# Rapport de Configuration : Authentification GitHub vers GCP

Ce document détaille la configuration de l'authentification sécurisée entre le dépôt GitHub skillforge-ai-monorepo et le projet Google Cloud skillforge-ai-mvp-25. L'objectif était de mettre en place une connexion sans mot de passe en utilisant la **Fédération d'identités de charges de travail (Workload Identity Federation)**, conformément à la Partie 1.4 du guide d'implémentation.

## 1. Objectif

L'objectif était de permettre aux pipelines CI/CD (GitHub Actions) d'accéder aux ressources Google Cloud et de les modifier de manière sécurisée, sans avoir à stocker de clés de service ou de secrets à longue durée de vie dans GitHub.

## 2. Résumé des Étapes de Configuration

Le processus a été réalisé en suivant une séquence logique pour établir la confiance entre les deux plateformes.

1. **Création du Dépôt GitHub :**
   * Un nouveau dépôt privé nommé **skillforge-ai-monorepo** a été créé sur GitHub.
   * Les branches initiales **main** et **develop** ont été créées.
   * Des **règles de protection de branche** ont été appliquées pour exiger des Pull Requests avant toute fusion, garantissant un flux de travail contrôlé.
2. **Création du Compte de Service sur GCP :**
   * Un compte de service dédié à la CI/CD, **sa-github-actions-cicd**, a été créé dans le projet skillforge-ai-mvp-25.
   * Ce compte a reçu le rôle de **Propriétaire (roles/owner)** sur le projet pour lui accorder les permissions nécessaires durant la phase d'initialisation.
3. **Configuration de la Fédération d'Identités :**
   * Un **Workload Identity Pool** nommé **skillforge-pool** a été créé pour gérer les identités externes.
   * Un **Fournisseur d'identité OIDC** nommé **github-provider** a été configuré pour faire confiance aux jetons d'authentification émis par GitHub Actions.
4. **Liaison Finale :**
   * Une politique IAM a été ajoutée pour lier le compte de service sa-github-actions-cicd au dépôt GitHub spécifique (sahemac/skillforge-ai-monorepo). Cela autorise le dépôt à "emprunter" l'identité du compte de service.
   * L'identifiant unique du fournisseur a été récupéré pour une utilisation future dans les secrets GitHub.

## 3. Problèmes Rencontrés et Solutions Appliquées

Plusieurs défis techniques ont été rencontrés, principalement liés à des évolutions de l'API Google Cloud et à des subtilités de l'interface.

### Problème 1 : Échec de la Création du Fournisseur d'Identité via gcloud

* **Symptôme :** La commande gcloud iam workload-identity-pools providers create-oidc échouait systématiquement avec une erreur INVALID\_ARGUMENT, même avec la syntaxe la plus simple.
* **Cause Racine :** L'API Google Cloud a renforcé ses exigences de sécurité. Elle n'accepte plus la création d'un fournisseur OIDC sans une **condition d'attribut** spécifiant explicitement quel dépôt ou quelle branche est autorisé à se connecter. La commande gcloud ne parvenait pas à formater cette condition correctement.
* **Solution Appliquée :** Le problème a été contourné en utilisant l'**interface graphique de la console Google Cloud**. Le fournisseur a été créé manuellement, en ajoutant une **"Condition d'attribut"** explicite pour n'autoriser que le dépôt concerné : attribute.repository == 'sahemac/skillforge-ai-monorepo'.

### Problème 2 : Menu "Fédération d'Identités" Grisé

* **Symptôme :** En essayant d'appliquer la solution ci-dessus, le menu "Fédération d'identités de charges de travail" était inaccessible (grisé).
* **Cause Racine :** L'interface de la console était positionnée au niveau de l'**Organisation** (emacsah.com) et non du **Projet**. La fédération d'identités est une ressource qui se gère au niveau du projet.
* **Solution Appliquée :** Le contexte de la console a été changé via le sélecteur en haut de la page pour sélectionner le projet **skillforge-ai-mvp-25**, ce qui a immédiatement débloqué l'accès au menu.

## 4. Paramètres Finaux et Identifiants Clés

* **Compte de Service CI/CD :** sa-github-actions-cicd@skillforge-ai-mvp-25.iam.gserviceaccount.com
* **Workload Identity Pool :** projects/584748485117/locations/global/workloadIdentityPools/skillforge-pool
* **Fournisseur d'Identité (à stocker dans les secrets GitHub) :** projects/584748485117/locations/global/workloadIdentityPools/skillforge-pool/providers/github-provider

La configuration est maintenant terminée et robuste.