L'Active Directory

Présentation d'Active Directory

Active Directory est un annuaire des objets du réseau, il permet aux utilisateurs de localiser, de gérer et d'utiliser facilement les ressources

Objet ACTIVE DIRECTORY

Active Directory stocke des informations sur les objets du réseau. Il existe plusieurs types d'objets : (serveurs • domaines • sites • utilisateurs • ordinateurs • imprimantes …)

Chaque objet possède un ensemble d'attributs :Les attributs permettent d'effectuer des recherches précises dans l'annuaire (trouver l'emplacement physique d'une imprimante, le numéro de téléphone ou l'adresse d'un utilisateur…

Schéma Active Directory

Il stocke la définition de tous les objets d'Active Directory comme les utilisateurs, les ordinateurs et les imprimantes stockés dans Active Directory. il comprend deux types de définitions :

1• Les classes d'objets : Décrit les objets d'Active Directory qu'il est possible de créer. Chaque classe est un regroupement d'attributs.

2• Les attributs : Ils sont définis une seul fois et peuvent être utilisés dans plusieurs classes.

Catalogue global

Un serveur de catalogue global est un contrôleur de domaine qui conserve une copie du catalogue global il contient une partie des attributs les plus utilisés de tous les objets Active Directory.il permet de :

1• Trouver des informations Active Directory sur toutes la forêt

2• Utiliser des informations d'appartenance à des groupes universels pour ouvrir une session sur le réseau.

Structure logique d'Active Directory

1)Les Domaines : domaine est un ensemble d'ordinateurs et/ou d'utilisateurs qui partagent une même base de données d'annuaire. Un domaine a un nom unique sur le réseau

2)Les Unités d'organisation : Une unité d'organisation est un objet utilisé pour organiser les objets au sein du domaine. Il peut contenir d'autres objets comme des comptes d'utilisateurs, des groupes, des ordinateurs, des imprimantes ainsi que d'autres unités d'organisation.

La création et la gestion d'unités d'organisation passent par quatre phases très importantes : (La planification. Le déploiement. La maintenance La suppression)

3)Les Arborescences : Une arborescence est un ensemble de domaines partageant un espace de nom contigu. Par exemple, supinfo.lan est le domaine parent du domaine paris.supinfo.lan et du domaine martinique.supinfo.lan

Le premier domaine installé est le domaine racine de la forêt

La relation d'approbation entre un domaine enfant et son domaine parent est de type bidirectionnel transitif.

4) Les forêts : Une forêt est un ensemble de domaines (ou d'arborescences) n'ayant pas le même nom commun mais partageant un schéma et un catalogue global commun. Par exemple, une même forêt peut rassembler deux arborescences différentes comme laboms.com et supinfo.lan.

5)Les objets : Il s'agit des composants les plus élémentaires de la structure logique. Les classes d'objets sont des modèles pour les types d'objets que vous pouvez créer dans Active Directory.

Structure Physique d'Active Directory

La structure physique permet d'optimiser les échanges d'informations entre les différents contrôleurs de domaine et ce en fonction des débits assurés par les réseaux qui les connectent.

1)Contrôleurs de domaine : Un contrôleur de domaine est un ordinateur exécutant Windows 2003 Server qui stocke un répliqua de l'annuaire. (Un domaine peut posséder un ou plusieurs contrôleurs de domaine)

2)Sites et liens de sites : Un site est une combinaison d'un ou plusieurs sous réseaux connectés entre eux par une liaison à haut débit fiable (liaison LAN). Il permet d'optimiser la communication entres les contrôleurs de domaine

3)Les partitions active directory

La partition de domaine contient les informations concernant tous les objets d'un domaine (les utilisateurs, les groupes, les machines, etc…)

La partition de configuration contient la topologie de la forêt, c'est-à-dire les informations concernant les domaines, les sites, les connexions entre les contrôleurs, etc…

La partition de schéma contient le schéma étendu au niveau de la forêt, c'est-à-dire l'ensemble des définitions des classes et attributs des objets pouvant être créer dans l'annuaire Active Directory.

Les partitions d'applications facultatives contiennent des objets non liés à la sécurité et utilisés par une ou plusieurs applications.

