Module 1 : Introduction à l'infrastructure Active Directory ®

1. Introduction.

Ce module présente la structure physique et logique du service d'annuaire Active Directory et sa fonction en tant qu'annuaire. Le module présente également les composant logiciels enfichables, les outils de ligne de commande et l'environnement d'exécution de scripts Windows vous permettant de gérer les composants Active Directory ainsi que ses processus de conception, de planification et d'implémentation.

2. Architecture d'Active Directory ®.

a) Introduction

Active Directory inclut des composants qui constituent sa structure logique et physique. Vous devez planifier les structures logique et physique d'Active Directory pour répondre à vos impératifs organisationnels. Pour gérer Active Directory, vous devez comprendre le rôle de ces composants et comment les utiliser.

b) Rôle d'Active Directory

- Centralisation du contrôle des ressources du réseau
- Centralisation et décentralisation de la gestion des ressources
- Stockage des objets de manière sécurisée dans une structure logique
- Optimisation du trafic réseau

Active Directory stocke des informations sur les utilisateurs, les ordinateurs et les ressources du réseau, afin de permettre aux utilisateurs et aux applications d'accéder à ces ressources. Il constitue un moyen cohérent de nommer, de décrire, de localiser, d'accéder, de gérer et de sécuriser les informations concernant ces ressources.

Active Directory fournit les fonctions suivantes :

- *Centralisation du contrôle des ressources du réseau.* La centralisation du contrôle des ressources, comme les serveurs, les fichiers partagé et les imprimantes, permet aux seuls utilisateurs autorisés d'accéder aux ressources dans Active Directory.
- *Centralisation et décentralisation de la gestion des ressources.* Les administrateurs peuvent gérer des ordinateurs clients distribués, des services réseau et des applications à partir d'un emplacement centralisé à l'aide d'une interface de gestion cohérente, ou distribuer des tâches d'administration en déléguant le contrôle des ressources à d'autres administrateurs.
- *Stockage des objets de manière sécurisée dans une structure logique.* Active Directory stocke toutes les ressources sous forme d'objets dans une structure logique hiérarchique sécurisée.
- *Optimisation du trafic réseau.* La structure physique d'Active Directory vous permet d'utiliser plus efficacement la bande passante du réseau. Il vous garantit que lorsque des utilisateurs se connectent au réseau, ils sont authentifiés par l'autorité d'authentification la plus proche de l'utilisateur, réduisant d'autant la quantité de trafic réseau.

c) Structure logique d'Active Directory

Active Directory offre un stockage sécurisé pour les informations concernant les objets dans une structure logique hiérarchique. Les *objets* Active Directory représentent des utilisateurs et des ressources. Certains objets en contiennent d'autres.

La structure logique d'Active Directory inclut les composants suivants :

- *Les objets.* Il s'agit des composants les plus élémentaires de la structure logique. *Les classes objets* sont des modèles pour les types d'objets que vous pouvez créer dans Active Directory. Chaque classe d'objet est définie par une liste d'*attributs*, qui définit les valeurs possibles que vous pouvez associer à un objet. Chaque objet possède une combinaison unique de valeurs d'attributs.
- *Le unités d'organisation (OU, Organizational Unit).* Vous utiliser ces objets conteneurs pour organiser d'autres objets de telle manière qu'ils prennent en compte vos objectifs administratifs. La disposition de ces objets par unité d'organisation simplifie la recherche et la gestion des objets. Vous pouvez également déléguer l'autorité de gestion d'une unité d'organisation. Les unités d'organisation peuvent être *imbriquées* les unes dans les autres, ce qui simplifie d'autant la gestion d'objets.
- *Les domaines.* Unités fonctionnelles centrales dans la structure logique d'Active Directory, les domaines sont un ensemble d'objets définis administrativement qui partagent une base de données d'annuaire commune, des stratégies de sécurité et de relations d'approbation avec d'autres domaines. Les domaines disposent des trois fonctions suivantes :
  - Une limite d'administration pour objets.
  - Une méthode de gestion de la sécurité pour les ressources partagées.
  - Une unité de réplication pour les objets.
- *Les arborescences de domaines.* Les domaines regroupés en structures hiérarchiques sont appelés arborescence de domaines. Lorsque vous ajoutez un second domaine à une arborescence, il devient *enfant* du domaineracine de l'arborescence. Le domaine auquel un domaine enfant est attaché est appelé *domaine* parent. Un domaine enfant peut à son tour avoir son propre domaine enfant.
  Le nom d'un domaine enfant est associé à celui de son domaine parent pour former son nom DNS (Domain Name System) unique. De cette manière, une arborescence a un *espace de noms contigu.*
- *Les forêts.* Une forêt est une instance complète d'Active Directory. Elle consiste en une ou plusieurs arborescences. Dans une arborescence unique à deux niveaux, qui est recommandée pour la plupart des organisations, tous les domaines enfants sont des enfants du domaine racine de la forêt afin de former une arborescence contiguë.
  Le premier domaine de la forêt est appelé le *domaine racine de la forêt.* Le nom de ce domaine fait référence à la forêt. Par défaut, les informations dans Active Directory ne sont partagées qu'à l'intérieur de la forêt. Ainsi, la forêt est une limite de sécurité pour les informations contenues dans l'instance d'Active Directory.

