Django へ SCIM2 + Azure App Service でログイン

背景

- 最近、Django に興味を持つ
- Django Rest Framework で静的サイト等にも利用できて面白そう
- しかし、Django のサイトを複数作るとユーザー管理が混乱しそう

少し調べてみると、Azure Active Directory(AAD) でユーザー管理(プロビジョニング)ができそうだったので試してみた。

方針

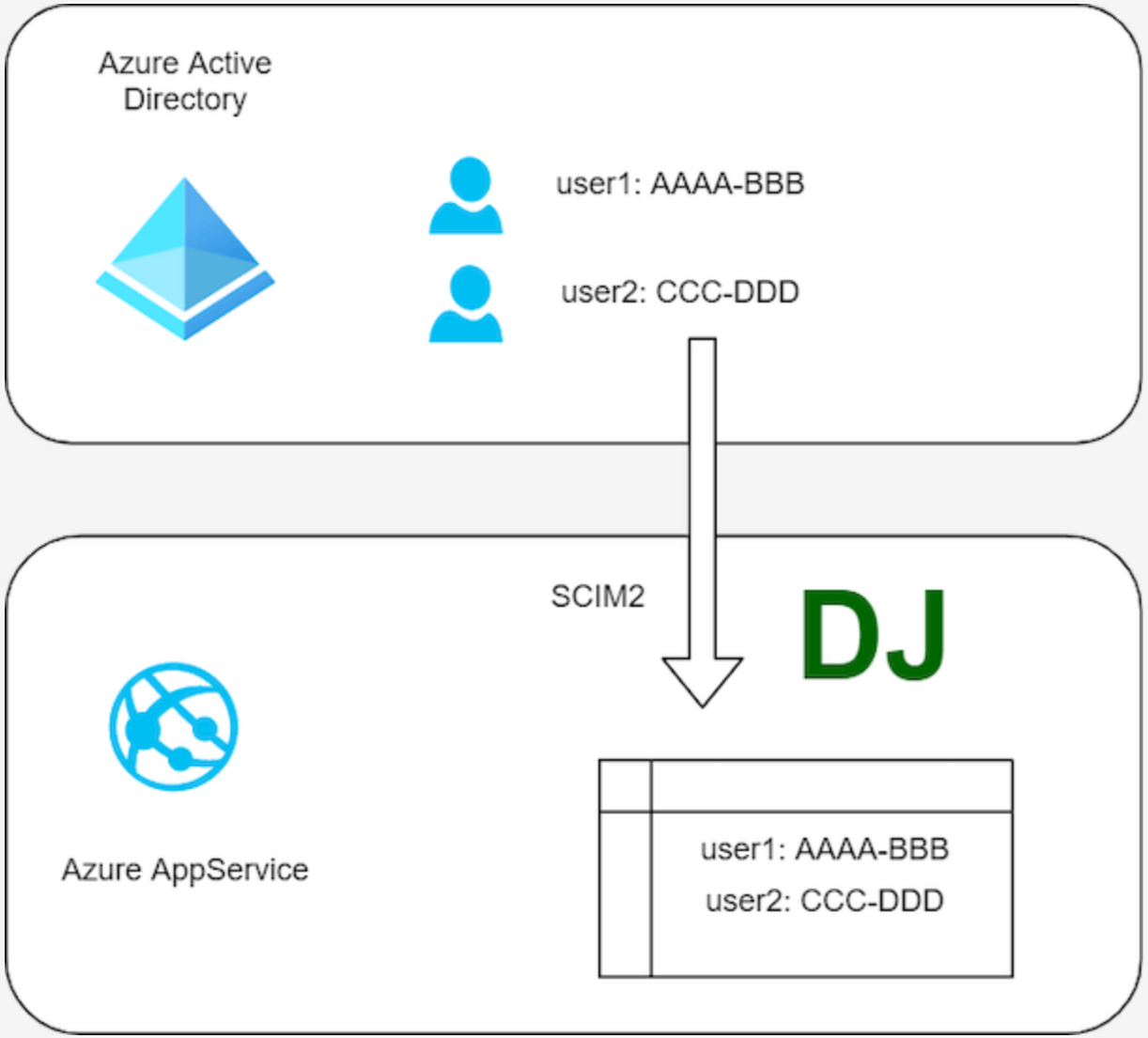
Azure AD で OIDC 認証するアプリを作ってみる - Qiita を参考に、以下のような方針としました。