Implémentation d'une structure de forêt et de domaine Active Directory

Condition requise pour pouvoir installer Active Directory :

Un ordinateur exécutant Windows 2003 serveur

250 Mo d'espace libre sur une partition NTFS

Les paramètres TCP/IP configuré pour joindre un serveur DNS

Un serveur DNS faisant autorité pour gérer les ressources SRV

Procédure de création du domaine racine de la forêt

Vous utilisez l'Assistant Installation de Active Directory pour créer une structure de forêt et de domaine. Lorsque vous installez Active Directory dans un réseau pour la première fois, vous devez créer un domaine racine de la forêt.

Pour créer un domaine racine de la forêt, procédez comme suit :

1. Cliquez sur **Démarrer**, sur **Exécuter**, puis tapez **dcpromo** en tant que nom du programme.

Espace de nom DNS et active directory

-le domaine DNS et Active directory utilise des noms de domaine identique ainsi les ordinateurs peuvent utiliser le DNS pour rechercher des CD et d'autres ordinateur fournissant des services Active directory

(le nom DNS=compte d'ordinateur stocké sur AD)

Les relations d'approbation :

Les approbations sont des mécanismes qui permettent à un utilisateur authentifié dans son propre domaine d'accéder aux ressources de tous les domaines approuvés. Dans Windows Server 2003, il existe deux types d'approbations : transitives et non transitives.

- Les outils d'administration d'Active Directory

Utilisateurs et ordinateurs Active Directory : C'est le composant le plus utilisé pour accéder à l'annuaire. Il permet de gérer les comptes d'utilisateurs, les comptes d'ordinateurs, les fichiers et les imprimantes partagés, les unités d'organisation. Utilisez ce composant logiciel enfichable lorsque vous n'avez que quelques objets Active Directory à gérer.

Sites et Services Active Directory : Ce composant permet de définir des sites, des liens de sites et de paramétrer la réplication Active Directory.

Domaines et approbations Active Directory : Ce composant permet de mettre en place les relations d'approbations et les suffixes UPN. Il propose aussi d'augmenter le niveau fonctionnel d'un domaine ou d'une forêt.

Schéma Active Directory : Ce composant permet de visualiser les classes et les attributs de l'annuaire. Pour pouvoir accéder à la console **Schéma Active Directory**, il faut dans un premier temps **enregistrer une DLL**. Pour cela, il vous faut ouvrir une invite de commande et taper la commande : **regsvr32schmmgmt.dll**

Gestion des Stratégies de Groupe : Ce composant permet de centraliser l'administration des stratégie de groupe d'une forêt, de vérifier le résultat d'une stratégie de groupe ou bien encore de comparer les paramètres de deux stratégies de groupe. Ce composant n'est pas disponible sur le CD-ROM de Windows 2003 Server, il doit être téléchargé sur le site de Microsoft.

ADSI Edit : Ce composant permet de visualiser l'arborescence LDAP réelle du service d'annuaire. Elle peut s'avérer utile pour lire ou modifier certains attributs ou certains objets de l'annuaire. Elle permet aussi d'attribuer des permissions sur les objets de l'annuaire avec une granularité plus fine. En outre, elle se révèle quasi indispensable pour développer une application accédant aux données contenues dans l'annuaire. Cette console doit être installée avec les outils de support situés sur le CD-ROM de Windows 2003 Server.

En complément des divers composants logiciels enfichables énumérés ci-dessus, divers outils sont mis à la disposition de l'administrateur pour gérer Active Directory :

Lpc.exe : Cet outil permet d'envoyer manuellement des requêtes LDAP vers n'importe quel annuaire LDAP (Active Directory, NDS, Open LDAP,…). Il peut être utilisé pour vérifier la connectivité entre une machine et l'annuaire ou bien pour lister des informations bien spécifiques dans une partie de l'annuaire. LPC affiche l'intégralité des données échangées entre le poste dient et le service d'annuaire. Il est disponible avec les outils de support situés sur le CD-ROM de Windows 2003 Server.

DSADD : Cet outil en ligne de commande permet d'ajouter des objets dans l'annuaire Active Directory.

DSMOD : Cet outil en ligne de commande permet de modifier des objets dans l'annuaire Active Directory.

DSMOVE : Cet outil en ligne de commande permet de déplacer un objet de son conteneur actuel vers un nouvel emplacement.

DSRM : Cet outil en ligne de commande permet de supprimer des objets dans l'annuaire Active Directory.

DSQUERY: Cet outil en ligne de commande permet d'interroger la base de données Active Directory selon des critères spécifiés.

Ldifde : L'outil en ligne de commande LDIFDE (LDAP Data Interchange Format Directory Export) permet d'importer des données à partir d'un fichier texte vers Active Directory ou bien d'exporter des données à partir d'Active Directory vers un fichier texte.

