Microsoft

Active Directory

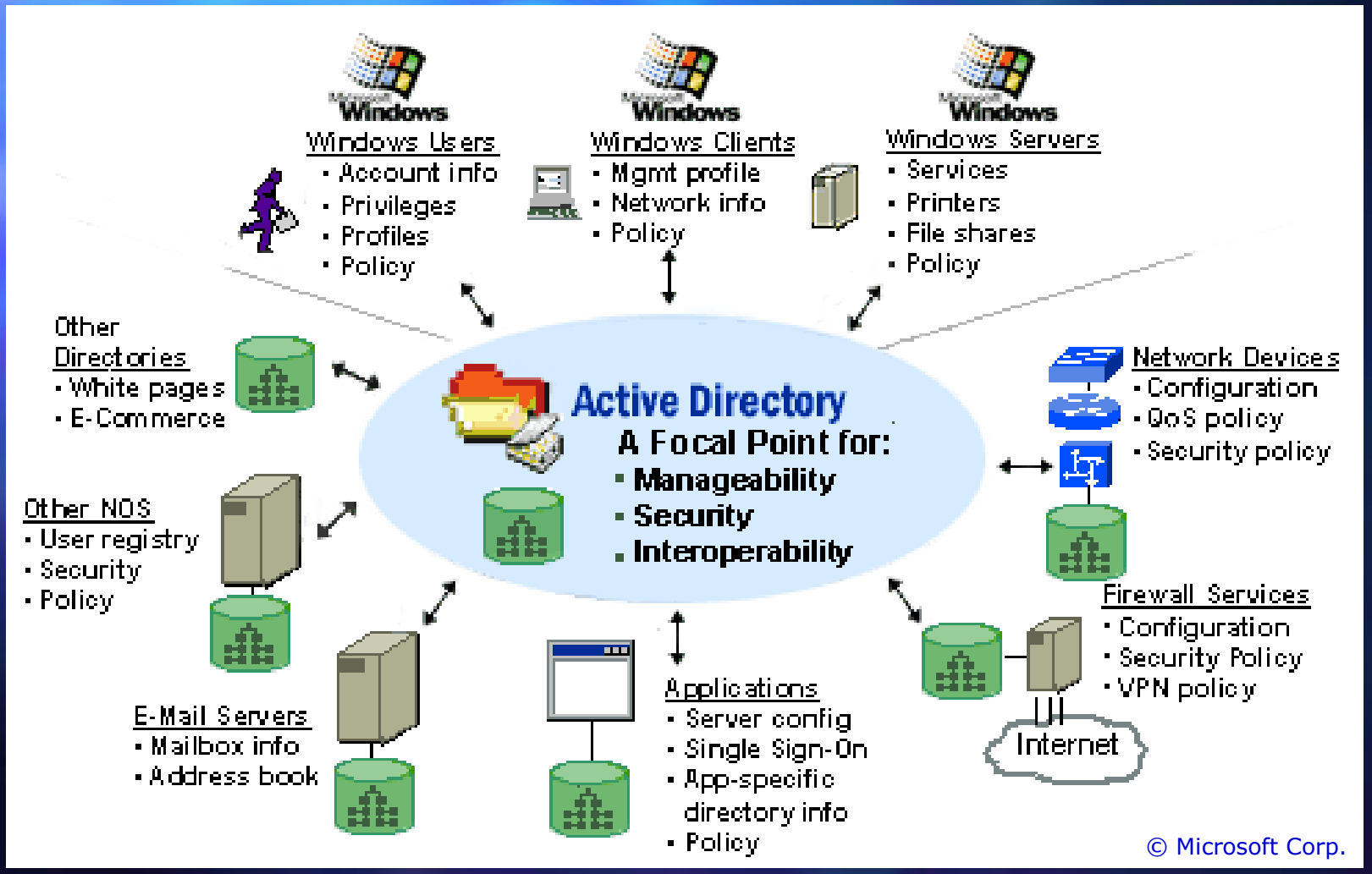
Structure et usage

® Michel CHABANNE – Ecole Polytechnique/DSI/RVDS – Octobre 2005

Active Directory ?

