

1 – Domaine Active Directory : contrôleur de domaine et machines membres

Introduction

Vous allez dans ce TP configurer votre serveur Windows 2008R2 en contrôleur de domaine Active Directory, et votre autres machines virtuelles en membres du domaine ; vous créerez et configurerez ensuite des comptes d'utilisateurs du domaine AD (Active Directory).

Active Directory est en fait l'implémentation par Microsoft d'un ensemble des technologies et protocoles destinés à faciliter la mise en œuvre et l'administration d'un réseau local. Son objectif principal est de fournir des services centralisés d'identification et d'authentification à un réseau d'ordinateurs utilisant le système Windows. Il permet également l'attribution et l'application de stratégies, la distribution de logiciels, et l'installation de mises à jour critiques par les administrateurs.

Active Directory répertorie les éléments d'un réseau administré tels que les comptes des utilisateurs, les serveurs, les postes de travail, les dossiers partagés, les imprimantes, etc.

Notion de Domaine et d'annuaire Active Directory

☞ Lisez le document pdf [Notion de Domaine Active Directory](#) et le paragraphe II de [Installation AD 2008R2](#).

Ils décrivent la structure d'un réseau local organisé selon un **domaine** contrôlé par un serveur tournant sous **Windows Server 2008**.

Quel sont selon vous les avantages et les inconvénients d'une organisation en domaine par rapport à un groupe de travail ?

Les différents ordinateurs et utilisateurs du domaine sont référencés sur le contrôleur dans un "annuaire" **Active Directory**.

A quoi sert, selon le document, l'annuaire Active Directory ? Quels services offre-t-il ? Quel est le protocole utilisé ?

*Active Directory introduit les notions de **domaine**, **forêt**, **arborescence**. Définissez ces termes :*


Qu'est ce qu'un contrôleur de domaine Active Directory ?

*Active Directory s'appuie donc sur organisation des machines en **domaines DNS**, dont il assure la bonne intégration ; sur une centralisation des informations des membres du réseau (machines, utilisateurs,) dans un annuaire **LDAP** ; sur une sécurisation forte par le protocole d'authentification **Kerberos** ; sur des partages de ressources (dossiers, imprimantes,...) par le protocole **SMB/CIFS***

*Le tout ensemble forme alors un **domaine Active Directory**, qui est désigné le même nom que celui du domaine DNS qu'il utilise.*

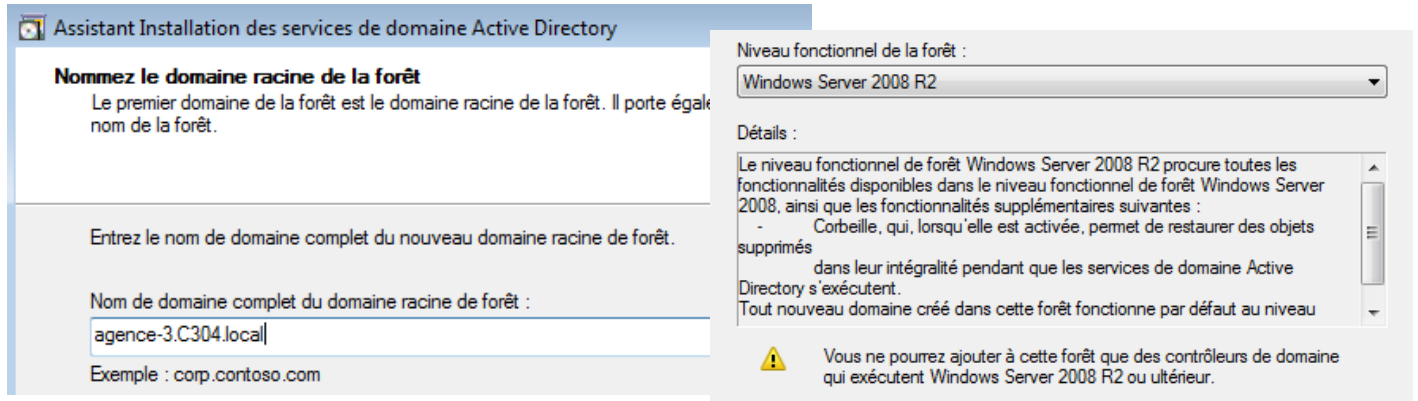
*Il sera possible d'intégrer une machine Linux à un domaine en configurant ces protocoles avec *Samba* et *Winbind*, destinés à intégrer Unix au monde Windows, ou bien encore en « couplant » les comptes et dossier partagés d'un domaine AD à ceux d'un domaine NIS/NFS.*

