OpenLDAP/Kerberos à l'IMB et l'ISM

Sylvain Allemand, Philippe Aurel

Octobre 2024

Contexte de l'IMB

L'institut de Mathématiques de Bordeaux :

- 300 utilisateurs
- environ 200 postes fixes (diskless) sous Linux
- des services : fichiers, mail, impressions (papercut), applications web (webmail sogo, GLPI, etc.)

Services utilisés à l'IMB

- Kerberos : Service d'authentification
- OpenLDAP : Service d'annuaire
  - Utilisateurs / Groupes
  - Objets divers... (clé SSH, configuration VPN, etc.)
- Objectifs : s'appuyer un maximum sur ce que fournit l'Université

Contexte Pôle Modélisation ISM

Les utilisateurs

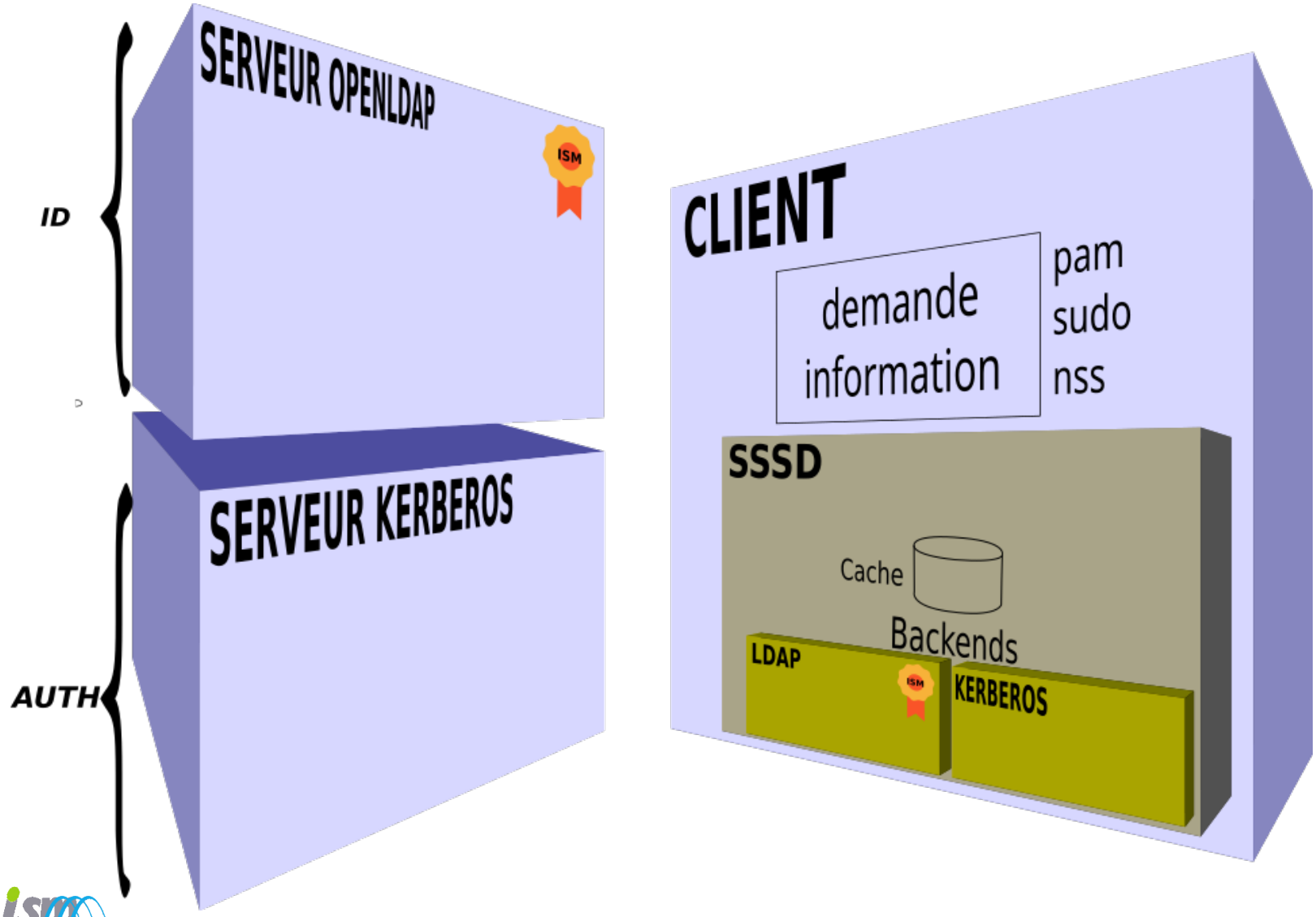
- 42 permanents
- 5 extérieurs
- 14 doctorants
- 48 étudiants

soit une centaine d'utilisateurs.

Les machines

- 1 cluster de calcul
- 27 postes de travail
- 4 serveurs de stockage
  - 2 stockages
  - 2 sauvegardes

