







STT	Người ký	Đơn vị	Thời gian ký	Ý kiến
1	TỔNG CÔNG TY GIẢI PHÁP DOANH NGHIỆP VIETTEL - CHI NHÁNH TẬP ĐOÀN CÔNG NGHIỆP - VIỆN THÔNG QUÂN ĐỘI		21/06/2022 16:55:35	Đã đóng dấu
2	LÊ THÀNH CÔNG	Phó Tổng Giám đốc - Ban Tổng Giám đốc - Tổng công ty Giải pháp doanh nghiệp Viettel	21/06/2022 16:51:08	
3	PHẠM NGỌC SƠN	Phó Giám đốc Trung tâm - Trung tâm Công nghệ thông tin - Tổng công ty Giải pháp doanh nghiệp Viettel	21/06/2022 09:28:54	
4	ĐẶNG TRUNG ANH	Giám đốc Trung tâm - Ban Giám đốc - Trung tâm Nghiên cứu và phát triển sản phẩm nền tảng - Tổng công ty Giải pháp doanh nghiệp Viettel	21/06/2022 07:52:47	
5	ĐỖ ĐÌNH THẮNG	Phó Giám đốc Trung tâm Giải pháp Doanh nghiệp - Ban Giám đốc - Trung tâm Giải pháp doanh nghiệp - Tổng công ty Giải pháp doanh nghiệp Viettel	20/06/2022 14:27:16	

	TỔNG CÔNG TY GIẢI PHÁP DOANH NGHIỆP VIETTEL		Mã hiệu: HD.VTS.TTGPDN.02
	TÀI LIỆU GUIDELINE KEYCLOAK		Ngày có hiệu lực: 20/06/2022
			Ngày hết hiệu lực: 20/06/2023
			Lần ban hành: 01
			Trang: 1/33

BẢNG THEO DÕI SỬA ĐỔI


TT	Trang	Nội dung sửa đổi	Ngày hiệu lực
		Soạn thảo lần đầu: [Bùi Văn Khánh Duy – Duybvk@viettel.com.vn – TT GPDN]	20/06/2022
1.	Toàn bộ	Tạo mới tài liệu	20/06/2022

	Biên soạn	Kiểm tra	Thẩm định	Phê duyệt
Chữ ký	Bùi Văn Khánh Duy	TRUNG TÂM GIẢI PHÁP DOANH NGHIỆP	TRUNG TÂM CÔNG NGHỆ THÔNG TIN	KT. TỔNG GIÁM ĐỐC PHÓ TỔNG GIÁM ĐỐC
		 Đỗ Đình Thắng	 Phạm Ngọc Sơn TRUNG TÂM CÔNG NGHỆ THÔNG TIN CỨU VÀ PHÁT TRIỂN NỀN TẢNG	 Thiếu tá Lê Thành Công
			 Đặng Trung Anh	

	TỔNG CÔNG TY GIẢI PHÁP DOANH NGHIỆP VIETTEL	Mã hiệu: HD.VTS.TTGPDN.02
	TÀI LIỆU GUIDELINE KEYCLOAK	Ngày có hiệu lực: 20/06/2022
		Ngày hết hiệu lực: 20/06/2023
		Lần ban hành: 01
		Trang: 2/33

MỤC LỤC

1. Mục đích.....	3
2. Phạm vi, đối tượng áp dụng	3
3. Tài liệu liên quan.....	3
4. Giải thích thuật ngữ và từ viết tắt.....	3
5. Nội dung.....	6
5.1 Giới thiệu về Keycloak.....	6
5.2 Cài đặt và cấu hình Keycloak.....	8
5.2.1 Cấu hình tối thiểu	8
5.2.2 Cấu trúc thư mục Distribution.....	8
5.2.3 Các mô hình hoạt động của Keycloak	8
5.2.3.1 Standalone mode	9
5.2.3.2 Standalone cluster mode	10
5.2.3.3 Domain cluster mode	13
5.2.4 Cấu hình Database.....	16
5.2.4.1 Tải xuống JDBC driver cho database cần dùng	16
5.2.4.2 Khai báo và load JDBC driver.....	18
5.2.4.3 Thay đổi cấu hình datasource	19
5.2.5 Cấu hình Cache	19
5.2.5.1 Eviction and expiration	20
5.2.5.2 Replica and failover	21
5.2.5.3 Disable caching	21
5.2.5.4 Clear cache in runtime	22
5.2.6 Cài đặt Keycloak Server trên Linux.....	22
5.2.6.1 Tải bộ cài đặt Keycloak Server.....	22
5.2.6.2 Cài đặt và cấu hình.....	22
5.2.6.3 Cấu hình keycloak chạy với Database Oracle	24
5.2.6.4 Cấu hình Keycloak chạy theo mô hình standalone cluster.....	25
5.3 Một số tính năng cơ bản trong Keycloak	27
5.3.1 Tạo tài khoản admin.....	27
5.3.2 Tạo realms	28
5.3.3 Tạo client trong realms.....	29
5.3.4 Tạo user	31

	TỔNG CÔNG TY GIẢI PHÁP DOANH NGHIỆP VIETTEL	Mã hiệu: HD.VTS.TTGPDN.02
	TÀI LIỆU GUIDELINE KEYCLOAK	Ngày có hiệu lực: 20/06/2022
		Ngày hết hiệu lực: 20/06/2023
		Lần ban hành: 01
		Trang: 3/33

NỘI DUNG TÀI LIỆU

1. Mục đích

Tài liệu này được xây dựng nhằm giúp tìm hiểu thêm về Keycloak và cơ bản về cách cấu hình, triển khai và cài đặt Keycloak.

2. Phạm vi, đối tượng áp dụng

Áp dụng cho toàn bộ các đơn vị sản xuất trực thuộc Tổng Công ty Giải pháp doanh nghiệp Viettel, phục vụ thành viên đội dự án trong việc xây dựng một hệ thống sử dụng Keycloak.

3. Tài liệu liên quan

TT	Tài liệu	Nguồn	Ngày ban hành
1.	Keycloak	https://www.keycloak.org/documentation	


4. Giải thích thuật ngữ và từ viết tắt

- Thuật ngữ


TT	Thuật ngữ	Diễn giải
1.	Keycloak	Keycloak là một sản phẩm phần mềm nguồn mở cho phép đăng nhập một lần (IdP) với Quản lý danh tính và Quản lý truy cập cho các ứng dụng và dịch vụ hiện đại. Phần mềm này được viết bằng Java và hỗ trợ các giao thức liên kết danh tính theo mặc định SAML v2 và OpenID Connect (OIDC) / OAuth2. Nó được cấp phép bởi Apache và được hỗ trợ bởi Red Hat
2.	API	Application Programming Interface Đó là các phương thức, giao thức kết nối với các thư viện và ứng dụng khác
3.	Java	Java là một ngôn ngữ lập trình hiện đại, bậc cao, hướng đối tượng, bảo mật và mạnh mẽ

- Từ viết tắt

TT	Từ viết tắt	Diễn giải
1.	GPDN	Giải pháp doanh nghiệp

	TỔNG CÔNG TY GIẢI PHÁP DOANH NGHIỆP VIETTEL		Mã hiệu: HD.VTS.TTGPĐN.02
	TÀI LIỆU GUIDELINE KEYCLOAK		Ngày có hiệu lực: 20/06/2022
			Ngày hết hiệu lực: 20/06/2023
			Lần ban hành: 01
			Trang: 4/33

TT	Từ viết tắt	Diễn giải
2.	LDAP	LDAP hay Lightweight Directory Access Protocol là một giao thức ứng dụng truy cập các cấu trúc thư mục. LDAP được thiết kế trên giao thức Internet TCP/IP. Một cấu trúc thư mục là một tập hợp các đối tượng có các thuộc tính hay đặc điểm tương tự và được sắp xếp theo logic thành nhiều cấp bậc
3.	SAML	SAML (Security Assertion Markup Language) là một chuẩn mở cho phép nhà cung cấp thực thể xác thực người dùng và ủy quyền cho người dùng sử dụng một dịch vụ nào đó của nhà cung cấp dịch vụ mà không bắt buộc người dùng phải tạo tài khoản đăng nhập vào dịch vụ đó.
4.	XML	Extensible Markup Language là ngôn ngữ đánh dấu mở rộng, có chức năng truyền dữ liệu và mô tả nhiều loại dữ liệu khác nhau.
5.	JDBC	(Java Database Connectivity) là một chuẩn API (Application Program Interface) cho phép kết nối các chương trình viết bởi Java với các hệ quản trị cơ sở dữ liệu
6.	HTTP	(HyperText Transfer Protocol) là giao thức truyền tải siêu văn bản được sử dụng trong www dùng để truyền tải dữ liệu giữa Web server đến các trình duyệt Web và ngược lại.
7.	JAR	JAR là viết tắt của cụm từ Java ARchive, cụ thể hơn là file nén. Chứa bên trong tệp JAR là nhiều tập tin khác nhau và được “đóng gói” lại với nhau nhằm mục đích giảm dung lượng lưu trữ. Là các ứng dụng được thiết kế để Java Runtime Environment sử dụng
8.	RDBMS	RDBMS là viết tắt của Relational Database Management System có nghĩa là hệ quản trị cơ sở dữ liệu quan hệ. RDBMS là cơ sở cho SQL, và cho tất cả các hệ thống cơ sở dữ liệu hiện đại như MS SQL Server, IBM DB2, Oracle, MySQL và Microsoft Access

	TỔNG CÔNG TY GIẢI PHÁP DOANH NGHIỆP VIETTEL	Mã hiệu: HD.VTS.TTGPDN.02
	TÀI LIỆU GUIDELINE KEYCLOAK	Ngày có hiệu lực: 20/06/2022
		Ngày hết hiệu lực: 20/06/2023
		Lần ban hành: 01
		Trang: 5/33

TT	Từ viết tắt	Diễn giải
9.	TCP	TCP (Transmission Control Protocol) là một giao thức truyền thông tin, sử dụng dữ liệu được truyền giữa các hệ thống qua mạng. Trong đó, dữ liệu được truyền dưới dạng packet. Nó bao gồm kiểm tra lỗi, đảm bảo việc phân phối và duy trì thứ tự của các packet.
10.	UDP	UDP (User Datagram Protocol) giống với giao thức TCP. Nhưng không đảm bảo việc kiểm tra lỗi và khôi phục dữ liệu. Nếu bạn sử dụng giao thức này, dữ liệu sẽ được gửi liên tục, không phân biệt vấn đề ở đầu nhận.
11.	IP	IP là viết tắt của từ Internet Protocol là một địa chỉ đơn nhất mà những thiết bị điện tử hiện nay đang sử dụng để nhận diện và liên lạc với nhau trên mạng máy tính bằng cách sử dụng giao thức Internet
12.	OTP	OTP là từ viết tắt của từ “One Time Password”, là mật khẩu chỉ sử dụng một lần duy nhất
13.	URL	URL là viết tắt của Uniform Resource Locator, dịch sang tiếng Việt là định vị tài nguyên thống nhất

	TỔNG CÔNG TY GIẢI PHÁP DOANH NGHIỆP VIETTEL	Mã hiệu: HD.VTS.TTGPDN.02
	TÀI LIỆU GUIDELINE KEYCLOAK	Ngày có hiệu lực: 20/06/2022
		Ngày hết hiệu lực: 20/06/2023
		Lần ban hành: 01
		Trang: 6/33

5. Nội dung

5.1 Giới thiệu về Keycloak

Keycloak là một sản phẩm phần mềm nguồn mở cho phép đăng nhập một lần với Quản lý danh tính và Quản lý truy cập cho các ứng dụng và dịch vụ hiện đại. Phần mềm này được viết bằng Java và hỗ trợ các giao thức liên kết danh tính theo mặc định SAML v2 và OpenID Connect / OAuth2. Nó được cấp phép bởi Apache và được hỗ trợ bởi Red Hat.

