Brookhaven National Laboratory

U.S. DEPARTMENT OF ENERGY

Federated Access and Tokens at BNL SDCC

Presenter(s)

Robert Hancock

Date: March 27 , 2023

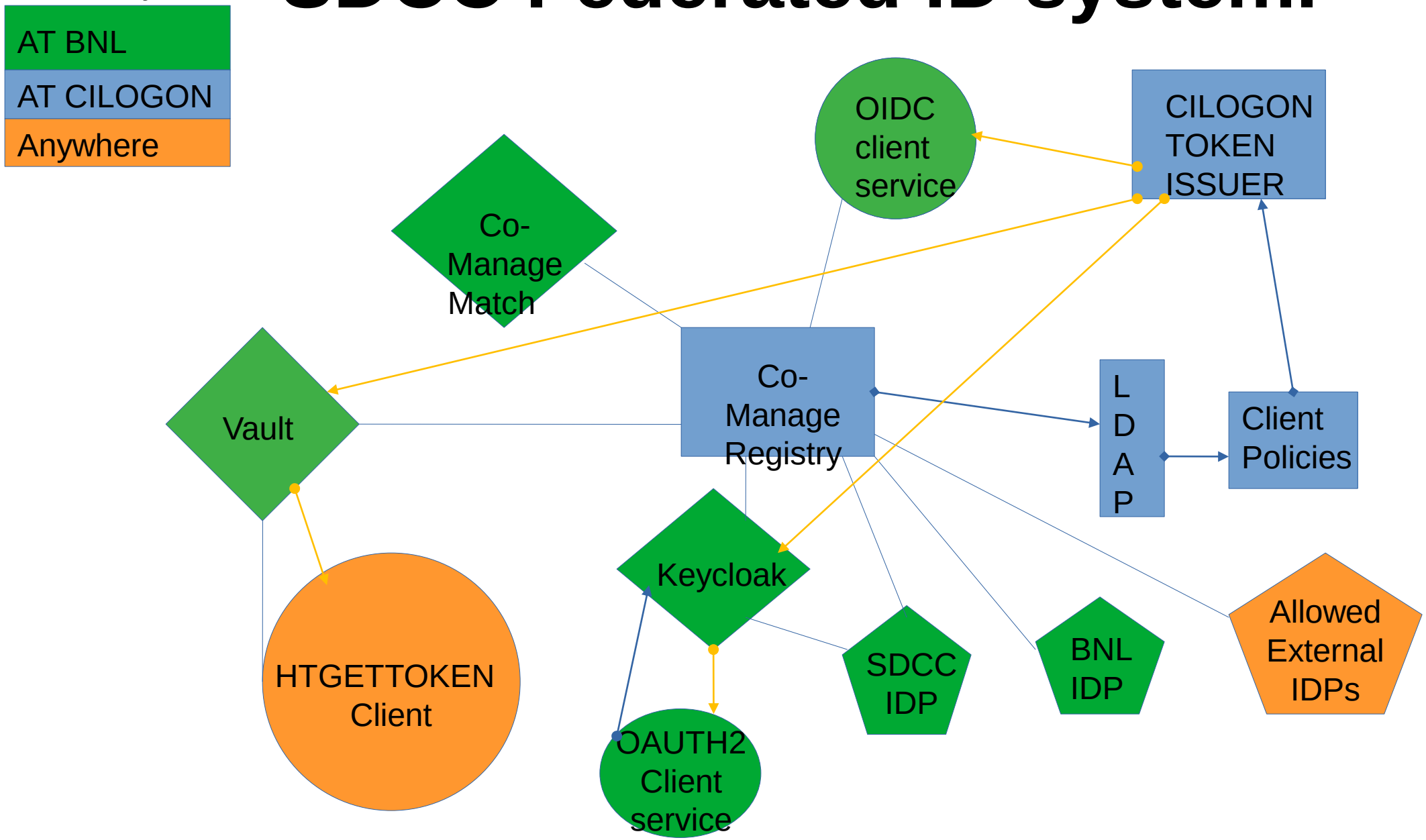
@BrookhavenLab

Driving Force

Why CoManage-Registry:

- Allow access to select SDCC resources without the need for SDCC account
- Allow users to use one set of credentials to access resources across sites
    - Map multiple identities to one central COPerson for a single point of authentication and authorization.
- Why CILogon – strong integration of token issuer with Registry. Outsource labor related to token issuer and IDP management due to staff shortages.