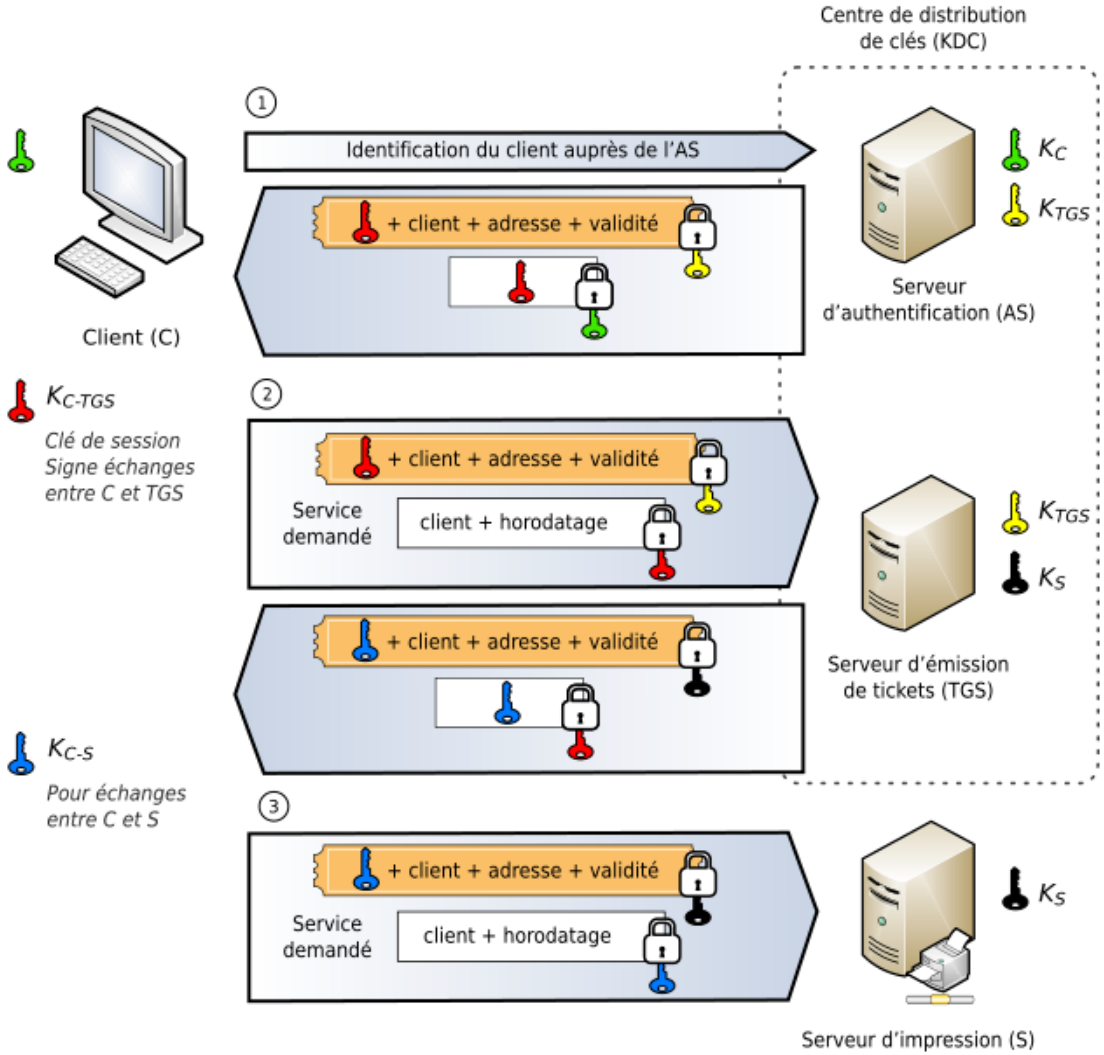
Le fonctionnement de SSSD



Kerberos

Authentifier les utilisateurs avec Kerberos

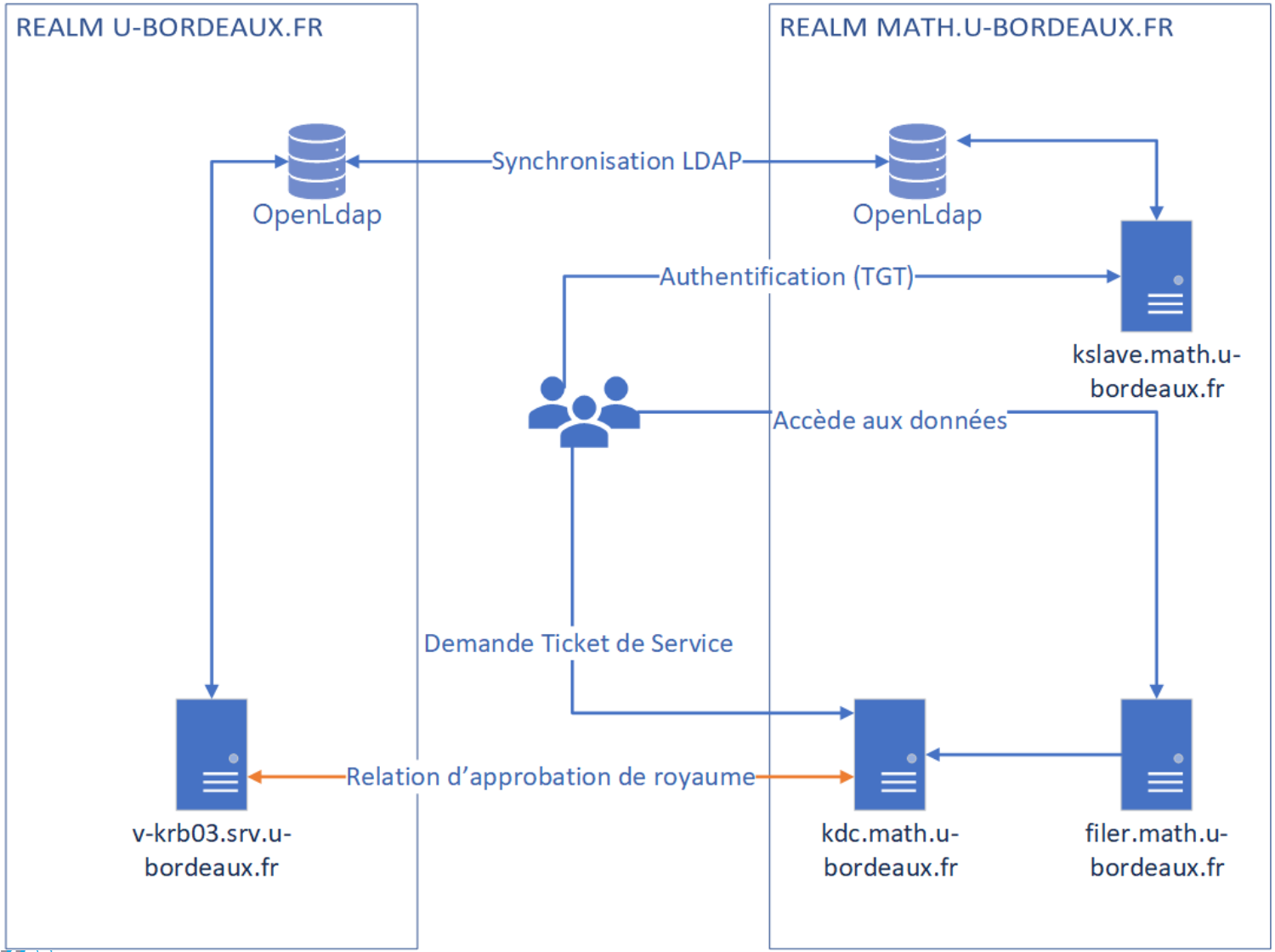
Kerberos


Centre de distribution de clés (KDC)
1
Identification du client auprès de l'AS
+ client + adresse + validité
Client (C)
Serveur d'authentification (AS)
K_C
K_{TGS}
$K_{C\text{-}TGS}$
Clé de session
Signe échanges entre C et TGS
2
+ client + adresse + validité
Service demandé
client + horodatage