Keycloak có các tính năng sau:

✓ **Single-Sign On**

Xác thực tập trung người dùng với Keycloak thay vì các ứng dụng riêng lẻ. Điều này có nghĩa là các ứng dụng của chúng ta không phải xử lý các biểu mẫu đăng nhập, xác thực người dùng và lưu trữ người dùng. Sau khi đăng nhập vào Keycloak, người dùng không phải đăng nhập lại để truy cập vào một ứng dụng khác.

✓ **Identity Brokering and Social Login**


Dễ dàng thêm đăng nhập bằng mạng xã hội thông qua bảng điều khiển dành cho quản trị viên. Chúng ta chỉ cần chọn mạng xã hội muốn thêm mà không cần mã hoặc thay đổi ứng dụng.

Keycloak cũng có thể xác thực người dùng bằng OpenID Connect hoặc SAML 2.0 Identity Provider. Chỉ cần cấu hình Nhà cung cấp danh tính thông qua bảng điều khiển dành cho quản trị viên.

✓ **User Federation**

Keycloak có hỗ trợ kết nối tới LDAP hoặc máy chủ Active Directory. Chúng ta cũng có thể kết nối tới cơ sở dữ liệu lưu trữ thông tin người dùng.

✓ **Admin Console**

	TỔNG CÔNG TY GIẢI PHÁP DOANH NGHIỆP VIETTEL	Mã hiệu: HD.VTS.TTGPDN.02
	TÀI LIỆU GUIDELINE KEYCLOAK	Ngày có hiệu lực: 20/06/2022
		Ngày hết hiệu lực: 20/06/2023
		Lần ban hành: 01
		Trang: 7/33

Người quản trị có thể tập trung quản lý tất cả các thành phần của Keycloak server.

Chúng ta có thể bật hoặc tắt nhiều tính năng, có thể tạo, quản lý các ứng dụng và dịch vụ, định nghĩa các chính sách để quản lý phân quyền, quản lý người dùng bao gồm quyền truy cập và phiên truy cập.

✓ **Account Management Console**

Người dùng có thể quản lý chính tài khoản của họ, có thể cập nhật thông tin người dùng, thay đổi mật khẩu và xác thực 2 lớp. Người dùng cũng có thể quản lý phiên truy cập, xem lịch sử của tài khoản truy cập.


Nếu chúng ta bật tính năng đăng nhập bằng mạng xã hội, người dùng có thể liên kết tài khoản của họ với các thông tin cung cấp bổ sung cho phép chúng ta xác thực vào cùng một tài khoản với các nhà cung cấp định danh khác nhau.

✓ **Standard Protocols**

Keycloak dựa trên các giao thức tiêu chuẩn và cung cấp hỗ trợ cho OpenID Connect, OAuth 2.0 và SAML.

✓ **Authorization Services**

Nếu ủy quyền dựa trên vai trò không đáp ứng được nhu cầu của chúng ta, Keycloak cũng cung cấp các dịch vụ ủy quyền chi tiết. Điều này cho phép chúng ta quản lý quyền đối với tất cả các dịch vụ của mình từ bảng điều khiển dành cho quản trị viên Keycloak và cung cấp cho chúng ta sức mạnh để xác định chính xác các chính sách chúng ta cần.

	TỔNG CÔNG TY GIẢI PHÁP DOANH NGHIỆP VIETTEL	Mã hiệu: HD.VTS.TTGPDN.02
	TÀI LIỆU GUIDELINE KEYCLOAK	Ngày có hiệu lực: 20/06/2022
		Ngày hết hiệu lực: 20/06/2023
		Lần ban hành: 01
		Trang: 8/33

5.2 Cài đặt và cấu hình Keycloak

5.2.1 Cấu hình tối thiểu

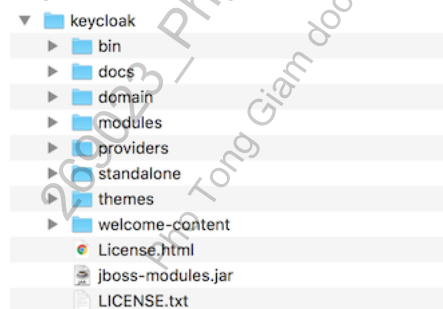
Cấu hình tối thiểu để chạy Keycloak server

- ✓ Java 8
- ✓ Ram: 512MB
- ✓ Disk: 50 GB

Nếu muốn chạy Keycloak trong một cluster thì sẽ cần một cơ sở dữ liệu như Postgres, MySQL, Oracle, MariaDB ...


5.2.2 Cấu trúc thư mục Distribution

Truy cập trang <https://www.keycloak.org/downloads> và tải bản distribution về và sau đó giải nén. Sau khi giải nén xong cấu trúc thư mục distribution sẽ dưới.



- ✓ **bin:** Thư mục chứa các script để khởi động, thực thi các action quản lý trên server
- ✓ **domain:** Thư mục chứa các tệp tin cấu hình và thư mục làm việc khi chạy Keycloak dưới dạng domain mode
- ✓ **modules:** Thư mục chứa các tất cả lib Java mà server sử dụng
- ✓ **providers:** Thư mục các extension tại đây
- ✓ **standalone:** Thư mục chứa các tệp tin cấu hình và thư mục làm việc khi chạy Keycloak dưới dạng standalone mode
- ✓ **themes:** Thư mục chứa các tệp tin html, style sheets, javascript và ảnh để hiển thị giao diện màn hình bởi server. Có thể chỉnh sửa hoặc tạo các tệp tin này.

5.2.3 Các mô hình hoạt động của Keycloak

	TỔNG CÔNG TY GIẢI PHÁP DOANH NGHIỆP VIETTEL	Mã hiệu: HD.VTS.TTGPDN.02
	TÀI LIỆU GUIDELINE KEYCLOAK	Ngày có hiệu lực: 20/06/2022
		Ngày hết hiệu lực: 20/06/2023
		Lần ban hành: 01
		Trang: 9/33

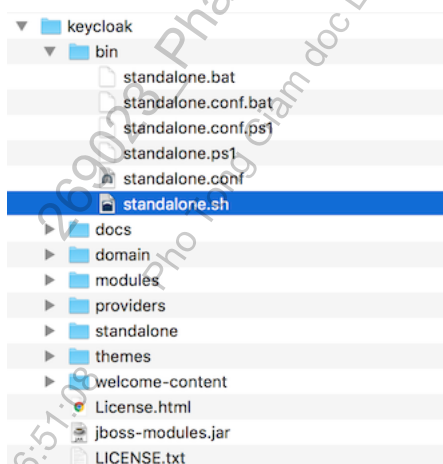
Trước khi triển khai Keycloak lên môi trường production, chúng ta cần chọn mô hình hoạt động của Keycloak mà muốn sử dụng. Keycloak có 3 mô hình để triển khai: Standalone mode, Standalone cluster mode và Domain cluster mode.

5.2.3.1 Standalone mode

Mô hình này chỉ hữu ích khi chúng ta chỉ chạy một Keycloak server instance. Nó không thể sử dụng cho triển khai cluster và không nên sử dụng mô hình này trên môi trường production bởi vì nếu server chạy ở mô hình này bị down chúng ta sẽ không thể truy cập hệ thống.

Mô hình này chỉ sử dụng để test và preview tính năng của Keycloak server.

Standalone Boot Script



Khi server chạy dưới mô hình standalone, ở trong thư mục bin có 1 script để khởi động Keycloak server.

Để khởi động Keycloak server

Linux/Unix

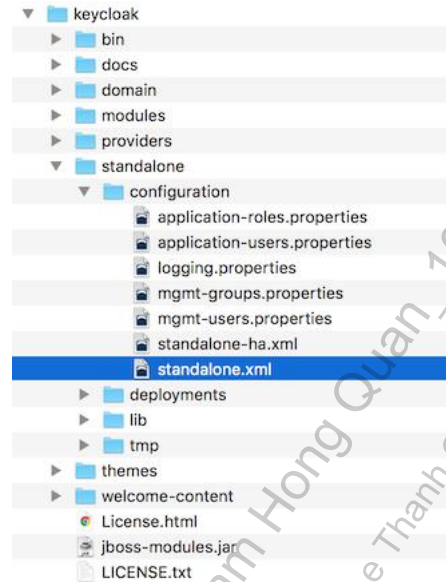
```
../bin/standalone.sh
```

Windows

```
../bin/standalone.bat
```

Standalone Configuration

	TỔNG CÔNG TY GIẢI PHÁP DOANH NGHIỆP VIETTEL	Mã hiệu: HD.VTS.TTGPDN.02
	TÀI LIỆU GUIDELINE KEYCLOAK	Ngày có hiệu lực: 20/06/2022
		Ngày hết hiệu lực: 20/06/2023
		Lần ban hành: 01
		Trang: 10/33




Tệp tin cấu hình mô hình này nằm trong thư mục
../standalone/configuration/standalone.xml

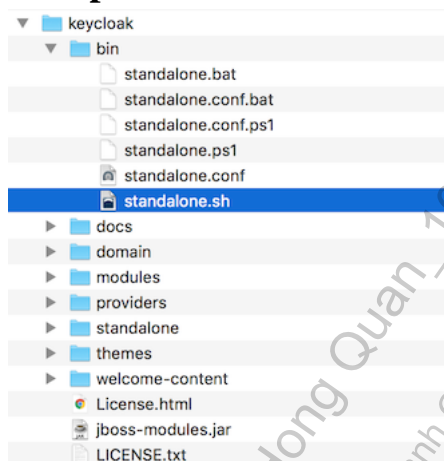
5.2.3.2 Standalone cluster mode

Mô hình này chạy Keycloak server trong một cluster. Yêu cầu chúng ta có một bản sao của bản phân phối Keycloak trên mỗi máy chúng ta muốn chạy một phiên bản máy chủ.

