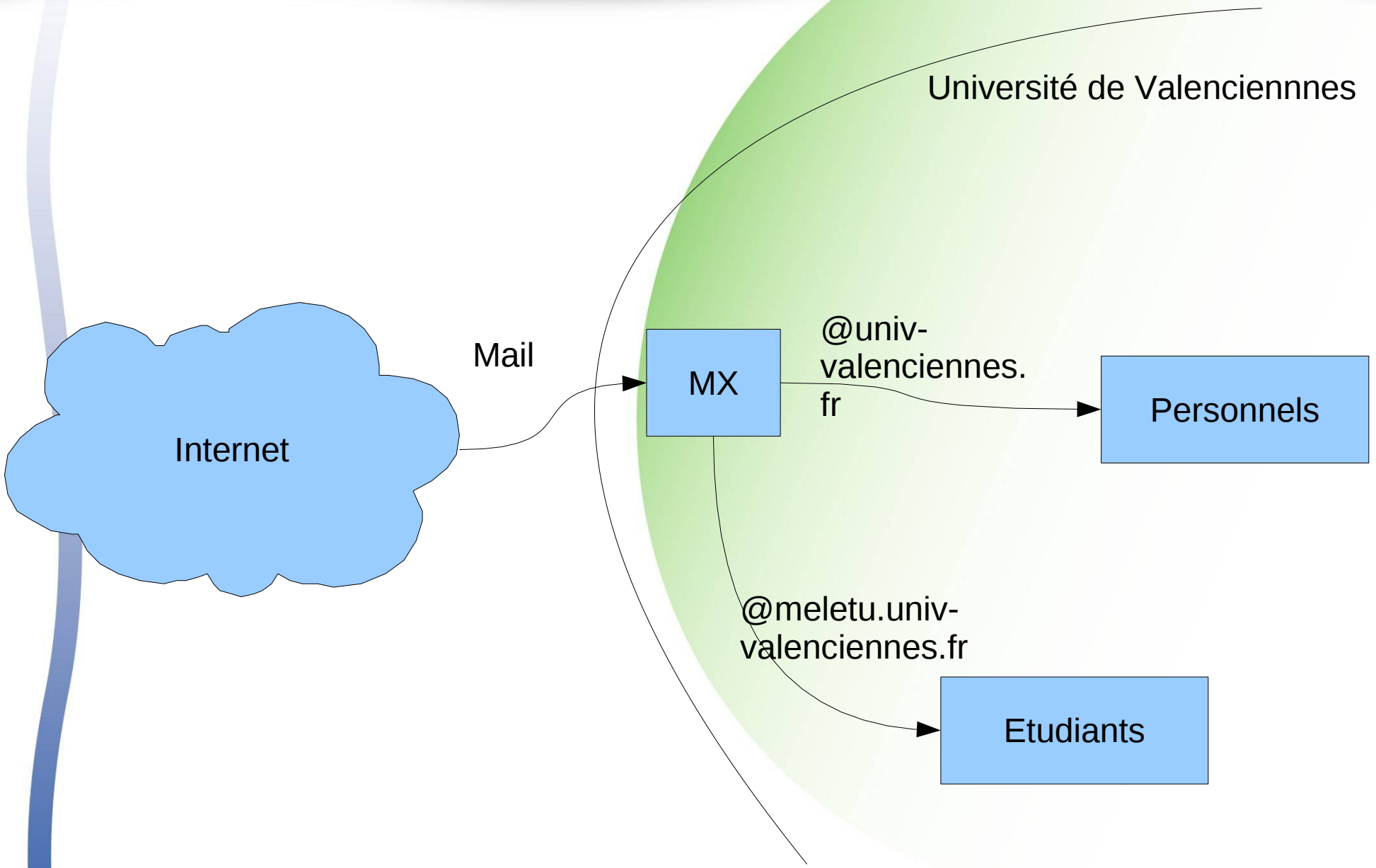
Intégration messagerie ex. de Valenciennes

Atelier FSP

14 novembre 2008

Paris 6

Architecture de Valenciennes



Architecture Valenciennes (2)

- 2 serveurs de messageries:
  - Un « étudiant »:
    - Env. 15000 BALs
  - Un « personnel »
    - Env. 2000 BALs active