Serveur d'émission de tickets (TGS)
K_{TGS}
K_S
$K_{C\text{-}S}$
Pour échanges entre C et S
3
Service demandé
Serveur d'impression (S)

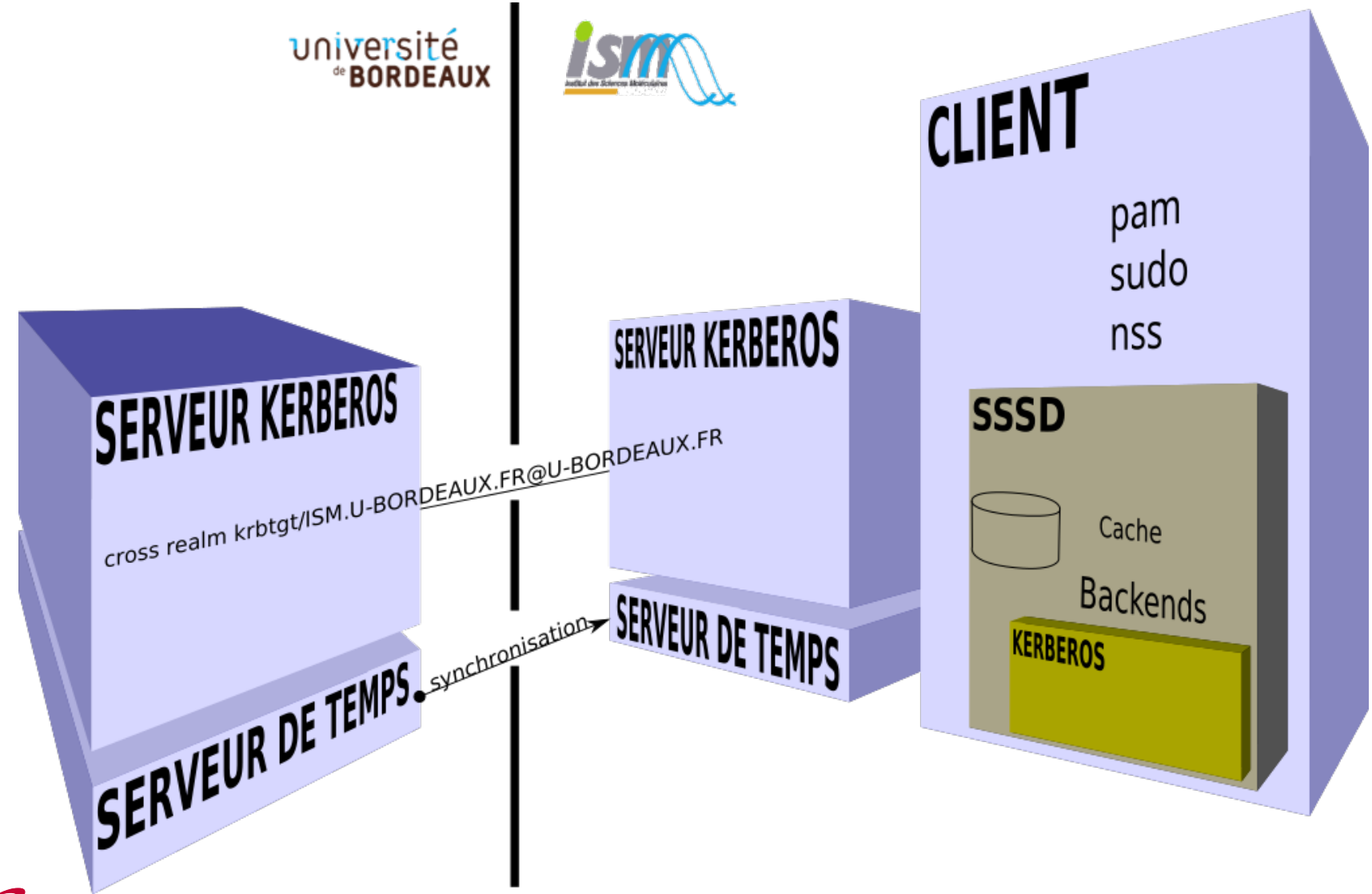
Points clé de Kerberos :

- la sécurité se joue sur le KDC et les utilisateurs
- chaque utilisateur, hôte et service est authentifié
  - salleman@U-BORDEAUX.FR
  - host/machine@MATH.U-BORDEAUX.FR
  - nfs/serveur@MATH.U-BORDEAUX.FR
- le réseau peut être "non-fiable" : le mot de passe ne circule pas, tout est chiffré

