Implementation of Keycloak IAM

Aaron Urrea • Professor Michael Soltys • COMP-499 Capstone Spring 2023

Background

Keycloak is an open-source identity and access management software tool used to authenticate and authorize users within a system. Specifically, Keycloak is a tool used to secure web applications and services with relative ease, and can be dynamically deployed to a variety of systems. Keycloak offers simple deployment and services such as Single Sign-On (SSO), User Registration, Social Media Login, Two Factor Authentication, and others.
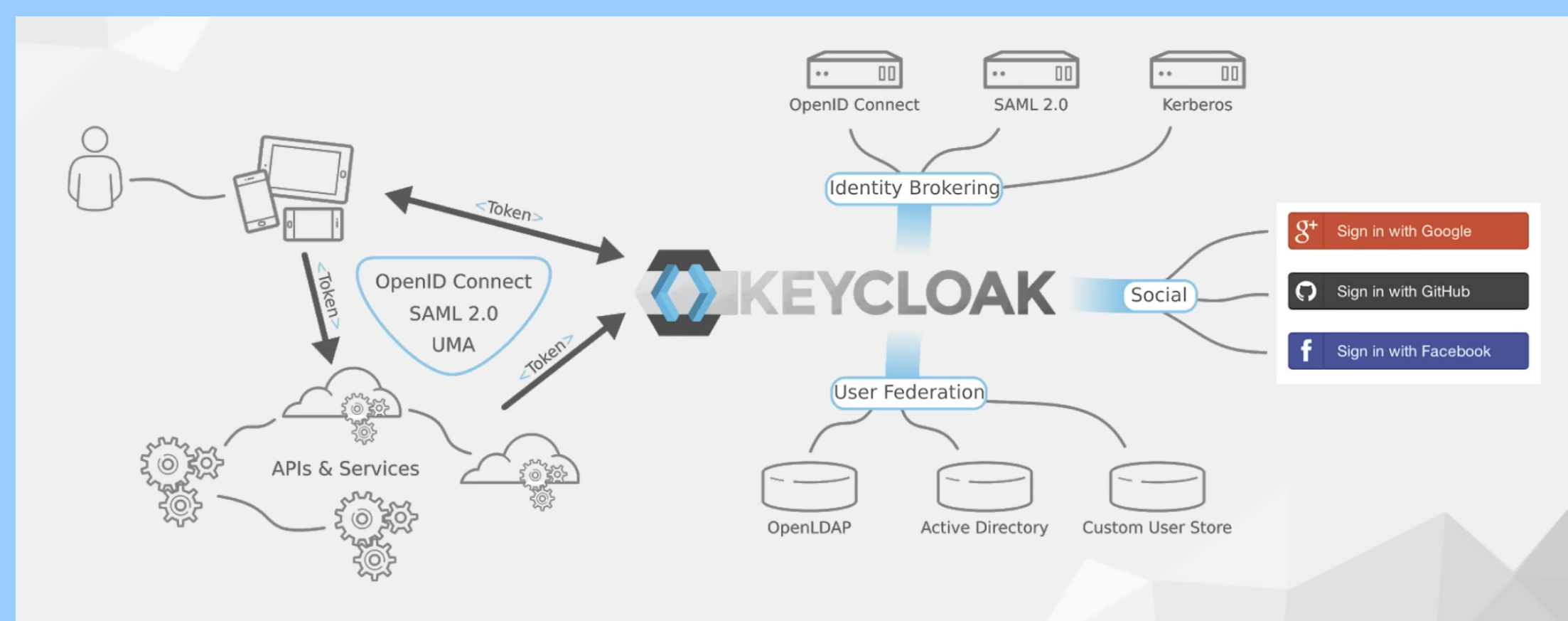

Figure 1: Scope of Keycloak's Ability

The application which Keycloak is going to be attached to is a Wordpress web server. Wordpress is a widely-used content management system (CMS) that allows users to create and manage websites easily. As a popular CMS, Wordpress is often targeted by hackers looking to exploit vulnerabilities in the system. One common method of attack is to steal user credentials, which can lead to unauthorized access and data breaches. With Keycloak, users can be authenticated using a range of methods, providing an extra layer of security to the Wordpress server.

Challenges

Some difficulties that arose with this implementation is that ideally, the Wordpress server would have been hosted on the already created + setup CI Keys server. However, due to lacking specific permissions, as well as not having enough space on the disk itself, the server needed to be hosted on an external computer. Because of this, outside resources (both financial and physical) were required that could not be provided by the university. While maintaining greater control is a benefit from self-hosting the applications demonstrated, there was also the cost of labor in regards to setting and configuring the server, whereas CI Keys is already configured to host a web server.

The majority of the time spent during this development was configuring Keycloak correctly and ensuring that there were minimal, if any, lapses in security. Configuring the Keycloak plugin for Wordpress can be complex, especially if you're not familiar with the underlying technology. Misconfiguration can cause unexpected behavior and potential security vulnerabilities, and weeks of research finally lead to a configuration which is secure, available, and functioning as expected.