SDCC Federated ID system.



Co-Manage Registry

- COPerson records act as a user store with various attributes. Some are brought from upstream IDPs, others can be manually added or programatically added through APIs
- Organizational Identities are created for each IDP a given person links to their COPerson
- Provides Organizational hierarchy / roles on which authorization decisions can be made.
- Feeds that information to LDAP database used by CILOGON token issuer to generate tokens according to policies.

CILogon

Consent to Attribute Release

harvester-sphnxpro requests access to the following information. If you do not approve this request, do not proceed.

- Your CILogon user identifier

Select an Identity Provider

Brookhaven National Laboratory

Type to search

Brookhaven National Laboratory

Brookhaven National Laboratory - SDCC.BNL.GOV

By selecting "Log On", you agree to the privacy policy.

Brookhaven National Laboratory

Brookhaven National Laboratory

BNL Federated Login

U.S. DEPARTMENT OF ENERGY

set (CILogon = CILogon facilitates secure access to CyberInfrastructure (CI).)
You have been redirected to this site by **CILogon**
Why am I here?

Login to CILogon

Username *

[redacted]

Enter your BNL domain account username.

Password *

••••••••••••••

Enter the password that accompanies your username.

Login

For Assistance

If you are experiencing problems, or if you think your account may be

NOTICE TO USERS:

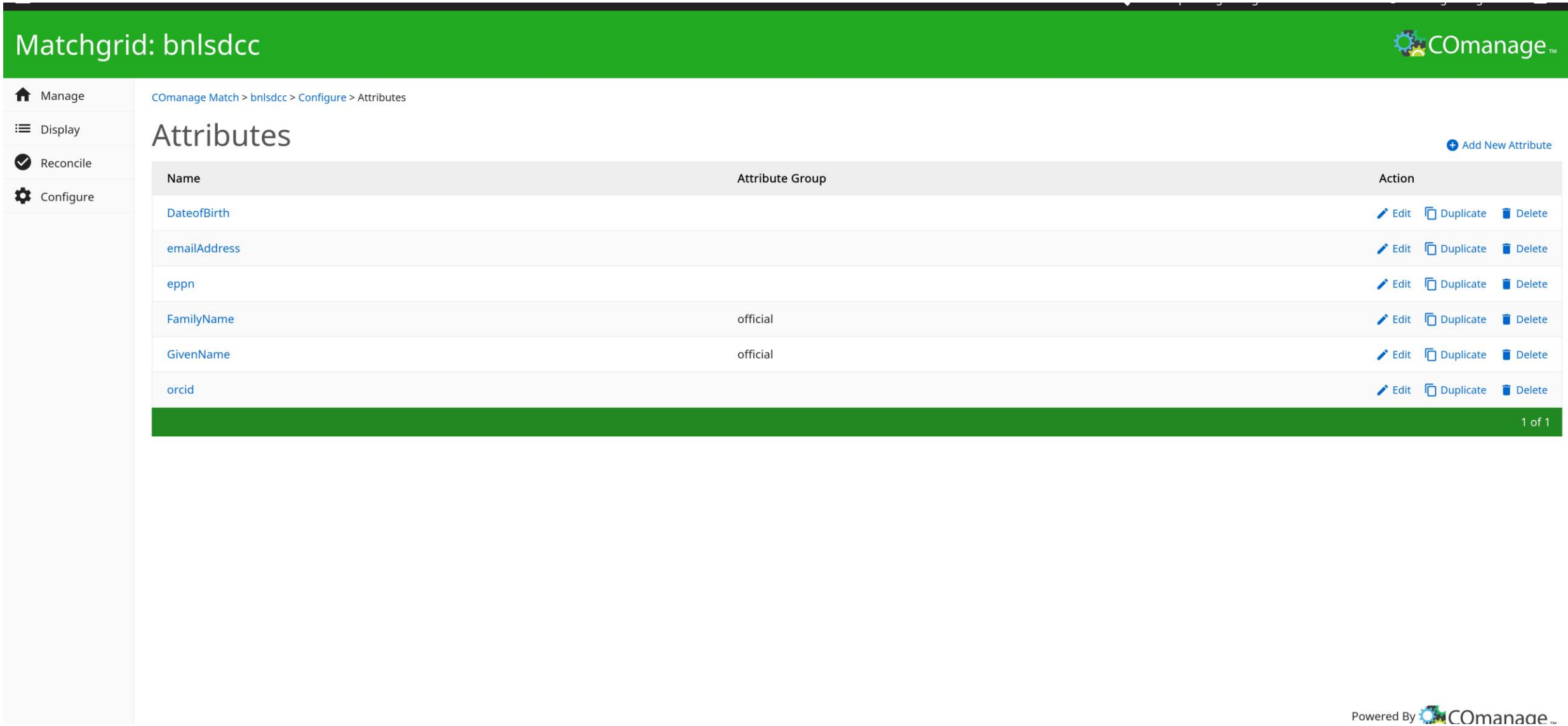
This is a Federal computer system (and/or it is directly connected to a BNL local network system) and is the property of the United States Government. It is for authorized use only. Users (authorized or unauthorized) have no explicit or implicit expectation of privacy.

