Gestion centralisée des

G.VALET – Version 1.11

G. Valet – genael.valet@diderot.org

Sommaire

- Dans ce chapitre, nous aborderons :
  - Définition d'un utilisateur et d'un groupe d'utilisateurs
  - Authentification centralisée
  - Protocole LDAP
  - Infrastructures d'annuaire
    - Open Ldap
    - Active Directory

Qu'est-ce qu'un utilisateur ?

- Définition :
  - Un utilisateur est un individu travaillant sur un ordinateur
    - Par extension, un utilisateur se définit par une identité numérique dans un système d'information
      - Un nom d'utilisateur / mot de passe
      - Une empreinte biométrique
      - ...
- La notion de compte utilisateur permet d'associer à la personne :
  - Un environnement de travail particulier (Logiciels, paramétrages)
  - Des droits d'accès aux ressources du système d'information

genael.valet@diderot.org

Les types d'utilisateurs

- Personne physique :
  - Cas d'un individu associé au système d'information
- Administrateur:
  - C'est un utilisateur ayant des droits lui permettant de modifier le paramétrage du système et d'accéder à des tâches d'administration
- Utilisateur système :
  - Associé à une fonction plus qu'à une personne physique.
    - Exemple : Compte utilisateur autorisé à démarrer un programme en tâche de fond

