Multiple Identities

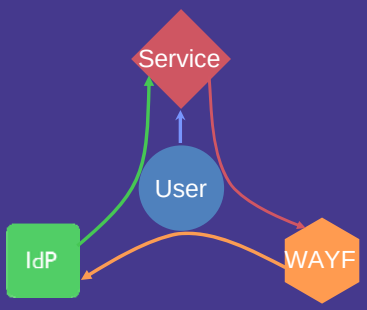
Automated installations of Shibboleth IdPs on Red Hat

Steve Holden
University of Brighton
steve@brighton.ac.uk
http://ns.brighton.ac.uk

What is Shibboleth?

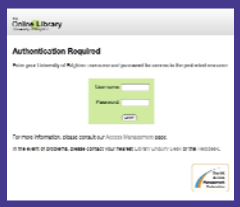
- Open standard allowing Single Sign-On (SSO) access to web-based resources
- Used to build a federation of trusted idproviders (IdPs) and service entity providers (SPs)
- Supports personalised content whilst maintaining user privacy

How does it work?



Institutional identities

idp.brighton.ac.uk



idp.bsms.ac.uk

Design decisions

- Shibboleth v1.3
- Use packages (less building)
- Red Hat approach
- Separate Tomcat instances
- Clean HTML, JSP and CSS

Components required

- DNS name and IP address
- Virtual interface (eg. eth0:1)
- Digital certificate for HTTPS
- Apache IP-based virtual host, listening on both 443 and 8443
- Local iptables rules for these ports
- Separate Tomcat instance (proxied by Apache)
- Separate Shibboleth application
- Distinct IdP authentication/authorisation
- Bespoke styling for its institution's "branding"

Automation (Kickstart)

- Kickstart (not Cobbler or Puppet)
- Shell scripts and functions
  - **create_virtual_nic** $IDP_HOST
  - **create_apache_ipbased_virtual_host** $IDP_HOST
  - **create_tomcat_instance** $IDP_HOST
- Template::Toolkit
  - Refactor HTML, JSP, CSS for easier templating

Automation (Shibboleth)

- Distinct, Red Hat-style directory paths
  - /etc/httpd/conf.d/idp.brighton.ac.uk.conf
  - /etc/sysconfig/idp.brighton.ac.uk
  - /etc/tomcat5/idp.brighton.ac.uk/
  - /var/log/tomcat5/idp.brighton.ac.uk/
- Shibboleth webapp and application
  - Modify build.properties
  - /usr/local/tomcat/instances/idp.brighton.ac.uk
  - /usr/local/shibboleth/idp.brighton.ac.uk/
  - Remove duplicate .jars, re-pack .war file
  - Double-check XML; run suite of *resolvertests*

Automation (site-specifics)

- Site identity (branding)
  - Prompted questions about support
- User identity (business logic)
  - *eduPersonTargetedID* attribute
  - *ScriptletAttributeDefinition* Java scriptlet generates *eduPersonAffiliation* attribute
  - Attribute Release Policy (ARP)

What I learnt

- Challenges
  - Steep learning curve
  - Disparate documentation
- Lessons
  - Documentation
  - Backup/restore v BMR Kickstart
- Irony
  - 10% Shibboleth, 10% OpenAthens, 80% EZproxy
  - Many SPs don't support multiple scopes

Future

- Cobbler
- Puppet
- Shibboleth v2
- Local SPs, internal federation

Questions and Thanks

- Bear in mind I'm no expert in Shibboleth, Tomcat or Kickstart!
- Thanks to:
  - Colleagues at the University of Brighton
  - Colleagues at the University of Sussex
  - The UK Federation
  - The Shibboleth developers