Any or all uses of this system and all files on this system may be intercepted, monitored, recorded, copied, audited, inspected, and disclosed to authorized site, Department of Energy, and law enforcement personnel, as well as authorized officials of other agencies, both domestic and foreign. By using this system, the user consents to such interception, monitoring, recording, copying, auditing, inspection, and disclosure at the discretion of authorized site or Department of Energy personnel.

Unauthorized or improper use of this system may result in administrative disciplinary action and civil and criminal penalties. By continuing to use this system you indicate your awareness of and consent to these terms and conditions of use. LOG OFF IMMEDIATELY if you do not

Co-Manage Match

- Connected to Co-Manage Registry with api user and key.
- Registry sends requests that contain email, ePPN, and if present, orcid.
- Match is configured with rules that try to match attributes
- If an existing record in Match matches, it returns a match reference which is used by Registry to detect duplicates
- If there is no Match, a new record is created and its match reference is returned which won’t match any in Registry



Brookhaven National Laboratory

Matchgrid: bnlsdcc

COmanage

- Manage
- Display
- Reconcile
- Configure

COmanage Match > bnlsdcc > Configure > Rules

Rules

Add New Rule

Name	Confidence Mode	Order	Action
Canonical Exact Eppn	Canonical	1	Edit Duplicate Rule Attributes Delete
Canonical Exact email	Canonical	2	Edit Duplicate Rule Attributes Delete
Canonical Exact orcid	Canonical	3	Edit Duplicate Rule Attributes Delete

1 of 1

Brookhaven National Laboratory

Keycloak

- Open source identity and Access Management system
- Has many different uses but in this case act as OAUTH2 provider and translates those requests to OIDC.
- Uses user federation connection to IPA to allows local service logins against SDCC IDP.

Vault Server

- Keeps the secret keys and acts as a variety of OIDC clients.
- Serves as a secure long duration refresh token storage
- Works in concert with htgettoken command line program
- Normal Flow: User runs htgettoken with switches to indicate a preconfigured issuer (OIDC client) profile in vault. Other switches can specify scopes and audiences to request.
- Vault server acts a proxy and reaches out to token issuer (CILOGON here) and access and refresh tokens, securely storing the refresh token while returning an access token and a “vault” token to the client. Vault token used to get more access tokens.

```
ocalhost ~]$ htgettoken -a https://v                    gov -i atlas-dcqos
Attempting to get token from https://v                    00 ... failed
Attempting kerberos auth with htt                    bnl    v:8200 ... failed
Attempting OIDC authentication with                    bnl    .8200

Complete the authentication at:
    https://cilogon.org/authorize?client_id=c                    e_challenge=osNPBoCBNyMcz8g45KO3qv0
5eorXCbpbXtV3B9PZLCw&code_challenge_method=S256&nonce=n_VBNceNv0qpwJGyLtYbEG&redirect_uri=h                    ault.sdcc.bnl.gov%3A8200%2Fv1%2Faut
                    2Fcallback&response_type=code&scope=openid+openid+email+profile+org.cilogon.userinfo+storage.read%3A%2F+storage.
create%3A%2F+storage.modify%3A%2F&state=st_6Ulen4VrCqpMforw1FSZ
Running 'xdg-open' on the URL
Waiting for response in web browser
Crash Annotation GraphicsCriticalError: |[0][GFX1-]: Unrecognized feature ACCELERATED_CANVAS2D (t=1.34112) [GFX1-]: Unrecognized feature ACC
ELERATED_CANVAS2D
Storing vault token in /tmp/vt_u1000
Saving credkey to /home/                    /.config/htgettoken/credkey-atlas-dcqos-default
Saving refresh token ... done
Attempting to get token from https://v                    :8200 ... succeeded
Storing bearer token in /run/user/1000/bt_u1000
                    localhost ~]$ httokendecode
{
  "wlcg.ver": "1.0",
  "aud": "https://dcqosdoor.usatlas.bnl.gov",
  "sub": "3e1db22c59                    fc342                    ",
  "nbf": 1679717831,
  "scope": "storage.create:/ storage.read:/ storage.modify:/",
  "iss": "https://cilogon.org/bnlsdcc",
  "exp": 1679721436,
  "iat": 1679717836,
  "jti": "https://cilogon.org/oauth2/5df51c8b7556eed503ea68c4853c84b2?type=accessToken&ts=1679717836230&version=v2.0&lifetime=3600000"
}
```