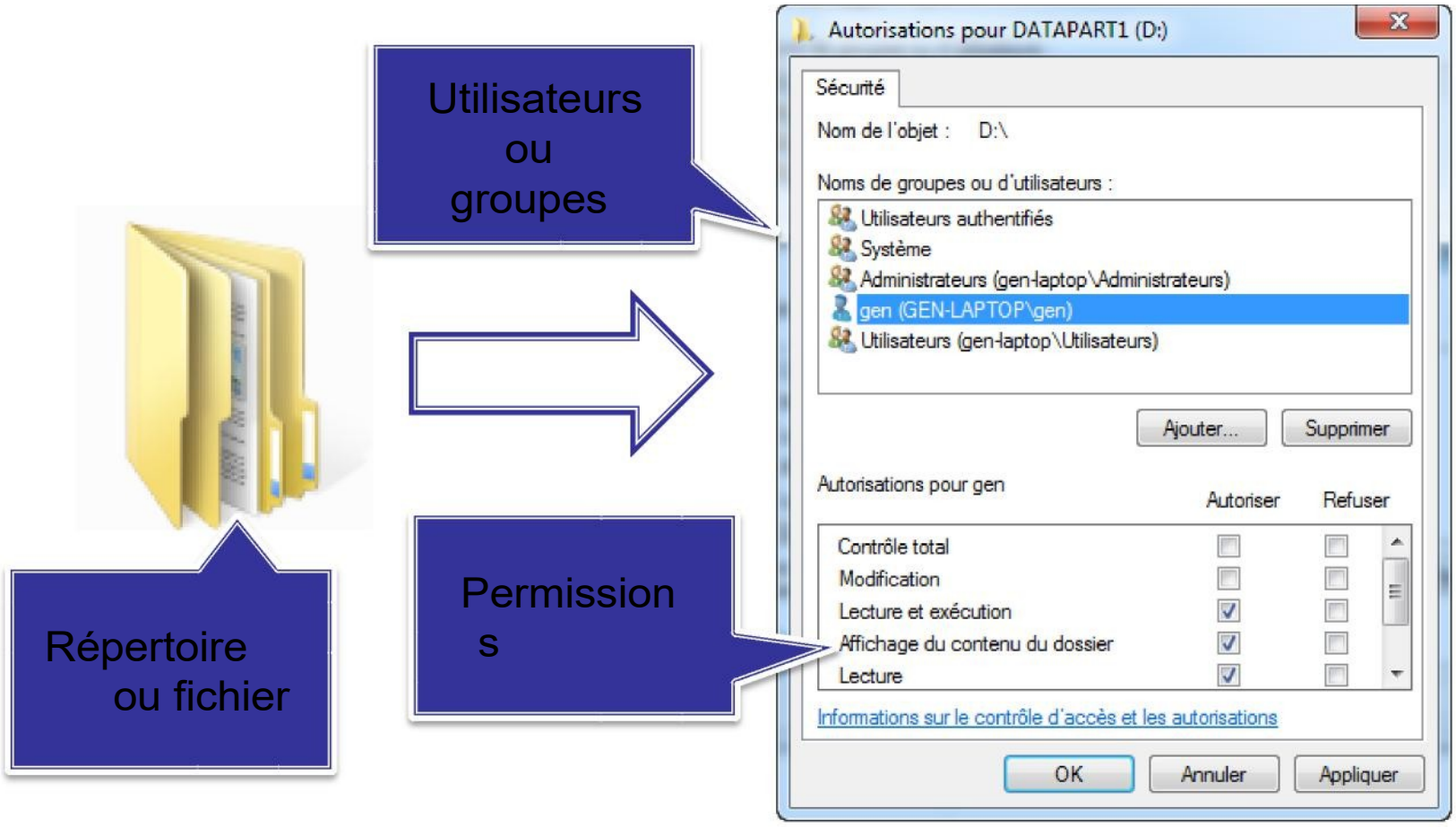
Et les groupes d'utilisateurs

- Il est parfois plus simple de regrouper les utilisateurs pour :
  - Définir des droits à tout un ensemble logique d'utilisateurs
    - Exemple : Tous les utilisateurs du service comptabilité ont les droits permettant d'imprimer les fiches de paie
  - La gestion est plus efficace et évite un travail répétitif d'affectation d'un droit à un utilisateur
- Tout membre du groupe bénéficie des droits accordés au groupe
- Permet de distribuer les rôles au sein du système
  - Opérateurs d'impression pour les imprimantes
  - Administrateurs pour la maintenance
  - ...

