

David Geffen School of Medicine



David Geffen School of Medicine



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

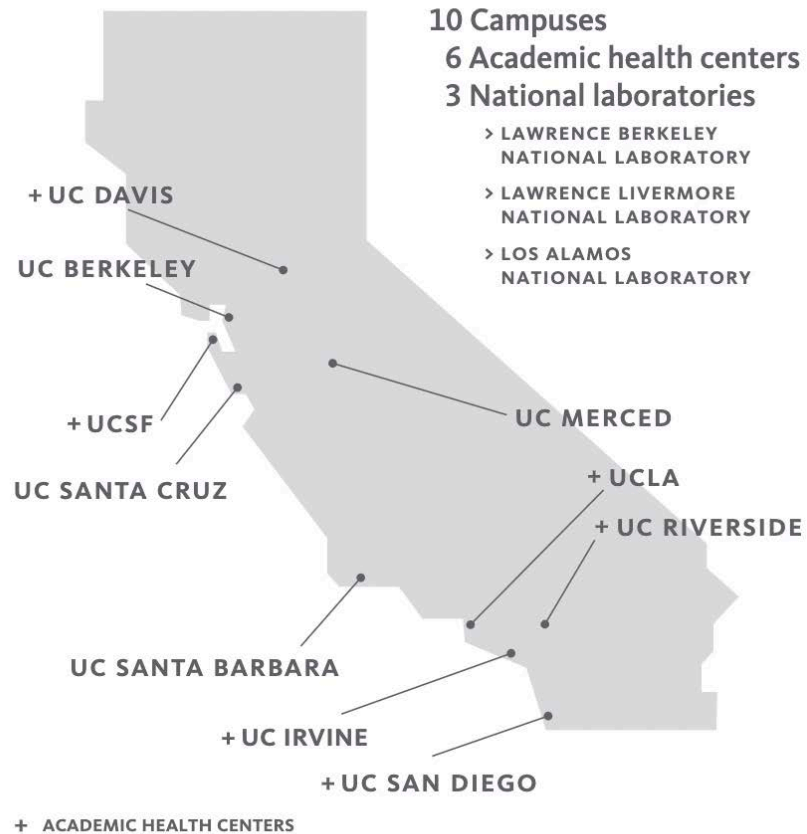
UCLA / CTRL

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



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

Berkeley
UNIVERSITY OF CALIFORNIA

UCLA

UCSF

UC San Diego

UC RIVERSIDE

UCI

UC SANTA CRUZ

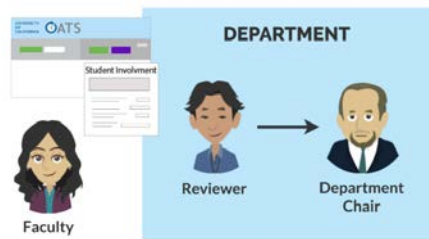
UCSB

UC DAVIS

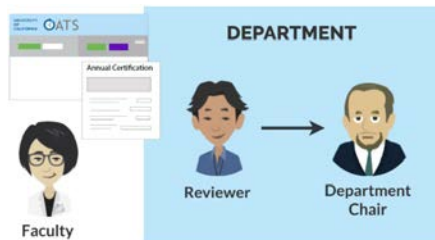
UNIVERSITY OF CALIFORNIA
MERCED

Forms requiring review

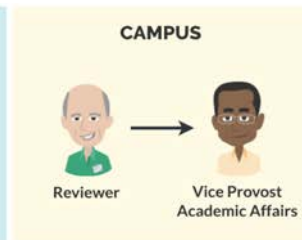
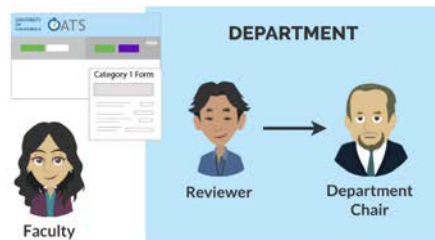
UC OATS is a role-based system. Forms (acs_object) follow different workflows



