data central

Access Control with All The Protocols

Dr Simon O'Toole – AAO-Macquarie

The structure of Data Central

- Main web portal (incl. Cone Search, Image Access)
- Documentation portal
- Accounts portal
- Cloud portal
- WebDAV access
- TAP service
- Connections to other (external) ASVO nodes

External Services

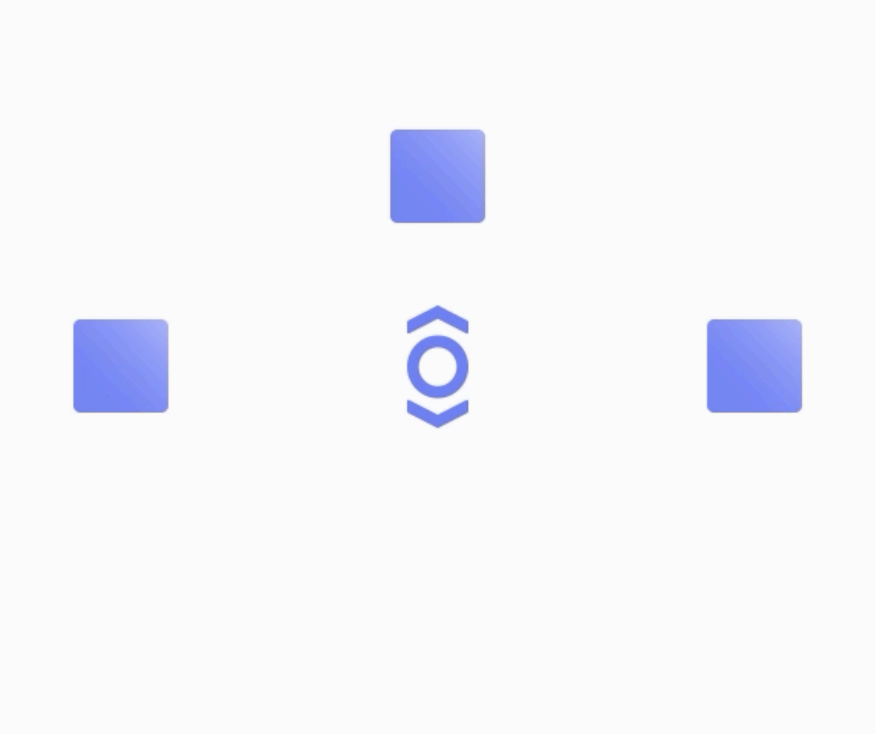
- SkyMapper ASVO
- Theoretical Astrophysical Observatory (TAO) ASVO
- MWA ASVO
- CASDA ASVO
- Any other interested archives/systems

How do we connect all internal and external services?

- Users want Single Sign On
- Bare minimum: Minimise different accounts and passwords

Solution #1 (from Nov 2018)

- Single Sign-On using OAuth 2.0 & Open ID Connect
- Identified ORY/Hydra as lightweight Identity Provider system (https://www.ory.sh)
- Allows straightforward integration with your existing local IDP
- Runs in Docker



Solution #2

- Single Sign-On using OAuth 2.0 & Open ID Connect
- Apereo CAS (Central Authentication Service) offers OAuth2.0 endpoints
- Also allows straightforward integration with your existing local IDP (LDAP, X.509, database, Radius, etc)
- Runs in Docker

Central Authentication Service

- Uses the CAS protocol https://apereo.github.io/cas/5.3.x/protocol/CAS-Protocol-Specification.html
- Implemented using https://apereo.github.io/cas/
- Uses a ticket based system
- Used primarily in academic systems
- Currently not part of IVOA SSO standard
    - *Proposal: add to list of approved authentication mechanisms*

CAS at Data Central

- What our CAS service provides:
    - CAS (in production)
    - OAuth2.0 (ready for production)
    - SAML 2.0 (ready for testing)
    - Basic HTTP (in development)
    - JSON Web Tokens (in development)
- What it does not provide, but could if required:
    - Multi-factor authentication
    - Delegated authentication – i.e. system could act as a OAuth/SAML client

Status

- Internal Data Central apps with CAS SSO:
  - main web: LIVE
  - documentation: LIVE
  - accounts: LIVE
  - cloud: IN TESTING
  - webDAV: IN TESTING
  - TAP: TO COME
- Data Central SSO pilot with SkyMapper ASVO using OAuth2.0

  ➡ Live at next public web app release
- Next steps: testing then implement at TAO ASVO

IVOA services

- Web-based systems: ✅
- Applications (e.g. TOPCAT, Aladin): ❌
    - HOWEVER: Primary use case for Basic HTTP Authentication integration
    - Can SSO be integrated?

Astronomical Data Archives workshop

August 5-8, 2019 in Sydney – register here http://bit.ly/data-archives-2019

Themes:

- Exploring different technologies for storage and querying (SQL, noSQL, Hadoop, Elasticsearch, etc, what works and what doesn't)
- Beyond Data Storage (What services should archives offer and what do they currently?)
- Interoperability (incl. IVOA)
- Tools (incl. access control and code-to-the-data)
- User Interfaces and User Experience
- Hardware (incl. cloud vs hosted vs hybrid)