WILD CODE SCHOOL

# Active Directory - partie 1

Service d'annuaire

Quelle est la différence entre un annuaire téléphonique et un annuaire informatique ?

# Plan

1 - Introduction

2 - Arborescence AD

3 - Composants AD

WILD CODE SCHOOL

# Introduction

# Au début

Active Directory (AD) est une mise en œuvre par Microsoft des services d'annuaire LDAP pour les systèmes d'exploitation Windows.

Objectif principaux :

- Fournir des services centralisés **d'identification**, **d'authentification**, et de **gestion de politiques** dans un réseau d'ordinateurs utilisant divers OS.
- Répertorier les éléments d'un réseau tels que les comptes utilisateurs, les serveurs, les postes de travail, et faciliter leur gestion.

# Evolution technique

- A l'origine : nommé NTDS (NT Directory Services).
- Introduit en 1996
- Première utilisation majeure avec Windows 2000 Server (1999)
- Evolution depuis la base de comptes de domaine SAM avec l'utilisation du protocole LDAP
- Evolution du stockage AD de Jet à ESENT

# Détail sur la base SAM

Avant AD, Windows utilisait la base SAM pour gérer les comptes d'utilisateurs et de groupes sur des ordinateurs locaux ou dans un domaine.
SAM était efficace pour les petits réseaux, mais limitée dans ses capacités de gestion et d'évolutivité pour les grands réseaux.

# Active Directory

Selon Microsoft :
Un répertoire est une structure hiérarchique qui stocke des informations sur les objets sur le réseau. Un service d'annuaire, tel que **Active Directory Domain Services (AD DS)**, fournit les méthodes permettant de stocker les **données d'annuaire** et de mettre ces données à la disposition des **utilisateurs et administrateurs du réseau**. Par exemple, les **services de domaine Active Directory** stockent des informations sur les comptes d'utilisateurs, comme les noms, les mots de passe, les numéros de téléphone et permettent aux utilisateurs autorisés du même réseau d'accéder à ces informations.

# Active Directory

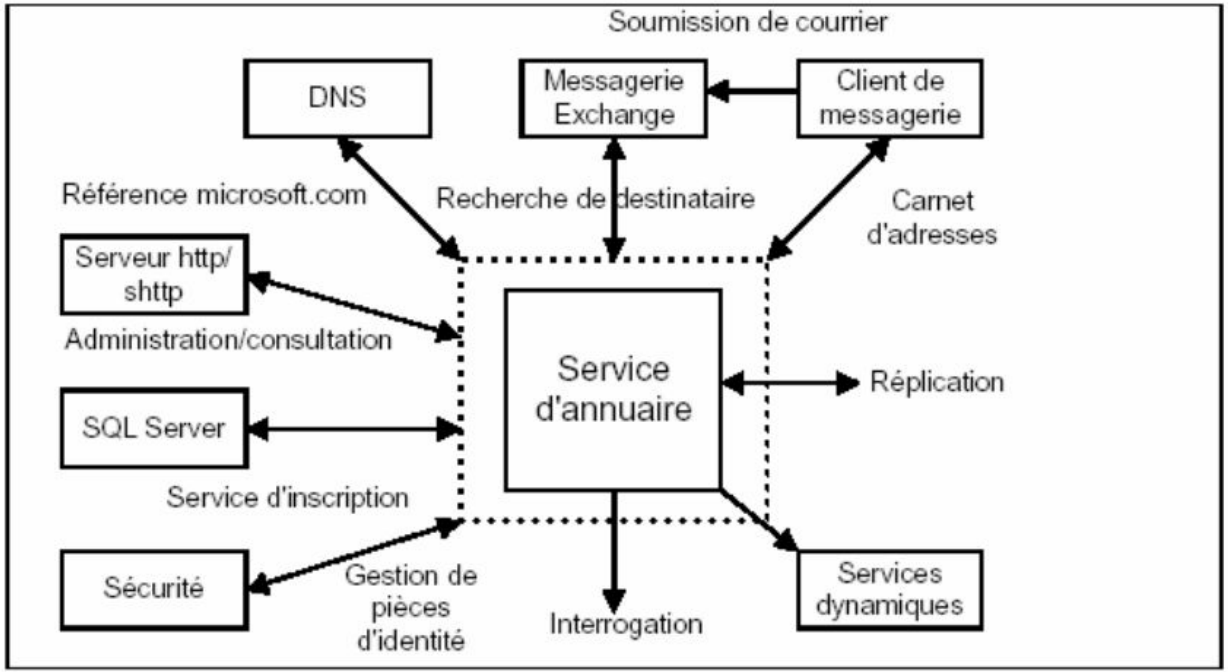
Selon wikipédia :
Active Directory (AD) est la mise en œuvre par Microsoft des **services d'annuaire LDAP** (*Lightweight Directory Access Protocol*, qui est une norme pour les systèmes d'annuaire) pour les systèmes d'exploitation Windows.

# Une définition plus concise

AD DS :

- Est un système qui intègre un stockage (une **base de données (BDD) hiérarchique)** et les **services** pour mettre en relation les utilisateurs et les ressources réseau.
- Contient des objets (utilisateurs, ordinateurs, services, …).
- Est administrable en GUI ou en CLI (PowerShell)
- Utilise LDAP pour accéder à l'annuaire

# Un chef d'orchestre



# Quelques chiffres

- 25% du marché dans la catégorie des outils de gestion d'identité et d'accès
- Nombre maximum d'objets pouvant être crée : plus de 2 milliards
- Nombre maximum de GPO applicable à un objet : 999
- Nombre maximum d'appartenance de groupe pour un objet : 1015

# Le protocole LDAP

AD utilise LDAP, un protocole standardisé et ouvert pour accéder et gérer les services d'annuaire.
Il permet de rechercher et de manipuler des données dans l'annuaire AD de manière structurée.