CILOGON Token Issuer

- Crafts tokens for, or rejects, requests according to defined client policies and information pushed into LDAP from Registry.
- Considers who / what group/roles can request tokens on a specific client as well as token structure (ID tokens, WLCG tokens, SCITOKENS, etc), available scopes / groups.
- When it rejects a token request it redirects the user to a parametric error page at SDCC. This PHP page reads the error type and description as well as a parameter indicating the service the user was trying to reach to generate helpful information on solving whatever problem led to their rejection.

Brookhaven™
National Laboratory

You have been denied access to the Mattermost service because you are not in the MattermostUsers Registry group.

You can check what groups you belong to here:

Show My Registry Groups.

You should be added automatically once the SDCC synchronization script verifies you.

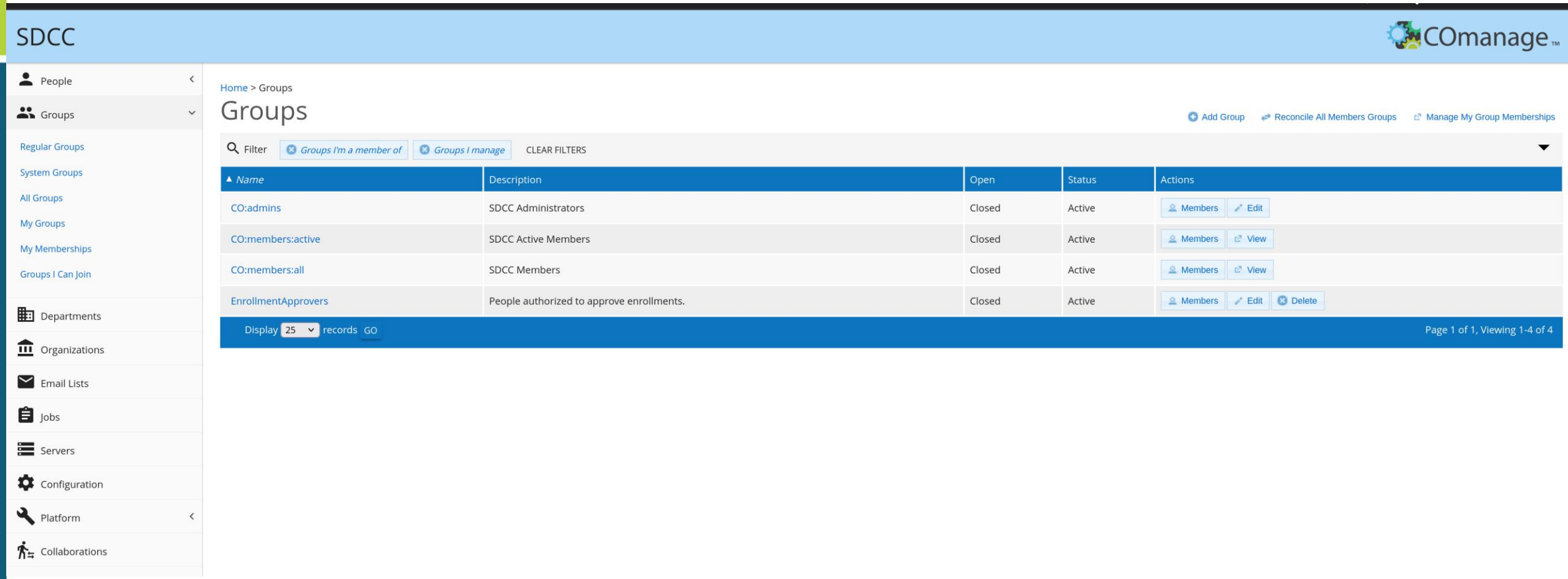
If it has been more than 24 hours since you registered for CoManage-Registry:

Please contact SDCC at RT-RACF-UserAccounts@bnl.gov with the subject "COmanage Authentication for mattermost Attempt Failed"

Please refer to this provided ID number when submitting your request: mattermost641d7f96da093

Error type: access_denied

Error Description: user not in group



Brookhaven National Laboratory

Brookhaven™
National Laboratory

You have been denied access to the Mattermost service because you attempted to log in with an identity that is not registered to CoManage Registry.

If you have never registered with SDCC Registry before, and are authorized to do so, the directions to enroll can be found here.

Enroll in SDCC CoManage Registry

If however, you have an existing SDCC CoManage Registry account, but are trying to log in with an unlinked identity, please follow these directions to link additional accounts

Link additional accounts to existing Registry user

Jupyter Attempt Failed

You attempted to log on to the SDCC COmanage service Jupyter using Comanage-Registry. This attempt failed.

Please contact SDCC at RT-RACF-UserAccounts@bnl.gov with the subject "COmanage Jupyter Attempt Failed"

Please refer to this provided ID number when submitting your request: Jupyter641d810e0e153

Error type: access_denied

Error Description: no user in group found.

Token Enabled Services

- Condor-CE configured to accept WLCG/SCITOKENs issued by:
  - https://cms-auth.web.cern.ch/
  - https://cilogon.org/gm2
  - https://cilogon.org/mu2e
  - https://cilogon.org/bnlsdcc
  - https://cilogon.org/fermilab
  - https://scitokens.org/osg
  - https://scitokens.org/ligo
  - https://chtc.cs.wisc.edu
  - https://zues.phys.uconn.edu
  - https://scicomp.jlab.org/scitokens/eic
  - https://wlcg.could.cnaf.infn.it

Tokens in dCache

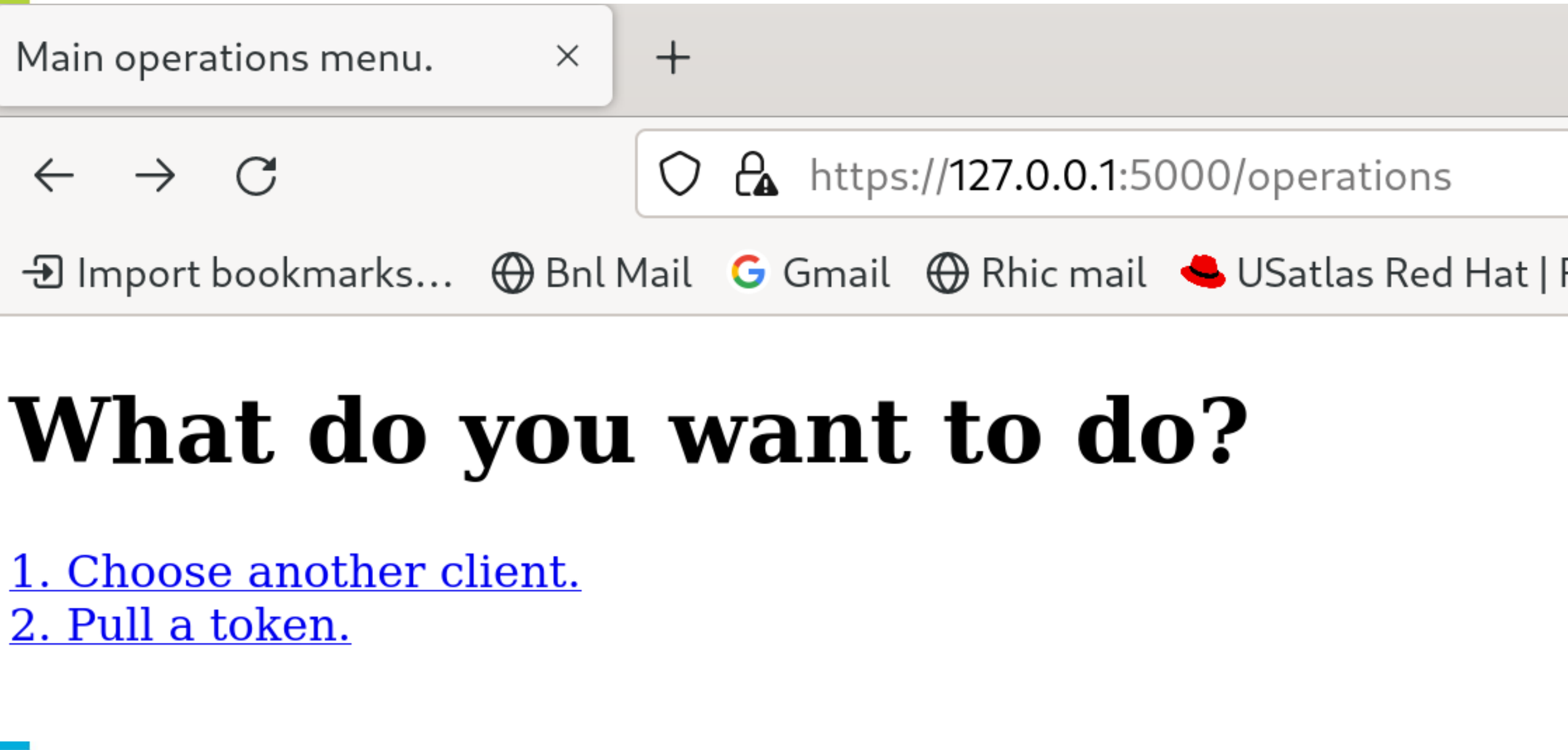
- ATLAS QOS can accept WLCG tokens issued by:
  - https://wlcg.cloud.cnaf.infn.it
  - https://atlas-auth.web.cern.ch
  - https://cilogon.org/bnlsdcc
-

