

*Document propriété de MICROFER Paris Nord
Reproduction et diffusion
interdite sans autorisation.*

005-Workgroup et domaine Windows



Domaine internet:

Toute machine connectée à Internet est identifiée par une adresse unique, dite "adresse IP", sous la forme d'un nombre binaire codé en IP V4 sur 32 bits (ou plus, cf. IP V6).

La manipulation de tels nombres n'étant pas pratique, on va donner à chaque machine un nom symbolique, appelé "nom de domaine", beaucoup plus parlant et plus facile à retenir par un humain.

C'est un "service d'annuaire" qui effectue la traduction d'un nom symbolique en adresse IP. Ce service, géré automatiquement par des serveurs dialoguant entre eux est appelé "DNS" (Domain Name Service)...

Chaque point, dans le nom symbolique, sépare ce qu'on appelle un "domaine" d'un "sous-domaine". L'arborescence doit être lue de droite à gauche.

Les domaines de 1er niveau (les plus à droite) sont définis à l'échelle mondiale par l'ICANN (Internet Corporation for Assigned Names and Numbers) (.com, .org, .net, ...) et de plus chaque pays possède son propre domaine (.be, .ca, .ch, .fr, .ch, ...)

Les domaines de 2ème niveau définissent une entité, une entreprise, un organisme, ... (ex : ".snf", ".microsoft", google, ...)

Les domaines de 3ème niveau et au-delà sont facultatifs, et sont gérés par les entités, les entreprises, les organismes, ... pour distinguer plusieurs serveurs éventuels.

Quand une entité décide de "déposer un nom de domaine", elle s'adresse à un prestataire habilité pour le faire qui va vérifier si le nom n'existe pas déjà, et ensuite va lui attribuer une (ou plusieurs) adresse(s) IP disponible(s).

Le couple domaine-adresse IP est ensuite communiqué à des serveurs DNS, tous connectés à Internet, qui vont dialoguer entre eux pour "répliquer" (si besoin est) cette mise à jour d'annuaire.

Domaine Microsoft:

Cela concerne l'organisation d'un réseau de machines utilisant des OS Microsoft et la façon de gérer les comptes des utilisateurs de ces machines. Il peut être organisé en "Groupe de travail" (Workgroup) ou en "Domaine".

Workgroup :

Chaque machine est autonome, et gère elle-même la liste des utilisateurs autorisés à s'y connecter (nom et mot de passe), avec leurs droits respectifs.

Si l'utilisateur "Daniel" de la machine "A", mot de passe "MicroFer", veut se connecter sur la machine "B" (utilisation d'une ressource partagée, disque ou imprimante), il faudra qu'il existe également sur cette machine B un compte identique ("Daniel"/"MicroFer").

Ce système est simple et ne demande aucune architecture particulière, un serveur n'est pas nécessaire. Par contre si le nombre d'utilisateurs est important, cela devient vite ingérable (il faut modifier la liste des comptes sur chaque machine pour que tout le monde puisse communiquer)

Un Workgroup est défini par un nom, totalement arbitraire, et il est fixé au niveau de chaque machine.

Sous session **Administrateur** >> **Panneau de configuration** >> **Système et sécurité** >> **Système** >> Dans la rubrique Paramètres de nom d'ordinateur, de domaine et de groupe de travail, cliquer sur le lien **Modifier les paramètres** ...

Dans un même réseau, il peut y avoir plusieurs groupes distincts (à la limite autant qu'il y a de machines!). Le fait d'appartenir au même workgroup facilite l'exploration du réseau et réduit les temps de recherche de machine ... Toute machine, quel que soit son OS, peut être membre d'un Workgroup.

Domaine (Microsoft):

La gestion des comptes (et des machines) est centralisée sur un ou plusieurs serveurs de domaine.

Lorsque l'utilisateur "Daniel" veut ouvrir une session sur sa machine "A", l'identification "Daniel"/"MicroFer" est transmise (automatiquement, par diffusion) sur le réseau, pour aboutir à un serveur responsable du domaine (le nom de ce domaine est indiqué dans la boîte dialogue de connexion).

Le serveur de domaine va examiner cette requête, en vérifiant que :

- la machine "A" est autorisée
- le compte "Daniel" est autorisé
- que le mot de passe "MicroFer" est correct

Il va retourner alors un "jeton" d'autorisation à "A", ce qui va permettre l'ouverture de la session en local, et aussi autoriser les montages de ressources éventuelles.

NB: pour qu'un utilisateur puisse se connecter depuis un poste de travail à un domaine, il aura fallu au préalable que cette machine ait été "déclarée" dans le domaine (opération effectuée par un administrateur de domaine)

Dans le cas d'un nouvel utilisateur, il suffit de créer son compte uniquement sur le serveur. A partir de cet instant, il pourra se connecter sur n'importe quelle machine du domaine, et accéder à n'importe quelle ressource, sous réserve de droits suffisants alloués par l'administrateur.

De plus, si l'administrateur a prévu la gestion de "profils itinérants" (stockés sur le serveur), l'utilisateur retrouvera, quelle que soit la machine sur laquelle il se connecte, l'environnement de travail qui lui est propre (fond d'écran, icônes, raccourcis, ...)

Tout domaine est identifié par un nom, arbitraire, qui a été défini une fois pour toutes sur le serveur principal.

La mise en place d'un domaine peut s'avérer très complexe (dans de très grandes entreprises cela peut nécessiter plusieurs mois) et nécessite obligatoirement la présence d'administrateur(s).

Document de travail, en cours de rédaction ...