G. Valet – genael.valet@diderot.org

Permissions accordées à un utilisateur

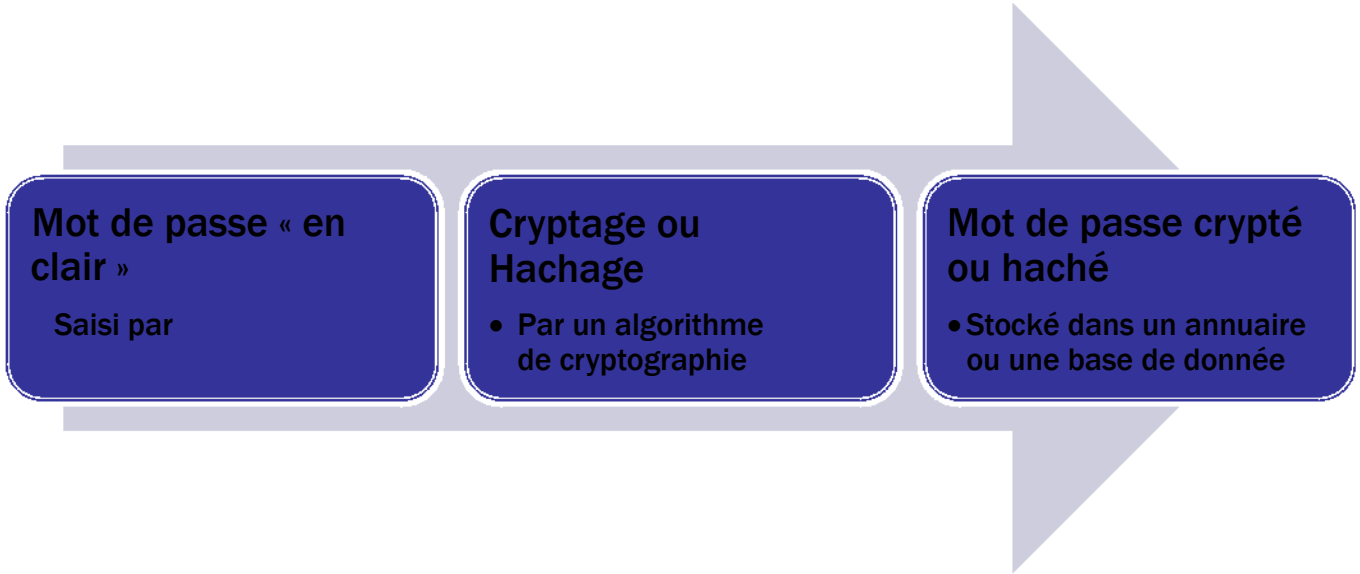
- Exemple du système de fichier NTFS



genael.valet@diderot.org

Authentification d'un utilisateur

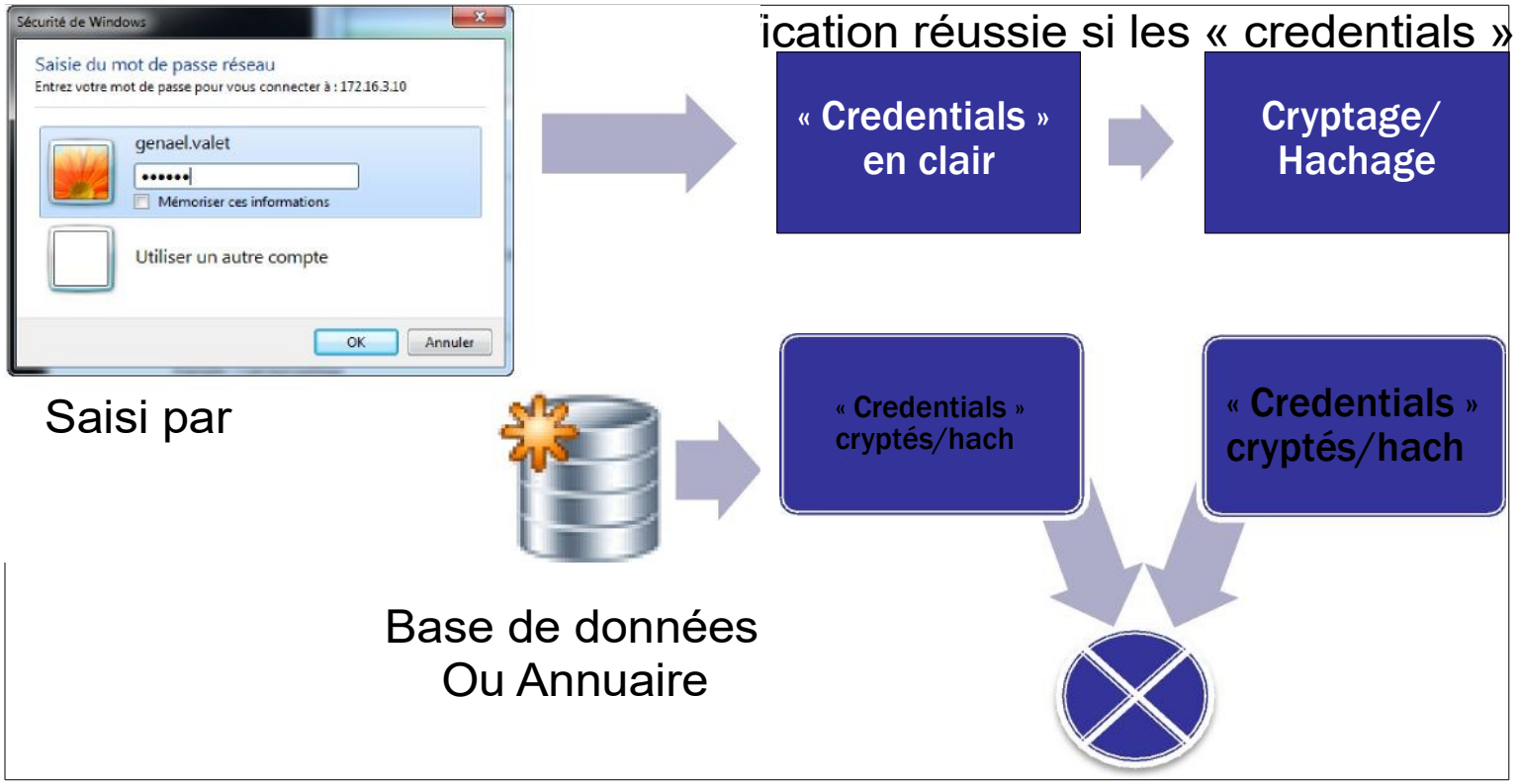
- L'authentification permet à l'utilisateur de fournir les informations nécessaires au système pour l'identifier
  - Nom d'utilisateur ou login
  - Mot de passe
- Le mot de passe n'est pas stocké tel quel :



genael.valet@diderot.org

Processus d'authentification

- Au niveau du système d'exploitation, le processus est le suivant :



