Séminaire EOLE
Dijon
19-20 octobre 2010

Réplication d'annuaire centralisée

Plan

- Technique de la réplication
- Mise en place sur EOLE
- Bilan et perspectives

Technique de la réplication

Réplication

Définition

La réplication est un mécanisme de copie automatique continue et permanente d'une base de données abritée sur un serveur vers au moins un autre.

Source : http://jargonf.org

Réplication

Cas d'utilisation

- remplacement immédiat du serveur principal en cas une panne
- parallélisation de l'exécution des requêtes de consultation et de modification
- rapprochement de l'utilisateur et des données consultées

Source : http://jargonf.org

Réplication

Réplication LDAP

Il est possible de répliquer tout ou partie d'un annuaire ldap vers un autre en choisissant les branches et les éléments (filtre) à répliquer.

Réplication

OpenLdap ≤ 3.3

Mécanisme : **slurpd**
Système : maître/esclave

Prérequis :
- compte en lecture sur le maître
- copier l'annuaire du maître sur l'esclave
- le maître doit connaître l'esclave
  (section : replica)

Réplication

OpenLdap ≥ 3.4

Mécanisme : **syncrepl** (LDAP Sync Replication engine)
Système : client/fournisseur

Prérequis :
- compte en lecture sur le fournisseur
- fournisseur configuré pour la réplication
  (module syncprov et activation du lastmod)

Réplication

Avantages de syncrepl

- plus robuste et mieux intégré que slurpd
  (mécanisme de reprise...)

- possibilité d'architectures complexes
  (mode multi-master,...)

Réplication

Modes de synchronistation

- **refreshOnly** : le client vient chercher les mises à jour à intervalles réguliers (pull)

- **refreshAndPersist** : le client initialise la synchronisation et ensuite, le fournisseur le contacte à chaque modification (pull and push)

Réplication

Sur Eole-2.2

OpenLdap 2.4 à partir d'Ubuntu 8.04 LTS

Paquet **openldap 2.4.11** recompilé par EOLE

Mise en place sur EOLE

Réplication EOLE

Idée de départ

Un annuaire Scribe contient les comptes :

- élèves
- enseignants
- personnels administratifs
- responsables légaux

=> Tous ces comptes pourraient être centralisés en répliquant les annuaires établissement sur un serveur (Seshat)

Réplication EOLE

Utilité

Créer un méta-annuaire établissement pour :

- centraliser l'authentification
- mettre en place des applications centralisées
- mettre en place la fédération d'identité

Réplication EOLE

Remarque

Possibilité de doublons sur les login, mais :

- unicité des couples numéro établissement/login
- possibilité d'utiliser un autre attribut
  (ex : ENTPersonLogin)

Réplication EOLE

Prérequis réseau

- le serveur Seshat doit accéder au port ldap (389) du Scribe

- Idéalement, le Scribe devrait pouvoir accéder au port ldap du Seshat (réplication temps réél)

Réplication EOLE

Prérequis Seshat

Seshat est nativement configuré pour être client de réplication ldap.

Réplication EOLE

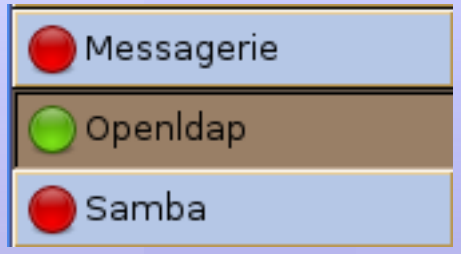
Prérequis Scribe (1/3)

Etre à jour, en particulier en ce qui concerne le paquet **slapd** :

