Fonctionnement d'un proxy CAS

Contraintes

- D'abord, celles d'un client CAS, mais avec accès au serveur CAS en https nécessairement
- Ensuite, l'application proxy CAS doit être elle même accessible en https du serveur CAS, au minimum sur l'URL de callback, qui doit être paramétrable.

Cinématique, et logs associés

Vérifier le fonctionnement client CAS simple

Vérifier que l'application fonctionne au moins en client CAS simple. Voir la rubrique dédiée à celà.

> **Important**
>
> La demande de ST doit se faire en https et sur l'URI serviceValidate; elle comporte un paramètre supplémentaire, pgtUrl, qui indique que l'application web veut être proxy ; ce paramètre indique l'URLde callback.

Voici les logs des serveur CAS et Appli web proxy lors du login (identique au précédent), puis de la demande de validation du ticket ; ici, 194.214.218.163 est l'adresse IP du navigateur W3, 194.214.218.40 le serveur CAS, 194.214.218.198 l'appli web proxy CAS (ici, webmail imp), 194.214.218.110 le service tiers (ici, serveur IMAP)

Serveur CAS, demande de ST

```
194.214.218.163 "GET /login?service=[https://webmail.univ.fr/cas/index.php] HTTP/1.1"
```

Appli web proxy, recup du ticket

```
194.214.218.163 "GET /cas/index.php?ticket=ST-1681-9IpDqJ2ang4SBf8aanzT HTTP/1.1"
```

Serveur CAS, validation du ST et demande du PGT (Proxy Granting Ticket)

```
194.214.218.198 "GET /serviceValidate?service=https://webmail.univ.fr/cas/index.php&ticket=ST-1681-9Ip...
&pgtUrl=https://webmail.univ-nancy2.fr/cas/casProxy.php
```

URL de callback

Avant de délivrer la réponse du GET précédent, le serveur CAS tente un connexion directe en https vers l'URL de callback de l'application web proxy, en passant 2 paramètres : PGTIOU et PGT

Appli web proxy

```
194.214.218.40 "GET /cas/casProxy.php?pgtIou=PGTIOU-547-mnkcs...&pgtId=PGT-1094-sxP1d4vj... HTTP/1.1"
```

Le serveur CAS répond seulement maintenant au GET serviceValidate, en passant l'identité de la personne, et le PGTIOU ; le proxy CAS peut maintenant associer le PGT reçu à l'utilisateur authentifié.

Requête de PT

L'application proxy dispose maintenant d'un PGT pour l'utilisateur (ici; PGT-1094-...). Elle va pouvoir requérir auprès du serveur CAS des Proxy-Ticket (PT) pour des applications tierces.

Cette demande de PT se fait nécessairement en https, en passant en paramètres le PGT et le 'service' associé, vers l'URI proxy.

Serveur CAS

```
194.214.218.198 "GET /proxy?targetService=imap://mail.univ.fr&pgt=PGT-1094-s.... HTTP/1.1"
```

Transmission du PT

le proxy CAS transmet le PT à l'application tierce ; si cette application logue ses accès, il est possible de 'tracer' cet envoi. Dans notre exemple, c'est le serveur imap Casifié, nous n'avons pas de logs

Validation du PT

l'application tierce (serveur IMAP, dans l'exemple) fait valider son PT directement auprès du serveur CAS.

Serveur CAS

```
194.214.218.110 "GET /proxyValidate?ticket=PT-1682-GMxYazU89ZuGIkpYOhyd&service=imap://mail.univ.fr HTTP/1.0"
```

On constate que les étapes 4 et 5 sont similaires à une authentification CAS simple, le proxy CAS remplacant le navigateur pour obtenir des PT.

Causes de non fonctionnement en mode proxy

Dans un premier temps, il faut déja s'assurer que l'application web cliente CAS fonctionnement correctement en mode non proxy.

Il faut que l'application proxy puisse accéder en https au serveur CAS, que le serveur CAS puisse accéder en https vers le proxy.

Il faut également que le service tiers accède en http(s) au serveur CAS (avec mod_cas et pam_cas, c'est nécessairement https).

Pour toutes ces connexions https, il faut que le client puisse valider le certificat du serveur, ou une autorité de certification ayant validé le certificat.

Dans le cas de mod_cas et pam_cas, il ne faut passer que le certificat de l'autorité racine.

La cause de loin la plus courante de dysfonctionnement se situe dans les connexions https, lorsque les clients n'ont pas les certificats pour valider la connexion https.

autres causes possibles :

- le nom de service passé pour valider le PT est différent de celui passé pour l'obtenir.
- URL de callback en http au lieu de https. Dans ce cas, le message suivant est écrit dans le fichier de log du serveur CAS :

```
PGT callback failed: java.io.IOException: only 'https' URLs are valid for this method
```