Les systèmes multi-utilisateurs

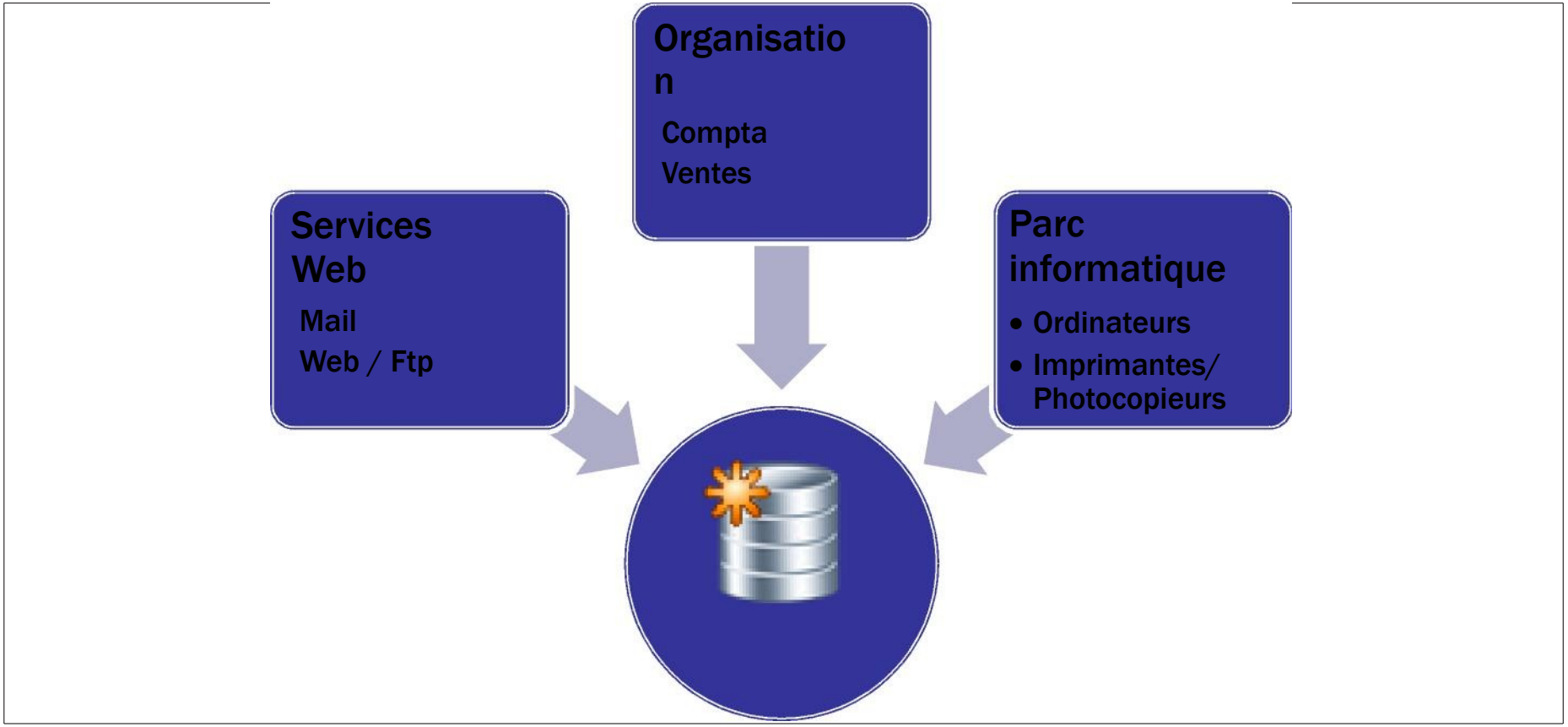
- Dans un système, plusieurs utilisateurs peuvent profiter des mêmes ressources simultanément
- Un système d'exploitation moderne permet un accès simultané à plusieurs utilisateurs
  - Aux ressources physiques : Imprimantes, Disque externe, ...
  - A un même système de fichier local ou distant
- L'identification d'un utilisateur est alors centralisée
  - La gestion des données d'authentification est centralisée sur un ou plusieurs serveurs/annuaires
  - Organisation des utilisateurs et des machines en « forêt »