Avantages :

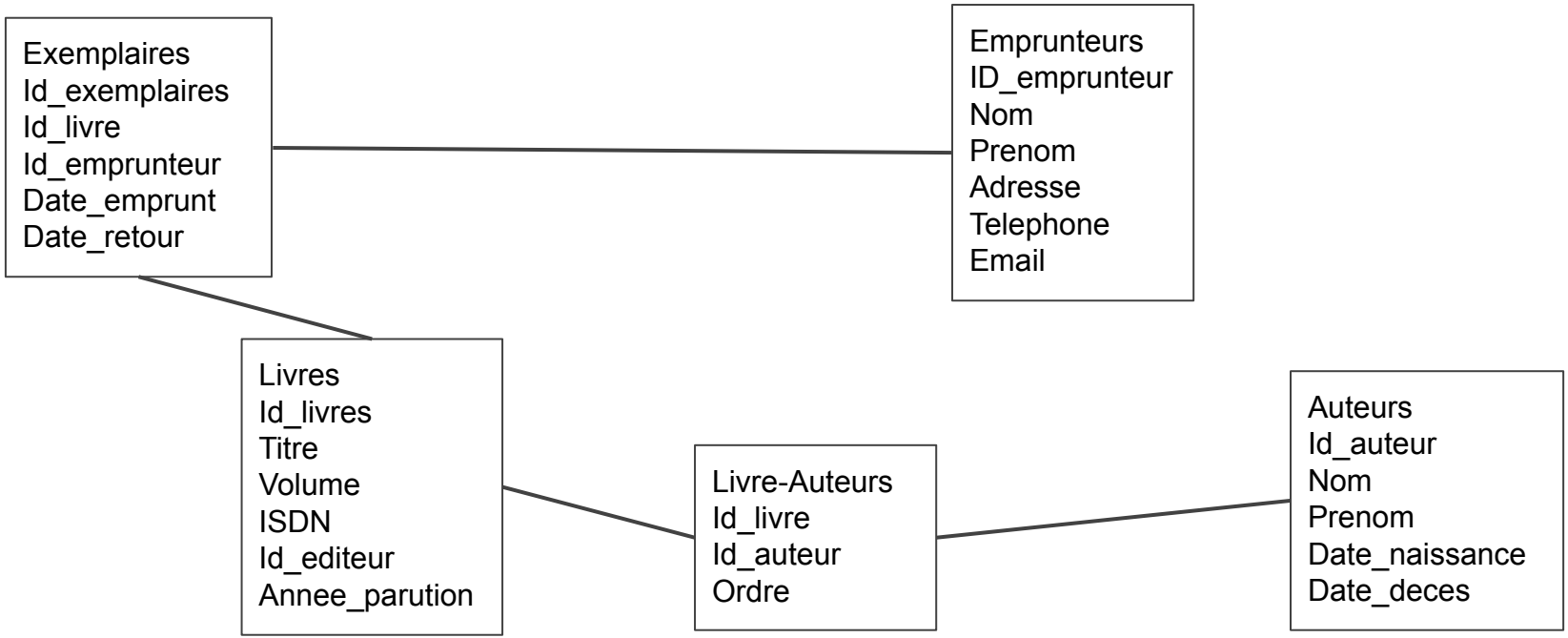
- Grande compatibilité avec de nombreux services et applications
- Méthode standard d'interrogation et de modification de l'annuaire.
- Intégration possible avec d'autres systèmes d'annuaire qui supportent LDAP (systèmes GNU/Linux, OpenLDAP, SSO, etc.)

# Annuaire LDAP

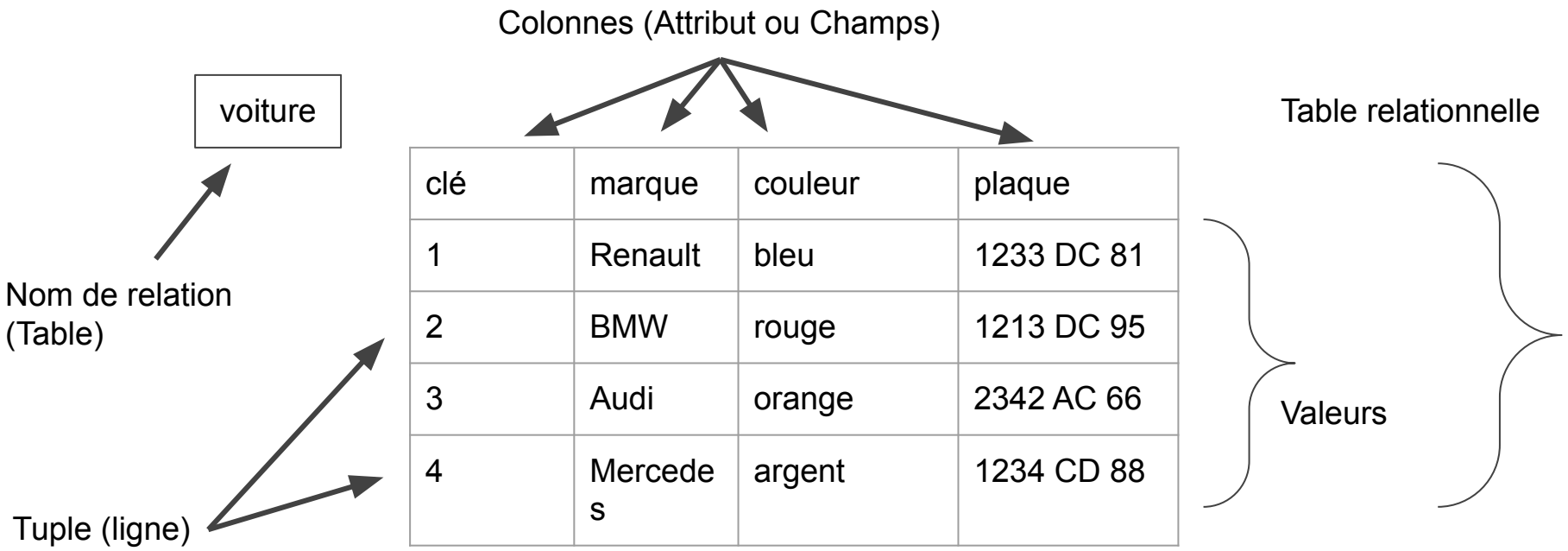
“**Un annuaire LDAP** est comme l'annuaire téléphonique”.