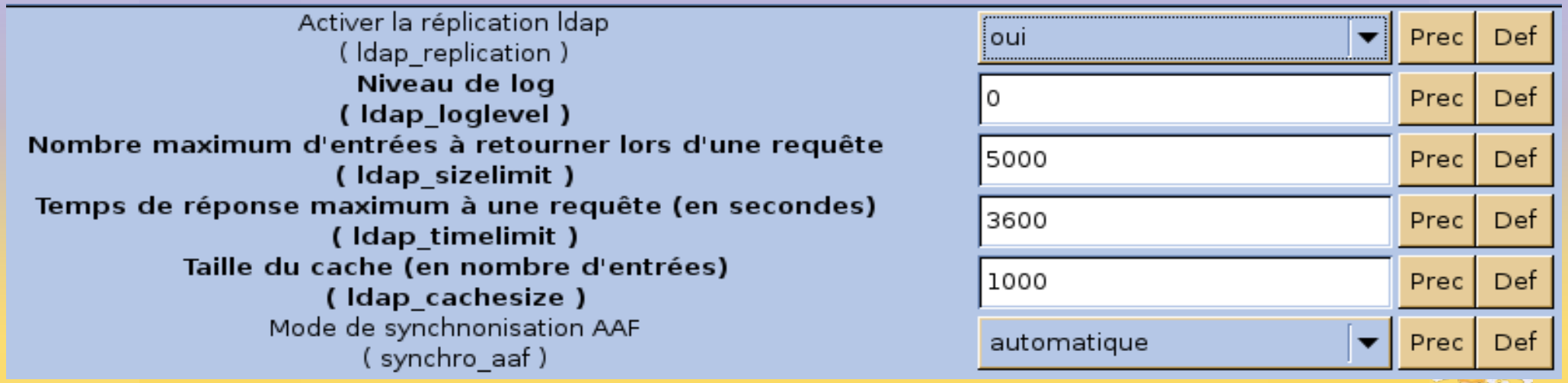
```
root@scribe7:~# dpkg -l slapd
Desired=Unknown/Install/Remove/Purge/Hold
| Status=Not/Installed/Config-f/Unpacked/Failed-cfg/Half-inst/t-aWait/T-pend
|/ Err?=(none)/Hold/Reinst-required/X=both-problems (Status,Err: uppercase=bad)
||/ Nom                  Version              Description
+++-====================-====================-===================================
ii  slapd                2.4.11-1eole2        OpenLDAP server (slapd)
root@scribe7:~#
```

Réplication EOLE

Prérequis Scribe (2/3)



Activer la réplication ldap dans l'interface de configuration du module *(onglet OpenLdap en mode expert)*



Réplication EOLE

Prérequis Scribe (3/3)

Le serveur doit avoir été reconfiguré au moins une fois après l'activation de la réplication ldap pour le serveur.

```
root@scribe7:~# reconfigure

*** Début de reconfiguration ***
chargement des paramètres : /etc/eole/dicos/0_scribe.xml
chargement des paramètres : /etc/eole/dicos/1_apache.xml
chargement des paramètres : /etc/eole/dicos/1_bacula.xml
chargement des paramètres : /etc/eole/dicos/1_clamav.xml
```

Réplication EOLE

Répliquer un Scribe (1/4)

Commande à lancer :

/usr/share/eole/active_replication.py

Réplication EOLE

Répliquer un Scribe (2/4)

```
root@scribe7:~# /usr/share/eole/active_replication.py

Sauvegarde de l'annuaire dans /root/annuaire-20101015.ldif

Stopping OpenLDAP: slapd.

Réindexation de l'annuaire

Starting OpenLDAP: slapd.

Création du compte de réplication

Génération de la configuration client
Adresse utilisée pour accéder au Scribe depuis le client
[192.168.230.206] :

Ecriture du fichier /root/replication-0000a.conf

fin
root@scribe7:~#
```

Réplication EOLE

Répliquer un Scribe (3/4)

Copier le fichier généré :

replication-<numero_etab>.conf

Sur le serveur Seshat, dans le répertoire :

/etc/ldap/replication

Réplication EOLE

Répliquer un Scribe (4/4)

Sur Seshat, lancer la commande :

/usr/share/eole/gen_replication.py

Réplication EOLE

Intégration Zéphir

Si les serveurs Scribe et Seshat
sont enregistrés sur le même Zéphir,
celui-ci peut se charger de la mise en place
de la configuration sur le serveur Seshat.

Réplication EOLE

Intégration Zéphir

```
root@scribe:~# /usr/share/eole/active_replication.py

Sauvegarde de l'annuaire dans /root/annuaire-20101015.ldif
```

```
Génération de la configuration client
Adresse utilisée pour accéder au Scribe depuis le client
[10.121.58.5] :

Ecriture du fichier /root/replication-0211227V.conf

Envoi de la configuration sur Zephir

Veuillez saisir votre identifiant Zéphir (rien pour annuler l'envoi) :jojo
Mot de passe pour jojo :

Identifiant Zéphir du serveur de réplication (rien pour annuler l'envoi) :103
Cette configuration sera prise en compte par le serveur
de réplication lors de sa prochaine connexion à Zéphir

fin
```

Réplication EOLE

Intégration Zéphir

Les configurations envoyées via Zéphir sont consultables dans son application web :

