Gestion d'identités PSL – Architecture technique

Entr'ouvert SCOP – http ://www.entrouvert.com

Table des matières

1 Principes

La solution SUPANN proposée ici comporte trois composants :

- un serveur LDAP compatible SUPANN 2009 : `slapd` du projet OpenLDAP accompagné d'outils d'aide à la configuration et à la gestion des données SUPANN 2009.
- un logiciel de gestion des données LDAP via le web : LdapSaisie, pré-configuré pour se connecter à un annuaire SUPANN 2009
- un fournisseur d'identité SAML 2.0 : Authentic2, pré-configuré pour se connecter à un annuaire SUPANN 2009 et s'intégrer à une fédération de type Renater.

L'ensemble est prévu pour fonctionner sur une architecture Debian GNU/Linux 7 (Wheezy).

La solution utilise un maximum de composants fournis par le projet Debian, permettant de profiter de l'assurance qualité de ce dernier. Les développements propres à la solution visent

à rendre l'ensemble des outils utilisés compatibles avec la norme SUPANN 2009 d'une part et avec la fédération Renater d'autre part.

1.1 Multi-annuaire, méta-annuaire

La solution est capable de gérer plusieurs bases (branches) de façon rigoureusement distinctes dans l'annuaire LDAP. Cela permet d'héberger plusieurs annuaires SUPANN sur une seule instance.

Le serveur LDAP peut également être un méta-annuaire, celui-ci disposant alors de plusieurs branches chacune synchronisée avec un annuaire cible distant.

2 Matériels et infrastructure requis

Chaque composant est destiné à être installé sur une machine dédiée.

L'installation sur *machine virtuelle* est préconisée. Tous les composants fonctionnent sur n'importe quelle machine virtuelle compatible Debian 7 (VMware, VirtualBox, kvm, etc).

2.1 Configuration réseau commune

- Les machines doivent avoir accès à Internet, au moins DNS et HTTP, pour télécharger les paquets logiciels de la solution puis leur mise à jour ;
- Les machines doivent disposer d'entrées DNS, par exemple `ldap.example.net`, `ldapsaisie.example.net`, `authentic.example.net`
- L'installation est plus simple sur un réseau piloté par *DHCP*.

2.2 Serveur LDAP

Caractéristiques minimales :

- Processeur : Intel ou AMD64, *64 bits* (architecture nommée « amd64 » pour Linux) 2 GHz monocoeur
- Mémoire vive : 2 Go
- Disque : 10 Go

Réseau :

- En entrée : accès LDAP (389/tcp)
- En sortie : DNS, web (pour mises à jour)

Note : il est possible d'instancier plusieurs serveurs LDAP qui opérerons en mode « *master-master* ». Idéalement, aucun des serveurs n'étant prépondérant par rapport aux autres, ils doivent tous avoir la même configuration matérielle.

2.3 Serveur interface de gestion du LDAP

Caractéristiques minimales :

- Processeur : Intel ou AMD64, *64 bits* (architecture nommée « amd64 » pour Linux) 2 GHz monocoeur
- Mémoire vive : 2 Go
- Disque : 5 Go

Réseau :

- En entrée : accès HTTPS (443/tcp)
- En sortie : LDAP vers le(s) serveur(s) LDAP de la solution, DNS, web (pour mises à jour)

2.4 Serveur IdP

Caractéristiques minimales :

- Processeur : Intel ou AMD64, *64 bits* (architecture nommée « amd64 » pour Linux) 2 GHz monocoeur
- Mémoire vive : 2 Go
- Disque : 5 Go

Réseau :

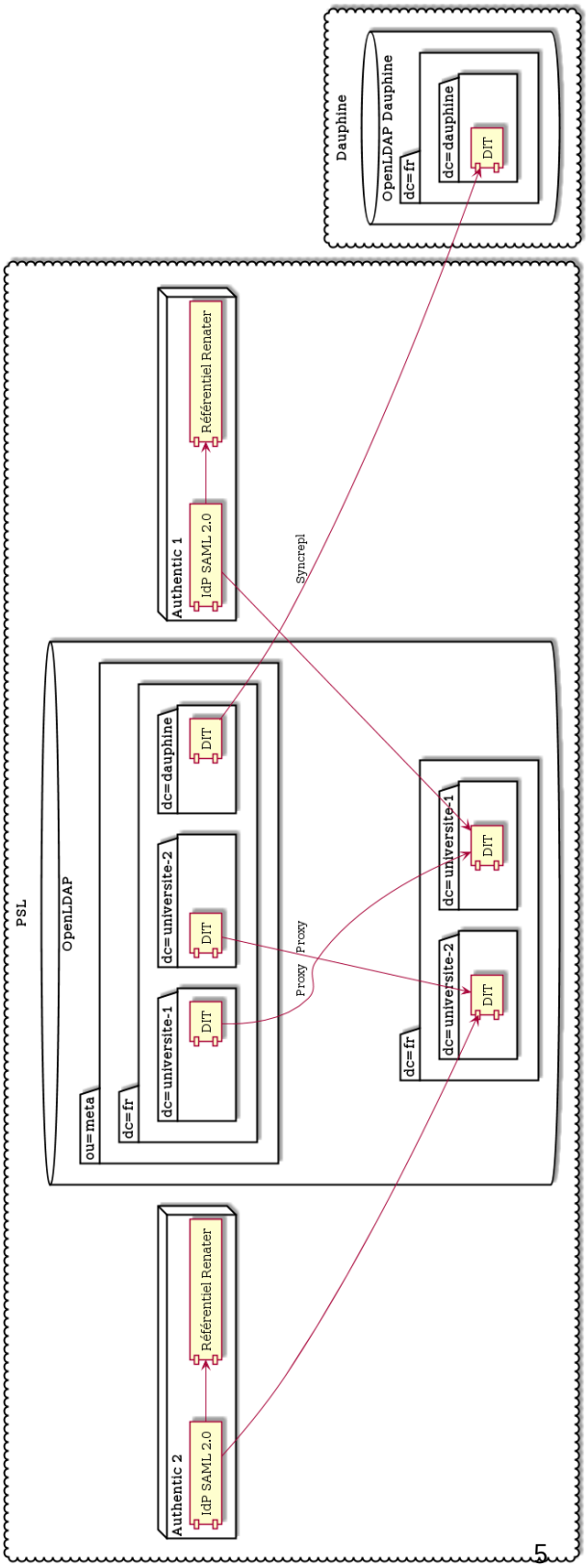
- En entrée : accès HTTPS (443/tcp)
- En sortie : LDAP vers le(s) serveur(s) LDAP, DNS, web HTTP et HTTPS (**chargement des métadonnées de fédération** et mises à jour logicielles)

2.5 Configuration des horloges

Il est très important de faire en sorte que toutes les machines de la solution soient à l'heure.

Typiquement, cela peut être fait via un système NTP. Cependant, aucun système de synchronisation d'horloge n'est installé par défaut par la solution, car certains systèmes de virtualisation peuvent proposer une horloge système déjà synchronisée par la machine hôte.

3 Schéma d'archicture technique



4 Documentations liées

Documentation spécifique à certaines briques utilisées dans le cadre de ce projet :

- Spécifications SUPANN : https://services.renater.fr/documentation/supann/
- LdapSaisie (en français) : http://ldapsaisie.easter-eggs.org/doc/all-in-one/LdapSaisie.html
- Authentic2 : http://authentic2.readthedocs.org/en/stable/
- OpenLDAP 2.4 : http://www.openldap.org/doc/admin24/

---

5 Historique du document

20150217 tnoel – première version