2013

Active Directory Windows Serveur 2008

CONFIGURATION ET RESOLUTION DES PROBLEMES

OLIVIER D.

Table des matières

1 Présentation des Services de Domaine AD

1.1 Identité et accès : IDA

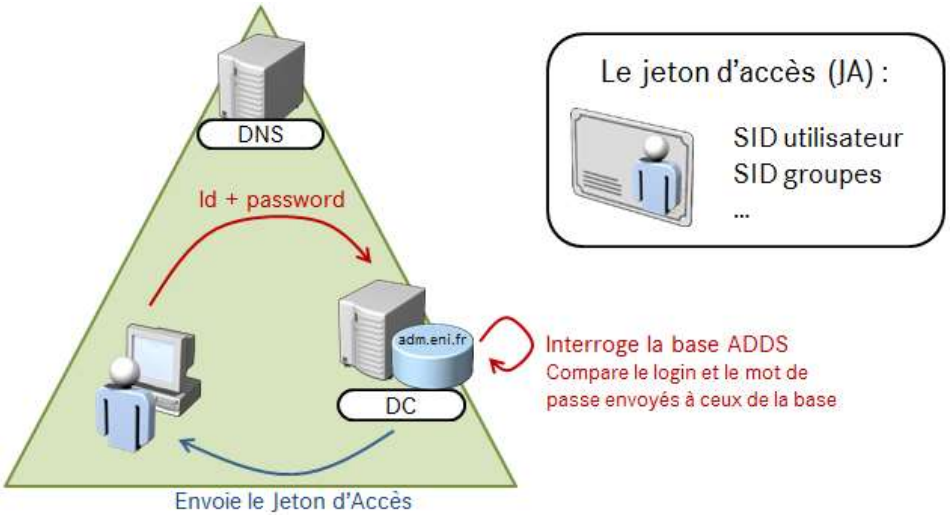
But : Restreindre les accès, vérification du SID (identifiant de sécurité)

Utilisateur → compte utilisateur → SID (déterminé par la machine, unique)

- La base de données annuaire contient tous les SID

Ressource à laquelle on demande l'accès implique des autorisations, implique des ACL / ACE

- Le jeton d'accès (JA) est comparé à la liste ACL pour autoriser le niveau d'accès demandé



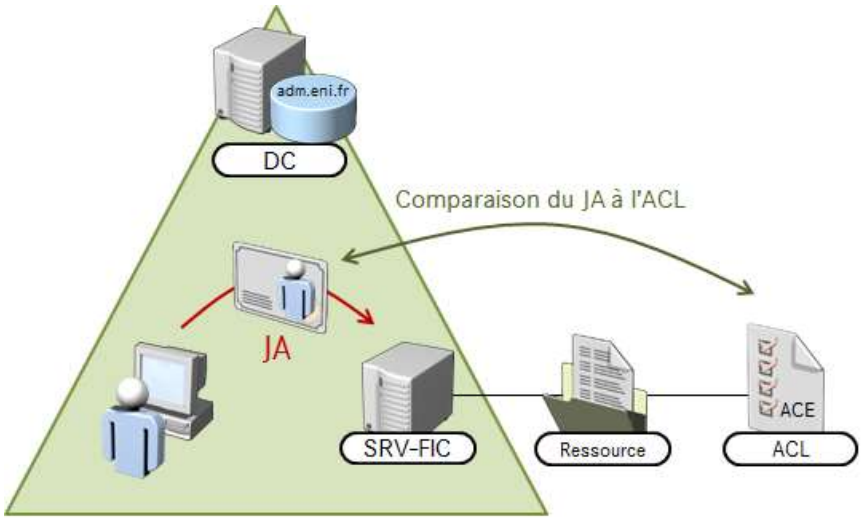
Opération d'obtention du Jeton d'accès (JA)

L'authentification est le processus de vérification de l'identité d'un utilisateur (Id + password)

- Ouverture de session locale (ordi local) → rare (pas le cas d'un domaine)
- Ouverture de session distante (ordi distant) → accès à des ressources

Un jeton d'accès contient : SID utilisateur, SID groupes d'appartenance, privilèges (droits utilisateur)

Ce jeton d'accès est conservé sur l'ordinateur local de l'utilisateur qui s'authentifie



Comparaison du jeton d'accès à l'ACL

Un peu de vocabulaire :

- Les SACL (informations d'audit), ACL / DACL (listes d'autorisations) et ACE (entrées d'autorisations) sont appelées 'Descripteurs de sécurité'. Ils sont liés à la ressource qui est accédée (le répertoire).
- Le jeton d'accès effectue une demande d'autorisation à la ressource.
- Le jeton d'accès contient les différents SID auxquels il appartient (SIDutilisateur, SIDgroupes)

Différence entre un poste autonome et un poste dans le domaine :

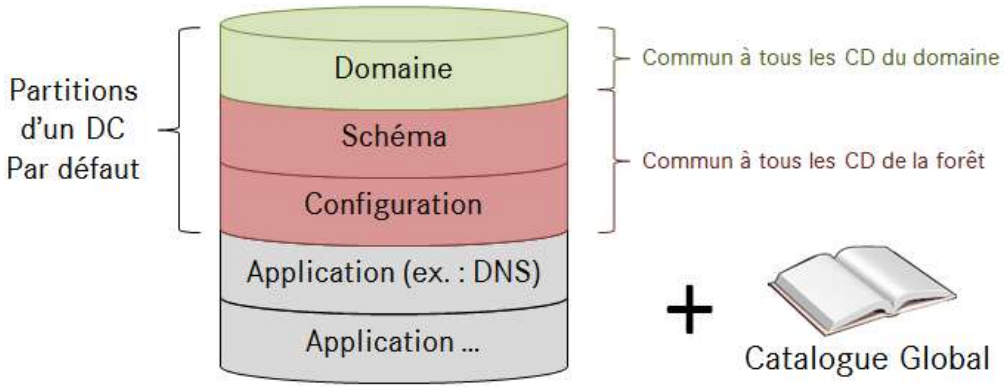
- Un poste autonome contient les informations d'authentification dans sa base SAM (seuls des DC n'ont pas de base SAM).
- Un poste dans un domaine Active Directory contient les informations d'authentification dans la base ADDS. Cette base est un magasin d'identités centralisé et approuvé par tous les membres du domaine sur le DC.

1.2 Composants d'AD

Outils d'administration > Util & ordi AD et Outils d'administration > Modification ADSI

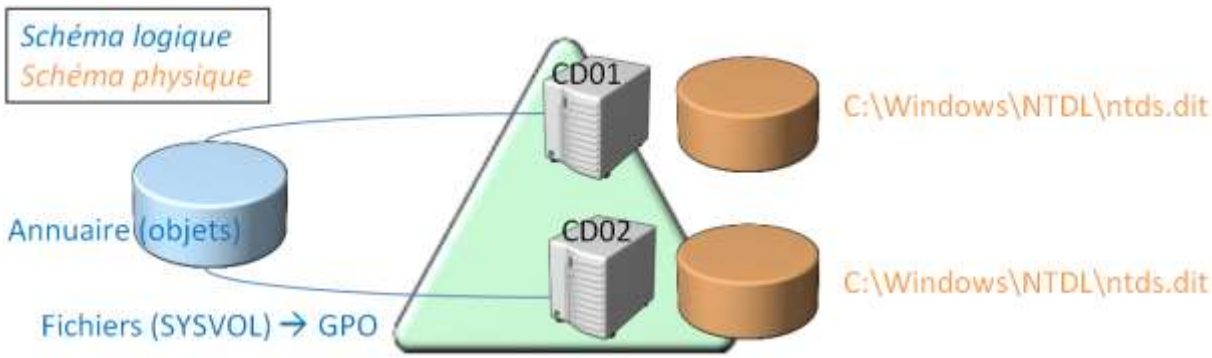
AD est une base de données. Elle contient des :

- Objets : utilisateurs, groupes, ordinateurs …
- Attributs : nom de connexion, SID, mot de passe, appartenance au groupes …
- Valeurs : valeur des attributs



Les partitions Active Directory et le Catalogue Global

Il est recommandé d'avoir 2 DC par domaine pour la disponibilité + répartition de la charge