d) Structure physique d'Active Directory

La structure physique d'Active Directory optimise le trafic réseau en déterminant où et quand se produit un trafic de connexions et de réplications.

Les éléments de la structure physique d'Active Directory sont :

- *Les contrôleurs de domaine.* (exécute Win Server 2003 ou Win 2000 et Active Directory). Chaque contrôleur de domaine exécute des fonctions de stockage et de réplication. Un contrôleur de domaine ne peut gérer qu'un seul domaine. Pour assurer une disponibilité permanente d'Active Directory, chaque domaine doit disposer de plusieurs contrôleur de domaine.
- *Les sites Active Directory.* Ces sites sont des groupes d'ordinateurs connectés par des liaisons rapides. Lorsque vous créez des sites, les contrôleurs de domaine au sein d'un même site communiquent fréquemment. Ces communications réduisent le délai de *latence de réplication* à l'intérieur du site ; autrement dit, le temps requis pour qu'une modification effectuée sur un contrôleur de domaine soit répliquée sur d'autres contrôleurs de domaine. Vous pouvez donc créer des sites pour optimiser l'utilisation de la bande passante entre des contrôleurs de domaine situés à des emplacements différents. (Pour plus d'infos sur les sites voir module 7).
- *Partitions Active Directory.* Chaque contrôleur de domaine contient les partitions Active Directory suivantes :
  - *La partition de domaine* contient les réplicas de tous les objets de ce domaine. La partition de domaine n'est répliquée que dans d'autres contrôleurs appartenant au même domaine.
  - *La partition de configuration* contient la topologie de la forêt. La *topologie* est un enregistrement de tous les contrôleurs de domaine et des connexions entre eux dans une forêt.
  - *La partition de schéma* contient le schéma étendu au niveau de la forêt. Chaque forêt comporte un schéma de sorte que la définition de chaque classe d'objet est cohérente. Les partitions de configurations et de schéma sont répliquées dans chaque contrôleur de domaine dans la forêt.
  - *Les partitions d'applications facultatives* contiennent des objets non liés à la sécurité et utilisés par une ou plusieurs applications. Les partitions d'applications sont répliquées dans des contrôleurs de domaine spécifiés dans la forêt.

  (Pour plus d'infos sur les partitions voir module 7)

e) Définitions des maîtres d'opérations

Lorsqu'un domaine est modifié, la modification est répliquée sur tous les contrôleurs du domaine. Certaines modifications, telles que celles apportées au schéma, sont répliquées dans tous les domaines de la forêt. Cette réplication est appelée *réplication multimaître.*

Opérations de maître unique.

Lors d'une réplication multimaître, un conflit de réplication peut se produire si des mises à jour d'origine sont effectuées simultanément sur le même attribut d'un objet sur deux contrôleurs de domaine. Pour éviter des conflits de réplication, vous utiliserez une *réplication à maître unique*, qui désigne un contrôleur de domaine comme étant le seul sur lequel certaines modifications de l'annuaire peuvent être effectuées. Ainsi, des modifications ne peuvent intervenir simultanément sur différents endroits du réseau. Active Directory utilise une réplication à maître unique pour des modifications importantes, comme l'ajout d'un nouveau domaine ou une modification dans le schéma au niveau de la forêt.

Rôles de maître d'opérations.

Les opérations utilisant une réplication à maître unique sont regroupées dans des rôles spécifiques dans une forêt ou un domaine. Ces rôles sont appelés *rôles de maître d'opérations.* Pour chaque rôle de maître d'opérations, seul le contrôleur de domaine possédant ce rôle peut effectuer les modifications dans l'annuaire correspondant. Le contrôleur de domaine responsable d'un rôle particulier est appelé *maître d'opérations* pour ce rôle. Active directory stocke les informations concernant le contrôleur de domaine qui joue un rôle spécifique.
Active Directory définit cinq rôles de maître d'opérations, chacun possédant un emplacement par défaut. Les rôles de maître d'opérations s'étendent au niveau d'une forêt ou d'un domaine.

