Gestion réseau des identités

Module Admin Sys Réseau – S26E03

Philippe Latu / Université de Toulouse
inetdoc.net

Comment gérer la sécurisation et la synchronisation des identités ?

Garantir une expérience utilisateur fluide

Respecter les réglementations sur la protection des données

Le plan

- Connecter un utilisateur
- Gérer la connexion sur un système Linux
- Gérer la mutualisation des identités
- Décrire les fonctions d’un annuaire LDAP

Connecter un utilisateur

Pourquoi le mot de passe a-t-il rompu avec la reconnaissance faciale (*face ID)* ?

Parce que leur relation semblait trop superficielle.

Sécuriser les connexions

- *What do I know ?*
  - Mot de passe
- *What do I have ?*
  - Smartphone, jeton, FIDO2, ...
- *What am I ?*
  - Empreinte digitale, reconnaissance faciale, ...

Évolution des méthodes d’authentification

Caractéristique	Authentification traditionnelle	Authentification moderne	Critère de choix
Sécurité	Mots de passe + SMS/TOTP	FIDO2 + IA comportementale	Résistance aux attaques
Performance	Latence 500-2000ms	Latence <100ms	Temps de connexion
Expérience utilisateur	Complexe, mémorisation	Transparente, biométrie	Facilité d’usage
Coût de gestion	Élevé (support, reset)	Faible (automatisé)	TCO et support
Implémentation	Simple	Modérée pour FIDO	Facilité de déploiement

Décrire le processus de connexion

- Un outil de connexion
  - Graphique, `login`, `ssh`, MFA, …
- Plusieurs étapes
  - **Rassembler** les informations sur l'utilisateur
  - **Authentifier** l'utilisateur
  - **Lancer les traitements** à l'ouverture de session

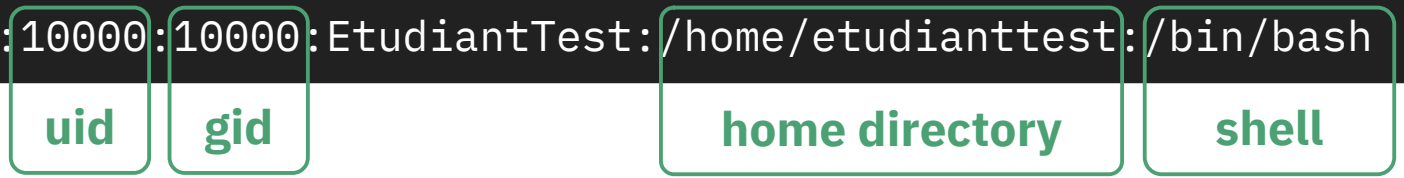
Comment l'outil de connexion ...

- Connaît-il tous les utilisateurs du système ?
  - Annuaires
- Connaît-il les propriétés ou attributs d’un utilisateur ?
  - Magasins d’identités
- Assure-t-il l’authentification ?
  - PAM (*Pluggable Authentication Modules*)

Tout utilisateur du système doit avoir...

- Un identifiant de propriétaire unique → uid
- Un identifiant de groupe unique → gid
- Un répertoire utilisateur → home
- Un Shell → Bash, Zsh, ...

```
$ getent passwd etudianttest
etudianttest:x:10000:10000:EtudiantTest:/home/etudianttest:/bin/bash
```



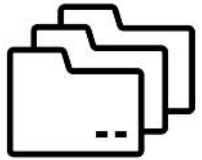
AAA : Authentication, Authorization, Accounting

- *Authentication* (Authentification)
  - Vérifie l'identité de l'utilisateur
  - Répond à la question : "Qui êtes-vous ?"
- *Authorization* (Autorisation)
  - Détermine les droits d'accès de l'utilisateur
  - Répond à la question : "Que pouvez-vous faire ?"
- *Accounting* (Comptabilité)
  - Enregistre les actions de l'utilisateur
  - Répond à la question : "Qu'avez-vous fait ?"

Connecter un utilisateur Unix/Linux

Représenter l'utilisateur Unix → Tout est fichier !

