IceCube User Management - OAuth2 in Practice

David Schultz, Steve Barnet, Vladimir Brik, Alec Sheperd, Benedikt Riedel
Wisconsin IceCube Particle Astrophysics Center, University of Wisconsin–Madison

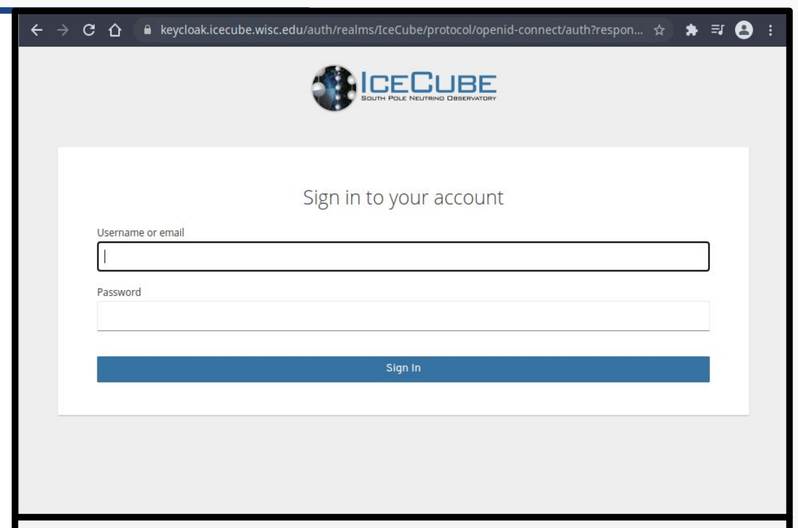
The IceCube Neutrino Observatory is a cubic kilometer neutrino telescope located at the geographic South Pole. The collaboration includes members from 58 institutions in 14 countries, and has grown significantly since the initial proposal. Technology has also advanced considerably in the nearly 2 decades since then. We document our transition from LDAP to Keycloak, and GridFTP to HTTP+tokens.

Old System

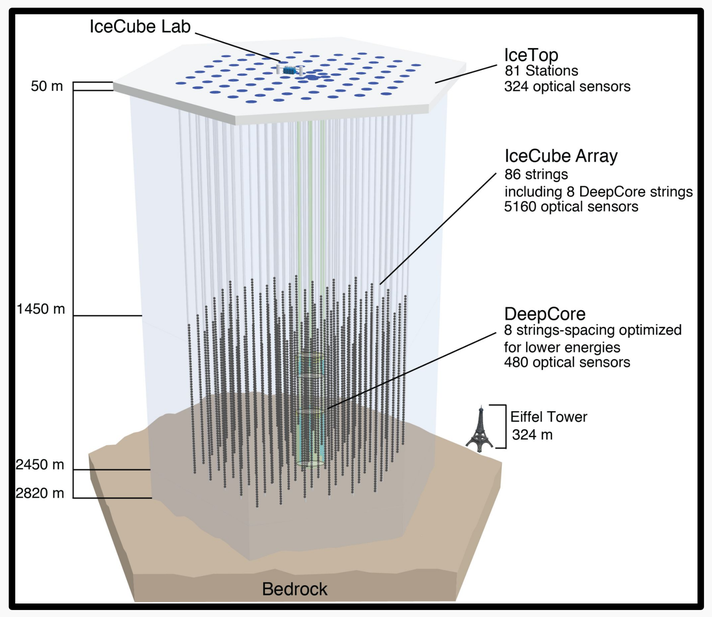
- LDAP-based, different logins per client
- IT admins manually update things