- *Rôles étendus au niveau d'une forêt :*
  - *Le contrôleur de schéma.* Il contrôle toutes les mises à jour du schéma. Le schéma contient la liste principale des classes et des attributs d'objets utilisés pour créer tous les objets Active Directory, comme les utilisateurs, les ordinateurs et les imprimantes.
  - *Le maître d'attribution des noms de domaine.* Il contrôle l'ajout ou la suppression de domaine dans une forêt. Lorsque vous ajoutez un domaine à la forêt, seul le contrôleur de domaine possédant le rôle de maître d'attribution des noms de domaine peut ajouter le nouveau domaine.

  L'ensemble de la forêt ne contient qu'un seul contrôleur de schéma et qu'un seul maître d'attribution des noms de domaine.

- *Rôles étendus au niveau d'un domaine :*
  - *L'émulateur de contrôleur principal de domaine (PDC, Primary Domain Controller).* Il se comporte comme un contrôleur principal de domaine Win NT pour la prise en charge de tout contrôleur secondaire de domaine *(BDC, Backup Domain Controller)* exécutant Win NT au sein d'un *domaine en mode mixte*. Ce type de domaine possède des contrôleurs de domaine exécutant Win NT 4.0. L'émulateur PDC est le premier contrôleur de domaine que vous créez dans un nouveau domaine.

- *Le maître des identificateurs relatifs (maître RID).* Lorsqu'un nouvel objet est créé, le contrôleur de domaine crée une nouvelle entité de sécurité qui représente l'objet et auquel un identificateur de sécurité (SID, Security IDentifier) unique. Cet identificateur consiste en un identificateur de sécurité de domaine, qui est le même pour toutes les entités de sécurité créées dans le domaine, et en un identificateur relatif (RID, Relative IDentifier) qui est unique pour chaque unités de sécurité créées dans le domaine. Le maître RID alloue des blocs d'identificateurs relatifs à chaque contrôleur de domaine du domaine. Le contrôleur de domaine affecte ensuite un maître RID aux objets créés à partir de son bloc de maîtres RID alloués.

- *Le maître d'infrastructure.* Lorsque des objets sont déplacés d'un domaine vers un autre, le maître d'infrastructure met à jour dans son domaine les références d'objets qui pointent sur l'objet dans l'autre domaine. La référence d'objet contient l'identificateur global unique (GUID, Globally Unique IDentifier) de l'objet, son nom unique, et un identificateur de sécurité. Active Directory met régulièrement à jour le nom unique et l'identificateur de sécurité sur la référence d'objet afin de refléter les modifications apportées à l'objet réel.

Dans une forêt, chaque domaine possède ses propres émulateur PDC, maître RID et maître d'infrastructure.
(Pour plus d'infos sur les rôles de maître d'opérations voir module 9)

3. Fonctionnement d'Active Directory

a) Introduction.

Cette partie présente la fonction d'Active Directory en tant que service d'annuaire. Comprendre le fonctionnement d'Active Directory vous aidera à gérer les ressources et à résoudre les problèmes d'accès à ces ressources.

b) Définition d'un service d'annuaire.

Dans de grands réseaux, les ressources sont partagées par de nombreux utilisateurs et applications. Pour permettre aux utilisateurs et aux applications d'accéder à ces ressources et aux informations les concernant, une méthode cohérente est nécessaire pour nommer, décrire, localiser, accéder, gérer et sécuriser les informations concernant ces ressources. Un service d'annuaire remplit cette fonction.

Définition d'un service d'annuaire.
Un service d'annuaire est un référentiel d'informations structuré concernant les personnes et les ressources d'une organisation. Dans un réseau Windows Server 2003, le service d'annuaire s'appelle Active Directory.

Fonctionnalités d'Active Directory.

