Administration Infrastructure

Séance 8

Sommaire

- Questions sur la séance labos
- Exercice Découpe LAN Correction
- Chapitre 8 : Annuaires et Authentification
- Exercice AD

Questions sur la séance labos ?

Annuaires et Authentification

- LDAP
  - Lightweight Directory Access Protocol
  - Standard pour interroger et de modifier un annuaire
  - Standard pour l’authentification
  - Très présent en entreprise via la solution M$: Active Directory

Annuaires et Authentification

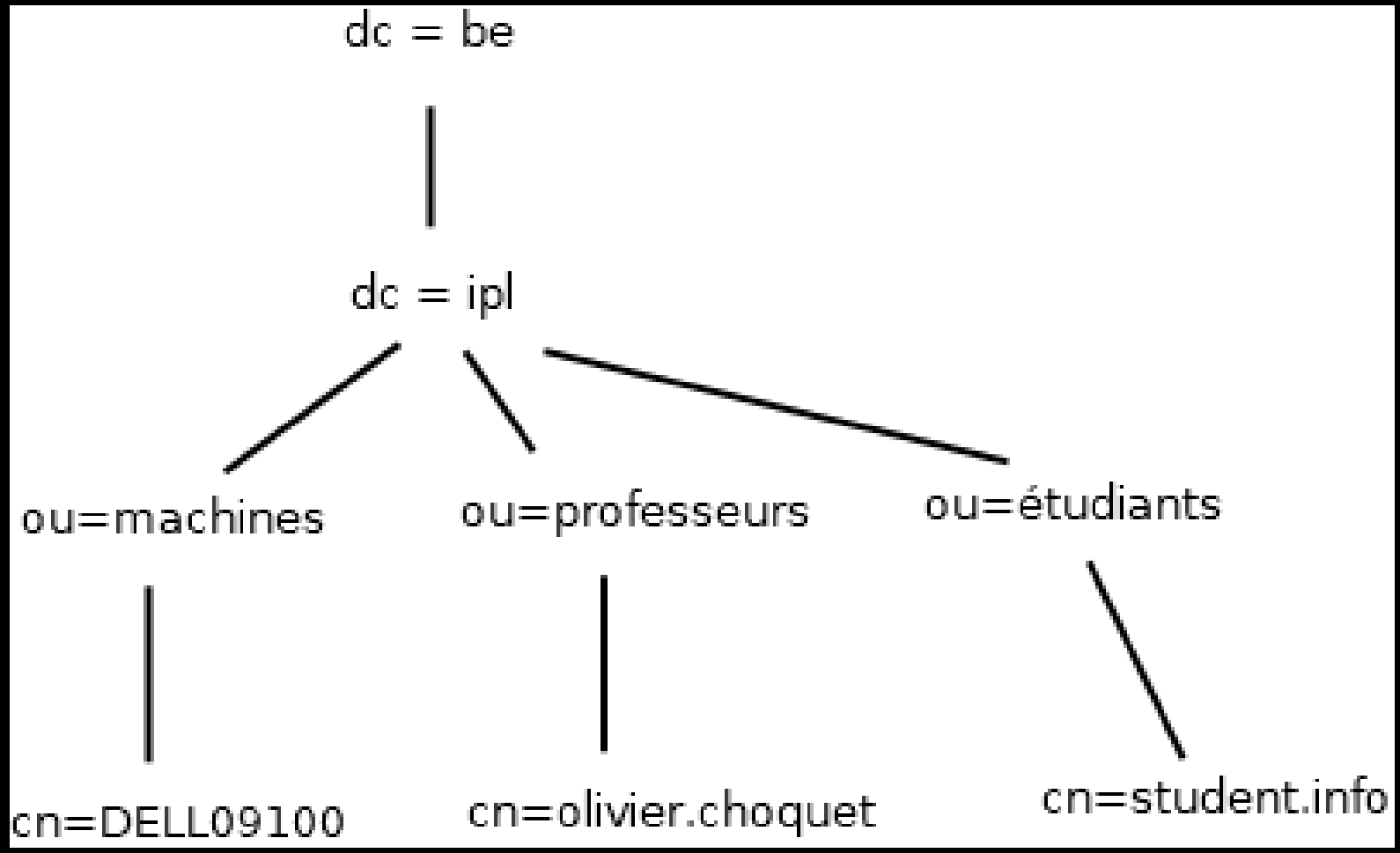
- LDAP
  - un protocole: comment sont échangées les données
  - un modèle de nommage: comment sont nommées les entrées dans l'annuaire
  - un modèle fonctionnel: quelles sont les méthodes pour accéder aux données
  - un modèle d'information: nature et description des données
  - un modèle de sécurité: description de la sécurité des données (quel chiffrement …)
  - Réplication: comment répliquer des données entre serveurs LDAP pour se prémunir des pannes? Ce point n'est pas encore standardisé.

