



Etat d'avancement du projet esup-CAS v4

Ludovic Auxepaules -- *Direction des Systèmes d'Information
de l'Université Pierre et Marie Curie*



ludovic.auxepaules@upmc.fr

<https://github.com/auxepaul/>

<https://github.com/EsupPortail/cas-toolbox-new>



Esup cas-toolbox-new

- ❖ Objectif du projet Esup cas-toolbox-new
 - * Faciliter la **configuration** et le **déploiement** d'un serveur CAS
 - Centraliser certains éléments de configuration et préconfigurer certains modules et fonctionnalités du serveur CAS
- ❖ Esup cas-toolbox-new disponible sur Github
 - * <https://github.com/EsupPortail/cas-toolbox-new>
- ❖ Présentation plus détaillée lors d'Open Apereo 2015
 - * <http://fr.slideshare.net/doclaux/open-apereo2015-castoolbox>
- ❖ Documentations officielles de CAS
 - * <http://jasig.github.io/cas/4.0.x>



Esup cas-toolbox-new v3 et v4

➤ « Double Overlays » basé sur Maven

cas-toolbox-core

(ajouts et pré-configurations d'Esup)

- * src/main

- java
- webapp

- * pom.xml

cas-toolbox-custom

(changements de l'établissement)

- * src/main

- webapp

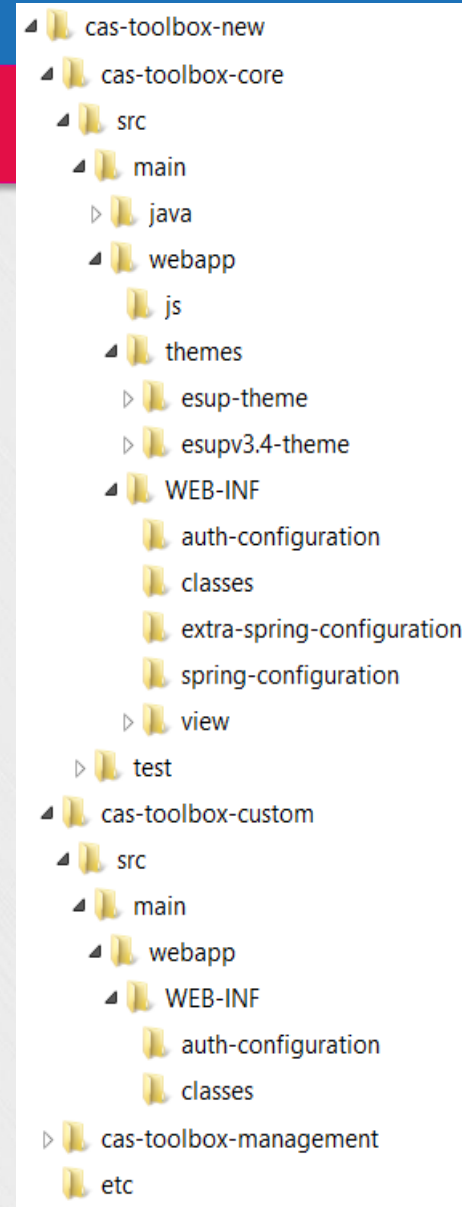
- * pom.xml

etc (guides HowTo, et exemples de « scripts »)

config.sample.properties (exemple de configuration)

pom.xml

- ❖ Meilleure différenciation des ajouts Esup (cas-toolbox-core), des changements de l'établissement (cas-toolbox-custom)



Possibilités offertes par Esup cas-toolbox-new

- ❖ Déploiement d'un serveur CAS dans un Tomcat existant
- ❖ Simplification et centralisation de la configuration
 - * Fichier **config.properties**, HandlersDiscover
- ❖ Pré-paramétrage des ajouts Esup
 - * **Thème, LDAP, Logging, TraceMe, Stats, BlockAttack, SAML...**
 - * A activer : **Memcached, Rest, Kerberos, LPPE, Clearpass...**
- ❖ Pas de quickstart construite avec Ant
- ❖ Possibilité d'utiliser jetty en localhost pour "tests"
(envisagé)