Mô hình này ban đầu có thể rất dễ triển khai, nhưng có thể trở nên khá cồng kềnh. Để thực hiện thay đổi cấu hình, chúng ta sẽ phải sửa đổi từng bản phân phối trên mỗi máy. Đối với một cụm lớn, điều này có thể trở nên tốn thời gian và dễ xảy ra lỗi.

	TỔNG CÔNG TY GIẢI PHÁP DOANH NGHIỆP VIETTEL	Mã hiệu: HD.VTS.TTGPDN.02
	TÀI LIỆU GUIDELINE KEYCLOAK	Ngày có hiệu lực: 20/06/2022
		Ngày hết hiệu lực: 20/06/2023
		Lần ban hành: 01
		Trang: 11/33

Standalone Cluster Boot Script



Mô hình này sử dụng script giống như mô hình standalone chỉ khác thêm một tham số để chỉ ra sử dụng tệp tin cấu hình HA.

Để khởi động Keycloak server

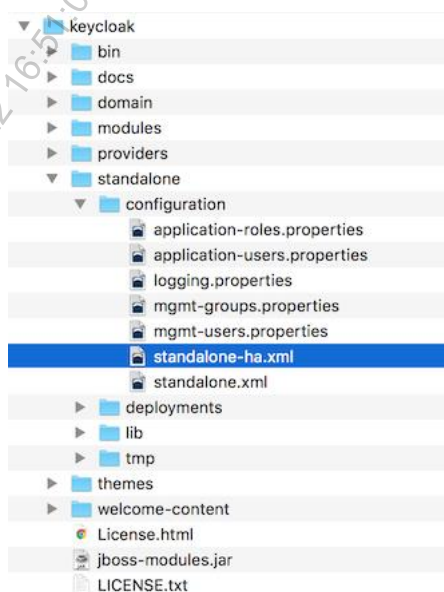
Linux/Unix

```
../bin/standalone.sh --server-config=standalone-ha.xml
```


Windows

```
../bin/standalone.bat --server-config=standalone-ha.xml
```

Standalone Cluster Configuration



Bản phân phối có tệp cấu hình máy chủ ứng dụng chủ yếu được định cấu hình trước để chạy trong một cụm. Nó có tất cả các cài đặt cơ sở hạ tầng cụ thể cho

	TỔNG CÔNG TY GIẢI PHÁP DOANH NGHIỆP VIETTEL	Mã hiệu: HD.VTS.TTGPDN.02
	TÀI LIỆU GUIDELINE KEYCLOAK	Ngày có hiệu lực: 20/06/2022
		Ngày hết hiệu lực: 20/06/2023
		Lần ban hành: 01
		Trang: 12/33

mạng, cơ sở dữ liệu, bộ nhớ đệm và khám phá. Tập này nằm trong ../standalone/configuration/standalone-ha.xml.

Chúng ta không thể chạy Keycloak trong một cụm mà không định cấu hình kết nối cơ sở dữ liệu được chia sẻ. Chúng ta cũng cần triển khai một số loại bộ cân bằng tải trước cụm

	TỔNG CÔNG TY GIẢI PHÁP DOANH NGHIỆP VIETTEL	Mã hiệu: HD.VTS.TTGPDN.02
	TÀI LIỆU GUIDELINE KEYCLOAK	Ngày có hiệu lực: 20/06/2022
		Ngày hết hiệu lực: 20/06/2023
		Lần ban hành: 01
		Trang: 13/33

5.2.3.3 Domain cluster mode

Để chạy một cluster sử dụng mô hình standalone mode có thể triển khai nhanh chóng, tuy nhiên nó trở nên phức tạp khi số lượng cluster phát triển. Mỗi lần chúng ta thay đổi cấu hình thì cần phải thực hiện mỗi node trong cụm cluster.

Mô hình domain mode sẽ giải quyết vấn đề này bằng cách đưa những thông tin cấu hình vào một nơi tập trung để lưu trữ. Điều này có thể phức tạp khi thiết lập ban đầu nhưng nó sẽ đem lại lợi ích sau này khi cần thay đổi thông tin cấu hình.


Một số khái niệm cơ bản về chạy mô hình domain mode.

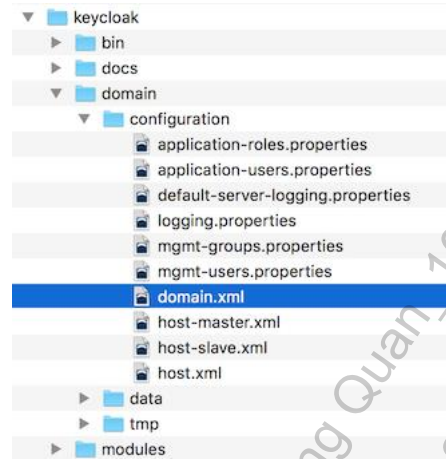
- ✓ **Domain controller:** chịu trách nhiệm lưu trữ, quản lý và cập nhật cấu hình chung cho mỗi node trong cụm cluster.
- ✓ **Host controller:** chịu trách nhiệm quản lý server instances trên mỗi máy. Chúng ta có thể cấu hình một hoặc nhiều server instances. Domain controller có thể tương tác với host controller trên mỗi máy để quản lý cluster. Để giảm số lượng server instances trong quá trình chạy, domain controller sẽ tương tác với host controller trên mỗi máy mà nó chạy.
- ✓ **Domain profile:** là một tập hợp cấu hình đã được đặt tên có thể được server sử dụng để khởi động.
- ✓ **Server group:** là một tập hợp các servers. Nó quản lý và cấu hình như một. Chúng ta có thể chỉ định một domain profile cho một server group và mỗi service trong group sẽ sử dụng domain profile làm cấu hình.

Trong mô hình này, domain controller được khởi động trên master node. Tiếp đến là host controller được khởi động trên mỗi máy trong cụm cluster. Mỗi host controller được triển khai cấu hình chỉ ra số lượng server instances sẽ được khởi động trên mỗi máy.

Domain configuration

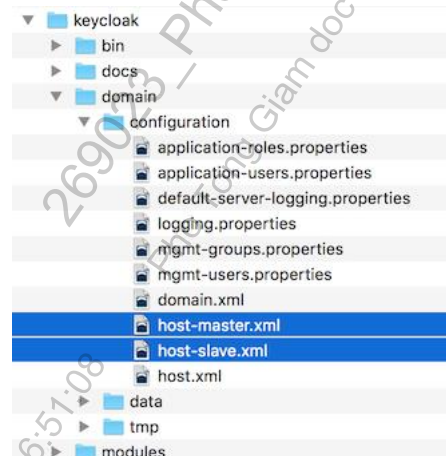
Mô hình này sử dụng file cấu hình tại ../domain/configuration/domain.xml

	TỔNG CÔNG TY GIẢI PHÁP DOANH NGHIỆP VIETTEL	Mã hiệu: HD.VTS.TTGPDN.02
	TÀI LIỆU GUIDELINE KEYCLOAK	Ngày có hiệu lực: 20/06/2022
		Ngày hết hiệu lực: 20/06/2023
		Lần ban hành: 01
		Trang: 14/33



Host controller configuration

Keycloak có 2 tệp tin cấu hình host controller bên trong thư mục ../domain/configuration là file host-master.xml và host-slave.xml.



Tệp tin host-master.xml là để cấu hình khởi động cho một domain controller, một load balancer và một server instance.

Tệp tin host-slave.xml là để cấu hình giao tiếp với domain controller và khởi động một server instance.

Chú ý: Load balancer không phải một service bắt buộc, nó tồn tại là để kiểm tra cluster trên máy phát triển. Trên môi trường production chúng ta có thể thay thế nó nếu chúng ta muốn sử dụng một load balancer phần cứng hoặc mềm khác mong muốn.

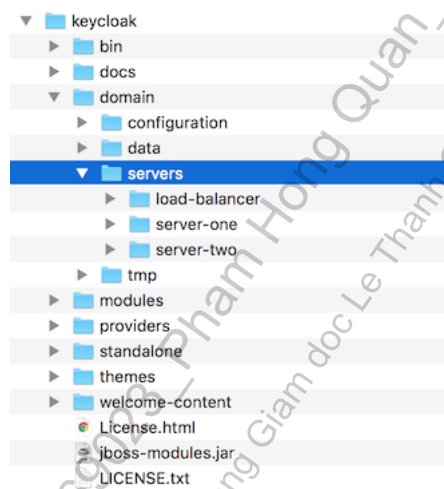
Để disable load balancer server instance, vào tệp tin host-master.xml tìm đến từ khóa “load-balancer” comment hoặc xóa.

```
<servers>  
  <server name="load-balancer" group="loadbalancer-group"/>  
</servers>
```

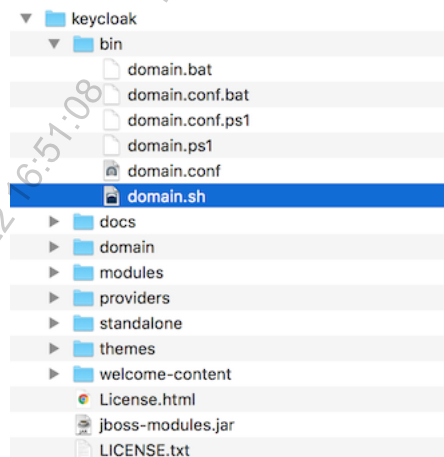
	TỔNG CÔNG TY GIẢI PHÁP DOANH NGHIỆP VIETTEL	Mã hiệu: HD.VTS.TTGPDN.02
	TÀI LIỆU GUIDELINE KEYCLOAK	Ngày có hiệu lực: 20/06/2022
		Ngày hết hiệu lực: 20/06/2023
		Lần ban hành: 01
		Trang: 15/33

Thư mục của server instance

Mỗi service instance được định nghĩa trong host files và được tạo thư mục bên trong đường dẫn ../domain/servers/{SERVER NAME}. Cấu hình bổ sung có thể được đặt ở đây và mọi tệp tạm thời, nhật ký hoặc dữ liệu mà server instance cần hoặc tạo cũng ở đây



Khởi động trong mô hình domain cluster mode



Khi server chạy dưới mô hình domain cluster mode, ở trong thư mục bin có 1 script để khởi động Keycloak server.