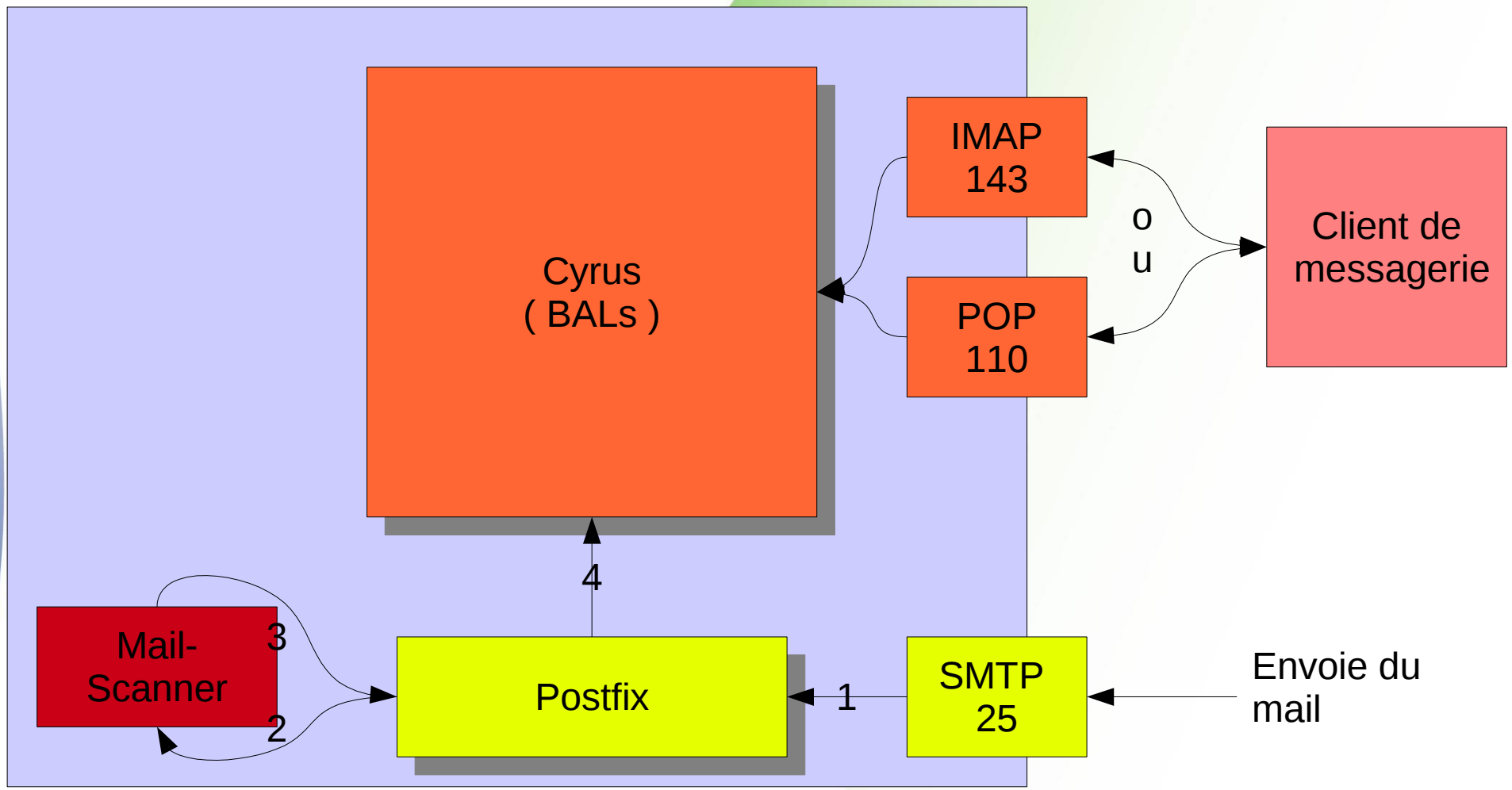
Architecture Valenciennes (3)

- Messagerie « étudiante »
  - cyrus.univ-valenciennes.fr
  - OS: Linux Debian v4.0
  - Espace disque: 170 Go de mail
  - Mémoire: 2 Go
  - Logiciels:
    - Protocole de messagerie: IMAP (cyrus v. 2.1.18)
    - SMTP: postfix

Architecture Valenciennes (4)

- Messagerie « personnel »
  - eiger.univ-valenciennes.fr
  - OS: Red Hat Enterprise Linux AS 4
  - Espace disque : 300 Go
  - Mémoire: 2,5 Go
  - Logiciel:
    - Protocole de messagerie: IMAP (143) / POP(110)
      - Cyrus v 2.1.19
    - SMTP: postfix

Exemple de la messagerie « personnel »



