Laboratoire 3
Configuration de l'authentification unique de Google pour une application Web dans Microsoft Azure

Université du Québec en Outaouais
Titre du cours : CYB1123 - Sécurité de l'infonuagique et des services Web

Date de remise : Avant lundi 4 Novembre 2024, 23 :59
Nom et Prénom : Sankara Kabem Abdoul Charif
Code permanent : Sank90300007

I Introduction

Ce laboratoire vise à mettre en pratique les compétences acquises dans le cours de sécurité en infonuagique en explorant l'intégration de l'authentification unique via Google Identity Platform dans une application Web. En configurant un fournisseur d'identité externe dans notre cas avec Google, Nous pourront expérimenter l'utilisation des API d'authentification de Google et constater les avantages de la délégation de l'authentification à un tiers sécurisé et éprouvé. Les tâches incluent la création et la configuration de l'API, la mise en place de Google comme fournisseur d'identité dans l'application, et la validation de la fonctionnalité d'authentification unique, avec des captures d'écran à l'appui pour illustrer chaque étape.

1)Listons au moins 3 avantages d'utiliser un fournisseur d'identité externe

Voici trois avantages d'utiliser un fournisseur d'identité externe, tel que Google Identity Platform, pour la gestion de l'authentification d'une application Web :

1. **Sécurité renforcée** : Les fournisseurs d'identité comme Google utilisent des normes de sécurité avancées, telles que l'authentification multifactorielle (MFA) et la détection des activités suspectes, pour protéger les informations d'identification des utilisateurs. Ils offrent également des mises à jour de sécurité régulières, réduisant les risques d'intrusion ou de vol de données.
2. **Simplicité d'utilisation pour les utilisateurs** : Les utilisateurs peuvent se connecter en utilisant leurs identifiants Google existants, ce qui simplifie l'expérience de connexion. Cela réduit également le besoin pour les utilisateurs de créer un compte spécifique, diminuant ainsi les risques de perte de mot de passe ou de compte inactif.
3. **Économie de temps et de coûts pour les développeurs** : Intégrer un fournisseur d'identité externe permet de déléguer la gestion des processus d'authentification (création de comptes, gestion de mots de passe, etc.). Cela réduit le besoin de développement et de maintenance d'un système d'authentification personnalisé, permettant aux développeurs de se concentrer sur d'autres aspects de l'application.

2) Exemple d'application Web où un fournisseur d'identité externe est contre-indiqué

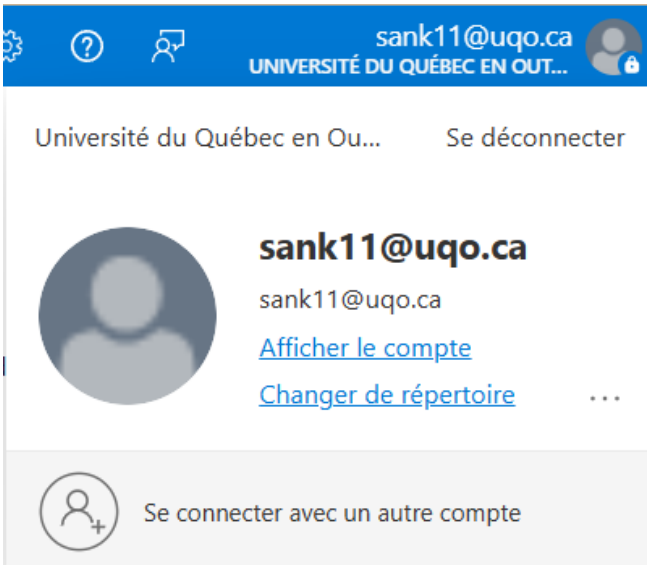
La gestion des informations de santé d'un hôpital ou d'une clinique.

Explication :

Dans le domaine de la santé, les données sont extrêmement sensibles et sont soumises à des réglementations strictes de protection de la vie privée. L'utilisation d'un fournisseur d'identité externe, tel que Google Identity Platform, pourrait poser des problèmes de conformité, car il impliquerait de partager certaines informations avec une tierce partie. En outre, les hôpitaux préfèrent souvent utiliser des systèmes d'authentification internes pour garder un contrôle total sur la gestion des accès et assurer une sécurité maximale. Ils peuvent ainsi garantir que toutes les données d'authentification et d'accès restent dans leur propre infrastructure, sans dépendre d'un service externe qui pourrait être vulnérable à des violations de données ou des politiques de confidentialité différentes.

