

UMR 6614

**coRia**

COMPLEXE DE RECHERCHE  
INTERPROFESSIONNEL EN AEROTHERMOCHIMIE

CNRS – UNIVERSITE et INSA de Rouen

# LDAP au CORIA

Journée RESINFO

10 juin 2005

Henri Cavalier

# PLAN

- Topologie des serveurs d'annuaire au CORIA
- Passerelle NIS/LDAP: ypldapd (PADL)
- Synchronisation LDAP/AD: ISW (SUN)
- Applications:
  - Authentification des utilisateurs
  - Mail :Postfix
  - Autres ...

# Serveurs d'annuaire au CORIA

- 3 domaines (coria.fr)
  - Domaine AD : monde Windows et Samba
  - Domaine LDAP : authentification sur machines unix récentes et annuaires divers (mail, ...)
  - Domaine NIS: authentification sur machines Unix qui ne supportent pas d'autres services
- Nécessité de synchronisation LDAP/NIS et LDAP/AD

# Topologie des serveurs d'annuaire au CORIA

## Serveur LDAP



Réplication  
multi-master

## Serveur LDAP

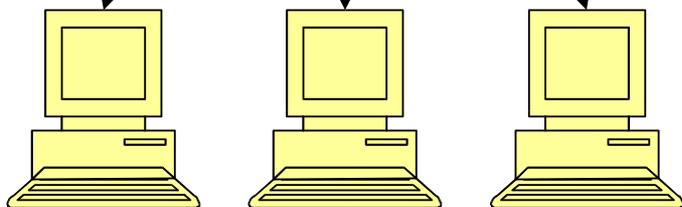


Synchro  
LDAP-AD

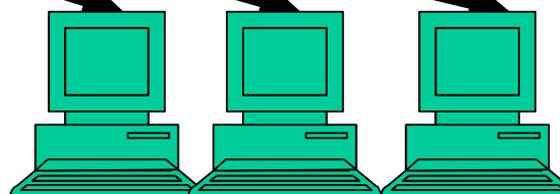
## Serveur AD



Passerelle nis-ldap

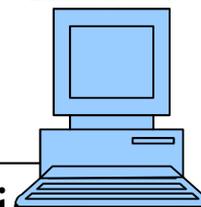


Clients NIS:solaris<2.8, vieux  
linux, TRU64<5.0, HPUX<11,...



Clients LDAP natifs: Solaris ≥  
2.8, linux récents, TRU64 ≥ 5.0,  
...

PC  
Windows



# Choix d'un serveur LDAP

- Choix de DIRECTORY SERVER (Sun Microsystems):
  - Connaissance de l'OS
  - Disponibilité d'un support Hot Line SUN au CORIA
  - Simplicité de mise en œuvre d'un doublon master-replica en mode multi-masters
  - Disponibilité d'un logiciel de synchronisation LDAP/Active Directory du même éditeur
- Prochainement disponible sous RedHat

# SunOne Directory Server

The screenshot displays the Sun Java System Directory Server interface, version 5.2, with the 'Directory' tab selected. The left pane shows a directory tree for 'replica.coria.fr:389'. The tree includes a folder 'dc=coria,dc=fr (11 acis)' containing various entries such as 'nsAccountInactivationTmp', 'aliases', 'coria users slice', 'ethers', 'group', 'Groups', 'history', 'hosts', 'liste de diffusion', 'netgroup', 'networks', 'People (5 acis)', 'peuple (2 acis)', 'printers', 'profile', 'protocols', 'relais de mail', 'rpc', 'services', 'SolarisAuthAttr', 'SolarisExecAttr', 'solarisProfAttr', 'Special Users', 'system', 'People (5 acis)', and 'Utilisateurs\_deductives'. The 'People (5 acis)' entry is highlighted in blue. A red circle highlights the 'People (5 acis)' entry at the bottom of the tree. Two callout boxes with orange arrows point to specific entries: one points to 'coria users slice' and 'liste de diffusion' with the text '« Spécial CORIA »', and another points to the 'People (5 acis)' entry with the text 'Smart Referral'. The status bar at the bottom shows 'ou=People, dc=coria,dc=fr'.

