Authentication and Authorisation for Research and Collaboration

LIGO Scientific Collaboration Pilot

SAML Proxy

Paul Hopkins
Cardiff University
LIGO Scientific Collaboration

FIM4R, Vienna
February, 11th 2019

Who am I?

- Paul Hopkins; Cardiff University and LIGO Scientific Collaboration (LSC)
- This work is motivated by Scott Koranda, Jim Basney and Warren Anderson (LSC)
- I have been supported by Arnout Terpstra, Simone Visconti, and Ioannis Igoumenos (AARC2)

Who is the LIGO Scientific Collaboration?

The LIGO Scientific Collaboration supports the LIGO Observatories in characterisation and analysis of the gravitational wave data and development of two detectors

- 1200+ Members
- 108 Institutions
- 18 Countries

The LSC works closely with the Virgo Collaboration which has a detector in Italy, and also the Japanese KAGRA collaboration.

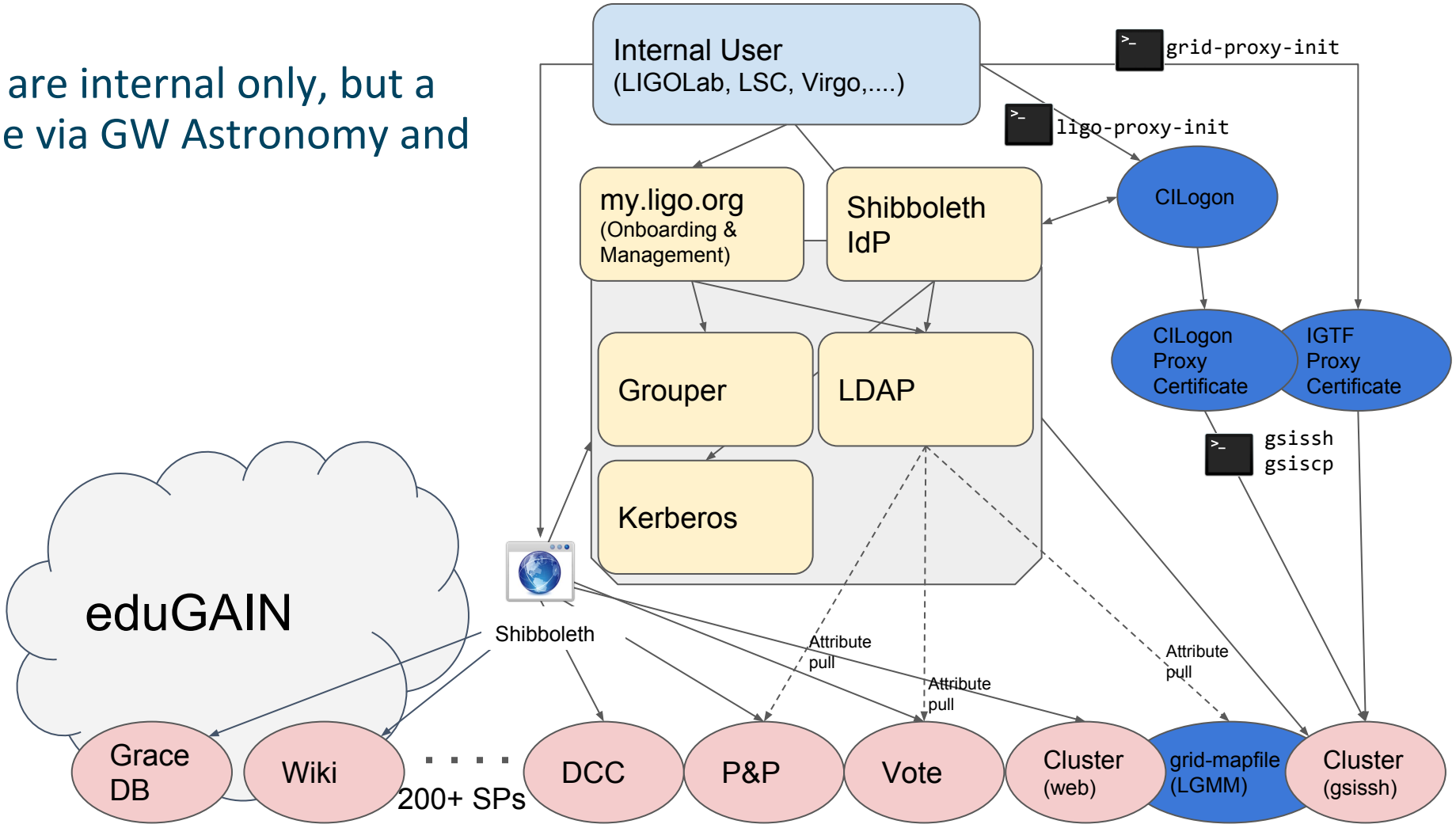
There is also the GW Astronomy organisation which manages links between the GW organisations and traditional astronomers, in particular for so-called EM Follow-up.