Etat des lieux

cas-toolbox-new avec CAS v4.0.5

- ❖ Intégration de l'authentification avec LDAP → OK
 - * (SSL/TLS, multi-LDAP, configurations spécifiques à vérifier)
- ❖ Remplacement de la fonctionnalité *Esup Block Attack* par *Throttling Authentication Attempts* → OK
- ❖ Attributs fournis avec SAML 1.1 → OK
- ❖ Intégration simple de Memcached → OK
 - Tester également la configuration proposée par Apereo
- ❖ Logs, Monitoring, statistiques, Agimus-NG → OK
- ❖ Réécriture des guides HowTo et création de liens vers la documentation officielle d'Apereo → En cours
- ❖ Nouveau Thème Esup (« Responsive ») → En cours



Etat des lieux et Perspectives

- ➔ ESUP cas-toolbox-new v4.0.x utilisable par les établissements
- ❖ Integration du Module REST → à tester
- ❖ Ajouts et préconfigurations d'autres moyens d'authentification
 - * Spnego (Kerberos), Trusted (REMOTE_USER)...
- ❖ Ajouts et préconfigurations d'autres modules et fonctionnalités
 - * LPPE, Clearpass...
- ❖ Avec CAS 4.1 : Etude et création de projets plus spécifiques ?
 - * **RBAC** (*Role-Based Access Control*) par service avec CAS et Grouper
 - * **MFA** (*Multi-Factor Authentication*) avec l'implémentation des LOA (*Levels of Assurance*) du serveur CAS





Nouveautés relatives au serveur CAS d'Apereo

Historique des versions du serveur CAS

<https://www.apereo.org/tags/cas-product-release>
<https://github.com/Jasig/cas/releases/>

- ❖ **CAS Server 4.1.0** **Septembre 2015**
- ❖ **CAS Server 4.0.5** **Septembre 2015**
- ❖ **CAS Server 3.6.0** **Juin 2015**
- ❖ CAS Server 4.0.1 Janvier 2015 recommandé en juin 2015
- ❖ CAS Server 4.0 Mai 2014 recommandé en juin 2014
- ❖ Patches de sécurité pour SAML2 (e.g. Google Apps), attaques HTTP
 - * **CAS Server 3.5.3** **Janvier 2015**
 - * CAS-server-security-filter 1.0 Aout 2014 2.0.x Mai 2015
 - * CAS Server 3.4.12.1 Avril 2014
- ❖ CAS Server 3.5.2 Février 2013 recommandé en juin 2013
- ...
- ❖ CAS Server 3.5.0 Juillet 2012
- ❖ CAS Server 3.4.12 Mai 2012 recommandé en juin 2012



Nouveautés introduites par CAS v4.0.x

- ❖ Nouveau protocole CAS v3
 - * Renvoi des attributs de l'utilisateur en plus de l'identifiant
- ❖ Meilleure modularité
 - * e.g. interface web de gestion des services séparée du serveur
- ❖ Remaniement des API d'authentification
- ❖ Mise à jour des dépendances
 - * e.g. remplacement de Spring LDAP par Ldapative
- ❖ Amélioration de l'interface Utilisateur ("Responsive")



CAS v4.1.x

- ❖ En développement depuis Mai 2014
- ❖ Sortie officielle **le 19 septembre 2015**
- ❖ Quelques nouveautés introduites par la version 4.1
 - * Management App Facelift
 - * Support consumption of SAML's Metadata MDUI
 - * Secure release of client credential, PGT and (optionally) CAS attributes
 - * Role-based Access Control and Authorization
 - * Refactoring of attributes filters, and attributes per service
 - * Proxy config per service should authorize callback urls
 - * CAS-specific truststore for proxycalls and handling SSL certs
 - * Client-side Spring Webflow session management
 - * JSON Service Registry
- ❖ Modules dépréciés
 - * Cache JBoss, Restlet, Uber War, Clearpass
- ❖ Documentation officielle
 - * <http://jasig.github.io/cas/4.1.0/>

