Gestion d'identités PSL – Installation IdP Authentic

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

Table des matières

1 Installation du système de base

La procédure décrite dans cette documentation doit être effectuée après l'installation du système de base décrite dans la documentation « *Gestion d'identités PSL – Installation de base* ».

1.1 Rappel sur la la synchronisation des horloges

Il est très important de faire en sorte que toutes les machines de la solution soient à l'heure. Dans le cas d'un IdP, toutes les assertions SAML/Shibboleth reçues et envoyées sont datées et seront refusées si elles ne sont pas bien à l'heure (exemple de message d'erreur sur une ressource : `Message rejected, was issued in the future.`).

Pour assurer la mise à l'heure de votre machine, vous pouvez installer le paquet `ntp` :

```
# apt-get install ntp
```

Éventuellement, si vous disposez d'un serveur NTP local, vous pouvez l'indiquer dans le fichier `/etc/ntp.conf`. Par défaut, `ntp` utilise les serveurs du projet Debian (`*.debian.pool.ntp.org`).

Note : le paquet `ntp` n'est pas installé par défaut car certains systèmes de virtualisation peuvent proposer une horloge système déjà synchronisée par la machine hôte.

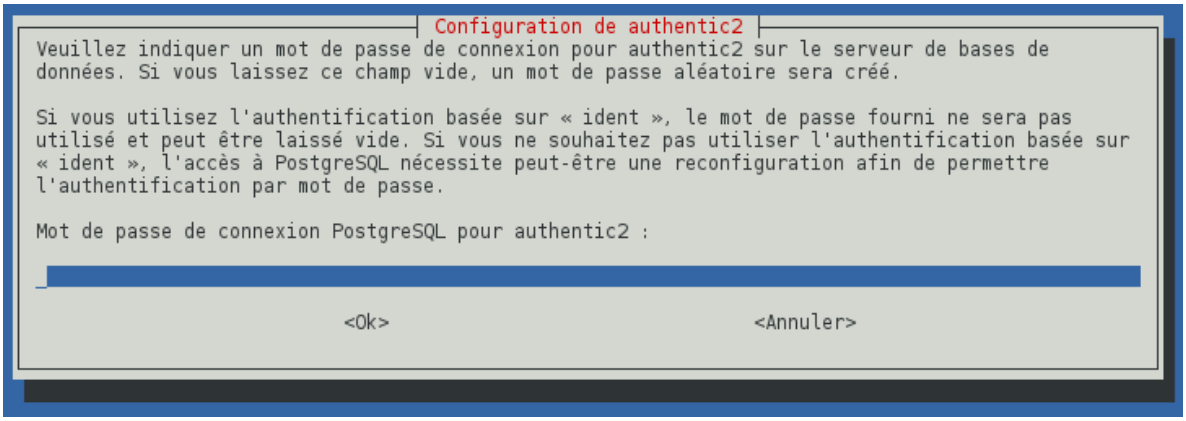
2 Installation du composant IdP Authentic2

Installer le paquet `authentic2-supann` :

```
# apt-get install authentic2-supann
```

Cette installation va déclencher l'installation de tous les composants logiciels (paquets) nécessaires à la mise en place du fournisseur d'identités (*Identity Provider*) connectable avec un annuaire SUPANN 2009.

Lors de l'installation il vous sera demandé un « **Mot de passe de connexion PostgreSQL pour authentic2** » : tapez juste `[Enter]`, un mot de passe aléatoire sera généré (vous n'aurez pas besoin de le connaître, il sera automatiquement configuré sur PostgreSQL et Authentic).



La configuration se fait ensuite en deux étapes

- configuration du logiciel Authentic proprement dit
- connexion du logiciel avec le serveur web Apache

3 Configuration d'Authentic2

Modifier le fichier `/etc/authentic2/supann.conf` pour faire correspondre les valeurs avec celles de la base créée dans l'annuaire LDAP (lors de la commande `slapd-supann newdb`) et renseigner la fédération dans laquelle sera intégrée le fournisseur d'identités.

Note : les éditeurs vi ou nano sont disponibles pour cela. Si vous êtes débutant sous Linux, préférez l'éditeur nano, plus accessible. Vous pouvez aussi installer d'autres éditeurs (`apt-get install vim` ou `apt-get instal emacs`)

```
# nano /etc/authentic2/supann.conf
```

Le fichier est un script shell, attention à la syntaxe, n'ajoutez pas d'espace avant ou après le signe =, conservez bien les `export`, etc.