Un annuaire LDAP (*Lightweight Directory Access Protocol*) est une **BDD hiérarchique**
=> Différent d'un **SGBD** (*Système de Gestion de Base de Données*) classique relationnel.

# Base de donnée relationnelle

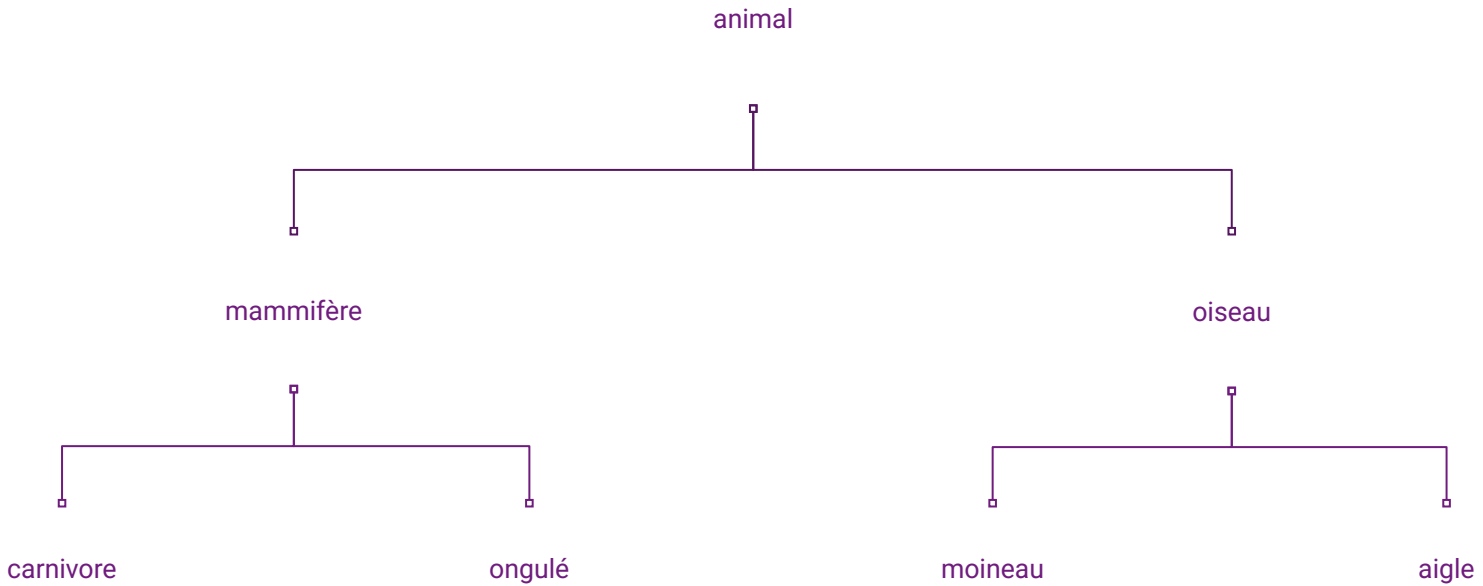


# Table de BDD relationnelle

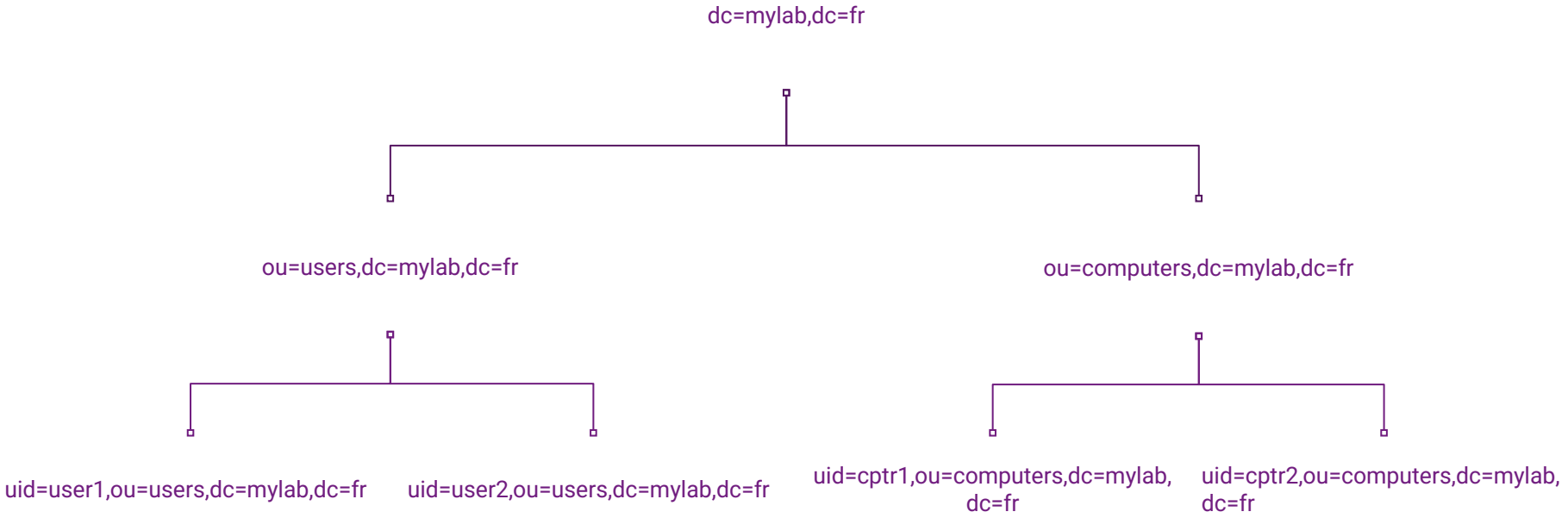



| clé | marque | couleur | plaque |
|---|---|---|---|
| 1 | Renault | bleu | 1233 DC 81 |
| 2 | BMW | rouge | 1213 DC 95 |
| 3 | Audi | orange | 2342 AC 66 |
| 4 | Mercedes | argent | 1234 CD 88 |

# Une base de données hiérarchique



# Une autre BDD hiérarchique



# Les rôles AD

**AD CS** (*Active Directory Certificate Service*)
- Gestion et création des clés ainsi que des certificats

**AD FS** (*Active Directory Federation Services*) - depuis Serv.2008
- Via un portail gestion d'un SSO (Single Sign-On) pour les applications

**AD RMS** (*Active Directory Rights Management Services*) - depuis Serv.2008 R2
- Gestion des autorisations fine sur les fichiers (uniquement sur applications compatibles, comme Office)

**AD LDS** (*Active Directory Lightweight Directory Services*)
- Service d'annuaire light, pas de domaine (pas de contrôle d'accès).

# Le rôle AD principal

**AD DS** (*Active Directory Domain Service*)

- Mise en œuvre d'un domaine et d'un annuaire Active Directory
- Gestion utilisateurs, ordinateurs, groupes, ouverture de session, contrôle d'accès aux ressources,…

WILD CODE SCHOOL

# Arborescence AD

# Une structure logique

Cette arborescence AD représente une structure logique indépendante du site.

# Objet AD

Les objets AD sont les éléments de base de la BDD AD et représentent les ressources physiques, logiques et les services au sein d'un environnement réseau.

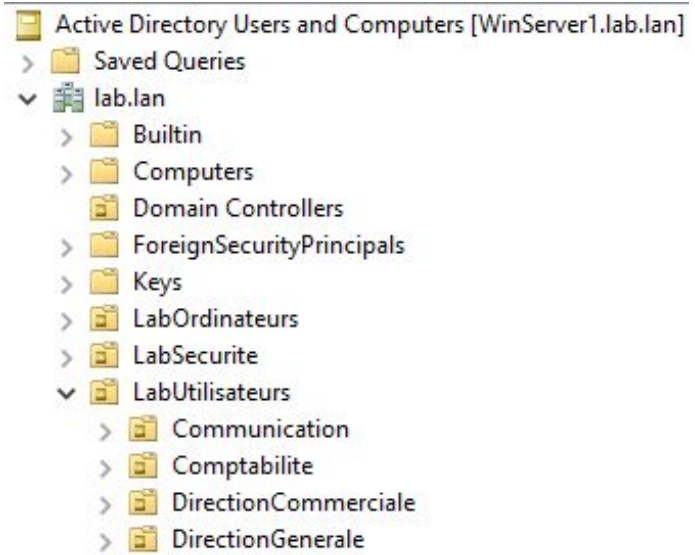
# Information sur un objet

```