Để khởi động Keycloak server

Linux/Unix

```
../bin/domain.sh --host-config=host-master.xml
```

Windows

```
.. \bin\domain.bat --host-config=host-master.xml
```

	TỔNG CÔNG TY GIẢI PHÁP DOANH NGHIỆP VIETTEL	Mã hiệu: HD.VTS.TTGPDN.02
	TÀI LIỆU GUIDELINE KEYCLOAK	Ngày có hiệu lực: 20/06/2022
		Ngày hết hiệu lực: 20/06/2023
		Lần ban hành: 01
		Trang: 16/33

5.2.4 Cấu hình Database

Keycloak đi kèm với database dựa trên Java được nhúng của riêng nó được gọi là H2. Đây là database mặc định mà Keycloak sẽ sử dụng để lưu trữ dữ liệu. Keycloak khuyến cáo nên thay thế nó bằng database khác như Oracle, MariaDB, MySQL... Database H2 không khả thi trong các tình huống đồng thời cao và cũng không nên được sử dụng trong một cluster.

Keycloak sử dụng hai công nghệ phân lớp để duy trì dữ liệu quan hệ của nó. Công nghệ phân lớp dưới cùng là JDBC. JDBC là một API Java được sử dụng để kết nối với RDBMS. Có các trình điều khiển JDBC khác nhau cho mỗi loại cơ sở dữ liệu được cung cấp bởi nhà cung cấp cơ sở dữ liệu.

Danh sách kiểm tra thiết lập database

- ✓ Tải xuống JDBC driver cho database của chúng ta
- ✓ Đóng gói file driver JAR bên trong module và cài đặt module này trên server
- ✓ Mô tả JDBC driver trong file cấu hình trên server
- ✓ Thay đổi cấu hình datasource để sử dụng JDBC driver database của chúng ta
- ✓ Thay đổi cấu hình datasource để xác định các tham số kết nối tới database của chúng ta

5.2.4.1 Tải xuống JDBC driver cho database cần dùng

Tìm và tải xuống JDBC driver JAR. Trước khi sử dụng driver này cần phải đóng gói và đẩy vào trong module và cài đặt trên server. Những module JAR được load vào Keycloak classpath.

Các bước thực hiện

Bước 1: Tạo cấu trúc thư mục để giữ định nghĩa module của chúng ta trong thư mục ../modules/ của bản phân phối Keycloak của chúng ta.

Quy ước là sử dụng tên gói Java của JDBC driver cho tên của cấu trúc thư mục. Ví dụ với PostgreSQL, hãy tạo thư mục org/postgresql/main.

Bước 2: Copy database driver JAR vào bên trong thư mục trên và tạo một file module.xml.



**TỔNG CÔNG TY GIẢI PHÁP DOANH
NGHIỆP VIETTEL**

Mã hiệu: HD.VTS.TTGPDN.02

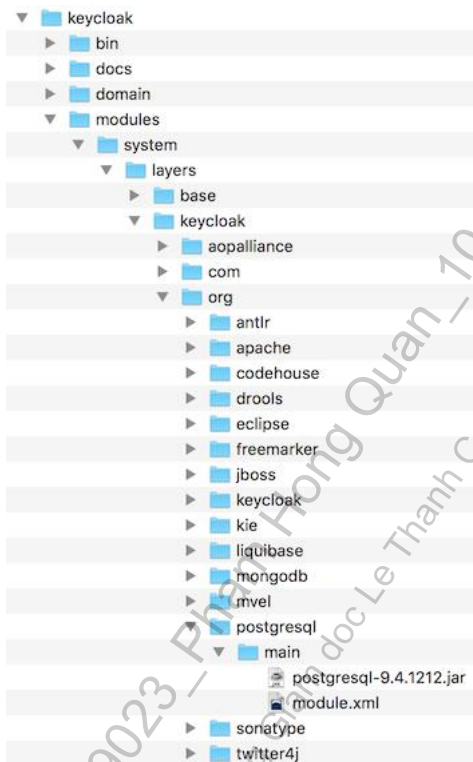
**TÀI LIỆU GUIDELINE
KEYCLOAK**

Ngày có hiệu lực: 20/06/2022

Ngày hết hiệu lực: 20/06/2023


Lần ban hành: 01

Trang: 17/33



Bước 3: Mở file module.xml và tạo như file xml sau

```
<?xml version="1.0" encoding="UTF-8"?>
<module xmlns="urn:jboss:module:1.3" name="org.postgresql">
  <resources>
    <resource-root path="postgresql-VERSION.jar"/>
  </resources>
  <dependencies>
    <module name="javax.api"/>
    <module name="javax.transaction.api"/>
  </dependencies>
</module>
```

	TỔNG CÔNG TY GIẢI PHÁP DOANH NGHIỆP VIETTEL	Mã hiệu: HD.VTS.TTGPDN.02
	TÀI LIỆU GUIDELINE KEYCLOAK	Ngày có hiệu lực: 20/06/2022
		Ngày hết hiệu lực: 20/06/2023
		Lần ban hành: 01
		Trang: 18/33

Ghi chú:

- ✓ Tên module nên giống với cấu trúc thư mục bên trong module của chúng ta. Vì vậy org/postgresql map org.postgresql
- ✓ Thuộc tính “resource-root path” nên chỉ rõ tên tệp Jar của driver

5.2.4.2 Khai báo và load JDBC driver

Điều kiện: Phải có gói JDBC driver

Các bước thực hiện

Bước 1: Khai báo JDBC sử dụng và cập nhật files cấu hình dựa trên mô hình triển khai.

Standard mode, file ../standalone/configuration/standalone.xml

Standard cluster mode, file ../standalone/configuration/standalone-ha.xml


Domain mode, file ../domain/configuration/domain.xml

Bước 2: Tìm trong file cấu hình, tìm khối XML drivers bên trong chứa subsystem datasource. Chúng ta sẽ thấy một driver được xác định trước được khai báo cho driver H2 JDBC. Đây là nơi chúng ta sẽ khai báo driver JDBC cho database cần dùng.

```
<subsystem xmlns="urn:jboss:domain:datasources:6.0">
  <datasources>
    ...
    <drivers>
      <driver name="h2" module="com.h2database.h2">
        <xa-datasource-class>org.h2.jdbcx.JdbcDataSource</xa-datasource-class>
      </driver>
    </drivers>
  </datasources>
</subsystem>
```

Bước 3: Trong khối XML drivers, khai báo bổ sung JDBC driver. Ví dụ như dưới

```
<subsystem xmlns="urn:jboss:domain:datasources:6.0">
  <datasources>
    ...
    <drivers>
      <driver name="postgresql" module="org.postgresql">
        <xa-datasource-class>org.postgresql.xa.PGXADatasource</xa-datasource-class>
      </driver>
      <driver name="h2" module="com.h2database.h2">
        <xa-datasource-class>org.h2.jdbcx.JdbcDataSource</xa-datasource-class>
      </driver>
    </drivers>
  </datasources>
</subsystem>
```


	TỔNG CÔNG TY GIẢI PHÁP DOANH NGHIỆP VIETTEL	Mã hiệu: HD.VTS.TTGPDN.02
	TÀI LIỆU GUIDELINE KEYCLOAK	Ngày có hiệu lực: 20/06/2022
		Ngày hết hiệu lực: 20/06/2023
		Lần ban hành: 01
		Trang: 19/33

```
</drivers>  
</datasources>  
</subsystem>
```

5.2.4.3 Thay đổi cấu hình datasource

Chúng ta sửa đổi cấu hình datasource hiện có mà Keycloak sử dụng để kết nối với database. Dưới đây là ví dụ thiết lập kết nối với database cho postgresql

```
<subsystem xmlns="urn:jboss:domain:datasources:6.0">  
  <datasources>  
    ...  
    <datasource jndi-name="java:jboss/datasources/KeycloakDS" pool-name="KeycloakDS"  
enabled="true" use-java-context="true">  
      <connection-url>jdbc:postgresql://localhost/keycloak</connection-url>  
      <driver>postgresql</driver>  
      <pool>  
        <max-pool-size>20</max-pool-size>  
      </pool>  
      <security>  
        <user-name>keycloak</user-name>  
        <password>keycloak@123</password>  
      </security>  
    </datasource>  
    ...  
  </datasources>  
</subsystem>
```


Thay đổi ExampleDS sang KeycloakDS

```
<default-bindings  
  context-service="java:jboss/ee/concurrency/context/default"  
  datasource="java:jboss/datasources/KeycloakDS"  
  managed-executor-service="java:jboss/ee/concurrency/executor/default"  
  managed-scheduled-executor-service="java:jboss/ee/concurrency/scheduler/default"  
  managed-thread-factory="java:jboss/ee/concurrency/factory/default" />
```

5.2.5 Cấu hình Cache

Keycloak có 2 kiểu cache. Kiểu cache thứ nhất là cache nằm ngay trước database nhằm để giảm việc truy cập vào database và tăng thời gian response time và dữ liệu được lưu trong memory. Dữ liệu realm, client, role và user metadata là dữ liệu dùng kiểu cache này và gọi là local cache.

Kiểu cache thứ hai là cache xử lý việc quản lý phiên làm việc của người dùng, offline tokens và theo dõi việc truy cập hệ thống thất bại để server có thể phát

	TỔNG CÔNG TY GIẢI PHÁP DOANH NGHIỆP VIETTEL	Mã hiệu: HD.VTS.TTGPDN.02
	TÀI LIỆU GUIDELINE KEYCLOAK	Ngày có hiệu lực: 20/06/2022
		Ngày hết hiệu lực: 20/06/2023
		Lần ban hành: 01
		Trang: 20/33

hiện, tìm ra những cuộc tấn công. Dữ liệu được lưu trữ trong các bộ nhớ đệm này là tạm thời, chỉ trong bộ nhớ nhưng có thể được sao chép toàn cụm cluster.

5.2.5.1 Eviction and expiration

Có nhiều cache khác nhau được cấu hình cho Keycloak. Tất cả các cache, giá trị mặc định là 10000 mục nhập và sử dụng ít nhất gần đây sử dụng chiến dịch trực xuất.

Có thể định cấu hình chính sách trực xuất và các mục nhập tối đa cho các bộ nhớ đệm này trong file standalone.xml, standalone-ha.xml hoặc domain.xml phụ thuộc vào mô hình cài đặt. Trong tệp cấu hình, có một phần với infinispn subsystem, trông tương tự như sau:

```
<subsystem xmlns="urn:jboss:domain:infinispn:12.0">
  <cache-container name="keycloak">
    <local-cache name="realms">
      <object-memory size="10000"/>
    </local-cache>
    <local-cache name="users">
      <object-memory size="10000"/>
    </local-cache>
    ...
    <local-cache name="keys">
      <object-memory size="1000"/>
      <expiration max-idle="3600000"/>
    </local-cache>
    ...
  </cache-container>
```

Để giới hạn hoặc mở rộng số lượng mục được phép, chỉ cần thêm hoặc chỉnh sửa phần tử đối tượng hoặc phần tử hết hạn của cấu hình bộ đệm cụ thể.