Type de client de messagerie

- Client de messagerie « lourd »:
  - Thunderbird, Outlook, Evolution …
  - Connection en POP ou IMAP
- Client de messagerie Web:
  - Horde/IMP, Canal du portail
  - Connection en IMAP
- Besoin de permettre la connection (authentification et autorisation) de manière à limitée les interactions utilisateurs

CAS: solution de SSO

- Objectif:
  - L'objectif premier d'un mécanisme de SSO web est bien sûr …

    d'offrir un service d'authentification unique simple et performant à des applications web.
  - CAS va bien plus loin en permettant de rendre compatibles différents services non web] tels que IMAP, FTP, ... avec son propre mécanisme.
    - Cassification d'appli Web
      - PhpCAS: Webmail Horde/IMP
      - API CAS Java
      - mod_cas: module Apache
    - Cassification d'appli non Web
      - pam_cas: Cyrus...

Solution PAM ?

- Il faut que le serveur IMAP soit compatible avec PAM:
  - C'est le cas de cyrus grace au démon saslauthd.

PAM

- PAM (Pluggable Authentication Module):
  - Système de gestion des tâches d'authentification des applications (services) sur le système.

« Linux-PAM is a system of libraries that handle the authentication tasks of applications (services) on the system. The library provides a stable general interface (Application Programming Interface - API) that privilege granting programs (such as login(1) and su(1)) defer to to perform standard authentication tasks. »

ext. Page de man pam

PAM (2)

- PAM (Pluggable Authentication Module):
  - La nature de de l'authentification est configurable dynamiquement.
  - L'administrateur système est libre de choisir individuellement de quelle manière les applications qui fournissent le service authentifierons les utilisateurs.
  - Configuration: fichiers de configuration individuels situés dans le répertoire **/etc/pam.d**

PAM (3)

- Séparation des tâches d'authentification en 4 groupes de gestions independants:
  - **Account** management:
    - Vérification des types de service du compte utilisateur.

      Mot de passe expire ? A-t'il le droit d'accéder au service demande ?
  - **Auth**entication management:
    - Correspondance entre l'utilisateur et ce qu'il pretend etre

      Defi reponse: ex: mot de passe, certificat ...
  - **Password** management:
    - Mettre à jour les mécanismes d'authentification (chgt de mdp)
  - **Session** management:
    - Point d'accroche à l'ouverture et à la fermeture des modules qui affectent les services disponibles: maintenance de la journalisation, montage de homedir...

PAM (4)

- required
  - Doit réussir, mais on continue à tester les autres modules malgré tout. Echec est renvoyé. L'avantage par rapport à requisite étant que l'on ne donne pas la raison de l'échec de la connexion.
- requisite
  - Doit réussir, on ne continue pas à lire les autres modules, Echec est renvoyé immédiatement.
- optimal
  - Est ignoré, en fait que le test réussisse ou pas cela ne change pas la suite.
- sufficient
  - Si le test est correct, on obtient immédiatement une acceptation.

PAM_CAS

- Module PAM pour CAS

  « *PAM_CAS est un module PAM permettant aux process ou aux démons UNIX implémentant cette interface d'utiliser l'authentification CAS.* »

  ext du site http://www.esup-portail.org

- Page du module sur le site esup Portail:
  - Projet abouti
  - http://www.esup-portail.org/x/qwA8

- Version originale developpee par l'université de Yale

PAM_CAS (2)

- Fonctionnement global du module:
  - Il reçoit de pam deux informations : le nom d'utilisateur et le PT (Proxy Ticket) passé comme mot de passe.
  - Il génère ensuite une connexion http(s) directe vers le serveur CAS, à l'url de validation de PT (en standard, /proxyValidate).
  - Il analyse le retour de cette requête, reçue en xml : validation du PT, identité de l'utilisateur, hiérarchie de proxies par lesquels le PT a été obtenu.
  - Il fait un controle du nom de proxy pour des raisons de sécurité, et s'assure que l'identité de l'utilisateur retournée par le serveur CAS correspond à celle passée par pam.
  - Il retourne à pam le code PAM_SUCCESS en cas de réussite, PAM_AUTH_ERR dans le cas contraire.

PAM_CAS (3)

- Modifications esup
  - Fichier de configuration
  - Gestion des connexions http(s)
  - Possibilités de debug
  - Comportements optionnels
    - choisir entre http ou https pour la validation des proxy ticket
    - ne plus contrôler le proxy qui a généré le Proxy Ticket.

