UC Davis SSO

AppDev SIG March 10, 2020

Grand Unified SSO Server

- CAS server implements three protocols
  - CAS Protocol
  - OAuth/OIDC
  - SAML 2.0
- SSO implemented with TGC (aka CAS protocol)
  - OAuth/SAML will redirect to CAS protocol to establish SSO
  - CAS Logout destroys any tokens created in that session

OAuth/OIDC

- New OAuth/OIDC features
  - Multiple redirect URLs
    - Localhost can be used
  - OAuth Access Tokens In JWT format
  - OIDC custom UCD Profile
  - More OIDC protocol supported
    - Proof Key Exchange
  - Tokens only valid for length of SSO Session
    - Logout will destroy tokens

SAML 2.0

- Support migrating from Shibboleth to CAS
  - CAS receives and handles SAML requests directly
  - Federated integrations using MDQ
- On prem and manual integrations move first
- Move services to OAuth if preferred by vendor
- InCommon/UC Trust Federation
  - New integrations still need to be done in Shibboleth
  - Automatically migrated when switch made to InCommon
- Shibboleth will be retired

Benefits

- Single authority for SSO sessions
- SAML logins are faster
- Improved SLO support
- Improved integration process
- A single domain can implement each protocol
  - You can figure all three protocols in your service
  - Parts of your service could be protected by different protocols

CAS Management

- One stop shop for SSO integration
  - All three protocols can be configured
- Updated to Angular 9
- Improved Performance
- Ability to destroy SSO sessions and Tokens
- I promise updated KB articles are coming

What you need to do

- Nothing
- Move Shibboleth integrations to CAS
  - All Current Shibboleth integrations added to ssodev
  - Test by overriding shibboleth.ucdavis.edu to 128.120.39.52(ssodev2)
- Consider moving SAML to OAuth
- Consider switching from CAS to OAuth (need attributes)

Going Forward

- Start using stage.cas.ucdavis.edu
  - Same infrastructure as production
  - Monitored and any downtime treated like production environment
  - Services with "qa" or "stage" in domain should be moved
- All CAS Services "claimed" in registry
- Remove service from registry if retired
- Automated Registry "cleaning"

Thank You

- Jeremy Philips
- Scott Kirkland
- Chris Lambertus
- Demi Beyene
- Tom Poage
- Mary Northup
- Ilvana Mesic