Kerberos à l'IMB



Kerberos à l'ISM CROSS-REALM



OpenLDAP

Obtenir les informations sur l'utilisateur avec OpenLDAP

OpenLDAP de l'Université

```
$ ldapsearch -LLL -W -H ldaps://ldap0.srv.u-bordeaux.fr -
    Dcn=imb,ou=admin,dc=u-bordeaux,dc=fr -b dc=u-bordeaux,
    dc=fr uid=salleman

dn: uid=salleman,ou=people,dc=u-bordeaux,dc=fr
uid: salleman
mail: sylvain.allemand@u-bordeaux.fr
ubxDateFinValidite: 0
eduPersonPrimaryAffiliation: staff
ubxStatutCompte: ACTIF
cn: Allemand Sylvain
givenName: Sylvain
sn: Allemand
displayName: Sylvain Allemand
[...]
```

OpenLDAP de l'IMB

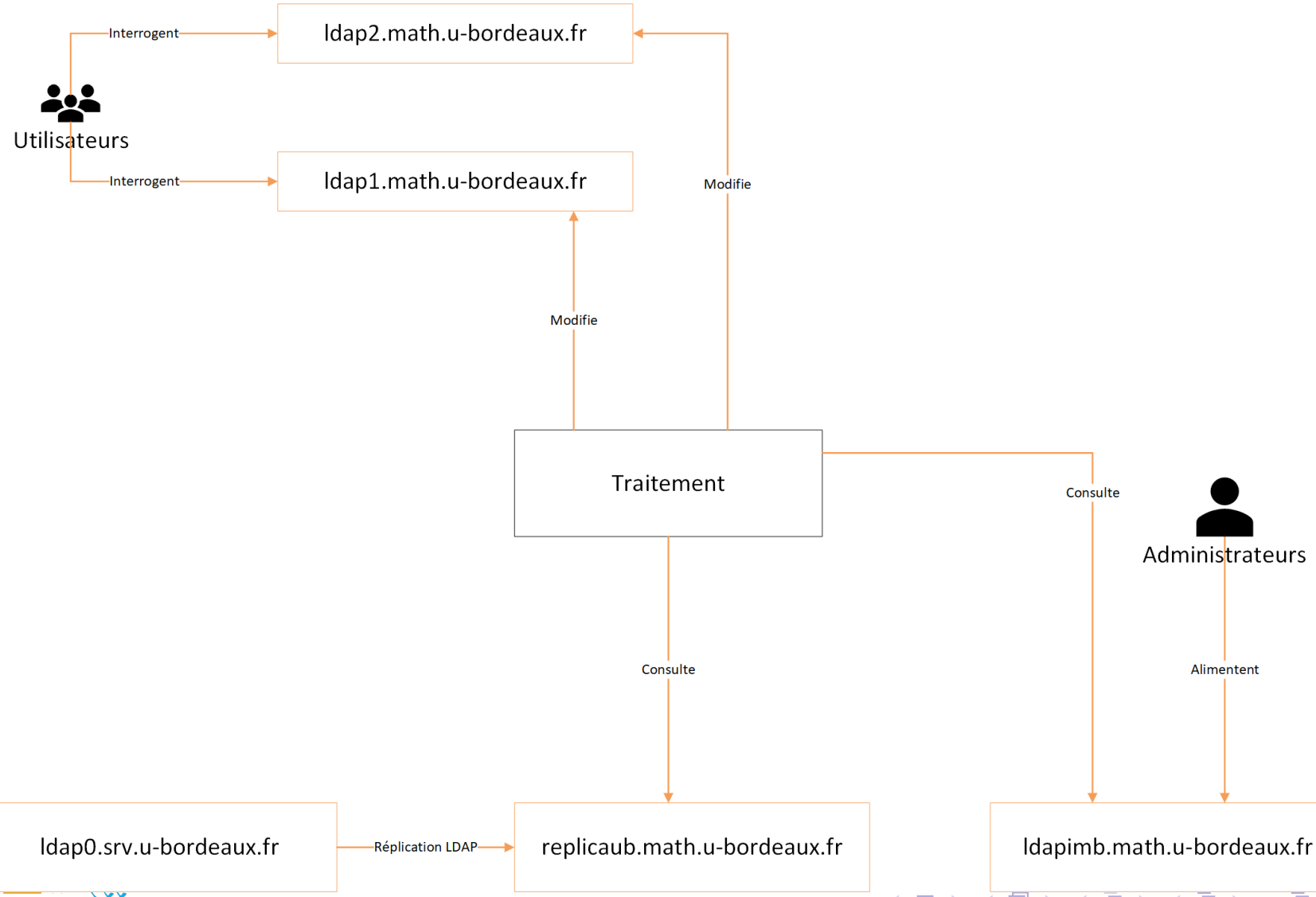
```
$ ldapsearch -LLL -x -H ldap://ldapimb -b dc=u-bordeaux,dc
    =fr uid=salleman

dn: uid=salleman,ou=people,dc=u-bordeaux,dc=fr
mailAlternateAddress: Sylvain.Allemand@math.u-bordeaux.fr
loginShell: /bin/bash
gidNumber: 10003
homeDirectory: /home/imb/salleman
uidNumber: 10003
uid: salleman
[...]
```

