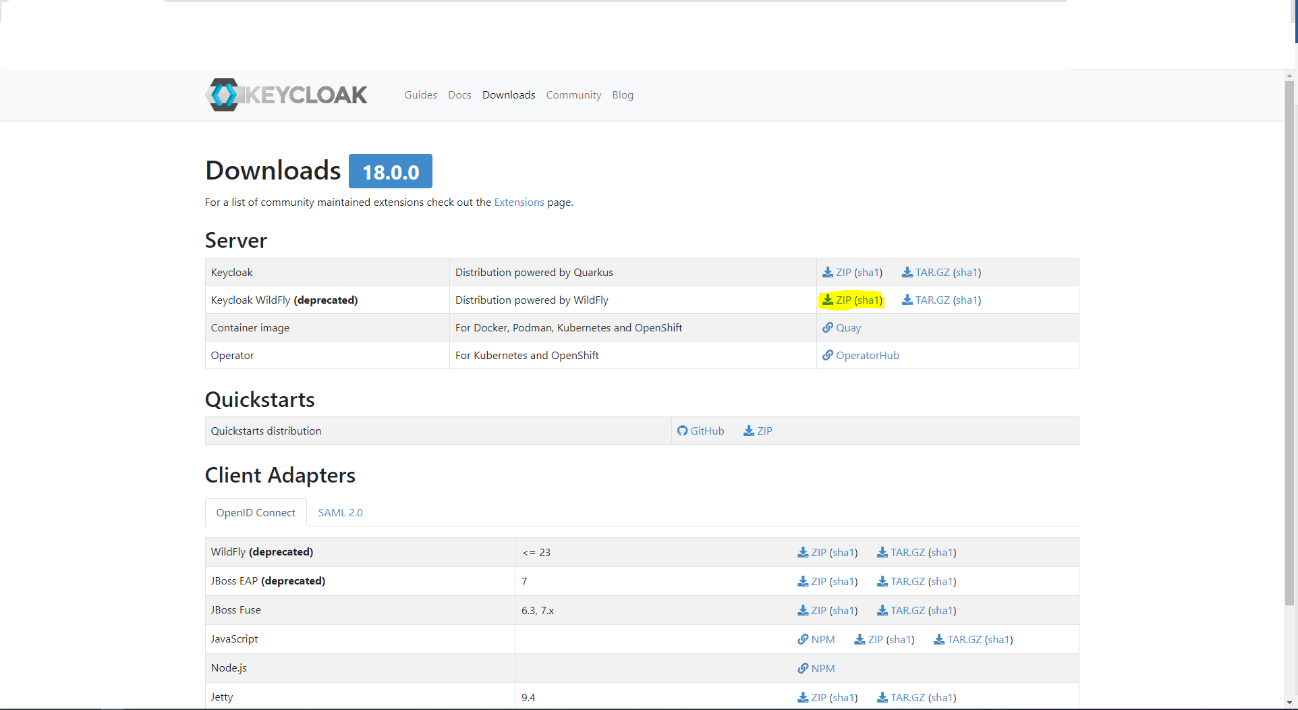
**Tìm hiểu về Keycloak**

1. **Keycloak là gì?**

* Keycloak nó là một công cụ mã nguồn mở dành cho việc quản lý access cho một ứng dụng bất kỳ.
* Mục đích chính của keycloak là cung cấp "giải pháp quản lý danh tính và quyền truy cập cho các ứng dụng hiện đại".
* Chúng ta có thể sử dụng nó để hiện thực phần authentication và authorization cho ứng dụng của mình.