# Cas des machines « vieillissantes »

➤ Pour certaines machines ( vieux linux, Solaris < 2.8, TRU64 < 5, HPUX < 11, ...)

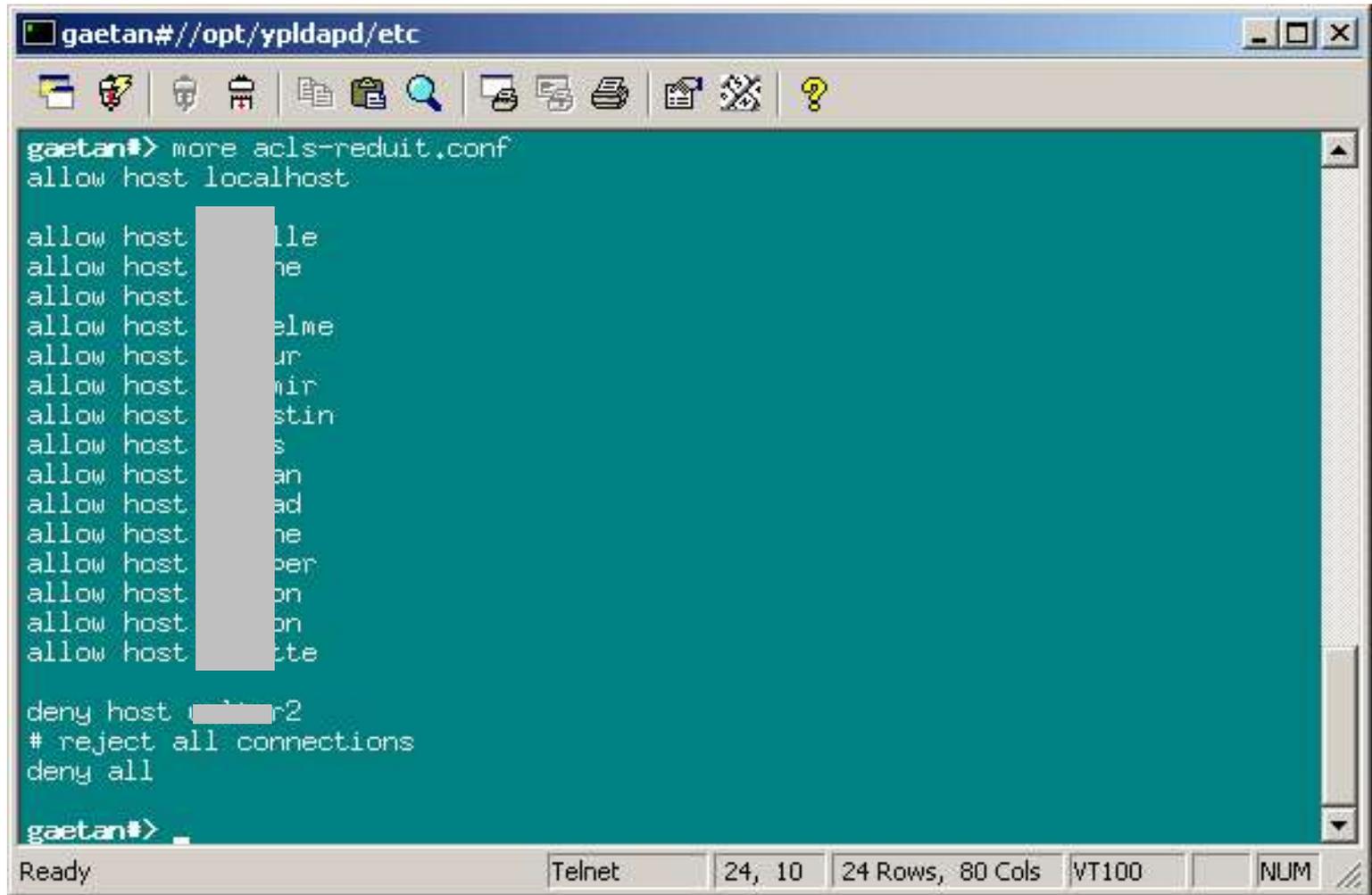
- Utilisation d'un domaine NIS (Partiellement pré-existant)
- Utilisation d'une passerelle NIS/LDAP: ypldapd de PADL

