Shynbolat Unaibayev, Practice 4 report

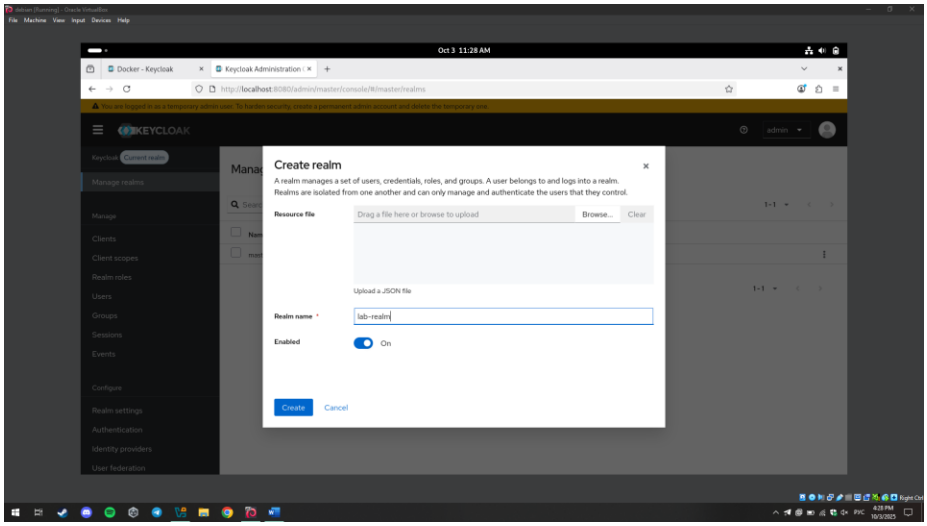
Keycloak Resource Server Integration Lab Report

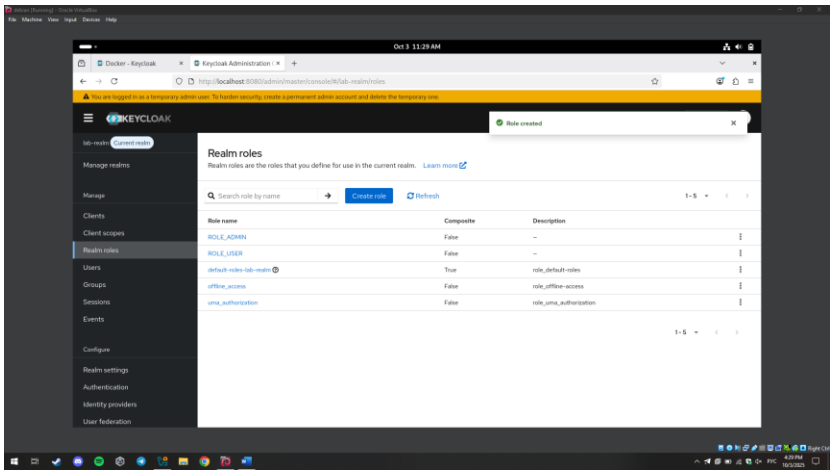
1. Introduction

The purpose of this lab is to integrate Keycloak as an Identity and Access Management (IAM) solution with a simple resource server. The lab demonstrates authentication and authorization using Keycloak-issued tokens, role-based access control, and token refresh functionality.

2. Environment Setup

Keycloak was installed locally and a new realm named 'lab-realm' was created. Two users were configured:
- user1 (assigned ROLE_USER)
- admin1 (assigned ROLE_ADMIN)