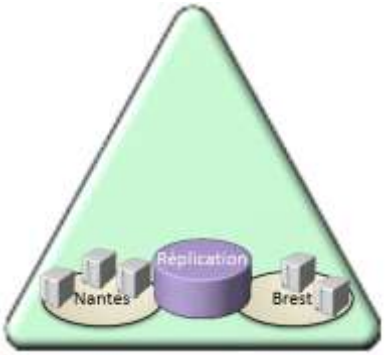


Domaine avec deux contrôleurs de domaine

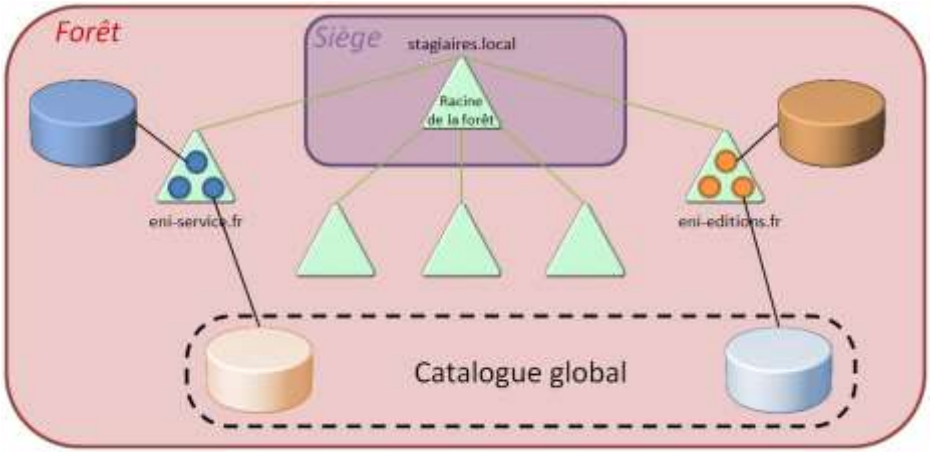
A propos des sites :

Outils d'administration > Sites et services Active Directory

- Les sites définissent la topologie de réplication
- Un site = un sous réseau (normal puisque chaque site a sa propre adresse de réseau !!!)



- Cibler les échanges
- Optimiser la réplication pour ne pas perturber les «échanges normaux»



Architecture d'exemple d'une forêt Active Directory

Rappel : le but principal d'un domaine est l'authentification

Il y a besoin de résoudre les noms : il faut donc un serveur DNS

Lors de l'authentification :

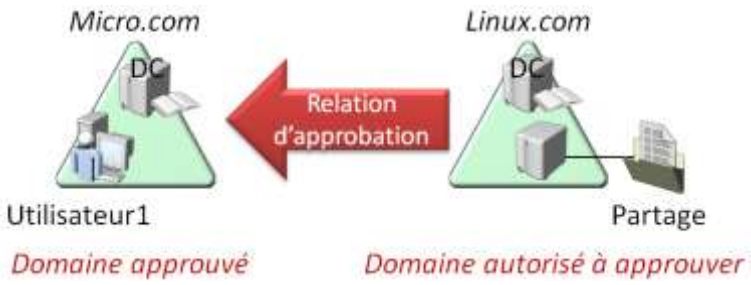
- Le client trouve le 1er DC disponible + interroge le catalogue global

Le catalogue global contient un résumé de TOUS les objets de la forêt

Niveau fonctionnel : différence selon les versions de l'AD (2000 … → … 2008R2). On ne peut pas revenir en arrière si on élève le NF

Active Directory repose sur DNS pour fonctionner (pour les GPO, pour la réplication …)

Il existe des relations d'approbations implicites au sein de la forêt entre les domaines



1.3 Installer les services de domaine Active Directory

1. Préparer l'installation : Niveau Fonctionnel, configuration IP, nom DC, nom domaine …
2. Changer le nom de serveur + @IP (puis redémarrer)
3. Installer le rôle Service de domaine Active Directory

   Exécuter **dcpromo.exe**
4. Ajouter les rôles, les services, les fonctionnalités supplémentaires, configurer le mot de passe de restauration Active Directory

2 Administration sécurisée et efficace d'AD

2.1 Utilisation des composants logiciels enfichables

La console **MMC** :

Utilisateurs & ordinateurs AD / Sites & services AD / Domaine & Approbations AD / Schéma

- Il faut les droits d'administrateur de domaine ou une délégation (à réaliser dans « sécurité » de l'OU)

Gestion à distance :

- WS2008 : ajouter la fonctionnalité Outils d'administration AD sur le DC
- Vista, Win7 : télécharger et installer **RSAT** + panneau de configuration …

Les fonctionnalités avancées permettent de voir plus d'options

Ajouter un dossier partagé :

- **MMC** > Ajouter un composant > lien vers une adresse web → ajouter un dossier partagé

2.2 Recherche d'objets dans AD

- Rechercher par type d'objets
- Privilégier les débuts de mots (adm → administrateurs …)
- **Nota :** Pour connaitre l'emplacement de l'objet : ajouter la colonne « publié à »

2.3 Commandes de type « DS »

Ces commandes utilisent le format LDAP → DN (nom unique) :

```
"cn=Jeff Ford,ou=Employees,ou=User Accounts,dc=contoso,dc=com"
```

- **dsquery** obtenir le DN (pour l'utiliser après)
- **dsget** obtenir les attributs
- **dsmod** modifier les attributs **/?** Aide sur les commandes
- **dsmove**modifier le conteneur = l'OU
- **dsadd** créer un objet
- **dsrm** supprimer un objet

Pour activer la gestion du schéma dans mmc :

```
C:\> regsvr32.exe schmmgmt.dll
```

pour exécuter un programme en tant qu'administrateur : [ctrl]+[alt]+[entree]

3 Gestion des objets « Utilisateur »

Définition : objet qui permet l'authentification des utilisateurs et qui a des attributs (SID par exemple)

Cet objet définit le comportement général de l'utilisateur (sécurité, accès…)

Login :

- UPN (avec @domaine) ou antérieur à Windows 2000 (type NetBIOS)

Création d'un objet utilisateur :

```
C:\> dsadd user "DN" …
```

- Attention au nom des attributs.
- Définir ensuite le mot de passe, qui devra être changé lors de la première ouverture de session

Différence entre le SAMAccountName et l'UPN :

- SAMAccountName : CONTOSO\Tony.Krijnen
- UPN : Tony.Krijnen@contoso.com

Modifier un objet utilisateur

- Modifier le CN :

```
C:\> dsmove
```

- Réinitialier le mot de passe :

```
C:\> dsmod
```

Suppression :

- Bonne pratique : déplacer le compte dans une OU particulière + désactiver le compte. Le supprimer ensuite

Pratique recommandée : utiliser des modèles d'utilisateurs :

- Définir des attributs généraux au modèle d'utilisateur
- Désactiver de compte de modèle
- Donner un nom spécial au modèle d'utilisateur
- Le copier (pour le renommer avec le nom du nouvel utilisateur) puis le modifier si besoin

3.1 Les commandes d'import/export

Commande d'import/export entre Active Directory et fichier .csv :

```
C:\> csvde [-l <liste d'attributs>]
```

Importer les données d'un fichier (-k permet d'ignorer les erreurs) :

```
C:\> csvde [-i <fichier>] [-k]
```

- Les mots de passe ne sont pas importés
- Inconvénient : Les comptes existants ne sont pas modifiés
- Avantage : format CSV (format souple type fichier excel)

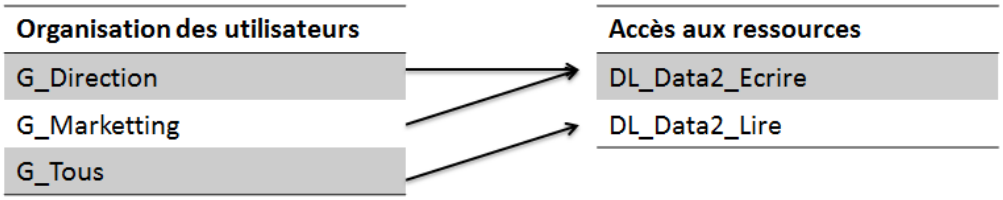
Commande d'import/export entre Active Directory et fichier .ldf :

```
C:\> ldifde [-i <fichier>] [-k]
```

- Avantage : Les comptes existants sont modifiés
- Avantage : On peut définir tous les attributs existants
- Inconvénient : format séquentiel

4 Gestion des objets « Groupe »

Rappel : Microsoft recommande d'utiliser la méthode **AGuDLP**



Exemple de relation entre G et DL

Avantage de la méthode AGuDLP : la modification des relations est souple est facile à comprendre

Inconvénient de la méthode AGuDLP : la création de 2 DL par partage est lourde au début

4.1 Convention de nommage + OU groupes :

Site (St Herblain)
|_ Groupes
| |_ **G_xxx** (membres des groupes G_xxx : objets utilisateurs)
| |_**DL_yyy** (membres des groupes DL_xxx : object G_xxx
|_ Ordinateurs
|_ Serveurs
|_ Utilisateurs

Types de groupes :

- Groupes Locaux : sur les membres du domaine ou WorkGroup → n'existent que sur celui-ci (sont inscrits dans la base SAM)
- Groupes Locaux de Domaines : sur les postes du domaine (ADDS). A privilégier pour les accès aux ressources
- Groupes Globaux : sur tous les DC du domaine. Limité au domaine. Peuvent faire partie des DL ou des U
- Groupes Universels : listés dans le catalogue global. Présents dans tous les domaines de la forêt. (G → [U] → DL)

Récupérer les membres imbriqués dans les groupes :

```
C:\> dsget group "DNGroupe" –members [-expand]
```

Copier les membres d'un groupe vers un autre groupe :

```
C:\> dsget group "DNGroupe" –members|dsmod group "DNGroupe" –addmbr
```

Attention : si on supprime un groupe de sécurité, il faut supprimer toutes les références à ce groupe dans les autres groupes.