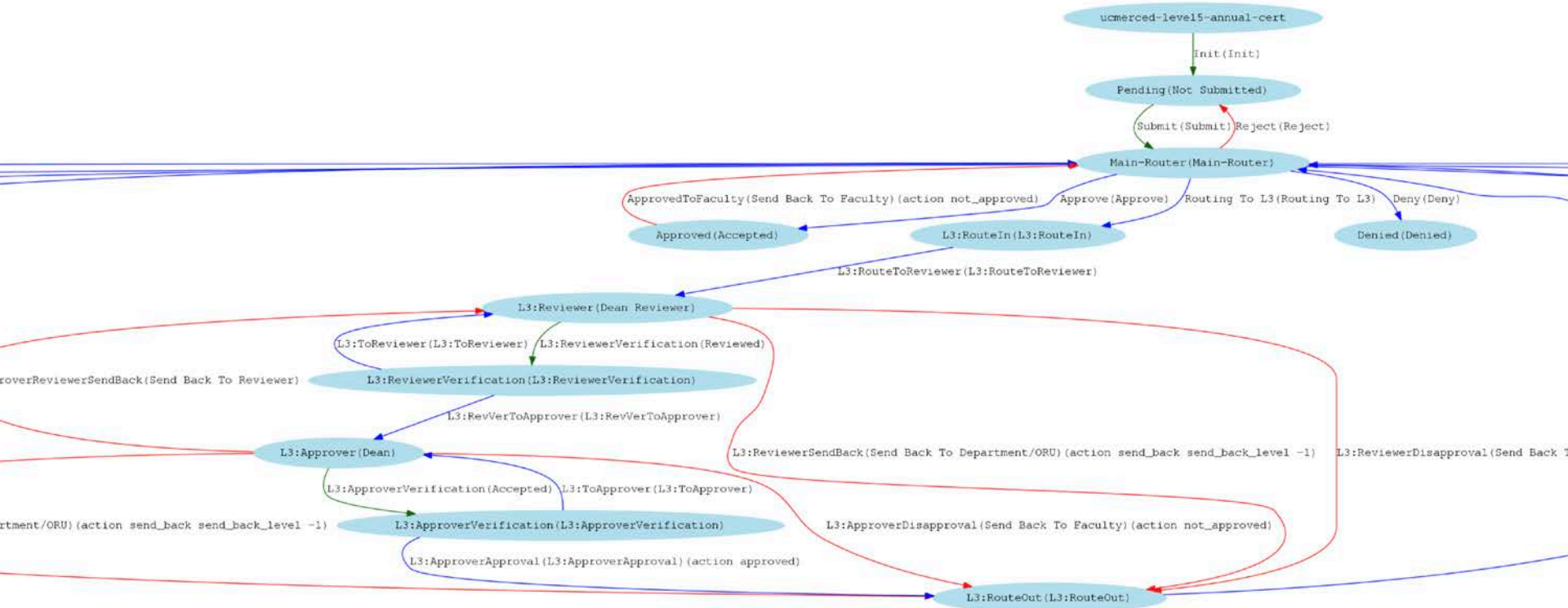
Involving Students in outside professional activity