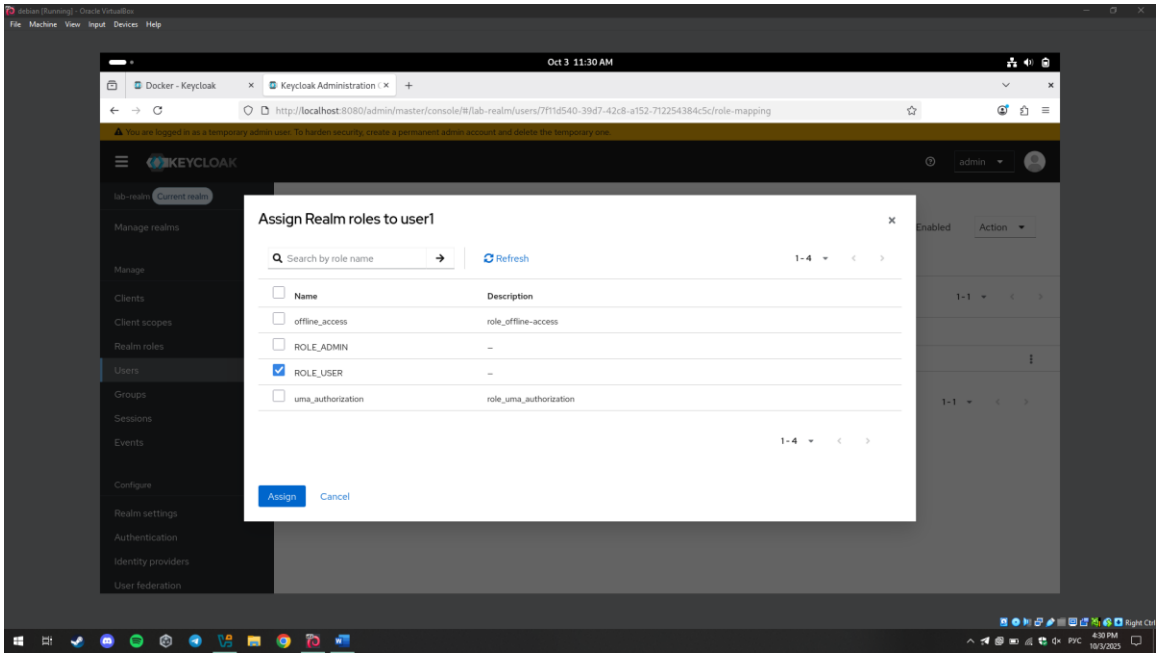




A demo client ('demo-client') was created with the following settings:

- Standard flow enabled
- Direct access grants enabled
- Client authentication disabled

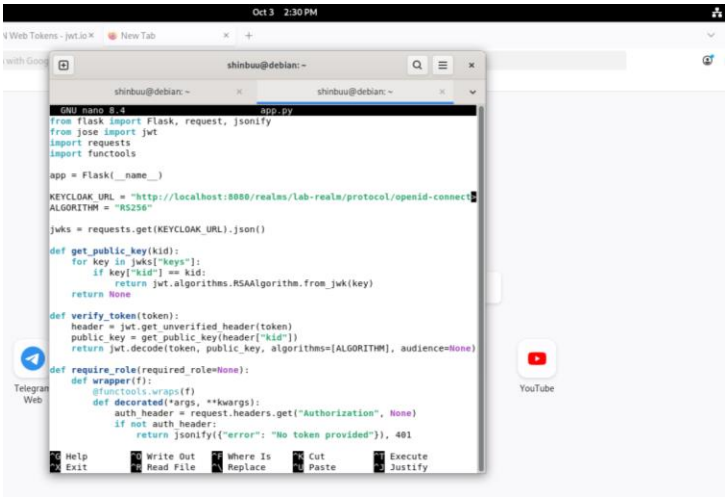
Screenshot:

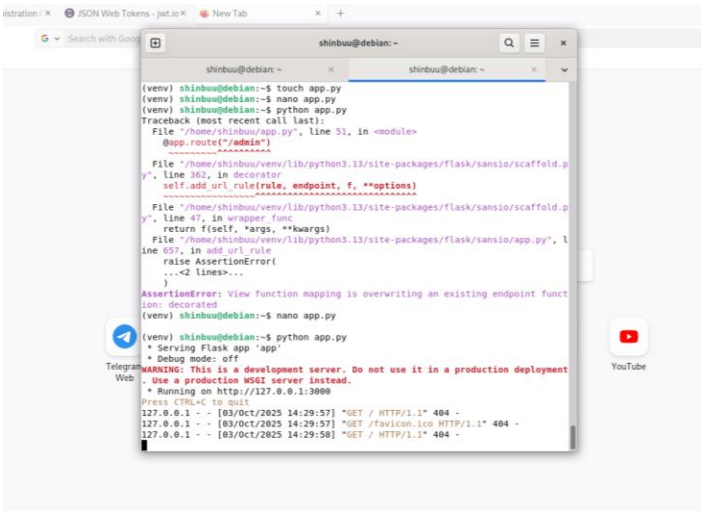


3. Resource Server Implementation

A simple Python Flask application was developed with two endpoints:
- /user → accessible to ROLE_USER and ROLE_ADMIN
- /admin → accessible only to ROLE_ADMIN

JWT validation was implemented using the Keycloak public key. Role checks were added to enforce access restrictions.





