Shibboleth: Installation & Setup

Nate Klingenstein
Internet2
ndk@internet2.edu

国立情報学研究所

２００７年６月１日

Installation Process & Requirements

- Setting up a Shibboleth IdP
    - Moving from testing to real use
- Setting up a Shibboleth SP
    - Moving from testing to real use
- Federation
- Again, this will get technical

Federated Identity Solutions from Vendors

- I want to encourage you to use all federated identity, including vendor products
  - EuroCAMP 2007 Panel Discussion
- Oracle Identity Federation 11gR2+ supports native Shibboleth
- Others, if SAML-compliant, can interoperate

Why Shibboleth?

- Free
- Open-source
- Standards-based
- Designed for use with big federations
- Works well with products from many vendors
- Very large deployment worldwide

Getting Ready to Install

- The hard part is the rest of the identity management system
  - Attributes
  - Enterprise authentication
  - Provisioning
- Shibboleth itself is much easier

Standard Shibboleth IdP Installation Procedure

- Install Tomcat
  - 4.0.x+
- Install and configure mod_jk or mod_ajp_proxy
- Install Shibboleth
  - Hit “Return” 4 times

Standard Shibboleth IdP Installation Procedure

- Connect an existing institutional authentication source to Apache
  - Or create one if needed
- Test with TestShib
  - Join the test federation
  - Get keys, certificates, and configuration made for you
  - Access http://sp.testshib.org to test

Standard Shibboleth IdP Installation Procedure

- Connect to your attribute sources
  - LDAP or SQL Database are easiest
- Test with others
- Entire process takes 1-4+ hours, mostly depending on how well you know Apache and Tomcat
- https://spaces.internet2.edu/display/SHIB/JKIdPInstall

Making the IdP ready for real use

- The Shibboleth IdP is extremely fast
  - One decent machine can handle 50,000+ logins/day and 50 logins/sec
- Penn State wanted to use Shibboleth for all its students to use Napster
  - Installed 5 very big Blade servers for IdP’s
  - No noticeable CPU load on any machine
  - Only needed 2 at most for very large access

Making the IdP ready for real use

- Multiple machines is necessary for backup in case one dies
    - Load-balancing can be done statelessly by cryptographically encoding information
    - Or more heavily through HA-Shib
- Almost any operating system is fine
    - But installing on Windows is probably hardest

Getting Ready to Install a Shibboleth SP

- SP must be installed on every machine hosting Shibboleth-protected resources
    - Unless you like reverse proxies
- Installation on Fedora-based Linux and Windows is very easy
    - RedHat, CentOS, etc.

Getting Ready to Install a Shibboleth SP

- Installation on Mac OS X and other Linux distributions is also pretty easy
- Installation on Sun Solaris can be easy, or very very hard
  - The XML-processing dependencies

Shibboleth SP Install by RPM/Installer

- Download RPMs/Installer
- Run RPMs/Installer
- Restart web server
- Start shibd
- Test with TestShib
- Binaries for Mac OS X are a little more complicated to install

Shibboleth SP SRPM's

- Source RPM's; like an RPM, only instead of binaries, it builds from source code
  - Works in more environments, but a little harder to use
  - Directions available for SuSE, Fedora, and Debian

Shibboleth SP: Build it from Source

- It’s easy on some platforms and impossible on others
- gcc 3/4 on Linux and Mac OS X
- Solaris GCC is unsupported; Solaris CC (usually) works
  - It’s the dependencies that are hard
  - Solaris 2.8 binaries are available

SP Installation

- Again, very little load; if it can run your webapps, it can run Shibboleth to protect them
- Total time is usually between 2-5 hours

Making a Shibboleth SP ready for real use

- Backup is very hard to do on the web
  - You have one chance; if it fails, the browser gives up, and you lose
- Clustering is easier, but usually done by the applications
  - Much better session management in Shibboleth 2.0 SP

Making your New Providers Talk Together

- If they both joined TestShib successfully, it’s very easy

1. Download fresh metadata
2. Tell the SP to choose your IdP to login
3. Tell your IdP which information to send to your SP

Creating a Federation

- Technical things
- Policy things

Technical things a Federation can do

- Metadata
- WAYF/DS Service
- Attribute definitions
- Attribute release and acceptance guidelines
- PKI keys and certificates

Policy things a Federation can do

- Identify the authoritative servers for each organization
- Ask important organizations to join
- Tell people what SP’s are available
- Helping with disagreements, liability
- Set basic rules for attribute use

International Federation

- There are working groups to connect together national federations
  - “Inter-federation” or “Confederation”
- NREN’s have MoU’s with each other
  - AIRC is the Japanese partner of Internet2
- 日本の主要大学と研究機関による、日本先進インターネット研究コンソーシアム。アメリカのInternet 2を推進するUCAID（ユーケイド）の実験ネットワークとも相互接続して共同研究を進めています。

Opportunities for Japan

- This is something you know better than I can
- Good identity management makes research great
  - More sensitive data
  - More researchers
  - More international collaboration

Opportunities for Japan

- Shibboleth- and SAML-Based SSO on individual campuses
- Japanese testing federation
- Research into NAREGI integration
- Contracts with individual content providers
- International team support

Deployment Resources

http://shibboleth.internet2.edu/

shibboleth-users@internet2.edu

http://spaces.internet2.edu/display/SHIB