OpenLDAP - Fusion

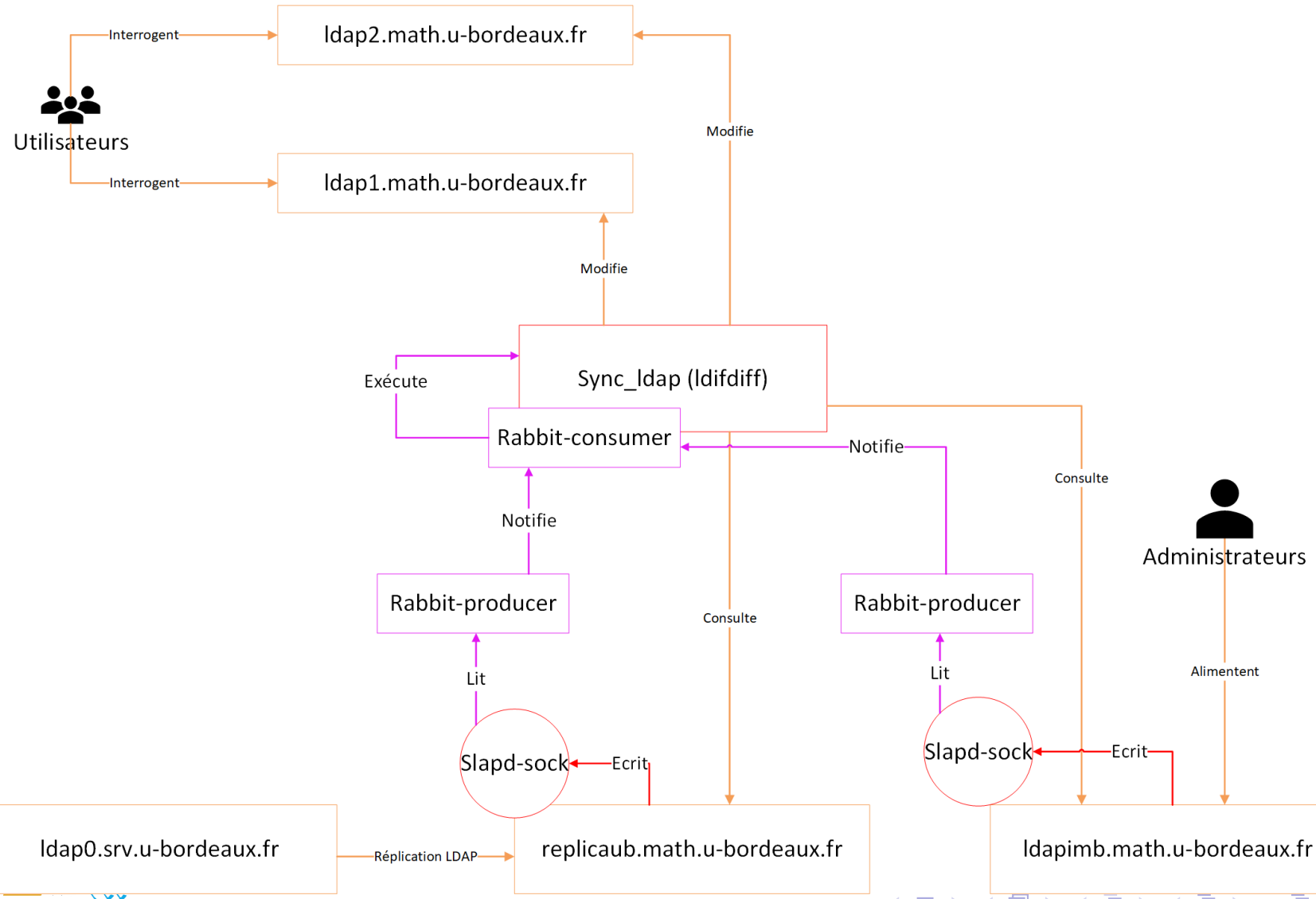
Comment fusionner les deux annuaires ?

- Combo overlay translucent + backend meta
  - Overlay translucent proxy : surcharger un annuaire distant avec des infos d'un annuaire local
  - Backend meta : proxy ldap permettant de fusionner le résultat de plusieurs annuaires
- outil ldifdiff

