Annuaire LDAP, SSO et certificats du CRU à l'Université Paris 1

Fabrice Jammes, Benoît Branciard, Yvonne Girard
et David Chopard-Lallier

Sécurisation du service d'authentification SSO

- Réplication sécurisée d'annuaire LDAP
- Optimisation de la base de données inhérente à LDAP
- Haute disponibilité du serveur SSO CAS

L'université Panthéon-Sorbonne

Une des plus importantes universités de

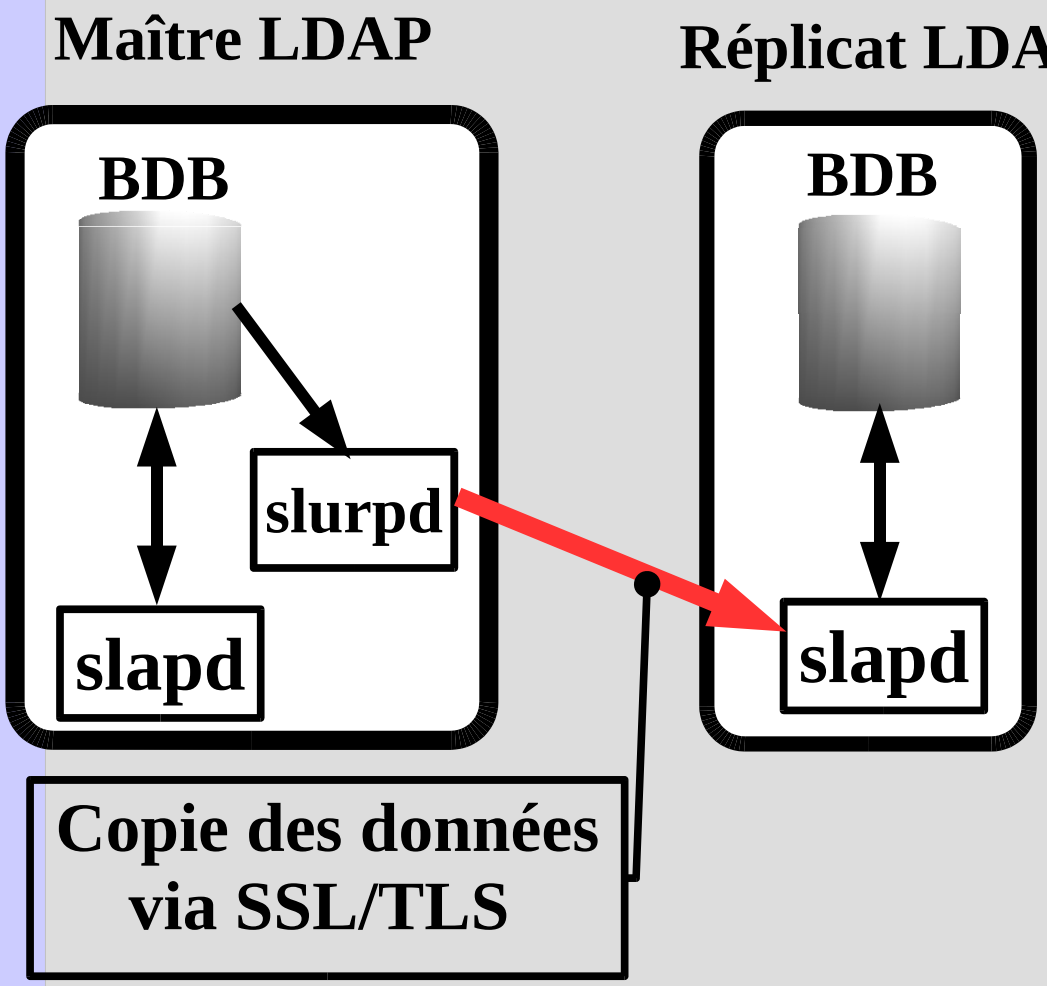
Réplication LDAP sécurisée : pourquoi ?

Mécanismes TLS : authentification du serveur par le client

Client Serveur

Mécanismes TLS : authentification du client par le serveur

Mécanismes TLS appliqués à la réplication LDAP



Attention !