- *Accès pour les utilisateurs et les applications aux informations concernant des objets.* Ces informations sont stockées sous forme de valeurs d'attributs. Vous pouvez rechercher des objets selon leur classe d'objet, leurs attributs, leurs valeurs d'attributs et leur emplacement au sein de la structure Active Directory ou selon toutes combinaison de ces valeurs.
- *Transparence des protocoles et de la topologie physique du réseau.* Un utilisateur sur un réseau peut accéder à toutes ressources sans savoir où celle-ci se trouve ou comment elle est connectée physiquement au réseau.
- *Possibilité de stockage d'un très grand nombre d'objets.* Comme il est organisé en partitions, Active Directory peut répondre aux besoins issus de la croissance d'une organisation.
- *Possibilité d'exécution en tant que service indépendant du système d'exploitation.* AD/AM (Active Directory in Application Mode) est une nouvelle fonctionnalité de l'Active Directory permettant de résoudre certains scénarios de déploiement liés à des applications utilisant un annuaire. AD/AM s'exécute comme un service indépendant du système d'exploitation qui ne nécessite pas de déploiement sur un contrôleur de domaine.

c) Définition d'un schéma

Le schéma Active Directory définit les genres d'objet, les types d'informations concernant ces objets, et la configuration de sécurité par défaut pour les objets pouvant être stockés dans Active Directory.

Définition du schéma.

Le *schéma* contient les définitions de tous les objets comme les utilisateurs, les ordinateurs et les imprimantes stockés dans Active Directory. Les contrôleurs de domaine ne comportent qu'un seul schéma pour toute une forêt. Ainsi, tous les objets créés dans Active Directory se conforme aux mêmes règles.

Le schéma possède deux types de définitions : Les classes d'objets et les attributs. *Les classes d'objets* décrivent les objets d'annuaires possibles que vous pouvez créer. Chaque classe d'objet est un ensemble d'attributs.

Les attributs sont définis séparément des classes d'objets. Chaque attribut n'est défini qu'une seule fois et peut être utilisé dans plusieurs classes d'objets.

Schéma Active Directory et extensibilité.

Vous pouvez créer de nouveaux types d'objets dans Active Directory en développant le schéma.

Modifications et désactivation de schéma.

Sur le contrôleur de domaine, vous pouvez annuler des modifications apportées à un schéma en les désactivant, permettant ainsi aux organisations de mieux exploiter les fonctionnalités d'Active Directory. Vous pouvez également redéfinir une classe ou un attribut de schéma. Vous pourriez, par exemple, modifier la syntaxe de la chaîne Unicode d'un attribut appelé SalesManager pour en faire un nom unique.

d) définition d'un catalogue global.

Dans Active Directory, les ressources peuvent être partagées parmi des domaines et des forêts. Le catalogue global d'Active Directory permet de rechercher des ressources parmi des domaines et des forêts de manière transparentes pour l'utilisateur. En l'absence de serveur de catalogue global, cette requête exigerait une recherche dans chaque domaine de la forêt.

Définition du catalogue global.

Le *catalogue global* est un référentiel d'informations qui contient un sous-ensemble des attributs de tous les objets d'Active Directory. Les membres du groupe Administrateurs du schéma peuvent modifier les attributs stockés dans le catalogue global, en fonction des impératifs d'une organisation. Le catalogue global contient :

- Les attributs les plus fréquemment utilisés dans les requêtes, comme les nom et prénom d'un utilisateur, et son nom d'ouverture de session ;
- Les informations requises pour déterminer l'emplacement de tout objet dans l'annuaire ;
- Un sous-ensemble d'attributs par défaut pour chaque type d'objet ;
- Les autorisations d'accès pour chaque objet et attribut stocké dans le catalogue global. Si vous recherchez un objet pour lequel vous ne possédez pas les autorisations de visualisation requises, cet objet n'apparaîtra pas dans les résultats de la recherche. Les autorisations d'accès garantissent que les utilisateurs ne puissent trouver que les objets pour lesquels ils possèdent un droit d'accès.

Définition d'un serveur de catalogue global.

Un *serveur de catalogue global* est un contrôleur de domaine qui traite efficacement les requêtes intraforêts dans le catalogue global. Le premier contrôleur de domaine que vous créez dans Active Directory devient automatiquement un serveur de catalogue global. Vous pouvez configurer des serveurs de catalogue global supplémentaires pour équilibrer le trafic lié aux authentifications de connexion et aux requêtes.

Fonctions du catalogue global.

Le catalogue global permet aux utilisateurs d'exécuter deux fonctions importantes :

- Trouver les informations Active Directory en tout point de la forêt, indépendamment de l'emplacement des données ;
- Utiliser les informations d'appartenance au groupe universel pour se connecter au réseau.

(Pour plus d'infos sur le catalogue, voir module 8)

e) Définition d'un nom unique et d'un nom unique relatif.