De plus on ne peut pas annuler une suppression :

```
Onglet objet > protéger contre la suppression accidentelle
```

4.2 Pratiques recommandées :

Ajouter les descriptions, les remarques : peut servir à identifier à quoi est utilisé ce groupe

Protéger contre les suppressions accidentelles

Onglet « géré par » > délégation pour les modifications des membres

BuiltIn / Users : groupes de l'ancienne SAM sur le serveur → stratégies locales sur le serveur : **Ne pas les utiliser !**

Utiliser le groupe « Utilisateurs Authentifiés » (enlever le groupe « Tout le monde ») pour les partages

5 Gestion des objets « Ordinateur »

Un ordinateur possède un SID et un mot de passe.

Il existe une relation de confiance entre Ordinateur et DC (elle est utilisée lors de l'authentification de l'utilisateur sur DC)

L'utilisateur doit avoir des droits sur le domaine ainsi que des droits sur l'ordinateur

A ne pas faire : joindre PC1 au domaine CONTOSO directement :

- Ajout automatique de l'objet Ordinateur dans le conteneur système « Computers »
- Comme ce conteneur « computers » n'est pas une OU, on ne peut pas y appliquer de GPO
- De plus, l'objet ordinateur n'est pas proprement organisé

A faire : créer le compte PC1 dans une OU puis joindre PC1 au domaine

- Le conteneur de l'objet est une OU, on peut y appliquer des GPO
- L'objet ordinateur est proprement organisé

Un utilisateur peut joindre des Ordinateurs au domaine (max 10 ordi par défaut) :

- Modifier la valeur de msDS-MachineAccountQuota : mettre 0

Joindre un ordinateur au domaine (peut être faire à distance !) :

```
C:\> netdom join / ?
```

Exporter/importer des comptes ordinateurs dans le domaine (format CSV) :

```
C:\> csvde
```

Ajouter / modifier un objet ordinateur / déplacer … :

```
C:\> ds...
```

Nota : « géré par » (pour l'objet Ordinateur) n'a qu'un but informatif. Ça n'accorde pas de droits (SAM locale ou GPO).

sAMAccountName : NomOrdi$ (le $ indique qu'un canal sécurisé est utilisé)

Le mot de passe entre l'ordinateur et DC est autogénéré

Les connexions de l'ordinateur au DC sont visibles dans les évènements de session

5.1 En cas de problème

Attention : ne pas supprimer l'ordi puis le recréer dès le 1er problème (règle de base !)

```
C:\> netdom reset NomOrdi /domain :NomDom /UserO :AdmLocal …
C:\> nltest /sc_reset:NomDom …
```

Solution plus radicale (oblige à quitter puis rejoindre le domaine et redémarrer) :

```
C:\> dsmod reset
```

Ensuite, réinitialiser le compte de l'objet Ordinateur

Si on supprime un compte ordinateur, on perd le SID et les relations dans les groupes

6 Implémentation d'une infrastructure de GPO

Outils d'administration > Gestion des stratégies de groupe

Stratégie de domaine (La partie Ordinateur ne concerne que les objets Ordinateurs / La partie Utilisateur ne concerne que les objets Utilisateurs)

Contoso.com (GPO_Domaine)
|_ OU Service1 (( )GPO_Service1)
|_ OU Service2 (GPO_Service2)
| |_ (ⓘ)OU RespService (GPO RespService ; GPO IE8)
|_ OU Groupes

6.1 Priorité d'application des GPO

Permet de savoir quelles GPO s'appliquent en premier ou en dernier , etc.

Cas normal	Bloquer Héritage (ⓘ)	Appliqué ( )
GPO_Domaine GPO_Service1 GPO_Service2 GPO_RespService GPO_IE8 (s'applique en dernier)	Stratégie locale GPO_IE8 GPO_RespService	Stratégie locale GPO_Service1 GPO_Service2 GPO_IE8 GPO_RespService ( ) GPO_Domaine

6.2 Modification des GPO

Pour pouvoir utiliser les 'Préférences', il faut installer un correctif sur les postes clients

Certaines stratégies ont des besoin en matière de prérequis sur les postes client (OS, logiciels …)

6.3 Paramètres pour les GPO

Fichiers .ADM :

- Copiés dans chaque GPO dans %systemroot%\SYSVOL\contoso.com\policies\

Fichiers .ADMX et .ADML :

Pour Office2007, il faut modifier le registre. Fichiers de paramétrages.

- Stockés dans %systemroot%\policydefinition (local) par défaut
- Stockés dans %systemroot%\SYSVOL\contoso.com\policies\policydefinition\ (magasin central)
- \\contoso.com\policies\policydefinition\ permet d'y accéder par le réseau lorsque les fichiers sont dans le magasin central

6.4 Appliquer la configuration Utilisateur à des objets Ordinateur

Modèle d'administration > système > stratégie de groupe > mode de fonctionnement par boucle de rappel

- Utile pour les « ordinateurs publics » pour définir des variables d'environnement

Forcer la mise à jour des stratégies (sur un poste client) :

```
C:\> gpupdate /force
```

Vérifier (sur un poste client) les GPO qui se lancent :

```
C:\> gpresult /r
```

Vérifier (sur le DC) le résultat de la stratégie de groupe :

- Simuler l'application des GPO

Stratégie locale (**gpedit.msc**) → administrateurs / non-administrateurs / ordinateur / utilisateur

7 Gestion de l'étendue de la stratégie de groupe

7.1 Groupes restreint

Il faut remplacer les membres des groupes des bases SAM des postes clients :

- il faut donner la liste COMPLETE (administrateurs …)

Ordinateur > Stratégie > Paramètres Windows > Groupes restreints

Cas de Windows Vista et Windows7 :

Ordinateur / Utilisateur > Préférences > Paramètres Du Panneau De Configuration > Utilisateurs & Groupes Locaux

7.2 Sécurité

Créer des modèles de sécurité :

(Modèles de sécurité)

Comparer les modèles de sécurité (les tester puis import/export vers les GPO) :

(Configuration et analyse de la sécurité)

7.3 Distribution de logiciel à l'aide de GPO (.msi)

Marche à suivre :

- Copier les fichiers .msi sur un lecteur réseau !

  Stratégies > paramètres du logiciel > installation du logiciel

- Publier : publie les programmes dans « programmes et fonctionnalités » et permet aux non-administrateurs d'installer des logiciels choisis

7.4 Audit

Définir des audits par le biais de GPO :

Paramètres de Sécurité >> Stratégies d'audit

Choisir les évènements à auditer :

Lecteur voulu > sécurité > avancé > audit

Récupérer les audits :

Observateur d'évènements > sécurité

Attention : ça peut vite devenir le bordel (beaucoup d'informations rapatriées). Il faut donc bien choisir QUOI auditer !

8 Administration sécurisée

8.1 Définir les droits de délégation

Méthode :

- Sur l'OU → clic droit « délégation de contrôle »
- Sur l'OU → propriétés > sécurité > avancé

8.2 MMC pour délégation de contrôle

Outils d'administration > Utilisateurs et Ordinateurs Active Directory

Nouvelle fenêtre à partir d'ici > sélectionner l'OU

Nouvelle vue de la liste des taches → ajouter les boutons « ajouter ordi, … »

- Affecter les autorisations à des DL (AGuDLP)
- « Refuser explicite » prioritaire sur « Autoriser explicite » prioritaire sur « Refusé hérité »
- Autorisations effectives : outils de diagnostic pour connaitre les autorisations des utilisateurs

Délégation : définit les autorisations pour les tâches administratives dans AD

8.3 Recommandations pour la conception d'OU

- GPO (stratégies de groupe) de ce conteneur
- Délégations d'organisation (délégation administrative)
- Organiser les objets (c'est un objectif SECONDAIRE)

8.4 Audit lors de délégation (gpedit.msc sur le DC)

Auditer :

```
C:\> auditpol /?
```

Accès DS :

```
C:\> auditpol /get /category:*
```

1. Définir les objets à auditer :

   Outils d'Administration > Utilisateurs et Ordinateurs Active Directory (U&OAD)

2. Activer les audits :

   ```
   C:\> auditpol /set …                                    (ou bien outil GPO)
   ```

Attention, il faut utiliser le guillemet apostrophe (ALT+0146) pour faire le symbole '

3. Aller voir dans observateur d'évènements

9 Amélioration de la sécurité

La GPO DefaultDomainPolicy ne doit servir que pour définir les stratégies de mots de passe (et seulement ça).