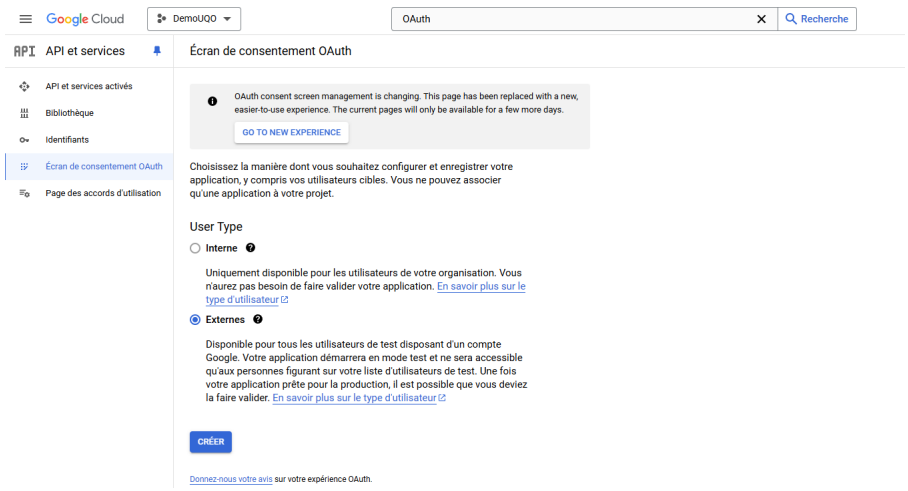
3) Captures d'écran requises et explications sur les differentes etapes du laboratoire

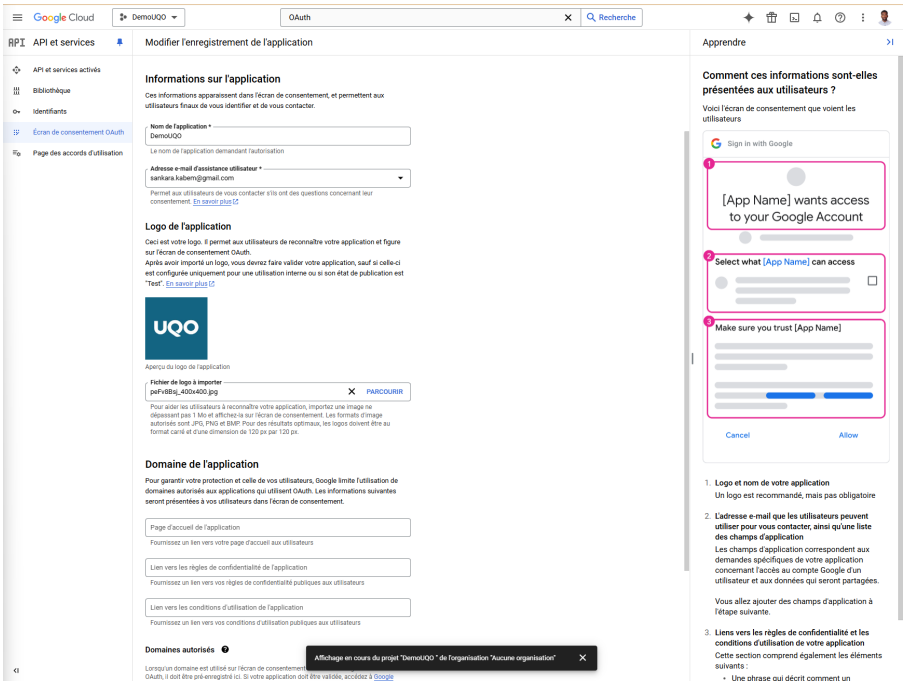
Les captures d'écran suivantes expliquent les grand point pour la configurations des API et dans l'autorisation dans Azure :



a) L'information sur votre application (App information, Partie 1 – Étape 7)