Les ordinateurs clients utilisent le protocole LDAP pour rechercher et modifier des objets dans une base de données Active Directory. Le protocole LDAP est un sous-ensemble de la norme ISO X.500 relative aux services d'annuaire. Il utilise les informations portant sur la structure d'un annuaire pour trouver des objets individuels possédant chacun un nom unique.

Définition.

Le protocole LDAP utilise un nom représentant un objet Active Directory par une série de composants concernant la structure logique. Cette représentation, appelée *nom unique* de l'objet, identifie le domaine dans lequel se trouve l'objet ainsi que le chemin complet permettant d'accéder à celui-ci. Un nom de ce type ne peut être qu'unique dans une forêt Active Directory.

Le *nom unique relatif* d'un objet identifie l'objet de manière unique dans son conteneur. Deux objets situés dans un même conteneur ne peuvent porter le même nom. Le nom unique relatif est toujours le premier composant du nom unique, mais il n'est pas toujours un nom usuel.

Exemple de nom unique

Chaque élément de la structure logique de l'utilisatrice Laura Bertoli de l'unité d'organisation Sales (ventes) du domaine Contoso.msft est représenté dans le nom unique suivant :

CN = Laura Bartoli, OU = Sales, DC = contoso, DC = msft

- CN (Common Name) est le nom usuel de l'objet dans son conteneur.
- OU (Organizatioal Unit) est l'unité d'organisation qui contient l'objet. Plusieurs valeurs d'OU peuvent exister si l'objet se trouve dans une unité d'organisation imbriquée.
- DC (Domain Component) est un composant de domaine, tel que « com » ou « msft ». Il existe toujours au moins deux composants de domaine, voire davantage si le domaine est un domaine enfant.

Les composants de domaine du nom unique sont basés sur le DNS (Domain Name System).

Exemple de nom unique relatif.

Dans l'exemple suivant, Sales est le nom unique relatif d'une unité d'organisation représentée par le chemin LDAP suivant :

OU = Sales, DC = contoso, DC = msft

f) Ouverture de session unique avec Active Directory.

L'activation d'une ouverture de session unique permet à Active Directory de rendre transparents pour l'utilisateur les processus complexes d'authentification et d'autorisation. Les utilisateurs n'ont pas besoin de gérer plusieurs ensembles d'autorisations.
Une ouverture de session unique consiste en :

- une *authentification*, qui vérifie les autorisations de la tentative de connexion ;
- une *autorisation*, qui vérifie que la demande de connexion est autorisée.

En tant qu'ingénieur système, vous devez comprendre le fonctionnement de ces processus afin d'optimiser et de dépanner votre structure Active Directory.

4. Analyse d'Active Directory

a) Introduction

Sous Windows Server 2003, les administrateurs disposent de composants logiciels enfichables et d'outils de ligne de commande pour gérer Active Directory. Ce chapitre présente ces composants et outils, et explique comment les utiliser pour analyser la structure logique et physique d'Active Directory.

b) Gestion d'Active Directory

L'utilisation d'Active Directory vous permet de gérer un grand nombre d'utilisateur, d'ordinateurs et de ressources réseau à partir d'un emplacement centralisé, à l'aide des outils et des composants logiciels enfichables d'administration de Windows Server 2003. Active Directory prend également en charge l'administration décentralisée. Un administrateur possédant l'autorité requise peut déléguer un ensemble sélectionnés de privilèges administratifs à d'autres utilisateurs ou groupes dans une organisation.

Prise en charge par Active Directory de la gestion centralisée.
Active Directory inclut plusieurs fonctionnalités de prise en charge de la gestion centralisée :

- *Informations concernant tous les objets et leurs attributs.* Les attributs contiennent des données qui décrivent la ressource que l'objet identifie ; comme les informations concernant toutes les ressources du réseau sont stockées dans Active Directory, un administrateur peut gérer et administrer ces ressources de façon centralisée.
- *Vous pouvez interroger Active Directory à l'aide de protocoles tels que LDAP*. Vous pouvez aisément localiser des informations concernant des objets en recherchant des attributs sélectionnés de l'objet, à l'aide d'outils prenant en charge le protocole LDAP.
- *Vous pouvez grouper en unités d'organisation des objets possédant des exigences similaires en termes d'administration et de sécurité.* Les unités d'organisations offrent plusieurs niveaux d'autorités administratives, de sorte que vous pouvez appliquer des paramètres de stratégie de groupe et déléguer le contrôle administratif. Cette délégation simplifie le travail de gestion de ces objets et vous permet de structurer Active Directory en fonction des impératifs de votre organisation.

