussi les systèmes d'exploitation invités 64 bits et 32 bits s'exécutant sur le même serveur consolidé. Enfin, Hyper-V supporte les accès directs aux disques. Les systèmes d'exploitation invités peuvent être configurés pour accéder directement au stockage local ou au réseau SAN (*Storage Area Network*), garantissant ainsi des performances supérieures aux applications d'E/S (entrées/sorties) intensives telles que SQL Server ou Microsoft Exchange Server.

5. Nouveautés apportées par Windows Server 2008 et Windows Server 2008 R2

Après le passage de Windows NT à Windows 2000, Windows Server 2008 est réellement le point de départ d'une nouvelle génération de Windows Server. Windows Server 2008 introduit les fonctionnalités ci-dessous, lesquelles sont pour la plupart sensiblement améliorées avec Windows Server 2008 R2. La liste des fonctionnalités ci-dessous illustre l'ensemble des évolutions :

- Windows Firewall with Advanced Security
- Server Manager
- Server Core Installation Option
- Active Directory Certificate Services Role
- AD CS: Enterprise PKI (PKIView)
- AD CS: Network Device Enrollment Service
- AD CS: Online Certificate Status Protocol Support
- AD CS: Policy Settings
- AD CS: Web Enrollment
- Cryptography Next Generation
- Active Directory Domain Services Role
- AD DS: Auditing
- AD DS: Fine-Grained Password Policies
- AD DS: Read-Only Domain Controllers
- AD DS: Restartable Active Directory Domain Services
- AD DS: Snapshot Viewer

- AD DS: User Interface Improvements
- Active Directory Federation Services Role
- Active Directory Lightweight Directory Services Role
- Active Directory Rights Management Services Role
- Application Server
- DNS Server Role
- File Services Role
- Windows Server Backup
- Services for Network File System
- Transactional NTFS
- Self-Healing NTFS
- Symbolic Linking
- Network Policy and Access Services Role
- Network Policy and Access Services
- Network Access Protection
- Streaming Media Services Role
- Services Bureau à distance : hôte de session Bureau à distance, hôte de virtualisation de services Bureau à distance, service Broker pour les connexions Bureau à distance, passerelle des services Bureau à distance, accès Bureau à distance par le Web (accès aux programmes RemoteApp)
- Services de Bureau à distance et Gestionnaire de Ressources Système
- Serveur Web (IIS)
- Windows Deployment Services Role
- BitLocker Drive Encryption
- Failover Clustering
- Network Load Balancing Improvements
- Next Generation TCP/IP Protocols and Networking Components
- Windows Reliability and Performance Monitoring

6. Innovations apportées à Active Directory

Comme cela a été le cas sous Windows Server 2003, les services d'annuaire Active Directory ont comme fonction et vocation première de gérer les utilisateurs, les ressources telles que les ordinateurs, les imprimantes et aussi des applications telles que Microsoft Exchange Server 2010 ou Microsoft Lync Server 2010.

Les services Active Directory de Windows Server 2008 R2 comprennent de nouvelles fonctionnalités dont la plupart n'étaient pas présentes dans les versions précédentes de Windows Server. De fait, les services d'annuaire Active Directory sont-ils rebaptisés Services de domaine Active Directory (AD DS, *Active Directory Domain Services*). Cette introduction présente ces nouveautés.

a. AD DS: Audit

Les contrôleurs de domaine Windows Server 2008 R2 supportent de nouvelles sous-catégories – (*Directory Service Changes*) pour consigner lors des opérations de changements d'attributs sur les objets Active Directory, les anciennes valeurs ainsi que les nouvelles valeurs d'attributs. Un nouveau paramètre, à définir dans la stratégie des contrôleurs de domaine – Audit directory service access, permet d'activer ou de désactiver cette nouvelle fonctionnalité. Bien sur, cette fonctionnalité est très intéressante pour tous ceux qui souhaitent surveiller les opérations réalisées sur les objets. Notez que l'administration des attributs à auditer est toujours définie au niveau des objets, permettant ainsi une extrême finesse de configuration. Les nouveaux services d'audit permettent donc de journaliser les valeurs des attributs lors des changements.