Ngoài ra, còn có các bộ nhớ đệm riêng sessions, clientSessions, offlineSessions, offlineClientSessions, loginFailures and actionTokens. Các bộ nhớ đệm này được phân phối trong môi trường cụm cluster và chúng có kích thước không giới hạn theo mặc định. Nếu chúng bị giới hạn, thì có thể một số phiên sẽ bị mất. Các phiên đã hết hạn được chính Keycloak xóa nội bộ để tránh tăng kích thước của các bộ nhớ đệm này mà không có giới hạn. Nếu chúng ta gặp sự cố bộ nhớ do số lượng phiên lớn, chúng ta có thể thử:

- ✓ Tăng số lượng node
- ✓ Tăng memory cho keycloak server
- ✓ Giảm số lượng owners (tham khảo mục replica và failover)
- ✓ Disable distributed cache

	TỔNG CÔNG TY GIẢI PHÁP DOANH NGHIỆP VIETTEL	Mã hiệu: HD.VTS.TTGPDN.02
	TÀI LIỆU GUIDELINE KEYCLOAK	Ngày có hiệu lực: 20/06/2022
		Ngày hết hiệu lực: 20/06/2023
		Lần ban hành: 01
		Trang: 21/33

✓ Giảm thời gian timeout

5.2.5.2 Replica and failover

Các cache như sessions, authenticationSessions, offlineSessions, loginFailures và một số bộ đệm được định cấu hình làm bộ đệm phân tán khi sử dụng thiết lập cluster.

Các mục nhập không được sao chép đến từng node, nhưng thay vào đó, một hoặc nhiều node được chọn làm chủ sở hữu của mục nhập đó. Nếu một node không phải là chủ sở hữu của dữ liệu bộ nhớ cache cụ thể, nó sẽ truy vấn cụm cluster để lấy nó. Điều này có nghĩa là đối với chuyển đổi dự phòng là nếu tất cả các node sở hữu một phần dữ liệu bị hỏng, dữ liệu đó sẽ bị mất vĩnh viễn. Theo mặc định, Keycloak chỉ chỉ định một chủ sở hữu cho dữ liệu. Vì vậy, nếu một node đó gặp sự cố thì dữ liệu đó sẽ bị mất. Điều này thường có nghĩa là người dùng sẽ đăng xuất và sẽ phải đăng nhập lại.

Chúng ta có thể thay đổi số node sao chép được phân dữ liệu. Thay đổi thuộc tính owners trong mô tả distributed-cache. Ở đây thay đổi số node ít nhất được sao chép dữ liệu là 2.

```
<subsystem xmlns="urn:jboss:domain:infinispan:12.0">  
  <cache-container name="keycloak">  
    <distributed-cache name="sessions" owners="2"/>  
  </cache-container>  
</subsystem>
```

Số lượng chủ sở hữu được đề xuất thực sự phụ thuộc vào việc triển khai của chúng ta. Nếu chúng ta không quan tâm đến việc người dùng có đăng xuất khi một nút gặp sự cố hay không, thì giá trị owners bằng 1 là đủ tốt và chúng ta sẽ tránh sao chép

5.2.5.3 Disable caching

Chúng ta có thể disable cache của realms và users. Thực hiện cập nhật file standalone.xml, standalone-ha.xml hoặc domain.xml tùy theo mô hình đang được cài đặt.

```
<spi name="userCache">  
  <provider name="default" enabled="true"/>  
</spi>  
  
<spi name="realmCache">  
  <provider name="default" enabled="true"/>  
</spi>
```

	TỔNG CÔNG TY GIẢI PHÁP DOANH NGHIỆP VIETTEL	Mã hiệu: HD.VTS.TTGPDN.02
	TÀI LIỆU GUIDELINE KEYCLOAK	Ngày có hiệu lực: 20/06/2022
		Ngày hết hiệu lực: 20/06/2023
		Lần ban hành: 01
		Trang: 22/33

</spi>

Cập nhật thuộc tính enabled thành false cho cache mà chúng ta muốn disable.
Sau đó reboot keycloak server để server cập nhật.

5.2.5.4 Clear cache in runtime

Chúng ta có thể xóa dữ liệu realm cache, user cache trên giao diện admin console. Truy cập admin console → Chọn Realm Settings → Chọn Cache Tab → Bấm nút Clear cache mà muốn xóa như hình bên dưới.



5.2.6 Cài đặt Keycloak Server trên Linux

5.2.6.1 Tải bộ cài đặt Keycloak Server

Kiểm tra trên trang <https://www.keycloak.org/downloads-archive.html> phiên bản mới nhất và tải xuống. Trong hướng dẫn này tải keycloak 16.1.1

Tải bộ cài vào thư mục /opt

```
$ cd /opt  
$ sudo wget https://github.com/keycloak/keycloak/releases/download/16.1.1/keycloak-16.1.1.tar.gz
```

Giải nén và thay đổi tên thành keycloak

```
$ sudo tar -xvzf keycloak-16.1.1.tar.gz  
$ sudo mv keycloak-16.1.1 /opt/keycloak
```


5.2.6.2 Cài đặt và cấu hình

Tạo user và group keycloak

```
$ sudo groupadd keycloak  
$ sudo useradd -r -g keycloak -d /opt/keycloak -s /sbin/nologin keycloak
```

Thay đổi permission và owner cho keycloak

```
$ sudo chown -R keycloak: keycloak  
$ sudo chmod o+x /opt/keycloak/bin/
```

	TỔNG CÔNG TY GIẢI PHÁP DOANH NGHIỆP VIETTEL	Mã hiệu: HD.VTS.TTGPDN.02
	TÀI LIỆU GUIDELINE KEYCLOAK	Ngày có hiệu lực: 20/06/2022
		Ngày hết hiệu lực: 20/06/2023
		Lần ban hành: 01
		Trang: 23/33

Tạo file cấu hình

```
$ cd /etc/  
$ sudo mkdir keycloak
```

Copy file cấu hình

```
$ sudo cp /opt/keycloak/docs/contrib/scripts/systemd/wildfly.conf /etc/keycloak/keycloak.conf
```

Copy file chạy

```
$ sudo cp /opt/keycloak/docs/contrib/scripts/systemd/launch.sh /opt/keycloak/bin/
```

Thay đổi quyền owner file chạy

```
$ sudo chown keycloak: /opt/keycloak/bin/launch.sh
```

Sửa file chạy

```
$ sudo vi /opt/keycloak/bin/launch.sh
```

với nội dung như sau

```
#!/bin/bash  
if [ "x$WILDFLY_HOME" = "x" ]; then  
    WILDFLY_HOME="/opt/keycloak"  
fi  
if [ [ "x$1" = "xdomain" ] ]; then  
    $WILDFLY_HOME/bin/domain.sh -c $2 -b $3  
else  
    $WILDFLY_HOME/bin/standalone.sh -c $2 -b $3  
fi
```

Copy file service

```
$ sudo cp /opt/keycloak/docs/contrib/scripts/systemd/wildfly.service  
/etc/systemd/system/keycloak.service
```

Sửa file service

```
$ sudo vi /etc/systemd/system/keycloak.service
```

với nội dung như sau

```
[Unit]  
Description=The Keycloak Server  
After=syslog.target network.target  
Before=httpd.service  
[Service]  
Environment=LAUNCH_JBOSS_IN_BACKGROUND=1  
EnvironmentFile=/etc/keycloak/keycloak.conf  
User=keycloak  
Group=keycloak
```

	TỔNG CÔNG TY GIẢI PHÁP DOANH NGHIỆP VIETTEL	Mã hiệu: HD.VTS.TTGPDN.02
	TÀI LIỆU GUIDELINE KEYCLOAK	Ngày có hiệu lực: 20/06/2022
		Ngày hết hiệu lực: 20/06/2023
		Lần ban hành: 01
		Trang: 24/33

LimitNOFILE=102642

PIDFile=/var/run/keycloak/keycloak.pid

ExecStart=/opt/keycloak/bin/launch.sh \$WILDFLY_MODE \$WILDFLY_CONFIG

\$WILDFLY_BIND

StandardOutput=null

[Install]

WantedBy=multi-user.target

Reload lại systemd

\$ sudo systemctl daemon-reload

\$ sudo systemctl enable keycloak

Bật service keycloak

\$ sudo systemctl start keycloak

Kiểm tra trạng thái

\$ sudo systemctl status keycloak

Có thể kiểm tra logs

\$ sudo tail -f /opt/keycloak/standalone/log/server.log

Hoặc truy cập địa chỉ keycloak server tại

<http://<instance-public-ip>:8080/auth/>

5.2.3.3 Cấu hình keycloak chạy với Database Oracle

Tại thư mục /opt/keycloak/modules/system/layers/keycloak, tạo thư mục con sau oracle/jdbc/main và copy ojdbc7.jar vào thư mục main. Chú ý: tạo thư mục xong như chown cho đúng user chạy và chmod +x

```
<?xml version="1.0" encoding="UTF-8"?>
<module xmlns="urn:jboss:module:1.3" name="oracle.jdbc">
  <resources>
    <resource-root path="ojdbc7.jar"/>
  </resources>
  <dependencies>
    <module name="javax.api"/>
    <module name="javax.transaction.api"/>
  </dependencies>
</module>
```

Thay đổi cấu hình keycloak trong file standalone.xml. Thay đổi thông tin IP, port, schema, username, password để kết nối đến database.

```
<datasources>
```


	TỔNG CÔNG TY GIẢI PHÁP DOANH NGHIỆP VIETTEL	Mã hiệu: HD.VTS.TTGPDN.02
	TÀI LIỆU GUIDELINE KEYCLOAK	Ngày có hiệu lực: 20/06/2022
		Ngày hết hiệu lực: 20/06/2023
		Lần ban hành: 01
		Trang: 25/33

```
<datasource jndi-name="java:jboss/datasources/KeycloakDS" pool-name="KeycloakDS"
enabled="true" use-java-context="true">
  <connection-url>jdbc:oracle:thin:@10.60.157.140:1521:db19c</connection-url>
  <driver>oracle</driver>
  <pool>
    <max-pool-size>100</max-pool-size>
  </pool>
  <security>
    <user-name>keycloak</user-name>
    <password>keycloak#123</password>
  </security>
</datasource>
<drivers>
  <driver name="oracle" module="oracle.jdbc">
    <driver-class>oracle.jdbc.OracleDriver</driver-class>
  </driver>
</drivers>
</datasources>
```

Thay đổi ExampleDS sang KeycloakDS

```
<default-bindings
context-service="java:jboss/ee/concurrency/context/default"
datasource="java:jboss/datasources/KeycloakDS"
managed-executor-service="java:jboss/ee/concurrency/executor/default"
managed-scheduled-executor-service="java:jboss/ee/concurrency/scheduler/default"
managed-thread-factory="java:jboss/ee/concurrency/factory/default" />
```

5.2.3.4 Cấu hình Keycloak chạy theo mô hình standalone cluster

Đối với môi trường product cần chạy nhiều node để Load balancing thì cần sử dụng file standalone-ha.xml thay vì sử dụng standalone.xml như phía trên, các cấu hình ở trên làm tương tự bên file standalone-ha.xml. Đồng thời, bổ sung một số config dưới đây:

Mở file standalone-ha.xml ở đường dẫn /opt/keycloak/standalone/configuration

Bước 1: Thay đổi stack mặc định từ UDP thành TCP trong jgroups subsystem

```
<channel name="ee" stack="udp" cluster="ejb"/>
```

Chuyển thành

```
<channel name="ee" stack="tcp" cluster="ejb"/>
```

Bước 2: Thay đổi cấu hình stack của TCP. Thay đổi socket-protocol type từ “MPING” sang “TCPPING” và cấu hình tham số “initial hosts” và “port range”.