- Le réplicat LDAP est serveur TLS
- Le maître LDAP est client TLS : sa biclé doit supporter des connexions clientes et serveurs.

Configuration d'OpenLDAP et du client LDAP

La configuration d'OpenLDAP pour réplication via TLS est disponible sur **la FAQ du CRU**, à l'adresse :
http://www.cru.fr/faqdata/cache/112.html

Optimisation de BDB

Les fichiers journaux des transactions doivent être sur un disque différent des fichiers de la base :

Dans /var/lib/ldap/DB_CONFIG :

set_lg_dif /espace/bdblogs

Optimisation de BDB

Il est impératif d'insérer régulièrement des

Un outil pour assurer la continuité du service CAS : cas-spare

CAS : pas de système de répartition de charge ou de **reprise sur panne**.

En effet, pour offrir une authentification persistante en cas de panne, on doit partager les tickets CAS entre les serveurs.

cas-spare : bascule entre deux services SSO *(pas d'authentification persistante)*

Gestion des pannes de CAS

Serveur CAS de secours

Panne du CAS principal

Les solutions concurrentes

- Heartbeat-drdb : solution générique de reprise sur panne.
- CCC avec Jgroups : réplication des tickets entre les serveurs CAS.
- BDD stockants les tickets : à implémenter
- Signature des tickets afin qu'ils soient reconnus par un ensemble de serveurs
- Insérer le nom du serveur CAS dans le ticket : utile uniquement pour la répartition de charge.