- Django-SCIM2 を利用して AAD とユーザーの同期(プロビジョニング)を行う
- 認証は Open ID Connect ではなく Azure App Service(WebApp) 組み込み機能を利用ぷ

Azure Active Directory とユーザー同期

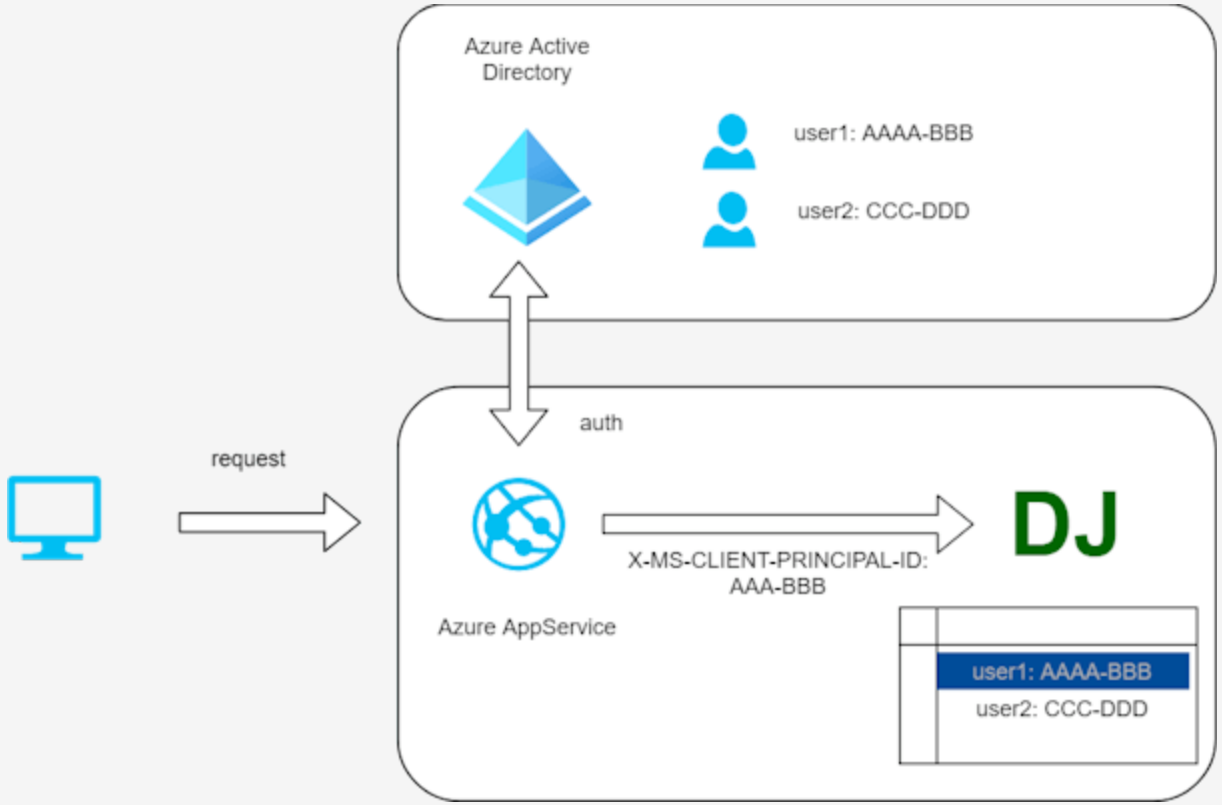
Django 側へログインユーザーを作成するため、AAD との同期(プロビジョニング)を SCIM2 で実施する。 なお、このときマッピングに `oid` を含める。

ユーザー同期の概要図


Azure Active Directory
user1: AAAA-BBB
user2: CCC-DDD
SCIM2
DJ
Azure AppService
user1: AAAA-BBB
user2: CCC-DDD