Ví dụ này thì đang sử dụng 2 IP 10.61.184.40 và 10.61.184.73, cả 2 đang cấu hình chạy port 7600.

	TỔNG CÔNG TY GIẢI PHÁP DOANH NGHIỆP VIETTEL	Mã hiệu: HD.VTS.TTGPDN.02
	TÀI LIỆU GUIDELINE KEYCLOAK	Ngày có hiệu lực: 20/06/2022
		Ngày hết hiệu lực: 20/06/2023
		Lần ban hành: 01
		Trang: 26/33

Lưu ý: tham số initial hosts sẽ liệt kê tất cả các ip trong cụm, lý do lắng nghe ở port 7600 ở initial_hosts vì phải trùng với port cấu hình jgroups-tcp ở phần socket-binding-group

```
<stack name="tcp">
  <transport type="TCP" socket-binding="jgroups-tcp"/>
  <socket-protocol type="MPING" socket-binding="jgroups-mping"/>
  <protocol type="MERGE3"/>
  <socket-protocol type="FD SOCK" socket-binding="jgroups-tcp-fd"/>
  <protocol type="FD_ALL"/>
  <protocol type="VERIFY_SUSPECT"/>
  <protocol type="pbcast.NAKACK2"/>
  <protocol type="UNICAST3"/>
  <protocol type="pbcast.STABLE"/>
  <protocol type="pbcast.GMS"/>
  <protocol type="MFC"/>
  <protocol type="FRAG3"/>
</stack>
```

Chuyển thành

```
<stack name="tcp">
  <transport type="TCP" socket-binding="jgroups-tcp"/>
  <protocol type="TCPPING">
    <property
name="initial_hosts">10.61.184.40[7600],10.61.184.73[7600]</property>
    <property name="port_range">0</property>
  </protocol>
  <protocol type="MERGE3"/>
  <socket-protocol type="FD SOCK" socket-binding="jgroups-tcp-fd"/>
  <protocol type="FD_ALL"/>
  <protocol type="VERIFY_SUSPECT"/>
  <protocol type="pbcast.NAKACK2"/>
  <protocol type="UNICAST3"/>
  <protocol type="pbcast.STABLE"/>
  <protocol type="pbcast.GMS"/>
  <protocol type="MFC"/>
  <protocol type="FRAG3"/>
</stack>
```

Bước 3: Set IP private interface. Tại phần **interfaces**, chèn thêm cấu hình **interface**. Địa chỉ IP phải tương quan với một trong các địa chỉ IP được chỉ định trong cấu hình initial_hosts:

```
<interface name="private">
  <inet-address value="${jboss.bind.address.private:10.61.184.40}"/>
```

	TỔNG CÔNG TY GIẢI PHÁP DOANH NGHIỆP VIETTEL	Mã hiệu: HD.VTS.TTGPĐN.02
	TÀI LIỆU GUIDELINE KEYCLOAK	Ngày có hiệu lực: 20/06/2022
		Ngày hết hiệu lực: 20/06/2023
		Lần ban hành: 01
		Trang: 27/33

</interface>

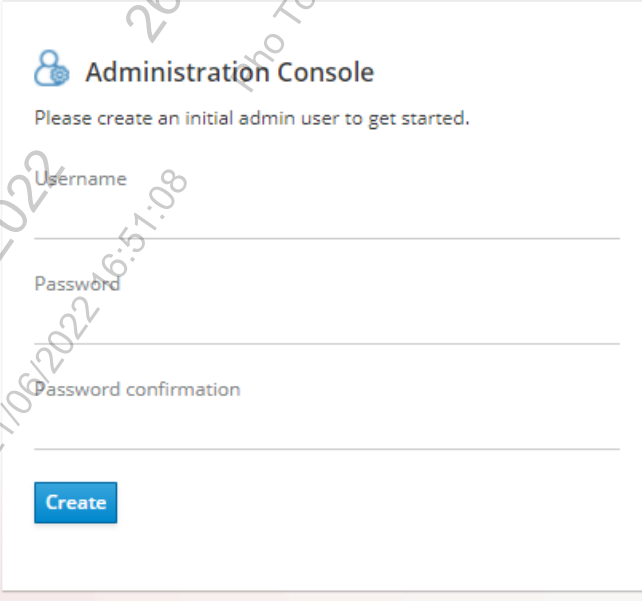
Lặp lại với các node khác, sau khi hoàn thành, start từng node lên và xem kết quả trong log. Nếu có kết quả tương tự ảnh dưới thì đã config thành công

```
985 INFO [org.infinispan.CONTAINER] (ServerService Thread Pool -- 59) ISPN000118: Infinispan version: Infinispan 'Corona Extra' 11.0.9.Final
986 INFO [org.infinispan.PERSISTENCE] (ServerService Thread Pool -- 61) ISPN000056: Starting user marshaller 'org.wildfly.clustering.infinispan.marshalling.jboss.JBossMarshaller'
987 INFO [org.infinispan.PERSISTENCE] (ServerService Thread Pool -- 58) ISPN000056: Starting user marshaller 'org.wildfly.clustering.infinispan.spi.marshalling.InfinispanProtocolStreamMarshaller'
988 INFO [org.infinispan.PERSISTENCE] (ServerService Thread Pool -- 62) ISPN000056: Starting user marshaller 'org.wildfly.clustering.infinispan.marshalling.jboss.JBossMarshaller'
989 INFO [org.infinispan.PERSISTENCE] (ServerService Thread Pool -- 60) ISPN000056: Starting user marshaller 'org.wildfly.clustering.infinispan.spi.marshalling.InfinispanProtocolStreamMarshaller'
990 INFO [org.infinispan.PERSISTENCE] (ServerService Thread Pool -- 59) ISPN000056: Starting user marshaller 'org.wildfly.clustering.infinispan.spi.marshalling.InfinispanProtocolStreamMarshaller'
991 INFO [org.infinispan.CLUSTER] (ServerService Thread Pool -- 60) ISPN000078: Starting JGroups channel e3b
992 INFO [org.infinispan.CLUSTER] (ServerService Thread Pool -- 58) ISPN000078: Starting JGroups channel e3b
993 INFO [org.infinispan.CLUSTER] (ServerService Thread Pool -- 61) ISPN000078: Starting JGroups channel e3b
994 INFO [org.infinispan.CLUSTER] (ServerService Thread Pool -- 59) ISPN000078: Starting JGroups channel e3b
995 INFO [org.infinispan.CLUSTER] (ServerService Thread Pool -- 62) ISPN000078: Starting JGroups channel e3b
996 INFO [org.infinispan.CLUSTER] (ServerService Thread Pool -- 58) ISPN000094: Received new cluster view for channel e3b: [vts-quangnguyen011] (2) [vts-quangnguyen01, vts-haib6]
997 INFO [org.infinispan.CLUSTER] (ServerService Thread Pool -- 60) ISPN000094: Received new cluster view for channel e3b: [vts-quangnguyen011] (2) [vts-quangnguyen01, vts-haib6]
998 INFO [org.infinispan.CLUSTER] (ServerService Thread Pool -- 59) ISPN000094: Received new cluster view for channel e3b: [vts-quangnguyen011] (2) [vts-quangnguyen01, vts-haib6]
999 INFO [org.infinispan.CLUSTER] (ServerService Thread Pool -- 62) ISPN000094: Received new cluster view for channel e3b: [vts-quangnguyen011] (2) [vts-quangnguyen01, vts-haib6]
1000 INFO [org.infinispan.CLUSTER] (ServerService Thread Pool -- 60) ISPN000078: Channel e3b local address is vts-haib6, physical addresses are [10.61.184.73:7600]
1001 INFO [org.infinispan.CLUSTER] (ServerService Thread Pool -- 58) ISPN000078: Channel e3b local address is vts-haib6, physical addresses are [10.61.184.73:7600]
1002 INFO [org.infinispan.CLUSTER] (ServerService Thread Pool -- 61) ISPN000078: Channel e3b local address is vts-haib6, physical addresses are [10.61.184.73:7600]
1003 INFO [org.infinispan.CLUSTER] (ServerService Thread Pool -- 59) ISPN000078: Channel e3b local address is vts-haib6, physical addresses are [10.61.184.73:7600]
1004 INFO [org.infinispan.CLUSTER] (ServerService Thread Pool -- 62) ISPN000078: Channel e3b local address is vts-haib6, physical addresses are [10.61.184.73:7600]
1005 INFO [org.infinispan.CONFIG] (MSC service thread 1-3) ISPN000152: Passivation configured without an eviction policy being selected. Only manually evicted entities will be passivated.
1006 INFO [org.infinispan.CONFIG] (MSC service thread 1-3) ISPN000152: Passivation configured without an eviction policy being selected. Only manually evicted entities will be passivated.
```