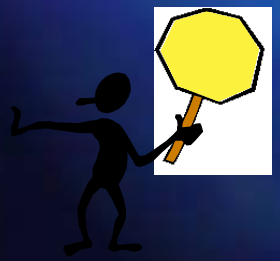
- Une implémentation de service LDAP pour une utilisation dans les environnements Windows
- Présenté en 1996, implémenté pour la première fois dans Windows 2000.
- Remanié pour Windows Server 2003.

Que faire avec AD ?



Infrastructure

- AD utilise extensivement le système DNS, et notamment les SRV
- AD utilise Kerberos v5 (en tout cas l'implémentation de Microsoft…)
- AD supprime totalement l'usage de NetBIOS/NetBEUI/WINS
  - Attention à vos applications !



Structure

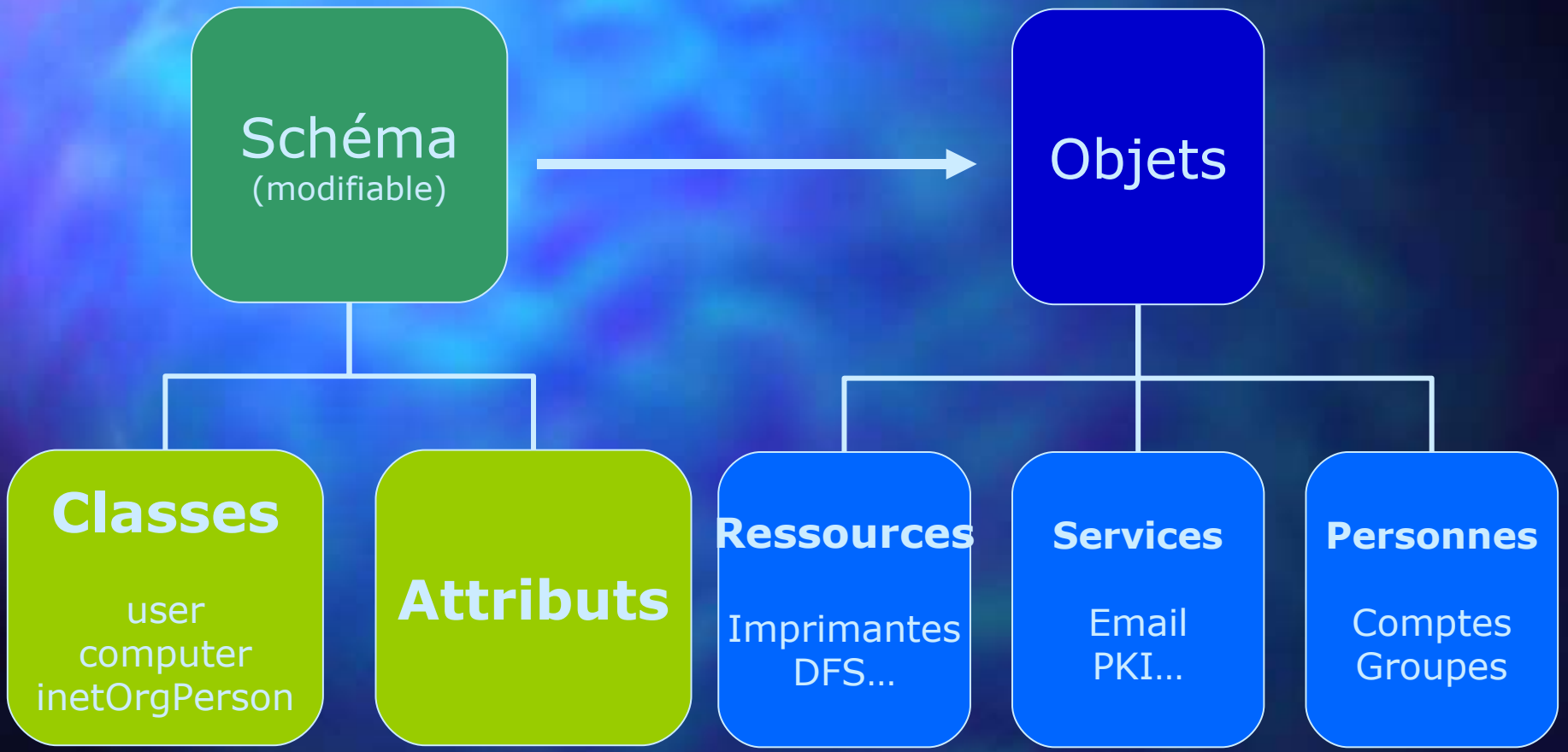
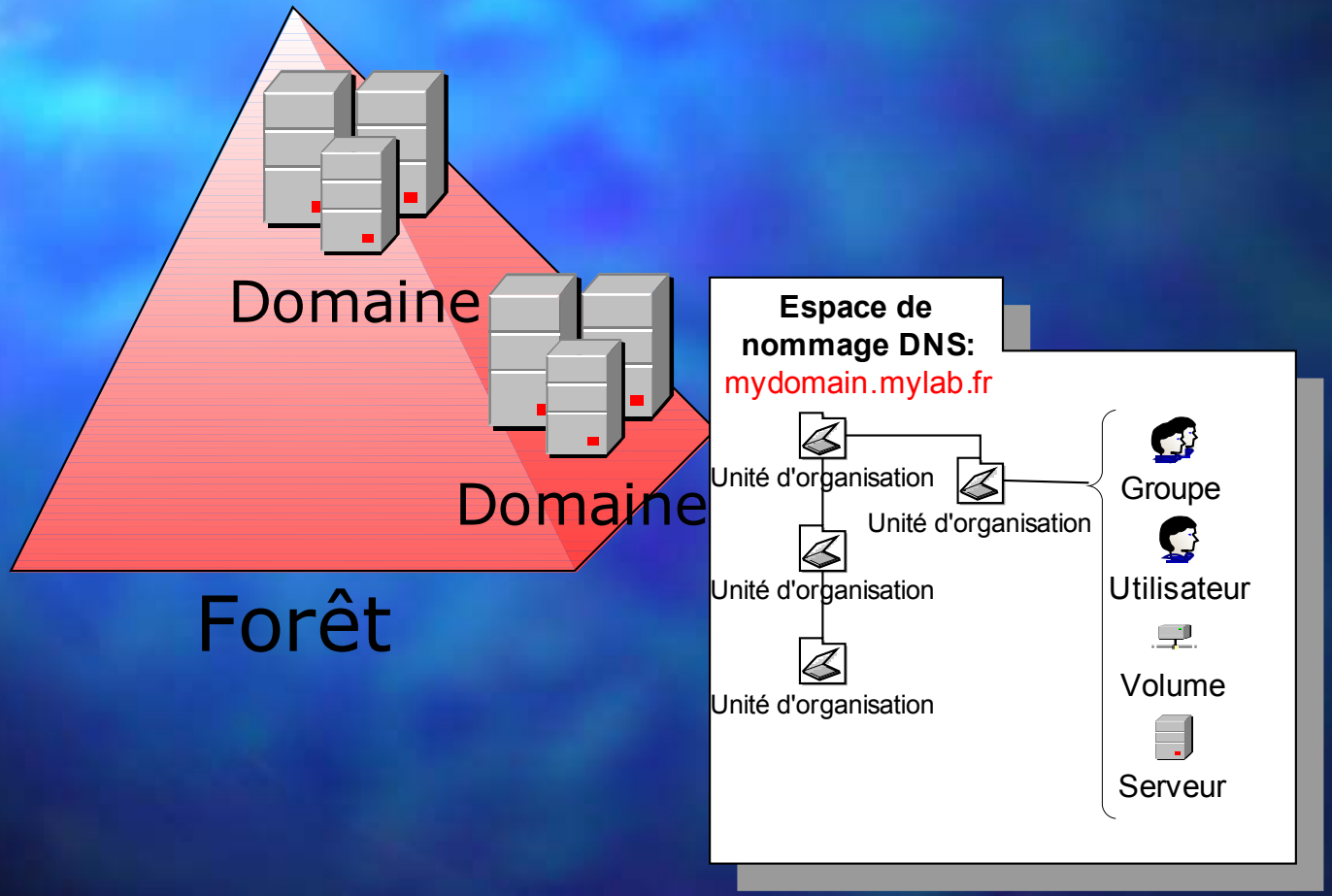