Compilation PAM_CAS

- Pré requis: openssl.
- Téléchargement:
  - http://sourcesup.cru.fr/frs/?group_id=213
  - Version: 2.0.11
- Installation:
  - cd sources
  - cp Makefile.Redhat Makefile (sous redhat, ou autre Makefile en fonction de l'OS).
  - make (compilation et création du module pam_cas.so)
  - make test (si vous désirez utiliser le binaire castest)

Configuration PAM_CAS

- Fichier de configuration:
  - /etc/pam_cas.conf

```
# host from CAS server. mandatory
host cas.univ-valenciennes.fr

# port from CAS server. Default to 80 or 443, depends from ssl instruction
port 80

# uri to validate ticket. Default to /proxyValidate
uriValidate /cas/proxyValidate

# https or no. values on or off. Default to on.
ssl off
```

Configuration PAM_CAS

- Fichier de configuration suite:

```
# proxy or proxies who deliver Proxy Ticket.

proxy https://webpers.univ-valenciennes.fr/casProxy.php
proxy https://webpers-test.univ-valenciennes.fr/casProxy.php
proxy https://cyrus.univ-valenciennes.fr/casimap.php
proxy https://ent1.univ-valenciennes.fr/CasProxyServlet

# trusted_ca. mandatory if ssl on.
# It a file in pem format. It can contents several certificates
# If the CAS server certificate is auto-signed, the file must content the certificate
# If the certificate is trusted by an Certificate Autority, The file must content
#    certificate from high level CA
trusted_ca /Cert/ac-racine.pem
```