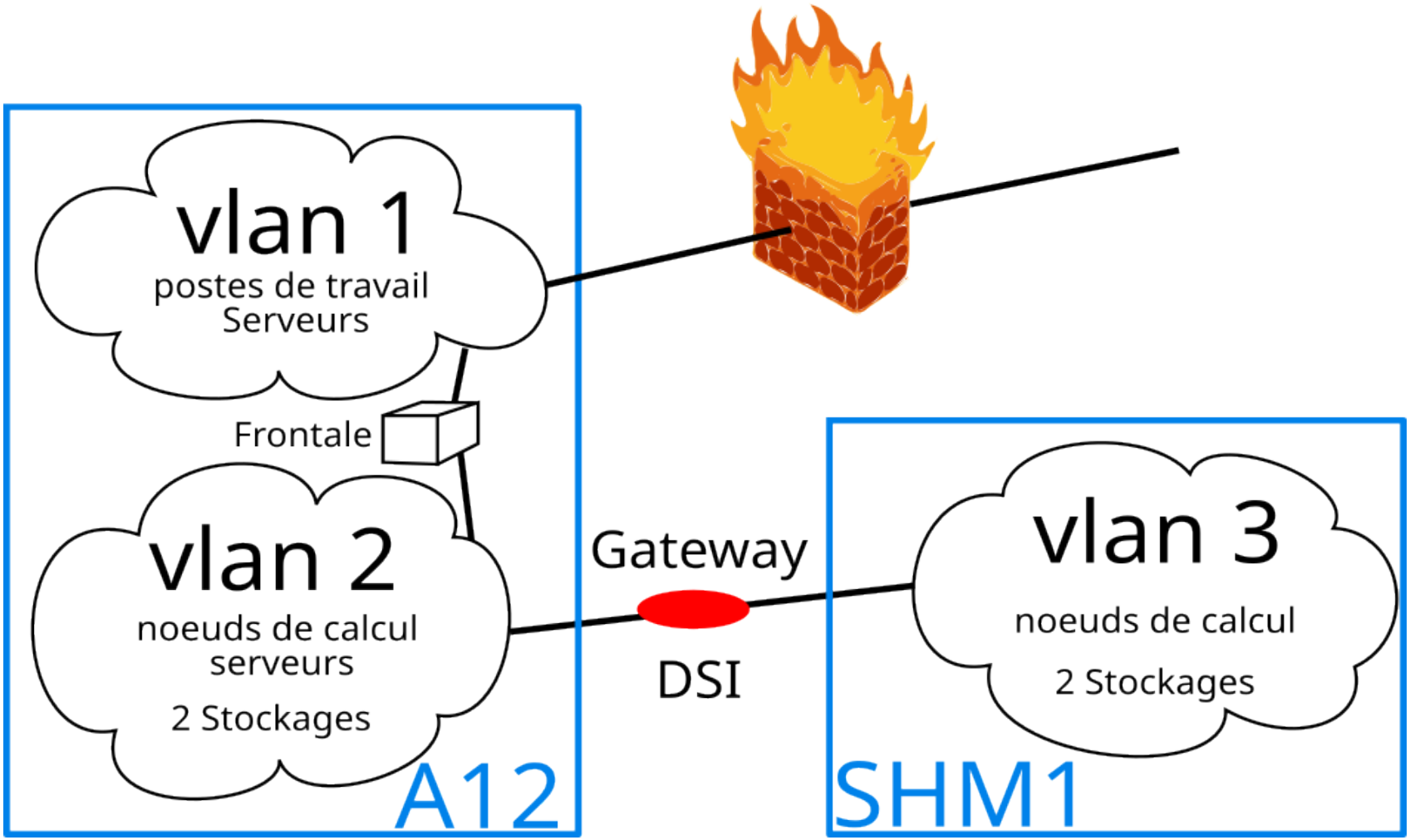
OpenLDAP à l'IMB - ldifdiff



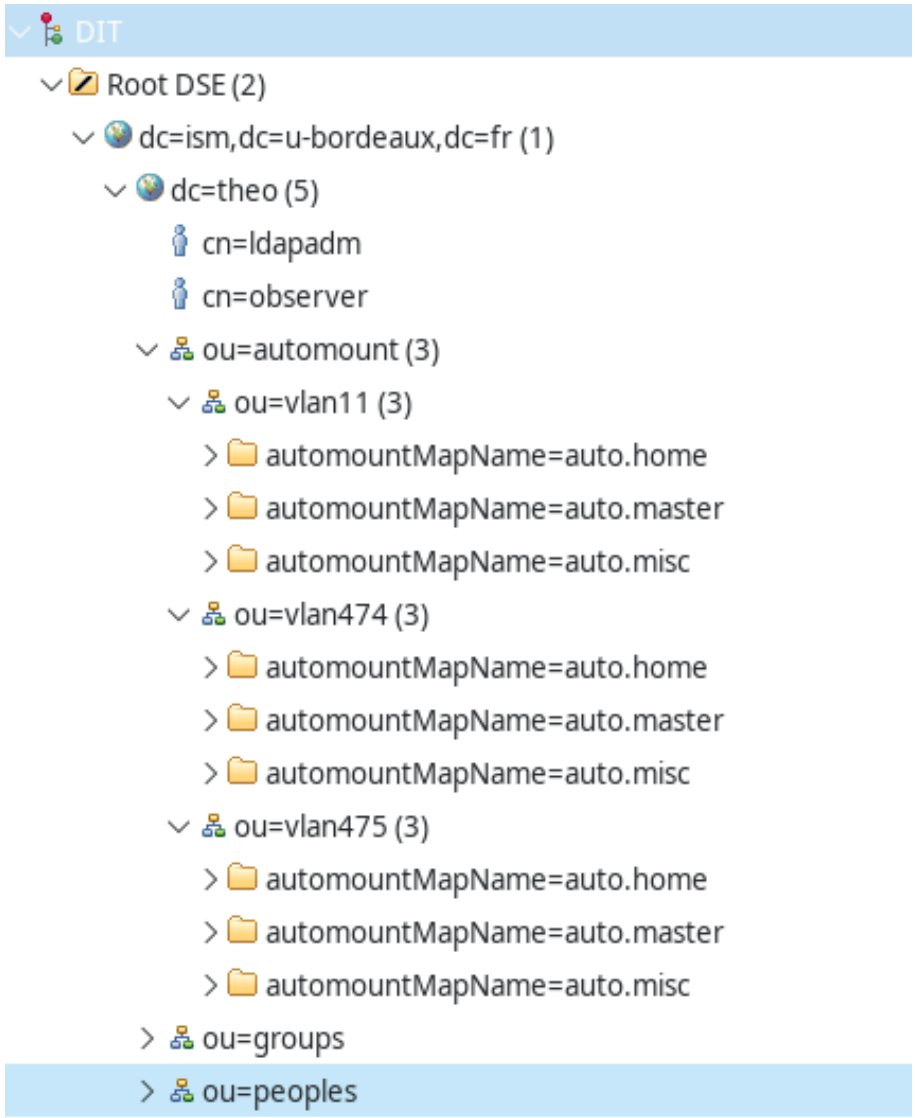
OpenLDAP à l'IMB - Ajout de RabbitMQ



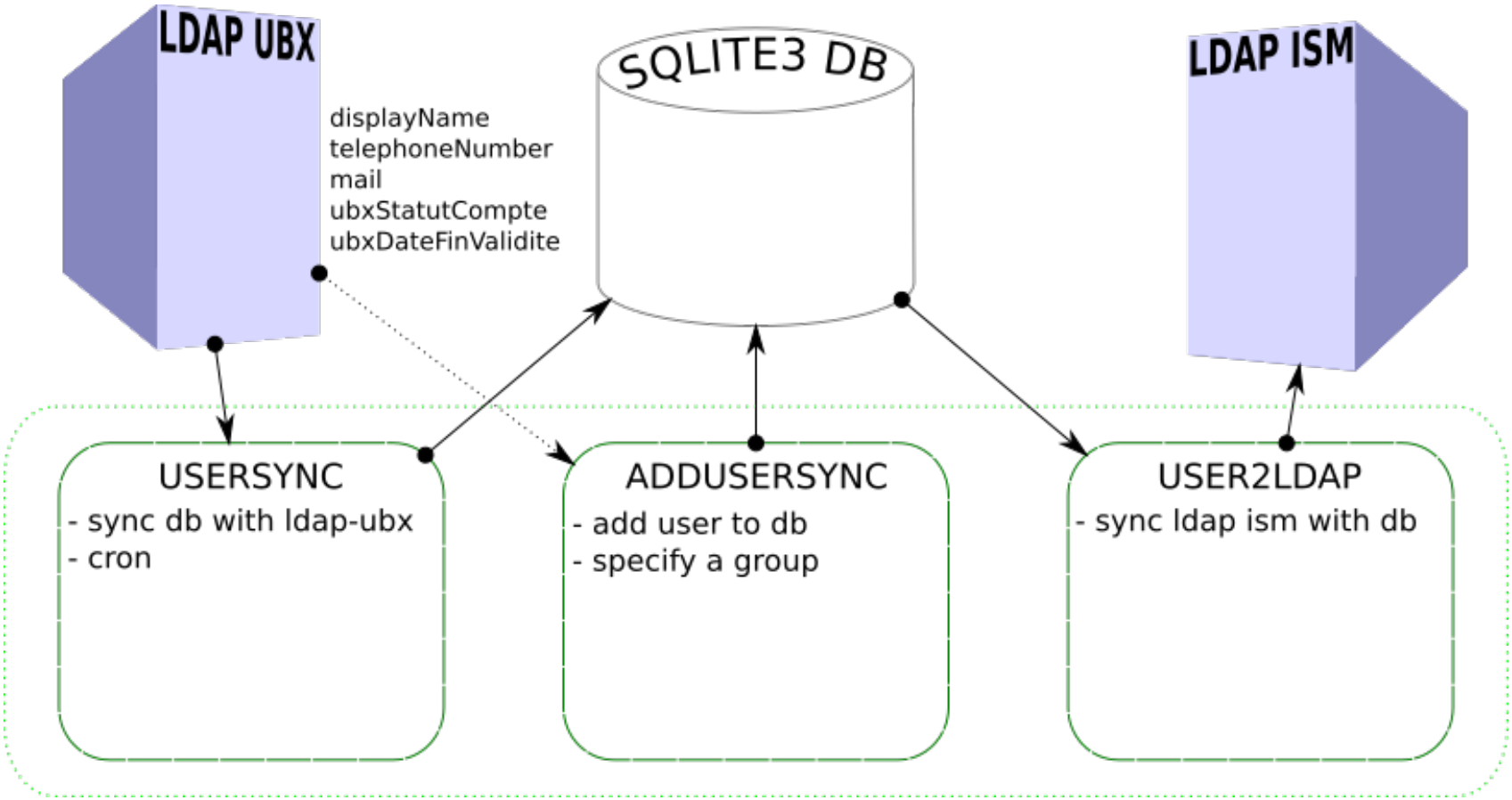
OpenLDAP à l'ISM - Problématique VLAN



OpenLDAP à l'ISM - Problématique VLAN



OpenLDAP à l'ISM - usersync pour approvisionner le ldap



Déploiement des solutions à l'IMB

- Kerberos installé par la DSI après mise à disposition d'une VM avec accès SSH
- LDAPs sous forme de containers, déployés avec Ansible

Configuration des clients avec SSSD à l'IMB

```
$ cat /etc/sssd/sssd.conf
[sssd]
config_file_version = 2
domains = math.u-bordeaux1.fr

[domain/math.u-bordeaux1.fr]
id_provider = ldap
ldap_uri = ldap://ldap1.math.u-bordeaux1.fr,ldap://ldap2.
    math.u-bordeaux1.fr
ldap_search_base = dc=u-bordeaux,dc=fr
auth_provider = krb5
krb5_server = kslave.math.u-bordeaux1.fr,v-krb03.srv.u-
    bordeaux.fr,v-krb04.srv.u-bordeaux.fr
krb5_realm = U-BORDEAUX.FR
krb5_validate = True
cache_credentials = True
```