- *Vous pouvez spécifier des paramètres de stratégie de groupe pour un site, un domaine, ou une unité d'organisation.* Active Directory applique ensuite ces paramètres de stratégie de groupe à tous les utilisateurs et ordinateurs à l'intérieur du conteneur.

Prise en charge par Active Directory de la gestion décentralisée.

Active Directory prend également en charge la gestion décentralisée. Vous pouvez affecter des autorisations et accorder des droits aux utilisateurs de manière très spécifique.

Vous pouvez déléguer l'affectation des autorisations :

- pour des unités d'organisation spécifiques à différents groupes de Domaine local ; par exemple, délégation de l'autorisation Contrôle total pour l'unité d'organisation Sales.
- pour modifier des attributs spécifiques d'un objet dans une unité d'organisation ; par exemple, affecter l'autorisation permettant de modifier les nom, adresse et numéro de téléphone d'un utilisateur et de réinitialiser les mots de passe sur l'objet compte d'utilisateur.
- pour exécuter la même tâche ; par exemple, réinitialiser les mots de passe, dans toutes les unités d'organisation d'un domaine

.

c) Outils et composants logiciels enfichables d'administration d'Active Directory.

Windows Server 2003 comporte plusieurs composants logiciels enfichables et outils de ligne de commande permettant de gérer Active Directory. Vous pouvez également gérer Active Directory à l'aide d'objets ADSI (Active Directory Service Interfaces) à partir de l'environnement d'exécution de scripts Windows. ADSI est une interface simple mais néanmoins puissante d'Active Directory permettant de créer des scripts réutilisables pour la gestion d'Active Directory.

Composants logiciels enfichables d'administration

Composant logiciel enfichable.	**Description**
Utilisateurs et ordinateurs Active Directory.	Cette console MMC est utilisée pour la gestion et la publication d'information dans Active Directory. Vous pouvez gérer des comptes d'utilisateur, des groupes et des comptes d'ordinateurs, ajoutez des ordinateurs à un domaine, gérer des stratégies de compte ainsi que des droits d'utilisateur, et procéder à l'audit des stratégie.
Domaines et approbations Active Directory.	Cette console MMC est utilisée pour gérer des approbations de domaines et de forêts, ajouter des suffixes au nom d'utilisateur principal, et modifier les niveaux fonctionnels de domaines et de forêts.
Sites et services Active Directory	Cette console MMC vous permet de gérer la réplication de données d'annuaire.
Schéma Active Directory	Cette console MMC vous permet de gérer le schéma. Il n'est pas disponible par défaut dans le menu Outils d'administration. Vous devez l'ajouter manuellement.

Vous pouvez personnaliser les consoles d'administration afin qu'elles correspondent aux tâches d'administration que vous déléguez à d'autres administrateurs. Vous pouvez également regrouper dans une même console toutes les consoles requises pour chaque fonction d'administration.

Outils de ligne de commande d'administration.

Outil	Description
Dsadd	Ajoute dans Active Directory des objets, comme des ordinateurs, des utilisateurs, des groupes, des unités d'organisation et des contacts.
Dsmod	Modifie dans Active Directory des objets, comme des ordinateurs, des utilisateurs, des groupes, des unités d'organisation et des contacts.
Dsquery	Exécute des requêtes dans Active Directory en fonction de critères spécifiés. Vous pouvez exécuter des requêtes portant sur des serveurs, des ordinateurs, des groupes, des utilisateurs, des sites, des unités d'organisation et des partitions.
Dsmove	Déplace un objet unique, à l'intérieur d'un domaine, vers un nouvel emplacement dans Active Directory ou renomme un objet unique sans le déplacer.
Dsrm	Supprime un objet dans Active Directory
Dsget	Affiche des attributs sélectionnés d'un ordinateur, d'un contact, d'un groupe, d'une unité d'organisation, d'un serveur ou d'un utilisateur dans Active directory
Csvde	Importe et exporte des données Active Directory à l'aide d'un format de séparation par virgule
Ldifde	Crée, modifie et supprime des objets Active Directory. Peut également prolonger le schéma Active Directory, exporter des informations utilisateur et de groupe vers d'autres applications ou service, et charger dans Active Directory des données d'autres services d'annuaire.

Environnement d'exécution de scripts Windows.