Annuaires et Authentification

- Modèle de nommage – structure en arbre
  - **DC : Domain Component. Racine de l’arbre**
  - **DN : Distinguished Name. Chemin complet vers un élément (Les DN sont uniques)**
  - **OU : Organizational Unit. Division de l’entreprise rassemblant des CN.**
  - **CN : Common Name. Nom d’un élément**

Annuaires et Authentification

Quel est l'intérêt d'avoir un arbre pour un système d'authentification ?



Connaissez-vous un protocole réseau qui utilise lui aussi une structure hiérarchique (en arbre) ?

Si je dois authentifié un utilisateur dans mon programme, quelle est la première opération ?

https://marketsplash.com/tutorials/node-js/node-js-ldap-authentication/

Annuaires et Authentification

- Modèle fonctionnel
  - **Bind : s'authentifier auprès du serveur LDAP. Ceci est nécessaire avant de demander au serveur une opération au serveur**
  - **Add/Modify/Delete : mise à jour de l'annuaire.**
  - **Search : «search» permettra de rechercher un élément ou plusieurs éléments dans l'annuaire en précisant une base, une portée et éventuellement des filtres (voir ci-dessous).**
  - **Compare : vérifie qu'un élément contient ou non un attribut**
  - **Unbind : se déconnecter du serveur**

Annuaires et Authentification

- Modèle fonctionnel
  - Base : uniquement la base
  - One : fils directs
  - Sub : récursif sur toute l'arborescence
- Les filtres courants
  - = , ~= , >= , : , & , !
- Exemple query LDAP
  - &(&(objectclass=prof)(cn=A*)(!(sexe=M)))
  - ldap://localhost:389/ou=professeurs,dc=ipl,dc=be?uid?sub

Annuaires et Authentification

- Modèle d'informations
  - **Entrée: composé d’attributs, possède un type (classe d’objets)**
  - **Schéma: définition des attributs possibles et classes d’objets**
  - **DN (Distinguished Name)**

Annuaires et Authentification

- Modèle d'informations - Exemple

```
dn: cn=olivier.choquet, ou=profs,
dc=ipl,dc=be\
objectClass: user\
cn: olivier.choquet\
mail: olivier.choquet@vinci.be\
bureau: A050\
```

Annuaires et Authentification

- Modèle de sécurité
  - SSL-TLS
- Modèle de réplication
  - Redondance
  - LDIF : **LDAP Data Interchange Format**
    - **Echange à froid d'informations entre serveurs LDAP**