Csvde : L'outil en ligne de commande CSVDE est utilisé pour importer des comptes d'utilisateurs à partir d'un fichier texte vers Active Directory.

WSH : WSH pour Windows Scripts Host est un environnement permettant d'exécuter des scripts en VBS ou en JScript.sur une plateforme Windows 9x ou NT

Délégation du contrôle administratif des unités d'organisation

Active Directory est un système intégrant la sécurisé : seuls les comptes ayant reçu les permissions adéquates peuvent effectuer des opérations sur ces objets (ajout, modification, …).Les administrateurs, en charge de cette affectation de permissions peuvent aussi déléguer des tâches d'administration à des utilisateurs ou des groupes d'utilisateurs

Implémentation de comptes d'utilisateurs, de groupes et d'ordinateurs

Compte d'utilisateur Un compte d'utilisateur permet à un utilisateur physique d'ouvrir une session unique sur le domaine et d'accéder aux ressources partagées.

Il existe trois types de comptes d'utilisateurs, chacun ayant une fonction spécifique :

1)Un compte d'utilisateur local permet à un utilisateur d'ouvrir une session sur un ordinateur spécifique pour accéder aux ressources sur cet ordinateur.

2)Un compte d'utilisateur de domaine permet à un utilisateur de se connecter au domaine pour accéder aux ressources réseau, ou à un ordinateur individuel pour accéder aux ressources sur cet ordinateur.

3)Un compte d'utilisateur intégré permet à un utilisateur d'effectuer des tâches d'administration ou d'accéder temporairement aux ressources réseau.

Compte d'ordinateur **:**Un compte d'ordinateur permet d'identifier un ordinateur physique dans un domaine par le biais d'un mécanisme d'authentification. Il est possible d'activer l'audit de l'accès d'un compte d'ordinateur aux ressources du domaine.

Compte de groupe **:** Un compte de groupe permet de simplifier l'administration en regroupant des comptes d'utilisateurs, d'ordinateurs ou bien d'autres comptes de groupes.

Un utilisateur peut être membre de plusieurs groupes. Les groupes se différencient de par leur type et de par leur étendue. Il existe deux types de groupes dans Active Directory :

Les groupes de sécurité :

Vous utilisez des groupes de sécurité pour affecter des droits et des autorisations aux groupes d'utilisateurs et d'ordinateurs. Les droits déterminent les fonctions que les membres d'un groupe de sécurité peuvent effectuer dans un domaine ou une forêt. Les autorisations déterminent quelles ressources sont accessibles à un membre d'un groupe sur le réseau.

Une méthode d'utilisation efficace des groupes de sécurité consiste à utiliser l'imbrication, c'est à dire, ajouter un groupe à un autre groupe. Le groupe imbriqué hérite des autorisations du groupe dont il est membre, ce qui simplifie l'affectation en une fois des autorisations à plusieurs groupes, et réduit le trafic que peut engendrer la réplication de l'appartenance à un groupe.

Les groupes de distribution :

Vous pouvez utiliser des groupes de distribution uniquement avec des applications de messagerie, telles que Microsoft Exchange, pour envoyer des messages à un ensemble d'utilisateurs. La sécurité n'est pas activée sur les groupes de distribution, ce qui signifie qu'ils ne peuvent pas être répertoriés dans des listes de contrôle d'accès discrétionnaire (DACL, Discretionary Access Control List). Pour contrôler l'accès aux ressources partagées, créez un groupe de sécurité.

Etendue des groupes:

L'étendue d'un groupe détermine la manière dont les permissions sont assignées à ses membres. Les groupes Windows Server 2003, qu'ils soient de type sécurité ou distribution, sont classifiés en trois étendues de groupe possibles : Domaine local, globale et Universelle.

Implémentation d'une stratégie de groupe

Une stratégie de groupes est un objet Active Directory qui va contenir un ensemble de paramètres. Une stratégie de groupe peut aussi être appelée GPO (Group Policy Object)

Les GPO sont des collections de paramètres de configuration allant des droits des utilisateurs à l'ouverture de session, aux privilèges d'accès aux logiciels qu'il sera possible d'exécuter su un système donné.

- Les différents niveaux fonctionnels dans Active Directory :

Le niveau fonctionnel d'un domaine ou d'une forêt dans Active Directory définit l'ensemble des fonctionnalités supportées par le service d'annuaire Active Directory dans ce domaine ou dans cette forêt.

