CAS 6.0 Update

Changes in CAS 6.0

Tomcat Upgrade

- Upgrade from 8.5 to 9.0.17

Java JDK Update

- Upgrade from JDK 1.8 to JDK 11

CAS Dependencies

- Spring Boot 2
- Spring v5

New Features

- OAuth/OIDC Protocols Supported
- Stage Environment
- Ability to revoke SSO sessions and OAuth Tokens
- Removed Annual Renewal
- Stage to Production promotion

Stage Environment

- New domain stage.cas.ucdavis.edu
  - Same Service Registry as CAS Production
  - Stable, only changes for production deployment
  - Requires service to be registered (No localhost)
- Dev Environment
  - New domain dev.cas.ucdavis.edu domain
  - Old ssodev.ucdavis.edu will remain.

OAuth/OIDC Protocols

- Supported Flows
  - Auth Code – response_type=code
  - Token/Implicit - response_type=token
  - Resource Owner – grant_type=password
    - Limited use to most likely only departmental accounts
  - Client Credentials - grant_type=client_credentials
    - Useful for machine to machine auth
  - Refresh Tokens
  - OIDC IdToken – response_type=id_token
- https://apereo.github.io/cas/6.0.x/installation/OAuth-OpenId-Authentication.html

JWTs

- CAS 6.0
  - Use OIDC IdToken for JWT Authentication
- CAS 6.1
  - Will be able to return Access Token as a JWT
  - Checkbox in CAS Management config screen.

Registering OAuth/OIDC Services

- New /oauth endpoint in CAS Management
  - Requires a service to be registered, does not work with wildcard
  - New services added to "stage" first
  - Once verified, promoted to "production"

CAS Management Updates

- Revoke TGTs
  - Ability to revoke individual, bulk and all SSO Sessions
  - Revoking TGT will attempt SLO to CAS clients
- Revoke OAuth Tokens
  - Ability to revoke individual, bulk and all OAuth Tokens
  - Revoking Token will not delete SSO Sessions
- Use base / context – https://casmgr.ucdavis.edu

CAS Management

- Annual renewal requirement removed
  - New process will monitor last time used
  - After a period of non-use email sent to service owners
  - Logging into service once resets timer
- Request Service be promoted to production
  - Probably only used for OAuth/OIDC
  - CAS Services can be "staged" and "promoted', but not required

CAS 6.1

- Late Summer/Early Fall
- JWT Access Tokens
- OAuth/OIDC Certified
- SAML Support
  - CAS handle SAML 2.0 requests
  - CAS Management used to upload and manage metadata