Annuaire et Authentification

8.7 LDAP vs SGBD

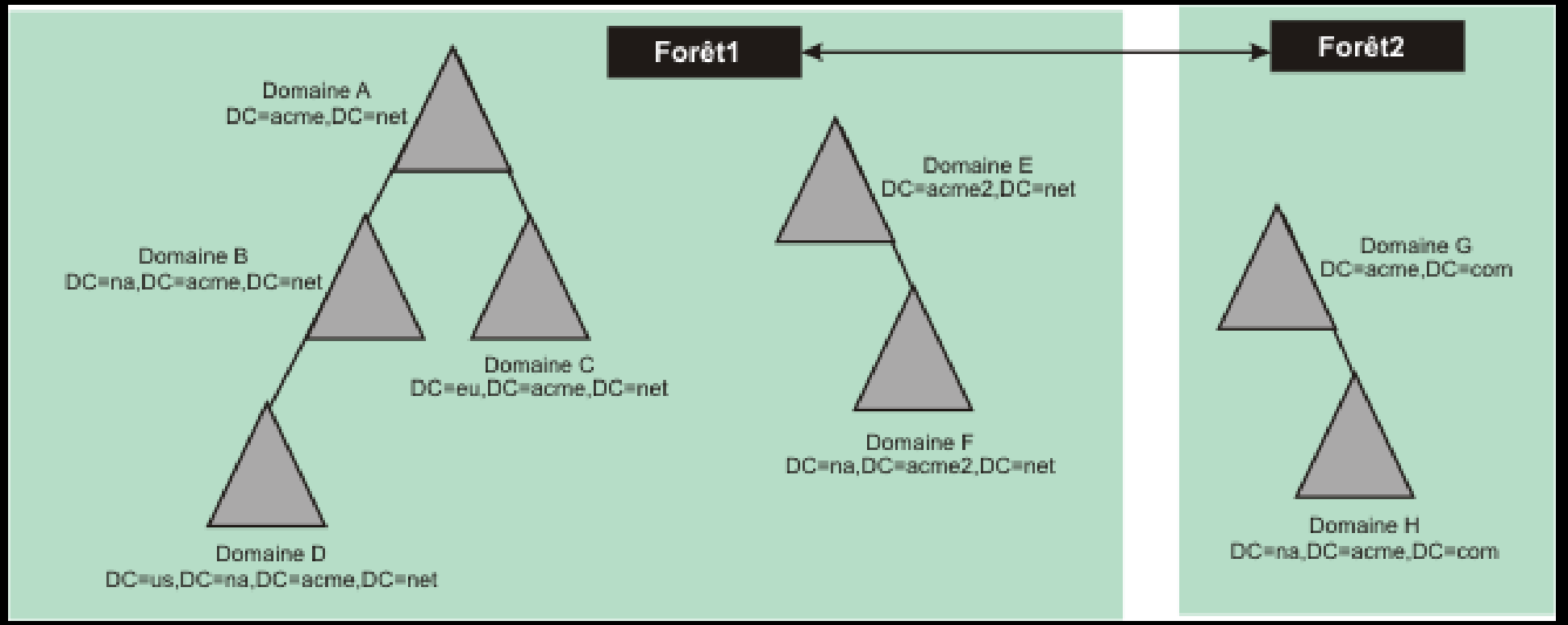
LDAP	SGBD
Optimiser pour la lecture, faible en écriture	Optimiser pour les lectures et écritures
Isolation pas garantie	**Support Transaction (ACID)**
Réplication aisée	Réplication plus complexe
Attribut multi-valeurs	/
Query LDAP	**Query SQL**
Modèle de données défini, **mais extensible facilement**	**Définition du modèle par le développeur, extensible mais difficile**

Annuaires et Authentification

- Active Directory (AD)
  - Implémentation +/- LDAP de M$
  - Centralisation gestion utilisateurs/machines
    - Authentification des utilisateurs
    - Parc de machines (domaine)
    - GPO (Group Policy Object)
      - application de stratégies (sécuritaires ou pas) sur les machines ou utilisateurs

Annuaires et Authentification

- Active Directory (AD)