4. Testing Access with Tokens

Access tokens were obtained via Direct Access Grants using cURL commands. The following tests were performed:

- Accessing /user with user1 → SUCCESS

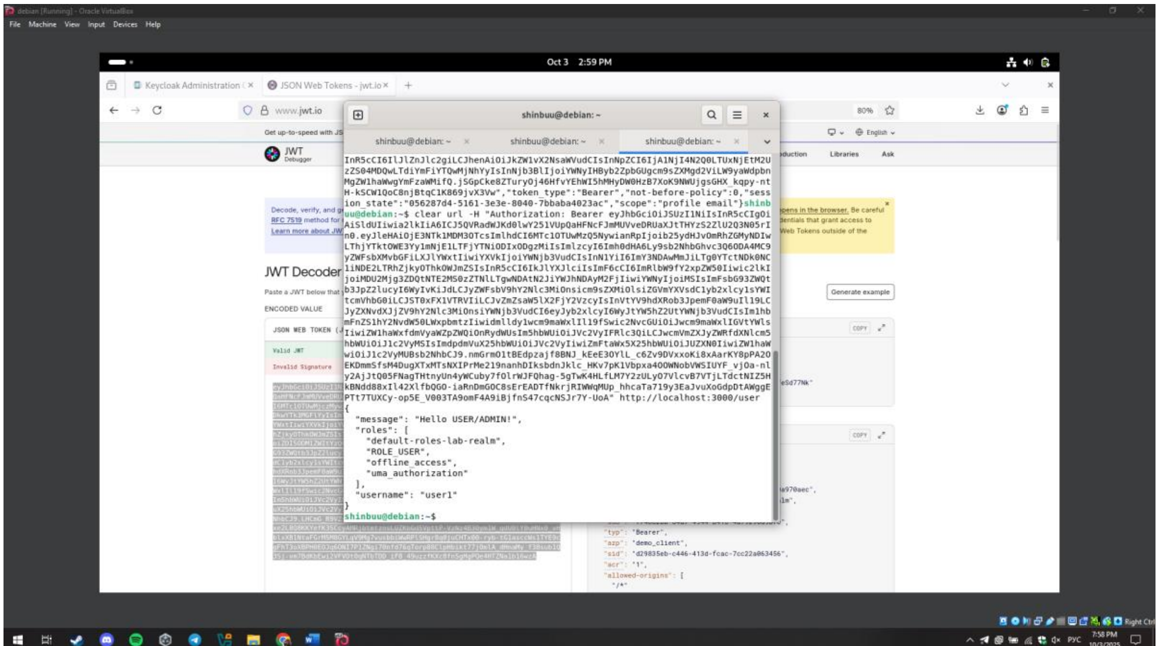
- Accessing /admin with user1 → FORBIDDEN