genael.valet@diderot.org

G. Valet – genael.valet@diderot.org

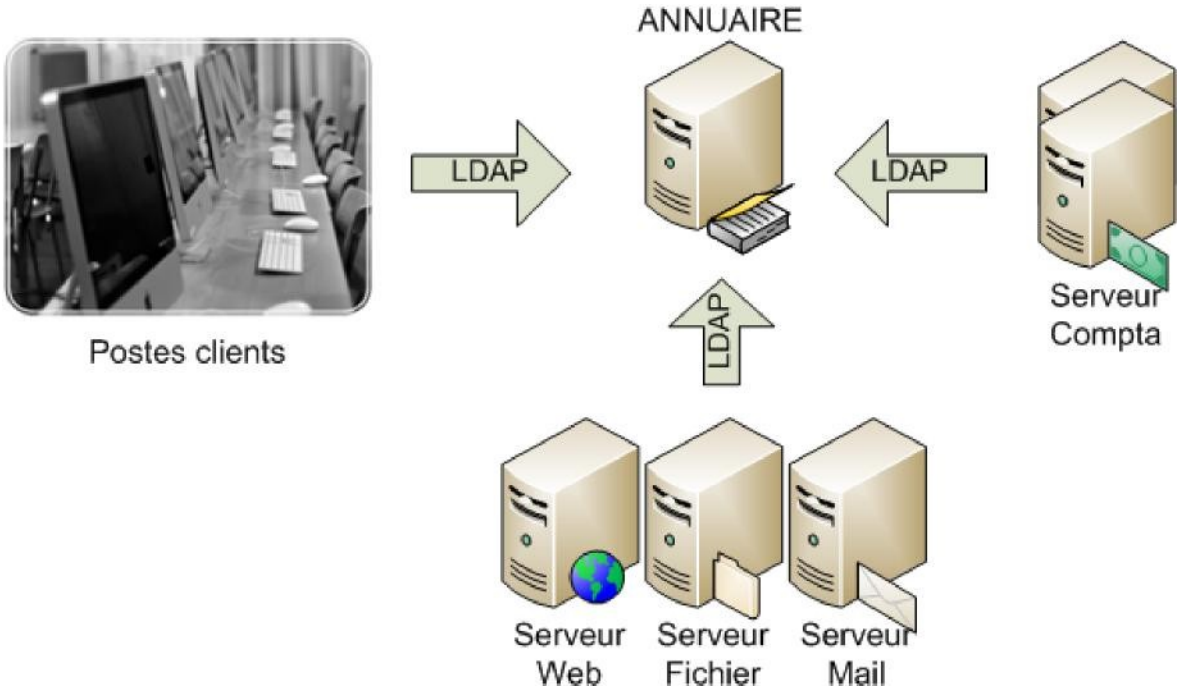
Système d'information avec authentification centralisée

- La centralisation permet de partager une base commune



Authentification depuis un annuaire

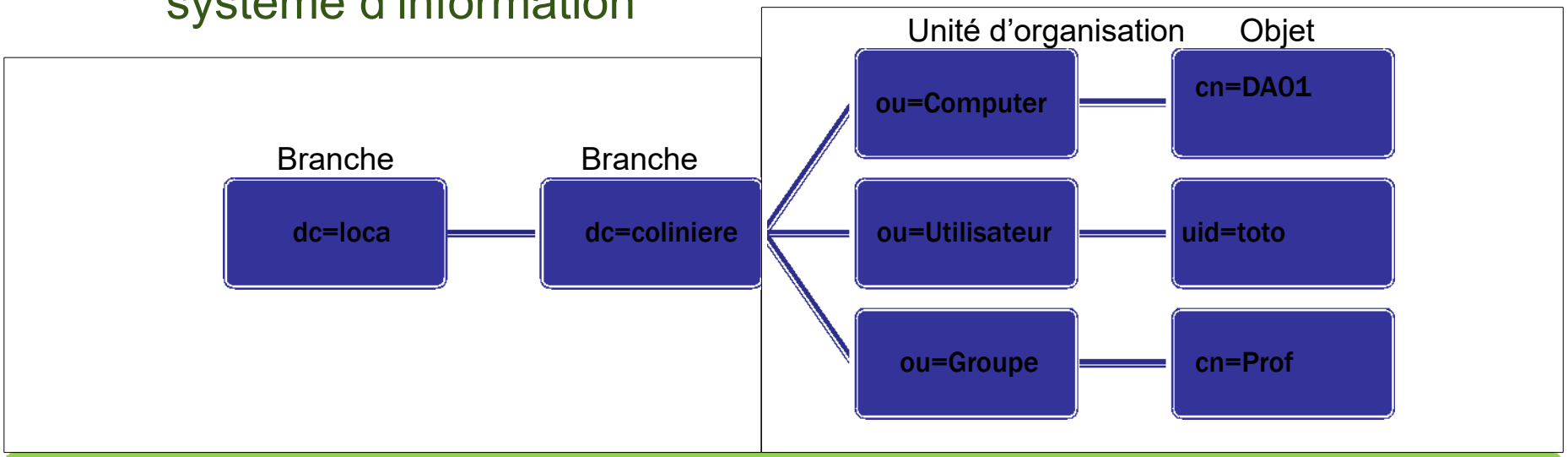
- Chaque entreprise ou entité bénéficie d'un annuaire centralisé
- Toutes les requêtes d'authentification passent par l'annuaire



