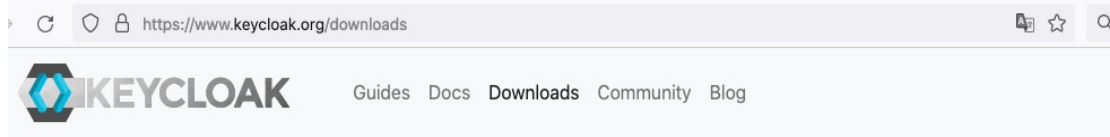


1. Download the latest keycloak server from <https://www.keycloak.org/downloads>.



Downloads 20.0.0

For a list of community maintained extensions check out the [Extensions](#) page.

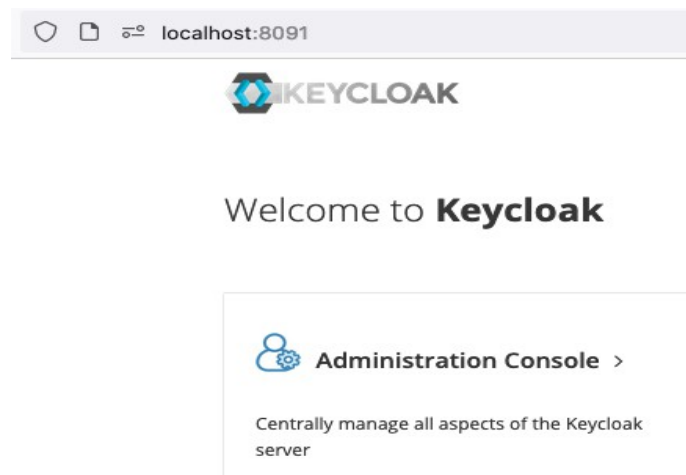
Server

Keycloak	Distribution powered by Quarkus	ZIP (sha1)
----------	---------------------------------	----------------------------

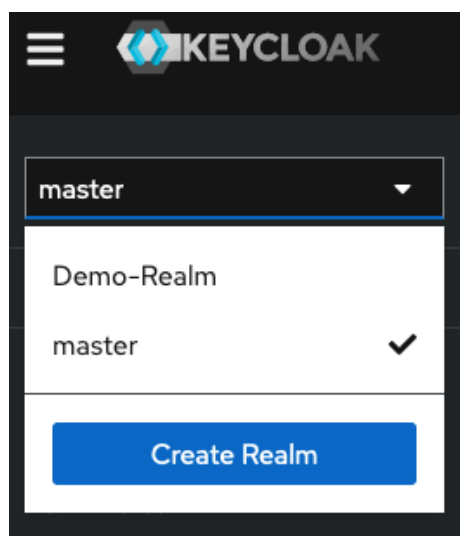
2. Unzip, open a terminal and change to directory keycloak-20.0.0 and run: `bin/kc.sh start-dev --http-port 8091`

```
[gho@macbook19 keycloak-20.0.0 % bin/kc.sh start-dev --http-port 8091
```

