The problem

https://jira.skatelescope.org/browse/SP-2859

My proposal at IVOA

The CADC Storage Inventory has the need to query a service to know which groups a user belongs to.
The auth-token released through IAM contains the ISS (issuer) field and my idea was to call the introspection endpoint to obtain info about user's groups membership (iss is not the right field, but we fix the iam endpoint):

curl -H "Content-Type: application/x-www-form-urlencoded" -u ${CLIENT_ID}:${CLIENT_SECRET} -d "token=${ACCESS_TOKEN}" https://iam-escape.cloud.cnaf.infn.it/introspect | jq '.'

My documentation source is
https://agenda.infn.it/event/20847/contributions/108730/attachments/69792/86836/IAM-corso-big-data.pdf
Pages 85-88-89

Authorization code flow

EOSC-hub

INFN
Istituto Nazionale di Fisica Nucleare

index / iam-test-web

Hi Enrico Vianello

This is the **/shared** section of this demo website.

You're now logged in as: **vianello**

This application has received the following information:

Copy your access token

- access_token (JWT):

eyJraWQiOiJyc2ExIiwiYWxnIjoiUlMyNTYifQ.eyJzdWIiOiJlMzM3MzU0My05NDM2LTQ1MGUtOTFiZi00MzlmM2VhMTg2MjliLCJpc3MiOiJodHRwczpcL1wvaWFtLWRlb

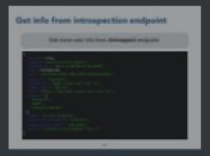
- access_token (decoded):


```
{
  "sub": "e3373543-9436-450e-91bf-439f3ea18622",
  "iss": "https://iam-demo.cloud.cnaf.infn.it/",
  "name": "Enrico Vianello",
  "groups": [
    "ibergrid",
    "demo",
    "ibergrid/feudal"
  "email": "enrico.vianello@cnaf.infn.it"
}
```

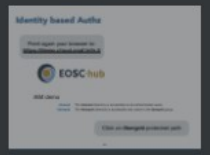

```
$ export ACCESS_TOKEN=[paste your copied token]
```


87

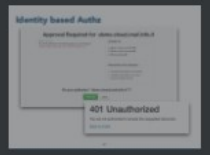
88



89



90



Get info from introspection endpoint

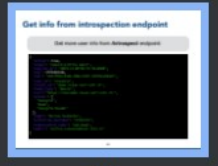
Get more user info from **/introspect** endpoint:

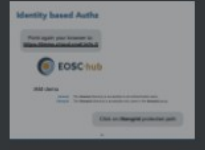
```
$ export CLIENT_ID=[paste your client id]
$ export CLIENT_SECRET=[paste your client secret]
```

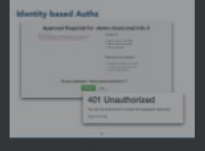
```
$ curl -H "Content-Type: application/x-www-form-urlencoded"
-u ${CLIENT_ID}:${CLIENT_SECRET} -d "token=${ACCESS_TOKEN}"
https://iam-demo.cloud.cnaf.infn.it/introspect | jq '.'
```


87


88


89


90


91

Get info from introspection endpoint

Get more user info from **/introspect** endpoint:


```
{
  "active": true,
  "scope": "openid profile email",
  "expires_at": "2019-12-08T20:25:36+0100",
  "exp": 1575833136,
  "sub": "e3373543-9436-450e-91bf-439f3ea18622",
  "user_id": "vianello",
  "client_id": "demo.cloud.cnaf.infn.it",
  "token_type": "Bearer",
  "iss": "https://iam-demo.cloud.cnaf.infn.it/",
  "groups": [
    "ibergrid",
    "demo",
    "ibergrid/feudal"
  ],
  "name": "Enrico Vianello",
  "preferred_username": "vianello",
  "organisation_name": "iam-demo",
  "email": "enrico.vianello@cnaf.infn.it"
}
```

Public
A aai
E esap
D dios
G general
E esap-ossr-metadata
E esap-interactive-analysis
W wossl
E esap-batch-processing
Direct
G grange
G giaco
dave
K kkliffen
3 dave
sarusso

aai

Hi **bertocco**, First, I think you probably want to know about the person, so the user-info endpoint is probably what you want (rather than the OAuth2 introspection endpoint), although there's nothing to say group-membership info couldn't be provided in the introspection endpoint. Second, your token needs to have the correct scope ("wlcg.groups", IIRC) before the token allows access to group-membership information. Third, (IIRC) ESCAPE IAM is configured to use the WLCG JWT profile. This profile places all the information within the token (assuming offline verification). The profile doesn't guarantee anything about the userinfo endpoint (nor the introspection endpoint, for that matter), so you might be missing group information for that reason. This can be fixed through configuration. Finally, if you want to know which to groups someone belongs, you might be able to use the OIDC-SCIM bridge, which I believe IAM supports.

bertocco 4:25 PM
Thank you for your answer. I thought to use the introspection endpoint on the base of the https://agenda.infn.it/event/20847/contributions/108730/attachments/69792/86836/IAM-corso-big-data.pdf page 89, but I'll try to follow the way you suggest.

bertocco 4:36 PM
If the escape-iam installation supports OIDC-SCIM bridge

Reply *3 replies* *October 24, 2022 4:40 PM*

grange 5:07 PM
(I think it may be useful to actually **paul** so that he gets notified 🙂)

bertocco 5:12 PM
You are right. I forgot it because I keep the chat window open and the notifications disabled 🙂

> If the escape-iam installation supports OIDC-SCIM bridge

G I asked Andrea about SCIM a while ago and he sent me this: https://indigo-iam.github.io/v/v1.7.1/docs/reference/api/scim-api/#get-scimme

Message

Token introspection endpoint

https://www.oauth.com/oauth2-servers/token-introspection-endpoint/

https://datatracker.ietf.org/doc/html/rfc7662