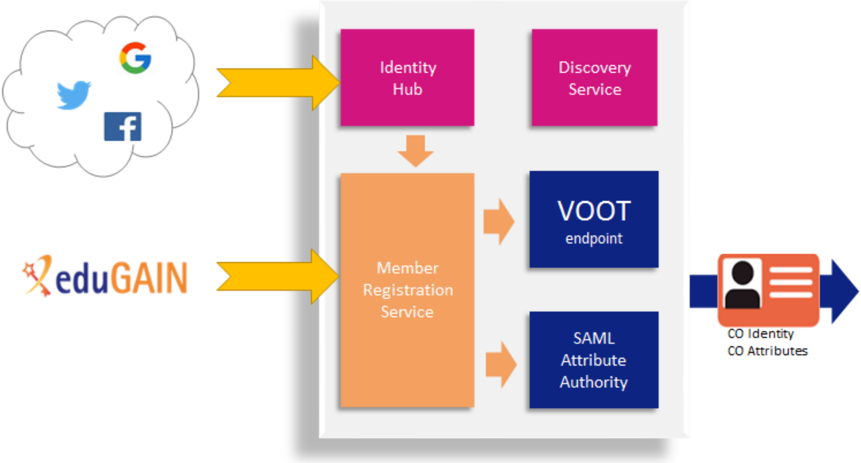
Authentication

Shih, A. Haigron, R. Le Sidaner, P.

IVOA Interop, Santiago 27-29/10/2017

EDUTEAM


eduGAIN
Identity Hub
Discovery Service
Member Registration Service
VOOT endpoint
SAML Attribute Authority
CO Identity
CO Attributes

Eduteams and Geant. . . is it THE solution for IVOA ?

- we met Chris Atherton from GEANT at EPSC in Riga
- He propose us to have look at Eduteam
- *https ://wiki.geant.org/display/gn42jra3/eduTEAMS https ://www.geant.org/Innovation/eduteams/Pages/How-eduTEAMS-works.aspx*
  - Membership management, Identity Hub for non eduGAIN users, Basic Groups, and Basic Provisioning.
  - allows end users of eduGAIN members to be able to login.
  - has infrastructure operation provided by GÉANT.
  - is offered to users at no additional cost.
  - allow multiple ID federation OpenID ...
  - propose to handle group for authorization
  - What time scale for UP and Running solution ?
  - What Advantage in the Non Free solution ?

What we have try to handle syntax and REST method

```
+--------+                       +----------+               +----------+
| VOOT   |                       | VOOT     |               | User     |
| Client +-----------------------+ Provider +---------------+ Group    |
|        | VOOT/OAuth/Basic |             | LDAP/SQL | Directory |
+--------+                       +----------+               +----------+
```