Azure App Service で認証

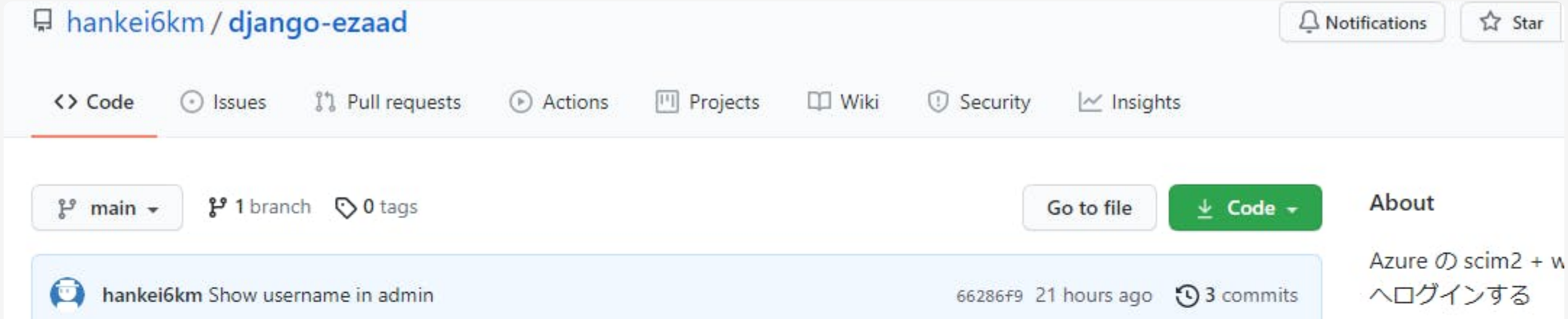
Azure App Service 上では request header 経由で認証状況を確認できるので、今回はそれを利用しログインする。



実装

以下のような再利用可能なアプリケーション [django-ezaad](#) を作成。

- SCIM2 対応
- `ezaad/login` を開くことで AAD へサインイン
- `X-MS-CLIENT-PRINCIPAL-ID` が合致するユーザーで Django へログイン