Utilisation de PAM_CAS

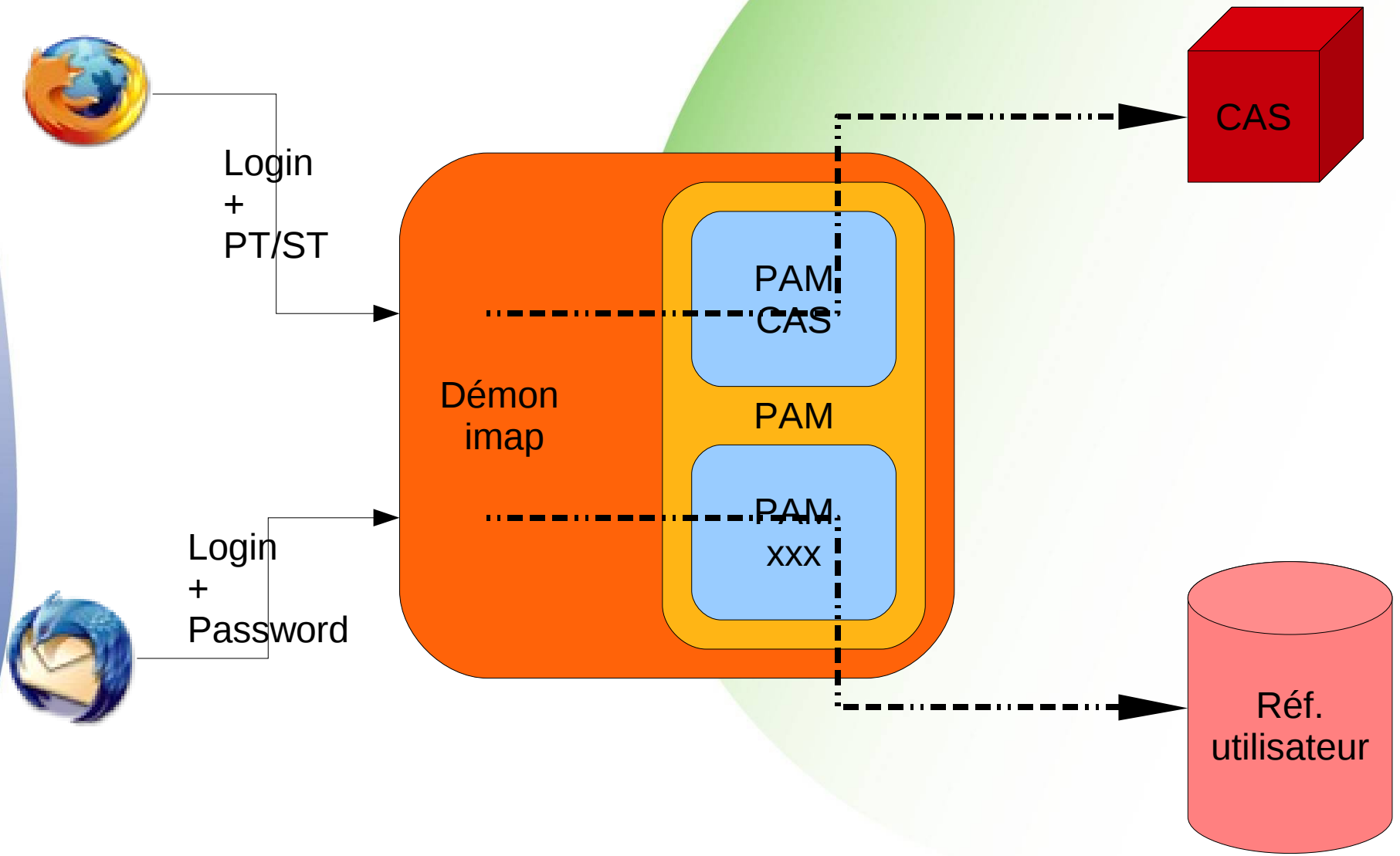
- cp pam_cas.so /lib/security/

- Adapter le fichier /etc/pam.d/imap:

```
#%PAM-1.0
auth sufficient /lib/security/pam_cas.so -simap://eiger.univ-valenciennes.fr  -f
/etc/pam_cas.conf
auth sufficient /lib/security/pam_ldap.so
auth       required     /lib/security/pam_stack.so service=system-auth

account sufficient /lib/security/pam_ldap.so
account    required     /lib/security/pam_stack.so service=system-auth
```

Schéma de l'authentification IMAP



Validation PAM_CAS

- on peut mettre pam_cas sans craintes de surcharge du serveur imap.
  - il ne fait de requêtes auprès du serveur CAS que si le mot de passe reçu ressemble à un PT ou un ST.
- Castest (/usr/local/src/Pam_cas sur eiger)
  - permet de générer des requêtes de validation de ticket auprès du serveur CAS
- casImap.php (https://cyrus.univ-valenciennes.fr/casimap.php)
  - Cet utilitaire permet de tester le fonctionnement d'un serveur IMAP CAS-ifié.

Conclusion PAM_CAS

- **pam_cas** permet de valider un ticket (PT ou ST) présenté comme un simple mot de passe de l'utilisateur passé dans la demande de validation.
- Le protocole IMAP:
  - les clients IMAP (webmails) ont tendance à générer de très nombreuses requêtes, avec rupture et ré-ouverture de connexions, donc nouvelles demandes d'authentification.
- Pour des raisons de performance, il est souvent nécessaire de "cacher" ce ticket afin de pouvoir le rejouer plusieurs fois.

« Cacher » les ticket

cyrus - saslauthd

- Démon livré avec la distribution cyrus-imap.
- Saslauthd peut être paramétré pour:
  - authentifier à l'aide de pam. Il est alors possible d'utiliser pam_cas pour cassifier saslauthd, donc cyrus
    - Flag « -a pam »
  - implémenter un cache de mot de passe (donc, éventuellement, de tickets).
    - Flag « -c »

/usr/local/sbin/saslauthd -m /var/run/saslauthd -a pam -c

cyrus – saslauthd (2)