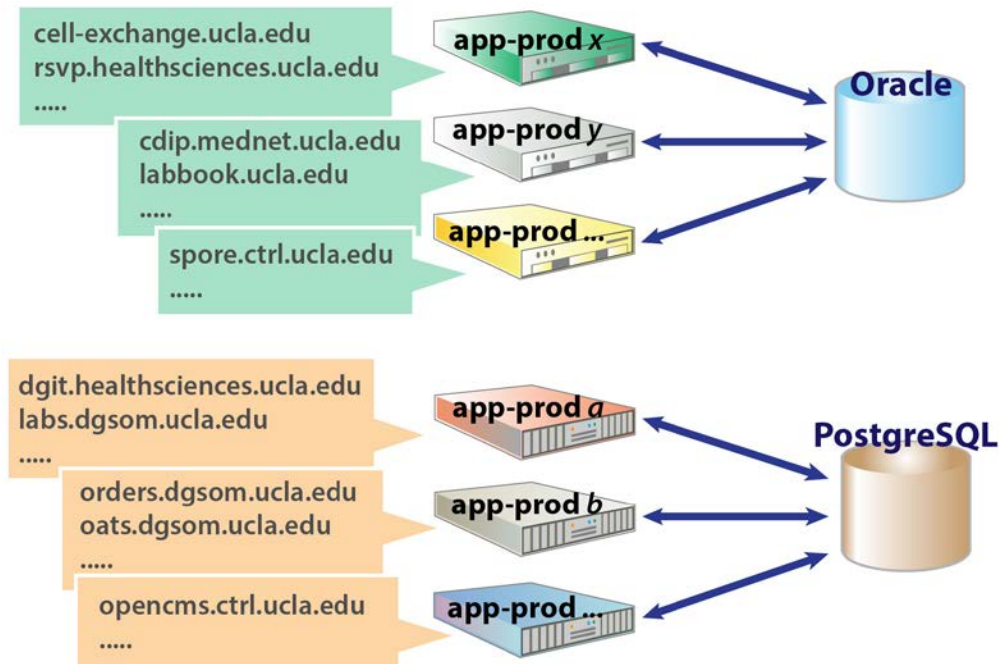
Annual Certification (all faculty 1 time / year)