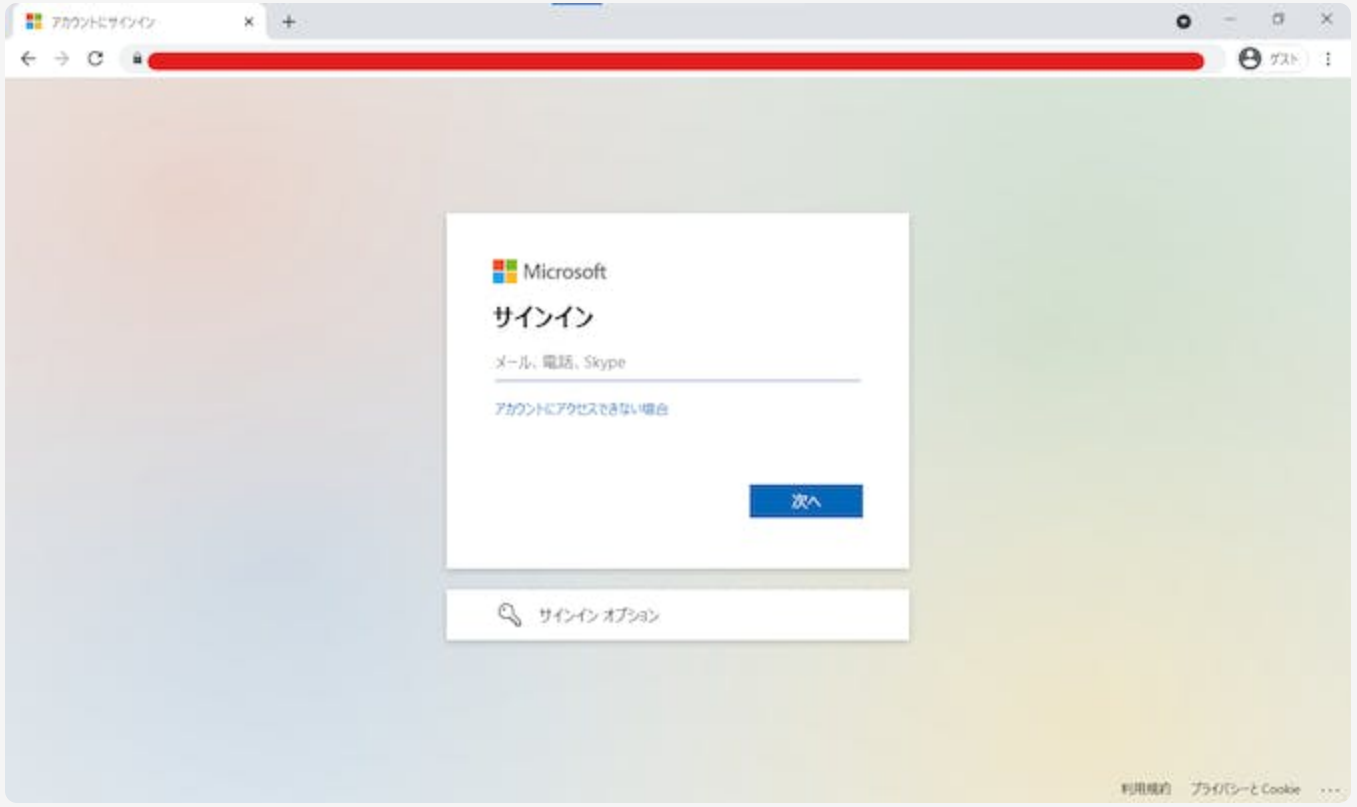
AAD 固有の注意点

ezaad を作成するにあたり、AAD 固有の注意点として以下のようなものがありました。

- SCIM2
  - 資格情報で refresh token を利用できない(ギャラリーに公開するとできるらしい)
  - `PATCH` 時の `active` が `boolen` でない等(参考)
- App Service 認証
  - 認証後にリダイレクトする場合、`/.auth/login/aad` へ `post_login_redirect_url` を付与する