PS C:\Lab>  Get-ADObject -Filter {Name -like "*server*"}

DistinguishedName                                Name        ObjectClass     ObjectGUID
-----------------                                ----        -----------     ----------
CN=Server,CN=System,DC=lab,DC=lan                Server      samServer       a15302e...
CN=WIN1,OU=Domain Controllers,DC=lab,DC=lan      WIN1        computer        357d4a5...
```

# Unité d'Organisation

L'**Unité d'Organisation**, ou **OU** (*Organizational Unit*) est le niveau le plus bas de la structure hiérarchique d'Active Directory.
Les OUs sont des "boites" dans lesquels les objets tels que les utilisateurs, les groupes et les ordinateurs sont organisés.



# Unité d'Organisation

Elles permettent :

- Une gestion et une délégation administratives fines
- D'organiser de façon logique les objets de l'annuaire
- De faciliter la délégation de pouvoir selon l'organisation des objets et de contrôler l'environnement des utilisateurs et des ordinateurs grâce à l'application de stratégie de groupe, ou **GPO** (*Group Policy Object*)

# Information sur une OU

```
PS C:\Lab>  Get-ADOrganizationalUnit -Filter {Name -like "*serveurs*"}


City                        :
Country                     :
DistinguishedName           : OU=Serveurs,OU=Bordeaux,OU=Ordinateurs,DC=lab,DC=lan
LinkedGroupPolicyObjects    : {}
ManagedBy                   :
Name                        : Serveurs
ObjectClass                 : organizationalUnit
ObjectGUID                  : 073ef3cc-76b6-4d30-a241-0e45aef90183
PostalCode                  :
State                       :
StreetAddress               :
```

# Domaine

Un domaine AD est une unité administrative et de sécurité dans un environnement AD.
Il représente un groupe de ressources réseau et d'utilisateurs qui sont gérés comme une seule entité.