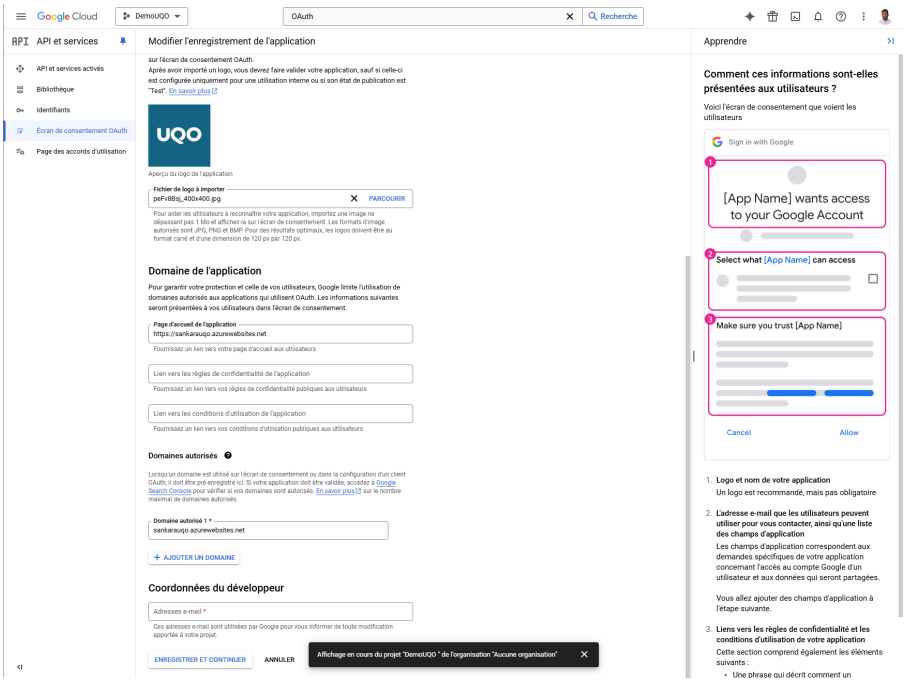
Après avoir créé un compte Google (si ce n'est pas déjà fait), nous accédons à la console développeur de Google. Nous y créons un nouveau projet, puis spécifions que nous souhaitons configurer un utilisateur de type externe. Ensuite, nous définissons le nom de l'application ainsi que l'adresse courriel qui permettra d'y accéder.

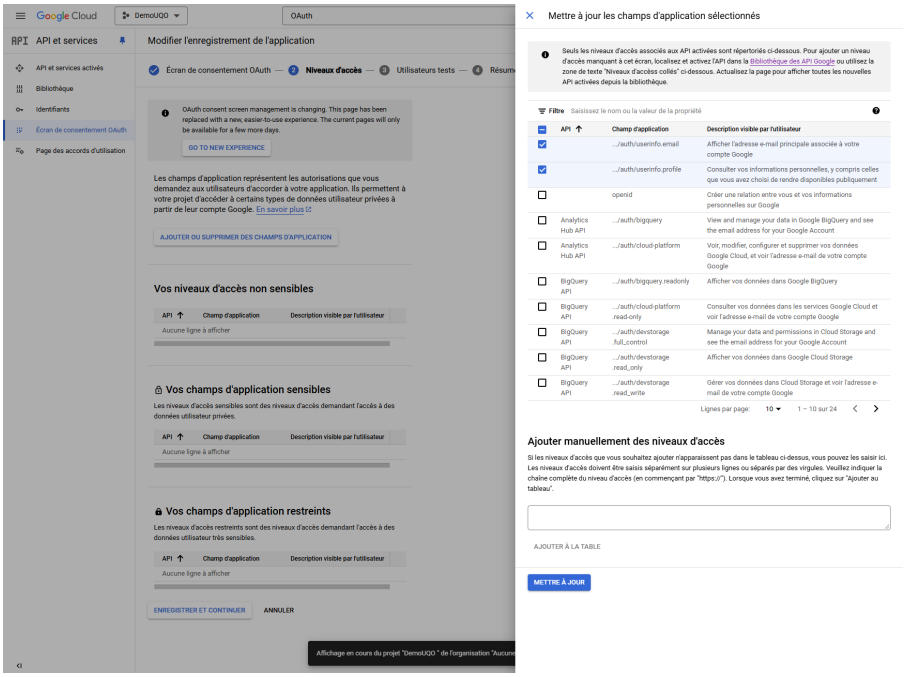




b) Votre domaine applicatif (App domain, dernière capture d'écran de la Partie 1 – Étape 8)