- REST API to access people and group info
  - Accessing group info for user lesidaner
    https ://auth.obspm.fr/groups/lesidaner

  -
    ```
    { "totalResults" : 1,
        "entry" : [
            {
                "description" : "Group for test",
                "id" : "testgroup"
            }
        ]
    }
    ```

What we have try to handle syntax and REST method

- REST API to access group info
  - Accessing all user for the group where lesidaner is member https ://auth.obspm.fr/peoples/lesidaner/testgroup

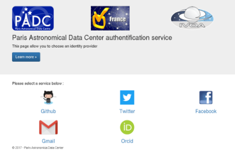
```
"entry" : [
        {
            "displayname" : "null",
            "mail" : [
                "jas01_11524096github_fake"
            ]
        },
        {
            "displayname" : "null",
            "mail" : [
                "0000-0001-9629-2922orcid_fake"
            ]
        },
    ]
"totalResults" : 2
```

Using topcat and DaCHS

- We have a internal tap server (not open to all internet) `http://voparis-jpl.obspm.fr/tap`
- We don't want to modify this application.
- We put a LDAP authenticate proxy in the front of that server.
  https ://voparis-srv-paris.obspm.fr/ivoa/
- It ask for user and password taken from integrated SSO.
  https ://auth.obspm.fr/

Using topcat and DaCHS

- Authentication



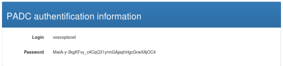
Paris Astronomical Data Center authentification service

This page allow you to choose an identity provider

Please select a service below :

© 2017 - Paris Astronomica Data Center

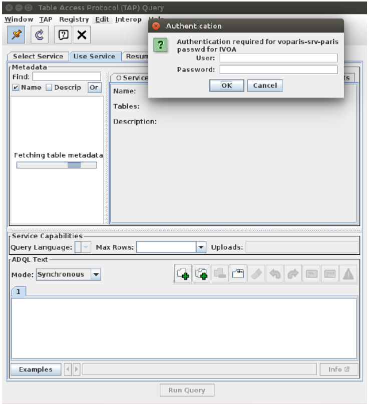
- Password



PADC authentification information

Login	voexoplanet
Password	MwiA-y-3kgKFvy_c4CqQ31yrmGAjaqhHgcGrwXAjOC4

- Login in tap



Fetching table metadata

Authentication

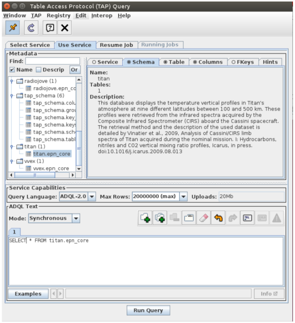
Authentication required for voparis-srv-paris passwd for IVOA

User:

Password:

Using topcat and DaCHS

- Select



Find:

☑ Name □ Descrip Or

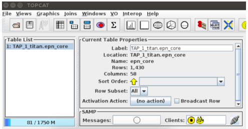
Name:
titan
Tables:
1
Description:
This database displays the temperature vertical profiles in Titan's atmosphere at nine different latitudes between 100 and 500 km. These profiles were retrieved from the infrared spectra acquired by the Composite Infrared Spectrometer (CIRS) aboard the Cassini spacecraft. The retrieval method and the description of the used dataset is detailed by Vinatier et al., 2009, Analysis of Cassini/CIRS limb spectra of Titan acquired during the nominal mission. I: Hydrocarbons, nitriles and CO2 vertical mixing ratio profiles, Icarus, in press. doi:10.1016/j.icarus.2009.08.013

Query Language: ADQL-2.0 Max Rows: 20000000 (max) Uploads: 20Mb

Mode: Synchronous

