**Analysis for Identity Management Providers**

We are looking for user management functionality with user authentication and API authorization. User authentication can have custom logic to validate to sign up and sign in.

* Custom logic the UI and workflow for user signup and sign in.
* Control on the database details.
* Terraform support for IaC
* Running of script with spring boot project
* Integrate with Office 365

**Amazon Cognito**

Cognito is a user identity service by Amazon Web Services (AWS). The service allows you to add the ability to register, authorize and control user access to mobile and Internet applications. Amazon Cognito scales to millions of users. Supports authorization with social identity providers (Apple, Facebook, Google, Amazon) as well as enterprise identity providers based on SAML 2.0 and OpenID Connect, OAuth 2.0.

**Advantages**

* Provides B2C authentication and authorization
* Pricing is very less as compared to other providers
* Integration with other AWS services

**Disadvantages**

* Setup is not very easy and not friendly
* Developer experience - Single service with three features - User Pools, Identity Pools and Sync.
* Development and issue support is not good
* Documentation is not good - some features are not documented with examples and use cases
* Features are limited and more related to functionality provided by AWS and its services.
* UI customisation is possible, but must write your own code
* Migration is not possible - does not allow to export password hashes
* Multi region support is not available

**Okta**

Okta is market leader in identity management. Okta offers authentication, hosted sign on experience by default, integration with multiple SSO provider

**Advantages**

* Focused on B2E, business's identity management
* Provides complex integration, legacy applications and other contractual support

**Disadvantages**

* Pricing is very high in compared to all identity providers
* Passwords are not part of profile
* Okta inline hooks does not take http and localhost URL.
* Need to provide your own authorization server
* Need to provide your own custom authentication
* Migration from one authenticator to another is not possible.
* <https://www.okta.com/pricing/>

**Auth0**

Auth0 provides multiple functionalities like single sign-on, breached password detection, multi-factor authentication, and user identity management solutions for customers, business partners, and employees. It also provides opportunities for developers and security professionals.

Its platform also allows users to authenticate to active directory, LDAP, SAML, Integrated Windows Authentication, Google Apps, Salesforce, and other IdPs.

Auth0 runs in their public cloud; however, they also offer options to host it in a private cloud.

Auth0 also provides custom logic integration for user authentication, terraform support, running project with spring boot etc.

**Advantages**

* Provides B2C authentication and authorization
* Simple setup - authentication with app is simple
* SDK and integration support
* Large feature set

**Disadvantages**

* Expensive than other providers except Okta
* Opaque pricing for large customer base
* Extensibility - adding rules and hooks is limited to pricing levels

**Functionalities reviewed with Auth0:**

* Able to create application for client id and secret
* Code and run it with Spring boot, we can do customizations
* Create custom database connection
* Create custom action for pre-registration
* Create user from signup page
* Support for secrets store

**To-do with Auth0:**

* Customize signup page
* Integration with custom domain
* Check for delete user script
* Integration for secrets and storage of secrets
* Check for other fields requirement
* Check for more options in actions
* Check for terraform script