Fonctionnement d'un client CAS

Le client CAS est en fait une application web, qui utilise le serveur CAS pour authentifier un utilisateur.

Contraintes

- Le navigateur W3 doit être capable de gérer les redirections http.
- L'application web client CAS doit pouvoir accéder directement en http (s) auprès du serveur CAS pour faire valider le Service Ticket (ST). Est-ce possible ?

Cinématique, et logs associés

Dans l'exemple, l'adresse IP du navigateur est 194.214.218.163, celle de l'appli web cliente 194.214.218.39.

Le navigateur accède pour la première fois à une application web.

Celle-ci le redirige (redirection http) vers le serveur CAS pour authentification.

regarder les logs d'accès du serveur CAS lors de la phase de login / récupération de Service Ticket (ST) pour vous assurer des paramètres de redirections passés (paramètre service)

Logs serveur CAS

```
194.214.218.163 "GET /index.jsp?service=http://ent.univ.fr/Login HTTP/1.1"&amp;nbsp;
```

L'application web cliente récupère le Service Ticket (ST).

Logs appli web cliente :

```
194.214.218.163 "GET /Login?ticket=ST-37-sIMC5FhJx15GRwZtJ1Q7 HTTP/1.1"
```

Validation du ticket

L'appli web cliente génère une requête http ou https pour faire valider le ticket, vers l'URI LegacyValidate (protocole CAS V1) ou ServiceValidate (protocole CAS V2). Le login sera retourné par le serveur CAS et réponse de cette requête.

Logs serveur CAS

```
194.214.218.39 GET /serviceValidate?service=http://ent.univ.fr/Login&ticket=ST-37-sIMC5FhJx15GRwZtJ1Q7 HTTP/1.1
```

S'assurer que le ticket est bien le bon, et que le service passé en paramètre correspond au service passé lors de la demande du ticket.

Validation du certificat

Si l'application web cliente CAS accède au serveur CAS en https pour faire valider son ST : il faut qu'elle soit capable de valider le certificat transmis par le serveur https.

Elle fait donc référence à un 'magasin de certificats', qui doit contenir au moins le certificat du server CAS, ou d'une autorité de certification ayant délivré le certificat.

Causes de non fonctionnement

1) l'application cliente CAS ne peut pas accéder en http(s) au serveur CAS : firewall, ACLs routeur, ...

2) l'application cliente fait valider le ST en https, alors que le certificat du serveur CAS n'est pas validé. Dans le cas d'une servlet hébergée par tomcat, un message est affiché dans le fichier catalina.out, du genre :

```
certificate no trusted
```

3) le nom de service passé pour valider le ST est différent de celui passé pour l'obtenir.