Après modification de ce fichier, relancer le service `authentic2` pour qu'il prenne en compte les nouveaux paramètres :

```
/etc/init.d/authentic2 restart
```

Exemple d'un fichier renseigné avec liaison avec la fédération de test Renater :

```
# Configuration du LDAP
#
# URL de l'annuaire LDAP
export SUPANN_LDAP_URL='ldap ://192.168.43.23/'
# Base DN de l'annuaire LDAP
export SUPANN_LDAP_BASE_DN='dc=quelquechose,dc=fr'
# Bind DN pour connexion à l'annuaire LDAP (optionnel)
export SUPANN_LDAP_BINDDN='uid=admin,ou=people,dc=quelquechose,dc=fr'
# Bind Password pour connexion à l'annuaire LDAP (optionnel)
export SUPANN_LDAP_BINDPW='as ;KUAq*6123'

# Données de fédération
# Fédération Renater de production
# URL des métadonnées
# RENATER_METADATA=https ://federation.renater.fr/renater/renater-metadata.xml
# URL des règles de filtrage des attributs
# RENATER_ATTRIBUTE_FILTERS=https ://federation.renater.fr/renater/filtres/renater-a
# URL du certificat de signature des métadonnées
# RENATER_CERTIFICATE=https ://federation.renater.fr/renater/metadata-federation-ren

# Fédération de Test
export RENATER_METADATA='https ://federation.renater.fr/test/renater-test-metadata.xml
export RENATER_ATTRIBUTE_FILTERS='https ://federation.renater.fr/test/filtres/renater-
export RENATER_CERTIFICATE='https ://federation.renater.fr/test/metadata-federation-re
```

```
# Raccordement EduGain
# Nom de l'organisation
export EDUGAIN_SCHAC_HOME_ORGANIZATION="Université de QuelquePart"
# Type de l'organisation
export EDUGAIN_SCHAC_HOME_ORGANIZATION_TYPE="urn :schac :homeOrganizationType :int :ur
#

# Local port for listening -- NE PAS MODIFIER
export BIND='127.0.0.1 :8080'

# Utiliser TLS pour communiquer avec le serveur LDAP, 0 pour désactiver, 1 pour
# activer, vous devez au préalable vous assurez que le certificat de votre
# serveur LDAP sera reconnu, par exemple en le déclarant dans
# /etc/ldap/ldap.conf avec la ligne
# TLS_CAPATH /chemin/du/certificat_ou_du_certificat_racine
export USE_TLS=0
```

Le reste de la configuration d'Authentic, automatiquement modifiée par le paquet `authentic2-supann`, est déjà conforme à SUPANN 2009.

3.1 Installation d'un certificat spécifique pour SAML

Lors de l'installation du paquet `authentic2-supann`, un certificat X.509 est généré pour la partie SAML 2.0 / Shibboleth. Il s'agit d'un certificat autosigné, valable 10 ans.

Si la fédération dans laquelle sera inscrite l'IdP nécessite un certificat SAML avec d'autres critères, il faudra le générer par la méthode qui sera indiquée, puis le poser à la place du certificat installé par défaut :

- `/etc/authentic2/cert.pem` : le fichier du certificat X.509
- `/etc/authentic2/key.pem` : la clé privée correspondante

Ces fichiers doivent être lisibles par l'utilisateur système `authentic` et la clé privée ne doit, par définition, pas être publique. Le réglage de ces droits d'accès peut se faire ainsi :

```
# chown authentic :authentic /etc/authentic2/cert.pem
# chmod 644 /etc/authentic2/cert.pem
# chown root :authentic /etc/authentic2/key.pem
# chmod 640 /etc/authentic2/cert.pem
```

Une fois ces fichiers mis en place, il faut relancer le service :

```
# /etc/init.d/authentic2 restart
```

3.2 Connexion au serveur LDAP en SSL/TLS

Pour demander à Authentic se connecte au serveur LDAP en TLS vous pouvez soit utiliser une URL de LDAP ayant comme mécanisme `ldaps ://` ou bien définir `USE_TLS` à 1 dans le fichier `/etc/authentic2/supann.conf` pour utiliser la commande `STARTLS` sur une connexion LDAP en clair.