Promotion de la machine Windows Server 2008R2 en contrôleur de domaine Active Directory

- ☞ Regardez la vidéo de création du domaine AD `C304.local` sur la machine contrôleur  [contrôleur de domaine AD C304.local.avi](#) `siege-societe` en suivant également les indications d'installation du paragraphe IV du document [Installation AD 2008R2](#)

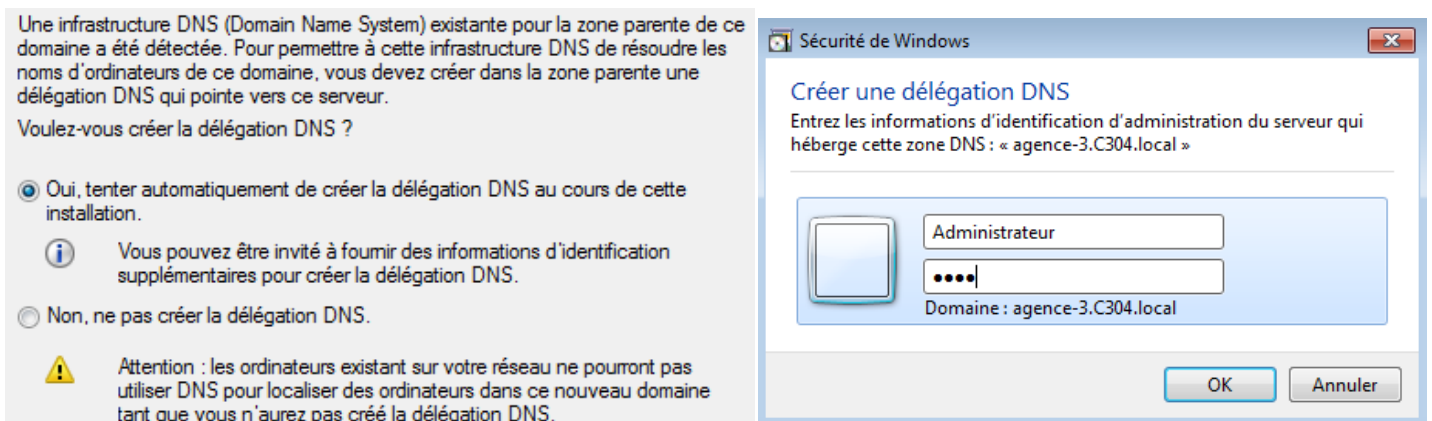
Vous allez configurer comme sur la vidéo votre réseau virtuel en un domaine AD « `agence-i.C304.local` » dans une nouvelle forêt

- ☞ En vous inspirant de la vidéo, installez le rôle « Services de domaine Active Directory », puis configurez votre machine `serveur` Windows Server 2008R2 en contrôleur du domaine racine AD « `agence-i.C304.local` » dans une nouvelle forêt





L'analyse de la configuration DNS devrait détecter que votre domaine DNS `agence-i.C304.local` peut être configuré comme domaine « fils » du domaine « parent » `C304.local` de la salle et vous proposer d'effectuer cette configuration (*délégation*)

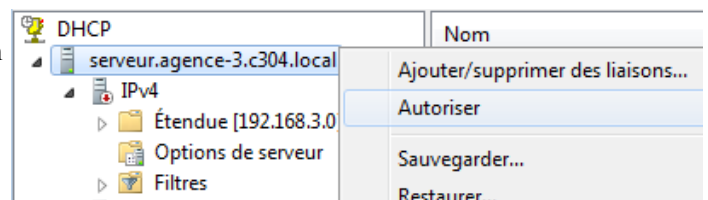
Utiliser le compte « Administrateur / C304 » du contrôleur `siege-societe` du domaine `C304.local` de la salle pour créer la délégation



- ☞ Après redémarrage de votre machine `serveur`, connectez-vous y avec le compte « `AGENCE-i\Administrateur` » du domaine
- Pour des raisons de sécurité, le serveur DHCP configuré au TP n°2 doit recevoir l'autorisation d'attribuer des adresses IP sur le domaine Active Directory par le contrôleur de domaine.