Current Infrastructure

- All LSC, LIGO Laboratory and Virgo members have an internal *albert.einstein* identity
- Account and password is managed at *my.ligo.org* and with other management websites
- These credentials are used:
  - to access web services using SAML
  - fetch CILogon X509 certificates via `command line`
  - Kerberos authentication
  - ….

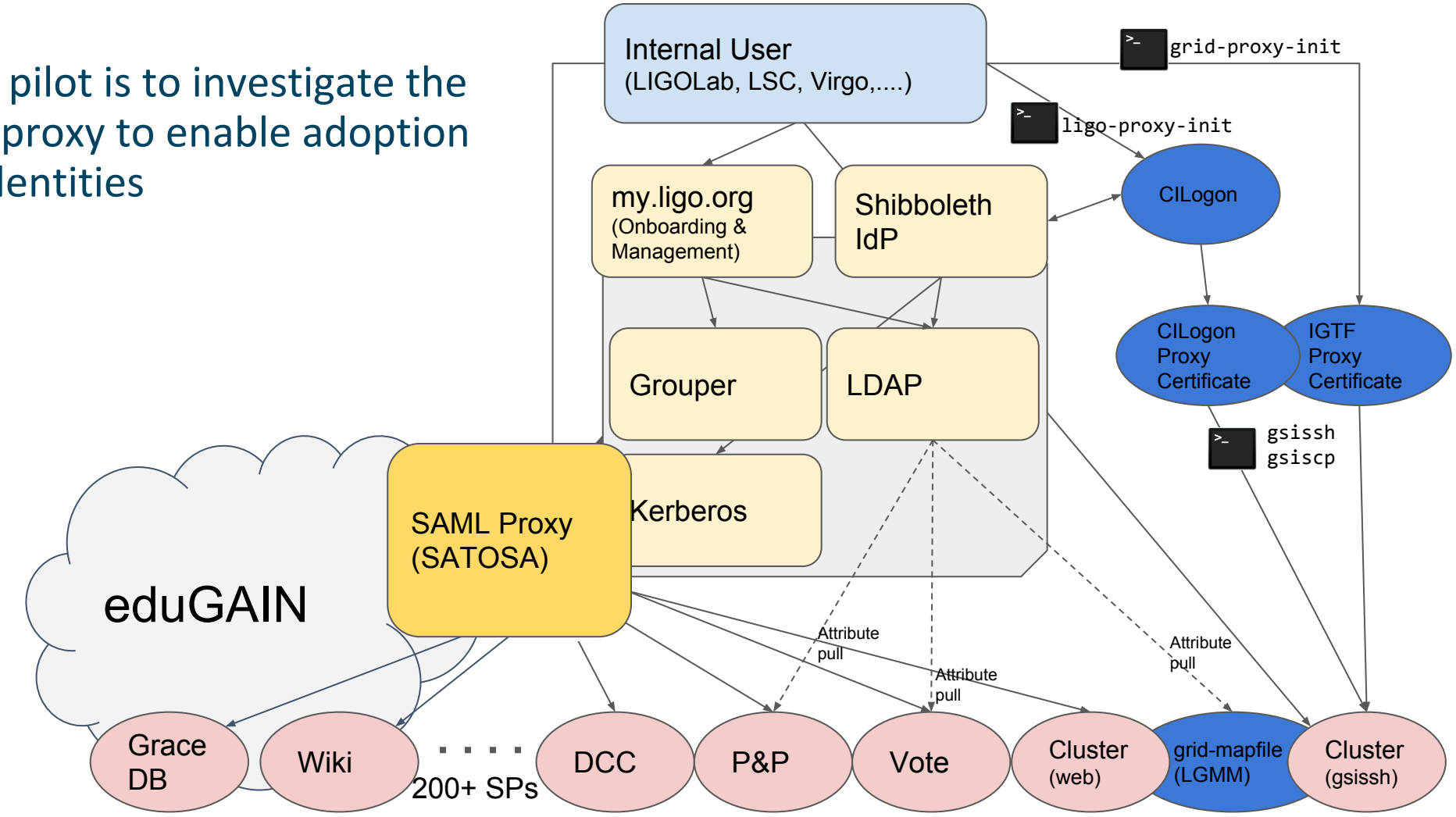
Current Infrastructure

- Most resources are internal only, but a few are available via GW Astronomy and Edugain