- Utilisateurs → `/etc/passwd`
- Groupes → `/etc/group`
- Noms d'hôtes → `/etc/hosts`



Mutualiser les informations entre hôtes

- Utilisateurs et groupes dans un annuaire LDAP
- Noms d'hôtes dans un service DNS

Globaliser dans les nuages

- Distribuer et découvrir les services dynamiquement
- *Identity & Access Management* → IAM

Mutualiser les informations utilisateur → API

- Les applications ont besoin de …
  - Transparence → accéder à tous les magasins
  - Modularité → agréger des sources d'identités hétérogènes
  - Indépendance → développer un code indépendant des sources
- Les représentations des données évoluent
  - Situation initiale
    - Un protocole par service avec mécanisme de réplication propre → LDAP, DNS
    - Un référentiel et une syntaxe propre → LDIF, RR
  - Évolution actuelle
    - Couples clé-valeur → YAML

Quiz connecter un utilisateur – question 1

Quel est le but principal de l'authentification dans le processus AAA ?

a) Déterminer les droits d'accès de l'utilisateur

b) Enregistrer les actions de l'utilisateur

c) Vérifier l'identité de l'utilisateur

Quiz connecter un utilisateur – question 2

Où sont traditionnellement stockées les informations sur les utilisateurs dans un système Unix/Linux ?

a) /etc/users

b) /etc/passwd

c) /etc/accounts

Quiz connecter un utilisateur – question 3

Quelle solution est souvent utilisée pour mutualiser les informations sur les utilisateurs et les groupes entre plusieurs hôtes ?

a) DNS

b) IAM

c) LDAP

Quiz connecter un utilisateur – question 4

Quel acronyme désigne la gestion des identités et des accès dans un environnement cloud ?

a) AAA

b) IAM

c) MFA

Quiz connecter un utilisateur – question 5

Comment la représentation des données d'identité évolue-t-elle actuellement ?

a) Utilisation exclusive de fichiers XML

b) Retour aux fichiers à plats

c) Utilisation de couples clé-valeur (YAML)

Gérer la connexion sur un système Linux

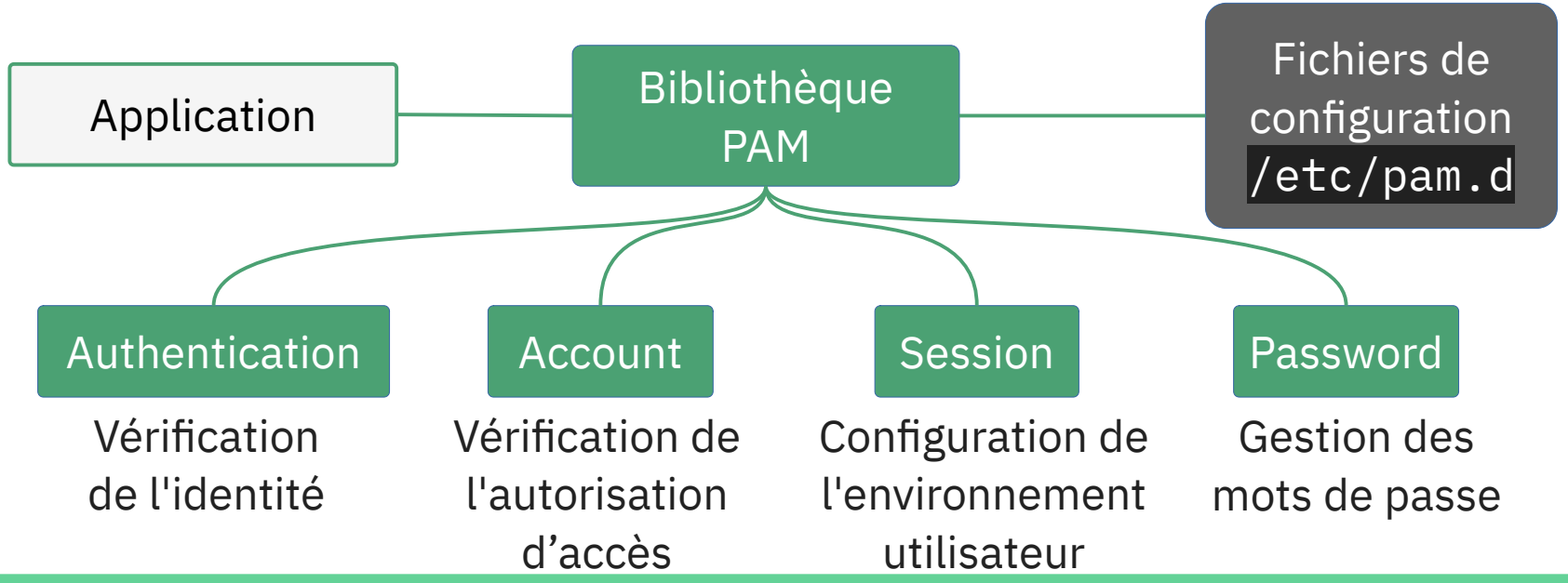
Même à l’échelle d’un unique système,
on a besoin d’une API … système