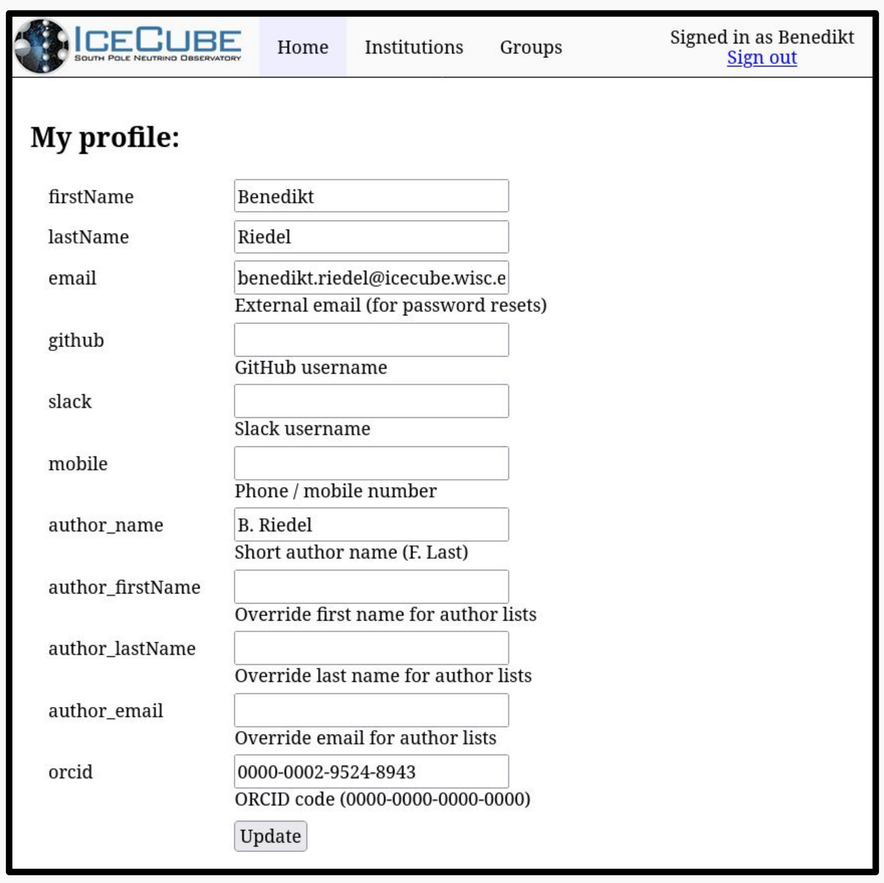
New System

- Keycloak-based
  - Supports OAuth2 and Single-Sign-On
  - Reset password via email
  - Offers MFA for web-based logins
- Self-service user management portal
  - Users: profile editor
  - Group admins: group management
  - Institution leads: membership and author list