# Ypldapd de PADL

## Passerelle entre NIS (yp) et LDAP

- Serveur de domaine NIS pour les clients NIS
- Client LDAP
- Les domaines NIS et LDAP ont le même nom
- S'installe sur une machine linux ou solaris préalablement cliente d'un serveur LDAP
- Synchronise les maps NIS périodiquement (10 mn) sur le serveur LDAP
- *Mais la mise à jour des passwd depuis les clients NIS n'est pas possible.*
- Supporte par configuration un minimum de sécurité:
  - Securenets: liste de réseaux sûrs
  - Filters: liste de maps NIS à cacher
  - ACLs: liste de machines ou réseaux allow/deny.

# Ypldapd: ACLs



```
gaetan# more acls-reduit.conf
allow host localhost

allow host [REDACTED]lle
allow host [REDACTED]ne
allow host [REDACTED]
allow host [REDACTED]elme
allow host [REDACTED]ur
allow host [REDACTED]mir
allow host [REDACTED]stin
allow host [REDACTED]s
allow host [REDACTED]an
allow host [REDACTED]ad
allow host [REDACTED]ne
allow host [REDACTED]per
allow host [REDACTED]on
allow host [REDACTED]on
allow host [REDACTED]cte

deny host [REDACTED]r2
# reject all connections
deny all

gaetan#
```