Annuaires et Authentification

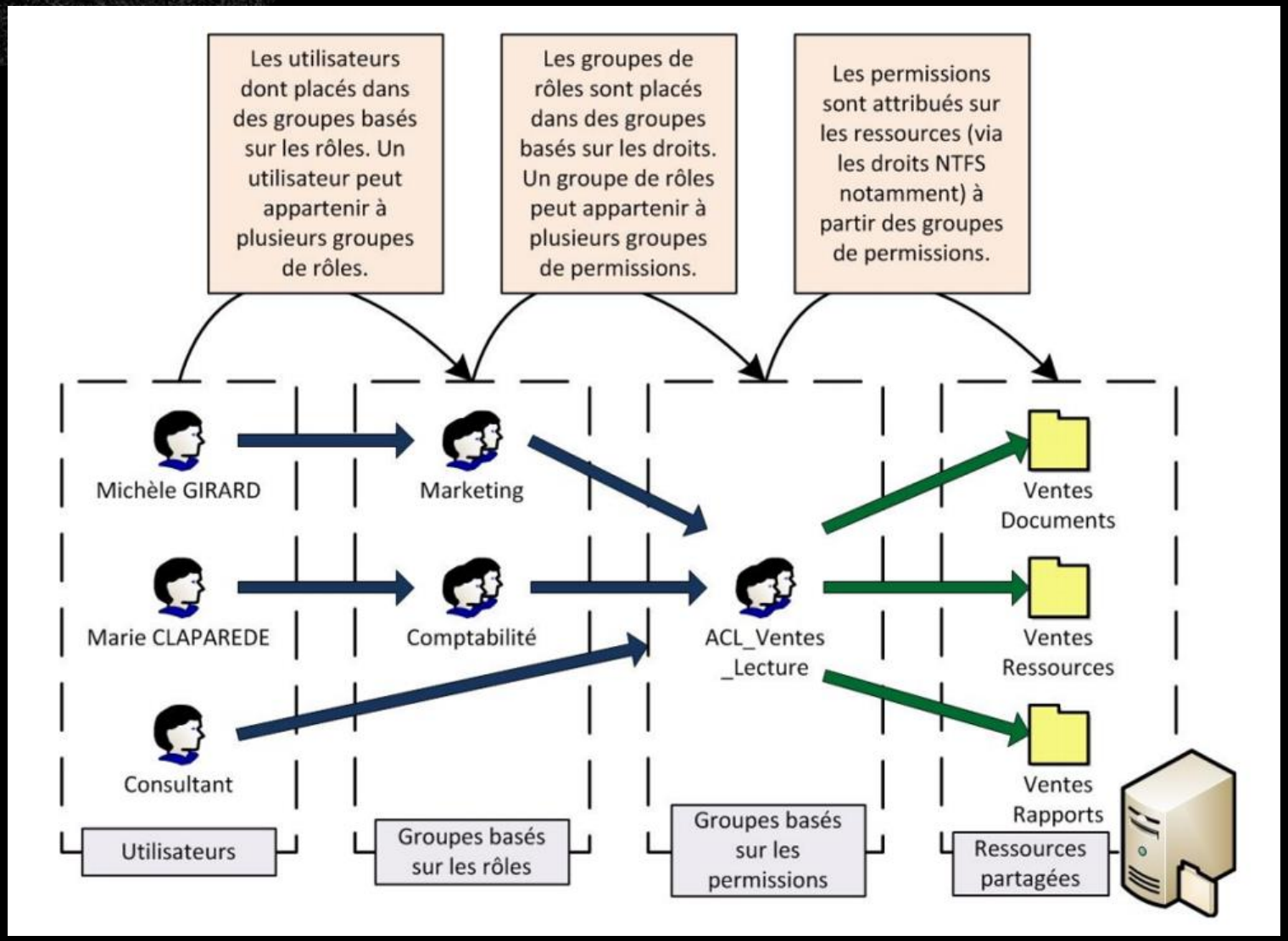
- Active Directory (AD)
  - Création pour l'entreprise – concepts de base
    - Forêt
    - Arbre
    - Domaine
    - **Un serveur hébergeant un Active Directory est appelé contrôleur de domaine. Il est conseillé d’avoir au minimum 2 contrôleurs de domaine par Active Directory pour se prémunir des pannes.**

Annuaires et Authentification

- Active Directory (AD)
  - Objets dans l'AD
    - Utilisateurs – Groupes de sécurité/distribution
      - Permissions NTFS / Permissions Partage Réseau
    - Unité d'organisation (UO/OU)
      - GPO

Annuaires et Authentification

- Active Directory (AD) - Permissions
- **Account → Global → (Universel) → Domain Local → Permission**



Annuaire et Authentification

- Permission les plus communes:
  - R (Read), W (Write) , RE (Read and Execution) ,M (Modify) , FC (Full Control)
  - Les permissions sont héritées
  - Démo

Annuaire et Authentification

- GPO