Dans Windows Server 2003, il existe quatre niveaux fonctionnels de domaine : Windows 2000 mixte (Par défaut), Windows 2000 natif, Windows Server 2003 intermédiaire et Windows Server 2003.Windows 2000 mixte **:** supporte la prise en charge des contrôleurs de domaine sous Windows NT 4, Windows 2000 et Windows Server 2003.

Windows 2000 natif **:** supporte la prise en charge des contrôleurs de domaine sous Windows 2000 et Windows Server 2003.

Windows Server 2003 intermédiaire**:** supporte la prise en charge des contrôleurs de domaine sous Windows NT4 et Windows Server 2003

Les zones DNS intégrées à Active Directory

Une zone est une partie de l'espace de nom de domaine possedant un groupement logique d'enregistrement de ressources qui permet de transrerer des zones et des enregistrement pour fonctionet autant qu'unité unique

Les zones intégrés a active directory sont des zones principales et stube stocké comme objet dans la base de donnés active directory

Les avantages des zones intégrées à AD

1)Mise à jour de configuration de maîtres multiples et sécurité avancée reposant sur les fonctionnalités d'Active Directory.

2)Zone peut être mise à jour par les serveurs DNS fonctionnant sur tout contrôleur de domaine du domaine.

3)Les zones sont automatiquement répliquées et synchronisées sur les nouveaux contrôleurs de domaine dès qu'ils sont ajoutés à un domaine Active Directory.

4)La réplication d'annuaire est plus rapide et efficace que la réplication DNS standard.

DHCP

Le protocole DHCP est une norme IP permettant de simplifier la gestion de la configuration IP hôte. La norme DHCP permet d'utiliser les serveurs DHCP pour gérer l'allocation dynamique des adresses IP et des autres données de configuration IP pour les clients DHCP de votre réseau.

Comment le protocole DHCP alloue des adresses IP :

Le protocole DHCP gère l'attribution et la libération des données de configuration d'adresse IP en louant la configuration d'adresse IP au dient par l'utilisation d'un bail.

Le bail DHCP spécifie la durée pendant laquelle le client peut utiliser les données de configuration IP

Le processus de création d'un bail DHCP est le processus permettant au client

Processus de création d'un bail DHCP

DHCP de recevoir des données de configuration d'adresse IP du serveur DHCP.

1)Le client DHCP diffuse un paquet DHCPDISCOVER pour localiser un serveur DHCP.

2)Le serveur DHCP diffuse un paquet DHCPOFFER au client. pour proposer le bail d'une adresse IP à un dient DHCP.

3)Le client DHCP diffuse un paquet DHCPREQUEST. Un paquet DHCPREQUEST est un message envoyé par un client au serveur DHCP pour demander ou renouveler le bail de son adresse IP.

4)Le serveur DHCP diffuse un paquet DHCPACK au client. pour accuser réception ce message contient un bail valide pour l'adresse ip ainsi que d'autre domaine de configuration.

Processus de renouvellement d'un bail DHCP

Le processus de renouvellement d'un bail ou de mettre à jour ses données de configuration d'adresse IP à l'aide du serveur DHCP.

Un client DHCP tente automatiquement de renouveler son bail lorsque sa durée a expiré de 50 %. Si le serveur DHCP est disponible, il renouvelle le bail et envoie au client un paquet DHCPACK contenant la durée du nouveau bail et les paramètres de configuration mis à jour.Si le serveur DHCP n'est pas disponible, le dient continue à utiliser ses paramètres de configuration en cours.

Autorisation DHCP

L'autorisation DHCP est le processus d'enregistrement du service Serveur DHCP dans le domaine du service d'annuaire Active Directory, afin de prendre en charge les clients DHCP.

Configuration d'une étendue DHCP

Une étendue est une plage d'adresses IP valides disponibles pour les baux ou l'attribution à des ordinateurs clients sur un sous-réseau spécifique.

C'est le pool d'adresse IP que le serveur peut attribuer au client DHCP (Une seul etendue peut etre attribuer a un sous réseau)

Configuration d'un agent de relais DHCP

Un agent de relais DHCP est un ordinateur ou un routeur configuré pour écouter les messages DHCP/BOOTP des clients DHCP et les transmettre aux serveurs DHCP sur différents sous-réseaux.