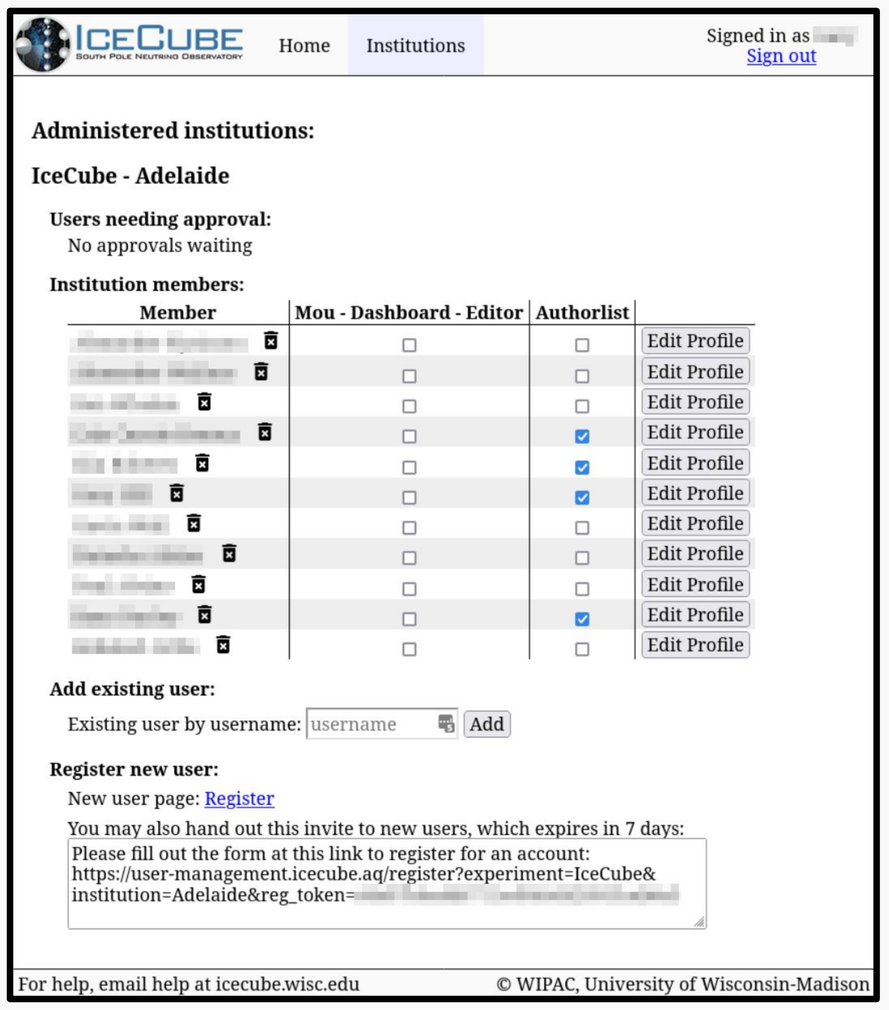
IceCube Single-Sign-On login page



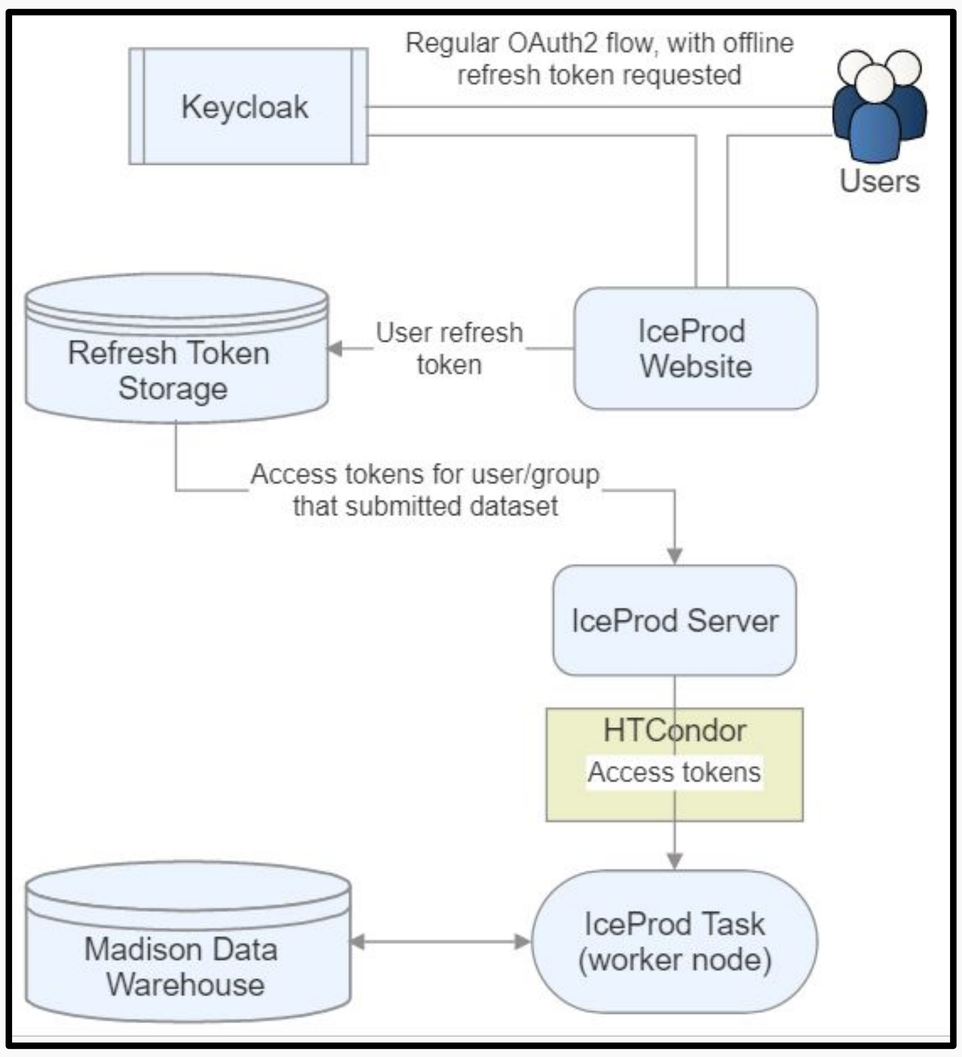


Profile self-management, including author list options.

Group management - shown here: control of an LDAP group providing command-line access to resources.



Institution leaders can edit membership.



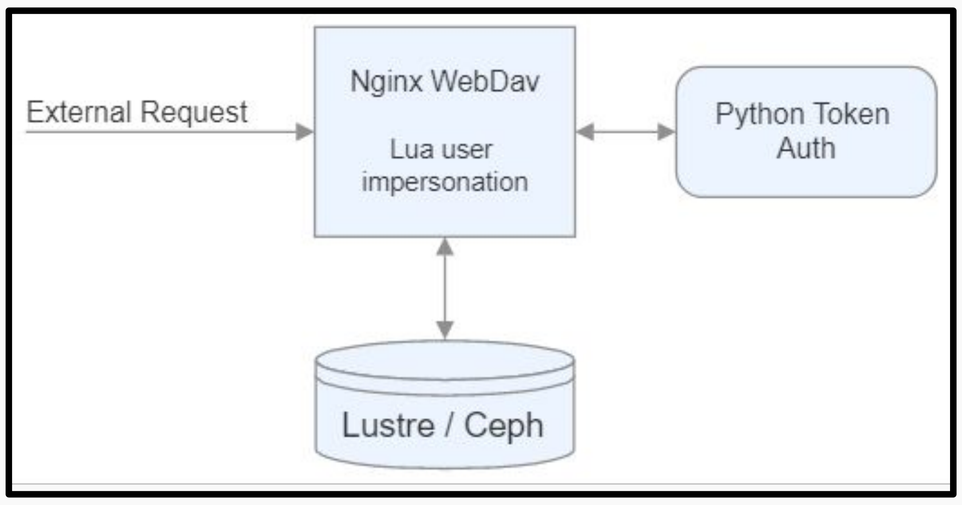
HTTP Data Transfers

Needed to replace the old system of X509 and GridFTP

New system based on OAuth2 tokens and HTTP

- Keycloak generates tokens
- Using Nginx for WebDav support
- Small Python script to verify tokens
- Tokens include uid/gid for user impersonation
  - Lua script inside Nginx handles impersonation

SCAN ME



Acknowledgements

This work was funded by the U.S. National Science Foundation (NSF) under grant OPP-2042807.