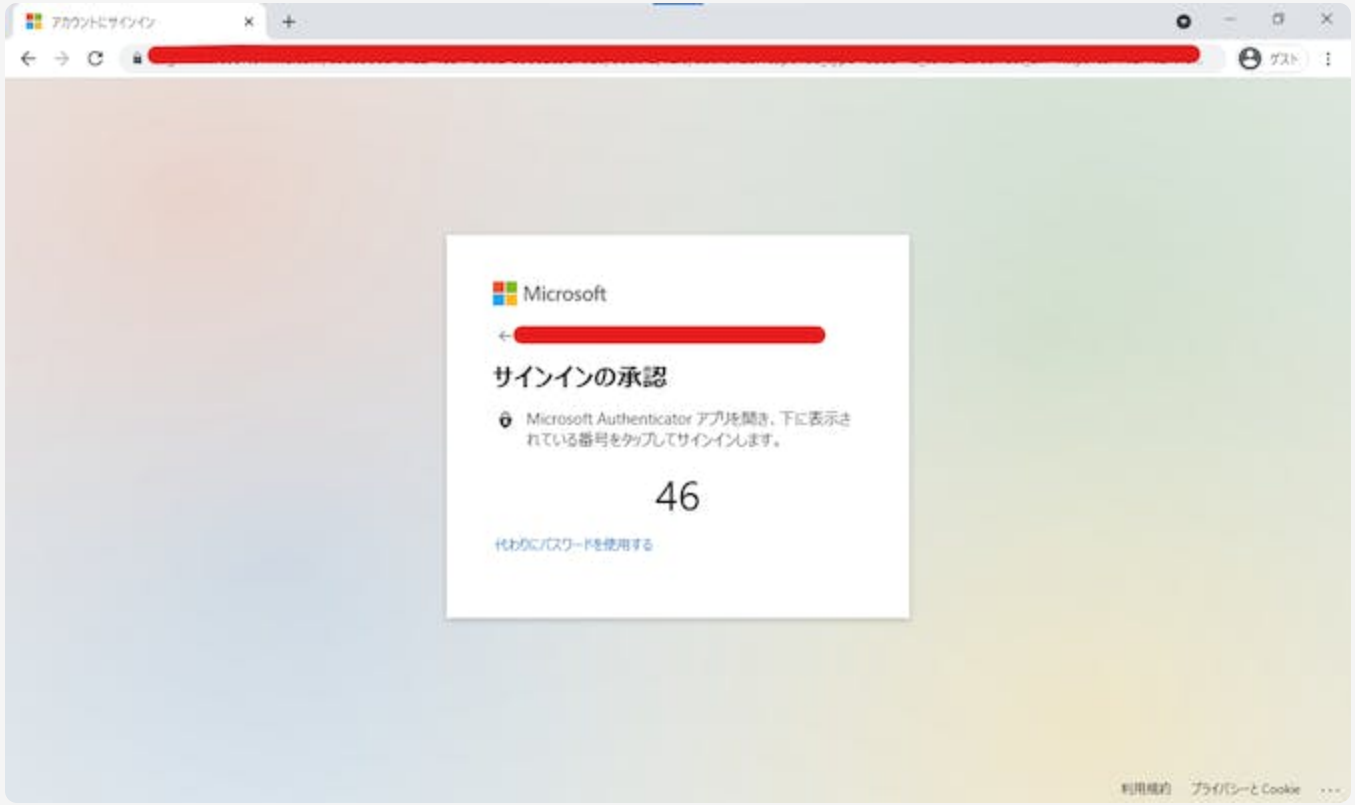
動作画面 1

`ezaad/login` を開くと AAD のサインイン画面へリダイレクト。



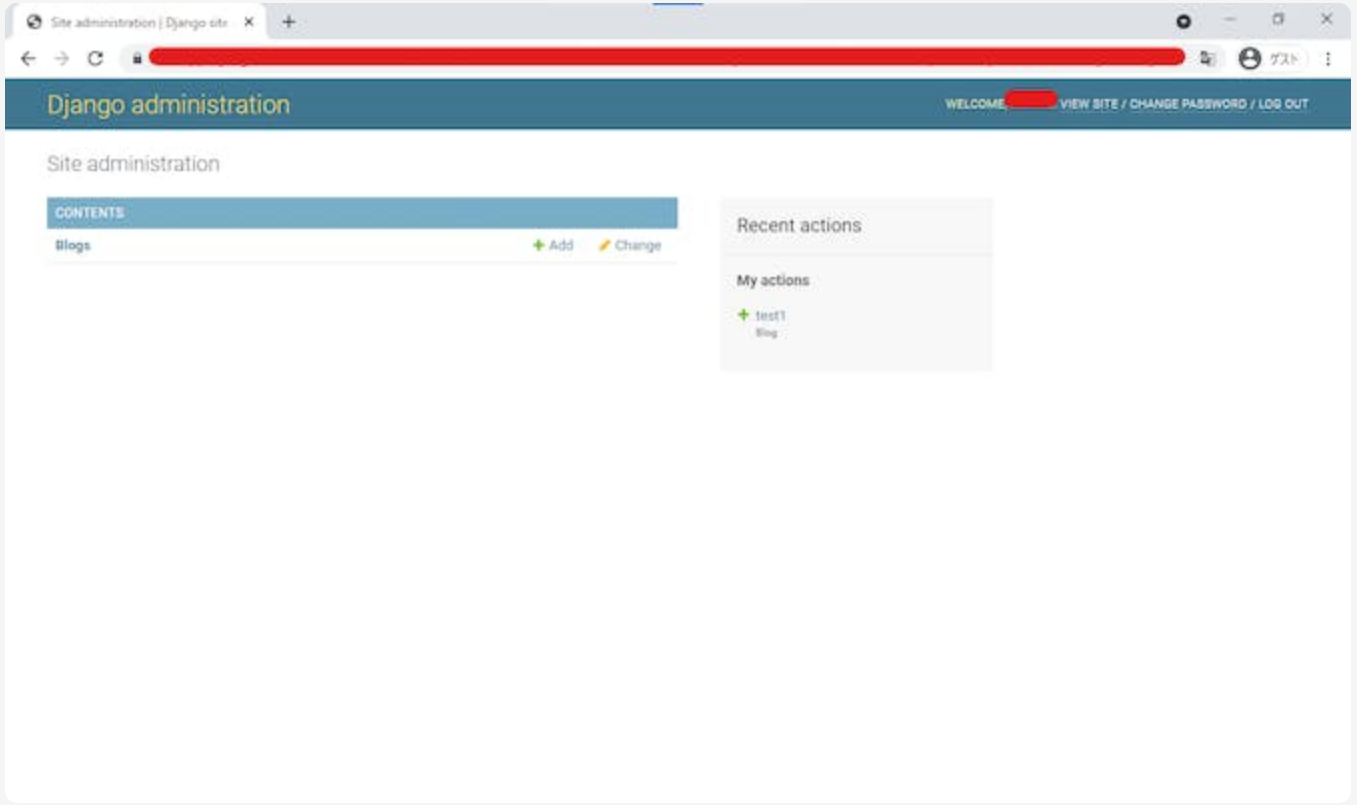
動作画面 2

AAD 側で設定していれば MFA、パスワードレス等も適用される。



動作画面 3

認証完了後は Django へログインしリダイレクト。



おわりに

基本的には目的としていた運用が可能なことは確認できました。しかし、以下のような問題もあるため、もう少し対応を考える必要もありそうです。

- Azure 非ギャラリーアプリでは SCIM2 資格情報の扱いが実用に適さない
  - cron 等での独自対応は難しそう(資格情報の更新方法が不明)
  - Access Token の有効期間を大きくとる方法は...