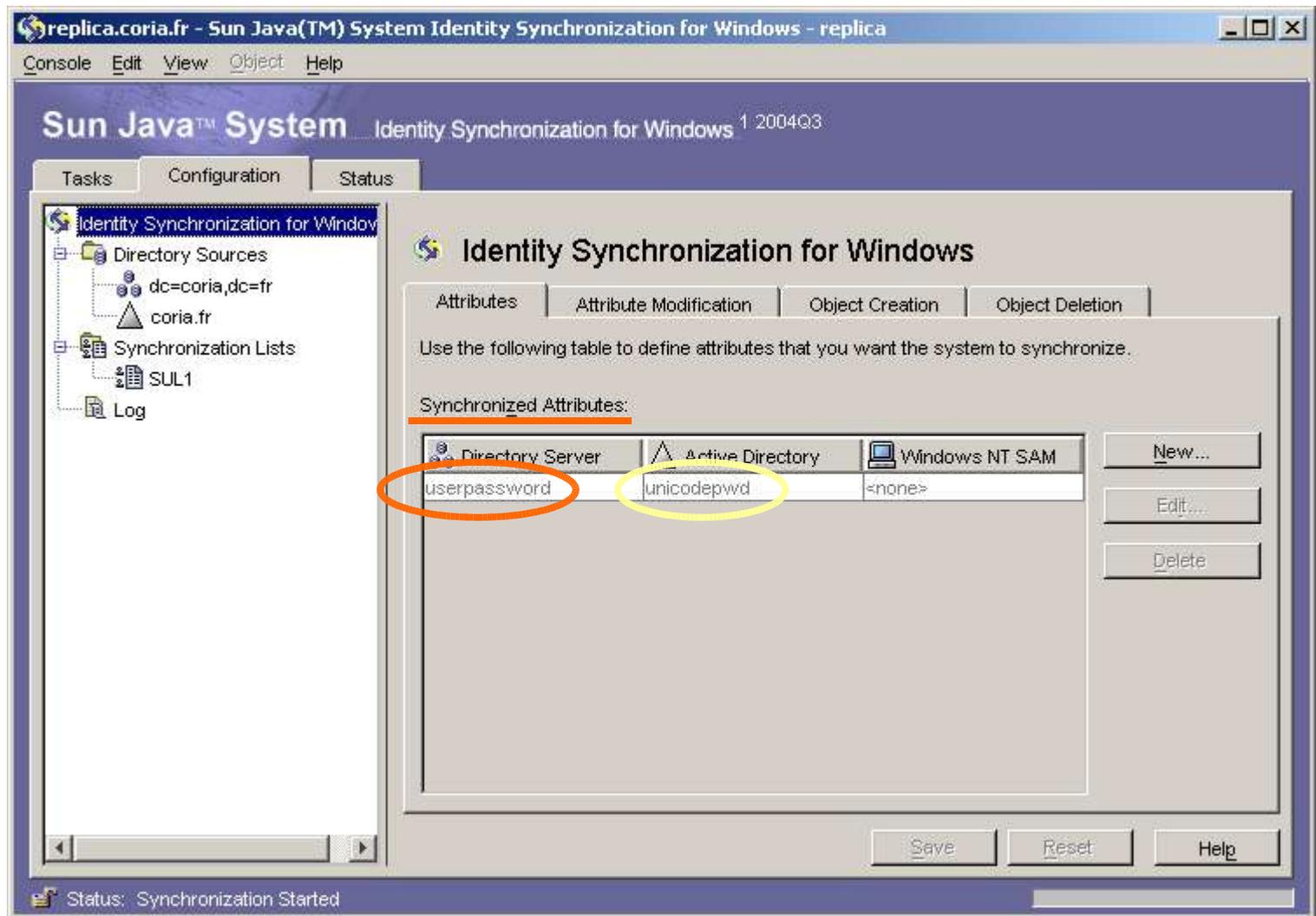
# ISW: Identity Synchronization for Windows

- Produit SUN installé sur un des 2 serveurs LDAP
- Assure la synchro bidirectionnelle des mots de passe entre LDAP et AD grâce à des « connecteurs » (Déploiement en cours)
- La réplication multi-masters propage les infos sur le 2<sup>ème</sup> serveur
- Peut assurer la synchro. à la création des users (Ultérieurement)

