InCommon Shibboleth IdP/SP Training - Overview
/Background

InCommon Trusted Access Platform

- The Trusted Access Platform (formerly known as TIER), an effort of Internet2, is "a community-driven, consistent approach to identity and access management."
- [https://www.internet2.edu/vision-initiatives/initiatives/trust-identity-education-research/](https://www.internet2.edu/vision-initiatives/initiatives/trust-identity-education-research/)
- The Trusted Access Platform delivers specialized packaging of these components:
  - Shibboleth IdP and SP
  - Grouper Group Management System
  - COmanage Registry and Collaboration Mgmt Platform
  - midPoint Provisioning System
- In development:
  - RabbitMQ messaging system

Shibboleth

- A popular open source implementation of the SAML specification.
- IdP, SP, EDS, MDA
- Developed by the Shibboleth Consortium
- [https://www.shibboleth.net/](https://www.shibboleth.net/)

SAML

- An international standard for federated/multi-domain SSO.
- Maintained by OASIS
- [https://www.oasis-open.org/standards#samlv2.0](https://www.oasis-open.org/standards#samlv2.0)

DevOps

- The blending of principles from software development into IT Operations and the building of a collaborative working relationship between the two teams.
- Operational people become more like developers; Developers become more operational
- "Infrastructure As Code"
- For example:
  - As a "new" sysadmin, I change my running machines by writing what amounts to code (in a Dockerfile, etc.) and then checking that into a code repository whereupon an automation system (Jenkins) will automatically build and test my machine, then, if successful, deploy it.

Containers

- A way of packaging an application/service?
- The evolution of VMs?
  - Similar idea, but "Look Ma - No Hypervisor!!"
  - And once you get used to that, "Look Ma, no OS!"
- How you run containers operationally is typically the job of a container orchestration system. There are many flavors of such things, ranging from entirely cloud-based, such as Amazon ECS/Fargate/EKS, to on-prem and hybrid solutions such as Docker Swarm, Kubernetes, Rancher, Marathon, and more. The world seems to be moving to Kubernetes (a product of Google), but it can be complicated, so just how you best run Kubernetes (cloud?) is still being evaluated...

Docker

- An ecosystem for building, packaging, and deploying applications using containers.
- Lots of new terms: Image, Container, Container Registry, Image Tags, Container Entrypoint, Volumes, Secrets, etc.
- Docker Swarm is a basic orchestration system that is built into the free community edition of Docker.
- Docker runs on most platforms.
- The 'docker-compose' utility makes it easy to bring up and tear down related containers (the settings are all defined in a file).

Cloud

The Shibboleth IdP and SP both run great in the cloud, but there are some things to consider:

- The IdP is not, by itself, everything involved in your SSO System. The IdP will talk to an authentication source(s) and perhaps a different attribute source(s). The communication path between them and the IdP should be considered, as well as the HA properties of the two environments.
- Likewise, for your SP. Where does its data come from/go to? How real time does it need to be?
- Your cloud environment will likely create certain constraints (or likewise, opportunities) with how you deploy your IdP/SP. For example, the use of secrets is something that tends to vary considerably between deployment platforms.