Ouvrez l'outil d'administration  **DHCP**, cliquez avec le bouton droit de la souris sur `serveur.agence-3.C304.local` et choisissez l'option « Autoriser », puis « Actualiser »

Vérifier que l'icône IPv4 est maintenant verte 




Remarque : Lors de la promotion d'une machine serveur en contrôleur d'un domaine AD, tous les comptes utilisateurs locaux de ce serveur / contrôleur de domaine sont automatiquement « transformés » en comptes du domaine Active Directory (d'ailleurs la branche « Utilisateurs et groupes locaux » disparaît de l'outil d'administration « Gestion de l'ordinateur »)

En particulier, le compte administrateur local initial du serveur promu en contrôleur de domaine devient alors **le compte administrateur du domaine** Active Directory créé.

Nous verrons par la suite que nous pourrions créer d'autres comptes du domaine sur ce contrôleur, qui pourront être utilisés pour se connecter depuis toute machine membre du domaine (y compris le contrôleur lui-même)

Nous pourrions également continuer à utiliser et créer des comptes purement locaux sur toutes les machines membres du domaine, sauf sur la machine contrôleur elle-même où tous les comptes sont du domaine

Intégration des machines clientes virtuelles comme membres du domaine Active Directory agence-i.C304.local

☞ Regardez la vidéo de l'intégration d'une machine au domaine AD C304.local  clients domaine AD 304.local.avi

A la fin de la vidéo, on se connecte 2 fois successivement sur la machine PC-6 avec des comptes administrateurs différents

La 1^{ère} connexion s'effectue avec le compte administrateur : local à la machine du domaine AD


La 2^{ème} connexion s'effectue avec le compte administrateur : local à la machine du domaine AD

Comment est désigné un compte local user à une machine de nom Netbios PC ?

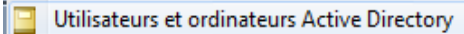
Comment est désigné un compte user d'un domaine AD de nom Netbios DOMAIN ?

Remarque : le nom Netbios d'un domaine correspond à la partie la plus à gauche de son nom complet, écrite généralement en majuscule
expl : SIEGE-SOCIETE pour le domaine siege-societe.C304.local

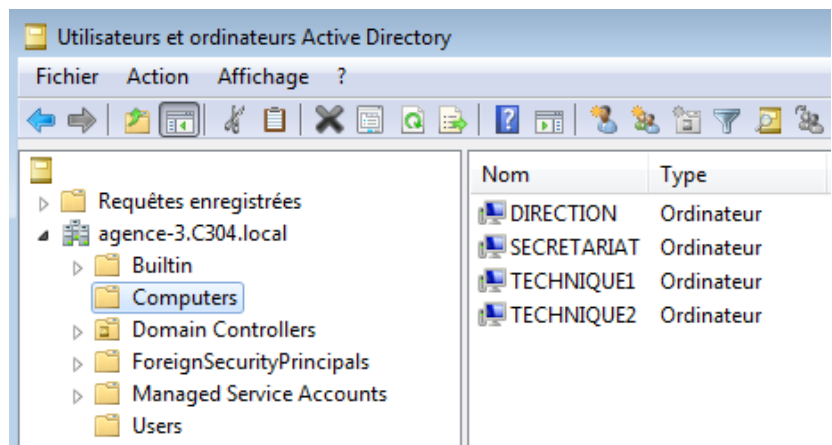
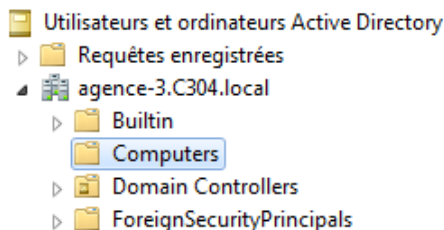
☞ Intégrez alors en vous inspirant de cette vidéo vos 4 machines virtuelles clientes à votre domaine AD agence-i.C304.local (démarrez et intégrez chacune des 4 machines virtuelles successivement pour éviter des accès disques physiques simultanés)

Vous pouvez mettre en pause  une machine virtuelle cliente une fois intégrée au domaine et redémarrée pour économiser la mémoire

Quel est le compte, dont les paramètres vous sont demandés, qui vous sert à effectuer cette intégration ?

