

# Cookie Authentication and VOSI Capabilities/securityMethods

Juan González-Núñez, J. Salgado, R. Gutiérrez-Sánchez, JC. Segovia, J. Duran, E. Racero, M. Marcos, D. Baines, A. Mora, J. Bakker, B. Merín, C. Arviset

ESAC Science Data Centre (ESDC) - ESA



ESA UNCLASSIFIED - For Official Use

# Topcat TAP11c & TAP+ auth

- Test of M. Taylor proposal in Paris 2019 Interop
- https://wiki.ivoa.net/internal/IVOA/InterOpMay2019DAL/tap11b.pdf
  - 11c TOPCAT with early implementation of Authentication
    - ftp://andromeda.star.bris.ac.uk/pub/star/topcat/pre/topcatfull\_tap11c.jar
  - ESA Gaia archive with extended /capabilities response

### The set of th

•

# Topcat TAP11c & TAP+ auth

- Retrieved archive session cookie:
  - curl -k -c cookies.txt -X POST -d username=USERNAME -d password=PASSWORD -L "https://#URL#/tap-server/login"
- Open Topcat and select 'VO->Table Acces Protocol (TAP) Query'.
- Select 'Select Service' tab, use 'https://#URL#/tap-server/tap' in 'TAP URL' textbox, select 'cookie' as authentication method.
- select 'data' and put the cookie we have retrieved using curl: JSESSIONID=xxxx

••	Table Access Protocol (TAP) Query
🖋 🕲 🗶	
Select Service	Use Service Resume Job Running Jobs
	Ose service Resume Job Ruinning Jobs
Metadata	
Find:	
✓ Name Descrip Or	Name: user_jgonza01
user_earlydr2 (17)	Tables:
user_fullgdr1 (19)	16
<ul> <li>user_ishih (4)</li> <li>user_iduran (7)</li> </ul>	Description:
v iser_jouran (7)	
user_jgonza01.cepheids_	
user_jgonza01.cepheids_	
user_jgonza01.t1477130	
III user_jgonza01.table1	
📼 usar iganza01 tabla fails	
	0
Service Capabilities	
Query Language: ADQL-2.0 ᅌ	Max Rows: 3000000 (default) 🗘 Uploads: 100Mb
ADQL Text	
Mode: Synchronous ᅌ	
	1
Examples	Info 🗷
	Run Query

# Some conclusions

- It works! Access to
  - general public archive data (DRx, external catalogues, etc)
  - User space data
  - Shared data from other users/groups
- Access process could be streamlined by extending the provision of metadata in /capabilities response
- We should indicate tools **how** to obtain the session cookie

### · = ■ ► = = + ■ + ■ = ≝ = ■ ■ ■ = = = ■ ■ ■ ■ ■ = ₩ = |

-<interface role="std" xsi:type="vs:ParamHTTP">
 <accessURL use="base">https:/#URL#/tap-server/tap</accessURL>
 -<securityMethod standardID="ivo://ivoa.net/sso#cookie">
 <accessURL use="base">https://#URL#/tap-server/tap</accessURL>
 <accessURL use="base">https://#URL#/tap-server/tap</accessURL>
 <accessURL use="base">https://#URL#/tap-server/login
- <securityMethod standardID="ivo://ivoa.net/sso#cookie">
 <accessURL use="base">https://#URL#/tap-server/login</accessURL>
 </accessURLs
 <accessURL use="base">securityMethod standardID="ivo://ivoa.net/sso#cookie">
 <accessURL use="base">securityMethod standardID="ivo://ivoa.net/sso#cookie">securityMethod</accessURL>
 <a classURL use="base">securityMethod="base">securityMethod standardID="ivo://ivoa.net/sso#cookie">securityMethod="base">securityMethod="base">securityMethod="base">securityMethod="base">securityMethod="base">securityMethod="base"/securityMethod">securityMethod="base"/securityMethod">securityMethod="base"/securityMethod></accessURL>
 <a classURL use="base">securityMethod</a>

</interface>

-<interface role="std" xsi:type="vs:ParamHTTP">

<accessURL use="base">https:/#URL#/tap-server/tap</accessURL>

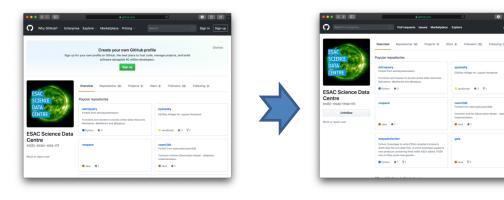
-<securityMethod standardID="ivo://ivoa.net/sso#cookie">

> <param id="url" ucd="meta.ref.url" utype="Access.reference">https://#URL#/tap-server/login</param>
 <param id="method" ucd="meta.ref.method" utype="Request.method">POST</param>
 <param id="user" ucd="login.name" utype="Request.param">username</param>
 <param id="pwd" ucd="login.name" utype="Request.param">username</param>
 <param id="pwd" ucd="login.password" utype="Request.param">password</param>
 <param id="cookie" ucd="login.cookie" type="Response.cookie">JSESSIONID</param>
 </param>
 </param>
 </param id="cookie" ucd="login.cookie" type="Response.cookie">JSESSIONID</param>
 </param>
 </param>
 </param>
 </param id="cookie" ucd="login.cookie" type="Response.cookie">JSESSIONID</param>
 </param>
 </param>
 </param>
 </param>
 </param>
 </param>
 </param id="cookie" ucd="login.cookie" type="Response.cookie">JSESSIONID</param>
 </param>
 </param>
 </param>
 </param>
 </param>
 </param>
 </param>
 </param id="cookie" ucd="login.cookie" type="Response.cookie">JSESSIONID</param>
 </param>
 </param>
 </param>
 </param>
 </param>
 </param>
 </param id="cookie" ucd="login.cookie" type="Response.cookie">JSESSIONID</param>
 </param>
 </param>

</interface>

# Separate login URL?

- In a general case, a single service may need to serve
  - Public data
  - Private or Proprietary data with complex sharing/grouping
  - Functionalities in the service that may change according to the user
- We could force users to authenticate for any URL invocation and not serve data (even public) to unauthenticated users
  - But that is certainly not very open 🔅
- What about 2 separate URLs, one for public, another enforcing authentication?