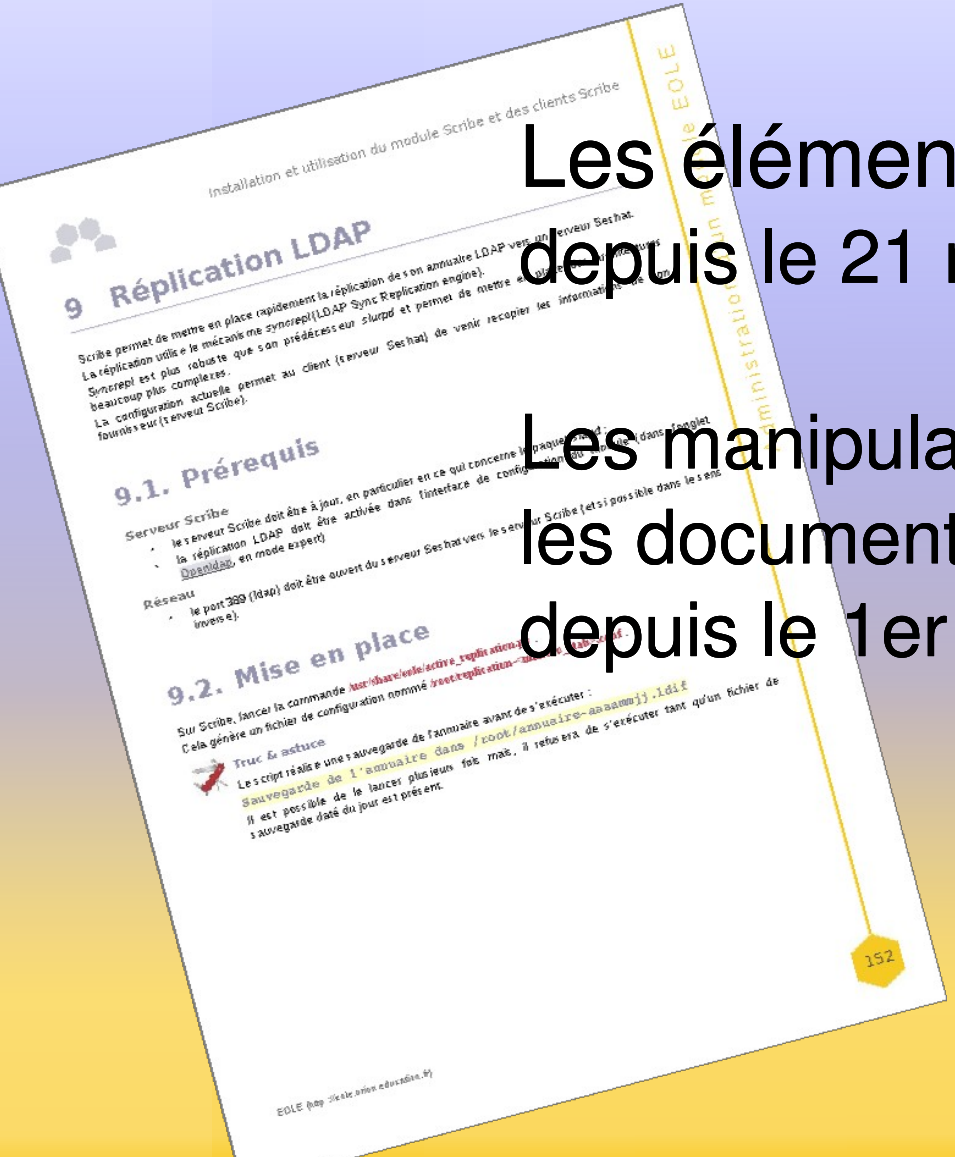
Configurations de réplication LDAP - Seshat Eole (103)

Retour à la page d'état

Fichier(s) de configuration des annuaires à répliquer	
replication-0210017E.conf	Supprimer ce fichier
replication-0211227V.conf	Supprimer ce fichier

Réplication EOLE

Mise à disposition


Installation et utilisation du module Scribe et des clients Scribe

9 Réplication LDAP

Scribe permet de mettre en place rapidement la réplication de son annuaire LDAP vers un serveur Seshat.
La réplication utilise le mécanisme syncrepl (LDAP Sync Replication engine).
Syncrepl est plus robuste que son prédécesseur slurpd et permet de mettre en [illegible]
beaucoup plus complexes.
La configuration actuelle permet au client (serveur Seshat) de venir recopier les informations [illegible]
fournisseur (serveur Scribe).

9.1. Prérequis

Serveur Scribe
- le serveur Scribe doit être à jour, en particulier en ce qui concerne le paquet [illegible] dans l'onglet
- la réplication LDAP doit être activée dans l'interface de config[illegible]
Dansguardian, en mode expert)

Réseau
- le port 389 (ldap) doit être ouvert du serveur Seshat vers le serveur Scribe (et si possible dans le sens inverse).

9.2. Mise en place

Sur Scribe, lancer la commande /usr/share/eole/active_replication[illegible]
Cela génère un fichier de configuration nommé /root/replication-[illegible]

Truc & astuce
Le script réalise une sauvegarde de l'annuaire avant de s'exécuter :
Sauvegarde de l'annuaire dans /root/annuaire-aaaammjj.ldif
Il est possible de le lancer plusieurs fois mais, il refusera de s'exécuter tant qu'un fichier de sauvegarde daté du jour est présent.

