Mix & Match Federation for OpenStack
(or enabling an OCX)

George Silvis III
Team: MingYing Lu, Kyle Liberti,
Ankita Gupta, Jon Bell
Open Cloud eXchange (OCX)

- Multiple “partners” participate in implementing and operating cloud:
  - eXchange Service Providers (XSP)
- Each XSP determines how to charge for her services
- Customers can select and move between services
- Domain specific intermediaries:
  - provide customers with simple model
  - enable optimization
- Multi-sided marketplace
Feedback of community

- Developed series of blueprints on requirements, received extensive feedback...
- Architecture of OpenStack amenable to OCX model.
  - Independent services that all communicate through external API
- This might be a pragmatic approach to defense in depth.
- There be dragons there. This won't work but we can't tell you why.
- Our plan: Develop a proof of concept and present in Tokyo
- Allow user to request compute (Nova) from one provider and storage (Cinder) from another
Keystone-to-Keystone Federation

1) User authenticates with Keystone, gets token
2) User exchanges token for SAML assertion
3) User exchanges SAML assertion for new token
4) User makes API call to foreign Openstack
5) Nova checks that user's token is valid
Resource Federation, using K2K Federation

1) User authenticates, gets token
2) User makes Nova API call
3) Nova validates token
4) Nova exchanges token for SAML
5) Nova exchanges SAML for token
6) Nova makes Cinder API call
7) Cinder validates token
Challenges

- Underlying storage must be visible externally
- Granting access to only some of the user's resources
  - At the underlying storage layer (e.g. Ceph/RBD, ISCSI); changes required to offer different authorizations for different resources
  - At the Openstack layer so user doesn’t need to share everything
- Expanding this to all the services…
Tokyo Summit

- Design summit meetings:
  - Cross project meeting – strong agreement, but only Keystone team was there…
  - Nova – request to break up into smaller steps and quickly develop new specs
  - Cinder – described some missed edge conditions, strongest feedback is that has broader set of use cases, we should accelerate
  - Consensus that the storage security issues exposes existing important problems, e.g., a compromised Hypervisor, that OpenStack should address
  - Discussed with Netapp and Ceph teams technical approaches with their technology