Hands-on

oidc-agent & WLCG JWT profile

Initial setup

- Install oidc-agent
- Use the Quantum Tea IAM instance for the exercises
  - if you do not already have an account, register one

Exercise

- Register an oidc-agent Client
  - check the local oidc-agent configuration
- Request an access token
  - decode the access token and check the JWT profile used
- Choose the WLCG JWT profile for your Client
  - Add the `wlcg` scope to your Client through the IAM dashboard
  - Update the local Client configuration by repeating the OAuth authZ flow
- Request a new access token
  - decode the access token and verify that the JWT profile used is WLCG

Exercise

- Print the group information in the access token
  - if your account does not belong to any group on IAM, request to be part of the `dev` group
    - IAM admins will accept your request
  - add the `wlcg.groups` scope to your Client through the IAM dashboard
  - update the local Client configuration by repeating the OAuth authZ flow
  - request a new access token by specifying the `wlcg.groups` scope
    - check it contains the group(s) to which you belong

If we have time

- Request to be part of the `dev/optional` group (optional group)
  - request a new access token by specifying the `wlcg.groups:/dev/optional` scope
    - check if it contains the optional group

Solution

- Register an oidc-agent Client

  $ eval $(oidc-agent)
  $ oidc-gen -w device test-client

  - check the local oidc-agent configuration

    $ oidc-add -p test-client

- Request an access token

  $ oidc-token test-client | cut -d. -f2 | base64 -d 2>/dev/null | jq

  There is no claim related to the `WLCG` profile, so the JWT profile used is the default one → `IAM`

Solution

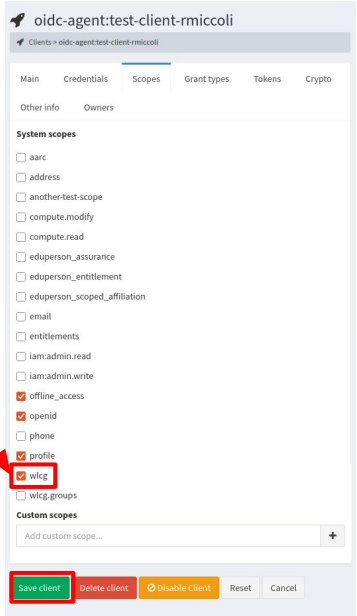
- Choose the WLCG JWT profile for your Client
  - After an admin has given you ownership of your client*, add the `wlcg` scope to your Client through the IAM dashboard
  - Update the local Client configuration by repeating the OAuth authZ flow

```
$ oidc-gen -m -w device test-client
```

- Request a new access token

```
$ oidc-token test-client | cut -d. -f2 | base64 -d 2>/dev/null | jq
```

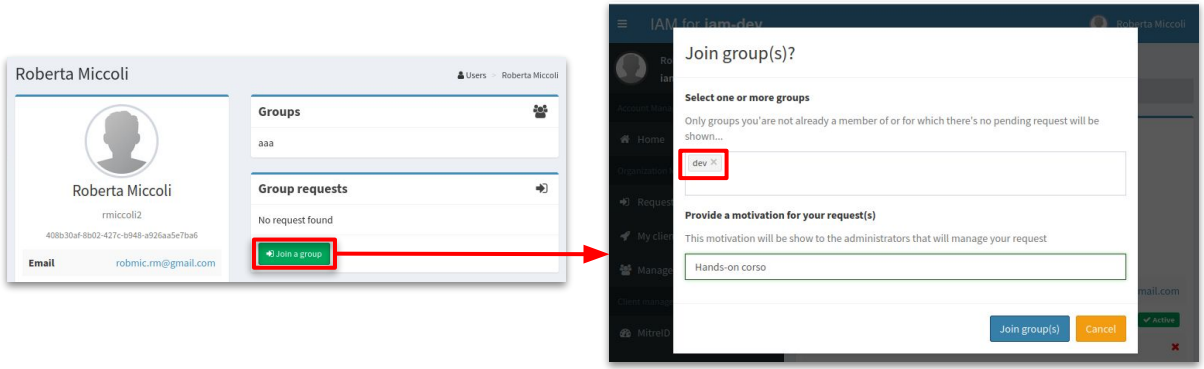
You should see now some wlcg-related claims, e.g., **`wlcg.ver`**



*The oidc-agent client is NOT automatically assigned to the user who approved it, so it will NOT be visible on the dashboard unless an admin assigns it manually. **This feature will be available in the next IAM release!**

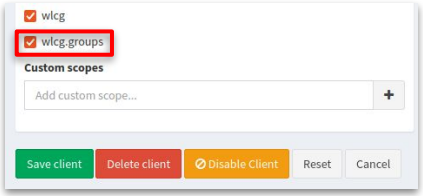
Solution

- Print the group information in the access token
  - request to be part of the `dev` group
    - IAM admins will accept your request



Solution

- Print the group information in the access token
  - add the `wlcg.groups` scope to your Client through the IAM dashboard



  - update the local Client configuration by repeating the OAuth authZ flow

```
$ oidc-gen -m -w device test-client
...
Scopes or 'max' (space separated) [openid profile offline_access]: wlcg.groups
```

Solution

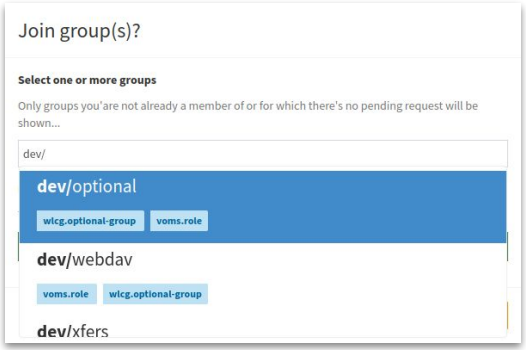
- Print the group information in the access token
  - request a new access token by specifying the `wlcg.groups` scope

```
$ oidc-token -s wlcg.groups test-client |  cut -d. -f2 | base64 -d 2>/dev/null | jq
```

You should get now the group information, e.g., **`"wlcg.groups": [ "/dev" ]`**

Solution

- Request to be part of the `dev/optional` group (optional group)
  - request a new access token by specifying the `wlcg.groups:/dev/optional` scope
    - check if it contains the optional group




```
$ oidc-token -s wlcg.groups:/dev/optional test-client |
cut -d. -f2 | base64 -d 2>/dev/null | jq
```

In the AT you should get

```
"wlcg.groups": [ "/dev/optional", "/dev" ]
```