Schéma
(modifiable)
Objets
Classes
user
computer
inetOrgPerson
Attributs
Ressources
Imprimantes
DFS…
Services
Email
PKI…
Personnes
Comptes
Groupes

Hiérarchie des objets



Nommage dans AD

- Distinguished name (DN)
  CN=user1,DC=mydomain,DC=mylab,DC=fr
- Relative Distinguished Name (RDN)
  CN=user1
- GUID (Globally Unique IDentifier)
  6B A7 AF D2 B0 A3 8C 4D A4 46 D7 7F 80 06 2A 5E
- User Principal Name (UPN)
  user1@mydomain.mylab.fr

Les rôles FSMO

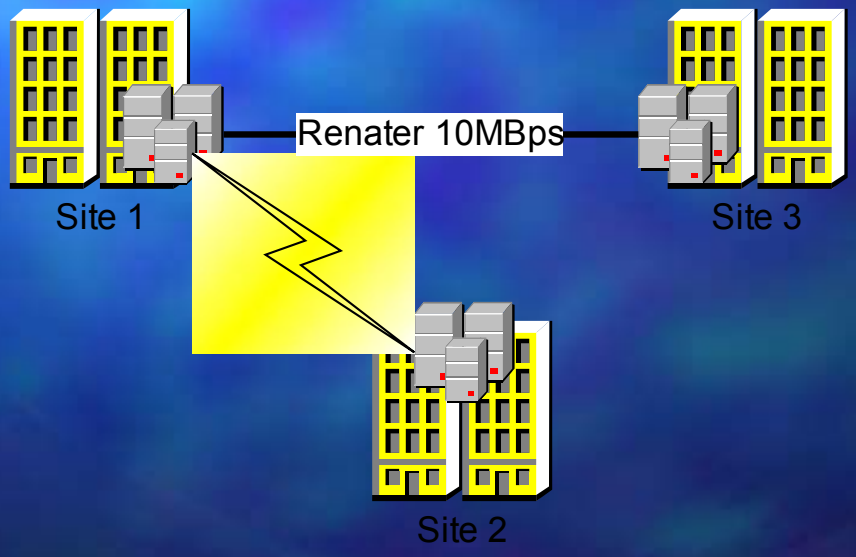
- *Flexible Single Master Operation*
- Cinq rôles
  - Maître de schéma: gère les MàJ du schéma
  - Maître d'attribution de nom de domaine: gestion des noms de domaine dans la forêt
  - Maître Relative ID: attribution des RID
  - Emulateur PDC: W32Time, account lockout…
  - Maître d'infrastructure: gestion des identificateurs d'objet inter-domaines
- Un seul serveur peut assurer un rôle

Réplication intra-site

- Contrôlée par le KCC
  Knowledge Consistency Checker
- Utilise RPC over IP
- Réplication en mode *pull*
- Temps d'attente par défaut: 5 minutes
  Configurable dans:
  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters
  Clé *Replicator notify pause after modify (secs)*
  REG_DWORD, hexadécimal, secondes, défaut=300

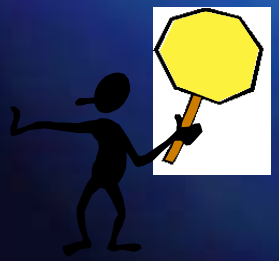
Réplication inter-site

- Configurable
- Repose sur un calcul de coût de liaison
- Utilise SMTP (!)