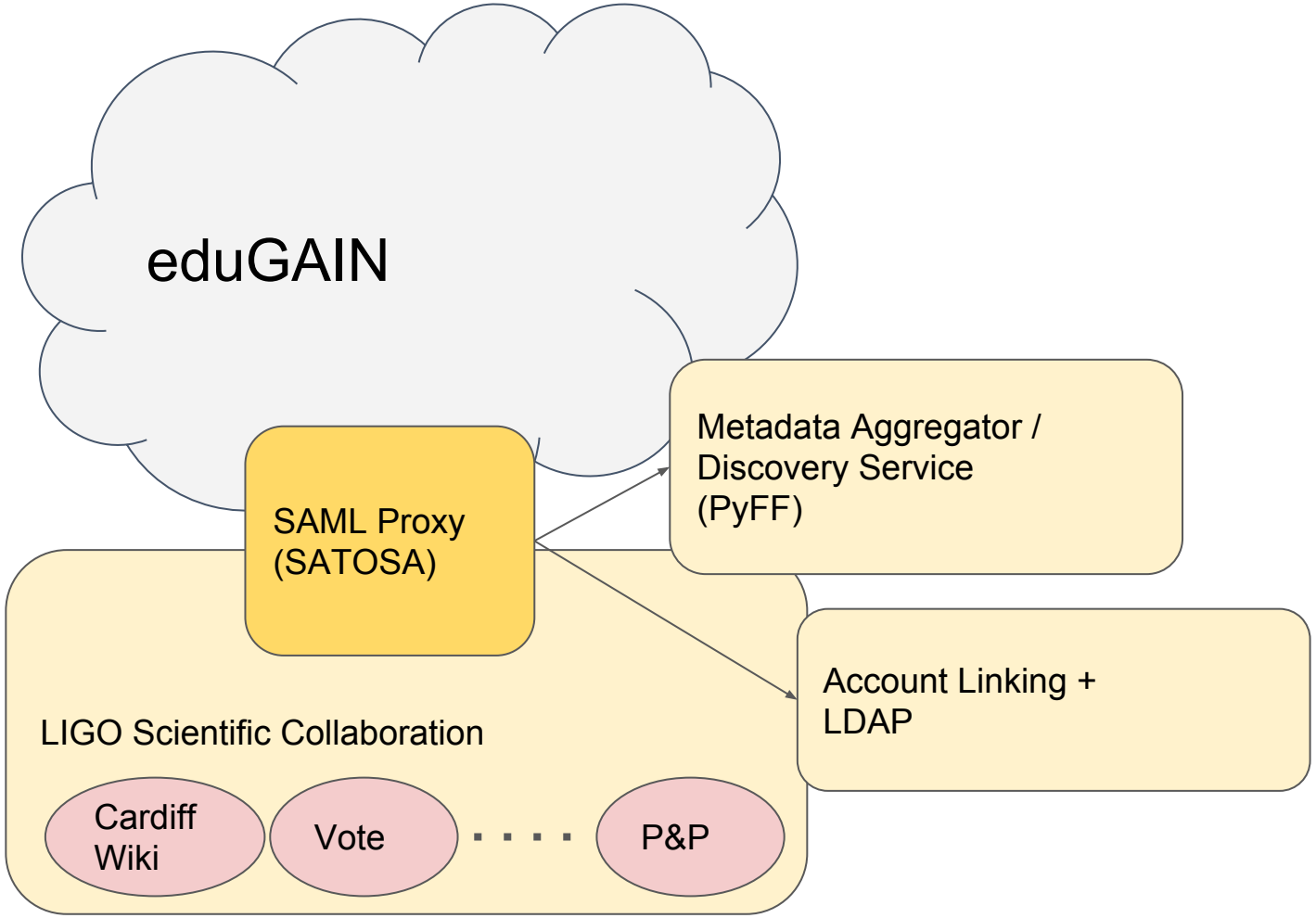


Planned Infrastructure

- The aim of the pilot is to investigate the use of a SAML proxy to enable adoption of federated identities



SAML Proxy Components



Progress

- ✓ Aims:
  - Add a SAML proxy for internal usage
  - Start moving SPs to the SAML proxy
  - Document changes required to SP configuration
  - Investigate PyFF for metadata aggregation and discovery service
- ✓ Progress:
  - Working closely with Scott Koranda (LIGO / Spherical Cow Group) and Jouke Roorda
  - Plan to implement Dockerised solution
  - Document changes required to SP configuration
- ✓ Next steps:
  - Actually create SAML Proxy and use internal LIGO IdP
  - Start switching my SPs over (e.g. Cardiff GitLab, wiki, Webserver, JupyterHub ….)
- ✓ Long term:
  - Switch away from my.ligo.org to CILogon hosted instance of COMangage?

Progress

Have deployed a SAML proxy using SATOSA

Frontend (IdP) is registered with LIGO Metadata and Backend (SP) is registered with Edugain

Uses existing microservices to process Authentication response

- First pick up correct identity attribute from differing IdPs
- Use identity attribute to lookup information in LIGO LDAP:
  - uid: paul.hopkins
  - sn: Hopkins
  - givenName: Paul
  - mail: paul.hopkins@ligo.org
  - isMemberOf: ….
  - …
- Correctly reproduces attribute behaviour of current system

Metadata aggregation and Login Chooser

- Have investigated the use of PyFF for metadata aggregation and login chooser
- Has also been shown to work with EduTeams login chooser
- Currently do not have a specific solution for institutional account linking

Deployment Notes

- Following Scott Koranda I have used used Docker Swarm for deployment
- Ansible used to automate deployment and configuration
- All materials will be made publically available