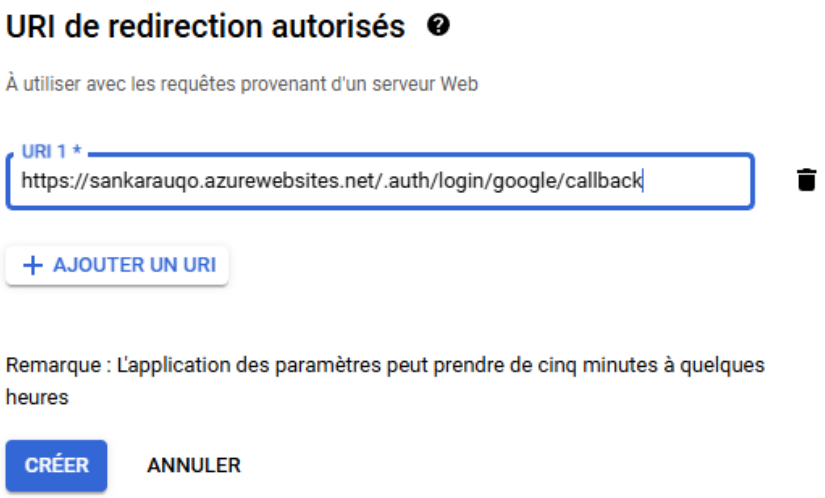
Après avoir saisi les informations liées à notre application, nous passons à la configuration des informations de domaine. Dans notre cas, l'application a été déployée sur Azure, donc nous avons ajouté le lien du domaine autorisé.





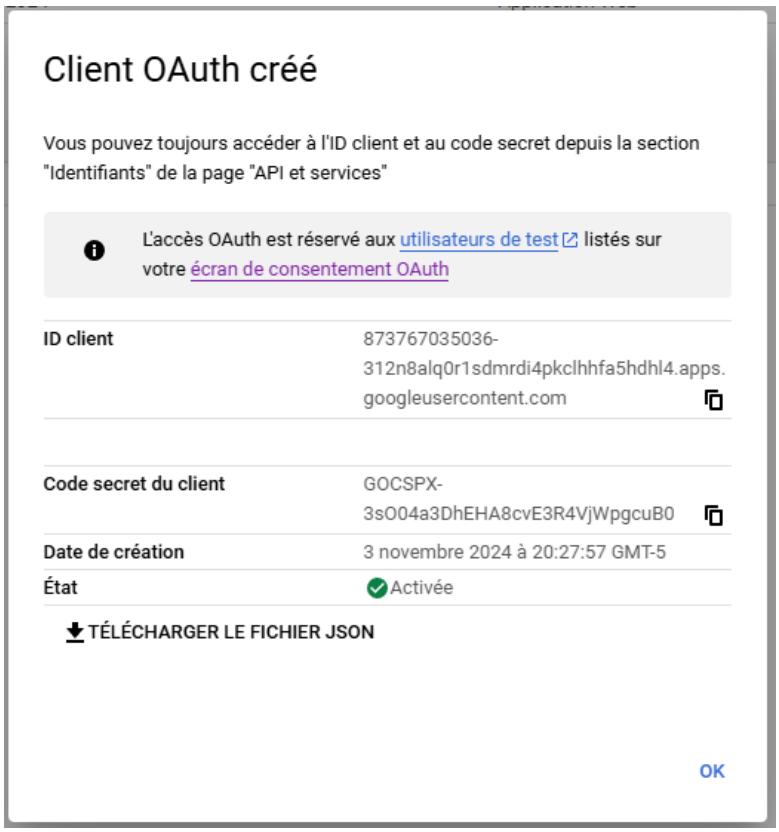
c) L'adresse de retour (Partie 1 – Étape 16)

Pour créer notre adresse de retour, nous avons ajouté le suffixe '/.auth/login/google/callback' à l'adresse générée automatiquement sur Microsoft Azure. L'adresse de retour obtenue est donc : 'sankarauqo.azurewebsites.net/.auth/login/google/callback'.