UNIVERSITÉ PARIS 1 – PANTHÉON - SORBONNE –

Mise en place d'un service SSO sécurisé

LDAP

LDAP et CAS sur la même
ile

Mécanismes de reprise sur panne avec cas-spare

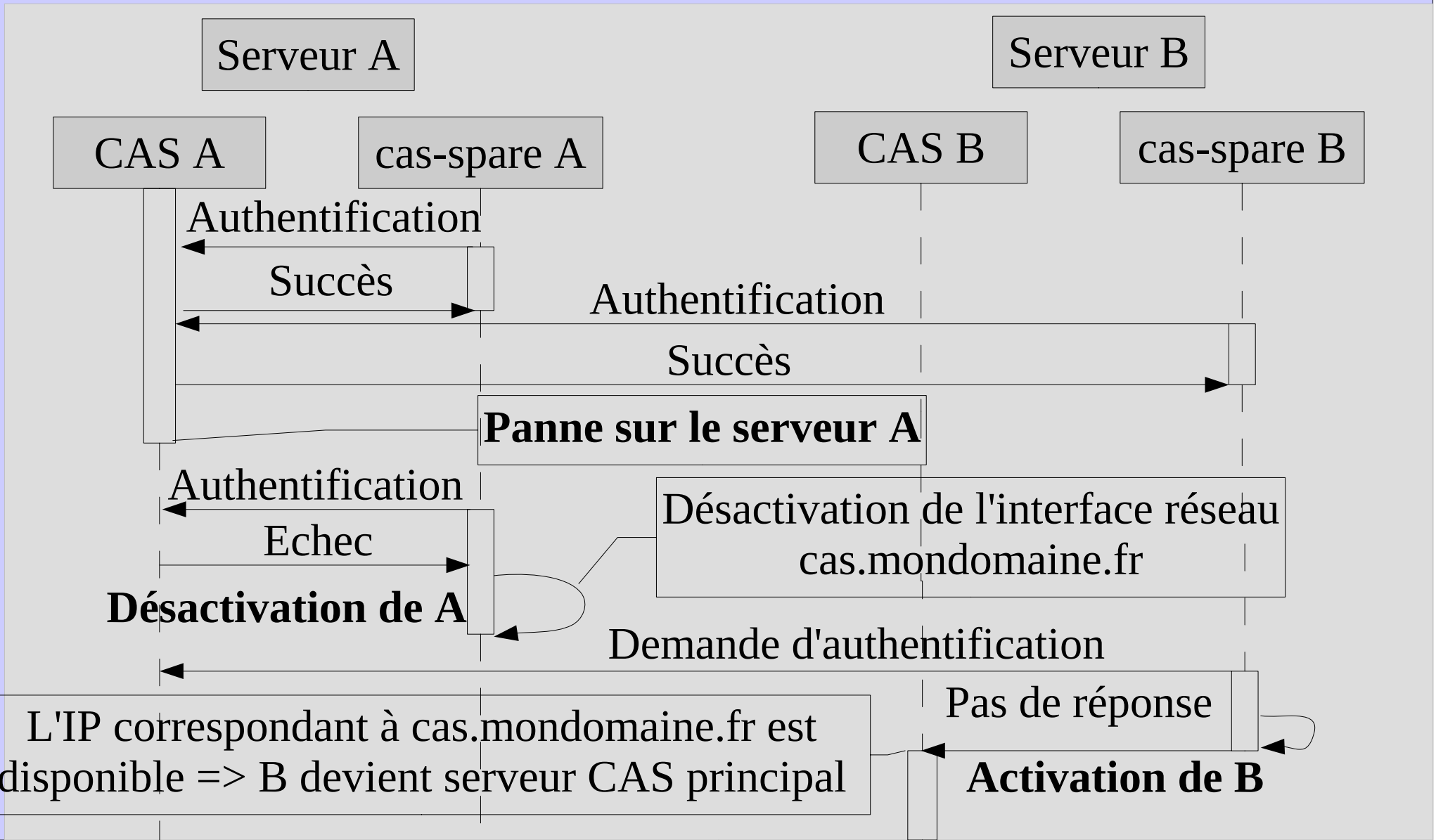
Serveur B

l,

Mécanismes de reprise sur panne avec cas-spare

Serveur B

Modélisation UML



Les limitations de cas-spare

- Obligation de se réauthentifier après une panne du serveur CAS
- Délai de reprise sur panne < 1min 30s
- cas-spare doit être installé sur chaque serveur
- cas-spare est un produit jeune

Les points forts de cas-spare ?

- Outil de surveillance puissant
- Facile à installer et configurer
- Le service CAS conserve la même IP
- Compatibilité possible avec d'autres SSO
- Compatible avec tous les systèmes Posix
- Compatible IPv6
- Aucune ressource matérielle supplémentaire
- Code très court (environ 600 lignes) sous licence LGPL

Comparatif

	Heartbeat-drdb	Jgroups	cas-spare
Répartition de charge	POSSIBLE	OUI	POSSIBLE
Reprise sur panne	OUI	NON	OUI
Réauthentification	OUI	NON	OUI
Qualité du monitoring	FAIBLE	X	EXCELLENTE
Temps de reprise	< 15sec	X	< 1min 30
Serveurs distants	POSSIBLE	?	OUI
Prise en main	DIFFICILE	?	SIMPLE
Support Ipv6	?	?	Oui
Coût matériel	ELEVE	TRES FAIBLE	TRES FAIBLE

cas-spare fonctionne !

Heure	Serveur	Evènement
15:21:31	A	**Arrêt de CAS**
15:22:23	B	Activation du CAS principal
15:23:35	B	**Arrêt de slapd**
15:24:55	A	Activation du CAS principal
15:25:58	A	**Arrêt de la machine**
15:26:21	B	Activation du CAS principal
15:31:41	B	**Arrêt violent de Tomcat**
15:32:56	A	Activation du CAS principal
15:34:23	A	**Coupure de lien réseau**
15:35:22	B	Activation du CAS principal

Perspectives

- Pour une authentification persistante :
  - signature des TGC : difficile à mettre en oeuvre
  - partage des tickets rejouables (TGC et PGT)

CAS v3 permet de stocker les tickets dans une BDD => authentification persistante

cas-spare pourrait être intégré à HeartBeat v2

Un service d'authentification robuste et sûr

- Réplication sécurisée des annuaires : protection des données confidentielles
- Optimisation de BDB : rechargement rapide et sûr des sauvegardes LDAP
- Haute disponibilité du service CAS : plus de 20 000 inscriptions par le web

cas-spare Home Page

http://sourcesup.cru.fr/cas-spare/

et sur le wiki CAS :

https://clearinghouse.ja-sig.org/wiki/display/CAS/Home