				Jump	1	learch	
NOA .	TWRI > NOA	Web > IvoaEv	ents > InterOpOct2019 > InterOp	Oct2019DAL (2019-10-10, M	rcoMolinars)	C Edit Attach	
Log In or Register IVOA.net With Home WebChanges WebThoeic Ist	DAL sessi Meeting		dule - IVOA October	2019 Groningen	Interop	perability	
Web/Statistics			Data Access Incleme			_	
Twiki Meta & Help INOA Know Main Santbox TWiki	Friday October 11, 15:30-17:00, DOT						
	Speaker		Title	1.00, 001	The	e Material	
	William W. (Trey)	Roby	TAP and Datalink features in Fi	αfv	27	pdf / key	
	Simon O'Toole The Data Central Cone Search Service, powered by pyVO			of 8C8 15			
	Tamara Civera & Javier Hernández VO implementation at Observatorio Astrofisico de Javalambre						
	Francois Bonnami Prov/TAP & Prov/HPS				207		
TAVA Hon	Ole Streicher		ProvSAP and W3C compatibility		15		
TWRI tutorial			discussion buffer		5		
User registration Notify me Workling Groups	DAL & GWS joint session						
Data Access Data Model			NIAuthZ next steps & caproles d				
CARS MODEL	Saturday October 12, 09:00-10:30, Student hotel						
Query Language	Speaker Title Time Mate			Material			
Registry	Brian Major	GMS status		15			
Stds&Procs Semantics	Brian Major	YouCat & TA		15'			
Semantics /OTable	Markus Demieltner Interoperable Authentication: Lessons learned from pyVO's TAP client 15'						
Applications	Juan Gonzalez Cookie authentication for the Gaia Archive 15'						
Interest Groups		Discussion of	n caproles	30			



0 6 0

A +- 🔤

- Spec already covers the need for one single URL with anonymous + authenticated support
- Standard practice to offer public, unauthenticated services + authenticated capabilities after login without URL change
  - Eg. GitHUB or IVOA Wiki

•

### · = ■ ► = = + ■ + ■ = ≝ = ■ ■ ■ = = = ■ ■ ■ ■ = = = ■ ₩ · ■

-<interface role="std" xsi:type="vs:ParamHTTP">

<accessURL use="base">https:/#URL#/tap-server/tap</accessURL>

-<securityMethod standardID="ivo://ivoa.net/sso#cookie">

> <param id="url" ucd="meta.ref.url" utype="Access.reference">https://#URL#/tap-server/login</param>
 <param id="method" ucd="meta.ref.method" utype="Request.method">POST</param>
 <param id="user" ucd="login.name" utype="Request.param">username</param>
 <param id="pwd" ucd="login.name" utype="Request.param">username</param>
 <param id="pwd" ucd="login.password" utype="Request.param">password</param>
 <param id="cookie" ucd="login.cookie" type="Response.cookie">JSESSIONID</param>
 </param>
 </param>
 </param id="cookie" ucd="login.cookie" type="Response.cookie">JSESSIONID</param>
 </param>
 </param>
 </param>
 </param id="cookie" ucd="login.cookie" type="Response.cookie">JSESSIONID</param>
 </param>
 </param>
 </param>
 </param>
 </param>
 </param>
 </param id="cookie" ucd="login.cookie" type="Response.cookie">JSESSIONID</param>
 </param>
 </param>
 </param>
 </param>
 </param>
 </param>
 </param>
 </param id="cookie" ucd="login.cookie" type="Response.cookie">JSESSIONID</param>
 </param>
 </param>
 </param>
 </param>
 </param>
 </param>
 </param id="cookie" ucd="login.cookie" type="Response.cookie">JSESSIONID</param>
 </param>
 </param>

</interface>

-<interface role="std" xsi:type="vs:ParamHTTP">

<accessURL use="base">https:/#URL#/tap-server/tap</accessURL>

-<securityMethod standardID="ivo://ivoa.net/sso#cookie">

> <param id="url" ucd="meta.ref.url" utype="Access.reference">https://#URL#/tap-server/login</param>
 <param id="method" ucd="meta.ref.method" utype="Request.method">POST</param>
 <param id="user" ucd="login.name" utype="Request.param">username</param>
 <param id="pwd" ucd="login.password" utype="Request.param">password</param>
 <param id="cookie" ucd="login.cookie" type="Response.cookie">JSESSIONID</param>
 </securityMethod>

</interface>

### \_ = !! ▶ :: ■ + !! ■ = !! !! = = ∷ = !! ₩ ₩ ₩ ₩

# Capabilities after authentication

- Several capabilities metadata may changes **after** authentication
  - Service limits?
    - retentionPeriod, executionDuration, outputLimit, uploadLimit
  - Additional query languages?
    - eg. posiblity to send native SQL queries for power users/admins
  - Further output formats?
- Declaration of the need to **reload** capabilities after authentication by implementing tools?

### \_ II ▶ == + II **=** ≝ \_ II II = = = M II = II = II ₩ ⊨

•

### Questions / Discussion



**European Space Agency**