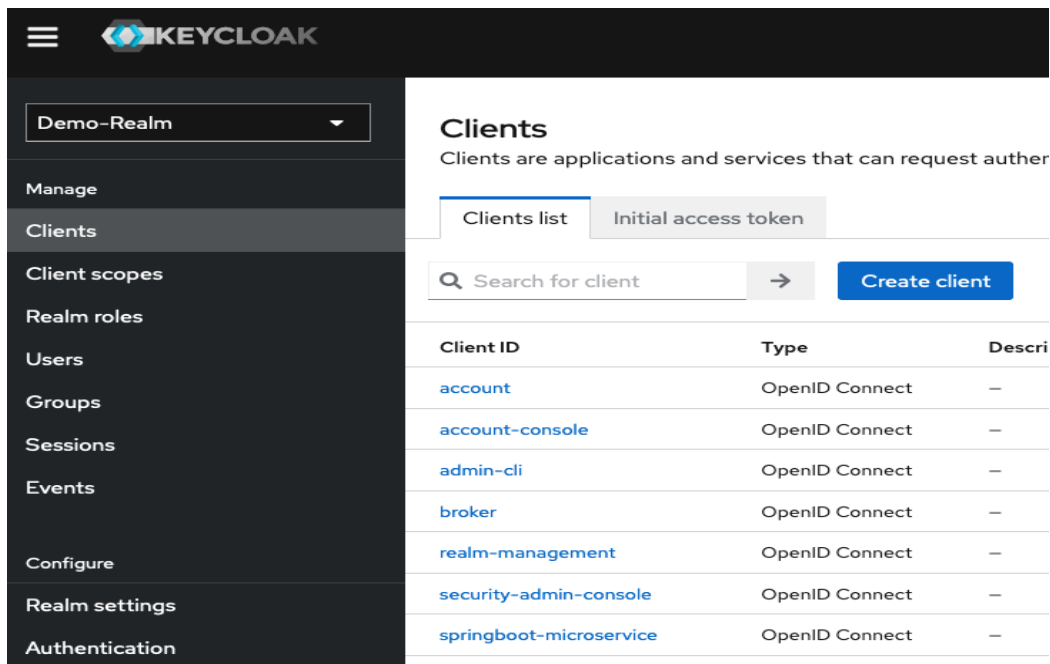
3. Open keycloak admin console



4. Have a look at <https://www.djamware.com/post/6225b66ba88c55c95abca0b6/spring-boot-security-postgresql-and-keycloak-rest-api-oauth2>
5. Create an admin account
6. Create a new Realm **Demo-Realm** and select it



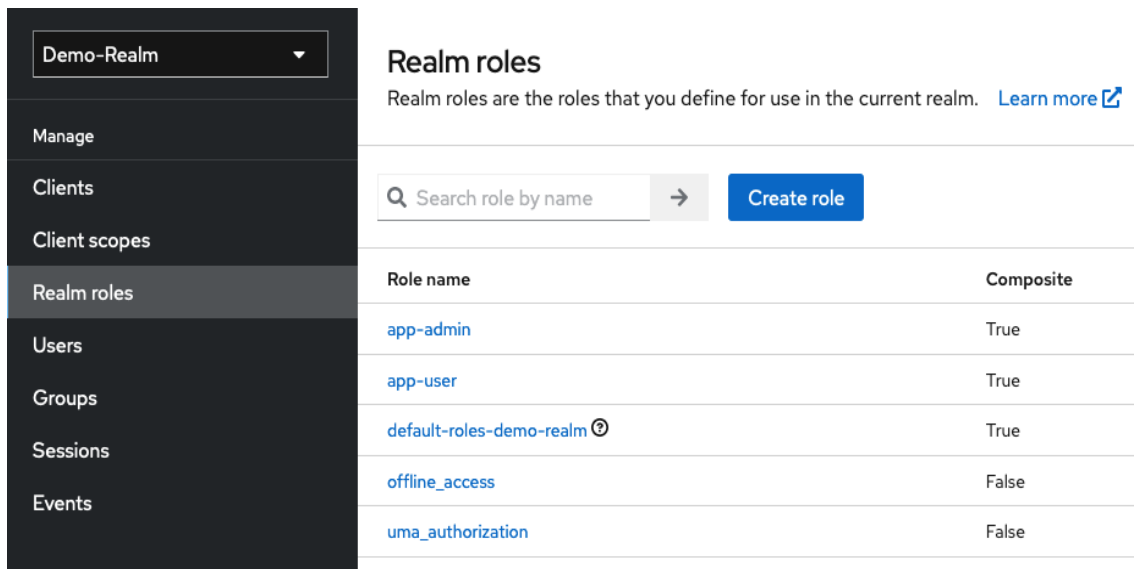
7. Create a new client **springboot-microservice**



The screenshot shows the Keycloak Admin Console for the 'Demo-Realm'. The left sidebar contains navigation links: Manage, Clients, Client scopes, Realm roles, Users, Groups, Sessions, Events, Configure, Realm settings, and Authentication. The 'Clients' page is active, displaying a list of clients. The 'Clients list' tab is selected, showing a search bar and a 'Create client' button. Below is a table of existing clients.