Rassembler les informations

- *Name Service Switch* (NSS)
  - Fournit une API standard pour accéder aux bases de données de configuration du système
  - Gère la résolution des noms d'utilisateurs, groupes, hôtes, etc.
  - Gère la mise en cache de façon sécurisée
  - Extensible → un module pour chaque type de source
- Configuration : `/etc/nsswitch.conf`
  - Fichiers locaux, LDAP, DNS, Active Directory, Bases de données

Authentifier l’utilisateur

- *Pluggable Authentication Modules* (PAM)
  - Fournit un Framework modulaire pour l'authentification des utilisateurs



Authentifier l’utilisateur

- La bibliothèque PAM ...
  - Standardise l'interface d'authentification pour les applications
  - Renforce la sécurité en combinant différentes méthodes d'authentification
  - Offre une architecture modulaire permettant d'utiliser différents modules d'authentification
    - pam_unix
    - pam_krb5
    - pam_ldap
    - pam_google_authenticator

Gérer la mutualisation des identités

L’intégration est une nécessité → les besoins

- On doit pouvoir enregistrer un client sans …
  - Connaître les détails de fonctionnement de l’annuaire
  - Maîtriser plusieurs technologies complexes
  - Rechercher des fichiers de configuration éparpillés
  - Connaître toutes les options de configuration

L’intégration est une nécessité → la réalité

- Pour gérer les comptes utilisateurs en volume
  - La distribution de fichiers atteint vite ses limites
    - Problèmes de synchronisation et de conservation
  - Il faut centraliser les informations sur les utilisateurs
    - Non seulement les identités, mais aussi les politiques …
  - Les standards de l’industrie sont multiples
    - Unix/Linux → LDAP, LDAP + Kerberos, NIS
    - Windows → Active Directory (LDAP + Kerberos)
- LDAP reste le magasin d'identité le plus courant

Utiliser LDAP sur un hôte Linux → état actuel

- Rassembler les informations → NSS
  - Paquet → `libnss-ldapd`
  - Fichier → `/etc/nslcd.conf`
- Authentifier l'utilisateur
  - Paquet → `libpam-ldapd`
  - Fichier → `/etc/ldap.conf`
  - Module `pam_ldap` → `/etc/pam.d/common-auth`
- Ajuster la configuration
  - Commande → `dpkg-reconfigure slapd`

Utiliser LDAP sur un hôte Linux → les limites

L’évolution actuelle impose de nouveaux défis

Une série de questions → Comment ?

- Connecter avec des comptes de différentes organisations depuis un seul client ?
- Assurer une correspondance « 1 à 1 » entre les identités et l'authentification ?
- Gérer les accès intermittents aux services ?
  - Itinérance
  - VPN
  - Migrations

Utiliser plusieurs magasins sur un hôte Linux

Une réponse aux nouveaux défis : sssd

SSSD → *System Security Services Daemon*

- Centralise et sécurise les accès à différents magasins
  - LDAP et/ou AD
- Gère la mise en cache et tolère les accès intermittents
- Améliore la cohérence du processus d'authentification
- Fournit un service SSO (*Single Sign-On*)
- Utilise un fichier de configuration unique

