Authentication & Authorization at the Canadian Astronomy Data Centre

A Technical Overview

Brian Major

January 2019

CADC - Service Oriented Architecture

REST APIs to all CADC functionality

Willing to interact with any client

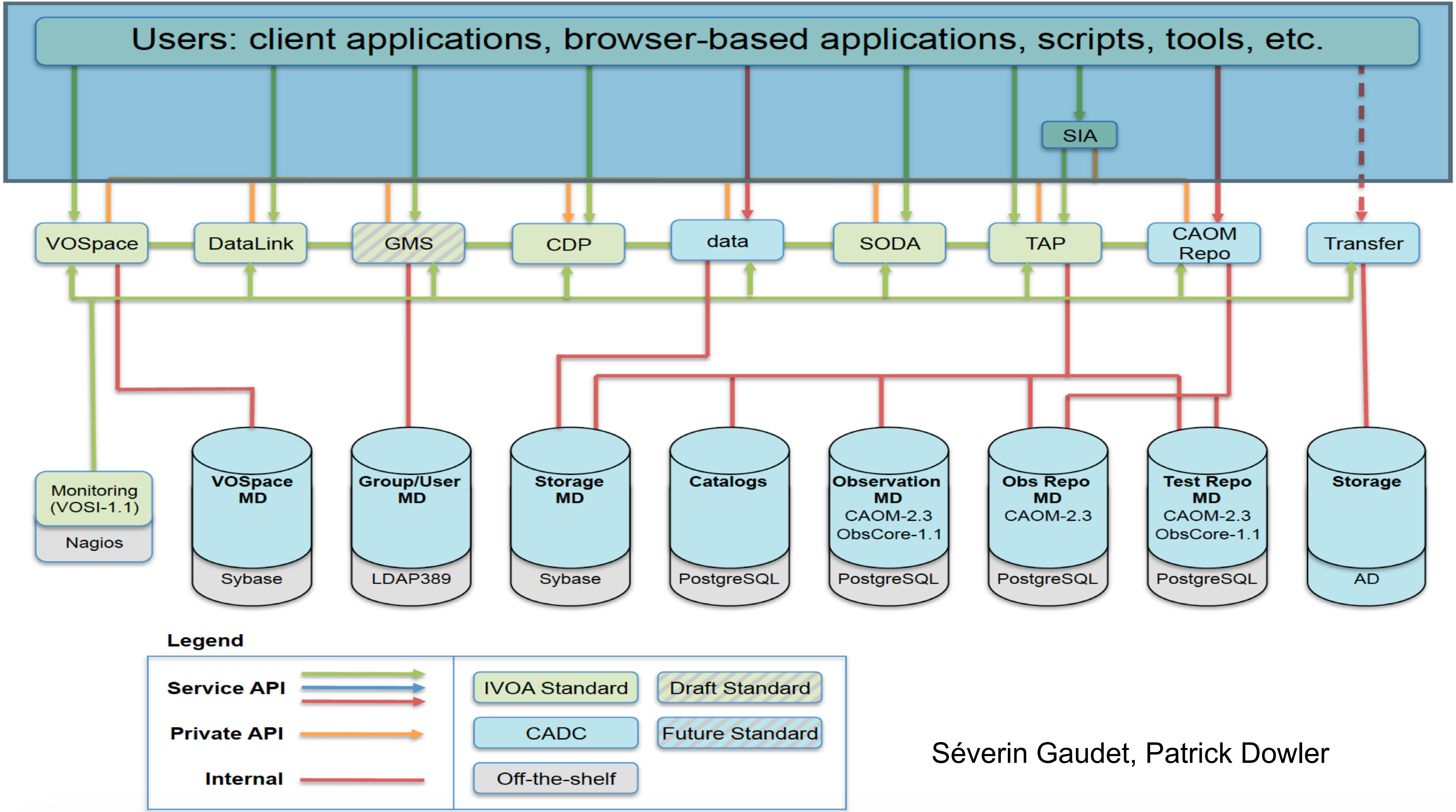
Services built on IVOA standards

All services support authentication in the same way

Many services support both users and other services

Credential Delegation is used for services to talk to each other

Resource ownership or group membership determine authorization



Séverin Gaudet, Patrick Dowler

Authentication Methods

Anonymous access
HTTP Basic Username/Password authentication
X.509 Certificates
Cookies / Tokens

Clients find the URL to the service capabilities through an internal Registry query.

Where are the capabilities for the TAP service on the JCMT observations?

Clients then query the capabilities with Standard ID and desired authMethods to find the access URL to the service.

What types of credentials can I use to asynchronously query this service?

Service use in January 2019

2 099 117 anonymous service transactions (3%)
66 356 042 authenticated transactions (97%)
Total: **68 455 159** transactions

Authenticated transactions breakdown:

< 1%	Cookie/Token
8%	HTTP Basic Username Password
91%	Client Proxy Certificate

Clients

- Python
  - cadc-data, vos, cadc-tap (username/password in .netrc, proxy certificates)
  - An astroquery cadc subpackage in progress (cookies/tokens)
- Javascript/browser access (cookies)
- Apps (eg. TOPCAT)
- Scripts: curl, wget (.netrc, proxy certificates)

Web Services

- 100% Pure Java
- All services support authenticated access the same way using core libraries
- User identities are ‘exploded’ upon service entry—get all identities associated with the one just used to authenticate.
  - Optimization when using cookies/tokens
- Don’t know *when*, *how* or *if* they’ll be used, so just make them available to the thread handling the request.
- *Why*: authorization checks

Groups

Groups for Protected Resources

- Owner (surrogate primary key)
- Group-read
- Group read/write
- Administrative group

- These are really just pre-defined *roles*
- Decoupling of these *grants* to A&A persistence – distributed references for scalability

LDAP – The Identity Holder

- Identity persistence: user identities as LDAP attributes
- Surrogate primary key identity that isn’t exposed to users and doesn’t change
  - Login/Posix username ← → LDAP Common name (CN)
  - Certificate DN ← → LDAP Distinguished name (DN)

User Registration

Getting a CADC Account

Users are vetted on registration.

Userids and CADC-signed X.509 certificates are created at registration.

X.509 certificates can be added or modified. Userids *could* be changed.

Interoperable A&A and services

Successful demonstration with INAF-OATs

- Use IVOA protocols (VOSpace, GMS*, CDP) to interoperate between data centres

- Dynamic user recognition & creation on first interaction with remote services

Bertocco et al: *Cloud access to interoperable IVOA-compliant VOSpace storage*

http://arxiv.org/abs/1806.04986

* Working draft status

Future CADC A&A Work

Moving A&A to external clouds

OpenStack Keystone Integration - Replicated, read-only LDAP host with minimal set of attributes exposed to Keystone to support user processing.

User Posix login on Virtual Machines and Containers using CADC credentials

OAuth / OpenID Connect Integration

Support users identified through Oauth, use tokens in CDP

More discussions on OAuth and IVOA during these meetings.

THANK YOU

Brian Major • CADC • brian.major@nrc-cnrc.gc.ca