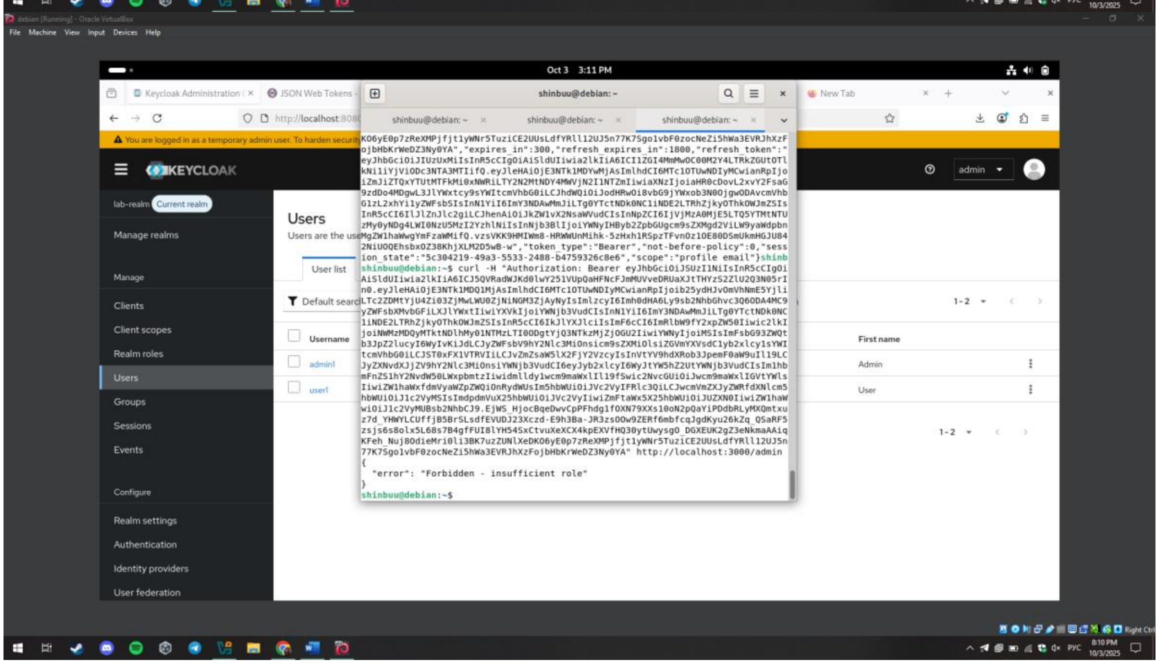
- Accessing /user with admin1 → SUCCESS

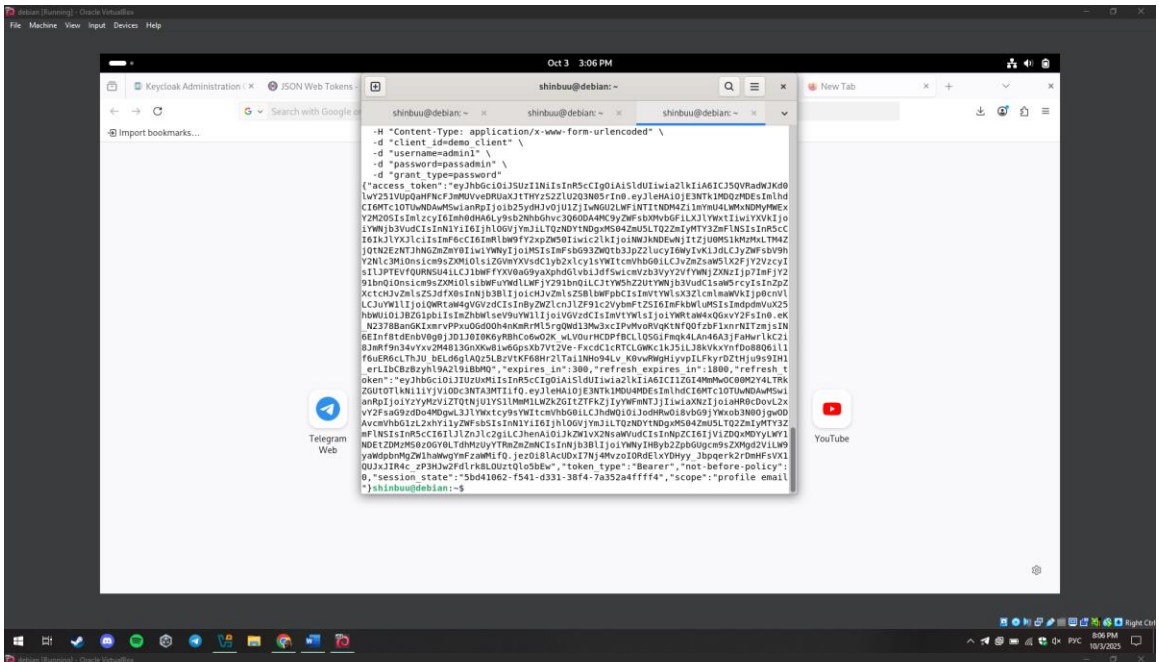
- Accessing /admin with admin1 → SUCCESS

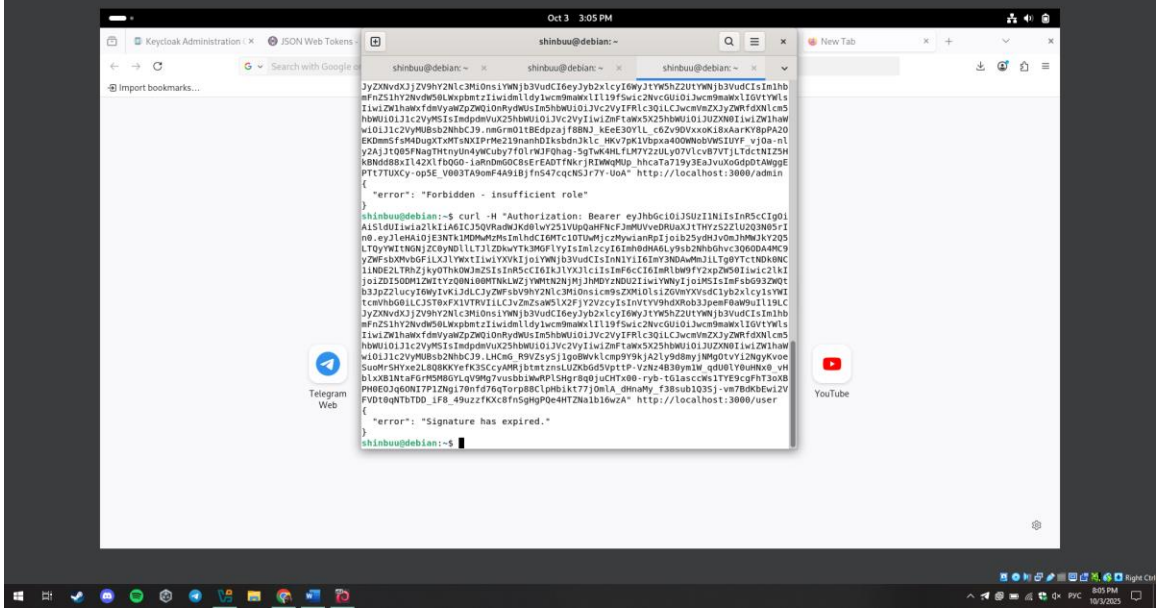
- Accessing without token → UNAUTHORIZED