Stratégies de groupes (GPO)

- Configurer administrativement des restrictions ou des paramètres à appliquer sur des ordinateurs ou des utilisateurs
- Déployer automatiquement des logiciels et leurs mises à jour



Clients Windows uniquement !

Interopérabilité clients

- Clients Windows: autoriser, authentifier, partager des ressources.
- Clients tierces:
  - Autoriser et authentifier au niveau système grâce à Kerberos5 et/ou LDAP
  - Authentifier au niveau applicatif par modules dédiés
  - Partager des ressources grâce à CIFS/SMB

Interop. clients - Authentifier

- pam_krb5: Authentification Kerberos5 avec le contrôleur de domaine, par un module PAM
- Interface LDAP v3: compatible avec librairies clientes OpenLDAP
  - Applis PAM-incompatibles? nss_ldap
  - Apache: mod_auth_ldap
  - PHP: fonctions LDAP
  - Postfix (Cyrus-SASL <-> LDAP)
  - Dovecot (POP3/IMAP4): LDAP support

Interopérabilité ID servers

- iPlanet/SunONE DS: Connecteur de réplication bidirectionnelle
- Réplication vers un serveur Redhat/Fedora DS: WinSync
- NIS/YP: MS SFU, NIS Server
- MS Identity Integration Server
- Dernier recours: fichiers LDIF !

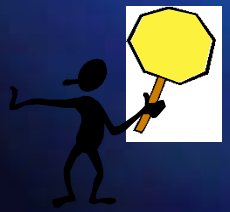
Pluggable Authentication Module

Concepts et mise en œuvre

® Michel CHABANNE – Ecole Polytechnique/DSI/RVDS – Octobre 2005

PAM

- Créé par SUN en 1995, spécifications ouvertes en 1997
- Interface de programmation pour des services d'authentification: plusieurs librairies dynamiques
- Définit des types d'authentification (modules)
- Définit des règles d'authentification (usage des modules, *policies*)



Toutes les applications ne sont pas compatibles !

Terminologie

- *Facilities*
  - Authentication
  - Account management
  - Session management
  - Account token update
- *Chains:* Suite de directives, 1/facility
- *Policy:* Dépendances inter-modules

Modules

- Une partie de code pour chaque *facility*
- Réalisent une action de contrôle
- Réalisent une action d'information
- Retournent une valeur indiquant le succès ou l'échec
- Une 20aine fournis avec les sources de PAM (http://www.kernel.org/pub/linux/libs/pam/)

Chains, policies

- Binding – Si OK tous modules, fin de chaîne
- Required – Si échec, la chaîne continue mais la requête sera refusée
- Requisite – Si échec, la chaîne s'arrête là et la requête est refusée
- Sufficient – Idem binding, mais la chaîne continue en cas d'échec
- Optional – Module optionnel