- Modification de cyrus:
  - Fichier /etc/imapd.conf

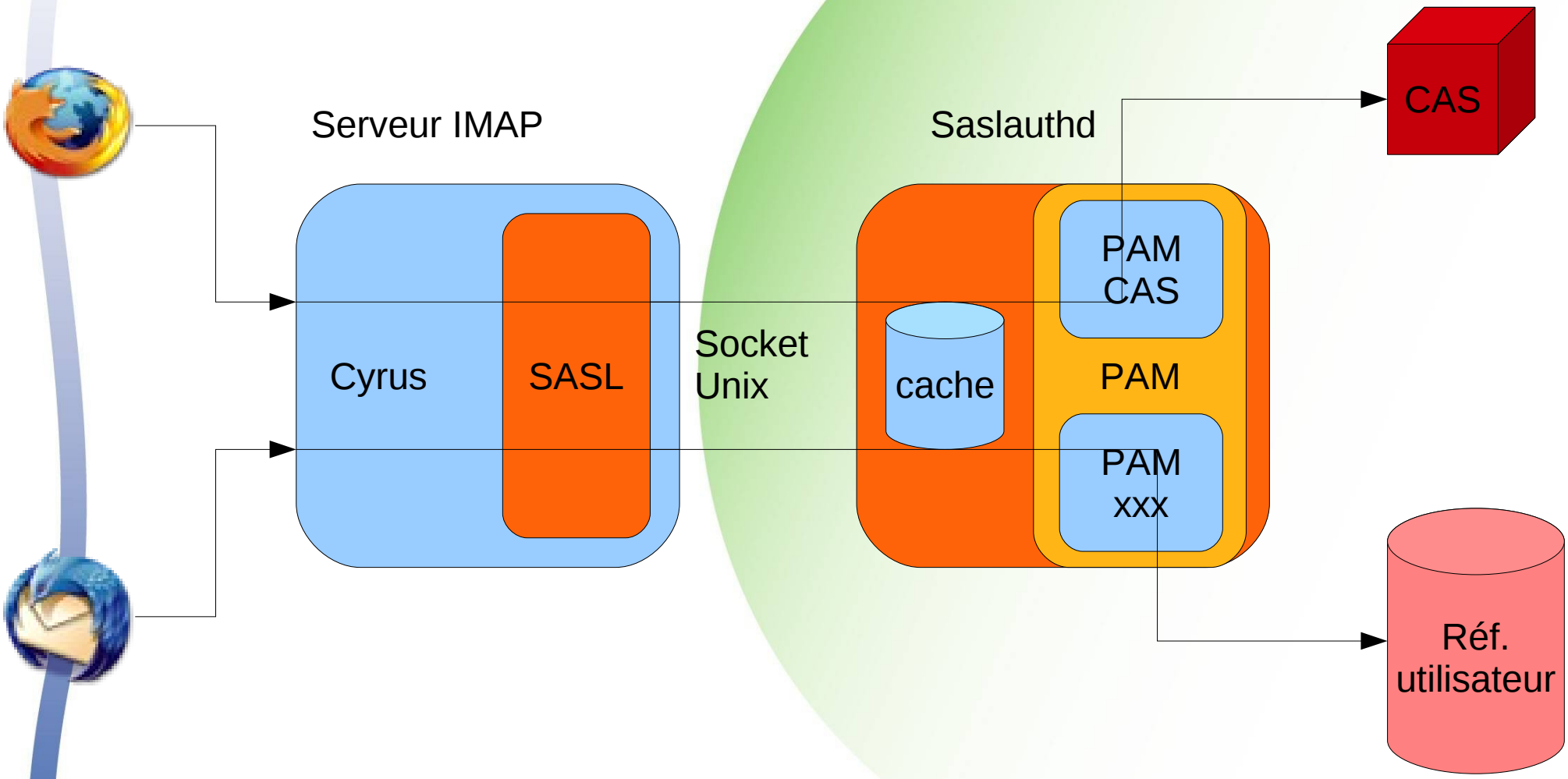
```
...
sasl_pwcheck_method: saslauthd
sasl_mech_list: PLAIN
...
```

cyrus – saslauthd (3)

- Un patch permet de le rendre capable de conserver en cache plusieurs mots de passe pour un utilisateur
  - optimise le mécanisme lorsque des sources différentes (ent, webmail, client lourd) génèrent en parallèle des requêtes IMAP, avec chacune un mot de passe différent:

http://www.esup-portail.org/display/PROJPAMCAS/03+-+patch+saslauthc

Schéma Cyrus- saslauthd



pam_ccreds

- module pam qui permet de cacher les mots de passe
- développé par PADL Software.

```
auth sufficient /lib/security/pam_ccreds.so action=validate
    service_specific
auth [success=ok new_authtok_reqd=ok ignore=done default=die]
    /lib/security/pam_cas.so -sftp://srvftp.univ-rennes1.fr
    -f/etc/pam_cas.conf
auth optional /lib/security/pam_ccreds.so action=store service_specific

account sufficient /lib/security/pam_ldap.so config=/etc/ldap.conf
```

imapproxy

- C'est une solution utilisée par certains établissements, qui semble donner satisfaction.
  - http://shib.kuleuven.be/docs/horde3-cas/proxyCAS.pdf
  - http://shib.kuleuven.be/docs/horde3-cas/
  - http://wiki.horde.org/CASAuthHowTo

Integration CAS Client messagerie

Cassification de Horde / IMP

- Horde: http://horde.org
  - Framework d'application
  - IMP, Turba, Kronolith, Ingo, Nag ....
- adapter le webmail (en l'occurrence, IMP) en lui donnant les fonctionnalités de mandataire (proxy) CAS.
  - librairie phpCAS (v 1.0 actuellement) http://www.ja-sig.org/wiki/display/CASC/phpCAS
- Adaptation réalisé par Esup:
  - Horde 3.x: packagé ESUP
  - Nouvelle version de Horde: Horde Webmail Edition
    - Documentation d'accompagnement de la cassification
  - Projet Horde ESUP: http://www.esup-portail.org/x/IIDg