G. Valet – genael.valet@diderot.org

Le serveur d'annuaire LDAP

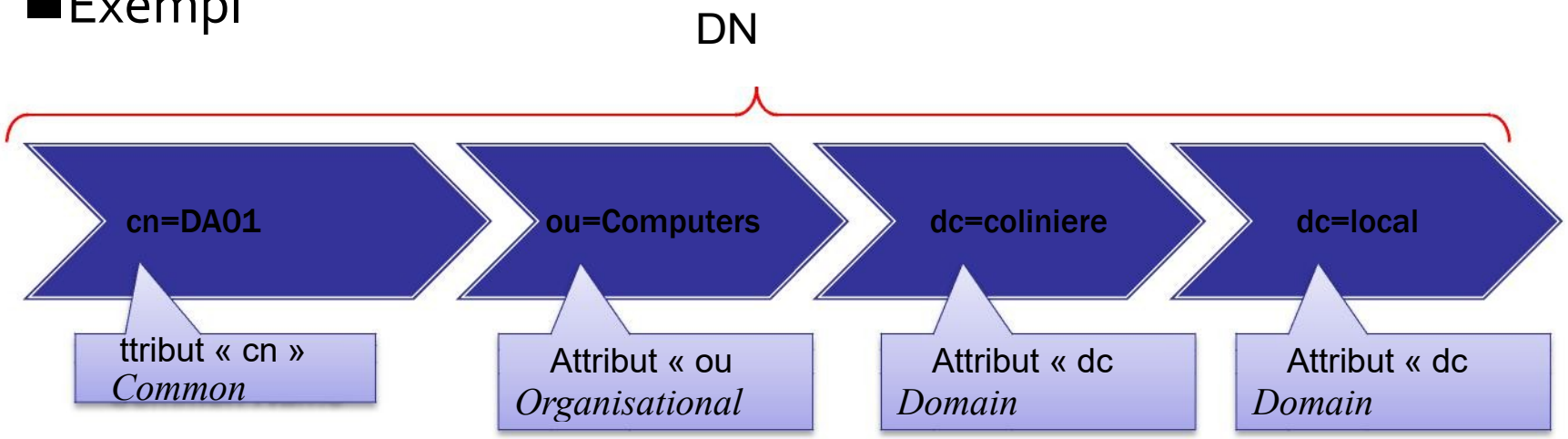
- LDAP : Lightweight Directory Access Protocol
  - Protocole réseau permettant l'accès à un annuaire
  - Repose sur TCP/IP
- Par extension, LDAP est devenu une norme pour les systèmes d'annuaire
  - Structure hiérarchique en arbre permettant d'organiser tout le système d'information



genael.valet@diderot.org

Le « Distinguished Name »