OpenID Connect (OIDC) → Authentification moderne

Protocole d'authentification basé sur OAuth 2.0

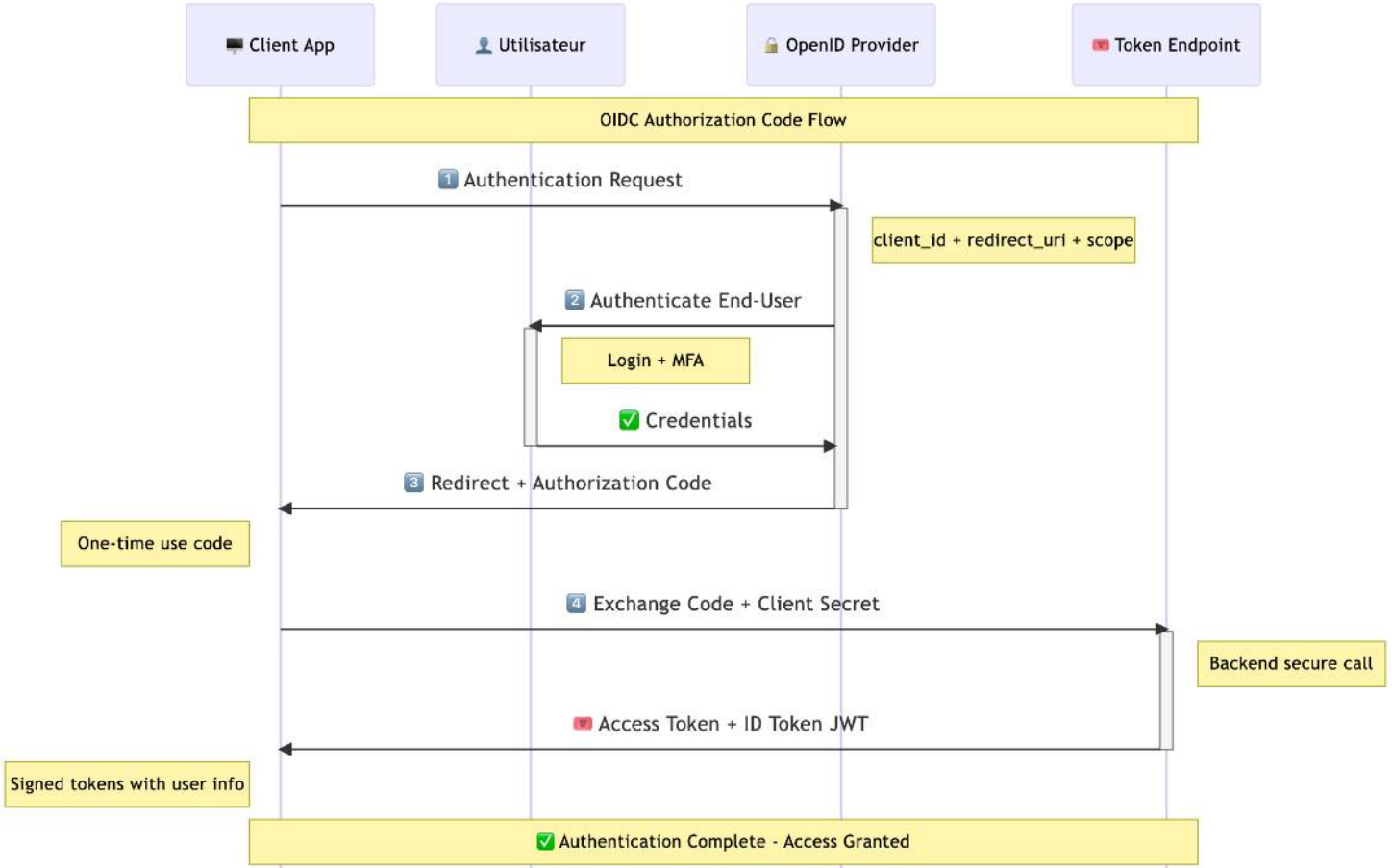
- Couche d'authentification au-dessus d'OAuth 2.0
- Standard industriel pour SSO et fédération d'identités
- Token JWT signé avec informations utilisateur
- Compatible cloud-native et applications mobiles
- OAuth 2.0 (Autorisation) + OIDC (Authentification) = Solution complète

OIDC Authorization Code Flow → Processus sécurisé

Flux d'authentification en quatre étapes

- 1. Redirection → Fournisseur d'identité (IdP)
- 2. Authentification utilisateur → Code d'autorisation
- 3. Échange code → Token d'accès + ID Token JWT
- 4. Validation → Accès sécurisé aux ressources
- Support PKCE pour applications mobiles/SPA
  (PKCE : *Proof Key for Code Exchange*)

OIDC Authorization Code Flow → Processus sécurisé



Décrire les fonctions d’un annuaire LDAP

« La complexité et la puissance des annuaires LDAP viennent du fait qu'il y a des tas d'attributs et des tas de classes d'objets généreusement dispersés dans des schémas apparemment aléatoires (et invariablement inutiles). »