Configuration Package Horde-esup

Fichier esup.properties

```
################################
# APPLICATION TO USE
################################
IMP_USE=1
INGO_USE=1
KRONOLITH_USE=1
MNEMO_USE=1
NAG_USE=1
TURBA_USE=1
CAS_USE=1
```

.../...

```
################################
# VERSION OF DISTRIB
################################
HORDE_VER=3.1.3
IMP_VER=h3-4.1.3
INGO_VER=h3-1.1.1
KRONOLITH_VER=h3-2.1.2
MNEMO_VER=h3-2.1
NAG_VER=h3-2.1.1
TURBA_VER=h3-2.1.2
```

.../...

Configuration Package Horde-esup (2)

```
#################################
# HORDE FTP URL
#################################
HORDE_FTP_URL=
http://ftp.horde.org/pub

#################################
# FOLDER CONFIG
#################################
BUILD_DIR=build
PACKAGE_DIR=packages
PATCH_DIR=PatchEsup
PERSO_DIR=Custom
UPDATES_DIR=UpdateEsup
DEPLOY_DIR=/var/www/webetu
```

```
#################################
# DB
#################################
DB_TYPE=mysql
DB_HOST=localhost
DB_USERNAME=xxxxxx
DB_PASS=xxxxx
DB_NAME=horde_etu
DB_PORT=3306
```

Configuration Package Horde-esup (3)

```
############################
# MAIL
############################
SMTPHOST=cyrus.univ-valenciennes.fr
MAIL_SERVER_NAME=eiger.univ-valenciennes.fr
MAIL_SERVER_PORT=143
MAIL_DOMAIN=meletu.univ-valenciennes.fr
MAIL_PROTO=imap/notls

############################
# LDAP
############################
LDAP_HOST=ldap2.univ-valenciennes.fr
LDAP_PORT=389
LDAP_BASEDN=ou=people,dc=univ-valenciennes,dc=fr
LDAP_BINDDN=
LDAP_BINDPASS=
LDAP_UID_KEY=uid
```

```
##############################
# CAS
##############################
CAS_HOST=cas.univ-valenciennes.fr
CAS_PORT=443
CAS_PATH=/cas
CAS_PROXY=https://wepers.
univ-valenciennes.fr/casProxy.php
CAS_LOGOUT=true
CAS_DEBUG=false
```

Configuration Package Horde-esup (4)

```
############################
# LOG
############################
LOG_LEVEL=E_ERROR
LOG_FILE=/tmp/horde_etu.log

############################
# MISC
############################
ADMIN_USERS=('admin','ffarenea')
URL_HORDE=/
KRONOLITH_REMINDER= rappel@univ-valenciennes.fr
```