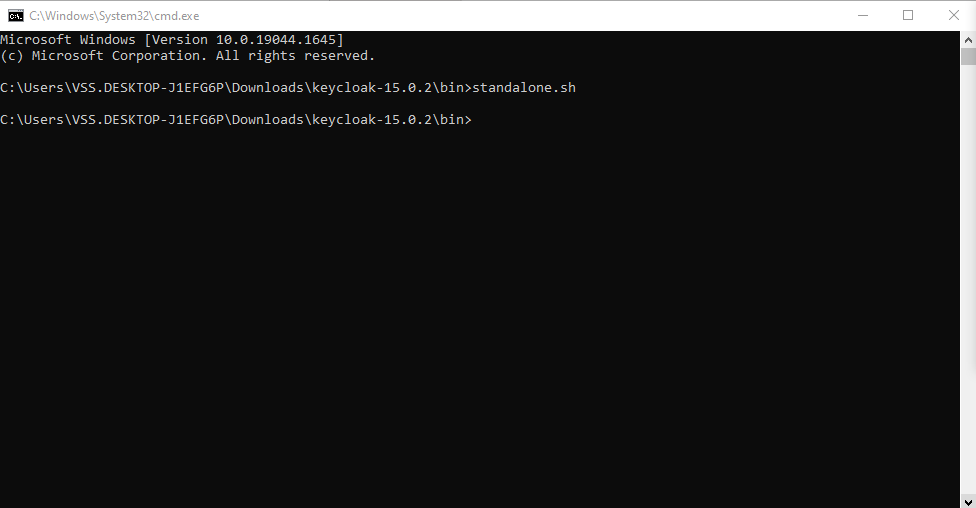
1. **Cài đặt Keycloak trên windows?**

* Truy cập trang: <https://www.keycloak.org/downloads>
* Chọn phiên bản mới nhất hoặc các phiên bản cũ hơn

****

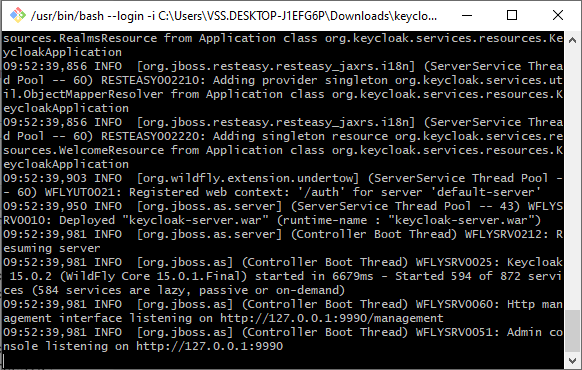
*Hình 1*

* Download và giải nén
* Để start server chúng ta đi đến thư mục **bin** của folder Keycloak vừa giải nén và chạy lệnh **standalone.sh** như hình 2