Stratégie de mots de passe affinés :

Outils d'administration > ADSIEdit > System > PSO

Outils d'administration > U&OAD > password > attributs étendus > AppliesTo

9.1 Audit de l'authentification

Ouverture de session locale :

- Crée un évènement de connexion au compte dans l'ordi local : base SAM (ou dans ADDS si l'ordi est intégré à un domaine)

Ouverture d'un partage RSO :

- Crée un évènement de connexion sur la machine jointe

Configurer l'audit de l'authentification par le biais d'une GPO :

GPO : Paramètres de Sécurité > Stratégie Locale > Stratégie d'audit

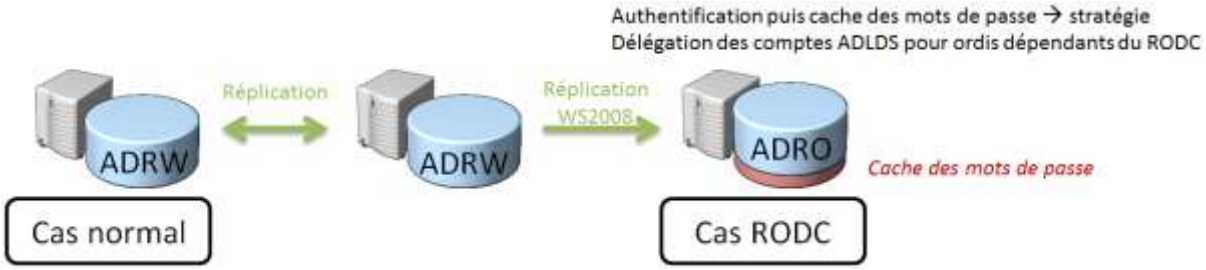
Ensuite on peut voir les évènements audités dans l'observateur d'évènements

9.2 Paramétrages des audits conseillés

GPO des serveurs de bureau à distance : auditer les évènements de connexion

GPO des DC : auditer les évènements de connexion au compte

9.3 Read-Only Domain Controller (RODC)



Fonctionnement des RODC

Usage pour les succursales (où le serveur n'est pas protégé dans un local à accès sécurisé)

Le RODC possède un groupe « administrateurs locaux » ADLDS

Prérequis : le niveau fonctionnel doit être ≥ WS2003

Si il a des DC < à WS2008, il faut exécuter

```
C:\> adprep /rodcprep
```

Il faut au moins DC 2008 qui communique avec le RODC (pour la réplication).

Créer un compte sur le RODC :

Utilisateurs & Ordinateurs Active Directory > contoso.com > Domain Controllers

+ Ajoute les groupes spéciaux dans Users

Gestion en ligne de commande de l'ADLDS du RODC :

```
C:\> dsmgmt
```

Gestion en ligne de commande de l'ADDS sur le DC

```
C:\> ntdsutil
```

La base ADLDS sur le RODC est un genre de base SAM pour gérer les groupes « locaux »

10 Configuration du système DNS

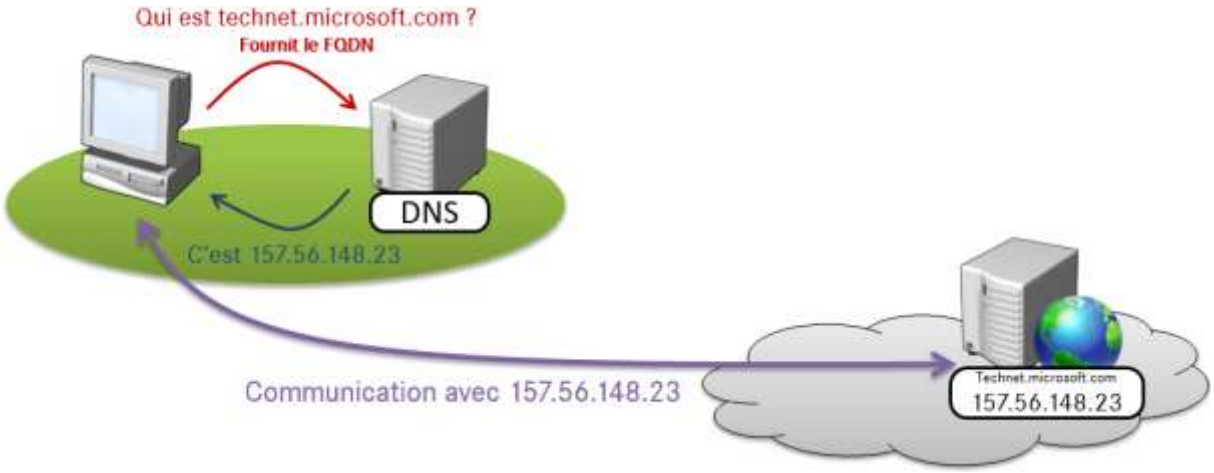
Un serveur DNS est utilisé pour :

- Obtenir une adresse IP à partir d'un nom d'ordinateur
- Obtenir un nom d'ordinateur à partir d'une adresse IP

Tout repose sur DNS dans ADDS.

FQDN (Fully Qualified Domain Name) : Nom hôte + suffixe DNS

- Exemple : technet.microsoft.com



L'utilité du serveur DNS

Une zone est définie par domaine. Cette zone a le même nom que le domaine :

- Exemple : zone « aareon.com » pour le domaine « aareon.com »
- Cette zone contient les noms et adresses IP des membres du domaine (PC1, DC, SRVFIC …)

Un DNS qui héberge une zone fait autorité sur la zone (attention à la résolution de type NetBIOS)

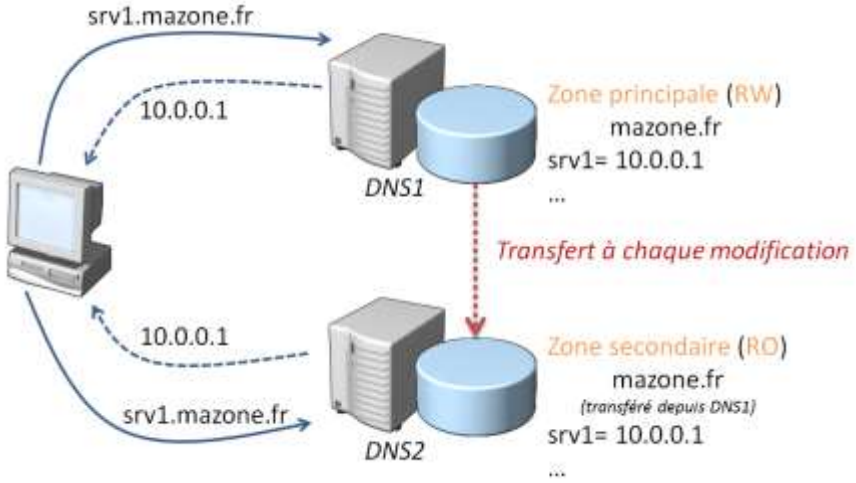
Exemple d'enregistrement de ressource sur un serveur DNS :

- Enregistrement de type A : PC1.domaine.local (FQDN) 192.168.0.101 (adresse IPv4)

10.1 Réplication d'une zone

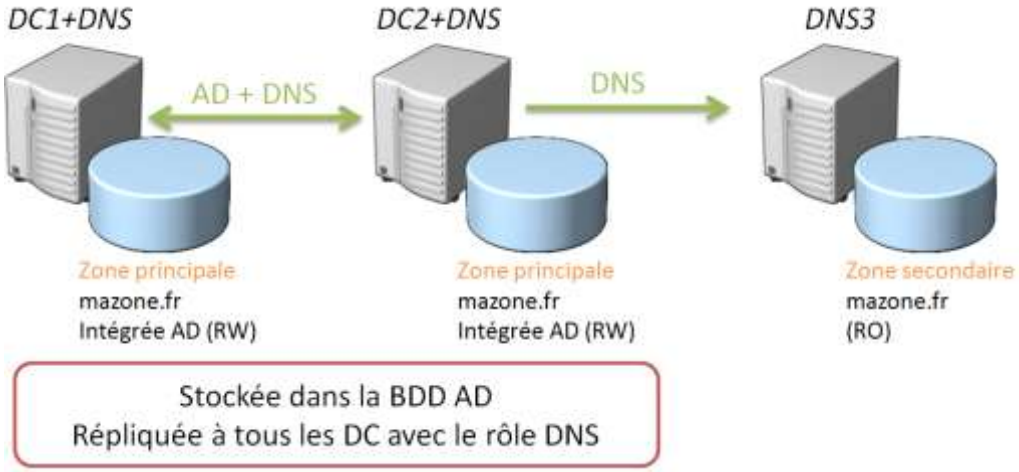
La réplication d'une zone est la copie de cette zone du serveur DNSprincipal vers un serveur DNSsecondaire.