Fonctionnement de l'agent de relais

1)client diffuse un paquet DHCPDISCOVER

2)L'agent de relais transmet le message DHCPDISCOVER au serveur DHCP

3)Le serveur envoie un message DHCPOFFER a l'agent de relais DHCP

4)L'agent de relais diffuse le paquet DHCPOFFER

5)CLIENT1 diffuse un paquet DHCPREQUEST

6)L'agent de relais transmet le message DHCPREQUEST au serveur DHCP

7)Le serveur envoie un message DHCPACK a l'agent de relais DHCP

8)L'agent de relais diffuse le paquet DHCPACK

Gestion d'une base de données DHCP

Base de données DHCP

La base de données DHCP est une base de données dynamique qui est mise à jour lorsque les clients DHCP obtiennent ou libèrent leurs baux d'adresses TCP/IP (Transmission Control Protocol/Internet Protocol).

Journal d'audit DHCP :

Un fichier journal d'audit DHCP est un journal où sont consignés des événements relatifs à un service, par exemple le moment où :1)le service démarre ou s'arrête ;2)des autorisations ont été vérifiées ; 3)des adresses IP sont louées, renouvelées, libérées ou refusées.

DNS

Définition
DNS est une base de données distribuée hiérarchisée qui contient les mappages de noms d'hôtes DNS à des adresses IP
Fonction de DNS
1)DNS prend en charge l'accès aux ressources à l'aide de noms alphanumériques.
3)Avec DNS, les noms d'hôtes résident dans une base de données qui peut être distribuée entre plusieurs serveurs, ce qui diminue la charge de chaque serveur et permet d'administrer le système de noms par partitions.
2)DNS prend en charge des noms hiérarchiques et permet d'inscrire divers types de données en plus du mappage de noms d'hôtes à adresse IP qui est utilisé dans les fichiers Hosts.
une comparaison entre les noms NetBios et DNS :
Noms d'ordinateur NetBios : Type(Plat) Taille maximale (15 caractères) Services de noms(WINS, monodiffusion NetBios, fichier Lmhosts)
Noms d'ordinateur DNS : Type(Hiérarchique) Taille maximale (63 octets par étiquette 255 octets par FQDN) Services de noms(DNS, fichier Hosts)

Espace de noms de domaines
est une arborescence hiérarchisée de noms utilisée par DNS pour identifier et trouver un hôte donné dans un domaine donné, par rapport à la racine de l'arborescence
Fonctioneent :Organiser les noms de ressource en une structure logique facile a comprendre
1)Domaine : toute arborescence ou sous arborescence se trouvant dans l'espace de noms de domaine.
2)Domaine racine : Représenté par un(.)indiquant que le nom et a la racise c'est-à-dire au plus haut niveau
3)Domaine de niveau supérieur : C'est la partie a l'extréme droite qui définit le statut organisationnel (.com , .ma..)
4)Domaine de second niveau :Un nom de domaine de second niveau est un nom unique de longueur variable. Dans l'exemple www.microsoft.com, le nom de second niveau est la portion « .microsoft » du nom de domaine, inscrite par InterNIC et affectée à Microsoft Corporation.
5)Sous-domaine : Quand une organisation subdivise son nom de domaine en ajoutant des services ou départemeny représenté par une portion distincte dans le nom de domaine (drif.ofppt.ma)
6)Nom de domaine pleinement qualifié : est un nom de domaine DNS qui a été défini de façon non ambiguë pour indiquer avec certitude son emplacement dans l'arborescence de l'espace de noms de domaine.