Définir un annuaire LDAP

Lightweight Directory Access ***Protocol*** – RFC 4511

- C’est une forme de base de données dédiée :
  - Aux lectures
  - Aux recherches multi-critères
- L’objet d’un annuaire est de :
  - Maintenir une très grande quantité de données
  - Assurer la cohérence à l’aide de schémas (référentiels)
  - Contrôler l’accès à l’information avec des ACLs

Définir un annuaire LDAP

Les données sont stockées …

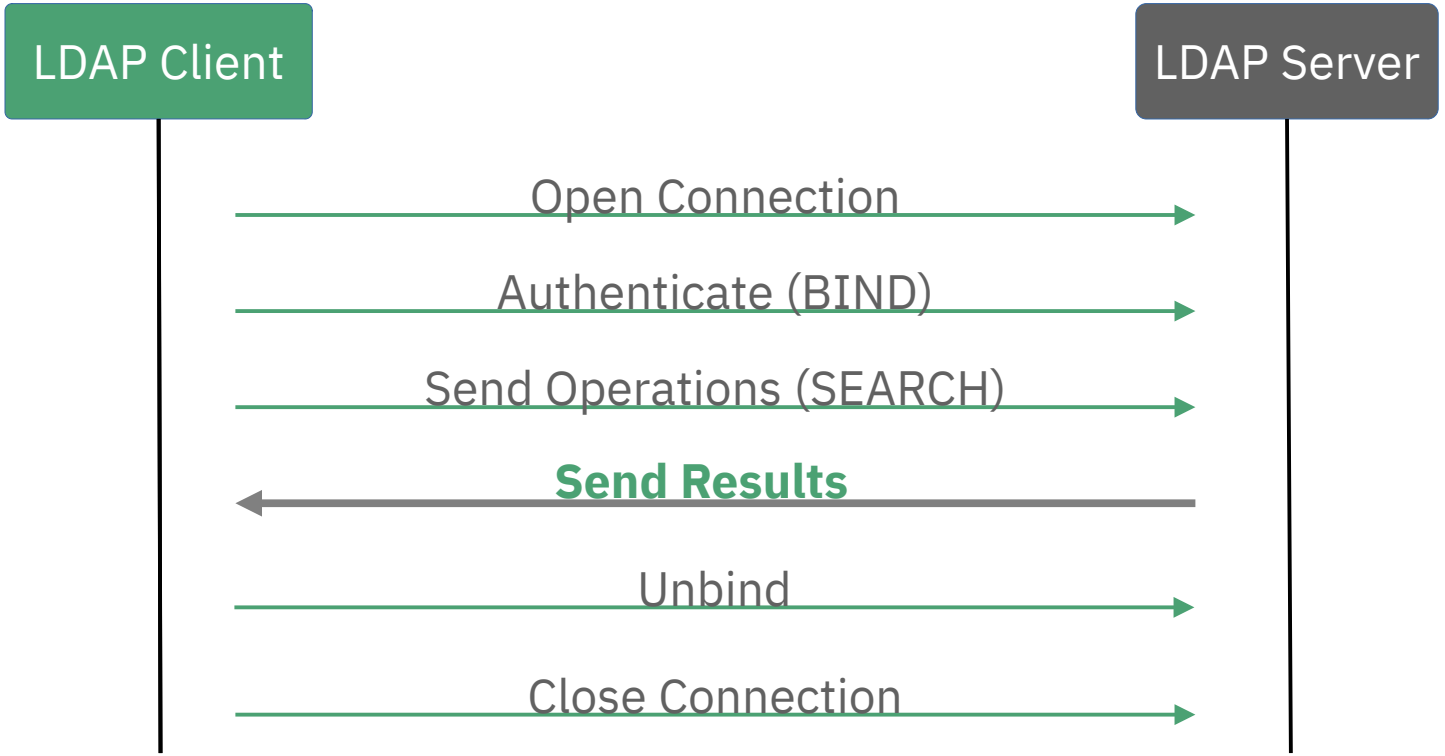
- Sous forme d’attributs
  - Une paire clé-valeur décrit une entité
- Sans restriction sur leur nature
  - Informations personnelles : authentification, contact, photos
  - Organisationnelles : rôles, fonctions
- Sans relation de dépendance entre objets
  - Aucune connaissance sur la structure de l’annuaire n’est requise

Définir un annuaire LDAP

Les composants LDAP

- Un protocole réseau
  - Réplications et synchronisations natives
- Des modèles
  - Informations → types de données
  - Nommage → référentiel des attributs
  - Fonctionnel → syntaxe des requêtes
  - Sécurité → contrôle d'accès
- API → Python, Java, PHP, etc.