5.3 Một số tính năng cơ bản trong Keycloak

5.3.1 Tạo tài khoản admin

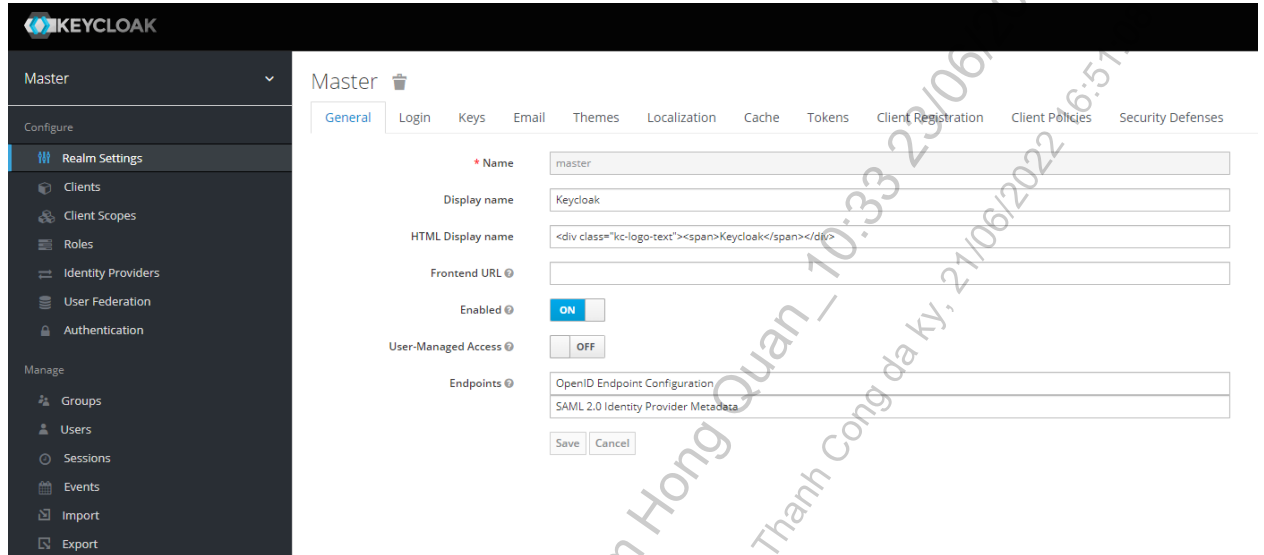
Đầu tiên sau khi cài đặt keycloak xong, chúng ta tạo account admin, việc này chỉ cần thực hiện duy nhất lần đầu tiên, cụ thể tại trang bắt đầu của keycloak <http://localhost:8080>



The screenshot shows the 'Administration Console' of Keycloak. It prompts the user to 'Please create an initial admin user to get started.' Below this, there are three input fields: 'Username', 'Password', and 'Password confirmation'. At the bottom, there is a blue 'Create' button.

Chúng ta nhập user, pass vào để tạo account admin. Sau khi tạo account thành công, hệ thống sẽ chuyển trang tới trang quản lý của keycloak,


	TỔNG CÔNG TY GIẢI PHÁP DOANH NGHIỆP VIETTEL	Mã hiệu: HD.VTS.TTGPDN.02
	TÀI LIỆU GUIDELINE KEYCLOAK	Ngày có hiệu lực: 20/06/2022
		Ngày hết hiệu lực: 20/06/2023
		Lần ban hành: 01
		Trang: 28/33

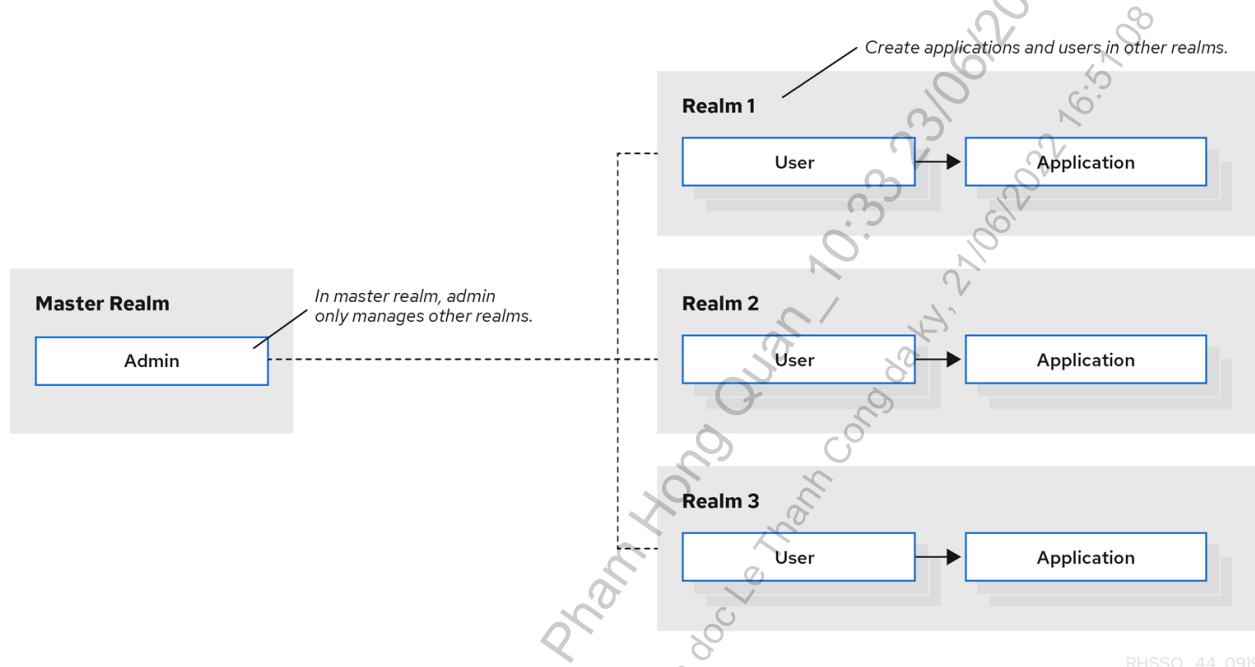


5.3.2 Tạo realms

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.

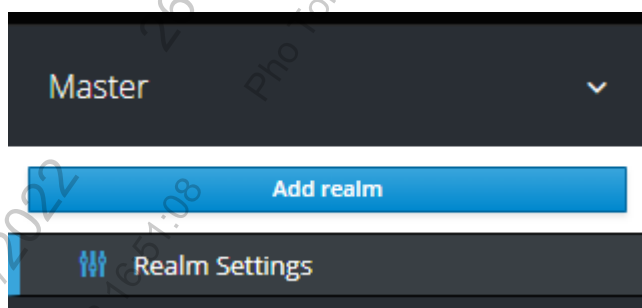
Mặc định ban đầu, Keycloak sẽ khởi tạo 1 realm có tên Master, realm này có quyền cao nhất trong các realm, bởi vậy chúng ta không nên sử dụng realm này để quản lý user và các thông tin liên quan. Nó chỉ nên được sử dụng để user admin của nó tạo và quản lý các realm. Mỗi realm cần phải có user admin riêng và chúng ta sẽ sử dụng user admin của từng realm để quản lý users cho realm đó.

	TỔNG CÔNG TY GIẢI PHÁP DOANH NGHIỆP VIETTEL	Mã hiệu: HD.VTS.TTGPDN.02
	TÀI LIỆU GUIDELINE KEYCLOAK	Ngày có hiệu lực: 20/06/2022
		Ngày hết hiệu lực: 20/06/2023
		Lần ban hành: 01
		Trang: 29/33

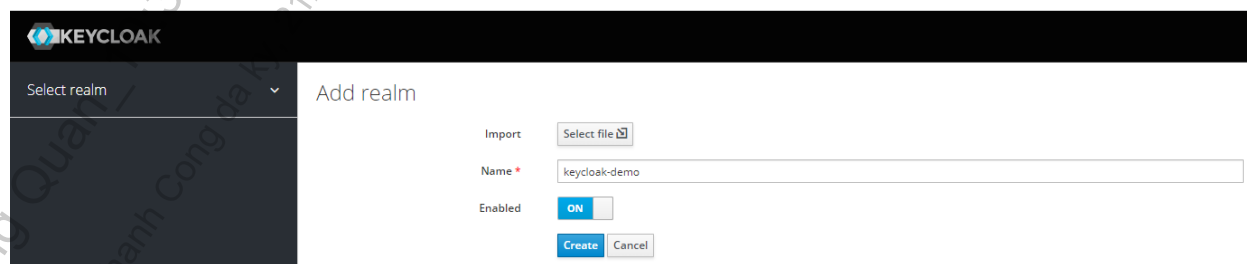


RHSSO_44_0919

Để tạo mới một realm trong Keycloak, trong trang Keycloak Admin Console, chúng ta chỉ cần click vào menu item “Add realm”:




Sau đó điền tên của realm và “Create”