# ISW: Remarques

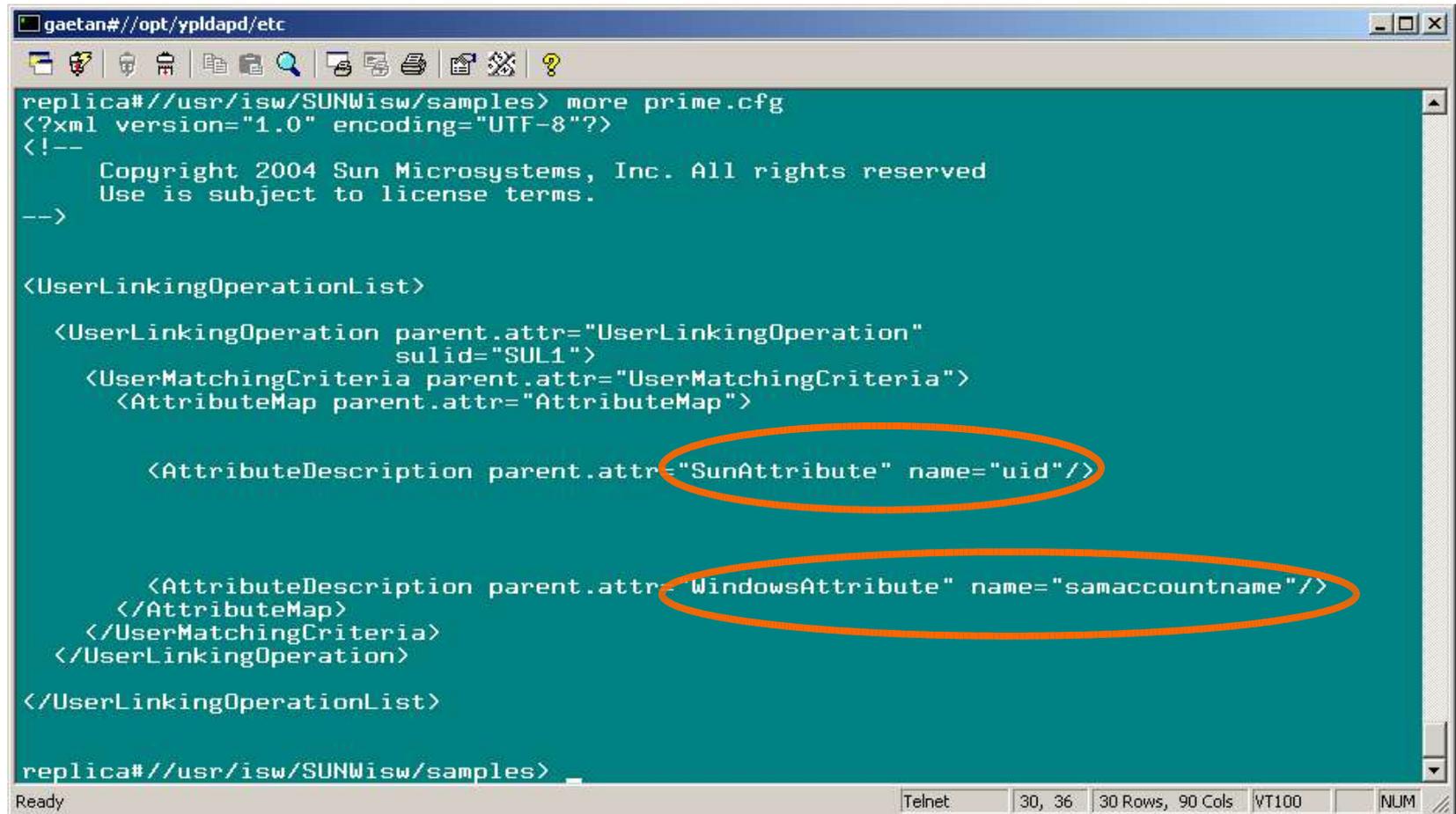
- Les mots de passe sur le DS doivent être au format « crypt » pour les NIS
- la synchronisation des passwd Windows vers Unix n'est pas problématique
- La synchronisation des passwd Unix vers Windows nécessite SSL (LDAPS) et donc la mise en place de certificats sur les 2 serveurs d'annuaire (Certificats CNRS standards)

# ISW Console



# ISW: critères de correspondance

- La correspondance entre les attributs LDAP et AD est effectuée via un fichier de config. au format XML



```
gaetan#//opt/ypldap/etc
replica#//usr/isw/SUNWisw/samples> more prime.cfg
<?xml version="1.0" encoding="UTF-8"?>
<!--
  Copyright 2004 Sun Microsystems, Inc. All rights reserved
  Use is subject to license terms.
-->

<UserLinkingOperationList>

  <UserLinkingOperation parent.attr="UserLinkingOperation"
    sulid="SUL1">
    <UserMatchingCriteria parent.attr="UserMatchingCriteria">
      <AttributeMap parent.attr="AttributeMap">

        <AttributeDescription parent.attr="SunAttribute" name="uid"/>

        <AttributeDescription parent.attr="WindowsAttribute" name="samaccountname"/>
      </AttributeMap>
    </UserMatchingCriteria>
  </UserLinkingOperation>
</UserLinkingOperationList>

replica#//usr/isw/SUNWisw/samples>
Ready Telnet 30, 36 30 Rows, 90 Cols VT100 NUM
```

# Applications 1

## Authentification des utilisateurs

- A la création des utilisateurs:
- Gestion de la répartition des « UidNumber »
- A l'instant
  - Pour créer les entrées LDAP utilisation de scripts PERL
  - Entrée directe sur le serveur AD des utilisateurs Windows
- A venir prochainement:
  - A partir d'une interface web, inscription des nouveaux arrivants dans le labo: téléphone, codes divers, création de login unix et windows (à terme par synchro ISW), ...