./build.sh esup.clean

./build.sh esup.getcomponents

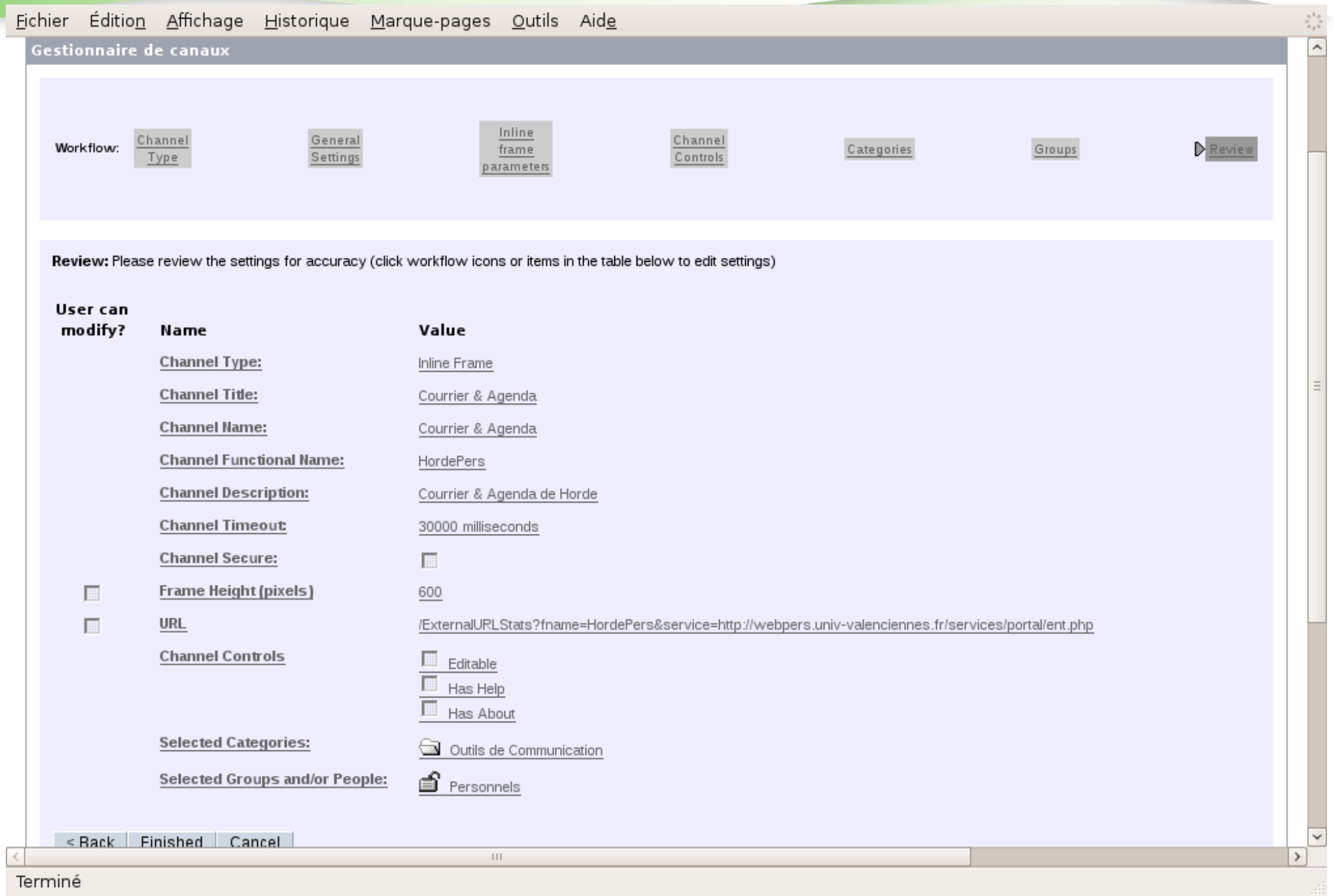
./build.sh esup.init

./build.sh esup.db.init

./build.sh esup.deploy

Integration portail - Iframe

Integration portail - Iframe



Integration portail – Canal Imap

webmail

Votre messagerie

Dossier	Nombre de mail(s) non lu(s)	Nombre total de mail(s)
Réception	11	23
Brouillons	0	1
Corbeille	9	10
Envoye	0	20
Florent	0	1

Fermer le d?tail | Actualiser

Canal IMAP - CIMAP

« Ce canal permet d'afficher le contenu de la boite imap d'un utilisateur et de ses sous-dossiers, et éventuellement de renvoyer vers l'url de l'utilisateur sur le webmail de l'établissement. »

http://www.esup-portail.org/x/WYAc

Téléchargement:

- http://sourcesup.cru.fr/frs/?group_id=205&release_id=694

Canal IMAP - Configuration

Fichier Cimap.xml:

```
<?xml version="1.0"?>
<!DOCTYPE CanalMail SYSTEM "CImap.dtd">

<Server
    key="PERS"
    hostname="eiger.univ-valenciennes.fr"
    port="143"
    protocole="imap"
    description="Serveur de messagerie du personnel"
    inboxName="INBOX"
    inboxLocalName="Reception"
    urlWebmail="https://webpers.univ-valenciennes.fr/imp/mailbox.php?mailbox=%m"
     />
```

Canal IMAP – Configuration (2)

```
<Attachements>
    <Group
      key="Personnels"
      serverKey="pers"
      description="Les Personnels "
    />
     <Attribut
      key="mail"
      value=".*@univ-valenciennes\.fr"
      serverKey="PERS"
      description="Personnels "
    />
  </Attachements>
</CanalMail>
```

Canal IMAP – Publication

- Publication du canal dans le portail:

User can modify?	Name	Value
	Channel Type:	
	Channel Title:	webmail
	Channel Name:	webmail
	Channel Functional Name:	webmail
	Channel Description:	webmail
	Channel Timeout:	100000 milliseconds
	Channel Class:	org.esupportail.portal.channels.CImap.CImap
☑	**Parameter:**	serverKey = pers
	Channel Controls	☐ Editable ☐ Has Help ☐ Has About
	Selected Categories:	Applications
	Selected Groups and/or People:	Everyone