# Fonctionnalités du domaine AD

**Contrôle Centralisé :**
Gestion centralisée des politiques de sécurité, des comptes d'utilisateurs, des comptes d'ordinateurs, etc.
→ permet une administration et une gestion simplifiées, entre-autre pour l'authentification et l'autorisation.

**Périmètre de Sécurité :**
A l'intérieur, les politiques et les contrôles d'accès peuvent être appliqués de manière cohérente.
Toutes les ressources du domaine sont soumise à ces politiques.

# Fonctionnalités du domaine AD

**Partage de Ressources :**
Les utilisateurs d'un même domaine peuvent partager des ressources (fichiers, imprimantes, applications, ...) avec des contrôles d'accès gérés centralisés.

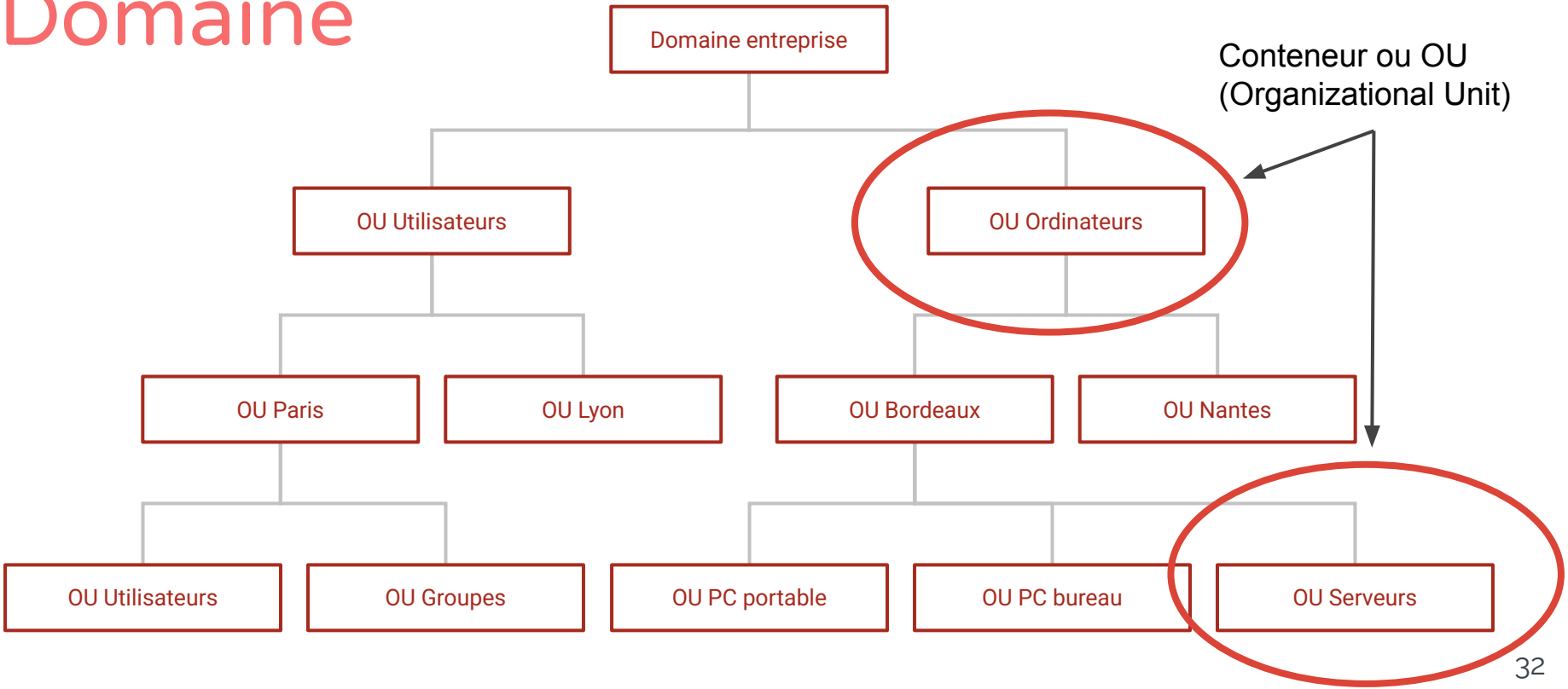
**Authentification et Autorisation :**
AD gère l'authentification des utilisateurs et des ordinateurs dans le domaine. Il contrôle leur accès aux ressources du réseau basé sur les politiques de sécurité définies.

# Fonctionnalités du domaine AD

**Réplication des Données :**
Les informations du domaine sont répliquées entre les **contrôleurs de domaine** pour assurer la cohérence et la disponibilité des données de l'annuaire dans tout le domaine.

**Structure Hiérarchique :**
Il peut faire partie d'une structure plus large appelée **forêt** AD, qui est une collection de plusieurs domaines.