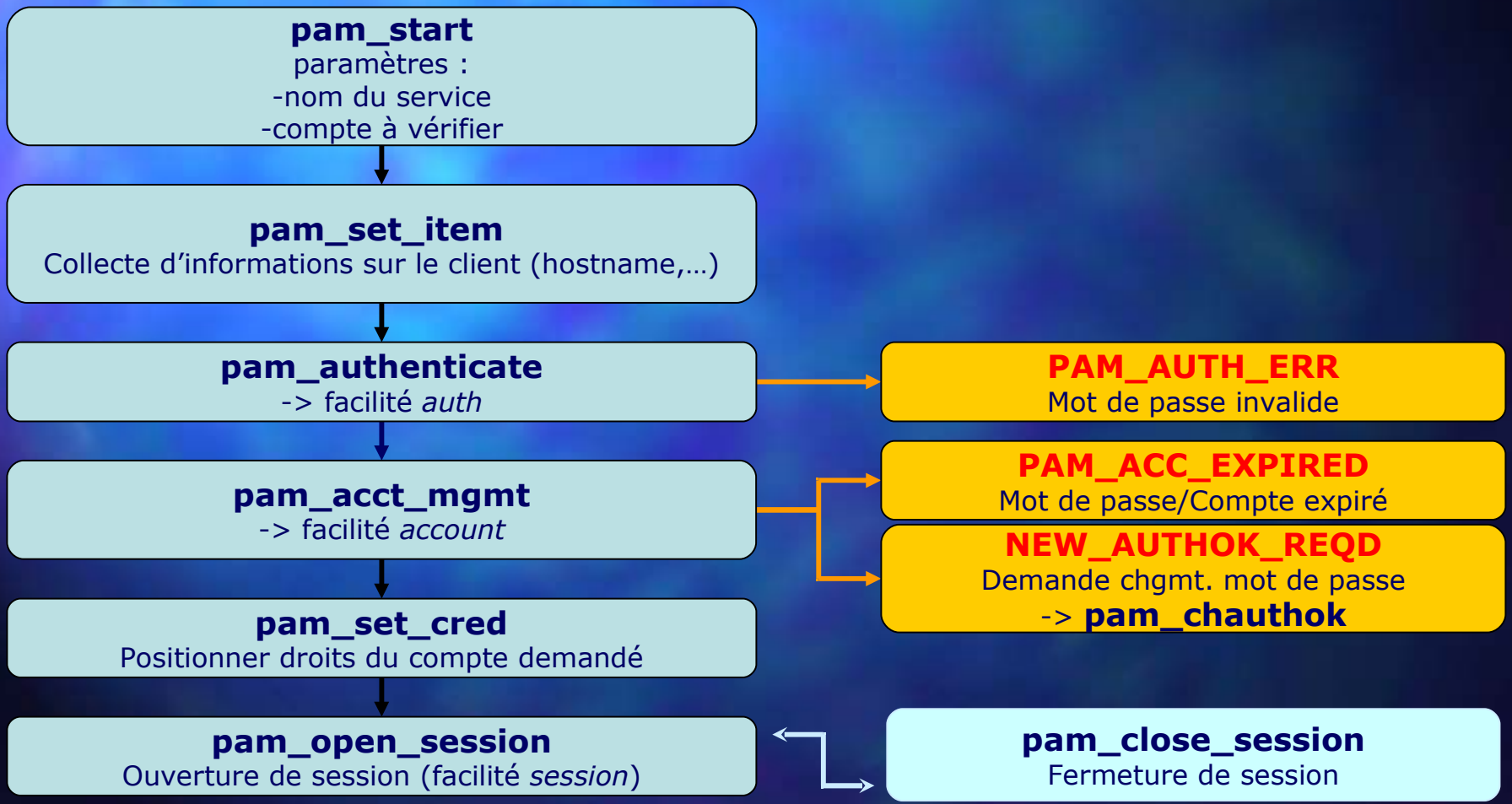
Configuration

- pam.conf, /etc/pam.d/*
- Format de ligne:

```
nom_service   facility   policy     module
login         auth       required   pam_unix.so
```

- Un fichier de configuration par service
- Chaque fichier est lu de haut en bas

Principe


pam_start
paramètres :
-nom du service
-compte à vérifier
pam_set_item
Collecte d'informations sur le client (hostname,…)
pam_authenticate
-> facilité auth
PAM_AUTH_ERR
Mot de passe invalide
pam_acct_mgmt
-> facilité account
PAM_ACC_EXPIRED
Mot de passe/Compte expiré
NEW_AUTHOK_REQD
Demande chgmt. mot de passe
-> pam_chauthok
pam_set_cred
Positionner droits du compte demandé
pam_open_session
Ouverture de session (facilité session)
pam_close_session
Fermeture de session