Client ID	Type	Description
account	OpenID Connect	—
account-console	OpenID Connect	—
admin-cli	OpenID Connect	—
broker	OpenID Connect	—
realm-management	OpenID Connect	—
security-admin-console	OpenID Connect	—
springboot-microservice	OpenID Connect	—

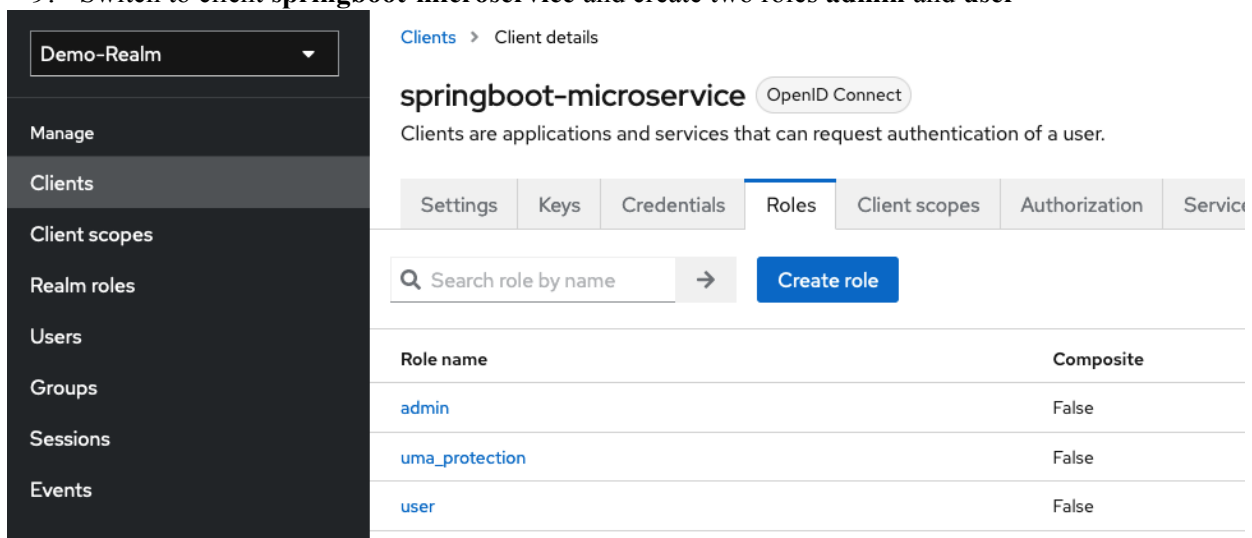
8. Create two Realm-Roles **app-admin** and **app-user**



The screenshot shows the 'Realm roles' page in the Keycloak Admin Console. The left sidebar is the same as the previous screenshot. The 'Realm roles' page has a search bar and a 'Create role' button. Below is a table of existing realm roles.

Role name	Composite
app-admin	True
app-user	True
default-roles-demo-realm	True
offline_access	False
uma_authorization	False

9. Switch to client **springboot-microservice** and create two roles **admin** and **user**



The screenshot shows the 'Client details' page for the 'springboot-microservice' client in the Keycloak Admin Console. The left sidebar is the same. The 'Clients' link is selected, and the 'Client details' page is active. The 'Roles' tab is selected, showing a search bar and a 'Create role' button. Below is a table of existing roles for this client.