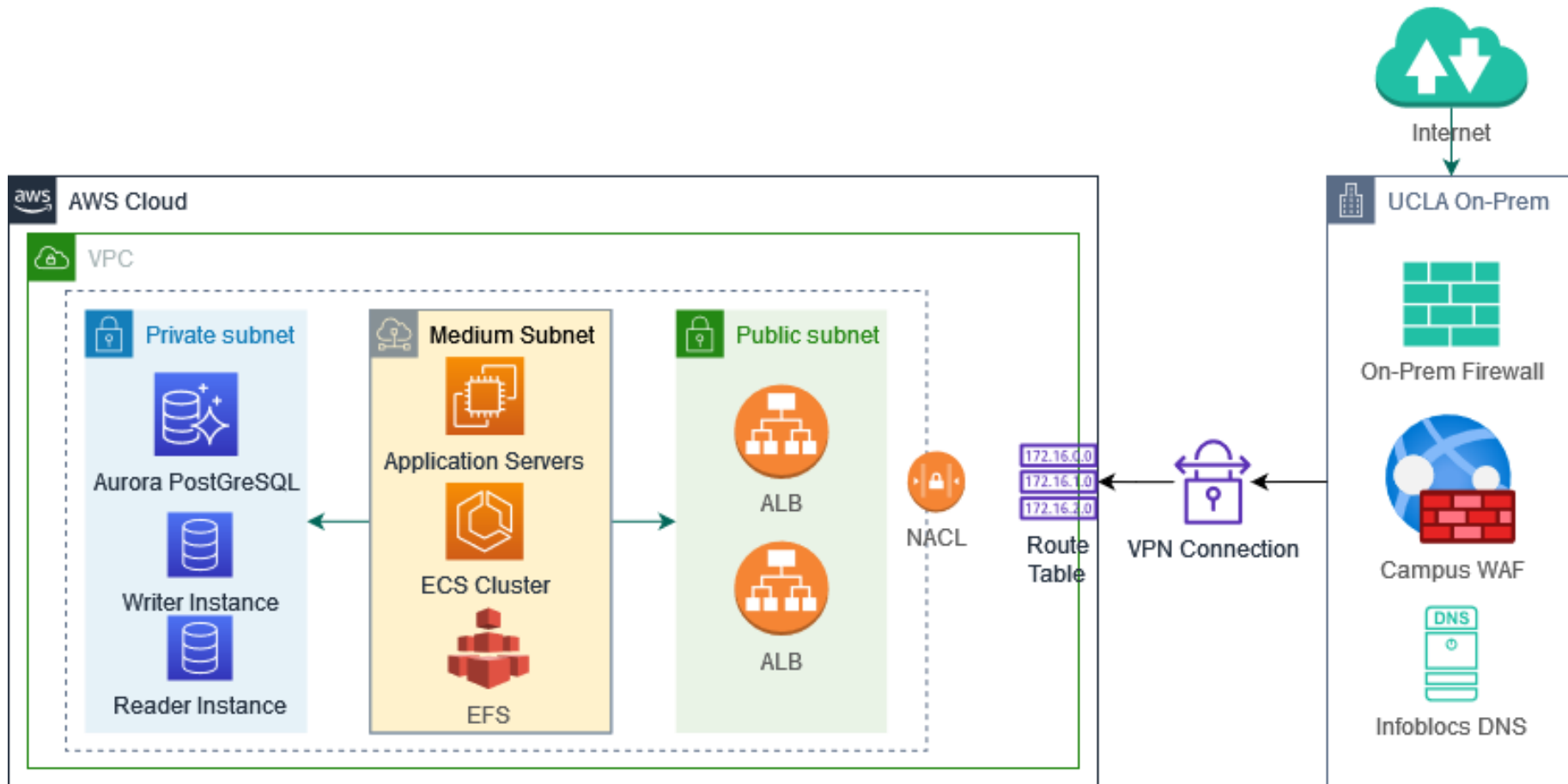
Category I Prior Approval Request to Exceed Effort/Earnings