Configuration Kerberos des clients à l'IMB

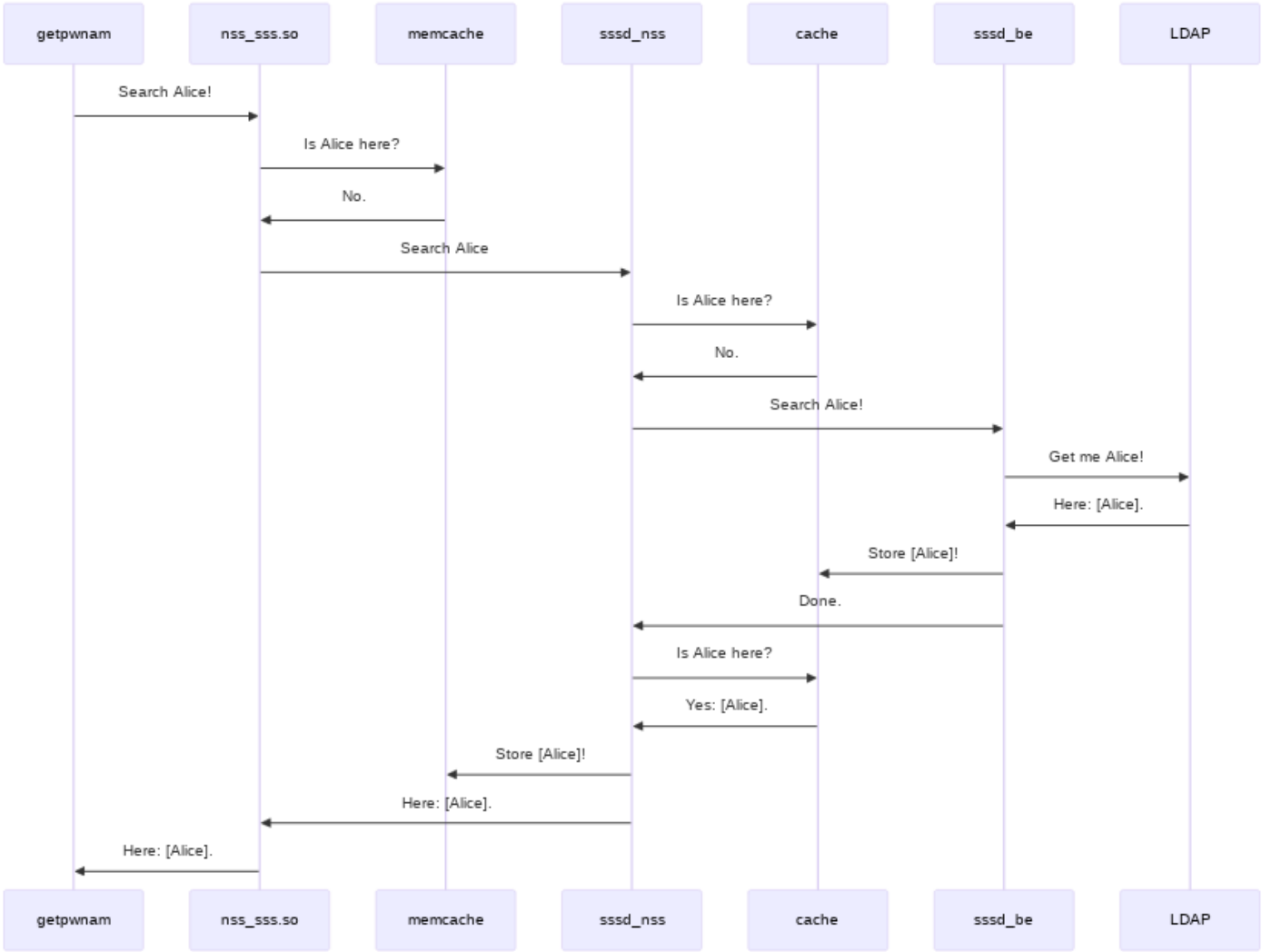
```
$ cat /etc/krb5.conf
[libdefaults]
        default_realm = U-BORDEAUX.FR

[realms]
        MATH.U-BORDEAUX1.FR = {
                kdc = kdc.math.u-bordeaux1.fr
                admin_server = kdc.math.u-bordeaux1.fr
        }
        U-BORDEAUX.FR = {
            kdc = kslave.math.u-bordeaux1.fr
                kdc = v-krb03.srv.u-bordeaux.fr
                kdc = v-krb04.srv.u-bordeaux.fr
        }
```

Déploiement des solutions à l'ISM

- Le serveur kerberos est une image KVM sous debian installée en 2013.
- Serveurs LDAPS déployés avec un playbook Ansible sur des images KVM Rocky9 et Debian12.
- La configuration sssd, serveur de temps, certificats et kerberos est déployée via:
  - un playbook ansible.
  - un preseed ou kickstart lors de l'installation.
- TODO:déploiement du monitoring des services avec telegraf, influxdb via playbook ansible.

Questions ?

fonctionnement cache sssd



Log Heimdal

```
# NFS service beetween nfs server and nfs client
2024-10-01T09:04:00 AS-REQ nfs/staurel.ism.u-bordeaux.fr@ISM.U-BORDEAUX.FR from IPv4:147.210.56.241 for krbtgt/ISM.U-BORDEAUX.FR@ISM.U-BORDEAUX.FR
2024-10-01T09:04:00 Looking for PK-INIT(ietf) pa-data -- nfs/staurel.ism.u-bordeaux.fr@ISM.U-BORDEAUX.FR
2024-10-01T09:04:00 Looking for PK-INIT(win2k) pa-data -- nfs/staurel.ism.u-bordeaux.fr@ISM.U-BORDEAUX.FR
2024-10-01T09:04:00 Looking for ENC-TS pa-data -- nfs/staurel.ism.u-bordeaux.fr@ISM.U-BORDEAUX.FR
2024-10-01T09:04:00 AS-REQ nfs/staurel.ism.u-bordeaux.fr@ISM.U-BORDEAUX.FR from IPv4:147.210.56.241 for krbtgt/ISM.U-BORDEAUX.FR@ISM.U-BORDEAUX.FR
2024-10-01T09:04:00 Looking for PK-INIT(ietf) pa-data -- nfs/staurel.ism.u-bordeaux.fr@ISM.U-BORDEAUX.FR
2024-10-01T09:04:00 Looking for PK-INIT(win2k) pa-data -- nfs/staurel.ism.u-bordeaux.fr@ISM.U-BORDEAUX.FR
2024-10-01T09:04:00 Looking for ENC-TS pa-data -- nfs/staurel.ism.u-bordeaux.fr@ISM.U-BORDEAUX.FR
2024-10-01T09:04:00 ENC-TS Pre-authentication succeeded -- nfs/staurel.ism.u-bordeaux.fr@ISM.U-BORDEAUX.FR using aes256-cts-hmac-sha1-96
2024-10-01T09:04:00 ENC-TS pre-authentication succeeded -- nfs/staurel.ism.u-bordeaux.fr@ISM.U-BORDEAUX.FR
2024-10-01T09:04:00 TGS-REQ nfs/staurel.ism.u-bordeaux.fr@ISM.U-BORDEAUX.FR from IPv4:147.210.56.241 for nfs/gritche.ism.u-bordeaux.fr@ISM.U-BORDEAUX.FR [canonicalize, forwardable]

# connection to host with paurel
2024-10-01T09:32:48 TGS-REQ paurel@U-BORDEAUX.FR from IPv4:147.210.56.241 for host/staurel.ism.u-bordeaux.fr@ISM.U-BORDEAUX.FR [forwardable]
2024-10-01T09:32:48 Client not found in database: no such entry found in hdb
2024-10-01T09:32:48 cross-realm U-BORDEAUX.FR -> ISM.U-BORDEAUX.FR
2024-10-01T09:32:48 TGS-REQ authtime: 2024-10-01T09:32:48 starttime: 2024-10-01T09:32:48 endtime: 2024-10-02T09:32:48 renew till: unset
2024-10-01T09:32:48 sending 692 bytes to IPv4:147.210.56.241
```

Diagramme de base de donnée