```
SELECT * FROM titan.epn_core
```

- Select



1: TAP_1_titan.epn_core

Label: TAP_1_titan.epn_core
Location: TAP_1_titan.epn_core
Name: epn_core
Rows: 1,430
Columns: 58
Sort Order:
Row Subset: All
Activation Action: (no action) □ Broadcast Row
Messages: Clients:

- Display

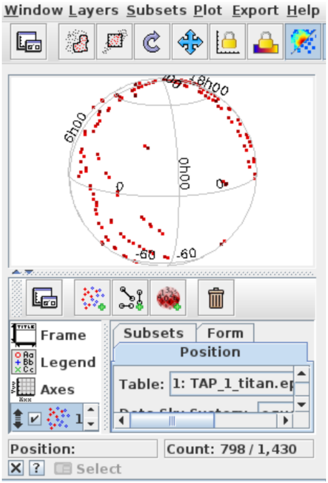


Table: 1: TAP_1_titan.ep

Position:

Count: 798 / 1,430

Conclusion

Does IVOA want a central Annuary ?

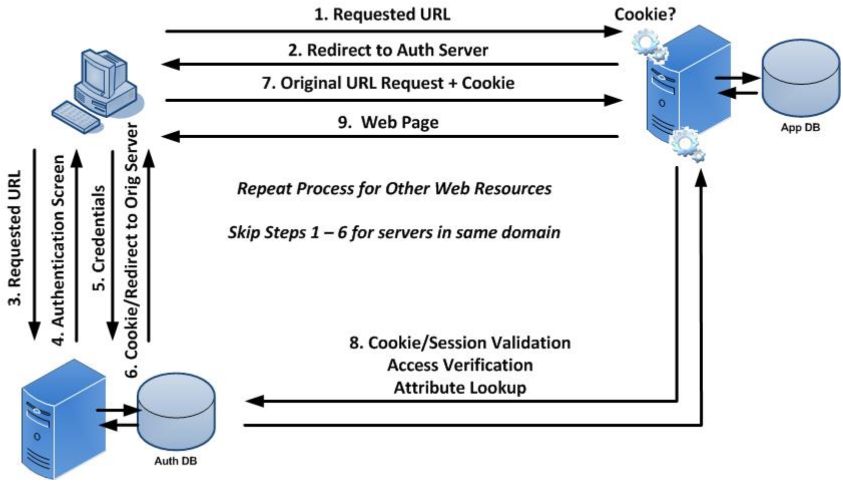
- separate Authentication between federation and application
- use LDAP like and delegate group administration VOOT ?
- have a centralised Authorisation system with delegation
- What link with large project CTA, SKA ....

Then make convergence and delegation for next interop ?

What we have try to handle last time

- Don’t want to manage people (no account creation no passwd management).
- Ability to authenticate non web application like `ssh/rsync also Aladin Topcat`.
- Ability to authenticate existent applications.
- Ability to manage easily authorizations.
- Easy to integrated in new applications **and old** applications.
- Easy to deploy.
- Easy to maintain with few manpower.
- Secure.

How SSO works


1. Requested URL
Cookie?
2. Redirect to Auth Server
7. Original URL Request + Cookie
9. Web Page
App DB
3. Requested URL
4. Authentication Screen
5. Credentials
6. Cookie/Redirect to Orig Server
Repeat Process for Other Web Resources
Skip Steps 1 – 6 for servers in same domain
8. Cookie/Session Validation
Access Verification
Attribute Lookup
Auth DB

Problems

- Highly based on `http-redirect`, don't work well outside web-browser.
- Hard to use on CLI (`ssh`, etc.)
- Lots of implementation : SAML2 (shibboleth), oauth, openid, etc.
- Complex to very complex to integrate.
- Don't integrate authorizations, each application must manage it own authorizations, meaning each application provider must implement his own tools.

LDAP

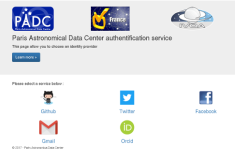
- Why
  - Use LDAP for authentication beckoned over ID Federation.
  - LDAP is well documented protocol.
  - All (almost) application can easily to use LDAP as authentication back-end.
  - Easy to use on CLI.
  - LDAP as « group » notion. Use LDAP group as authorizations back-end.
  - Easy to centralize.
- But
  - Don't want to populate the LDAP.
  - Don't want to manage expiration.

LDAP+SSO

- Using SSO
- Populate a LDAP

Prototype

- User ask to choose a authentication service (like OrcId, Google, Github, Facebook etc.)



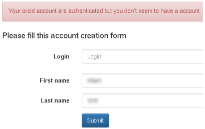
Paris Astronomical Data Center authentification service

This page allow you to choose an identity provider

Please select a service below :

© 2017 - Paris Astronomica Data Center

- If he don’t have a account, we invite him to create one.

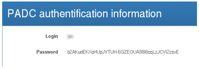


Your orcid account are authenticated but you don't seem to have a account

Please fill this account creation form

Login	Login
First name	[redacted]
Last name	[redacted]

- We generate a temporary password and add it to a LDAP



PADC authentification information

Login	[redacted]
Password	b2AKudEKXcHUpJYTUH-6GZEOUA98I8cqLzJCVI2zcvE

Prototype

- Use this couple login/password in all your applications.
- The password is temporary same as the TTL of a cookie any web application.
- All providers can use this LDAP authentication.

Authorizations

- Easy to manage authorizations
- Create group (in LDAP) like `cn=myapplication, ou=groups, dc=padc, dc=fr, dc=ivoa`
- Authorizations with *memberOf* test.
- For example :
  - Apache : `Require ldap-group myapplication`
  - Pam : `pam_filter |(member=cn=myapplication,ou=groups,dc=padc,dc=fr`
  - sshd : `Allowgroups` and `ldap.conf`

The future

- Accounts convergences :
  - Peoples who have multiple account
  - Peoples who change institution.
- Create Authorizations service.
- Delegation by branch in the LDAP.
- Delegation of the authorizations services.
- Add SAMLv2 (Shibboleth/Edugain).