Implementation

The implementation of this software is fairly straightforward, as there are three main components the deployment:

- MySQL Database
- Wordpress Web Server
- Keycloak IAM

Each component is hosted locally on an external computer hosted outside of campus. In addition to this, each component is running off of a Docker image as to support ease of distribution and future proofing for potential Kerberos deployment.

Figure 2: Docker Container Running on Server

In order to communicate to and from the Keycloak application, the Wordpress plugin "miniOrange SSO using SAML 2.0" is used. From here, the user would login through the Wordpress application portal, and be met with the ability to login through Keycloak. The application then redirects the user to authenticate with Keycloak, and with valid credentials, the user is then permitted to access the application.
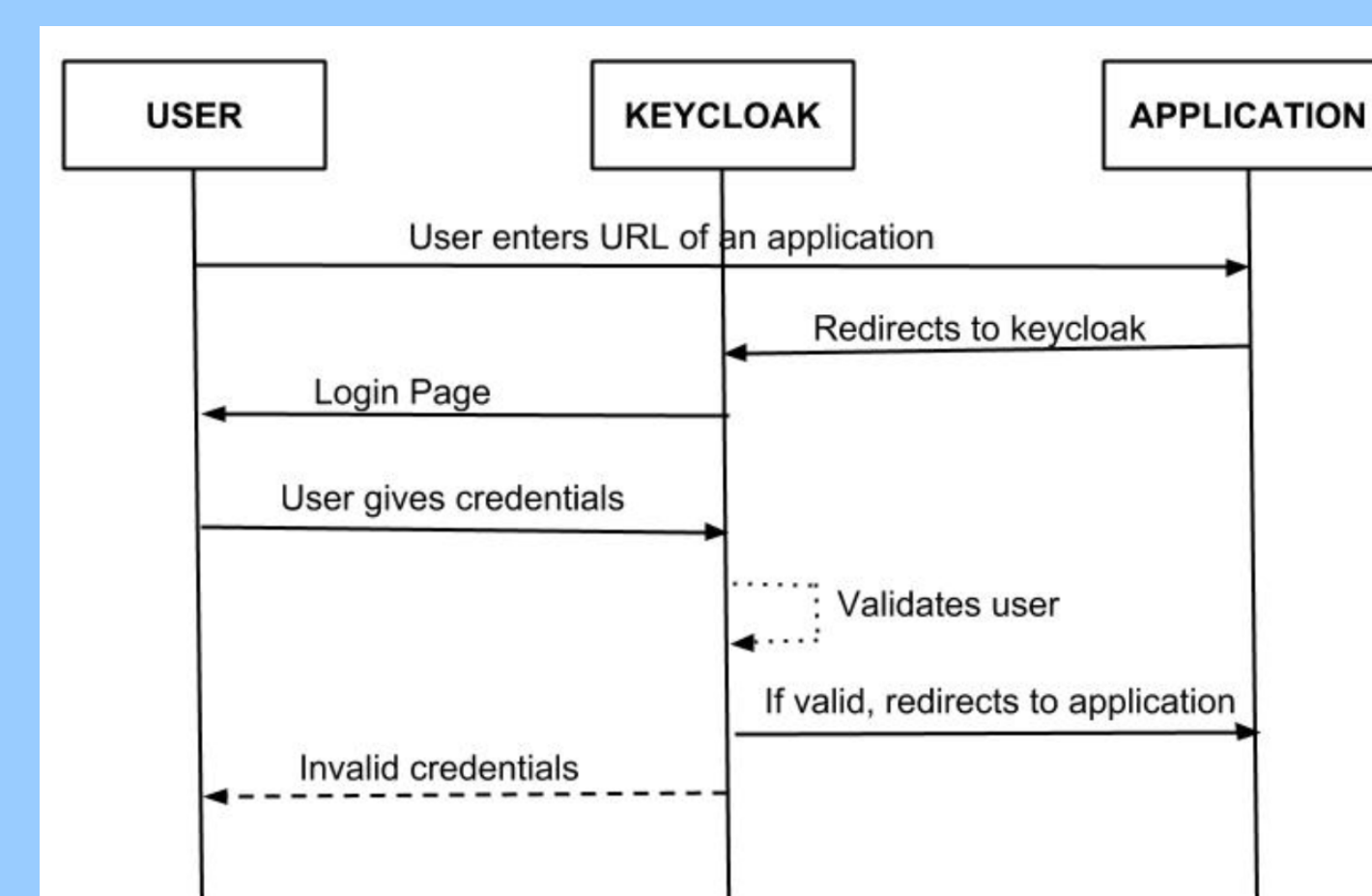

