University of California OATS: an OpenACS-based application in the AWS cloud

Khy Huang, Sung Hyuk-Hong, Josue Cardona, Juan Tapia, Gene Lacson, Eric Yuen, Veronica De La Cruz, Robert Dennis

UCLA – Computing Technologies Research Lab (UCLA / CTRL)

European OpenACS and Tcl Conference, Vienna 2022
Background -

• UCLA School of Medicine since 1996
  • NaviServer and IllustraDB (pre ACS days)
  • GnnServer and Solid DB
  • Aolserver and Oracle 8i….

• ~70 currently operating openACS-based web applications:
  • Core Lab Management System
  • Basic CMS site, Faculty Lab site, department sites, etc.
  • Clinical Trials Management Systems (Surveys)
  • Research data collection, management and reporting systems
  • Request for proposal submission and review systems
  • … but oddly, never a course management system
University of California

UC SYSTEM

10 Campuses
6 Academic health centers
3 National laboratories

- LAWRENCE BERKELEY NATIONAL LABORATORY
- LAWRENCE LIVERMORE NATIONAL LABORATORY
- LOS ALAMOS NATIONAL LABORATORY

UC BERKELEY
UC SANTA CRUZ
UC SANTA BARBARA
UC IRVINE
UC SAN DIEGO
UC DAVIS
UCSF
UC MERCEDE
UC RIVERSIDE
UC
+ ACADEMIC HEALTH CENTERS
UC OATS General requirements

- University of California - public university with 10 campuses
  - Each campus is separate and independent
  - Campus-specific authentication (shibboleth)
  - OACS subsite for each campus
- UC policies on conflict of commitment – limits on time and earnings from outside professional activity, e.g., consulting, etc.
  - Types of outside professional activity (cat 1, 2, 3)
- Role-based – Faculty, staff reviewers, faculty administrators, auditors
- Workflow-driven – certain types of activities require review and approval by several offices
- System or record – official repository of legal disclosures
- Reliability and availability – no down time
Forms requiring review

UC OATS is a role-based system. Forms (acs_object) follow different workflows.

Involving Students in outside professional activity

Annual Certification (all faculty 1 time / year)

Category I Prior Approval
Request to Exceed Effort/Earnings
AWS- VPC architecture
**OACS cluster vs cloud elasticity**

- **OACS clustering**
  - Canonical server and member servers (leader and followers)
  - Canonical server runs scheduled procs!
  - Assumes that the set of members is static (IP addresses are known)

- In the “Cloud” server infrastructure becomes virtual
  - Elasticity replaces capacity
  - Key benefit is being able to scale servers up or down according to traffic/load
  - Need to dynamically declare members
  - Need to manage member retirements
Current Setup

ALB rules route traffic based on hostname

Canonical Server
www.ucoats.org

EC2
ucla.ucoats.org

EC2
ucsd.ucoats.org

EC2
uci.ucoats.org

AWS Aurora Postgres Cluster
Dynamic cluster member management - /ctrl-db-utils

- **cluster_member_sweep_time**: 300
  - The number of seconds to run the sweeper. It requires a system restart to apply. If is set to 0 then the sweeper won't activate.

- **manageAuthorizedIP**: 1
  - This will indicate if the Authorized IP list will be updated when removing members.

- **member_stale_takedown_time**: 3600
  - The number of seconds that a member can stay stale before it is removed from the member list.

---

**Cluster Status**

- Is Clustering Enabled? : Yes
- Is Clustering Logging Enabled? : Yes
- Current Server IP: 10.34.21.252
- Is this Server the Canonical Server (Canonical IP: 10.34.21.252) ? : Yes

**Member IP List**

<table>
<thead>
<tr>
<th>IP</th>
<th>Is Privileged</th>
<th>Is Active</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.34.21.252</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>10.34.21.200</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>10.34.26.45</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>10.34.22.174</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>

Showing 0 to 0 of 0 entries.
PIPELINE IN TEST/STAGING

AWS CODE PIPELINE

.git

AWS CodeBuild

ECS CodeDeploy

ECS
FUTURE SETUP WITH CI/CD WITH AUTOMATED TESTING
Moving DB between different environments

Import DB → Configuration Script → DB Ready
Goal for production environment...

UCOATS

Canonical Service

Member Service

1..1

ALB

www.ucoats.org
ucla.ucoats.org
ucberkeley.ucoats.org
ucsf.ucoats.org

Task1

Task1

TaskN

AWS Aurora Postgres Cluster
Challenges, lessons & questions

Clustering - what happens if the canonical server dies?

• External monitor?
• Can a member of the cluster be elevated to Canonical status?
  • Raft consensus algorithm (https://raft.github.io/)?

Security and performance

• OpenACS – very open
• . /shared/whos-online
• . /api-doc/
• Default Permissions too open (beware of “... Inherit Permissions from Main ....)
• How can we programmatically update permissions?
• NaviServer performance tuning secret sauce?
Closing or Transition Slide