Role name	Composite
admin	False
uma_protection	False
user	False

10. Switch to Realm-Roles and select Role **app-user**, click on Action and select „Add associated roles“

[Realm roles](#) > Role details

app-user Composite

Details

Associated roles

Attributes

Users in role

Permissions

Action

Add associated roles

Delete this role

Role name *

app-user

Description

Save

Revert

11. Select „filter by clients“ and enter „springboot-microservices“ and select role **user**
Assign roles to app-user account

Filter by clients

Q spring

1-3



Name

Description



springboot-microservice admin



springboot-microservice uma_protection



springboot-microservice user

1-3

Assign

Cancel

12. Realm-Role app-user is now a composite role

[Realm roles](#) > Role details

app-user Composite

Details

Associated roles

Attributes

Users in role

Permissions

Q Search by name



☒ Hide inherited roles

Assign role

Unassign



Name

Inherited

Description



springboot-microservice user

False

—

13. Do the same with Realm-Role app-admin and associate role admin

app-user Composite

Details Associated roles Attributes Users in role Permissions

Search by name



☒ Hide inherited roles

Assign role

Unassign

<input type="checkbox"/>	Name	Inherited	Description
<input type="checkbox"/>	springboot-microservice user	False	—

14. Create 3 Users named employee1 – employee3, set „Email verified“ to „On“

[Users](#) > Create user

Create user

Username *	<input type="text" value="employee1"/>
Email	<input type="text" value="m0.m0@company.com"/>
Email verified ?	<input checked="" type="checkbox"/> On
First name	<input type="text" value="Max0"/>
Last name	<input type="text" value="Mustermann0"/>
Required user actions ?	<input type="text" value="Select action"/>
Groups ?	<input type="button" value="Join Groups"/>
<input type="button" value="Create"/> <input type="button" value="Cancel"/>	

15. Set user credentials

[Users](#) > User details

employee1


Details

Attributes

Credentials

Role mapping

Groups

?	Type	User label
⋮	Password	My password 

16. Assign Realm-Role **app-user** to employee1

[Users](#) > User details

employee1

Details

Attributes


Credentials

Role mapping

Groups

Consents

Identity providers

 ☒ Hide inherited roles Assign role Unassign

<input type="checkbox"/> Name	Inherited	Description
<input type="checkbox"/> app-user	False	—
<input type="checkbox"/> default-roles-demo-realm	False	`\${role_default-roles}`

17. Remove all actions in field „Required user action“ and save

18. Repeat everything from point 14-17 with employee2 and assign Realm-Role app-admin

[Users](#) > User details

employee2

Details


Attributes

Credentials

Role mapping

Groups

Consents

 ☒ Hide inherited roles Assign role

<input type="checkbox"/> Name	Inherited
<input type="checkbox"/> default-roles-demo-realm	False
<input type="checkbox"/> app-admin	False

19. Repeat everything from point 14-17 with employee3 and assign Realm-Role **app-admin** and **app-user**

[Users](#) > User details

employee3

Details	Attributes	Credentials	Role mapping	Groups	Conse
---------	------------	-------------	--------------	--------	-------

☒ Hide inherited roles

<input type="checkbox"/> Name	Inherited
<input type="checkbox"/> app-user	False
<input type="checkbox"/> default-roles-demo-realm	False
<input type="checkbox"/> app-admin	False

20. Switch to client scopes and add new scope read

Client scopes

Client scopes are a common set of protocol mappers and roles that are shared between i

<input type="checkbox"/> Name	Assigned type	Protocol
<input type="checkbox"/> read	None	OpenID Conn

21. Assign Realm-Roles app-admin, app-user and Roles user and admin to scope read

[Client scopes](#) > Client scope details

read openid-connect

Settings	Mappers	Scope
----------	---------	-------

☒ Hide inherited roles

<input type="checkbox"/> Name	Inherited
<input type="checkbox"/> app-user	False
<input type="checkbox"/> app-admin	False
<input type="checkbox"/> springboot-microservice admin	False
<input type="checkbox"/> springboot-microservice user	False

22. sdfsd