Zone à base de fichiers (standard) : données copiés de la zone principale (RW[1]) vers la zone secondaire zone secondaire (RO[2]) :



Réplication d'une zone à base de fichiers

Zone intégrée à AD : données stockées dans la BDD AD (fichier ntds.dit) :



Réplication d'une zone intégrée à Active Directory

Il est conseillé d'ajouter le rôle serveur DNS aux Contrôleur de Domaine

[1] RW (Read Write) : en lecture écriture

[2] RO (Read Only) : en lecture seule

10.2 Ce qui se passe sur l'ordi local

L'ordinateur va d'abord interroger son cache à l'aide du service client DNS (un service windows) :

- Il interroge le cache de résolution DNS (historique des recherches précédentes)
- Ce cache est aussi alimenté par le contenu du fichier hosts

Si le cache n'a pas donné la réponse, le client interroge le serveur DNS :

- Celui-ci interroge les informations de sa zone ainsi que les informations qui sont contenues dans son cache.

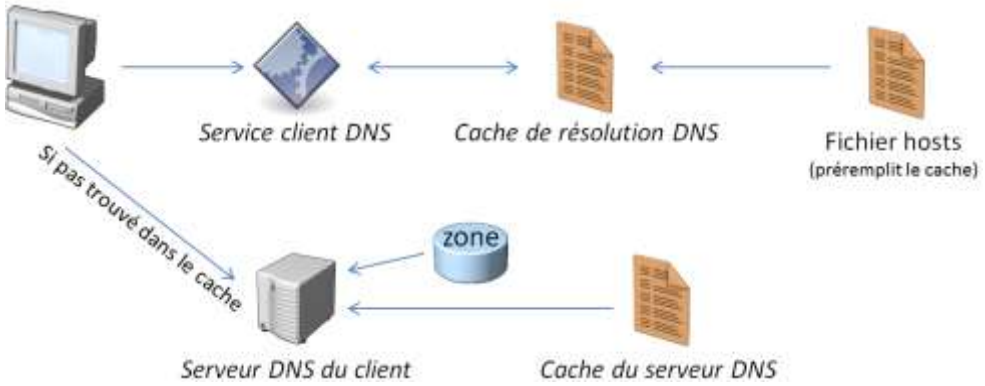


Schéma de résolution de nom sur un ordinateur

Si il y a un problème de résolution de nom, vérifier les paramètres DNS :

Vider le cache de résolution DNS (de l'ordinateur local donc) :

```
C:\> ipconfig /flushdns
```

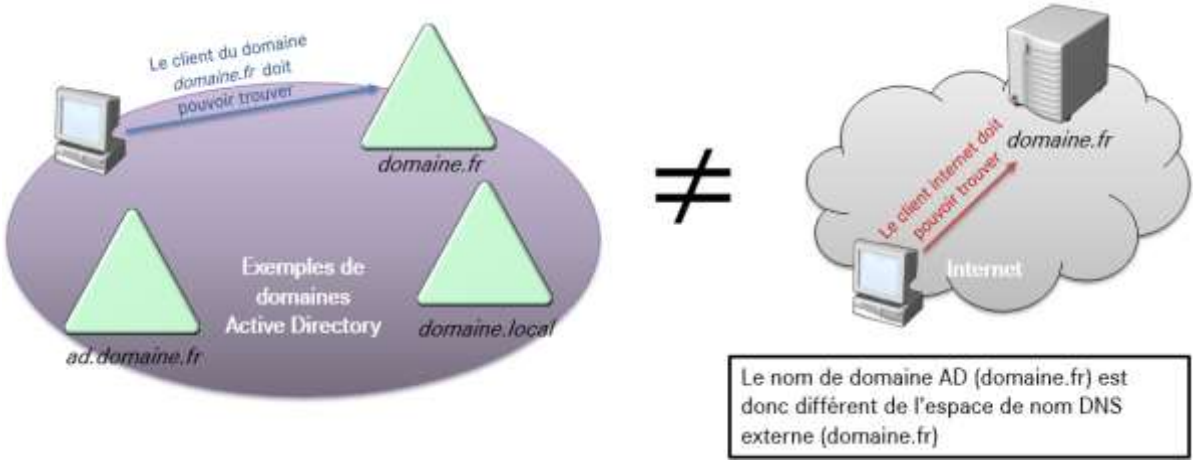
Interroger le serveur DNS sans passer par le cache de résolution DNS :

```
C:\> nslookup.exe
```

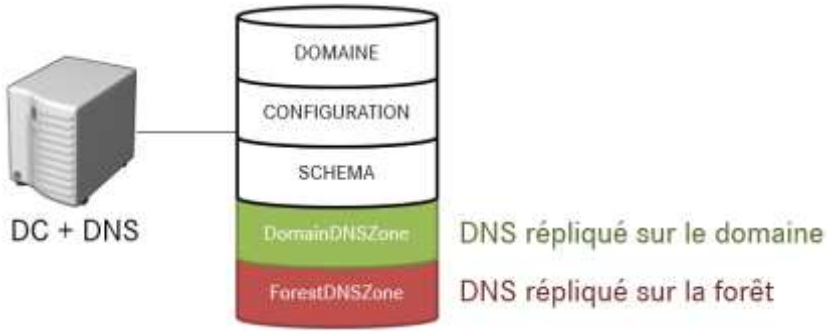
10.3 Configuration du service DNS

Les transferts de données vont de la Zone Principale (ZP) vers la Zone Secondaire (ZS)

Il faut penser à BIEN configurer le serveur DNS du client ! Si le client n'a pas le bon serveur DNS, la résolution ne peut pas se faire.



Nom de domaine AD et nom de DNS externe



Les partitions d'un DNS intégré à l'Active Directory

Le service **netlogon** :

- Il vérifie les demandes d'ouverture de session et enregistre, authentifie et localise les contrôleurs de domaine. Il gère aussi la réplication de la base ADDS
- Il définit qui est responsable de quoi : LDAP, FTP, KERBEROS, Catalogue Global …

Pour mettre à jour ces informations de netlogon, il faut arrêter puis redémarrer le service :

```
C:\> netlogon stop
C:\> netlogon start
```

10.4 Nettoyage des enregistrements DNS

Les Paramètre de vieillissement permettent d'enlever les informations obsolètes :

- à configurer sur le serveur
- à configurer sur chaque zone

10.5 Fonctionnement correct DNS

Effectuer un diagnostic du service DNS :

```
C:\> dcdiag
```

Afficher la configuration réseau :

```
C:\> ipconfig /all
```

Interroger le serveur DNS directement (à faire souvent en cas de problème) :

```
C:\> nslookup
```

Interroger le cache de résolution DNS de l'ordinateur local :

```
C:\> ipconfig /displaydns
```

Vider le cache de résolution DNS de l'ordinateur local :

```
C:\> ipconfig /flushdns
```

Réenregistrer ses informations sur le serveur DNS (à faire lors des modifications réseau) :

```
C:\> ipconfig /registerdns
```

11 Administration des DC ADDS

Installer ou désinstaller le service ADDS :

```
C:\> dcpromo.exe
```

Installer le service ADDS en utilisant un fichier de réponses (obligatoire pour les serveurs CORE) :

```
C:\> dcpromo /unattend:"chemin"
```

- Nota : le fichier réponses peut être créé lors du dcpromo (sur la page de résumé, exporter les paramètres)

Préparer la forêt avant un DCPROMO ou lors d'une augmentation du NF :

```
C:\> adprep /forestprep
```

Préparer le domaine (modifie le schéma) avant un DCPROMO ou lors d'une augmentation du NF :

```
C:\> adprep /domainprep / gprep
```

Préparer pour l'intégration d'un RODC dans le domaine :

```
C:\> adprep /rodcprep
```

Nota : dans certains cas, il faut exécuter ADPREP32 au lieu d'ADPREP

11.1 Pour un RODC

- créer un compte de contrôleur RODC (ex : mise en cache des MDP)
- délégation de l'installation du RODC (créer un administrateur « local » RODC)
- association du DC au compte RODC :

```
C:\> dcpromo /UseExistingAccount:attach /unattend: "chemin"
```

11.2 Installation à partir d'un support (IFM)

IFM = Install From Media

```
C:\> ntdsutil
```

Indiquer qu'on travaille sur ntds.dit :

```
ntdsutil> activate instance ntds
```

Créer un support d'installation :

```
ntdsutil> ifm
ntdsutil> help
```

Graver ensuite cela sur un DVD.

Sur le DC à installer :

```
C:\> dcpromo
```

Installation avancée en mode graphique puis définir

```
ReplicationSourcePath option /...
```

11.3 Installation minimale de Windows (serveur Core)

Tout se fait en ligne de commande

Lancer une commande dans une autre console :

```
C:\> start <commande>
```

Ajouter et|ou lister les rôles du serveur :

```
C:\> ocsetup | oclist
```

Le bureau à distance permet une administration graphique à distance.

Installer ou désinstaller le rôle ADDS :

```
C:\> dcpromo
```

11.4 Gestion des Maitres d'Opération (MO)

Les rôles sont transférables (on peut les déplacer sur un autre serveur).