Attention, le certificat du serveur LDAP doit être valide. Si ce n'est pas le cas (par exemple lors de tests) vous devez modifier la configuration du client LDAP du système et lui dire de toujours accepter les certificat. Pour ce faire, ajouter la ligne suivante dans `/etc/ldap/ldap.conf` :

```
TLS_REQCERT never
```

Pour activer la validation d'un certificat valide au final, le fichier `/etc/ldap/ldap.conf` doit ressembler à cela (en changeant le chemin vers le certificat) :

```
# cat /etc/ldap/ldap.conf

# Exemple d'un fichier /etc/ldap/ldap.conf·qui accepte
# n'importe quel certificat serveur

# See ldap.conf(5) for details
# This file should be world readable but not world writable.

# TLS certificates (needed for GnuTLS)
TLS_CACERT      /chemin/du/certificat/ldap.pem
TLS_REQCERT     hard
```

Le fichier de certificat doit être lisible par l'utilisateur authentic.

4 Configuration d'Apache pour exposer Authentic

Le serveur HTTP Apache est déjà installé par `authentic2-supann`. Il reste à le configurer. Une configuration par défaut est fournie qu'il suffit d'activer, voici la procédure pour cela.

Activer les modules nécessaires à Apache :

```
# a2enmod ssl
# a2enmod headers
# a2enmod proxy_http
```

Puis activer la configuration par défaut du site qui exposer Authentic :

```
# a2ensite authentic2-supann.conf
```

Il faut ensuite indiquer le *ServerName* au niveau de la configuration du site, dans le début du fichier `/etc/apache2/sites-enabled/authentic2-supann.conf` :

```
# nano /etc/apache2/sites-enabled/authentic2-supann.conf
```

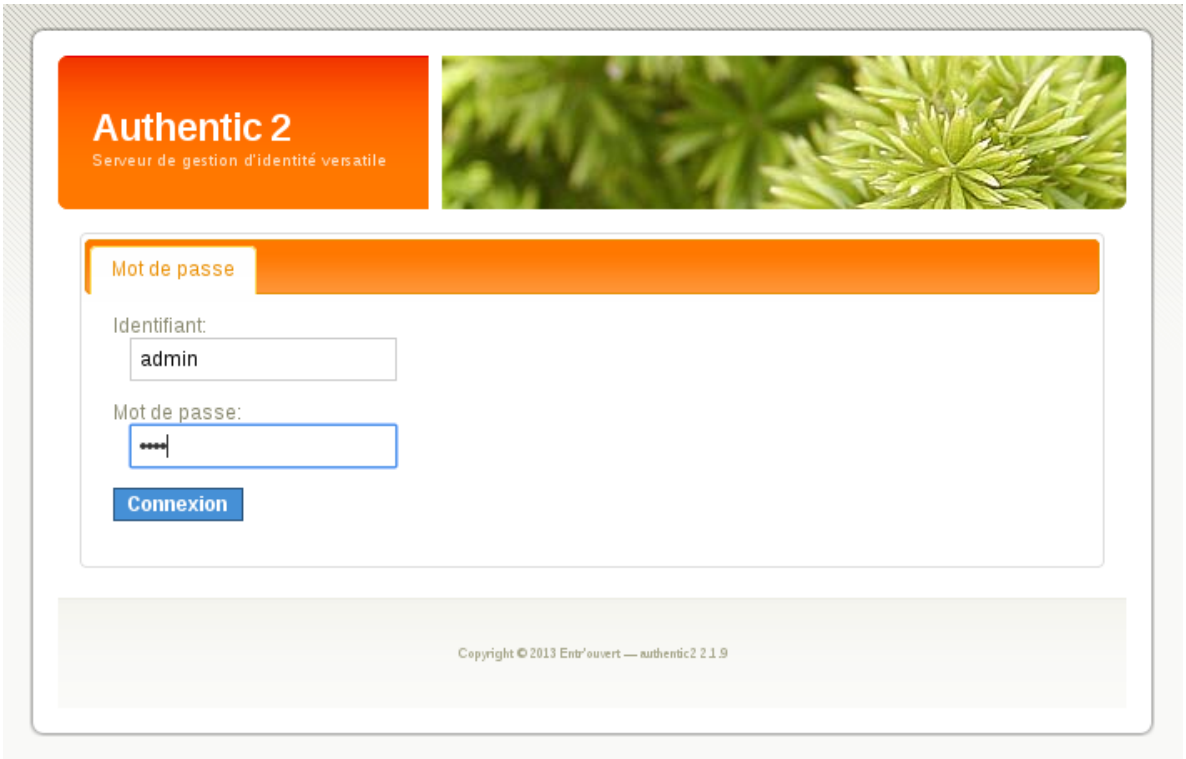
Par exemple :

```
# extrait de /etc/apache2/sites-enabled/authentic2-supann.conf
# où il faut modifier le ServerName
<VirtualHost * :443>
  ServerName idp.quelquechose.fr   # <-- indiquer ici le nom DNS de la machine
  ...
```