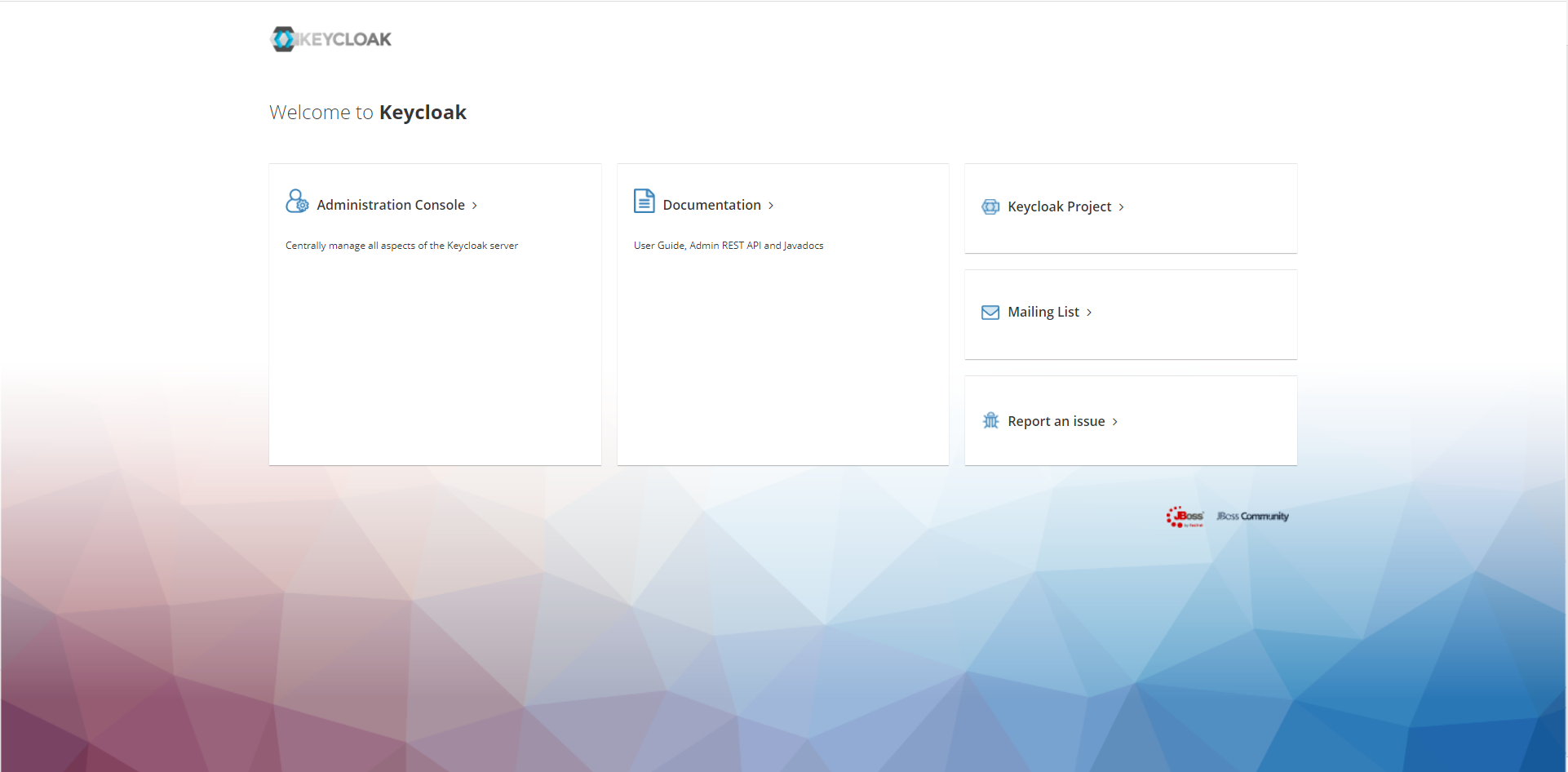
*Hình 2*

* Chạy server thành công chúng ta được kết quả:



*Hình 3*

* Sau khi start Keycloak server xong, chúng ta cần truy cập tới địa chỉ <http://localhost:8080/>



*Hình 4*

1. **Tại sao lại sử dụng Keycloak?**

* Khi chúng ta có 1 website. Các thành viên trong team có thể vào weblate qua các account tôi tạo hoặc invite họ qua email. Tất nhiên điều này không có vấn đề gì khi số lượng user không lớn, tôi có thể tạo bằng tay hoặc nhập email của các bạn trong team rồi invite để họ vào, set password là có thể sử dụng.
* Vấn đề chỉ xuất hiện khi số lượng người dùng trở nên nhiều hơn, và tôi thì lười invite bằng tay. Vậy có cách nào để một user có thể dùng tài khoản đang có để login vào Weblate? Xa hơn nữa thì bất kỳ ứng dụng nào cũng có thể login được bằng tài khoản công ty cấp mà không cần đăng ký mới lằng nhằng? Vấn đề này sẽ được giải quyết bằng KEYCLOAK – công nghệ hàng đầu thế giới cho việc quản lý user tập trung!