Maitre d'opérations à l'échelle de la forêt :

- **MO des noms de domaine** : droit d'ajouter/supprimer les domaines

  Outils d'administration > Domaines & Approbations AD

- **Contrôleur de schéma :** droit de modifier le schéma

  Outils d'administration > Gestion du Schéma

MO à l'échelle du domaine :

Utilisateur et Ordinateurs Active Directory > domaine.local >> Maitres d'Opérations

- **Maitre RID :** utilisé pour générer les SID
- **Infrastructure :** multidomaine seulement, vérifie les interconnections des objets multidomaines (CG)
- **Contrôleur de domaine principal** (=émulateur PDC) : gère les mises à jour des mots de passe, met à jour des GPO, est source de l'heure de référence du domaine.

Nota : depuis la console MMC on ne peut faire que du TRANSFERT de zone.

Conseils d'attribution des rôles de MO :

- Rôle Infra et rôle CG sur des DC différents
- Placer tous les MO forêt sur le même DC
- Placer le rôle RID + le rôle émulateur PDC sur le même DC
- Prévoir un plan de basculement en cas de panne
- Envisager de configurer le Catalogue Global sur tous les DC (au minimum un CG par site)

Nota : depuis la commande ntdsutil on peut s'accaparer un rôle (SEIZE) :

```
C:\> ntdsutil > roles > connections
```

Attention : ne pas remettre l'ancien MO en ligne (sauf RID ; sauf PDC)

Savoir quel serveur a les rôles de maître d'opération :

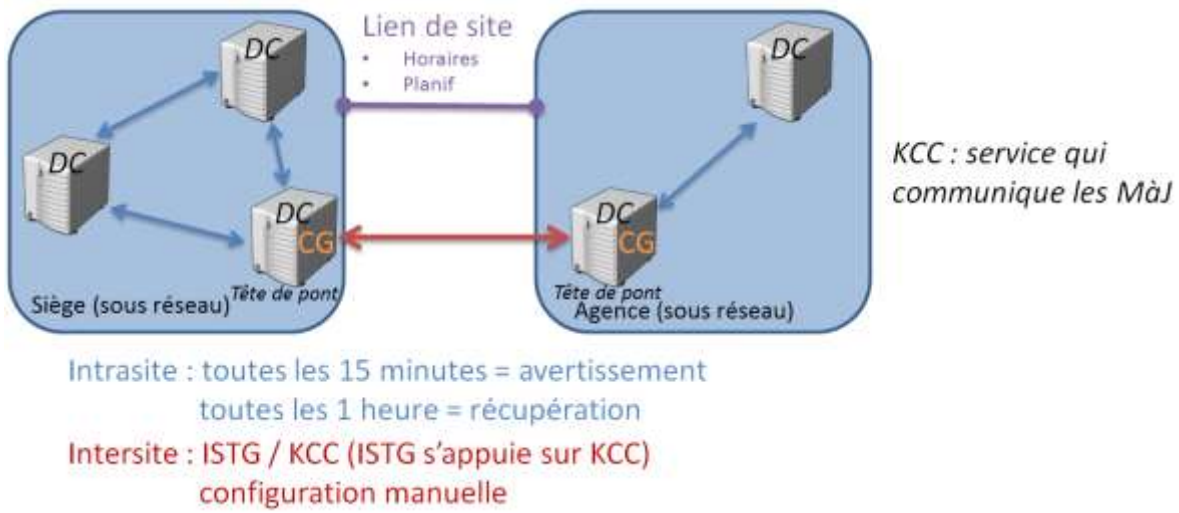
```
C:\> netdom query fsmo
```

11.5 Configuration de la réplication DFSR du dossier SYSVOL

Type de réplication :

- Réplication FRS : niveau fonctionnel WS2003
- Réplication DFSR : niveau fonctionnel WS2008 (outil dfsrmig)

12 Réplication AD et gestion des sites



Exemple de réplication intersite

Un site sert à : réplication ADDS / localisation des services / emplacement géographique

Outils d'administration > sites et services Active Directory

Configuration de la réplication AD :

1. Ajouter des sites
2. Ajouter des subnet (1 client d'un sous réseau va privilégier les serveurs de son site)
3. Définir les liens entre les sites :

   Sites et services Active Directory > Sites > Inter-site Transports > IP

4. Lier les serveurs aux sites

Conseil : réplication toutes les 15 minutes + définir des serveurs « tête de pont IP »

- radical : ça répond ou ça plante

On peut définir des liens inter-sites IP et des liens inter-sites SMTP :

- IP : connexion permanente
- SMTP : connexion à la demande des serveurs

Les DC inscrivent les enregistrements SRV (emplacements de services) dans le service DNS puis sont privilégiés par les clients de leur site Active Directory

Le Catalogue Global est souvent utilisé (par les serveurs Exchange notamment)

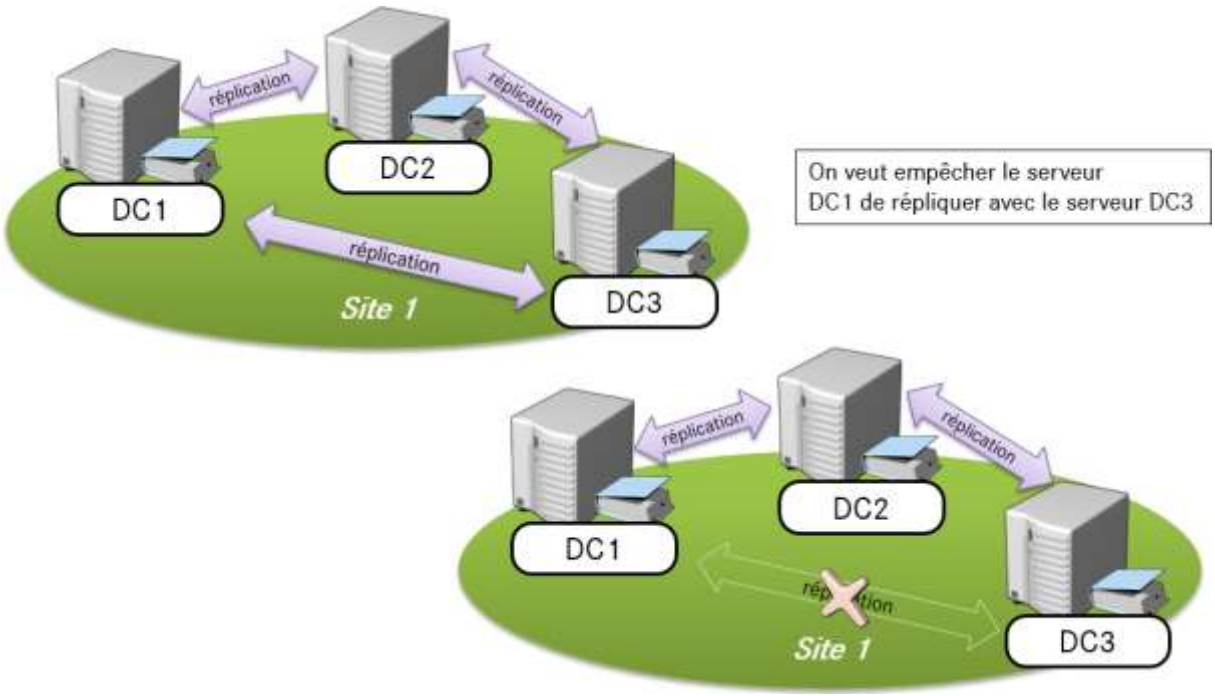
Activer le catalogue global :

Sites &Services Active Directory > Se placer sur le serveur > NTDS Settings >> propriétés > cocher ‘catalogue global’

Ou alors :

Utilisateurs et Ordinateurs Active Directory > OU ‘Domain Controllers’ > Sélectionner le serveur >> propriétés > bouton ‘Paramètres NTDS…’ > cocher ‘catalogue global’

12.1 Annuler la transitivité des sites



Pour désactiver la transitivité des sites (déconseillé). Il faut ensuite recréer les ponts en définissant des liens spécifiques entre contrôleurs de domaine :

Sites et services Active Directory > Sites > Inter-site Transports > IP ou SMTP >> propriétés > décocher ‘relier tous les liens de sites’

12.2 Surveiller la réplication

Afficher les partenaires de réplication et les dates de dernières réplications des partitions ADDS :

```
C:\> repadmin /showrepl
```

Afficher les object connexion entre les partenaires :

```
C:\> repadmin /showconn
```

Lister les erreurs de réplication :

```
C:\> dcdiag /test:KccEvent
C:\> dcdiag /test:Replications
C:\> dcdiag /test:Topology
```