Other services using Tokens

- Mattermost – customized ID tokens issued by:
  - https://cilogon.org/bnlsdcc
- Drupal (various instances) using ID tokens issued by:
  - https://cilogon.org (some still in line to be converted)
  - https://cilogon.org/bnlsdcc
- Zenodo
- Condor (not CE) is not set up for tokens but this effort starts soon.
  - This is expected to use the htgettoken integration with Condor.
- Configuration for S3 token usage is underway. Current model requires using token to get temp access key/secret which is then used to perform operations.

Supporting tools

- Python wrappers around APIs for Mattermost, Keycloak, Co-Manage Registry.
- Scripts that duplicate check against Registry by comparing more fields than Match is configured to consider.
- Scripts that synchronize service identifiers like “mattermostid” between Mattermost/Keycloak/Registry
- Scripts that map Registry Groups to LDAP groups
- OIDC client impersonator(python3) for debugging OIDC / token issues.
  - Keeps a JSON file of OIDC client credentials
  - Local web server that allows requesting tokens by selecting client and scopes.
  - Decodes/displays tokens, reads/displays userinfo endpoint, and logs errors in detail.



What do you want to do?

1. Choose another client.
2. Pull a token.

Select OIDC provider to test.

- ○ "CILOGON_test_shared"
- ○ "CILOGON_prod_dedicated"
- ○ "CILOGON_prod_shared"
- ○ "CILOGON_test_dedicated"
- ○ "Keycloak2CilogonDedicatedSDCCRealm"
- ○ "ExistingTestMattermostCilogon"
- ○ "MatterMostProd"
- ○ "testMattermost2Keycloak2"
- ○ "Keycloak2CilogonDedicatedNewRealm"
- ○ "Mattermost2Keycloak2NewRealm"
- ○ "satosaProdIDP2prodKeycloak"
- ○ "prodKeycloak2ProdCILOGON"
- ○ "atlasTalk2prodkeycloak"
- ○ "harvester-sphnxpro"
- ○ "prodKeycloak2testCILOGON"
- ○ "atlas-dcqos-test"
- ○ "harvester-sphnxpro-test"
- ◉ "atlas-dcqos"

Leave these blank to use default data from config file chosen client. Fill in to override.

Client ID

Client Secret

Save

Use the check boxes below to select appopriate scopes for the test token request.

Do not uncheck openid unless you know what you are doing.