1. **Tính năng của Keycloak?**

* **Hỗ trợ nhiều giao thức:** OpenId Connect, OAuth 2.0, SAML 2.0
* **SSO:** Keycloak có hỗ trợ cho đăng nhập 1 lần và đăng xuất 1 lần
* **Bảng điều khiển dành cho quản trị viên:**
  + Cung cấp GUI trên web
  + Chúng ta có thể tự custom tất cả các cấu hình mà phiên bản của bạn yêu cầu để hoạt động như bạn mong muốn.
* **Danh tính người dùng và quyền truy cập:**
  + Keycloak có thể được sử dụng làm trình quản lý truy cập và nhận dạng người dùng độc lập bằng cách cho phép chúng ta tạo CSDL người dung với các vai trò và nhóm tùy chỉnh. Thông tin này có thể được sử dụng them để xác thực người dung trong ứng dụng của chúng tôi và bảo mật các phần của nó dựa trên các vai trò được xác định trước.
* **Đồng bộ hóa nguồn nhận dạng bên ngoài:**
  + Trong trường hợp khách hang bên ngoài của bạn hiện có một số loại CSDL người dung, Keycloak cho phép đồng bộ hóa vs CSDL đó.
  + Theo mặc định, nó hỗ trợ LDAP và Active Directory nhưng bạn có thể tạo tiện ích mở rộng tùy chỉnh cho bất kỳ CSDL người dung nào bằng cách sử dụng API lưu trữ người dung Keycloak.
* **Môi giới nhận dạng:**
  + Keycloak cũng có thể hoạt động như một proxy giữa người dung của bạn và một số nhà cung cấp hoặc nhà cung cấp danh tính bên ngoài.
  + Danh sách của họ có thể được chỉnh sửa từ Keycloak Admin Panel.
* **Nhà cung cấp danh tính xã hội:**
  + Keycloak cho phép chúng ta sử dụng nhà cung cấp nhận dạng xã hội.
  + Nó hỗ trợ tích hợp Google, Twitter, Facebook, StackOverFlow nhưng bạn phải cấu hình tất cả chúng theo cách thủ công từ bảng quản trị viên
* **Tùy chỉnh trang:**
  + Keycloak cho phép bạn tùy chỉnh tất cả các trang được nó hiển thị cho nguoiwf dung của bạn.
  + Các trang đó có .ftl định dạng để bạn có thể sử dụng các HTML đánh dấu và CSS kiểu cổ điển để làm cho trang phù hợp với kiểu ứng dụng và thương hiệu công ty của bạn.
* **Phân phối của Keycloak:**
  + Hiện tại, Keycloak có 3 phân phối chính:
    - Người phục vụ:
      * Ứng dụng độc lập có thể tải xuống từ trang Keycloak dưới dạng tệp lưu trữ tar hoặc zip với tất cả các tập lệnh, tài liệu và nội dung cần thiết để hoạt động bình thường.
      * Hiện tại có hai phiên bản chính của bản phân phối này: WIldFLy, Quarkus
    - Docker Image:
      * Phân phối thích hợp cho Docker, Podman, Kubernetes và OpenShift
    - Nhà điều hành:
      * Phân phối cho kuberntes và OpenShift dựa trên SDK của nhà điều hành.