152

Les éléments présentés sont disponibles depuis le 21 mai 2010 (maj 2.2.2-02)

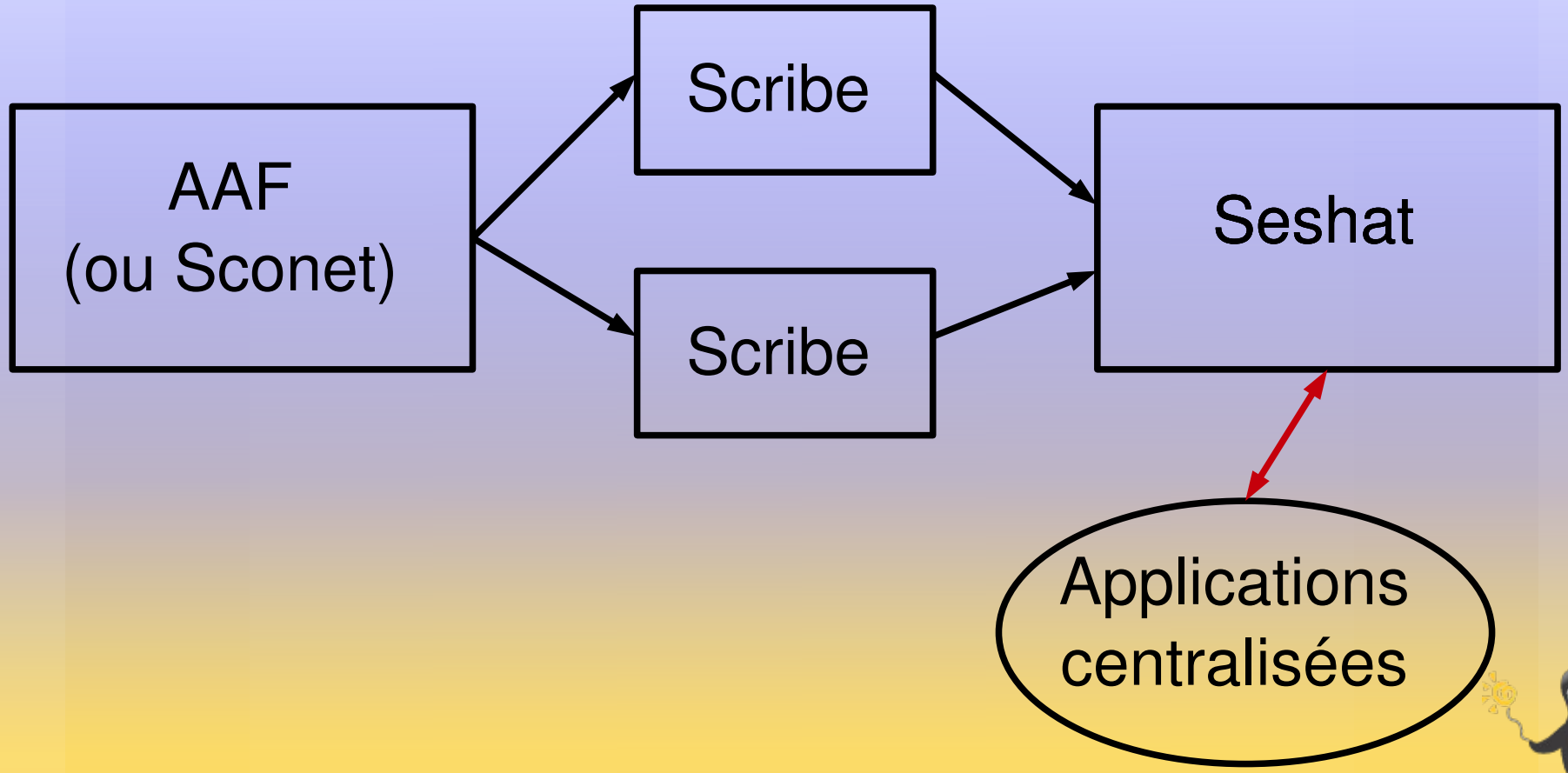
Les manipulations décrites sont incluses dans les documentations officielles *scribe* et *seshat* depuis le 1er juin 2010.

http://eoleng.ac-dijon.fr/documentations/

Bilan et perspectives

Bilan et perspectives

Le schéma actuel



Bilan et perspectives

Perspectives

- étudier la possibilité de fournir des comptes pour les autres établissements sur Seshat

- constitution d'un annuaire de référence académique (gestion des comptes sur Seshat)

Merci de votre attention