# Domaine


Domaine entreprise
Conteneur ou OU
(Organizational Unit)
OU Utilisateurs
OU Ordinateurs
OU Paris
OU Lyon
OU Bordeaux
OU Nantes
OU Utilisateurs
OU Groupes
OU PC portable
OU PC bureau
OU Serveurs

# Information sur le domaine

```
PS C:\Lab>  Get-ADDomain | Select-Object DomainControllersContainer,DomainMode,DomainSID,Name | Format-List


DomainControllersContainer  : OU=Domain Controllers,DC=lab,DC=lan
DomainMode                  : Windows2016Domain
DomainSID                   : S-1-5-21-3649124935-1597064440-2657112874
Name                        : lab
```

## Workgroup

Tous les ordinateurs ont le même rôle standard

On peut se connecter uniquement où un compte local a été créé

Tous les ordinateurs doivent être sur le même réseau local

Limite de gestion fonctionnelle à quelques dizaines de machines

Aucune centralisation

## Domaine

Un ou plusieurs ordinateurs sont des serveurs (DC)

On peut se connecter n'importe où avec un compte de domaine

Les ordinateurs peuvent être sur des réseaux différents

Il n'y a pas de limite au nombre de machines

Centralisation avec les DC

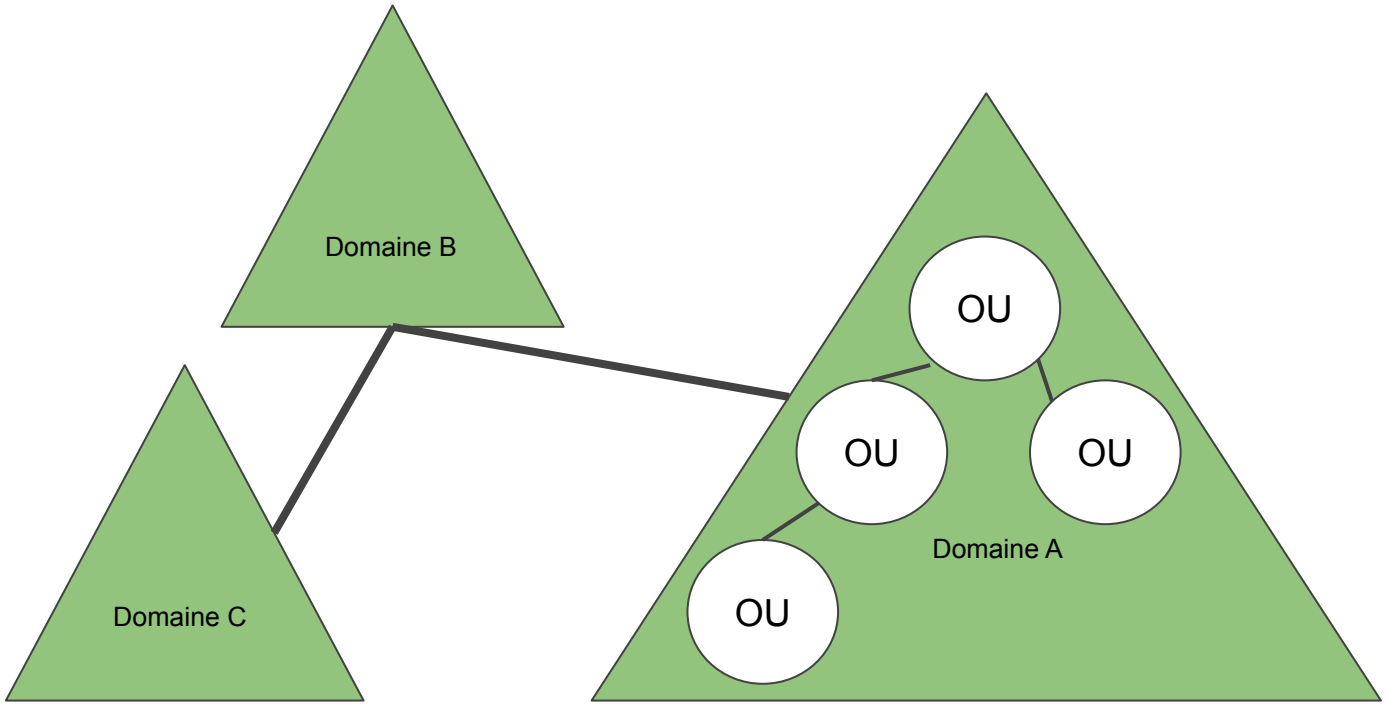
# Arbre

Un arbre est une arborescence de domaines.

Un arbre est constitué de plusieurs domaines qui partagent un schéma et une configuration communs, formant un **espace de noms contigu**.
Les domaines d'une arborescence sont également liés par des **relations d'approbation**.
2 visions possibles :

- Vue par les relations d'approbation entre les domaines
- Vue par l'espace de noms de l'arborescence de domaine.