# Applications 2

## Autres applications

- Mail: ***postfix*** consulte ses informations sur le serveur LDAP
  - Entrée liste de diffusion
  - Entrée relais de mail
  - Entrée utilisateur standard
- Tables dhcp, copiées périodiquement sur le serveur dhcp (indépendance des services par sécurité) (en projet)

# Postfix: Liste de diffusion

- Listes gérées en tant qu'alias (passé ...)
- « ou » composée de classes « mailgroup »
- Modification du schéma (Non standard)
- Comprend essentiellement 3 objets obligatoires:
  - Nom de la liste
  - mail de la liste (unique)
  - mailMember (multiple) qui peut être lui-même une liste. Exemple:



# Postfix: relais de mail

- Pour les utilisateurs n'ayant pas de compte local
  - On se limite à renvoyer leur mail vers une adresse extérieure
- « ou » « relais de mail » composée de pseudo-users inaccessibles à l'authentification
- Consultation par postfix après les users standards de « ou=people »

# Postfix: Exemple de relais de mail

Generic Editor - uid=borghi, ou=relais de mail,dc=coria,dc=fr

accountstatus	active
Full name	
createtimestamp	20050315125329Z
creatorsname	uid=admin,ou=administrators,ou=to
entrydn	uid=,ou=relais de mail,dc=cor
entryid	1450
First name	
hassubordinates	FALSE
Email address	i@coria.fr
mailforwardingaddress	@esm2.imt-mrs.fr

dn: uid=borghi, ou=relais de mail,dc=coria,dc=fr

View

- Show Attribute Names
- Show Attribute Description
- Show only Attributes with Values
- Show DN