Décrire le protocole LDAP



Décrire le modèle d’informations

Les éléments du modèle d’informations LDAP (1/2)

- Une entrée
  - Contient les informations sur un objet
- Un attribut
  - Décrit les caractéristiques d’un objet
- Une classe d’objets
  - Spécifie les attributs obligatoires et facultatifs qui peuvent être associés à une entrée de cette classe

Décrire le modèle d’informations

Les éléments du modèle d’informations LDAP (2/2)

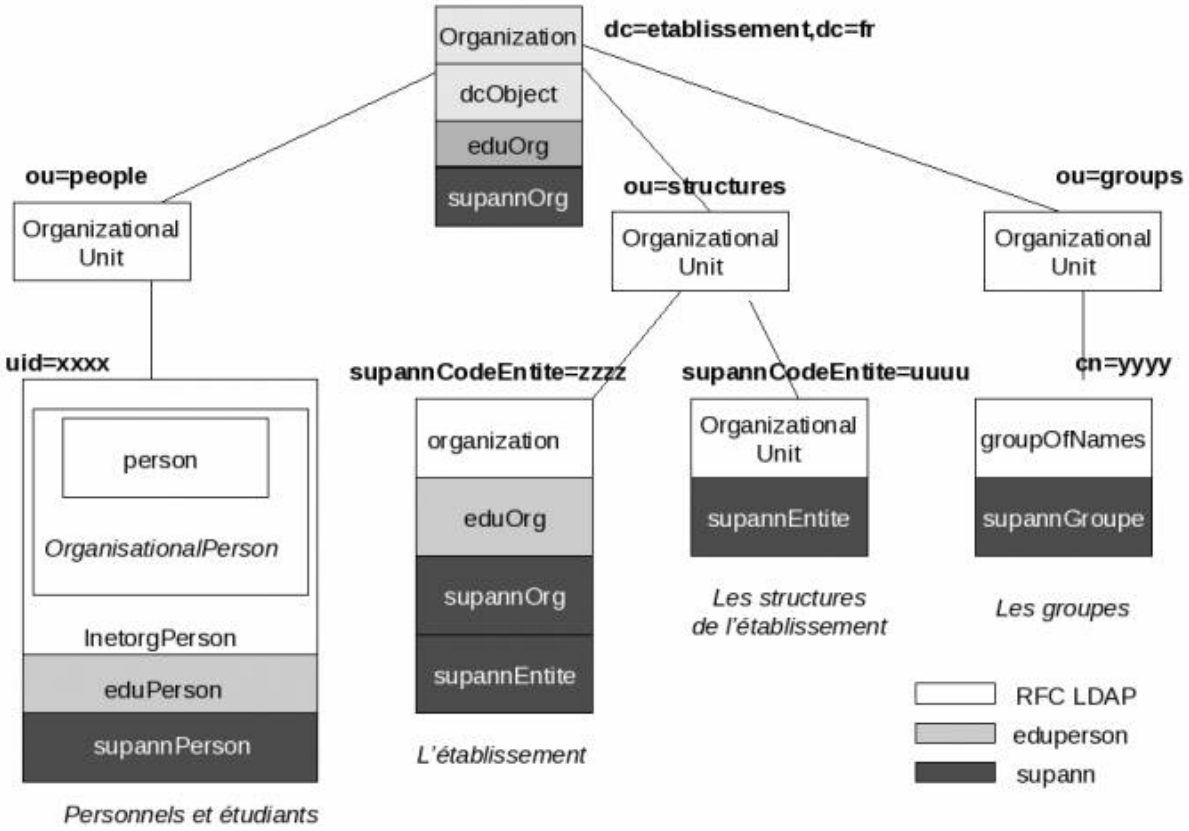
- Un schéma (référentiel)
  - Définit l'ensemble des objets, des attributs et la syntaxe d’un annuaire LDAP
- La syntaxe et le type d’un attribut
  - Définit un identifiant d’objet (OID) avec son type de données LDAP OID Reference Guide
- Des règles de correspondance
  - Liste les comparaisons possibles