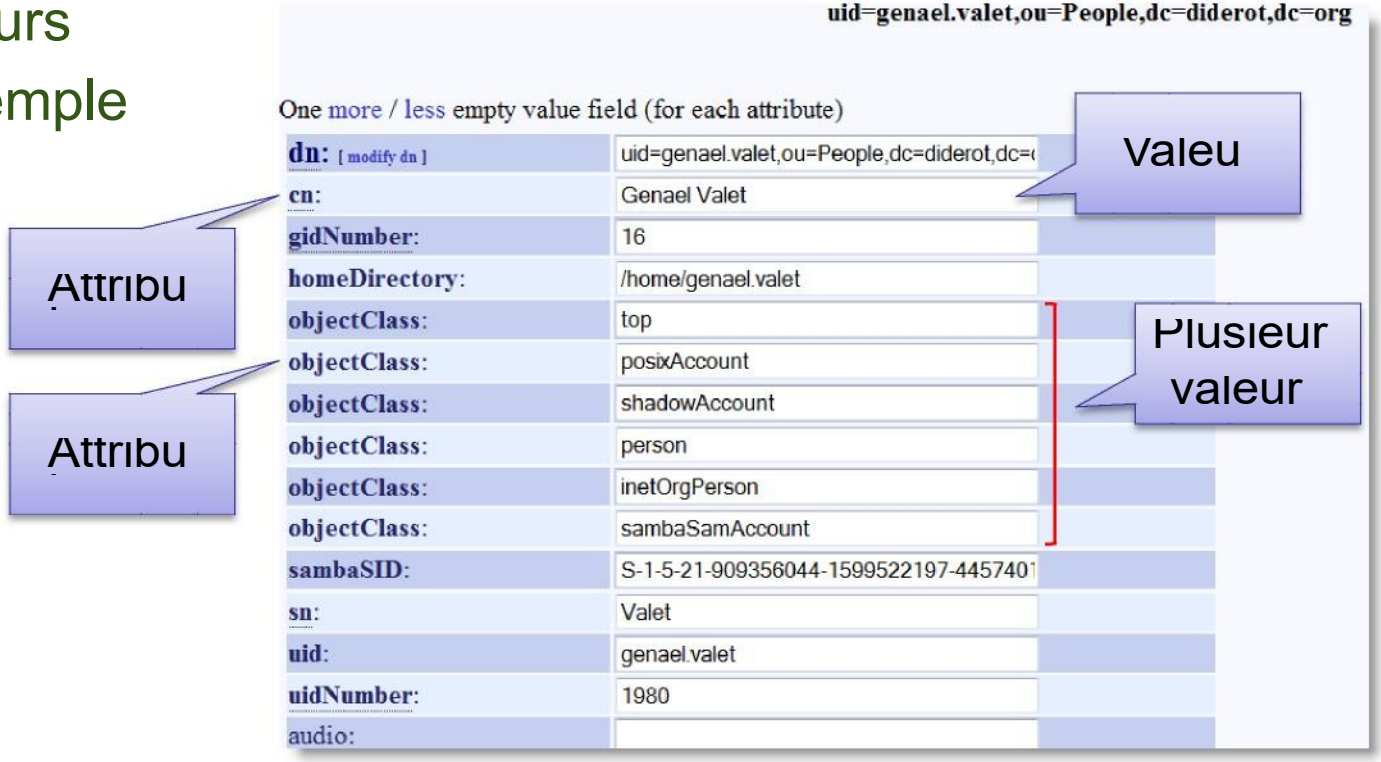
- Chaque entrée possède un identifiant unique
  - Distinguished Name (DN)
  - Exemple : « uid=toto, ou=Utilisateurs, dc=colinière, dc=local »
  - Il permet de situer l'entrée au sein du modèle d'organisation
- Cette entrée est unique et ne peut être dupliquée au sein du même annuaire
- Exempl



genael.valet@diderot.org

- Chaque entrée de l'annuaire est composée d'un ensemble d'attributs
  - Chaque attribut possède un nom, un type et une ou plusieurs valeurs

Exemple



G. Valet – genael.valet@diderot.org

Caractéristiques d'un Open LDAP annuaire

- Caractérisé par un ou plusieurs schémas LDAP
  - Un schéma définit la structure hiérarchique et les attributs disponibles
- Contient des index
  - Ils permettent d'effectuer des recherches plus rapides
- L'organisation d'un annuaire est hiérarchique
  - Il contient des entités ou des objets sous la forme de
    - Personnes (Les utilisateurs)
    - Ressources (Ordinateurs, imprimantes, ...)
    - Unités d'organisations (Compta, Marketing, ...)
- L'accès à distance est possible pour toute recherche
  - Possibilité de sécuriser l'accès à l'annuaire