Windows Server 2003 avait la possibilité de consigner les événements de modification des attributs, mais il ne permettait pas d'enregistrer ni les anciennes, ni les nouvelles valeurs. Notez aussi que les nouvelles fonctionnalités d'audit des services de domaine Active Directory s'appliquent de la même manière sur les services AD LDS (*Active Directory Lightweight Directory Services*).

b. AD DS: Gestion granulaire des stratégies de mot de passe

Avec les domaines Windows 2000 et Windows Server 2003, une seule et unique stratégie de mots de passe et de verrouillage des comptes pouvait être appliquée à l'ensemble des utilisateurs d'un domaine. Les services de domaine Active Directory de Windows Server 2008 R2 permettent désormais de définir différentes stratégies de mots de passe ainsi que différentes stratégies de verrouillage des comptes.

Cette nouvelle fonctionnalité intéressera les nombreux administrateurs qui recherchaient cette possibilité. Il est désormais possible de créer de multiples stratégies de mot de passe au sein du même domaine et de les appliquer sur différents ensembles d'utilisateurs. Ces nouvelles stratégies de comptes s'appliquent uniquement sur des objets utilisateurs, de la classe inetOrgPerson mais aussi sur des groupes globaux de sécurité.

c. AD DS: Contrôleurs de domaine en lecture seule

Les contrôleurs de domaine fonctionnant sous Windows 2000 Server ou Windows Server 2003 sont par définition disponibles en lecture et en écriture. Lorsque les contraintes d'architecture réseau l'exigent, il est nécessaire de placer sur un site distant un contrôleur de domaine afin d'authentifier les utilisateurs et d'offrir les services d'infrastructure habituels. Le problème est que, trop souvent, les sites distants ne disposent pas du niveau de sécurité nécessaire à des serveurs d'infrastructure, tels que des contrôleurs de domaine disponibles en écriture.

Windows Server 2008 R2 permet désormais d'installer un nouveau type de contrôleur de domaine appelé contrôleur de domaine en lecture seule ou RODC (*Read-Only Domain Controller*). Cette nouvelle solution permet de déployer des contrôleurs de domaine dans les emplacements ou un bon niveau de sécurité ne peut être garanti. En plus de forcer la base de données Active Directory en mode lecture seule, les RODC introduisent aussi d'autres améliorations telles que la réplication unidirectionnelle, la mise en cache des données d'identification, la séparation des rôles ainsi que la prise en charge de la problématique des inscriptions dynamiques DNS dans les zones DNS intégrées à des bases de données Active Directory disponibles en lecture seule.

d. AD DS: Redémarrage des services de domaine Active Directory

Les serveurs Windows Server 2008 permettent aux administrateurs d'arrêter et de démarrer les services AD DS à l'aide des outils habituels de Windows Server. Cette nouvelle fonctionnalité est très intéressante lors du passage de certaines mises à jour ou lors d'une opération de défragmentation de la base de données Active Directory, sachant que les services ne dépendant pas d'Active Directory peuvent continuer de fonctionner normalement.

e. AD DS: Aide à la récupération des données

Avant l'utilisation des contrôleurs de domaine Windows Server 2008 R2, lorsque des objets étaient accidentellement détruits, la seule façon de déterminer quels objets avaient été effacés était de restaurer la base de données Active Directory.

Bien que la fonctionnalité d'aide à la récupération des données Active Directory ne permette pas de directement restaurer les données éventuellement effacées, elle aidera lors de la procédure de récupération des données.

Grâce à l'outil de montage de base Active Directory, les données Active Directory enregistrées dans les clichés instantanés sont exposées. De cette manière, l'administrateur peut comparer les données à différents moments sans aucun arrêt système.

Pendant la phase Beta de Windows Server 2008, cette fonctionnalité était appelée Snapshot Viewer.

f. AD DS: Améliorations de l'interface Active Directory

Windows Server 2008 R2 introduit un nouvel assistant d'installation des services Active Directory. Il permet notamment d'installer les nouveaux contrôleurs de type RODC, ainsi que de définir les options de réplication des mots de passe sur ces contrôleurs. La nouvelle console de gestion Utilisateurs et ordinateurs Active Directory permet aussi de pré-créer et de déléguer l'installation d'un contrôleur de domaine en mode lecture seule.

En plus de ces améliorations, l'assistant d'installation d'Active Directory supporte une nouvelle option qui permet d'utiliser un mode plus avancé. Ce nouveau mode permet notamment :

- Lors de l'installation d'un nouveau contrôleur de domaine dans un domaine enfant, de détecter lorsque l'IM – *Infrastructure Master*, est positionné sur un GC – *Global Catalog*.