# Arbre



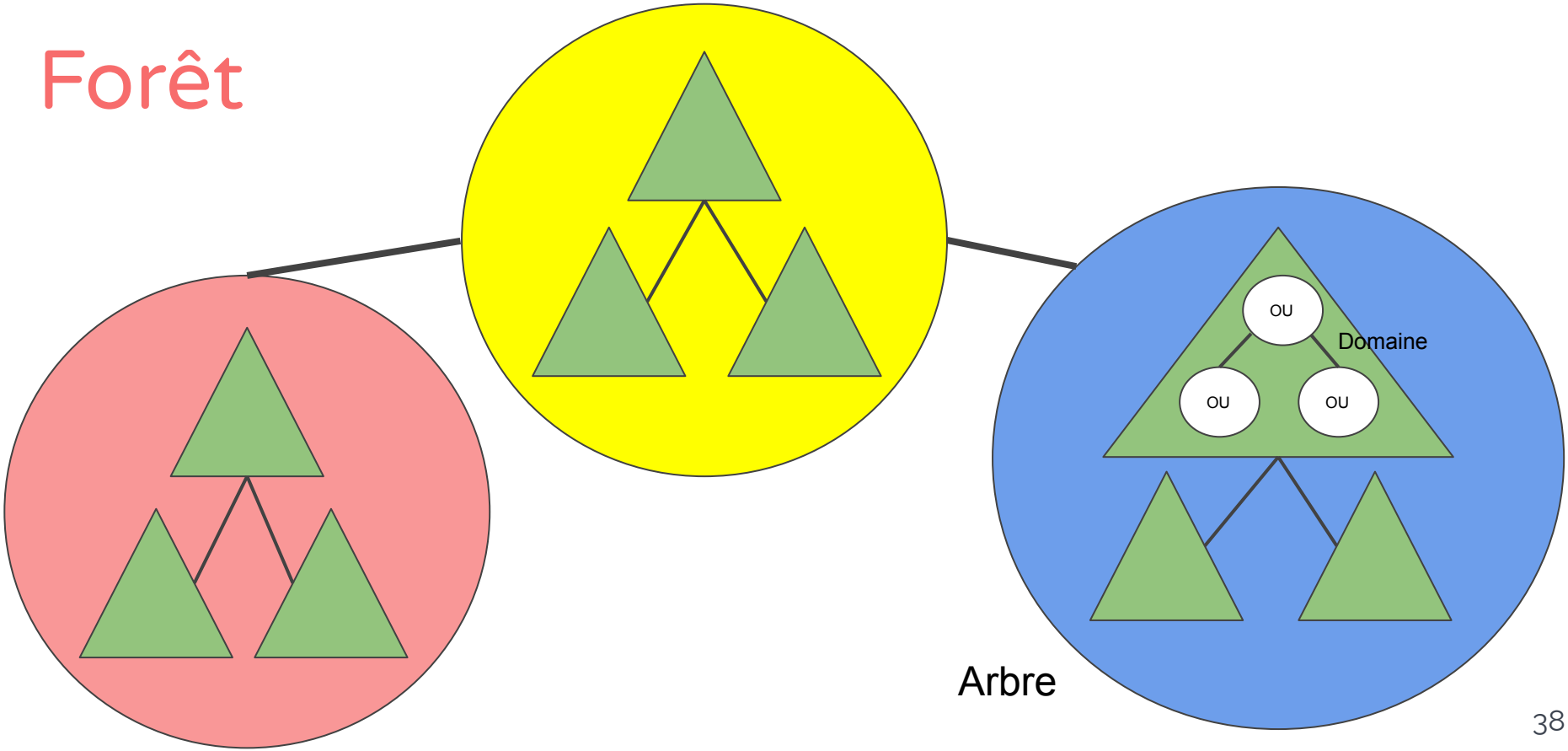
# Forêt AD

Une forêt est une structure hiérarchique de plusieurs domaines indépendants.

Dans une forêt :

- Tous les **arbres** partagent un **schéma d'annuaire** commun
- Tous les domaines :
  - Partagent un « Catalogue Global » commun
  - Fonctionnent de façon indépendante
  - Ont des relations possibles entre-eux

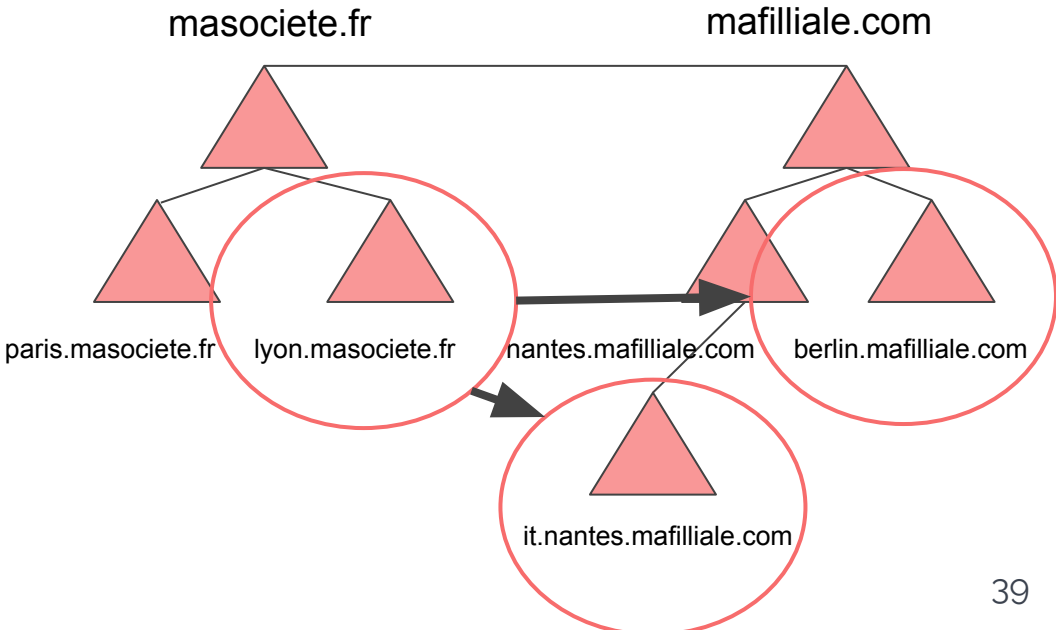
# Forêt



# Avantage d'une forêt ?

Simplification de l'administration et flexibilité.

ex: Un utilisateur du domaine *lyon.masociete.fr* pourra accéder à des ressources situées dans le domaine *it.nantes.mafilliale.com*, ou se connecter sur une machine du domaine *berlin.mafilliale.com* (avec les autorisations).