General architecture of web systems on premise (1997-2017)



AWS- VPC architecture



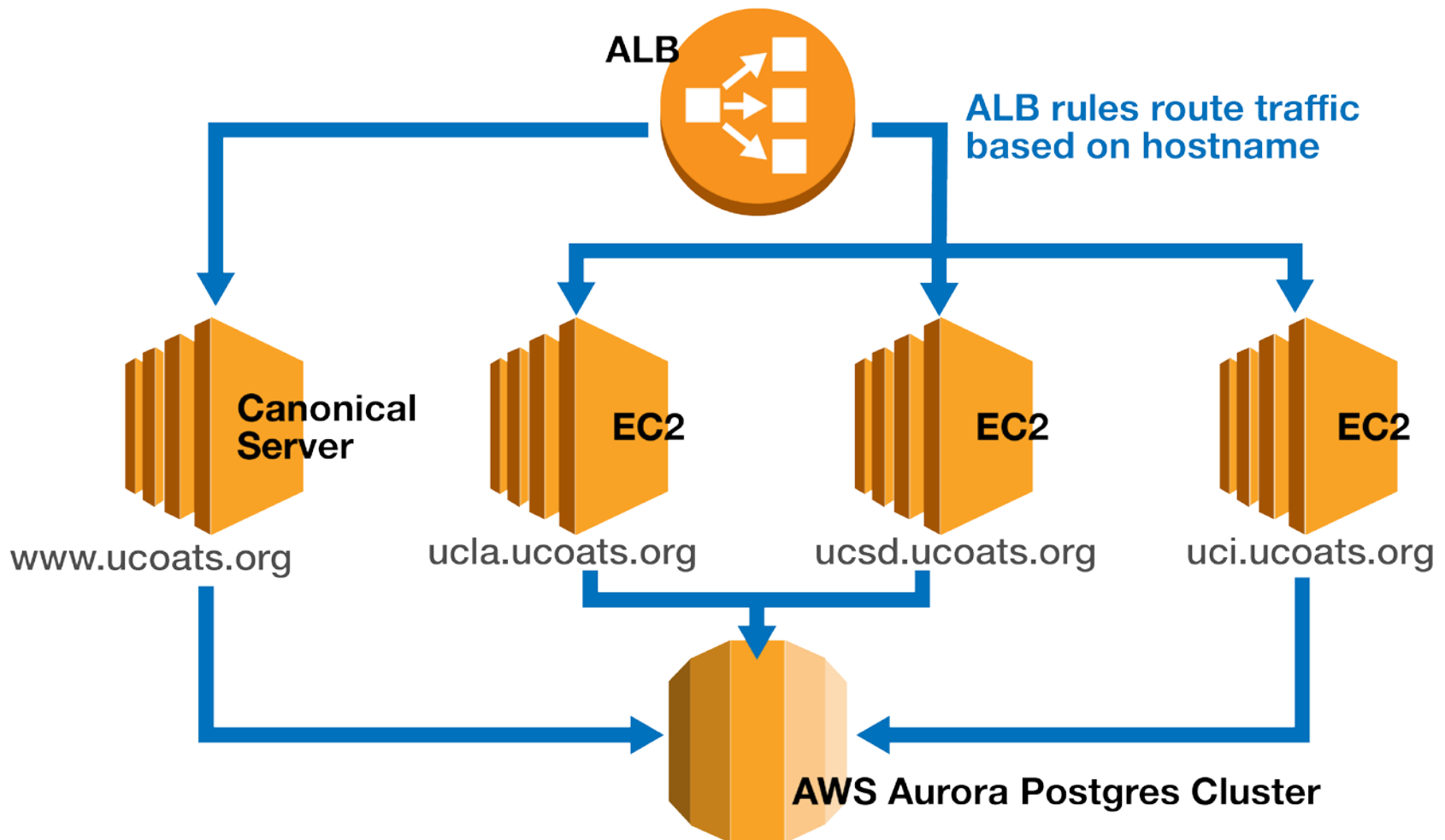
OACS cluster vs cloud elasticity

- 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

Server cluster

CanonicalServer	<input type="text" value="10.10.13.249"/>	<small>ⓘ In the list of IPs above, which is the canonical (primary) server? If a port is not listed, we assume port 80.</small>
ClusterAuthorizedIP	<input type="text" value="10.10.13.249 10.34.14.248"/>	<small>ⓘ A space separated list of which machines can issues requests (e.g., flushing) to the cluster. Can use glob m</small>
ClusterEnabledP	<input type="text" value="1"/>	<small>ⓘ is clustering enabled?</small>
ClusterPeerIP	<input type="text" value="10.10.13.249 10.34.14.248"/>	<small>ⓘ A space separated list of servers in the cluster. This server's IP may be included too.</small>
EnableLoggingP	<input type="text" value="1"/>	<small>ⓘ log clustering events?</small>

Current Setup



Dynamic cluster member management- /ctrl-db-utils

cluster_member_sweep_time

ⓘ the number of seconds to run the sweeper. It requires a system restart to apply. If is set to 0 then the sweeper wont activate

manageAuthorizedIP

ⓘ This will indicate if the Authorized IP list will be updated when removing members

