MAXIME PLACES & LOUIS FELDMAR - CYBERSÉCURITÉ

Analyse des systèmes de SSO (single sign-on)

Quel système choisir, et pourquoi ?

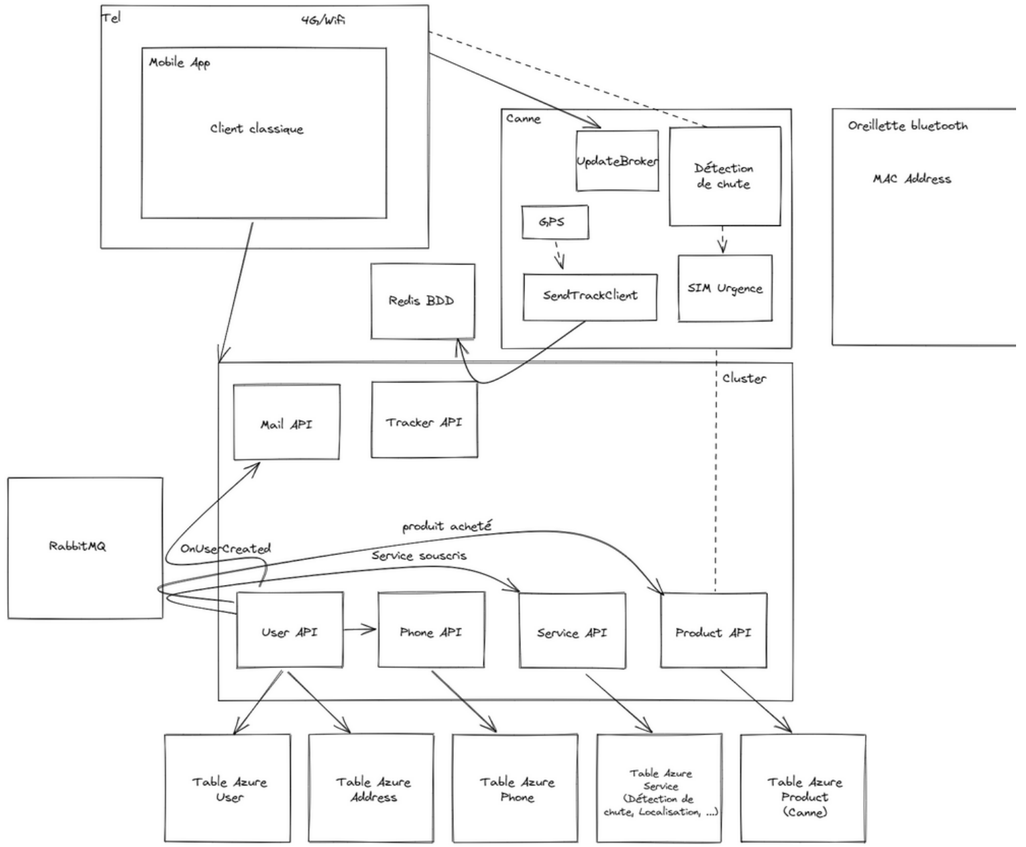
Contexte d'utilisation

Architecture micro-services

Options :