les requêtes DNS
Une requête est une demande de résolution de noms envoyée à un serveur DNS. Il existe deux types de requêtes : requêtes récursives et requêtes itératives.
Requête récursive :
-le client DNS demande au serveur de fournir une réponse complète.
-le serveur peut uniquement renvoyer une réponse complète ou indiquer qu'il ne sait pas résoudre le nom
-Une requête récursive ne peut pas être redirigée vers un autre serveur DNS.
-Les requêtes récursives sont lancées par un client DNS ou par un serveur DNS configuré pour utiliser des redirecteurs
-La réponse à une requête récursive peut être positive ou négative.
Les données demandées.
Un message d'erreur indiquant que les données du type demandé n'existent pas.
Un message indiquant que le nom de domaine spécifié n'existe pas.
Fonctionnement d'une requête récursive
1. Le client envoie une requête récursive au serveur DNS local.
2. Le serveur DNS local essaie de trouver une réponse dans la zone de recherche directe et dans le cache.
3. S'il trouve la réponse à la requête, le serveur DNS la renvoie au client.
4. S'il ne trouve pas de réponse, le serveur DNS utilise l'adresse d'un redirecteur ou des indications de racine pour chercher plus haut dans l'arborescence.
Requêtes itératives
Une requête itérative est une requête envoyée à un serveur DNS dans laquelle le client DNS demande la meilleure réponse que peut fournir le serveur DNS sans faire appel à d'autres serveurs DNS. Les requêtes itératives sont parfois appelées requêtes non récursives.
Fonctionnement d'une requête itératives
1. Le serveur DNS local reçoit une requête récursive d'un client DNS.
2. Le serveur DNS local envoie une requête itérative au serveur racine pour obtenir un serveur de noms faisant autorité.
3. Le serveur Racine répond par une référence à un serveur DNS plus proche du nom de domaine demandé.
4. Le serveur DNS local envoie ensuite une requête itérative au serveur DNS plus proche du nom de domaine demandé.
5. Le processus continue jusqu'à ce que le serveur DNS local reçoive une réponse faisant autorité.
6. Cette réponse est alors envoyée au client DNS.

Définition d'un redirecteur :
Un redirecteur est un serveur DNS que d'autres serveurs DNS internes désignent comme responsable du transfert des requêtes pour la résolution de noms de domaines externes ou hors site.

Les indications de racine
Les indications de racine sont des enregistrements de ressources DNS stockés sur un serveur DNS qui répertorient les adresses IP des serveurs racines du système DNS.
Fonction d'une indication de racine
-le serveur DNS reçoit une requête DNS, il consulte sa mémoire cache. S'il n'a pas l'adresse IP du serveur DNS faisant autorité pour ce domaine et qu'il est configuré avec les adresses IP des indications de racine, le serveur DNS interroge un serveur racine sur le domaine situé à gauche du domaine racine de la requête.
-Le serveur continue de parcourir le FQDN jusquu'a ce qu'a ce qu'il trouve le serveur faisont autorité
-Les indications de racine sont stockées dans le fichier Cache.dns qui se trouve dans le dossier %Systemroot%\System32\Dns.
Les redirecteurs
Un redirecteur est un serveur DNS que d'autres serveurs DNS internes désignent comme responsable du transfert des requêtes pour la résolution de noms de domaines externes ou hors site.

La mise en cache du serveur DNS
La mise en cache est le processus qui consiste à stocker temporairement dans un sous-système de mémoire spécial des informations ayant fait l'objet d'un accès récent pour y accéder plus rapidement ensuite.
Fonctionnement du cache des serveurs DNS
Les données placées dans la memoire cache ont une durée de vir TTL qui décrement avec le temps.le serveur doit alors les supprimés du mémoire cache

Configuration des zones DNS
Enregistrements de ressources
A : résout un d'hôte en adresse IP
PTR : Résout une adresse IP en nom d'hôte
SOA : premier enregistrement dans tout fichier de zone
SRV : Résout les noms des serveurs qui fournissent des services
NS : identifie le serveur DNS associé a chaque zone
MX : serveur de messagerie.
CNAME :Résout un nom d'hôte en nom d'hôte