member_stale_takedown_time

ⓘ 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

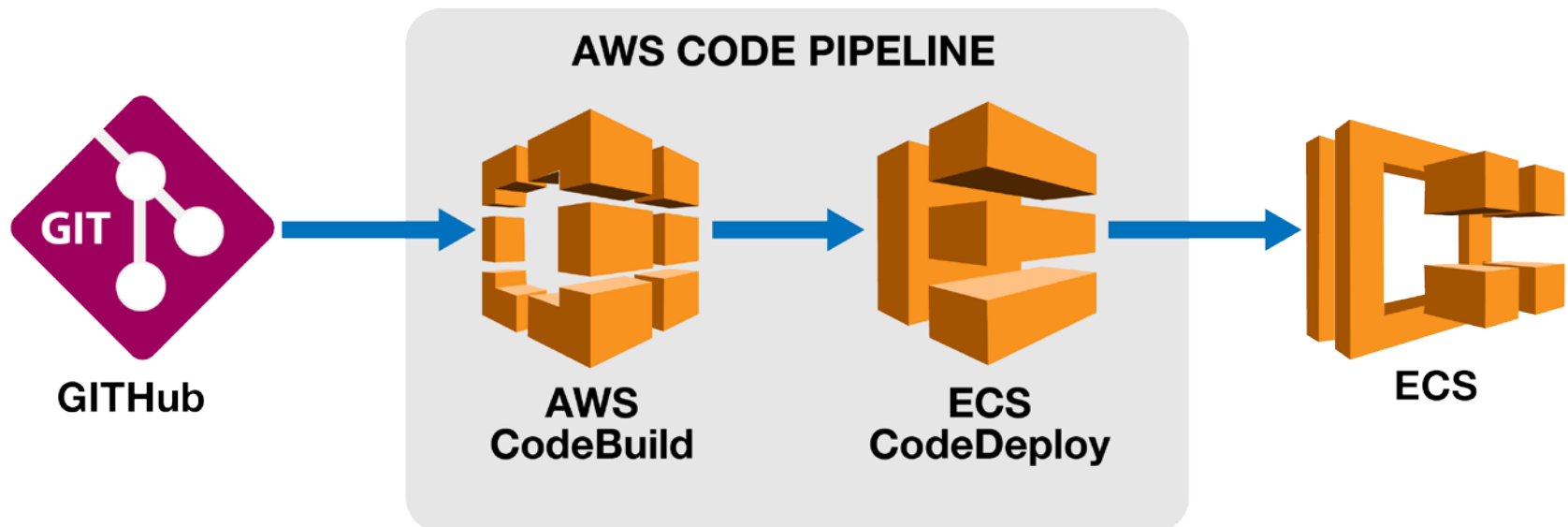
Is this Server the Canonical Server (Canonical IP: 10.34.21.252) ? : Yes

Member IP List :