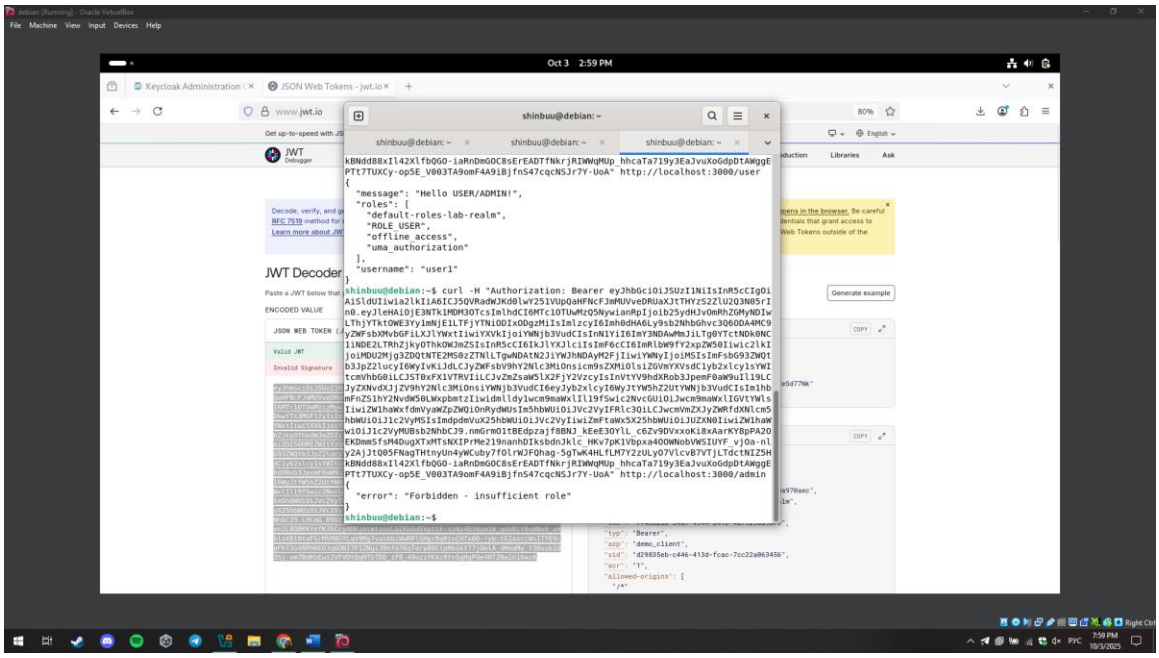
- Accessing with expired token → INVALID TOKEN


Oct 3 2:59 PM
Keycloak Administration
JSON Web Tokens - jwt.io
shinbuu@debian: ~
JWT Decoder
{
"message": "Hello USER/ADMIN!",
"roles": [
"default-roles-lab-realm",
"ROLE_USER",
"offline_access",
"uma_authorization"
],
"username": "user1"
}
shinbuu@debian:~$


Oct 3 3:11 PM
Keycloak Administration
shinbuu@debian: ~
KEYCLOAK
lab-realm
Current realm
Manage realms
Manage
Clients
Client scopes
Realm roles
Users
Groups
Sessions
Events
Configure
Realm settings
Authentication
Identity providers
User federation
Users
User list
Username
First name
admin1
Admin
user1
User
{
"error": "Forbidden - insufficient role"
}
shinbuu@debian:~$