Figure 3: Flowchart of Keycloak Operation

Once this initial implementation was accomplished, Keycloak offers a variety of additional services that were implemented. For example, Keycloak allows for users to sign in with social media accounts, allowing for further user experience and ease. Currently integrated are Google, Instagram, and LinkedIn. Keycloak makes this process very easy, as all that is necessary is to create an "application" through the appropriate provider, which provides Keycloak with a Client ID and a Secret Key, and which Keycloak provides a redirect url.
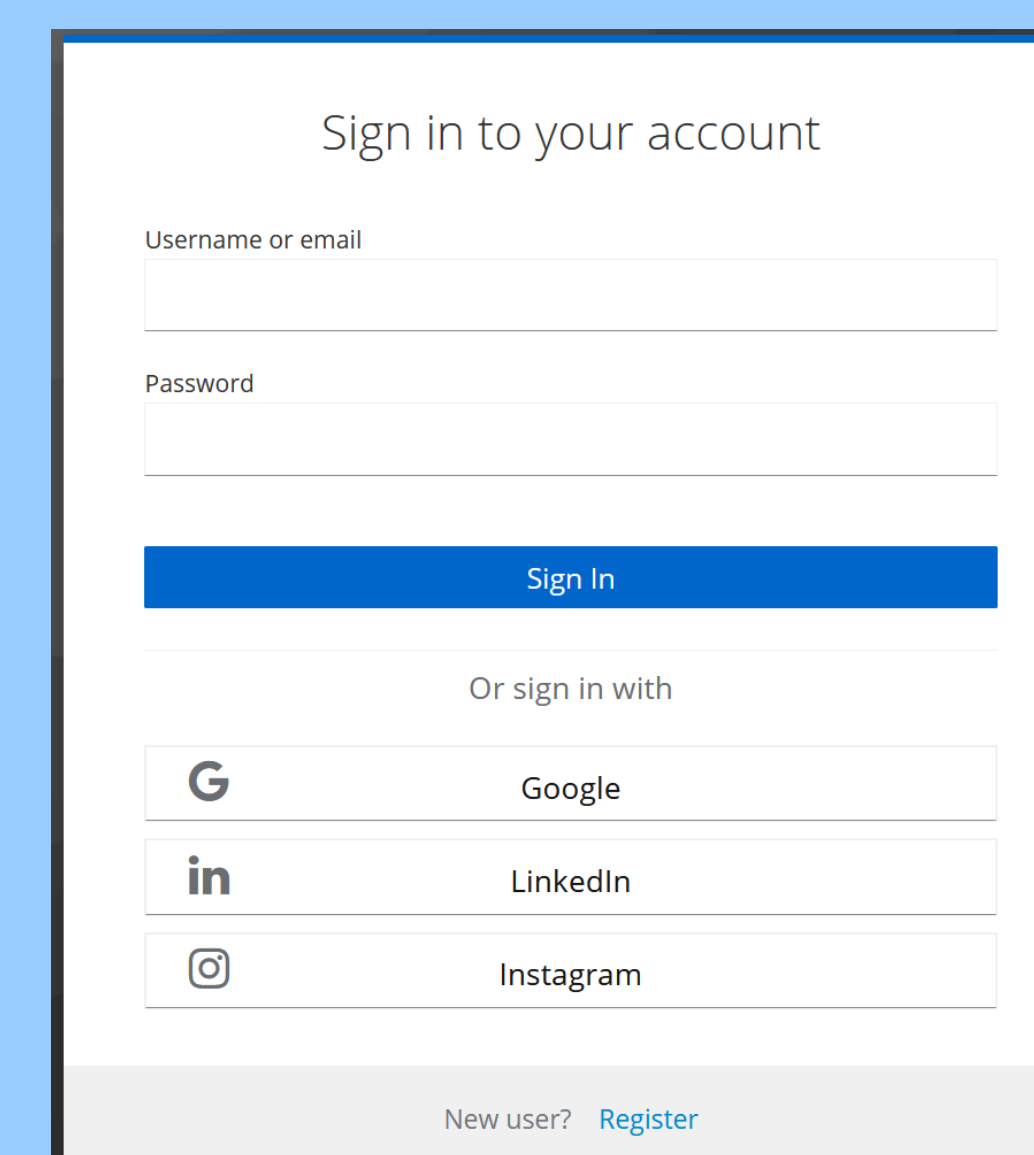

Figure 4: Social Media Integration

Results

After much configuration, testing, and design, the resulting implementation have met not only requirements but expectations as well. A fully functional MySQL database, Wordpress web server, and Keycloak IAM with desired features.

Figure 5: QR Code Leading to Web Server

Conclusions

After researching and implementing a Wordpress server with Keycloak integration, the following conclusions can be drawn:

1. Keycloak provides a layer of security to the Wordpress server, allowing for a centralized and secure way of managing user access and permissions.
2. With Keycloak integration, user management is centralized, making it easier to manage user access and permissions across multiple applications.
3. Keycloak provides the ability to scale user authentication and authorization across multiple applications, making it a reliable solution for businesses that require high scalability.
4. The integration process between Wordpress and Keycloak is straightforward and well-documented, making it easy for developers to integrate the two platforms.
5. With Keycloak integration, users can log in to multiple applications with a single set of credentials, enhancing the overall user experience.

Overall, the integration of Keycloak with a Wordpress server provides a secure, scalable, and user-friendly solution for managing user access and permissions to many applications. In the future, I will most definitely integrate Keycloak into my personal projects, as the ease of deployment and security benefits are very beneficial.

Acknowledgements