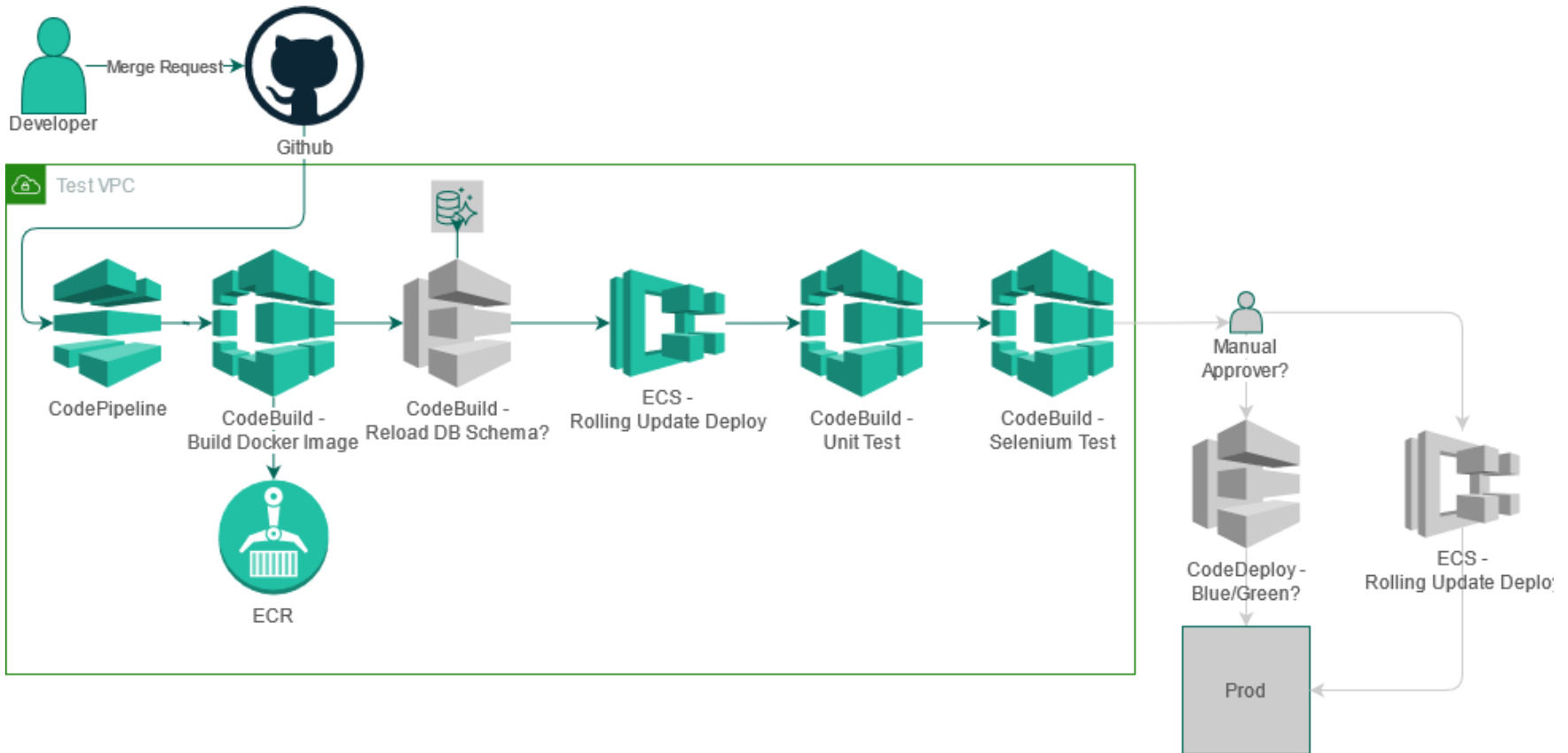
IP	↓ ⓘ	Is Privileged	Is Active
10.34.21.252		Yes	
10.34.21.200		Yes	
10.34.26.45		Yes	
10.34.22.174		Yes	