Exemple

- **sshd auth required pam_nologin.so no_warn**
  Module: nologin=vérifie la présence de /etc/nologin, et refuse alors toute connexion d'un compte autre que root. Facilité *auth*, tout échec est fatal.
- **sshd auth required pam_unix.so no_warn try_first_pass**
  Module: unix=Lecture classique du mot de passe unix pour comparaison. Facilité *auth*, tout échec est fatal.
- **sshd account required pam_login_access.so**
  Module: login_access=Implémente la gestion du fichier login_access(5) qui spécifie les combinaisons user/host/tty autorisées à se connecter. Facilité *account*, tout échec est fatal.
- **sshd account required pam_unix.so**
  Module: unix=On utilise ici d'autres fonctionnalités de ce module, notamment sa capacité à vérifier l'expiration du mot de passe fourni. Facilité *account*, tout échec est fatal.
- **sshd session optional pam_lastlog.so no_fail**
  Module: lastlog=Ecriture des journaux wtmp/utmp. Facilité *session*, échec ignoré.
- **sshd password required pam_unix.so nullok obscure min=4 md5**
  Module: unix=Oblige des mots de passe mini 4 caractères, vide possible, encodés en MD5. Facilité *password*, tout échec est fatal.

Application

Authentifier les utilisateurs SSHd par pam_ldap

® Michel CHABANNE – Ecole Polytechnique/DSI/RVDS – Octobre 2005

Pré-requis

- Un serveur LDAP fonctionnel, schéma conforme RFC 2798 (inerOrgPerson) et RFC 2307 (« NIS »)
- Serveur SSH = Client LDAP, Unix
- pam_ldap (www.padl.com/OSS/**pam_ldap.html**)

1. Configuration SSHd

- Vérifier support PAM dans démon SSHd
  `# ldd `which sshd` | grep libpam`
  Sinon=recompilation from scratch!
- sshd_config: UsePam = Yes
- Tester fonctionnement PAM avec config par défaut (pam_unix)

2. /etc/pam.d/sshd

```
auth       required    pam_nologin.so
auth       sufficient  pam_ldap.so
auth       required    pam_unix_auth.so
account    sufficient  pam_ldap.so
account    required    pam_unix_acct.so
password   required    pam_cracklib.so
password   sufficient  pam_ldap.so
password   required    pam_unix_passwd.so
use_first_pass md5 shadow
session    required    pam_unix_session.so
```

3. /etc/ldap.conf

```
host ldap1.polytechnique.fr \
   ldap2.polytechnique.fr
base \
   ou=Recherche,dc=polytechnique,dc=xxx
scope sub
binddn \
   cn=ldapuser,ou=Users,dc=polytechnique,dc=xxx
bindpw password
port        636
ldap_version 3
ssl start_tls
tls_cacertfile /etc/ssl/certs/ldap.crt
crypt md5
```

Projet LDAP à l'Ecole Polytechnique

École Polytechnique

200 ans d'enseignement et de recherche

® Michel CHABANNE – Ecole Polytechnique/DSI/RVDS – Octobre 2005

Objectifs

- Consolider un annuaire central des personnels et collaborateurs de l'Ecole
- Authentification centralisée des services communs (mail, sites web…)

  –> Single Sign-On
- Autorisation d'accès à ces services
- Authentification centralisée pour les postes clients (Linux, Windows, OSX)
- Authentification forte (certificats), notamment pour les réseaux sans-fils –> PKI

Phasing

- Mars-Oct.: Groupe de travail: définition du schéma, choix des produits
- Nov.-début 2006: Maquettage (implémentation EAP Wi-Fi)
- Mi-2006: Architecture finale.