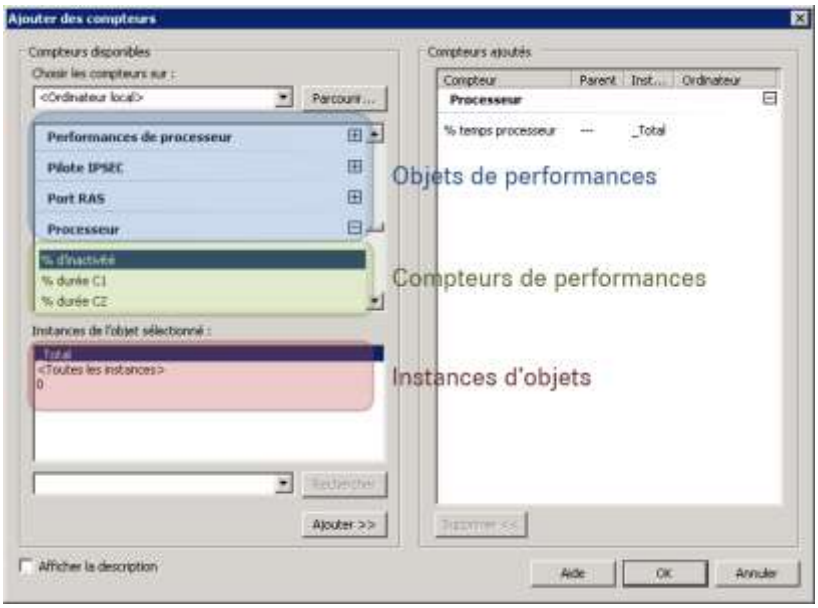
13 Continuité du service d'annuaire

13.1 Analyseur de performances

Outils d'administration > Analyseur de performances

Sélectionner des compteurs à surveiller :

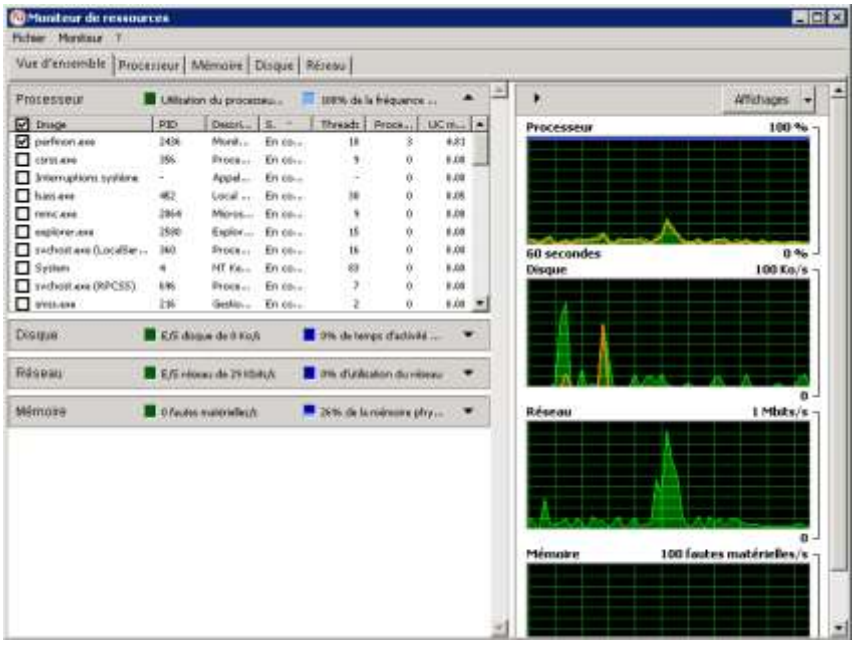
Performance > Outil d'analyse > Analyseur de performances >> propriétés > Onglet Données > bouton 'Ajouter…'



Ajouter des données à surveiller

13.2 Gestionnaire des taches

Démarrer > exécuter> taskmgr.exe > Onglet performance > bouton 'Moniteur de ressource…'



Vue d'ensemble du moniteur de ressources

13.3 Collecteurs de données

Outils d'administration > Analyseur de performances

Sélectionner des données à collecter :

Performance > Ensemble de collecteurs de données > Système > 'en sélectionner un'. Partie droite>> propriétés, sélectionner les données à collecter (faire du tri)

Définir aussi les conditions d'arrêt (par défaut, collecte pendant 5 minutes).

13.4 Observateur d'évènements

Outils d'administration > Observateur d'évènements

Les 'journaux des applications et des services' reportent les évènements liés aux rôles du serveur.

Conseil : Clic droit sur le journal souhaité > Filtrer la vue

Fonctionnement des abonnements (récupérer des évènements d'autres postes WS2008) :

1. Sur chaque machine émettrice source d'évènements :

```
C:\> winrm quickconfig
```

2. Sur l'ordinateur collectant les informations :

```
C:\> wecutil qc
```

3. Créer l'abonnement :

   Outils d'administration > Observateur d'évènements > Abonnements >> Créer un abonnement

   - Sélectionner l'ordinateur cible (dans le même domaine)
   - Sélectionner les évènements à récupérer
   - S'identifier

4. Lire les évènements transmis :

   Outils d'administration > Observateur d'évènements > Journaux Windows > Evénements transférés

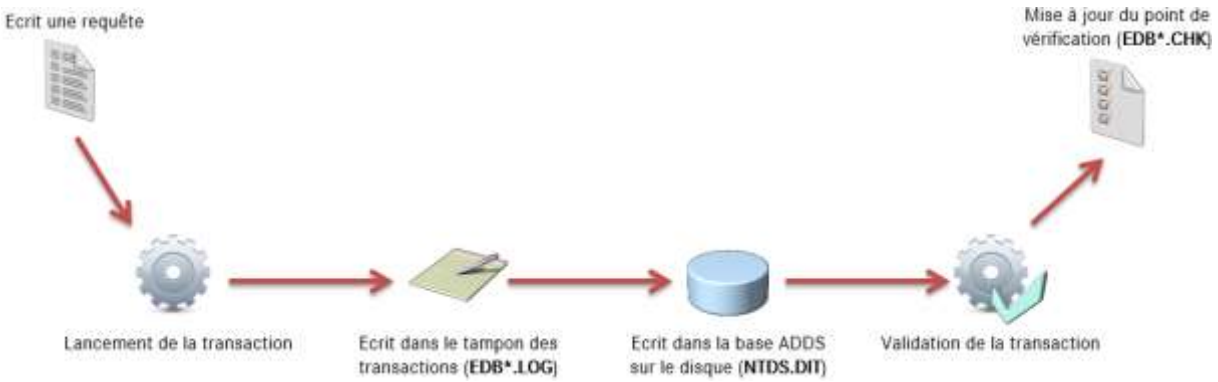
13.5 Gestion de la base AD

C:\Windows\System32\NTDS\ntds.dit : fichier de la base de données ADDS. Contient toutes les partitions et les objets ADDS du contrôleur de domaine

EDB*.log : journaux des transactions

EDB.chk : fichier de vérification

EDB*.jrs : fichiers pour assurer de l'espace pour la base ADDS, sinon erreur



Procédure de mise à jour de la base ADDS

13.6 Maintenance de la base de données

```
C:\> ntdsutil
```

Attention : pour déplacer les fichiers journaux ou la base on ne fait pas de copier/coller des fichiers !

Il faut utiliser la commande :

```
C:\> ntdsutil > files
```

La défragmentation lorsque la base est en ligne ne libère pas d'espace disque. Il faut exécuter une défragmentation hors ligne pour libérer de l'espace.

Tombstone lifetime : durée pendant laquelle un objet supprimé est gardé avant d'être supprimé définitivement. Par défaut, cette durée est de 180 jours.

Pour nettoyer les objets supprimés :

```
C:\> ntdsutil > mediadata cleanup
```

Pour effectuer une défragmentation hors ligne, il faut arrêter les services de domaine AD :

Gestionnaire de serveur > Roles > Services de domaine Active Directory. Partie droite, Arrêter le service système « Service de domaine Active Directory »

Lorsque le serveur n'est plus catalogue global, il récupère beaucoup d'espace disque.

13.6.1 Les snapshots

Un snapshot est une sauvegarde de l'annuaire. Son unique but est de voir les attributs des objets tels qu'ils étaient au moment du snapshot. Cependant, **il n'est pas possible de restaurer un annuaire ADDS à partir d'un snapshot**.