Refresh

Add Value

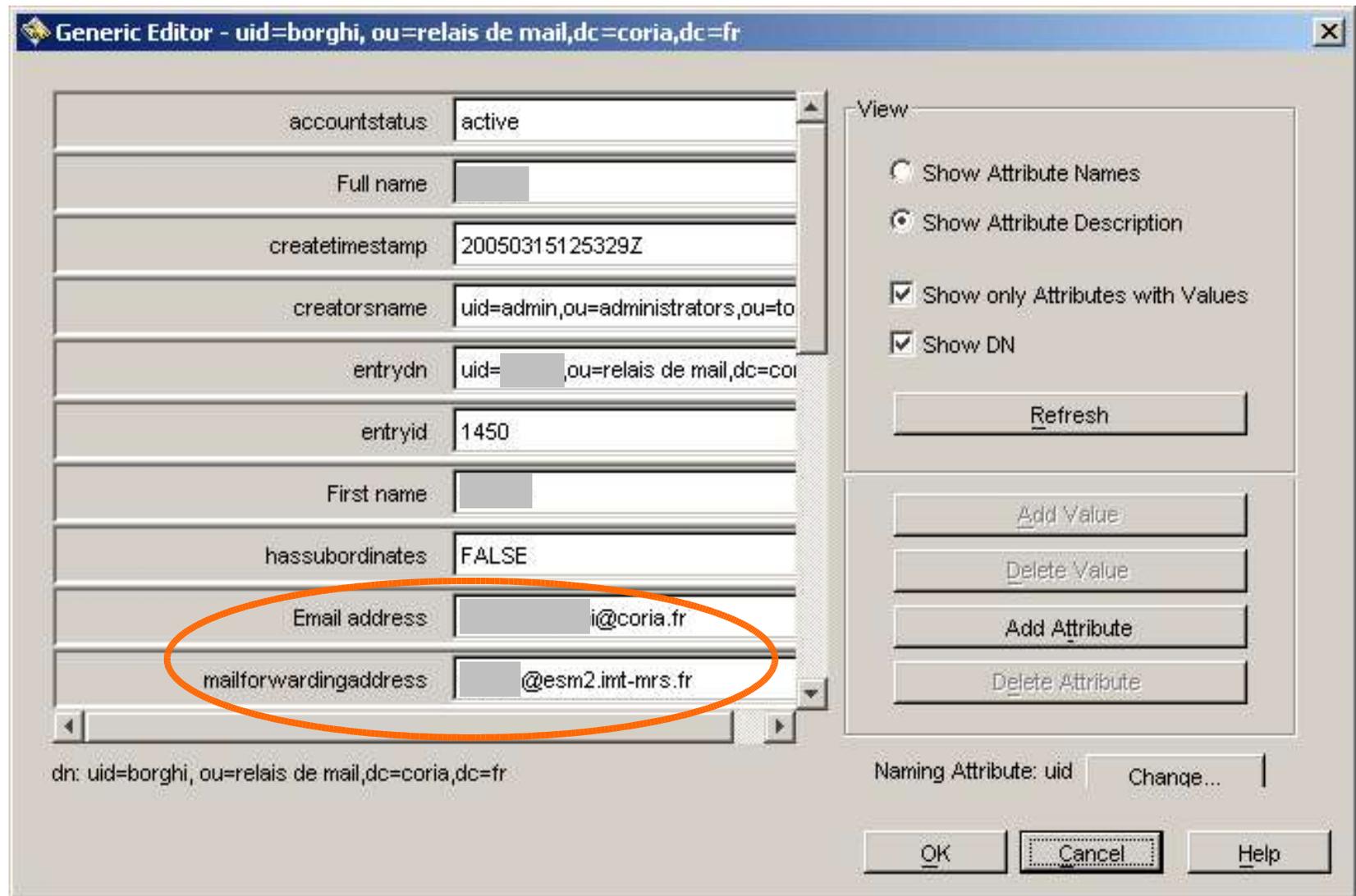
Delete Value

Add Attribute

Delete Attribute

Naming Attribute: uid Change...

OK Cancel Help



# Postfix: Exemple d'utilisateur

Generic Editor - uid=henri,ou=people,dc=coria,dc=fr

creatorsname	cn=directory manager
entrydn	uid=henri,ou=people,dc=coria,dc=f
entryid	36
gecos	HENRI
gidnumber	400
hassubordinates	FALSE
homedirectory	/home/Henri
loginshell	/usr/bin/tcsh
Email address	henri@coria.fr
mailalternateaddress	@coria.fr
mailalternateaddress	@coria.fr
mailalternateaddress	@coria.fr
mailalternateaddress	hc@coria.fr
mailforwardingaddress	henri@pop.coria.fr
modifiersname	uid=henri,ou=people,dc=coria,dc=f

dn: uid=henri,ou=people,dc=coria,dc=fr

View

- Show Attribute Names
- Show Attribute Description
- Show only Attributes with Values
- Show DN