☞ Ouvrez sur votre machine serveur l'outil d'administration (menu démarrer)


Développez la « branche » relative à votre domaine et sélectionnez la « feuille » Computers pour vérifier que vos machines clientes sont bien membres du domaine



☞ Vérifier que depuis les machines virtuelles de votre domaine, vous pouvez de ping la machine siege-societe du domaine parent C304.local et celles d'autres domaines virtuels d'agences agence-k.C304.local

```
C:\Users\Administrateur>ping siege-societe.C304.local

Envoi d'une requête 'ping' sur siege-societe.C304.local [192.168.0.20] avec 32 octets de données :
Réponse de 192.168.0.20 : octets=32 temps=22 ms TTL=127
Réponse de 192.168.0.20 : octets=32 temps=14 ms TTL=127
Réponse de 192.168.0.20 : octets=32 temps=15 ms TTL=127
Réponse de 192.168.0.20 : octets=32 temps=15 ms TTL=127

Statistiques Ping pour 192.168.0.20:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 14ms, Maximum = 22ms, Moyenne = 16ms

C:\Users\Administrateur>ping technique1.agence-9.C304.local


Envoi d'une requête 'ping' sur technique1.agence-9.C304.local [192.168.9.101] avec 32 octets de données :
Réponse de 192.168.9.101 : octets=32 temps=25 ms TTL=126
Réponse de 192.168.9.101 : octets=32 temps=2 ms TTL=126
Réponse de 192.168.9.101 : octets=32 temps=1 ms TTL=126

Statistiques Ping pour 192.168.9.101:
    Paquets : envoyés = 3, reçus = 3, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 1ms, Maximum = 25ms, Moyenne = 9ms
```

Pourquoi à votre avis toutes ces machines sont-elles joignables par leurs noms qualifiés (noms sur leurs domaines) ?

2 – Création et configuration de comptes utilisateurs du domaine Active Directory

Modification de paramètres de sécurité des mots de passe

- ☞ Regardez la vidéo  [sécurité mots de passe domaine AD.avi](#) et modifiez de même les paramètres de sécurité des mots de passe de votre domaine Active Directory `agence-i.C304.local` pour simplifier la création des comptes utilisateurs

Comptes utilisateurs du domaine Active Directory

- ☞ Lisez le document pdf [Comptes utilisateurs du domaine](#)

A quel mécanisme du TP n°1 sous Linux peut-on rapprocher celui des comptes utilisateurs du domaine Active Directory ?

Vous allez créer et configurer de manière optimale les comptes suivants dans votre domaine Active Directory `agence-i.C304.local` :

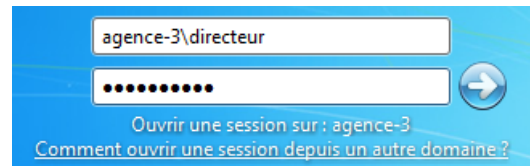
- un directeur, pouvant ouvrir une session n'importe quand sur tous les ordinateurs du domaine
- une secrétaire, dépendant du directeur, travaillant du Lundi au Vendredi de 8h à 17h, et ne pouvant ouvrir de session que sur l'ordinateur `secretariat` aux horaires de travail.
- deux techniciens employés en CDI, , dépendant du directeur, pouvant ouvrir des sessions à n'importe quel moment sur les ordinateurs `technique1` et `technique2` et également sur l'ordinateur `secretariat`.
- un technicien stagiaire, présent du Lundi au Jeudi de 9h à 16h jusqu'au 30 juin, dépendant du premier technicien en CDI, et ne pouvant ouvrir de session que sur les ordinateurs `technique1` et `technique2` pendant ses heures de présence.