Limitations of Federated Identities

- X509 Certificates:
  - **Users currently use ligo-proxy-init command line tool to download certificates via ECP**
  - **This will not be possible using federated identities**
  - **-> Users could use CILogon web interface, or LSC could adopt OAuth based system?**
- WLAN Outages at LIGO Lab Sites:
  - **Both US LIGO Observatories in rural locations**
  - **Sites often experience WLAN outages**
  - **Currently duplicate IdPs, Kerberos and some other resources at each site**
  - **-> Would need to retain LIGO credentials for site staff and visitors**

Next steps

- Register the SAML Proxy SP as R&S; which will allow IdPs to release more attributes
- Complete configuration of PyFF for metadata aggregation and discovery service
- Enable account linking service
- Make it more widely available for testing
- Research solutions for high availability, e.g. LSC is transitioning to a cloud based IdP

Limitations of Federated Identities

- ✓ Observatories:
  - LIGO Observatories are in rural locations
  - WAN often fails
  - Currently replicate authentication, IdP, and SPs
  - Would need to retain dedicated LIGO authentication for observatory staff and visitors
- ✓ SSH Access:
  - Still struggling to find good federated solution for SSH access
  - As well as CILogon proxy certificate + gsissh switching to password and/or centrally managed SSH key
  - In a federated world we could create a dedicated password for SSH access
- ✓ Virgo:
  - LIGO work closely with Virgo collaboration and share many resources
  - Virgo does not use any SSO solution or federated identities.

Thank you

Any Questions?

HopkinsP@cardiff.ac.uk

https://aarc-project.eu

The work leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 730941 (AARC2).