# Information sur la forêt

```
PS C:\Lab> Get-ADForest

ApplicationPartitions      : {DC=ForestDnsZones,DC=lab,DC=lan, DC=DomainDnsZones,DC=lab,DC=lan}
CrossForestReferences      : {}
DomainNamingMaster         : AD1.lab.lan
Domains                    : {lab.lan}
ForestMode                 : Windows2016Forest
GlobalCatalogs             : {AD1.lab.lan}
Name                       : lab.lan
PartitionsContainer        : CN=Partitions,CN=Configuration,DC=lab,DC=lan
RootDomain                 : lab.lan
SchemaMaster               : AD1.lab.lan
Sites                      : {Default-First-Site-Name}
SPNSuffixes                : {}
UPNSuffixes                : {}
```

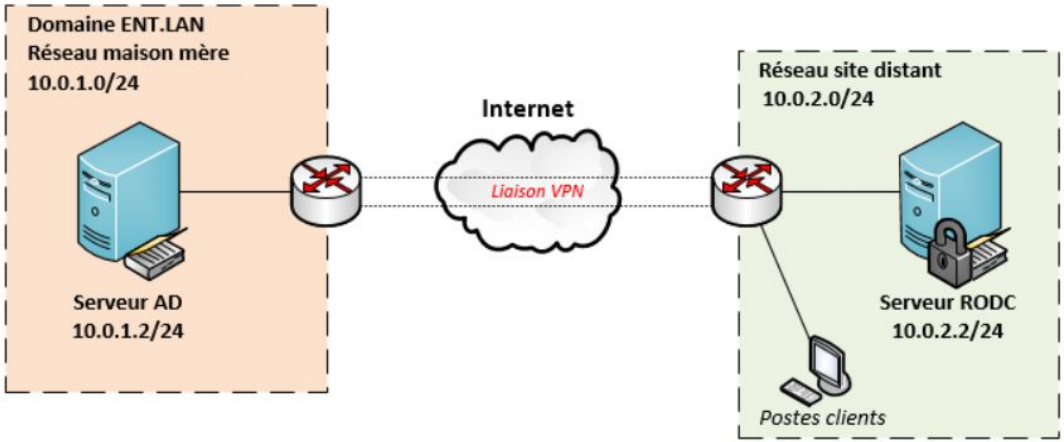
WILD CODE SCHOOL

# Composants AD

# Contrôleur de domaine

Un **contrôleur de domaine**, ou **DC** (*Domain Controler*) est un serveur important pour un domaine.
Tous les domaines ont un DC.
Un DC est indispensable au bon fonctionnement du domaine.
Si le DC est éteint ou corrompu → Le domaine est inutilisable.

# RODC (Read Only Domain Controller)




- Serveur ayant le rôle de DC
- Possède des droits de lecture seule
- Souvent utilisé pour les sites distants

# Pourquoi utiliser un RODC ?

Améliorations d'**équilibrage de la charge**.

**Continuité de service** :

- Le serveur AD du site local transmettra les modifications de l'AD au RODC du site distant
- Transmission également des modifications du DNS afin que les utilisateurs du site distant disposent toujours d'un service de résolution de nom en local pour accéder à Internet en cas de coupure de la liaison internet du DC principal.

# Information sur un DC

```
PS C:\Lab> Get-ADDomainController

ComputerObjectDN            : CN=AD1,OU=Domain Controllers,DC=lab,DC=lan
DefaultPartition            : DC=lab,DC=lan
Domain                      : lab.lan
Enabled                     : True
Forest                      : lab.lan
HostName                    : AD1.lab.lan
IPv4Address                 : 10.10.1.2
IsGlobalCatalog             : True
IsReadOnly                  : False
LdapPort                    : 389
Name                        : AD1
OperatingSystem             : Windows Server 2022 Standard Evaluation
OperatingSystemVersion      : 10.0 (20348)
OperationMasterRoles        : {SchemaMaster, DomainNamingMaster, PDCEmulator, RIDMaster...}
ServerObjectDN              : CN=AD1,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=lab,DC=lan
Site                        : Default-First-Site-Name
SslPort                     : 636
```

# Le catalogue global

Le catalogue global AD est une version spéciale d'un DC qui contient des informations étendues sur l'ensemble de la forêt AD, en plus des données de son propre domaine.

# Fonctionnalités du catalogue global

**Contrôleur de Domaine Étendu** :
C'est un DC qui contient (en plus de sa propre BDD) des informations sur tous les domaines de la forêt.
Grâce à sa vue complète, un DC avec le rôle de catalogue global peut localiser des objets dans toute la forêt. Les autres DC s'appuient sur lui pour cette fonctionnalité

**Répliqua Partiel pour tous les Domaines** :
Il possède un répliqua partiel de tous les attributs de tous les domaines de la forêt ⇒ il dispose ainsi d'informations globales sur la forêt entière.

# Qui est Catalogue Global ?

Le 1er DC créé au sein d'une forêt est automatiquement catalogue global.

⇒ A l'installation d'un AD → nouveau domaine dans une nouvelle forêt → ce DC sera catalogue global.

Il est possible de configurer d'autres DC en tant que serveur de catalogue global afin de réguler le trafic.

# Conclusion

- Définir ce qu'est un annuaire LDAP et une base de données hiérarchique
- Connaître les éléments de la structure logique de l'arborescence AD (objet, OU, domaine, arbre, forêt)
- Les différences entre un domaine et un workgroup
- DC, RODC, et Catalogue Global