Dockerized Shibboleth, the Holy Grail?

Carol Brothers  
Senior DevOps Engineer  
Email: carol.brothers@ucop.edu  
Phone: (510) 587-6224  
University of California, Office of the President  
300 Lakeside Drive, 12th floor, 12216  
Oakland, CA 94612

Steve Hunter  
Senior DevOps Engineer  
Email: steven.hunter@ucop.edu  
Phone: (510) 987-0138  
University of California, Office of the President  
300 Lakeside Drive, 12th floor  
Oakland, CA 94612
The Mission

- Move a production web application to the cloud (AWS in particular)
- Employee best practice design and operations
  - CD/CI
  - Infrastructure as code
  - Cloud services whenever possible
- Poster child app for future move of entire portfolio to AWS
The Application

❖ Infrastructure:
  ➢ Apache
    ■ mod_jk: tomcat connector
    ■ mod_shib: Shibboleth Service Provider plugin
  ➢ Tomcat

❖ Code:
  ➢ Java
    ■ Spring MVC, Spring Security, Hibernate

❖ Execution environment:
  ➢ Linux VM
  ➢ Hosted at SDSC
The Design

- Dockerize apache and tomcat
- Code pipeline
- Define as a CloudFormation template
The Problem

❖ Getting mod_shib working an configured properly inside a docker container
What is Docker?

❖ Packaging technology that allows OS, libraries, and application code to be layered together
❖ Container executes on any Docker engine
❖ Alleviates problems with environmental differences between systems, say, dev and prod
❖ Infrastructure includes repository to store containers, making them reusable
❖ All major open source projects have reference containers that you can start with, e.g. tomcat, nodejs, nginx, etc.
What is Docker?

- Containers defined by a Dockerfile, which lists the starting container and all the layers you wish to include in your container.
- You define networking, parameters, and startup scripts here as well.
What is Docker?

- Engine allows inter-container and container-outside networking
- This enables containers to be treated as building blocks
- Example: One container runs CDN app on Ruby on Rails, another Lucene as indexing against content
What is Docker?

FROM debian:stretch-slim
LABEL maintainer="NGINX Docker Maintainers <docker-maint@nginx.com>"
ENV NGINX_VERSION 1.17.1
ENV NJS_VERSION 0.3.3
ENV PKG_RELEASE 1~stretch

# forward request and error logs to docker log collector
RUN ln -sf /dev/stdout /var/log/nginx/access.log \
    && ln -sf /dev/stderr /var/log/nginx/error.log
EXPOSE 80
STOPSIGNAL SIGTERM
CMD ["nginx", ",g", ",daemon off;"]
AWS Docker Services

❖ Elastic Container Repository (ECR)
❖ Elastic Container Service (ECS)
  ➢ Entails running a full EC2 instance
❖ Fargate
  ➢ ECS as a service
    ■ No visible EC2 instances
    ■ Lower cost
    ■ Application more opaque
What is Shibboleth?

❖ is any custom or tradition, a phrasing that distinguishes one group of people from another. Shibboleths have been used throughout history in many societies as passwords, simple ways of self-identification, signaling loyalty and affinity, maintaining traditional segregation, or protecting from real or perceived threats.

❖ The modern use derives from an account in the Hebrew Bible, in which pronunciation of this word was used to distinguish Ephraimites, whose dialect used a differently sounding first consonant.
Shibboleth Single Sign-on and Federating Software

Shibboleth is an open-source project that provides Single Sign-On capabilities and allows sites to make informed authorization decisions for individual access of protected online resources in a privacy-preserving manner.

InCommon operates the identity management federation for U.S. research and education. Through InCommon, Identity Providers can give their users single sign-on convenience and privacy protection, while online Service Providers control access to their protected resources.
Dockerized Shibboleth, the Holy Grail?
AWS Services

DOCKER
❖ ECR
❖ ECS
❖ FarGate
❖ Auto Scale

CI/CD
❖ CloudFormation
❖ CodeCommit
❖ CodePipeline
❖ CodeBuild
❖ Cloud9

Infrastructure
❖ Route53
❖ Elastic Load Balancers
❖ RDS
❖ Secrets Manager
❖ Lambda
❖ Network
❖ CloudWatch
❖ S3
❖ Certificate Manager
❖ SES

Security
❖ IAM
❖ Config
❖ CloudTrail
❖ GuardDuty
❖ Billing and Cost

TOPIC  Dockerized Shibboleth, the Holy Grail?
Dockerized Shibboleth, the Holy Grail?
Dockerized Shibboleth, the Holy Grail?
SP is Service Provider is our app shib configuration
IdP is campus identity provider
InCommon is the metadata broker/coordinator

1. For different env/app, rename all ajsdev to ajsqa (dns entries) in:
   - sp/etc-httpd/conf.d/sp.conf
   - sp/etc-shibboleth/shibboleth2.xml

   ```
   <ApplicationDefaults entityID="https://ajsdev.ucop.edu"
   homeURL="https://ajsdev.ucop.edu/TestJSP/shibheaders.jsp"
   REMOTE_USER="epnn persistent-id targeted-id"
   signing="true" encryption="false">
   ```
2. Change main pages in sp/etc-httpd/var-www-html

3. Attributes in attributes.xml - request from your campus IdP to release specified attributes you need. For example, Shib-emailAddr, Shib-eppn, Shib-displayName that you will check for and use in your application.

4. Create Shibboleth ssl certificate by doing:
   sudo /etc/shibboleth/keygen.sh -f -h ajs.ucop.edu -e
   https://ajs.ucop.edu/shibboleth -o /etc/shibboleth -u shibd -g shibd
5. Modify your application to check the https header for the attributes you need.

- **Shibboleth RequestHeaderAuthenticationFilter**
  Handles for Shibboleth request headers to create Authorization ids.

- **ShibbolethLoginHandler**
  Interface for pre-login handling. These events occur after the Id is found, and before UserManager attempts a login of the user.

- **LoginHandler**
  Handles creation and updating of user account details when authenticating a user.
Dockerfile-asteroid-apache-shibd:

FROM centos:centos7
MAINTAINER Carol Brothers
RUN yum -y update \
    && yum -y install wget \
        /etc/yum.repos.d \
    && yum -y install httpd mod_ssl shibboleth \
    && yum -y clean all
COPY ucop_apache/sp/etc-shibboleth /etc/shibboleth/
COPY ucop_apache/sp/etc-httpd /etc/httpd/
COPY ucop_apache/sp/etc-httpd/var-www-html /var/www/html/
COPY ucop_apache/sp/httpd-foreground /usr/local/bin/
RUN chown shibd.shibd /etc/shibboleth/sp-cert.pem
RUN chown shibd.shibd /etc/shibboleth/sp-key.pem
RUN echo "SELINUX=disabled" > /etc/selinux/config
EXPOSE 443
CMD ["httpd-foreground"]
httpd-foreground

#!/bin/bash

# Apache and Shibd gets grumpy about PID files pre-existing from previous runs
rm -f /etc/httpd/run/httpd.pid /var/lock/subsys/shibd

# Start Shibd
/etc/shibboleth/shibd-redhat start

# Start httpd
exec httpd -DFOREGROUND
QUESTIONS?

Steve Hunter
Senior DevOps Engineer

Email: steven.hunter@ucop.edu
Phone: (510) 987-0138
University of California, Office of the President
300 Lakeside Drive, 12th floor
Oakland, CA 94612
Dockerized Shibboleth, the Holy Grail?
TOPIC: Dockerized Shibboleth, the Holy Grail?