Refresh

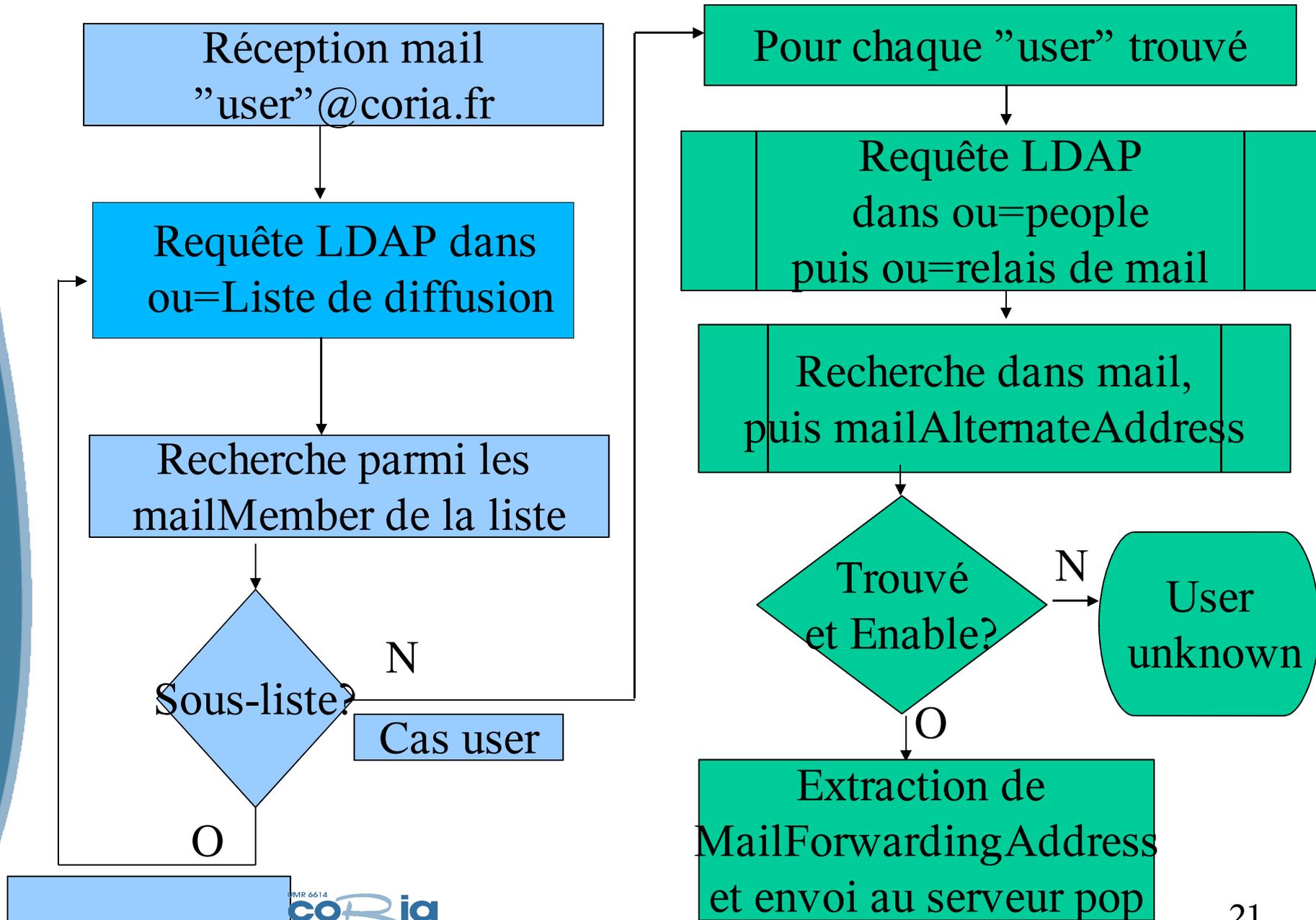
Edit

- Add Value
- Delete Value
- Add Attribute
- Delete Attribute

Naming Attribute: uid Change...

OK Cancel Help

# Postfix: requêtes à l'annuaire LDAP



# CONCLUSION

- Système actuellement largement surdimensionné pour l'utilisation
- Tests de charge à faire quand les applications seront plus nombreuses
- Attention à ne pas installer sur le serveur tous les services (*pas tous les œufs dans le même panier !*), par sécurité et par simplicité de résolution des problèmes. Ex.: DHCP.

# CONCLUSION

# VOS QUESTIONS