- ☞ Définissez les paramètres de vos 5 comptes dans le tableau suivant, puis créez-les dans votre domaine AD `agence-i.C304.local`

| Prénom | Nom | Identifiant | Mot de passe | Gestionnaire | Expiration | Horaires | Ordinateurs |
|--------|-----|-------------|--------------|--------------|------------|----------|-------------|
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

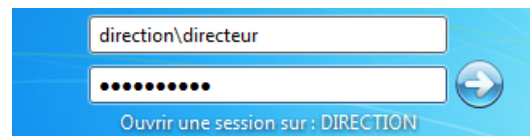
- ☞ Vérifiez que vous pouvez bien ouvrir une session avec votre compte « directeur » sur votre domaine `agence-i.C304.local` depuis la machine virtuelle membre `direction`

Créez-y ensuite un fichier quelconque sur le bureau



- ☞ Fermez la session et essayez d'en ré-ouvrir une avec votre compte « directeur » localement sur la machine `direction`

Y parvenez-vous ? Pourquoi ?



- ☞ Mettez en pause la machine `serveur` contrôleur du domaine, et essayez d'ouvrir sur la machine `secretariat` une session du domaine `agence-i` avec le compte « secrétaire ».

Essayez maintenant sur la machine `direction` de ré-ouvrir une session du domaine `agence-i` avec le compte « directeur ».


Que se passe-t-il ? Dans quel cas la session s'ouvre-elle ? Quel profil utilisateur retrouve-t-on alors ?

- ☞ Fermez la session précédente, rallumez la machine `serveur`, puis ouvrez une autre session, toujours avec votre compte « directeur » du domaine, mais cette fois-ci sur la machine `secretariat`

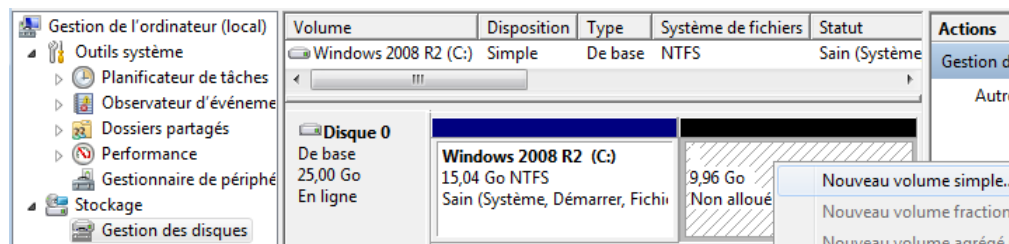
Retrouvez-vous le fichier précédemment créé sur le bureau ? Les fichiers du profil utilisateur « directeur » sont-ils locaux (propres à chaque machine du domaine) ou hébergés sur le serveur et commun à l'ouverture de session sur chaque machine ?

4 - Profils d'utilisateurs itinérants du domaine Active Directory

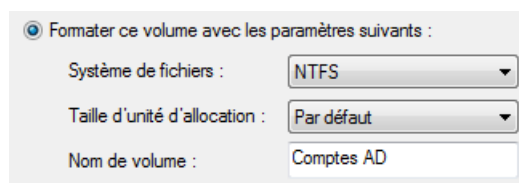
Nous allons tout d'abord créer une nouvelle partition sur le serveur, qui contiendra les profils des utilisateurs itinérants

- ☞ Sur votre machine contrôleur de domaine `serveur`, lancez l'outil d'administration  **Gestion de l'ordinateur** et sélectionnez le menu « Gestion de disques »

Cliquez avec le bouton droit sur la zone non allouée du disque dur et choisissez « Nouveau volume simple »



Choisissez la taille maximum et la lettre d'unité et formatez cette partition en NTFS sous le nom « Comptes AD »



Après le formatage, vérifiez de la nouvelle unité `E:` dans l'explorateur

- ☞ Ouvrez maintenant le document pdf **Profils utilisateurs itinérants** et lisez-le entièrement.

En suivant les différentes étapes, créez des **profils itinérants** sur la partition E: pour le « directeur » et les « techniciens »

Pourquoi cela ne présente-t-il pas d'intérêt de créer des profils itinérants pour la secrétaire ?

- ☞ Ouvrez ensuite une session du domaine avec votre compte « directeur » sur la machine cliente `direction`

La machine `direction` possède-t-elle une copie locale du dossier du profil itinérant du « directeur » ? Ou se situe cette copie ?