1. **Tổng quan về các khái niệm trong Keycloak:**

* **Realms:**
* Realm là một khái niệm trong Keycloak để chỉ một đối tượng quản lý một tập các user cùng với thông tin đăng nhập, role và group của những user đó.
* Một user trong Keycloak chỉ thuộc về một realm và user khi đăng nhập vào Keycloak sẽ đăng nhập vào realm của user đó.
* Chúng ta có thể có nhiều realm trong một Keycloak server, các realm này sẽ độc lập với nhau và chúng chỉ manage users của chúng.
* Khi start Keycloak server, mặc định 1 master realm sẽ được khởi tạo.
  + Master realm là realm có quyền lực cao nhất trong các realm, user admin trong master realm sẽ có quyền xem và quản lý các realm khác.
  + Không nên sử dụng master realm để quản lý users và các thông tin khác của chúng trong Keycloak. Nó chỉ nên được sử dụng để user admin của nó tạo và quản lý các realm. Mỗi realm cần phải có user admin riêng và chúng ta sẽ sử dụng user admin của từng realm để quản lú users cho realm đó.
* Realms: là một lĩnh vực quản lý 1 tập hợp User, Credential, Role và Group. Một người dùng thuộc về và đăng nhập vào một lĩnh vực. Các lĩnh vực không thể giao tiếp với nhau.
* **Client trong Keycloak:**
* Client trong Keycloak là những ứng dụng sẽ tương tác với nó để authentication và authorization.
* Việc thêm mới client trong Keycloak là để nó quản lý tất cả những client sẽ connect tới nó, theo giao thức, chuẩn authentication và authorization.
* Clients: là các thực thể có thể yêu cầu Keycloak xác thực người dùng. Thông thường, client là các ứng dụng (application) và dịch vụ (service).
* **User:**
* Người dùng là các thực thể có thể đăng nhập vào hệ thống.
  + Các thuộc tính: email, username, password, address, phoneNumber, dateOfBirth.
  + User có thể được gán vào Group có các Role cụ thể.
  + User có thể được gán Role cụ thể.
* **Authentication:** Quá trình xác định và xác thực người dùng
* **Authorization:** Quá trình cấp quyền truy cập cho người dùng
* **Credentials:** Thông tin xác thực là những phần dữ liệu mà Keycloak sử dụng để xác minh danh tính của người dùng. Một số ví dụ là password, password dùng một lần, chứng chỉ kỹ thuật số hoặc thậm chí cả dấu vân tay.
* **Roles:** Vai trò xác định một loại hoặc danh mục người dùng.
* **User role mapping:** Gán user vào các role mà user đó có thể có
* **Composite roles:** Thể hiện sự kế thừa trong việc phân quyền (quyền to hơn có thể thực hiện được quyền nhỏ hơn khi đã thực hiện mapping role).
* **Groups:** Groups quản lý các nhóm người dùng. Các thuộc tính có thể được xác định cho một nhóm. Có thể gán các Role cho một Group. User trong 1 nhóm kế thừa các thuộc tính và Role mà nhóm đó xác định.
* **Consent:** là khi bạn với tư cách là quản trị viên muốn người dùng cấp quyền cho một client trước khi ứng dụng đó thể tham gia và quá trình xác thực. Sau khi người dùng cung cấp thông tin đăng nhập của họ, Keycloak sẽ bật lên màn hình xác định khách hàng yêu cầu đăng nhập và thông tin nhận dạng nào được yêu cầu của người dùng. Người dùng có thể quyết định có cấp yêu cầu hay không.
* **Client scope:** Khi một client đã đăng ký, scope xác định phạm vi vai trò cho ứng dụng khách.
* **Client role:** Client có thể xác định role cụ thể cho client.
* **Identity token:** Cung cấp thông tin nhận dạng về người dùng
* **Access token:** Cung cấp quyền truy cập vào dịch vụ đang được gọi.
* **Assertion:** Thông tin về người dùng trong phản hồi xác thực SAML đã cung cấp siêu dữ liệu nhận dạng về người dùng đã được xác thực.
* **Service account:** Mỗi khách hàng có một tài khoản dịch vụ tích hợp cho phép khách hàng có được access token.
* **Direct grant:** Một cách để khách hàng có được Access Token thay mặt cho người dùng thông qua lệnh gọi REST.
* **Protocol mappers:**  OIDC hoặc SAML
* **Session:** Khi người dùng login, một phiên được tạo để quản lý phiên đăng nhập. Một phiên chứa thông tin như thời điểm người dùng đăng nhập và những ứng dụng nào đã tham gia trong một lần đăng nhập trong phiên đó. Cả quản trị viên và người dùng đều có thể xem thông tin phiên.
* **User federation provider:** Keycloak có thể lưu trữ và quản lý người dùng. LDAP hoặc Active Directory để lưu trữ thông tin người dùng và thông tin xác thực.
* **Identity provider:** Nhà cung cấp danh tính (IDP) là một dịch vụ có thể xác thực người dùng. Keycloak là một IDP.
* **Identity provider federation:** Keycloak có thể được xác định cấu hình để ủy quyền xác thực cho một hoặc nhiều IDP (Facebook Google). Keycloak có thể ủy quyền xác thực cho bất kỳ OpenID Connect hoặc SAML 2.0 IDP nào khác.
* **Identity provider mappers:** Khi thực hiện liên kết IDP, bạn có thể ánh xạ các mã thông báo và xác nhận đến với các thuộc tính người dùng và phiên. Điều này giúp bạn truyền thông tin nhận dạng từ IDP bên ngoài đến khách hàng của bạn yêu cầu xác thực.
* **Required actions** : Các hành động mà người dùng phải thực hiện trong quá trình xác thực. Người dùng không thể kết thúc quá trình xác thực nếu không required actions.
* **Authentication flows** : Các luồng xác thực là các luồng công việc mà người dùng phải thực hiện khi tương tác với các khía cạnh nhất định của hệ thống.
* **Events** : Sự kiện là các luồng kiểm tra mà admin có thể xem và tham gia.
* **Themes** : Keycloak cung cấp themer mặc định . Có thể sửa themes.