Showing 0 to 0 of 0 entries

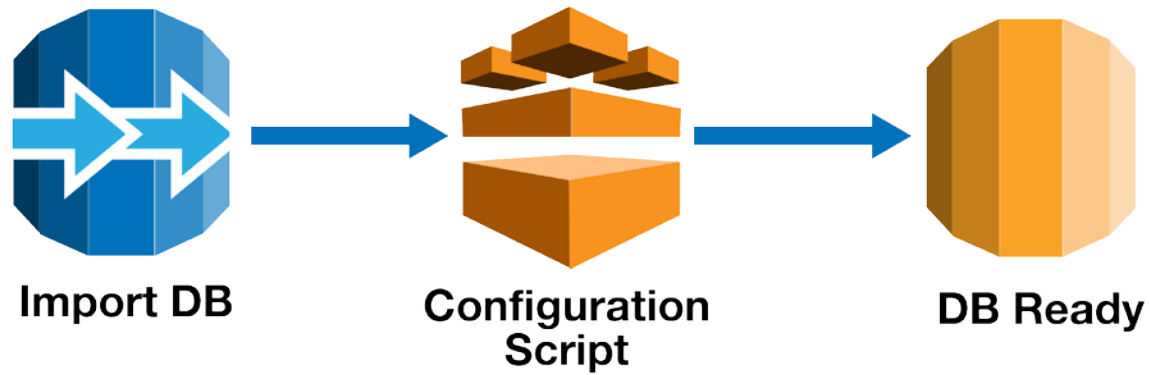
PIPELINE IN TEST/STAGING



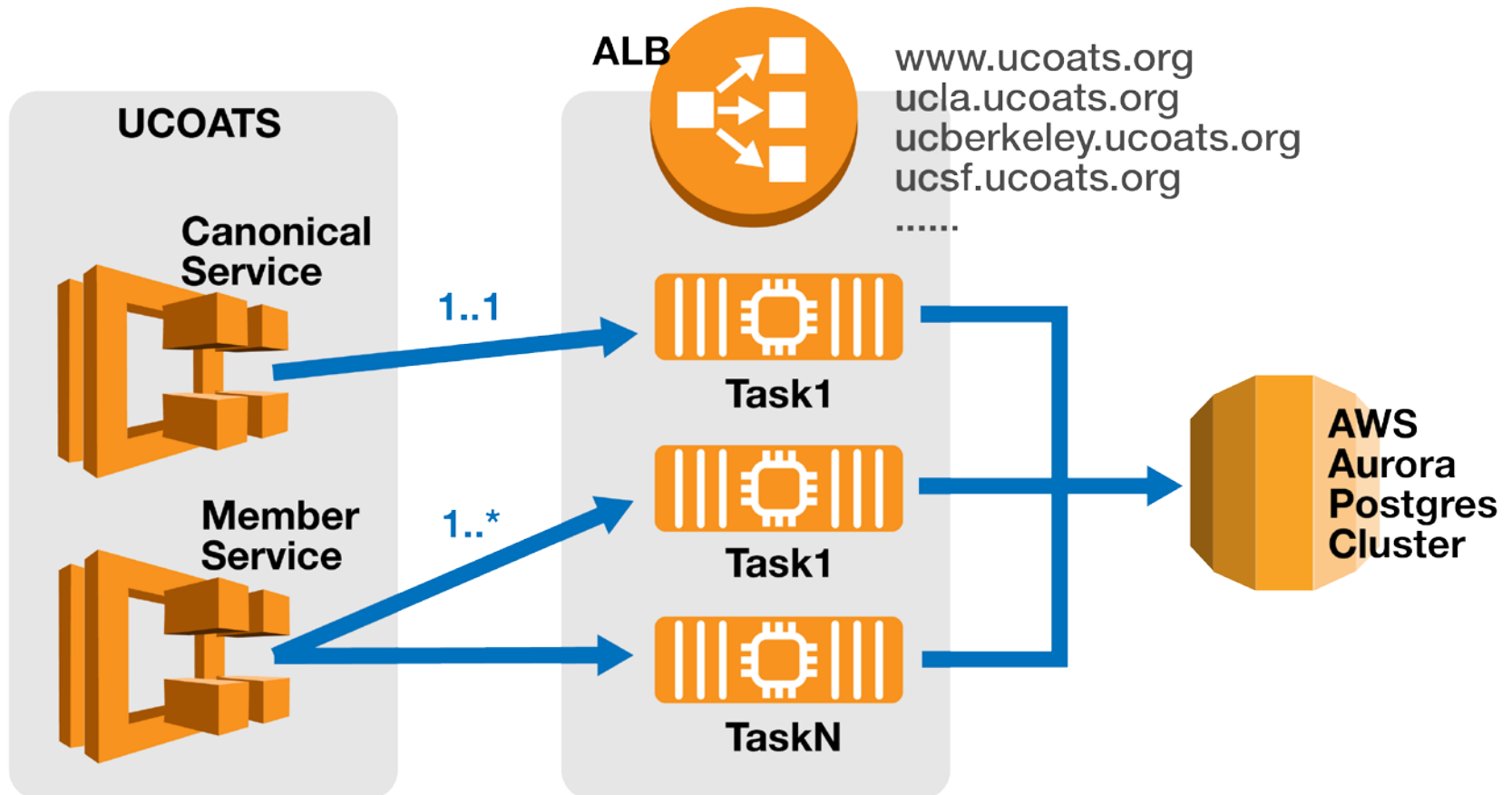
FUTURE SETUP WITH CI/CD WITH AUTOMATED TESTING



Moving DB between different environments



Goal for production environment...



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