Décrire le modèle de nommage

Arborescence d'informations hiérarchique appelée *Directory Information Tree* (DIT)

- Un objet nommé avec un *Distinguished Name* (DN)
  - Exemple : `uid=leia,ou=people,dc=lab,dc=local`
- Une structure en branches et nœuds
  - Chaque nœud représente un objet
  - Exemple : Annuaires pour l'Enseignement Supérieur (Supann)
- Autre dénomination de la structure → conteneurs et feuilles
  - Conteneur = nœud / feuille = données de l'entrée

Décrire le modèle de nommage



Décrire la représentation des données

Format standard : *LDAP Data Interchange Format* (LDIF)

- Un jeu d'opérations
  - Extraire
  - Importer
  - Créer
  - Ajouter
  - Modifier

```
# Anakin Skywalker
dn: uid=anakin,ou=people,dc=lab,dc=local
objectClass: inetOrgPerson
objectClass: shadowAccount
objectClass: posixAccount
cn: Anakin
sn: Anakin Skywalker
uid: anakin
uidNumber: 10001
gidNumber: 10001
loginShell: /bin/bash
homeDirectory: /ahome/anakin
userPassword: {SSHA}
hFGouu+ytfnH0qPy7y9G0L0Rb6R6slZ4
gecos: Anakin Skywalker
```

Quiz gérer les identités – question 1

Quel est l'objectif principal d'un annuaire LDAP ?

a) Faciliter la création de nouvelles bases de données

b) Maintenir une très grande quantité de données et assurer la cohérence à l'aide de schémas

c) Réduire le nombre de requêtes réseau

Quiz gérer les identités – question 2

Quel est le principal bénéfice apporté par SSSD (*System Security Services Daemon*) ?

a) Fournir un accès direct aux bases de données

b) Centraliser et sécuriser les accès à différents magasins

c) Servir de pare-feu pour les connexions réseau

Quiz gérer les identités – question 3

Quel type de structure est utilisé pour organiser les informations dans un annuaire LDAP ?

a) Arborescence d'informations hiérarchique appelée Directory Information Tree (DIT)

b) Base de données relationnelle

c) Liste linéaire de données

Quiz gérer les identités – question 4

Quel paquet est utilisé pour rassembler les informations sur un hôte Linux utilisant LDAP ?

a) libpam-ldapd

b) slapd

c) libnss-ldapd

Quiz gérer les identités – question 5

Quel est le format standard pour représenter les données LDAP ?

a) XML

b) JSON

c) LDIF (LDAP Data Interchange Format)

Pour conclure

On reprend...

Les concepts clés

- Objectifs de la gestion des identités et des accès (IAM)
  - Sécuriser et synchroniser les identités
    - Expérience utilisateur et conformité aux réglementations
    - AAA → vérifier l'identité, déterminer les droits d'accès et enregistrer les actions
  - Évolution des méthodes d'authentification
    - Traditionnelle → Mots de passe + SMS / TOTP (latence élevée)
    - Moderne → FIDO2 + IA comportementale (<100ms)
    - Standard industriel → OpenID Connect (OIDC)
  - Intégrer des systèmes hétérogènes
    - API pour le développement
    - Protocoles standards → LDAP, DNS, Kerberos
- Technologies et Protocoles
  - Legacy → LDAP (centralise identités, schémas, ACLs)
  - Moderne → OAuth 2.0 + OIDC (cloud-native, JWT, SSO)

Les perspectives et défis

- Évolution des Systèmes
  - Transition vers architectures cloud-native et Zero Trust
  - OIDC remplace progressivement LDAP pour nouvelles applications
  - Formats déclaratifs (YAML, JWT) vs syntaxe RFC (LDIF)
- Solutions hybrides actuelles
  - SSSD → Pont entre systèmes historiques et modernes
  - Fédération d'identités → Interopérabilité multi-domaines
- Défis technologiques actuels
  - Authentification sans mot de passe généralisée
  - Accès intermittents et services dynamiques
  - Intégration IA pour analyse comportementale
  - Conformité réglementaire (GDPR, NIS2) dès la conception