A New Authorization System for IceCube Applications

David Schultz
WIPAC, UW-Madison
Outline

▪ What is IceCube

▪ Authentication and Authorization
  ● Previous hodgepodge and new system

▪ Rollout Status
IceCube Neutrino Observatory

The IceCube Neutrino Observatory

Design and construction

Detector Design
- 1 gigabyte of Instrumented Ice
- 5,160 light sensors, or digital optical modules (DOMs), digitizes and timestamp signals
- 1 square kilometer surface array, Isotemp, with 304 DOMs
- 2 nanosecond time resolution
- IceCube Lab: 61.1 hours data processing and storage and sends 100 Gb of data north by satellite daily

Detector Construction
- 7 sessions of construction, 2004-2011

- 28,000 person-days to complete construction, or 77 years of continuous work
- 4.7 million pounds of cargo shipped, 1.2 million of which was the URL
- 48 hours to drill and 11 hours to deploy sensors per hole
- 4.7 megawatts of drill thermal power with 200 gallons of water per minute delivered at 88°C and 0.6 psi
Primary auth is LDAP at UW-Madison
- Used for ssh, some web pages

Secondary auth is x509
- Accessing storage servers via gridftp

Several more auths on an ad-hoc basis
- Primarily web applications
Authentication - New / Future

Use OAuth2
- Web sites / applications
- Storage
- ...

Currently a wrapper on top of LDAP
- Potential transition to Google as Identity Provider
Authorization - Previous

For most web sites, all or none
- If you can authenticate, you have access

Some web applications have local groups
- Difficult to manage

Storage based primarily on local mapping
- Except in DESY, which has VOMS
Tokens with granted scopes
- Central authority / signing
- Uses public/private keys

Compliant with SciToken syntax
- JSON web token
Each service registers a scope handler
- Handler is given user info from OAuth2 IDP
- Can return Yes/No, or a more detailed scope string

Example:
- Requested scope “myapp”
  - Yes result gives token with scope “myapp”
  - No result fails the token request
  - String result “foo” gives token with scope “myapp:foo”
Each service registers a scope handler
- Handler is given user info from OAuth2
- Can return Yes/No, or a more detailed scope string

This matches with SciTokens for storage
- Requested scope “write:/users”
  -- Normal users get their username appended:
     “write:/users/dschultz”
Authorization - New / Future

OAuth 2

Identity Provider

JWT Service

Auth A

Auth B

Service A

Service B
Revocation
- Tokens have short expiration, so most services rely on that
  -- Configurable, but usually 20-60 minutes
- Not good enough for some services (at least I was told this)

So like any good developer, I programmed a solution
- Token service now registers each token that is created
- User can access their token list, and revoke them
  (admin can revoke any)
- Services can download new revocation list as needed
  (every 1 minute, maybe?)
Current status

- OAuth2 wrapper for LDAP since early 2019
- Token service running since March
- Several developer services transitioned this summer
  -- Prometheus configuration, S3 presigned urls, file catalog
- Works well in production
  -- Testing container specifically for dev / CI
Current status

- OAuth2 wrapper for LDAP since early 2019
- Token service running since March
- Several developer services transitioned this summer
  -- Prometheus configuration, S3 presigned urls, file catalog
- Works well in production
  -- Testing container specifically for dev / CI

All running in Kubernetes
Current status

- Storage at Madison will support tokens by the end of 2019
- Simulation production infrastructure will then switch
- Analysis jobs should follow rapidly (not too many users)
  -- At this point, X509 should only exist for DESY gridftp
  -- Need to talk more with them
- Other web applications to switch in mid 2020

By the end of 2020, the transition should be complete
Conclusions

- IceCube had a proliferation of different authorization and authentication methods.
- These are now consolidated going forward.
- Tokens now in use at IceCube.