debian [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Oct 3 3:06 PM
shinbuu@debian: ~
shinbuu@debian: ~
shinbuu@debian: ~
shinbuu@debian: ~
-H "Content-Type: application/x-www-form-urlencoded" \
-d "client_id=demo_client" \
-d "username=admin1" \
-d "password=passadmin" \
-d "grant_type=password"
{"access_token":"eyJhbGciOiJSUzI1NiIsInR5cCIgOiAiSldUIiwia2lkIiA6ICJ5QVRadWJKd0
lwY251VUpQaHFNcFJmMUVveDRUaXJtTHYzS2ZlU2Q3N05rIn0.eyJleHAiOjE3NTk1MDQzMDEsImlhd
CI6MTc1OTUwNDAwMSwianRpIjoib25ydHJvOjU1ZjIwNGU2LWFiNTItNDM4Z1lmYmU4LWMxNDMyMWEx
Y2M2OSIsImlzcyI6Imh0dHA6Ly9sb2NhbGhvc3Q6OTA4MC9yZWFsbXMvbGFiLXJlYWxtIiwiYXVkIjo
iYWNjb3VudCIsInN1YiI6IjhlOGVjYmJiLTQzNDYtNDgxMS04ZmU5LTQ2ZmIyMTY3ZmFlNSIsInR5cC
I6IkJlYXJlciIsImF6cCI6ImRlbW9fY2xpZW50Iiwic2lkIjoiNWJkNDEwNjItZjU0MS1kMzMxLTM4Z
jQtN2EzNTJhNGZmZmY0IiwiYWNyIjoiMSIsImFsbG93ZWQtb3JpZ2lucyI6WyIvKiJdLCJyZWFsbV9h
Y2Nlc3MiOnsicm9sZXMiOlsiZGVmYXVsdC1yb2xlcy1sYWItcmVhbG0iLCJvZmZsaW5lX2FjY2VzcyI
sIlJPTEVfQURNSU4iLCJlbWFfYXV0aG9yaXphdGlvbiJdfSwicmVzb3VyY2VfYWNjZXNzIjp7ImFjY2
9lbnQiOnsicm9sZXMiOlsibWFuYWdlLWFjY291bnQiLCJtYW5hZ2UtYWNjb3VudCIsaW5rcyIsInZpZ
XctcHJvZmlsZSJdfX0sInNjb3BlIjoicHJvZmlsZSBlbWFpbCIsInVtYWlsX3ZlcmlmaWVkIjp0cnVl
LCJuYW1lIjoiQWRtaW4gVGVzdCIsInByZWZlcnJlZF91c2VybmFtZSI6ImFkbWluMSIsImdpdmVuX25
hbWUiOiJBZGlpbiIsImZhbWlseV9uYW1lIjoiVGVzdCIsImVtYWlsIjoiYWRtaW4xQGxvY2FsIn0.eK
_N2378BanGKIxmrvPPxuOGdOOh4nKmRrMlSrgQWd13Mw3xcIPvMvoRVqKtNfQOfzbF1xnrNITzmjsIN
6EInf8tdEnbV0g0jJD1J0I0K6yRBhCo6wO2K_wLVOurHCDPfBCLlQ5GiFmqk4LAn46A3jFaHwrlkC2i
8JmRf9n34vYxv2M4813GnXKw8iw6GpsXb7Vt2Ve-FxcdC1cRTCLGWKc1kJ5iLJ8kVkxYnfDo88Q6il
f6uER6cLThJU_bELd6glAQz5LBzVtKF68Hr2lTa11NHo94Lv_K0vwRHgHiyvpILFkyrDZtHjuOs9IH1
_erLIbCBzBzyhl9A2l9iBbMQ","expires_in":300,"refresh_expires_in":1800,"refresh_t
oken":"eyJhbGciOiJIUzUxMiIsInR5cCIgOiAiSldUIiwia2lkIiA6ICI1ZGI4MmMwOC00M2Y4LTRk
ZGUtOTlkNi1iYjViODc3NTA3MTIifQ.eyJleHAiOjE3NTk1MDU4MDEsImlhdCI6MTc1OTUwNDAwMSwi
anRpIjoiYzYyMzViZTQtNjU1YS1lMmM1LWZkZGItZTFkZjIyYWFmNTJjIiwiaXNzIjoiaHR0cDovL2x
vY2FsaG9zdDo4MDgwL3llYWxtcy9sYWItcmVhbG0iLCJhdWQiOiJodHRwOi8vbG9jYWxob3N0OjgwOD
AvcmVhbG1zL2xhYi1yZWFsbSIsInN1YiI6IjhlOGVjYmJiLTQzNDYtNDgxMS04ZmU5LTQ2ZmIyMTY3Z
mFlNSIsInR5cCI6IlJlZnJlc2giLCJhenAiOiJkZW1vX2NsaWVudCIsInNpZCI6IjViZDQxMDYyLWY1
NDEtZDMzMS0zOGY0LTdhMzUyYTRmZmZmNCIsInNjb3BlIjoiYWNyIHByb2ZpbGUgcm9sZXMgd2VlLW9
yaWdpbnMgZW1haWwgYmFzaWMifQ.jezQi81AcUDxI7NjdMvzoIORdElxYDHyy_Jbpqerk2rDmHFsVXI
QUJxJIR4c_zP3HJw2FdlrkBLOUztQlo5bEw","token_type":"Bearer","not-before-policy":
0,"session_state":"5bd41062-f541-d331-38f4-7a352a4ffff4","scope":"profile email
"}shinbuu@debian:~$
Telegram Web
YouTube
Right Ctrl
PYC
8:06 PM
10/3/2025