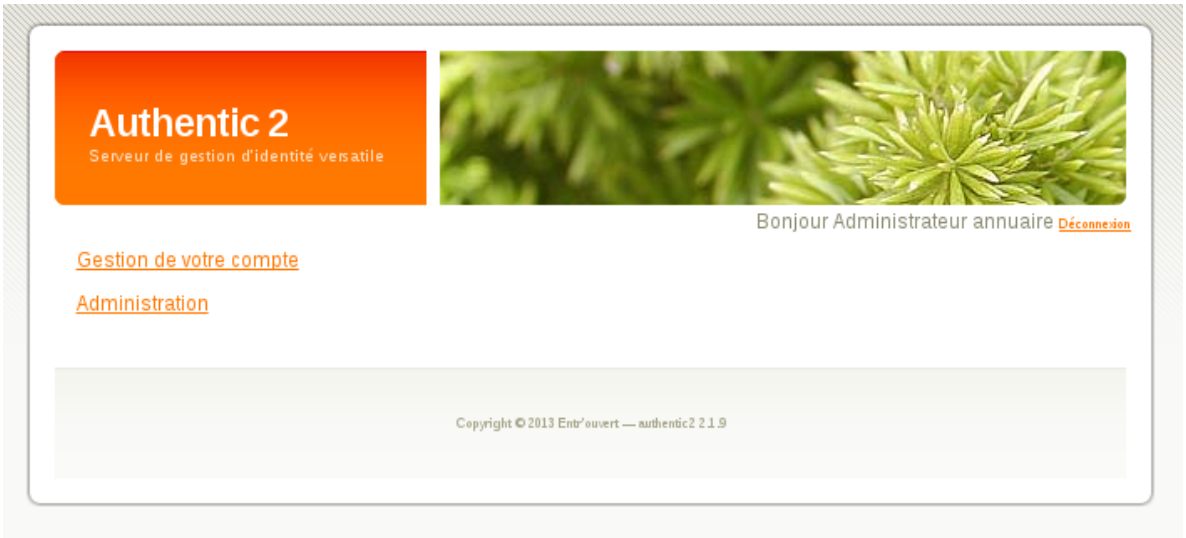
Enfin, relancer le service `apache2` pour prendre en compte ces modifications de sa configuration :

```
# service apache2 restart
```

L'interface est alors accessible sur `https ://idp.quelquechose.fr`



Pour se connecter, utiliser l'identifiant `admin` et le mot de passe choisi lors de la création de la base sur le serveur LDAP (`newdb`).



4.1 Installation d'un certificat pour HTTPS

Le certificat installé par défaut pour Apache est bien entendu invalide.

Pour installer un certificat valide (correspondant au nom du serveur et signé par une autorité reconnu) il faut en copier les clés un répertoire, par exemple `/etc/apache2/ssl` qui peut être créé pour l'occasion, puis indiquer l'emplacement des clés dans la configuration `/etc/apache2/sites-enabled/authentic2-supann.conf` :

```
# extrait de /etc/apache2/sites-enabled/authentic2-supann.conf
(...)
SSLCertificateFile    /etc/apache2/ssl/certificate.pem
SSLCertificateKeyFile /etc/apache2/ssl/private-key.key
```

Ensuite relancer le service pour prendre en compte la modification

```
# service apache2 restart
```

4.2 Adaptations de la configuration Apache

Le fichier `authentic2-supann.conf` fourni par la solution pour configurer Apache est un modèle, un exemple. Si vous connaissez bien la configuration Apache pour exposer un service PHP, et/ou si vous avez des besoins spécifiques de configuration, vous pouvez tout à fait créer votre propre configuration Apache. Vous pouvez même utiliser un autre serveur HTTP.