1. Services externes sur différents Cloud Providers
2. Auto-hébergé sur le cluster

kubernetes

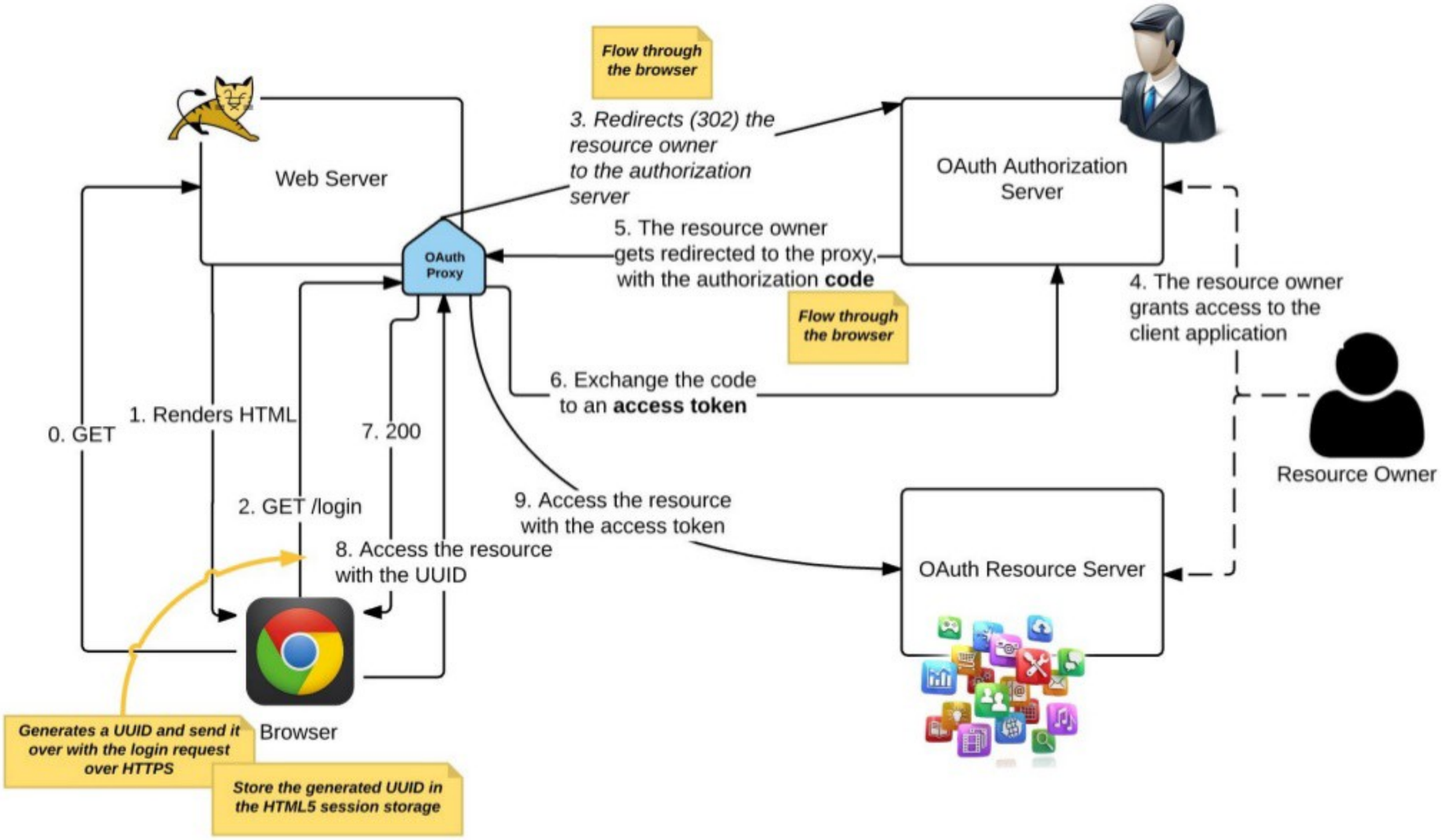


Qu'est-ce que le SSO?

- Centraliser l'authentification d'un utilisateur
- Gestion de droits d'accès aux ressources

Securing SPAs

OAuth Proxy



Protocol expérimental

- Implémentation d'applications utilisant les différents services SSO
- Test de performance avec Selenium
- Comparaison des coûts, performances et facilités d'implémentation/d'administration

Microsoft Azure Active Directory

- Depuis la plateforme Microsoft Azure.
- Création d'un Azure Active Directory (système d'authentification)
- Gestion d'un "Flux utilisateur" (base de données des utilisateurs)
- Configuration depuis la plateforme des données récoltées.
- Utilisation d'une librairie Javascript pour une implémentation frontend pré conçue.