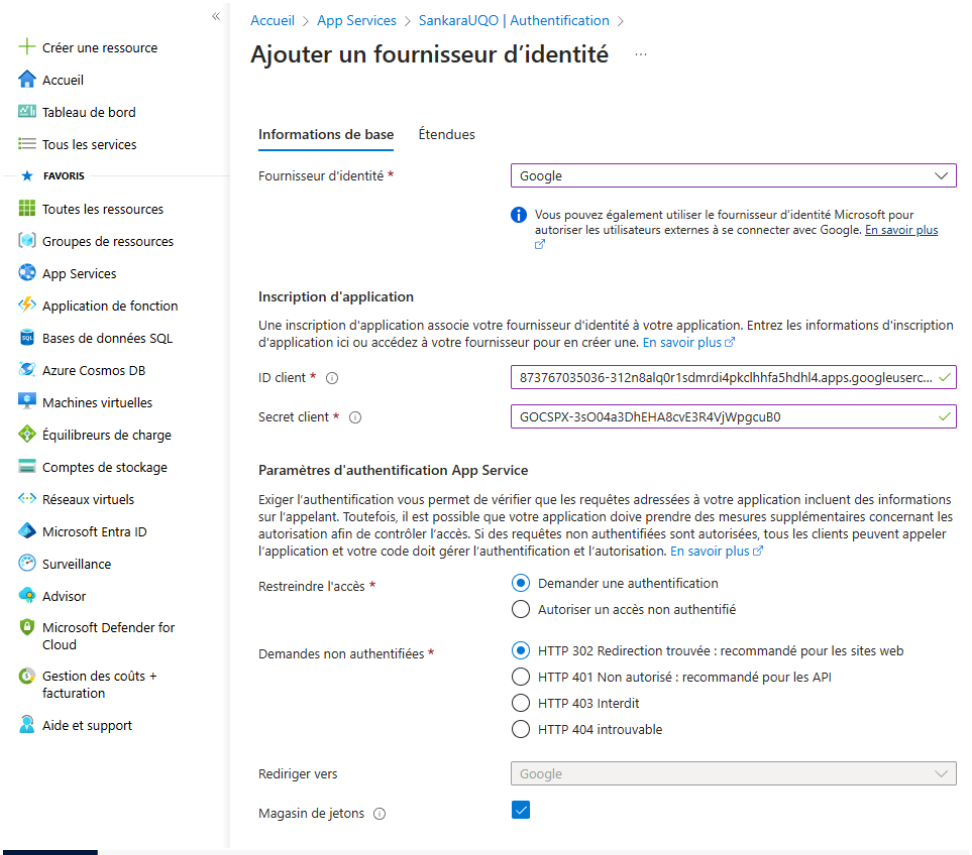
d) Les valeurs du Client ID et du Client secret (Partie 1 – Étape 17)

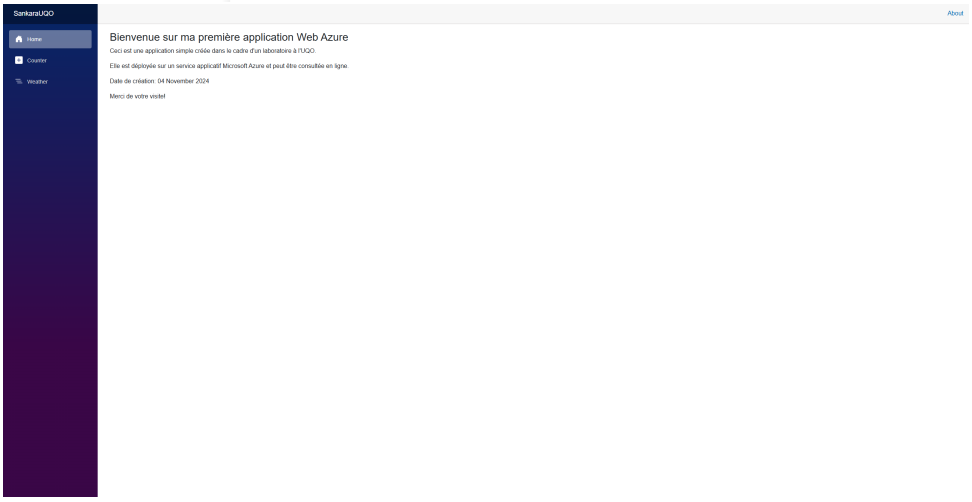
— **Client ID** : 873767035036-312n8alq0r1sdmrdi4pkclhhfa5hdhl4.apps.googleusercontent.com
— **Client secret** : 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



e) Configuration du fournisseur d'identités (Partie 2 – Étape 5)

Après avoir configuré notre application dans l'espace développeur de Google, nous accédons au portail de Microsoft Azure et allons dans notre section *App Services* pour démarrer notre application. Ensuite, nous ajoutons le fournisseur d'identité Google en sélectionnant *Identity Provider*. À ce stade, nous configurons l'application en entrant l'ID client généré ainsi que le code secret du client. Désormais, en tentant de se connecter à l'adresse de notre domaine, nous constatons qu'un accès au compte Google est requis en premier lieu.





II Conclusion

Ce laboratoire nous a permis de nous familiariser avec les concepts pratiques de sécurité infonuagique en mettant en œuvre une solution d'authentification unique basée sur un fournisseur d'identité externe. À travers la configuration de Google Identity Platform et son intégration dans l'application, la simplicité et la sécurité qu'apporte un fournisseur d'identité de grande envergure. Les connaissances acquises dans ce laboratoire soulignent l'importance de la sécurité dans les applications Web, tout en mettant en évidence les avantages, les limites et les particularités des solutions d'authentification infonuagique dans un environnement applicatif réel.