Illinois: Cloud First, What Next?

Keith Wessel, Illinois

With Contributions from Erik Coleman and David Riddle
First Things First

• Began our "Cloud First" initiative in 2016
  – Move all services to AWS or hosted vendors
  – Containerized where possible
• TIER ramping up at the same time
  – TIER packages dockerized
  – Perfect to run in AWS Fargate
  – Thanks, TIER!
Putting TIER in the Cloud

- TIER packages needed little modification
  - Disable HTTPS (ALB handles SSL)
- Configurations and branding layered on top with Docker
- Environment-specific configuration/keys
  - Passed as environment variables
  - Or leveraging AWS Parameter Store and Secret Manager
Orchestrating (Cloud Tinker Toys)

- Using Drone to automate builds
- AWS CodePipeline for CI
- Library of Reusable Terraform modules
  - Easy to incorporate to build infrastructure
  - Just set variables and include modules
- Special bonus
  - AWS CLI/API login with Shibboleth ECP
  - Our ECP supports MFA too!
Let’s Take a Look...

- Grouper deployed to AWS
- Part of our “Authorization Manager” service to campus
Layered Configuration

```dockerfile
FROM tier/grouper:2.4.0-a2-u0-w0-p0
LABEL author="tier-packaging@internet2.edu <tier-packaging@internet2.edu>"
MAINTAINER techservices-iamu@illinois.edu <techservices-iamu@illinois.edu>
COPY ./container_files/grouper/**.properties /opt/grouper/conf/
COPY ./container_files/httpd/host-key.pem /run/secrets/
COPY ./container_files/httpd/host-cert.pem /etc/pki/tls/certs/
COPY ./container_files/httpd/cachain.pem /etc/httpd/conf.d/
COPY ./container_files/httpd/ilo-gauthman*.png /opt/grouper/grouper.ui/grouperExternal/public/assets/images/
COPY ./container_files/startup/docker-entrypoint.sh /
RUN /usr/lib/jvm/zulu-8/jre/bin/keytool -importcert -noprompt -file /etc/pki/tls/certs/cachain.pem -storepass changeit
```
Infrastructure as Code

```bash
1  terraform = {
2      include {
3          path = "${find_in_parent_folders()}
4      }
5  }
6  
7  terraform {
8      source = "git@github.com:cites-illinois/as-aws-modules//ecs-service"
9  }
10
11  # ECS configuration
12  name = "authman-ui"
13  desired_count = "1"
14
15  # Load Balancer configuration.
16  load_balancer {
17      name = "public"
18      port = "443"
19      container_name = "authman-ui"
20      container_port = "80"
21      host_header = "authman-test.techservices.illinois.edu"
22      certificate_domain = "authman-test.techservices.illinois.edu"
23  }
24
25  health_check {
26      interval = "300"
27      timeout = "30"
28      unhealthy_threshold = "3"
29      path = "/grouper/status?diagnosticType=trivial"
30  }
31
32  # Define service network configuration. (aws-vpc mode only)
33  network_configuration {
```
The AWS Console
A Grouper Subject

Coleman, Erik C

Unique ID: 659676474
Name: Coleman, Erik C
Description: Coleman, Erik C

dn: CN=ecc,ou=People,dc=ad,dc=uillinois,dc=edu
mail: ecc@illinois.edu
displayname: Coleman, Erik C
givenname: Erik
uid: 659676474
samaccountname: ecc
sn: Coleman
Member ID: b768ed26b38a49168a113ae0565705a3
Source ID: ldap
Source name: ADDEV People

Less
Modified subject.properties

5 ectApi.source.ldap.types = person
6 ectApi.source.ldap.adapterClass = edu.internet2.middleware.grouper.subj.GrouperJndiSource
7 ectApi.source.ldap.param.INITIAL_CONTEXT_FACTORY.value = com.sun.jndi.ldap.LdapCtxFactory
8 ing port 389 simple with TLS
9 ectApi.source.ldap.param.PROVIDER_URL.value = ldap://ldap-ad-aws.ldap.illinois.edu:389
10 ectApi.source.ldap.paramSECURITY_AUTHENTICATION.value = simple
11 ectApi.source.ldap.paramSECURITY_PROTOCOL.value = tls
12 ed to reset this to service account
13 ectApi.source.ldap.paramSECURITY_PRINCIPAL.value = CN=authman-subject-bind,OU=CITI-PM
14 ectApi.source.ldap.paramSECURITY_CREDENTIALS.value.elConfig = ${java.lang.System.getenv}
15 ectApi.source.ldap.paramSubjectID_AttributeType.value = uiucEduUIN
16 ectApi.source.ldap.paramSubjectID_formatToLowerCase.value = false
17 ectApi.source.ldap.param.Name_AttributeType.value = displayName
18 ectApi.source.ldap.param.Description_AttributeType.value = department
19 ectApi.source.ldap.param.VTLDAP_VALIDATOR.value = ConnectLdapValidator
20 ectApi.source.ldap.param.subjectVirtualAttribute_0_searchAttribute0.value = ${subjectUtil}
21 ectApi.source.ldap.param.sortAttribute0.value = sn
22 ectApi.source.ldap.param.searchAttribute0.value = samAccountName
23 
24 ATUS SECTION for searches to filter out inactives and allow
25 e user to filter by status with e.g. status=all
Push images to AWS
Stop and Restart Container

The following task may have been started by an automated process. If a task is started by a service, select Cancel and update the service to stop the task. Are you sure you want to stop the following task IDs in cluster default?

- 141e6fdd-a875-4ef2-a3d3-0501d62144da, startedBy=ecs-svc/9223370511271688923

Options:
- Cancel
- Stop
Grouper, Modified

The following table lists all groups in which Coleman, Erik C is a member.

<table>
<thead>
<tr>
<th>Folder</th>
<th>Group name</th>
<th>Membership</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Show: 50
Contact Us

- Keith Wessel (kwessel@illinois.edu)
- Erik Coleman (ecc@illinois.edu)
- David Riddle (ddriddle@illinois.edu)

Python module for AWS CLI login with Shib ECP: https://pypi.org/project/awscli-login/