Enregistrez un petit texte « `essai.txt` » avec le bloc-note sur le bureau de la machine `direction` sous votre compte « directeur »

Que se passe-t-il lorsque vous fermez la session ? Ou retrouve-t-on le fichier texte précédent sur le contrôleur de domaine ?

Pour chaque utilisateur itinérant du domaine, Windows 2008 **synchronise** son dossier de profil sur le serveur avec leurs copies locales des différentes machines membres du domaine. A l'ouverture ou à la fermeture de session, lorsqu'une version d'un fichier diffère entre le serveur et la machine cliente, la version la plus récente est gardée : une copie s'effectue pour remplacer la plus ancienne. (une copie s'effectue également lorsque le fichier n'existe pas d'un côté)

Que se passerait-il à la fermeture de session avec un profil itinérant si vous téléchargez avec un fichier de 10 Go sur votre Bureau ? Et à l'ouverture de session sur une autre machine client que celle où s'est effectué le téléchargement ?

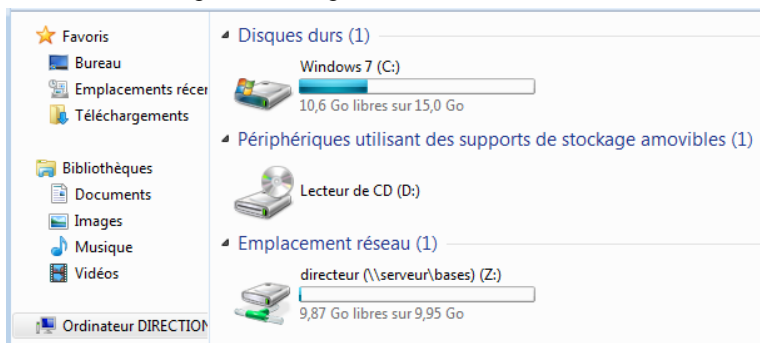
- ☞ Fermez la session « directeur » sur la machine cliente `direction`

5 - Création et configuration des dossiers de base

Ouvrez le document pdf **Dossiers de base** et lisez-le entièrement.

En suivant les différentes étapes, créez des **dossiers de base** sur la partition E: pour le « directeur » et les « techniciens »

Ouvrez une session du domaine sur la machine *direction* avec le compte « directeur » et vérifiez dans l'explorateur la présence du lecteur réseau associé à son dossier de base.



Quel est l'intérêt de stocker des fichiers dans son dossier de base plutôt que dans le dossier "Mes documents" ?

De quel mécanisme du TP n°1 celui des dossiers de base se rapproche-t-il ? Quelles en sont les différences ?

Remarque : Il est également possible de changer l'emplacement de certains dossiers du profil d'un utilisateur (par exemple « Bureau » et « Documents ») pour les situer dans le dossier de base, tout en les excluant du profil itinérant. Cela permet d'éviter les transferts de synchronisation, le travail s'effectuant directement sur les documents du lecteur réseau et non pas sur une copie locale.

Ouvrez une session du domaine sur la machine *secretariat* avec le compte « directeur »

Vérifiez la présence sur le bureau du fichier texte « essai.txt » créé à l'étape 4. Supprimez-le.

Créez un fichier texte « bureau.txt » sur le bureau et un autre « base.txt » dans le dossier de base Z: et écrivez-y "Secretariat".

Sans fermer celle sur la machine *secretariat*, ouvrez une autre session du domaine avec le compte « directeur » mais de nouveau sur la machine *direction*

Que trouve-t-on sur le bureau de la machine secretariat et dans le dossier de base ? Expliquez.

Sur la machine *direction*, créez ou modifiez le fichier « bureau.txt » sur le bureau et le fichier « base.txt » dans le dossier de base écrivez-y "Direction".

Arrêtez d'abord la machine *direction*, puis la machine *secretariat*, et allez sur le contrôleur Windows 2008 voir les fichiers de votre directeur dans le dossier "Bureau" de son profil, et dans son dossier de base.

Quelles versions des fichiers voit-on alors sur le contrôleur du domaine ? Expliquez pour chacun des fichiers.