Google Cloud Platform
via Firebase

- Depuis la plateforme Google Cloud Platform
- Création d'un service d'authentification clé en main, via Firebase
- Gestion des utilisateurs depuis Firebase qui agît comme API d'authentification et base de donnée.
- Configuration des données récoltées dans l'implémentation
- Pas de libraire "toute faite" pour l'implémentation

Microsoft Azure Active Directory B2C

Point par point, les détails

01 La première installation

À l'aide d'une documentation complète (mais un peu vieillissante), la mise en place se fait relativement facilement. La grande communauté d'utilisateurs permet un accès à beaucoup de ressources.

02 Les installations suivantes

Une fois que nous avons un compte Azure configuré et que nous avons déjà réalisé notre première mise en place, la reproduction est très facile. Les étapes sont simples et logiques une fois la prise en main faite.

03 La rapidité d'authentification

Moyenne sur 100 connexions constatée à 1663 millisecondes.
Temps le plus haut : 2165 ms, le plus court : 1404 ms.

04 Le prix

Gratuit pour moins de 50k utilisateurs par mois.
Au delà de 50k utilisateurs par mois : 0,002925 € par utilisateurs actifs mensuels. Prix max : 1681875€ par mois.

Google Cloud Platform

Firebase Google Cloud Platform

Point par point, les détails

01 La première installation

La mise en place du service Firebase se fait littéralement en trois clicks. Pour cela, il faut savoir trouver la liste des solutions clés en main proposées par GCP mais il n'y a rien de compliqué. Cependant, l'implémentation frontend n'est pas facilitée par une librairie et est donc bien plus chronophage.

02 Les installations suivantes

On ne perd pas de temps à la navigation mais on ne gagne pas tant de temps tant la solution est facile à mettre en place côté GCP. Implémentation bien plus rapide en mimant le fonctionnement de notre première application.

03 La rapidité d'authentification

Moyenne sur 100 connexions constatée à 936 millisecondes.
Temps le plus haut : 1268 ms, le plus court : 713 ms.

04 Le prix

Gratuit pour moins de 25k utilisateurs par mois.
Au delà de 25k utilisateurs par mois : pas de prix fixe par utilisateurs actifs mensuels. Prix max : 1157,80€ par mois.

Keycloak Auto-hébergé

Point par point, les détails

01 La première installation

Le déploiement de la solution Keycloak sur le cluster demande sur certaine connaissance des technologies DevOps (Kubectl, docker, ...). Il est nécessaire de déployer une base de donnée (auto-hébergée ou non) et d'administrer des perimètres et des clients de la même manière que les services SSO précédents.

02 Implémentation du SSO dans une application

L'utilisation de la librairie Keycloak-js demande une certaine expertise dans le langage choisis. Nous n'avons pas pu mener a bout son intégration.

03 Le prix

Le prix dépend du nombre d'instances de Keycloak à déployer. Plus nous avons d'instances d'applications utilisant le SSO, plus nous devons déployer d'instance de Keycloak et augmenter la taille et le nombre de réplicats de la base de donnée.

La comparaison

Les éléments clés pour savoir choisir

1ère implémentation

Concernant la première implémentation, GCP est plus simple à prendre en main si on a un background de développeur.

2ème implémentation

En revanche, pour la seconde implémentation et en ayant la connaissance du produit, M-AAD est plus pratique à reproduire et lancer sur un autre projet.

La performance

En terme de performance, GCP est plus efficace, et de loin. Battant M-AAD en étant plus de deux fois plus rapide.

Le coût d'utilisation

Pour une petite application, M-AAD sera moins cher pour plus d'utilisateurs. En revanche, lors d'un grand dimensionnement, GCP devient bien plus rentable.

Notre choix

Azure Active Directory pour sa simplicité d'implémentation, sa gratuité jusqu'à 50k utilisateurs. Aussi, nous estimons la différence de performance négligeable dans notre contexte.

Fin de la présentation
Des questions ?

Merci de votre attention