L'annuaire peut être répliqué pour éviter toute perte de données

genael.valet@diderot.org

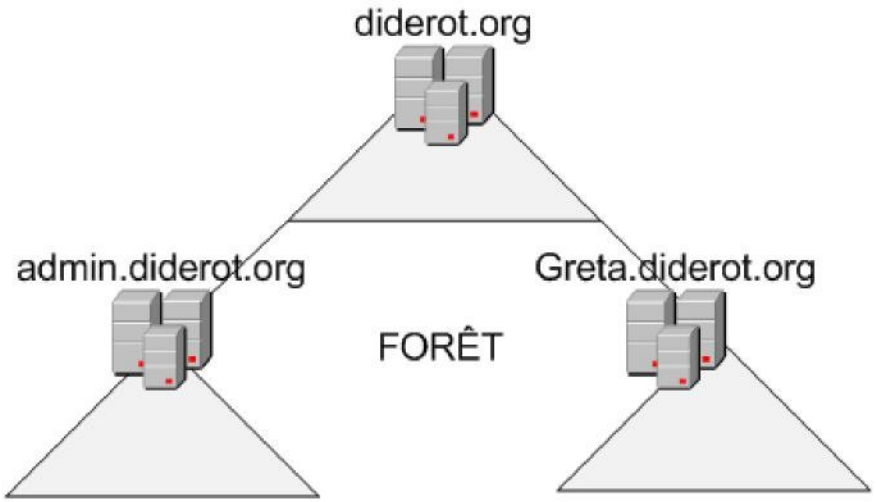
- Implémentation libre du protocole LDAP

  - Pour tout système d'exploitation : Linux, Windows, Max Osx, ...
  - Très utilisé dans le monde de l'Unix/Linux

- Le serveur OpenLdap est accessible depuis le réseau
  - Le serveur se nomme « slapd » (d comme démon)
  - En écoute sur le port 389
- Il peut servir à de multiples applications :
  - Authentification Unix/Linux ou authentification Windows (via SAMBA)
  - Authentification depuis toute application qui gère le protocole LDAP
    - Serveur Mail (Pour authentifier les adresses emails)
    - Serveur web (Pour authentifier les utilisateurs du web)
- http://www.openldap.org

Active Directory

- Microsoft a développé son propre modèle d'annuaire
  - Active directory est un service d'annuaire utilisé pour stocker des informations relatives aux ressources réseaux d'un domaine
- AD est utilisé pour l'infrastructure serveur de Microsoft
  - Windows 2003/2008 serveur
- Organisé en «forêts »



genael.valet@diderot.org

Structure AD (suite)

- Les forêts AD sont organisées autour des éléments suivants :

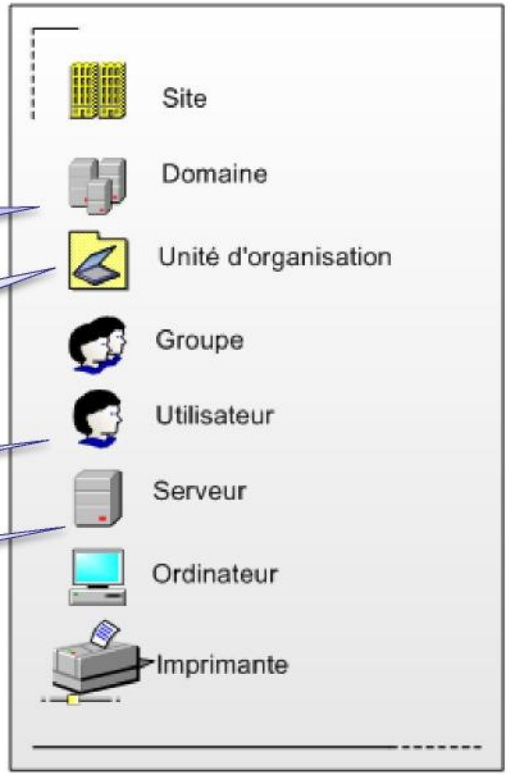
Possibilité d'organiser différents
Wan

Ensemble d'ordinateurs/d'utilisateurs partagent la même base de d'annuair

Objet conteneur utilisé pour organiser objets au sein d'un domaine
Service_compta, direction, ...)

Utilisateurs ou groupe

Serveur membre ou contrôleur de



Conclusion

- La gestion centralisée des utilisateurs permet :
  - Une gestion cohérente des utilisateurs sur un ensemble d'applications, de domaines, de parc informatique
- Cette gestion est réalisée avec un annuaire
  - L'annuaire centralise toutes les informations sur
    - Les utilisateurs et les groupes d'utilisateurs
    - Les machines
    - Tout autre ressource
- Le protocole standard est LDAP
- Les 2 approches de la notion d'annuaire sur la marché sont :
  - OpenLdap (+Samba ou autre) sous Unix/Linux
  - Active Directory de Microsoft

genael.valet@diderot.org