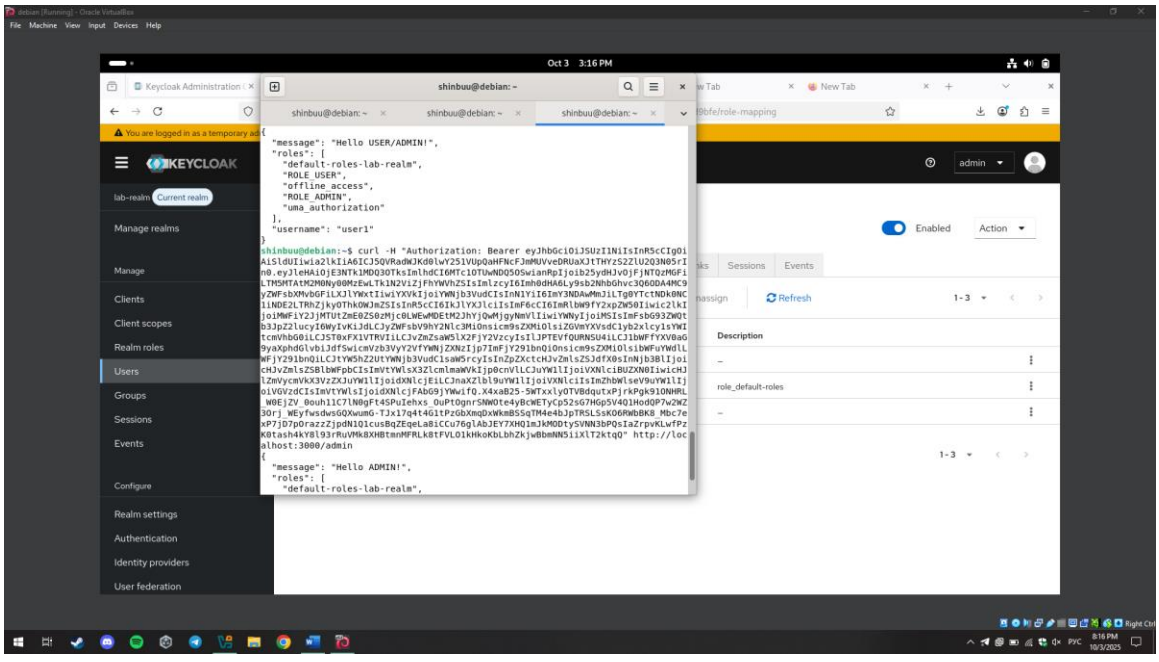

debian [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Oct 3 3:05 PM
shinbuu@debian: ~
shinbuu@debian: ~
shinbuu@debian: ~
shinbuu@debian: ~
JyZXNvdXJjZV9hY2Nlc3MiOnsiYWNjb3VudCI6eyJyb2xlcyI6WyJtYW5hZ2UtYWNjb3VudCIsIm1hb
mFnZS1hY2NvdW50LWxpbmtzIiwidmlldyIsImd9maWxlIl19fSwic2NvcGUiOiJwcm9maWxlIGVtYWls
IiwiZW1haWxfdmVyaWZpZWQiOnRydWUsIm5hbWUiOiJVc2VyIFRlc3QiLCJwcmVmZXJyZWRfdXNlcm5
hbWUiOiJlc2VyMSIsImdpdmVuX25hbWUiOiJVc2VyIiwiZmFtaWx5X25hbWUiOiJUZXN0IiwiZW1haW
wiOiJ1c2VyMUBsb2NhbCJ9.nmGrmQ1tBEdpzajf8BNJ_kEeE3OYlL_c6Zv9OVxxoKi8xAarKY8pPA2O
EKDmmSfsM4DugXTxMTsNXIPrMe219nanhDIksbdnJklc_HKv7pK1Vbpxa4OOWNobVWSIUYF_vjOa-nl
y2AjJtQ05FNagTHtnyUn4yWCuby7fOlrWJFQhag-5gTwK4HLfLM7Y2zULyO7VlcvB7VTjLTdctNIZ5H
kBNdd88xIl42XlfbQGO-iaRnDmGOC8sErEADTfNkrjRIWWqMUp_hhcaTa719y3EaJvuXoGdpDtAWggE
PTt7TUXCy-op5E_V003TA9omF4A9iBjfnS47cqcN5Jr7Y-UoA" http://localhost:3000/admin
{
"error": "Forbidden - insufficient role"
}
shinbuu@debian:~$ curl -H "Authorization: Bearer eyJhbGciOiJSUzI1NiIsInR5cCIgOi
AiSldUIiwia2lkIiA6ICJ5QVRadWJKd0lwY251VUpQaHFNcFJmMUVveDRUaXJtTHYzS2ZlU2Q3N05ri
n0.eyJleHAiOjE3NTk1MDMwMzMsImlhdCI6MTc1OTUwMjczMywianRpIjoib25ydHJvOmJhMWJkY2O5
LTQyYWItNGNjZC0yNDllLTJlZDkwYTk3MGFlYyIsImlzcyI6Imh0dHA6Ly9sb2NhbGhvc3Q6ODA4MC9
yZWFsbXMvbGFiLXJlYWxtIiwiYXVkIjoiYWNjb3VudCIsInN1YiI6Im9jNDAwMmJiLTg0YTctNDk0NC
1lNDE2LTRhZjkyOThkOWJmZSIsInR5cCI6IkJlYXJlciIsImF6cCI6ImRlbW9fY2xpZW50Iiwic2lkI
joiZDI5ODM1ZWItZjQ0Ni00MTNkLWZjYWMtN2NjMjJhMDYzNDU2IiwiYWNyIjoiMSIsImFsbG93ZWQt
b3JpZ2lucyI6WyIvKiJdLCJyZWFsbV9hY2Nlc3MiOnsicm9sZXMiOlsiZGVmYXVsdC1yb2xlcy1sYWI
tcmVhbG0iLCJST0xFX1VTRVIiLCJvZmZsaW5lX2FjY2VzcyIsInVtYV9hdXRob3JpemF0aW9uIl19LC
JyZXNvdXJjZV9hY2Nlc3MiOnsiYWNjb3VudCI6eyJyb2xlcyI6WyJtYW5hZ2UtYWNjb3VudCIsIm1hb