Bien que Windows Server 2003 fournisse plusieurs composants logiciels enfichables et outils de ligne de commande pour gérer Active Directory, ceux-ci ne sont pas adaptés pour des opérations de commandes destinées à effectuer des modifications dans Active Directory impliquant des conditions complexes. En pareils cas, vous pouvez procéder plus rapidement à des modifications à l'aide de scripts

Vous pouvez créer des scripts à partir de l'environnement d'exécution de scripts Windows utilisant ADSI pour exécuter les tâches suivantes :

- Extraire les informations concernant les objets Active Directory ;
- Ajouter des objets dans Active Directory ;
- Modifier les valeurs d'attributs pour les objets Active Directory ;
- Supprimer des objets dans Active directory ;
- Etendre le schéma Active Directory.

ADSI utilise le protocole LDAP pour communiquer avec Active Directory.

5.

Processus de conception, de planification et d'implémentation d'Active Directory.

a) Vue d'ensemble de la conception, de la planification et de l'implémentation d'Active Directory

Conception d'active Directory

Un ou plusieurs architectes de systèmes créent la conception d'Active Directory, en se basant sur les besoins d'une entreprise. Ces besoins déterminent les spécifications fonctionnelles pour la conception.

Plan d'implémentation d'Active Directory

Le plan d'implémentation d'Active Directory détermine la mise en œuvre de la conception d'Active Directory en fonction de l'infrastructure matérielle de l'organisation. La conception d'Active Directory peut spécifier le nombre de contrôleur de domaine pour chaque domaine sur la base de la configuration d'un serveur spécifique. Cependant, si cette configuration n'est pas disponible, lors de la phase de planification vous pouvez décider de modifier le nombre de serveurs afin de répondre aux besoins de l'entreprise.

Après avoir implémenté Active Directory, vous devez gérer et assurer la maintenance d'Active Directory afin de garantir disponibilité, fiabilité et sécurité du réseau.

Implémentation d'Active Directory

Durant le déploiement d'Active Directory, les ingénieurs système :

- Créent la structure du domaine et de la forêt, et déploient les serveurs ;
- Créent la structure de l'unité d'organisation ;
- Créent les comptes d'utilisateur et d'ordinateur ;
- Créent des groupes de sécurité et de distribution ;
- Créent les objets Stratégies de groupe (GPO, *Groupe Policy Object*) qu'ils appliquent aux domaines, aux sites et aux unités d'organisation ;
- Créent les stratégies de distribution de logiciels.

b) Processus de conception d'Active Directory

Une conception d'Active Directory inclut plusieurs tâches. Chacune définit les besoins fonctionnels pour un composant de l'implémentation d'Active Directory.

Tâches incluses dans le processus de conception d'Active Directory.

- *Collecte d'informations sur l'organisation.* Cette première tâche définit les besoins en service d'annuaire et les besoins de l'entreprise concernant le projet. Les informations sur l'organisation incluent notamment un profil organisationnel de haut niveau, les implantations géographiques de l'organisation, l'infrastructure technique et du réseau, et les plans liés aux modifications à apporter dans l'organisation.

- *Analyse des informations sur l'organisation.* Vous devez analyser les informations collectées pour évaluer leur pertinence et leur valeur par rapport au processus de conception. Vous devez ensuite déterminer quelles sont les informations les plus importantes et quels composants de la conception d'Active Directory ces informations affecteront. Soyez prêt à appliquer ces informations dans l'ensemble du processus de conception.
- *Analyse des options de conception.* Lorsque vous analyser des besoins d'une entreprise spécifiques, plusieurs options de conception peuvent y répondre. Comme chaque choix que vous faites affecte les autres composants de la conception, restez flexible dans votre approche de la conception durant tout le processus.
- *Sélection d'une conception.* Développez plusieurs conceptions d'Active Directory, puis comparez leurs points forts et leurs points faibles. Lorsque vous sélectionnez un conception, analyser les besoins d'une entreprise qui entre en conflit et tenez compte de leurs effets sur les choix de vos conceptions. Il se peut qu'aucune des conceptions soumises ne fasse l'unanimité. Choisissez la conception qui répond le mieux à vos besoins d'entreprise et qui représente globalement le meilleur choix.
- *Affinage de la conception.* La première version de votre plan de conception est susceptible d'être modifiée avant la phase pilote de l'implémentation. Le processus de conception est itératif parce que vous devez tenir compte de nombreuses variables lorsque vous concevez une infrastructure Active Directory. Révisez et affinez plusieurs fois chacun des concepts de votre conception pour prendre en compte tous les besoins d'entreprise.