Zones DNS
Une zone est un ensemble de mappages de nom d'hôte à adresse IP pour des hôtes situés dans une portion contiguë de l'espace de noms DNS.
Les données d'une zone sont gérées sur un serveur DNS et peuvent être stockées de deux manières :
• En tant que fichier de zone plat contenant des listes de mappages ;
• Dans une base de données Active Directory.
•Un serveur DNS fait autorité pour une zone s'il héberge les enregistrements de ressources correspondant aux noms et aux adresses que les clients demandent dans le fichier de zone.
• Une zone DNS est :
-soit une zone principale, secondaire ou de stub.
- soit une zone de recherche directe ou inversée.
Sécurisation d'une zone DNS
Pour plus de sécurité, vous pouvez contrôler les personnes autorisées à administrer les zones DNS en modifiant la liste de contrôle d'accès. La liste DACL permet de contrôler les autorisations accordées aux utilisateurs et aux groupes Active Directory qui peuvent contrôler les zones DNS.
Types de zones DNS
1)Zone principale : Une zone principale est l'exemplaire faisant autorité de la zone DNS. Les enregistrements de ressources y sont créés et gérés.
2)Zone secondaire : Une zone secondaire est une copie en lecture seule de la zone DNS.
Zone de stub
3)Les zones de stub : sont des copies d'une zone qui contiennent uniquement les enregistrements de ressources nécessaires à l'identification du serveur DNS faisant autorité pour la zone en question. Une zone de stub contient un sous ensemble des données de la zone qui se compose d'un enregistrement SOA, NS et A, également appelé enregistrement de résolution par requêtes successives.
Zones de recherche
1) Zone de recherche directe : Dans le système DNS, une recherche directe est un processus d'interrogation qui recherche le nom affiché du domaine DNS d'un ordinateur hôte pour trouver son adresse IP
2)Zone de recherche inversée :Dans le système DNS, une recherche inversée est un processus d'interrogation qui recherche l'adresse IP d'un ordinateur hôte pour trouver son nom affiché dans le domaine DNS.
Transferts de zone DNS
Un transfert de zone est le transfert total ou partiel des données d'une zone à partir du serveur DNS vers un serveurs DNS secondaires Il existe deux types de transferts de zone DNS :
1)Transfert de zone complet : Lorsqu'une requête DNS est effectuée avec le type de requête AXFR, la réponse est un transfert de l'intégralité de la zone. Une requête AXFR est une demande de transfert de zone complet.
2)Transfert de zone incrémentiel :Type de requête utilisé par certains serveurs DNS pour mettre à jour et synchroniser les données d'une zone lorsque celle-ci a subi des modifications depuis la dernière mise à jour.
Processus de transfert de zone
SRV SECONDAIRE > REQUETE SOA POUR UNE ZONE
SRV PRINCIPALE > RQUETE A LA REQUETE SOA
SRV SECONDAIRE > Requête IXFR OU AXFR POUR UNE ZONE
SRV PRONCIPALE> REPONCE A LA REQUETE IXFR (TRANSFERT DE ZONE)

Notification DNS (DNS Notify)
DNS Notify est une mise à jour de la spécification d'origine du protocole DNS qui permet d'informer les serveurs secondaires lorsqu'une zone est modifiée.
Fonctionnement de DNS Notify
1. La zone locale hébergée sur un serveur DNS principal est mise à jour.
2. Dans l'enregistrement de ressource SOA, le champ Numéro de série est mis à jour pour indiquer qu'une nouvelle version de la zone a été écrite sur un disque.
3. Le serveur principal envoie un message de notification à tous les serveurs qui figurent dans sa liste de notification.
4. Tous les serveurs secondaires de la zone qui reçoivent le message de notification réagissent en renvoyant une requête de type SOA au serveur principal expéditeur de la notification

Mise à jour dynamique :
Une mise à jour dynamique est le processus par lequel un client DNS crée, inscrit ou met à jour de façon dynamique ses enregistrements dans des zones maintenues par des serveurs DNS qui peuvent accepter et traiter des messages pour des mises à jour dynamiques

Délégation d'une zone DNS
En termes techniques, la délégation est le processus qui affecte l'autorité sur les domaines enfants de votre espace de noms DNS à une autre entité en ajoutant des enregistrements dans la base de données DNS
Surveillance du service DNS :
Nslookup : permet d'effectuer des requêtes de test vers des serveurs DNS et d'obtenir des réponses détaillées depuis l'invite de commande
Journal des événements DNS :VLe journal des événements DNS est un journal système configuré pour n'enregistrer que les événements DNS
Enregistrement de débogage DNS : L'enregistrement de débogage DNS est un outil journal facultatif pour DNS, qui stocke les informations DNS