Get Token

"openid"	☑
"profile"	☑
"email"	☑
"org.cilogon.userinfo"	☑
"storage.read:/"	☐
"storage.create:/"	☐
"storage.stage:/"	☐
"storage.modify:/"	☐
"storage.read:/test"	☐
"compute.create"	☐
"compute.cancel"	☐
"compute.read"	☐
"wlcg.groups"	☐
"wlcg.capabilityset"	☐

Check all

Uncheck all

Check CILOGON standard

```
access_token:
  header:
    alg:          "RS256"
    kid:          "968517DD793541FA51CD292D3C4322AF"
    typ:          "JWT"
  payload:
    aud:          "cilogon:/client_id/57703e2084[redacted]"
    exp:          1679733364
    iat:          1679729764
    iss:          "https://cilogon.org/bnlsdcc"
    jti:          "https://cilogon.org/oauth2/539ce231da76ceebd7d9947897af37b7?type=accessToken&ts=167[redacted]rsion=v2.0&life
    nbf:          1679729759
    scope:        "storage.create:/ compute.create storage.read:/ compute.read compute.cancel storage.modify:/"
    sub:          "dd7cdab5d437fcc4aa[redacted]"
    wlcg.ver:     "1.0"
  signature:      "cXhKv-XyZIv1as_7oczEAQqiHWD_p04MvbVuAEdkWro8c9-qieYgjvIZvUvfkyC76jSK6KzW1DX_g1cFQSF5dFLQv_2tmG1QC6h03c6LUoDnA8a
  token:          "eyJ0eXAiOiJKV1QiLCJraWQiOiI5Njg1MTdERDc5[redacted]sImFsZyI6IlJTMjU2In0.eyJ3bGNnLnZlciI6IjE
                  XyZIv1as_7oczEAQqiHWD_p04MvbVuAEdkWro8c9-qieYgjvIZvUvfkyC76jSK6KzW1DX_g1cFQSF5dFLQv_[redacted]
expires_in:       3600
```

```
id_token:
  header:
    alg:            "RS256"
    kid:            "968517DD793541FA51CD292D3C4322AF"
    typ:            "JWT"
  payload:
    acr:            "https://refeds.org/profile/mfa"
    aud:            "cilogon:/client_id/57703e20847055a699[redacted]"
    auth_time:      1679729763
    cert_subject_dn: "/DC=org/DC=cilogon/C=US/O=Brookhaven National Laboratory/CN=Robert Hancock [redacted]"
    email:          "hancock@bnl.gov"
    eppn:           "[redacted]"
    eptid:          "https://idp.bnl.gov/idp/shibboleth!https://cilogon.org/shibboleth![redacted]="
    exp:            1679730664
    family_name:    "Hancock"
    given_name:     "Robert"
    iat:            1679729764
    idp:            "https://idp.bnl.gov/idp/shibboleth"
    idp_name:       "Brookhaven National Laboratory"
    iss:            "https://cilogon.org/bnlsdcc"
    jti:            "https://cilogon.org/oauth2/idToken/594d9c0806fbeb1ced8d04209660b3f/1679729764145"
    name:           "Hancock, Robert"
    sub:            "http://cilogon.org/serverA/users/[redacted]"
  signature:        "M5SjIj8AqXapnorwHVvCUprIx5UAlYInkZzOOQ42IC1T6kAKJearUPOywXIRjtXZQ0tV7O5HndQNf-CKm-bCi4Tuc0frk2OVhE
```

```
refresh_token:      "NB2HI4DTHI[redacted]OFZXXEZZPN5QXK5DIGIXTCODGGY2GEOBZMU4[redacted]JXGIZDCZR7OR4
scope:              "openid profile email org.cilogon.userinfo"
token_type:         "Bearer"
userinfo_endpoint:
  acr:              "https://refeds.org/profile/mfa"
  aud:              "cilogon:/client_id/57703e20847055a69[redacted]"
  cert_subject_dn:  "/DC=org/DC=cilogon/C=US/O=Brookhaven National Laboratory/CN=Robert Hanco[redacted]"
  email:            "hancock@bnl.gov"
  eppn:             [redacted]
  eptid:            "https://idp.bnl.gov/idp/shibboleth!https://cilogon.org/shibboleth![redacted]"
  family_name:      "Hancock"
  given_name:       "Robert"
  idp:              "https://idp.bnl.gov/idp/shibboleth"
  idp_name:         "Brookhaven National Laboratory"
  iss:              "https://cilogon.org/bnlsdcc"
  jti:              "https://cilogon.org/oauth2/idToken/594d9c0806fbeb1ced8d04209660b3f/1679729764145"
  name:             "Hancock, Robert"
  sub:              "http://cilogon.org/serverA/users/[redacted]"
```

The end.

Questions?