Résultat du processus de conception d'Active Directory

- *La conception du domaine et de la forêt.* La conception de la forêt inclut des informations comme le nombre de forêts requis, les consignes de création des approbations et le nom de domaine pleinement qualifié (FQDN, *Fully Qualified Domain Name)* pour le domaine racine de chaque forêt. La conception inclut également la stratégie de contrôle des modifications de la forêt, qui identifie les processus de propriété et d'approbation pour les modifications de la configuration présentant un impact sur toute la forêt. Identifiez la personne chargée de déterminer la stratégie de contrôle des modifications de chaque forêt dans l'organisation. Si votre plan de conception comporte plusieurs forêts, vous pouvez évaluer si des approbations de forêts sont requises pour répartir les ressources du réseau parmi les forêts.

  La conception du domaine indique le nombre de domaines requis dans chaque forêt, le domaine qui sera le domaine racine pour chaque forêt et la hiérarchie des domaines si la conception comporte plusieurs domaines. La conception du domaine inclut également le nom DNS pour chaque domaine et les relations d'approbation entre domaines.

- *La conception de l'unité d'organisation.* Elle indique comment vous créerez les unités d'organisation pour chaque domaine dans la forêt. Incluez une description de l'autorité d'administration qui sera appliquée à chaque unité d'organisation, et à qui cette même autorité sera déléguée. Pour finir, incluez la stratégie utilisée pour appliquer la stratégie de groupe à la structure de l'unité d'organisation.
- *La conception du site.* Elle spécifie le nombre et l'emplacement des sites dans l'organisation, les liens requis pour relier les sites et le coût de ces liens.

c) Processus de planification d'Active Directory

Composant d'un plan Active Directory

- *Stratégie de compte.* Elle inclut des informations comme les consignes d'attribution de nom aux comptes et la stratégie de verrouillage, la stratégie en matière de mots de passe et les consignes portant sur la sécurité des objets.
- *Stratégie d'audit.* Elle détermine comment suivre les modifications apportées aux objets Active Directory.
- *Plan d'implémentation d'unité d'organisation.* Il définit quelles unités d'organisation créer et comment. Si la conception d'unité d'organisation spécifie que ces unités seront créées géographiquement et organisées par division à l'intérieur de chaque zone géographique, le plan d'implémentation des unités d'organisation définit les unités à implémenter. Le plan fournit également des consignes portant sur la délégation d'autorité.
- *Plan de stratégie de groupe.* Il détermine qui crée, relie et gère les objets de stratégie de groupe, et comment cette stratégie sera implémentée.
- *Plan d'implémentation du site.* Il spécifie les sites, les liens qui les relient, et les liaisons de sites planifiées. Il spécifie également la planification et l'intervalle de réplication ainsi que les consignes en matières de sécurisation et de configuration de la réplication entre sites.
- *Plan de déploiement de logiciels.* Il spécifie comment vous utiliserez la stratégie de groupe pour déployer de nouveaux logiciels et des mises à niveaux logiciels. Il peut spécifier si les mises a niveau de logiciels sont obligatoires ou facultatives.
- *Plan de placement des serveurs.* Il spécifie le placement des contrôleurs de domaine, des serveurs de catalogue global, des serveurs DNS intégrés à Active Directory et des maitre d'opérations. Il spécifie également si vous activerez la mise en cache des appartenances à un groupe universel pour les sites ne possédant pas de serveur de catalogue global.

Lorsque tous les plans de composants sont terminés, vous devez les combiner pour former le plan complet d'implémentation d'Active Directory.

d) Processus d'implémentation d'Active Directory

Processus d'implémentation.

Vous devez exécuter les tâches suivantes pour implémenter Active Directory.

- *Implémentation de la forêt, du domaine et de la structure DNS.* Créez le domaine racine de la forêt, les arborescences de domaines et tout autre domaine enfant constituant la forêt et la hiérarchie des domaines.
- *Création des unités d'organisation et des groupes de sécurité.* Créez la structure d'unité d'organisation pour chaque domaine dans chaque forêt, créez des groupes de sécurité et déléguez l'autorité administrative à des groupes administratifs dans chaque unité d'organisation.
- *Création des comptes d'utilisateur et d'ordinateur.* Importez les comptes d'utilisateurs dans Active Directory.
- *Création des objets de stratégies de groupe.* Créez des objets Stratégies de groupe basés sur la stratégie de groupe, puis reliez-les à des sites, a des domaines ou à des unités d'organisation.
- *Implémentation des sites.* Créez des sites en fonction du plan des sites, créez des liens reliant ces sites, définissez les liaisons de sites planifiées et déployez sur les sites des contrôleurs de domaine, des serveurs de catalogue global, des serveurs DNS et des maîtres d'opérations.