Résolution de noms NetBIOS à l'aide du service WINS
Composants du service WINS
Serveur WINS est un Ordinateur qui traite les requêtes d'inscription de nom provenant des clients WINS, inscrit les noms et adresses IP du client, puis répond aux requêtes de noms NetBIOS soumises par les clients. Le serveur WINS renvoie ensuite l'adresse IP d'un nom demandé, si ce dernier figure dans la base de données du serveur.
Base de données WINS stocke et réplique les mappages des noms NetBIOS aux adresses IP d'un réseau.
Client WINS est un Ordinateurs que vous pouvez configurer pour utiliser directement un serveur WINS ; ces ordinateurs possèdent généralement plusieurs noms NetBIOS .
Agents proxy WINS est un Ordinateur qui contrôle la diffusion des requêtes de noms et répond lorsque les noms ne figurent pas sur le sous-réseau local. Le proxy communique avec un serveur WINS pour résoudre les noms, puis les met en cache pour une période donnée.
Présentation d'un type de noeud NetBIOS
Nœud de diffusion B : Méthode utilisant les diffusions pour l'inscription et la résolution de noms.
Nœud point à point P : Méthode n'utilise pas de diffusions car il interroge directement le serveur de noms, ce qui permet aux ordinateurs de résoudre les noms NetBIOS en franchissant les routeurs.
Nœud M : Combine le noeud B et le noeud P, mais fonctionne par défaut comme un noeud B. Si le noeud M ne peut pas résoudre un nom par diffusion, il utilise le serveur de noms NetBIOS du noeud P.
Noeud hybride H : Combine le noeud P et le noeud B, mais fonctionne par défaut comme un noeud P. Si le noeud H ne peut pas résoudre un nom via le serveur de noms NetBIOS, il utilise une diffusion.
Configuration de la réplication WINS
Bien qu'un seul serveur WINS puisse traiter les requêtes de résolution de noms NetBIOS pour des milliers de clients, vous devez appliquer une tolérance aux pannes supplémentaires en configurant un deuxième ordinateur exécutant Windows Server 2003. Cet ordinateur fera office de serveur WINS secondaire
Fonctionnement de la réplication par émission
La réplication par émission est le processus qui consiste à copier les données WINS mises à jour d'un serveur WINS sur d'autres serveurs WINS, à chaque fois que le serveur WINS contenant ces données mises à jour atteint un seuil de modifications spécifié.
1. Un partenaire émetteur avertit ses partenaires de réplication à chaque fois que le nombre de modifications apportées à sa base de données WINS dépasse un seuil spécifique, configurable.
2. Lorsque les partenaires de réplication répondent à sa notification par une requête de réplication, le partenaire émetteur leur envoie les réplicas de ses nouvelles entrées de base de données.
Fonctionnement de la réplication par réception
La réplication par réception est le processus qui consiste à copier les données WINS mises à jour d'un serveur WINS sur un autre serveur WINS à des intervalles spécifiés, configurables.
Le processus de réplication par réception se déroule comme suit :
1. Un partenaire récepteur demande, à intervalles réguliers, les modifications apportées à une base de données WINS.
2. Les partenaires de réplication répondent à cette demande en envoyant toutes les nouvelles entrées de la base de données au partenaire récepteur.

Création une OU :
dsadd ou "ou=bemoussi,ou=casa,dc=yassine,dc=ma"
renommer une Ou :
dsmove "ou=yassine,dc=maroc,dc=ma" -newname yassinet
déplacer une OU :
dsmove "ou=yassine,dc=maroc,dc=ma" -newparent ou=casa,dc=maroc,dc=ma
Création d'un utilisateur :
dsadduser"cn=yassine2,ou=casa,dc=yassine,dc=ma" -samid yassine2
-upn yassine2@yassine.ma -fn rakhif -ln yassine2
-display "yassine2 rakhif" -pwd P@ssw0rd
Création d'un compte ordinateur :
dsadd computer"cn=pc1,ou=casa,dc=yassine,dc=ma"
supprimer un compte utilisateur:
dsrm "cn=yassine,ou=casa,dc=yassine,dc=ma"
Modifier un compte d'utilisateur :
dsmod user "cn=yasine,ou=casa,dc=yassine,dc=ma" -tel 065412541
Modifier un compte d'ordinateur :
dsmod computer "cn=pc1,ou=casa,dc=yassine,dc=ma" -loc "batiment 2"
Activer ou désactiver un compte utilisateur :
dsmod user "ou=yassine,dc=maroc,dc=ma" -disabled yes/no
Création d'un groupe :
dsaddgroup"cn=group1,ou=casa,dc=yassine,dc=ma" -secgrp yes -scope g/L -samid group1
supprimer un groupe :
dsrm "cn=group1,ou=casablanca,dc=yassine,dc=ma"
Voir les groupes qu'un user apartient:
dsgetuser"cn=yassine,ou=casablanca,dc=yassine,dc=ma" –memberof
rechercher un utilisateur :dsquery user -name t*
rechercher un ordinateur :dsquery computer -name pc*
Partager un fichier :
net share dossier=c:/windows/dossier /cache:'manual,documents,programs,none'
Monter un lecteur reseau:
net use Z: \\serveurX\NomDossier
Démonter un lecteur reseau :
net use Z: /delete
Voir les groupes qu'un user apartient:
dsgetuser"cn=yassine,ou=casablanca,dc=yassine,dc=ma" -memberof