mFnZS1hY2NvdW50LWxpbmtzIiwidmlldyIsImd9maWxlIl19fSwic2NvcGUiOiJwcm9maWxlIGVtYWls
IiwiZW1haWxfdmVyaWZpZWQiOnRydWUsIm5hbWUiOiJVc2VyIFRlc3QiLCJwcmVmZXJyZWRfdXNlcm5
hbWUiOiJ1c2VyMSIsImdpdmVuX25hbWUiOiJVc2VyIiwiZmFtaWx5X25hbWUiOiJUZXN0IiwiZW1haW
wiOiJ1c2VyMUBsb2NhbCJ9.LHCmG_R9VZsySj1goBWvklcmp9Y9kjA2ly9d8myjNMgOtvYi2NgyKvoe
SuoMrSHYxe2L8Q8KKYefK3SCcyAMRjbtmtznsLU2Xb6d5VptP-VzNz4B30ym1W_qdU0lY0uHNx0_vH
blxXB1NtaF6rHSM8GYLqV9Mq7vusbbiWwPlSHgr8q0juCHTx00-ryb-tGlasccWs1TYE9cgFhT3oXB
PH0EOJq6ONI7P1ZNgi70nfd76qTorp88ClpHbikt77jOmlA_dHnaMy_f38sub1Q3Sj-vm7BdKbEwi2V
FVDt0qNTbTDD_iF8_49uzzfKXc8fnSgHgPQe4HTZNa1b16wZA" http://localhost:3000/user
{
"error": "Signature has expired."
}
shinbuu@debian:~$
Telegram Web
YouTube
Right Ctrl
PYC
8:05 PM
10/3/2025



5. Role Modification

User roles were modified in Keycloak. For example, ROLE_ADMIN was removed from admin1. After obtaining a new token, the user could no longer access the /admin endpoint. This confirmed that Keycloak role assignments directly affect authorization.

Screenshot:



7. Comparison of Flows

Two authentication flows were compared:
- Password Grant (Direct Access Grants): Simple to test with cURL, but less secure because it requires the client to handle user credentials directly.
- Authorization Code Flow (Standard Flow): More secure, since credentials are only entered at Keycloak's login page and the client receives only tokens.

The lab primarily used Direct Access Grants, but Standard Flow is recommended for production.

8. Conclusion

The lab successfully demonstrated Keycloak integration with a resource server, role-based access control, and token management. Key results include:
- Verified access control based on roles
- Demonstrated role modification impact
- Tested refresh token usage
- Compared Direct Access vs Standard Flow