Cependant, la solution n'est supportée que pour Apache et pour un fichier de configuration qui ne soit pas trop distant du modèle `authentic2-supann.conf`.

5 Validation dans la fédération de test Renater

Le préalable pour cette opération est de disposer d'un compte sur la fédération, au minimum un *compte CRU*. Les comptes CRU sont des comptes ouverts à toute personne disposant d'une email, pour se créer un compte il faut aller sur https://cru.renater.fr/sac/.

5.1 Inscription du fournisseur dans la fédération

L'inscription d'un fournisseur dans la fédération se fait sur le **guichet de la fédération** à l'adresse https://federation.renater.fr/registry. Voici la procédure détaillée pour y inscrire un IdP Authentic nouvellement installé.

Tout d'abord aller sur https://federation.renater.fr/registry, choisir son IdP de connection dans la boite en haut à droite.

Désormais sur la page d'accueil, cliquer sur « *Ajouter un fournisseur d'identités* »

Une page s'affiche qui demande les informations techniques concernant le fournisseur à déclarer. Voici les réponses à donner :

- Intitulé du fournisseur d'identités : le nom de votre fournisseur d'identité par exemple "Chimie-ParisTech"
- Intitulé du fournisseur d'identités (en anglais) : la même chose en anglais pour Edugain
- domaine : le ou les noms de domaine de votre établissement
- description en français et en anglais
- Cliquer sur l'onglet Rattachement à un organisme et n'en sélectionner aucun

- Cliquer sur l'onglet Contacts et renseigner les informations de contact technique
- Cliquer sur l'onglet **Informations techniques** et indiquer les informations suivantes :
    - EntityID : `https://idp.quelquechose.fr/idp/saml2/metadata` (remplacer le nom `idp.quelquechose.fr` par celui de votre machine)
    - URL du profil SAML2/POST/SSO : `https://idp.quelquechose.fr/idp/saml2/sso`
    - URL du profil SAML2/Redirect/SSO : `https://idp.quelquechose.fr/idp/saml2/sso`
    - Certificat X.509 : il faut ici recopier le contenu de la balise XML *X509Certificate* que vous trouverez dans le fichier XML à l'URL `https://idp.quelquechose.fr/idp/saml2/meta`
      Ce même contenu est aussi visible dans le fichier `/etc/authentic2/cert.pem` sur le serveur où est installé Authentic (attention, enlever les l'entête et le pied de page du fichier, `-----BEGIN CERTIFICATE-----` et `-----END CERTIFICATE-----` avant de copier son contenu dans l'interface du guichet Renater)
    - Aller à l'onglet Soumettre et valider

5.2 Configuration des fédérations éducation/recherche

La configuration des fédérations éducation/recherche dans l'IdP se fait par lecture de fichiers situés dans `/etc/authentic2/federations.d/`. Ces fichiers de script shell doivent porter l'extension `.sh` et déclarer deux variables :

- METADATA : le nom du fichier XML de métadonnées
- SOURCE : un identifiant de la fédération (e.g. 'renater', 'edugain'), nécessaire à authentic pour distinguer les multiples fédérations.

À l'installation du paquet Debian, des fichiers d'exemple sont fournis dans le dossier `/usr/share/doc/authentic2-supann/federations.d-examples`.

La configuration des fédérations est effectuée par la commande suivante :

```
# su -s /bin/sh -c /usr/lib/authentic2-supann/load-multiple-federations.sh
```

Note : cette opération est aussi automatisée pour être exécutée toutes les heures.

Note : Une fois effectuée l'inscription de votre IdP à une fédération, les autres services de la fédération mettent normalement à jour les métadonnées de la fédération toutes les heures. Il faudra donc **attendre au moins une heure** suite à l'inscription pour pouvoir commencer les tests.

Si votre IdP est inscrit sur la fédération Renater de test, vous pourrez aller sur la **ressource de test** mise à disposition par Renater à l'adresse https://services.renater.fr/federation/test/ressource. Vous serez renvoyé sur le service de découverte et devrez choisir dans le menu le nom donné à votre IdP.

Note : le service de test ne gérant pas la déconnexion, il faudra effacer vos cookies pour recommencer un test.

6 Historique du document

20150217 tnoel – première version 20171115 pmarillonnet – configuration des fédérations éducation/recherche