1. Créer un snapshot :

```
C:\> ntdsutil> snapshot > activate instance ntds > create > list all
```

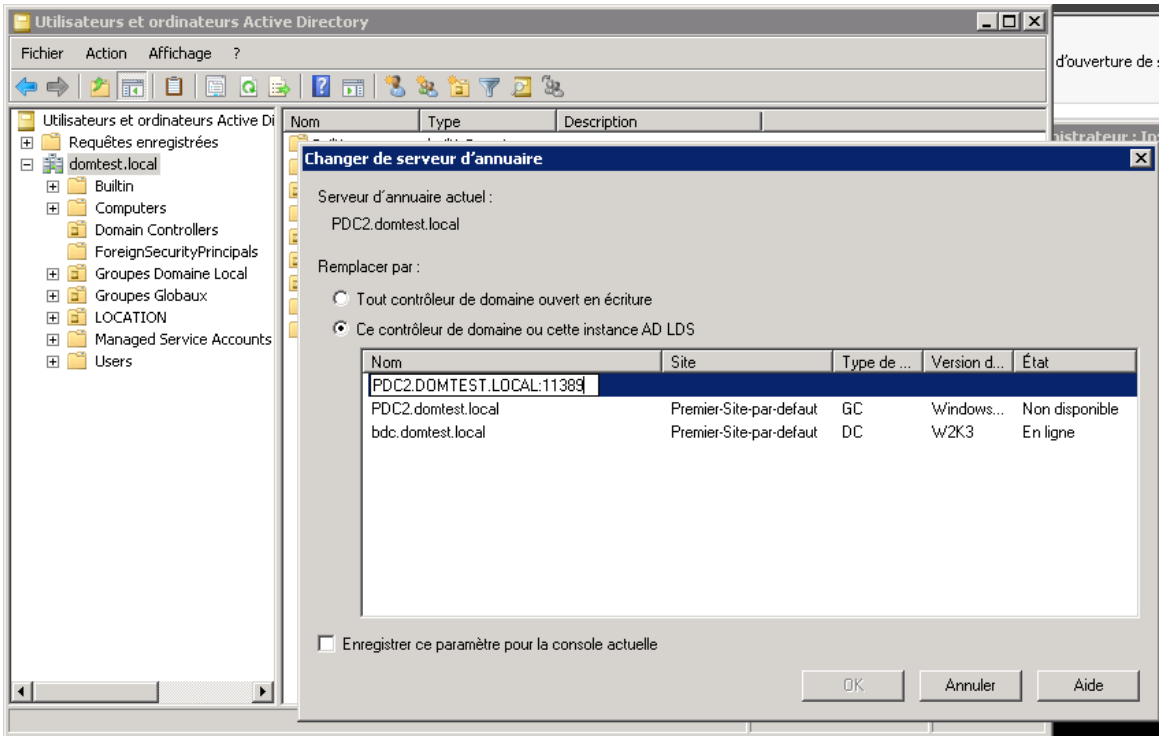
2. Monter un snapshot :

```
C:\> ntdsutil > snapshot > activate instance ntds > list all > mount XX
Mounted as C:\$SNAP_201305040042_VOLUMEC$\
```

3. Se connecter au snapshot monté :

```
C:\> dsamain /dbpath  C:\$SNAP_201305040042_VOLUMEC$\Windows\NTDS\ntds.dit /ldapport 11389
```

4. Ouvrir la console Utilisateurs et Ordinateurs Active Directory et se connecter sur le serveur au port défini :



Sélectionner le port LDAP défini dans dsamain

Nota : les outils LDP et ADSEDIT sont aussi disponibles

5. Démonter le snapshot :

```
C:\> ntdsutil > snapshot > activate instance ntds > list mounted > unmount XX
```

6. Supprimer le snapshot :

```
C:\> ntdsutil > snapshot > activate instance ntds > list all > delete XX
```

Nota : idée de script .bat à executer chaque semaine (pour des besoins éventuels de restauration) :

```
@echo off
ntdsutil snapshot "activate instance ntds" create quit quit
```

13.7 Sauvegarde et restauration des services ADDS et des DC

Sauvegarde :

```
C:\> wbadmin
```

Gestionnaire de serveur > Stockage> Sauvegarde de Windows Server

Pour sauvegarder les services ADDS, il faut sauvegarder (sur un disque à part) :

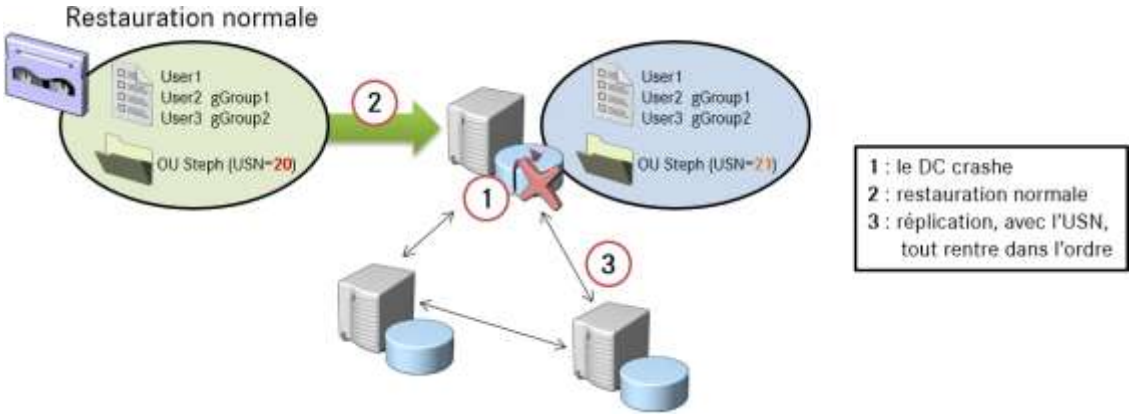
- C:\Windows\NTDS*.log *.jrs *.chk ntds.dit
- C:\Windows\SYSVOL

Restauration :

- A un autre emplacement, pour tester l'intégrité de la sauvegarde
- Complète du serveur, dans le cas d'un serveur HS par exemple

Une restauration normale (ne faisant pas autorité) est utile lorsqu'un serveur crashe :

- Le serveur de remplacement récupère la restauration
- La réplication met à jour à partir de l'USN de restauration



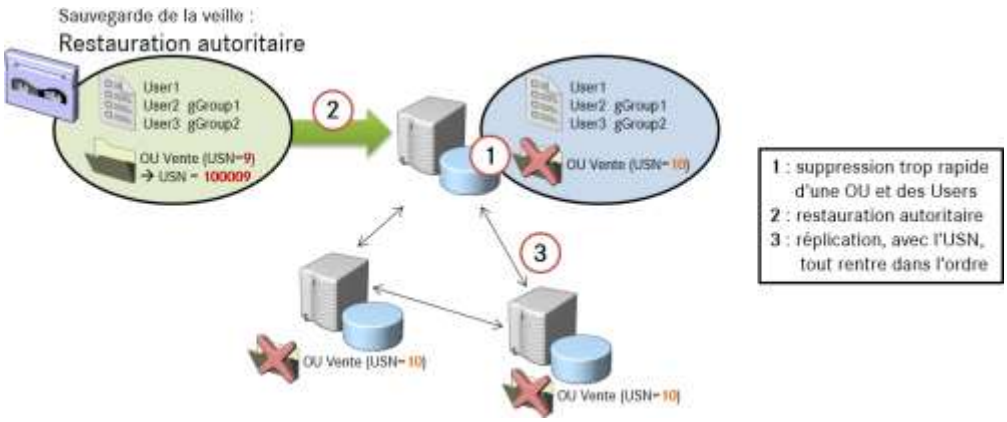
Cas d'une restauration ne faisant pas autorité

Une restauration faisant autorité est utile lors d'une mauvaise manipulation de l'annuaire :

- La partie à restaurer (OU, objet…) est récupérée sur la sauvegarde avec un numéro d'USN très élevé

```
C:\> ntdsutil > autoritative restore > restore subtree:"OU=vente,OU=orleans,DC=domaine,DC=local"
```

- Ainsi, cette restauration va se propager aux autres DC du domaine



Cas d'une restauration faisant autorité

USN : Update Sequence Number. C'est en quelque sorte un numéro de version de l'objet

Au démarrage du serveur (celui qui remplace le DC crashé), il est possible d'appuyer sur la touche [F8] pour rentrer dans le « Mode restauration des services d'annuaire ». A partir de là, il est possible d'utiliser la commande **wbadmin** pour restaurer l'annuaire ADDS.

Pour restaurer un annuaire à distance :

```
C:\> bcdedit /set safeboot dsrepair
C:\> shutdown –t 0 –r
[attendre le redémarrage puis]
```

Effectuer les operations de sauvegarde :

```
C:\> bcdedit /deletevalue safeboot repair
C:\> shutdown –t 0 –r
[attendre le redémarrage et appuyer sur [F8]]
```

Lister les sauvegardes :

```
C:\> wbadmin get version
```

Restaurer :

```
C:\> wbadmin start systemstaterecovery
```

14 Gestion de plusieurs domaines et forêts

Une relation d'approbation est une relation de confiance entre des domaines/des forêts

Il est dit que les ressources approuvent les comptes. La flèche part des ressources et va vers les comptes.

Outils d'administration > Domaines et Approbations Active Directory

Au sein d'un domaine, les relations d'approbations sont :

- Bidirectionnelles
- Transitives
- Authentification Kerberos (utilisées pour l'authentification entre Kerberos et ADDS)

Il est possible de faire de l'authentification sélective, c'est-à-dire de sélectionner les serveurs qui sont concernés par la relation d'approbation.

Utilisateurs & Ordinateurs Active Directory > sélectionner le serveur > propriétés > sécurité > liste dans les ACL > autorisation d'authentifier