Vậy là chúng ta đã tạo thành công Realm

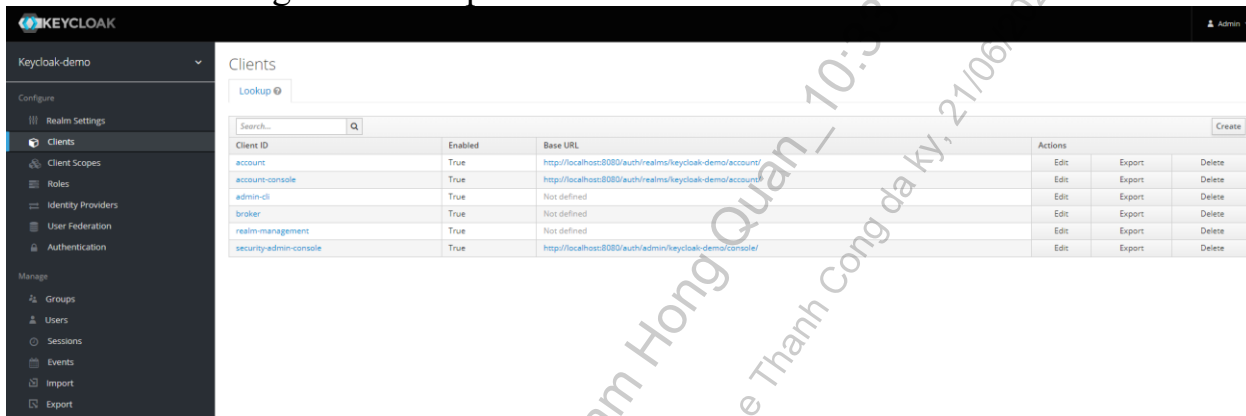
5.3.3 Tạo client trong realms

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

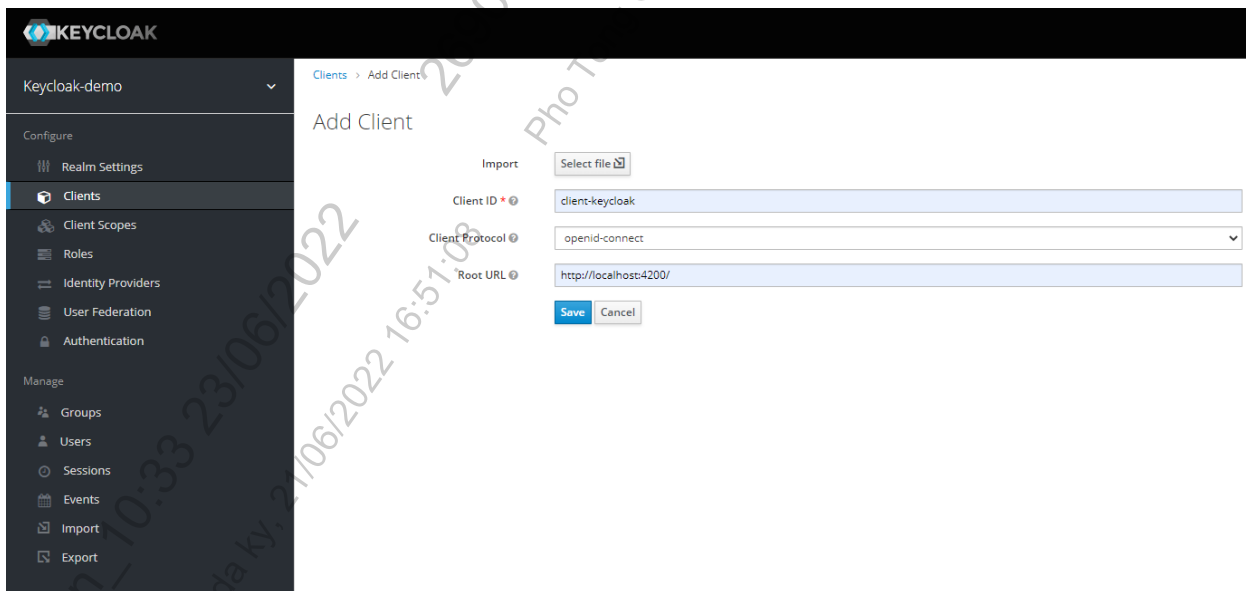
	TỔNG CÔNG TY GIẢI PHÁP DOANH NGHIỆP VIETTEL	Mã hiệu: HD.VTS.TTGPDN.02
	TÀI LIỆU GUIDELINE KEYCLOAK	Ngày có hiệu lực: 20/06/2022
		Ngày hết hiệu lực: 20/06/2023
		Lần ban hành: 01
		Trang: 30/33

quản lý tất cả những client sẽ connect tới nó, theo giao thức, chuẩn authentication và authorization nào.

Sau khi tạo xong realm, tiếp theo chúng ta tạo client, click vào menu Client chọn button “create” ở góc trên bên phải màn hình.



Chúng ta nhập Client ID, Root URL sau đó chọn client protocol. Nhấn nút “save” để tạo client



Tùy thuộc vào option Client Protocol mà chúng ta chọn, tương ứng với đó sẽ hiển thị ra option khác nhau sau khi “save”. Ví dụ dùng client protocol là openid-connect thì kết quả sau khi click “Save” sẽ như sau

The screenshot shows the Keycloak Admin Console interface. On the left is a sidebar with navigation options: Keycloak-demo, Configure (Realm Settings, Clients, Client Scopes, Roles, Identity Providers, User Federation, Authentication), and Manage (Groups, Users, Sessions, Events, Import, Export). The main panel is titled 'Client-keycloak' and contains various configuration tabs: Settings, Keys, Roles, Client Scopes, Mappers, Scope, Revocation, Sessions, Offline Access, and Installation. The 'Settings' tab is active, displaying the following configuration options:


- Client ID: client-keycloak
- Name: (empty)
- Description: (empty)
- Enabled: ☒ ON
- Always Display in Console: ☐ OFF
- Consent Required: ☐ OFF
- Login Theme: (dropdown menu)
- Client Protocol: openid-connect
- Access Type: public
- Standard Flow Enabled: ☒ ON
- Implicit Flow Enabled: ☐ OFF
- Direct Access Grants Enabled: ☒ ON
- OAuth 2.0 Device Authorization Grant Enabled: ☐ OFF
- Front Channel Logout: ☐ OFF
- Root URL: http://localhost:4200
- * Valid Redirect URIs: /*
- Base URL: (empty)

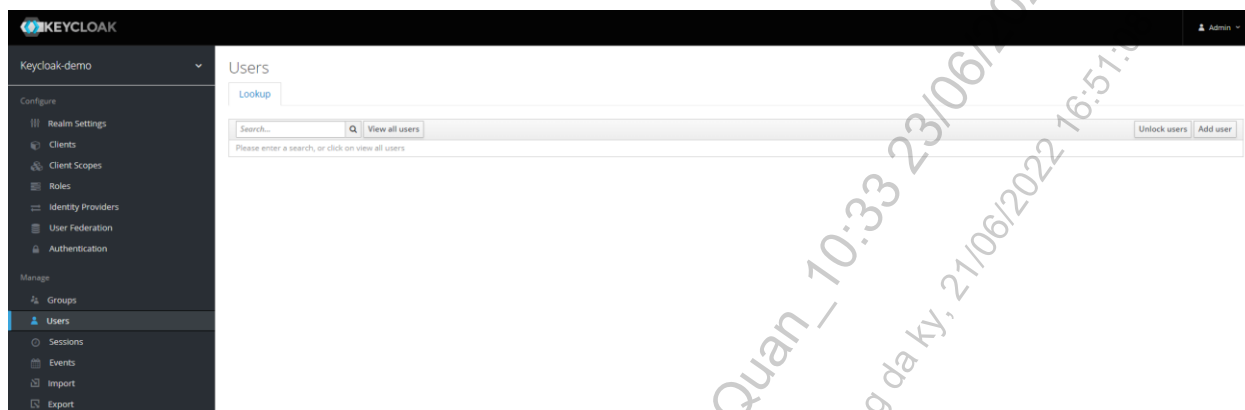
Tùy vào dự án mà có các option phù hợp mà keycloak đưa ra, tuy nhiên cần chú ý một số các option chính cần phải cấu hình:

- Root URL: là một giá trị sẽ được sử dụng để phân giải các đường dẫn tương đối.
- Valid Redirect URIs: đầu vào có thể là 1 pattern hoặc là 1 url trực tiếp, trường này bắt buộc có, ví dụ trong ảnh trên, sau khi login thành công, keycloak sẽ redirect tới 1 địa chỉ khớp với pattern http://localhost:4200/*
- Web Origins: sử dụng để cấu hình Cross-Origin Resource Sharing

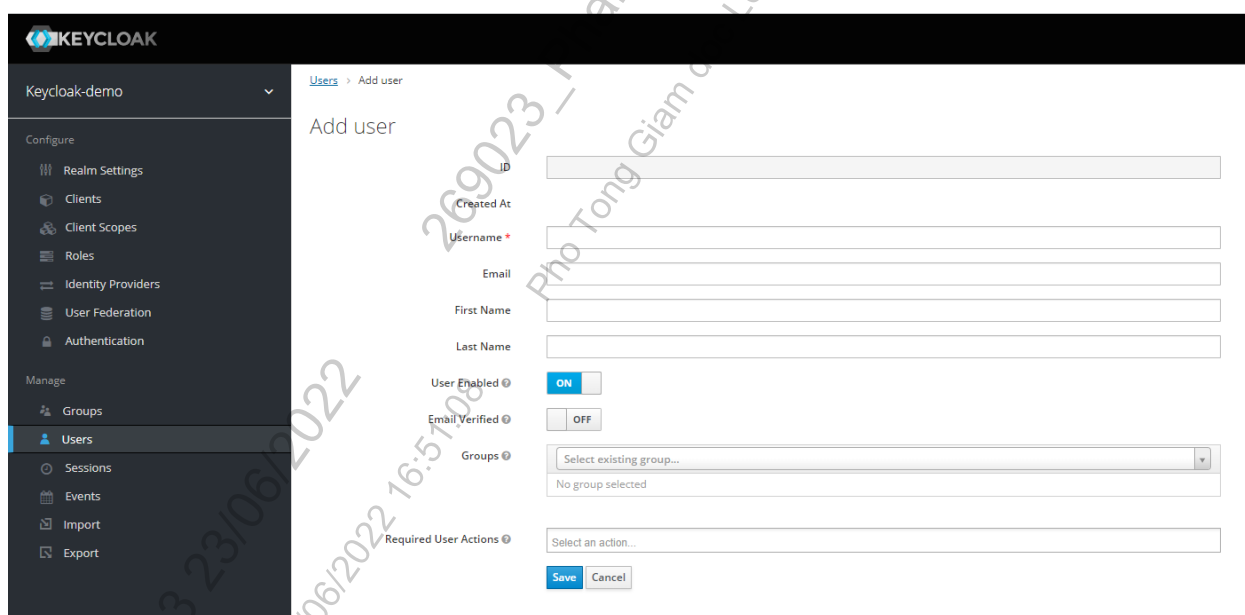
5.3.4 Tạo user

Để sử dụng các application mà chúng ta sử dụng Keycloak cho authentication và authorization, chúng ta cần có user để đăng nhập. Thông thường ở các hệ thống lớn thì thông tin user sẽ được lưu trữ trong Active Directory (AD) hoặc LDAP, Keycloak có thể kết nối tới các hệ thống này để lấy thông tin user. Nó cũng có thể lưu trữ thông tin user trực tiếp. Để tạo user trên keycloak sẽ là như sau:

	TỔNG CÔNG TY GIẢI PHÁP DOANH NGHIỆP VIETTEL	Mã hiệu: HD.VTS.TTGPDN.02
	TÀI LIỆU GUIDELINE KEYCLOAK	Ngày có hiệu lực: 20/06/2022
		Ngày hết hiệu lực: 20/06/2023
		Lần ban hành: 01
		Trang: 32/33



Click vào button “Add user” ở góc phải phía trên màn hình để hệ thống hiển thị ra form tạo thông tin user, sau đó điền thông tin vào các trường và chọn “save”



Có 1 số trường cần lưu ý:

- ID và Created At: được tự động sinh ra khi chúng ta tạo thành công user.
- Username: là tên username để người dùng đăng nhập
- Email: email của người dùng
- Firstname và Lastname: thông tin họ tên người dùng
- User Enable: trạng thái hoạt động của user.
- Email Verified: Người dùng có cần dùng email để xác thực không ?
- Group: Nhóm mà user được tham gia, có thể chọn nhiều nhóm khác nhau
- Required User Actions: Trường này sẽ yêu cầu người dùng thực hiện hành động một hoặc nhiều hành động sau:



**TỔNG CÔNG TY GIẢI PHÁP DOANH
NGHIỆP VIETTEL**

Mã hiệu: HD.VTS.TTGPDN.02

**TÀI LIỆU GUIDELINE
KEYCLOAK**

Ngày có hiệu lực: 20/06/2022

Ngày hết hiệu lực: 20/06/2023

Lần ban hành: 01

Trang: 33/33

- + Configure OTP: bắt buộc người dùng cài đặt mã OTP trên thiết bị di động để đăng nhập
- + Update Password: yêu cầu user cập nhật 1 mật khẩu mới
- + Update profile: Yêu cầu người dùng nhập thông tin cá nhân mới
- + Verify Email: hệ thống gửi yêu cầu xác thực tới email, yêu cầu người dùng check mail và xác thực.