Identity Management and SSO for jboss.org Community Systems

Vlastimil Eliáš
JBoss Community Team

17.2.2012
Red Hat Developer Conference, Brno, 2012
Agenda

• Something about JBoss Community
• jboss.org user accounts management
• SSO Login server for jboss.org
• CAS SSO protocol details
JBoss Community

- Open Source middleware
- Java and other JVM-based languages
- Led by Red Hat
- 150+ OSS projects, not only JBoss Application Server ;-)
- www.jboss.org
JBoss Community Team

- Red Hat's dedicated team to support JBoss Community
- Part of team are Software engineers and System administrators dedicated to develop and operate systems for Collaborative Open Source software development
- HW already provided by Red Hat
Main jboss.org Systems

- CMS for Project web pages – www.jboss.org
  - Magnolia CMS
- Development Forums, Wiki, Blogs – community.jboss.org
  - SBS by Jive Software
- Issue Tracker & Agile Project Management - issues.jboss.org
  - JIRA with GreenHopper by Atlassian
- Documentation Editor - docs.jboss.org
  - Confluence by Atlassian
- Source Code Repositories – svn.jboss.org
  - Subversion
- Source Code Analysis and Reviews – source.jboss.org
  - FishEye with Crucible by Atlassian
- Maven Repository – repository.jboss.org
  - Nexus by Sonatype
- and the many others
jboss.org User Account

• Self-registration for jboss.org user accounts
• Many services need the user accounts
• Centralized system for user profile and authentication data management
  – User: Register (email validation), Edit profile, Change password, Forgot my username, Forgot my password
  – Admin: Search user, Edit user, Disable user, Delete user
User Profile Data

• Shared user profile data
  – Username
  – Full name
  – Email
  – Avatar image
  – (Password)

• Extra user profile data per service
  – UI preferences, Notification settings, ...
  – Managed by each service
Authorization

• No centralized solution for authorization
• Each service uses its own authorization system
  – User groups
  – User roles
  – Permissions
• Centralized user roles/groups management complicated due
  – inconsistent projects/subprojects structures
  – differences in distinct services authorization systems
User Profile Sharing Architecture

• Shared user database
• Custom authenticators for services
  – Create/update profile record in service's DB
  – Check password (login, RPC calls)

jboss.org services
SSO Login System Requirements

- Login once, access all services
- Web technology (http/s)
- Subdomains used (*.jboss.org)
- Support of various web browsers
- Simple extensibility of login flow (postlogin hooks)
- Simple implementation into services
- Simple HA cluster
- “Remember me” feature
Central Authentication Service

- Authentication system originally created by Yale University
- Open-source Java server component
- Library of clients for Java, .Net, PHP, Perl, Apache and others
- Open and well-documented protocol + SAML support
- http://www.jasig.org/cas
SSO Login System User GUI

- sso.jboss.org
SSO Login System Admin GUI

- Audit log browser
- System informations
CAS SSO Protocol Details

1: Request to SP 1
   1.1: Request URL requiring login
      1.1.1: Check local logged in - NO
      1.1.2: Send redirect for Auth request to IP
      1.2: Auth request to IP
      1.2.1: Check globally logged in - NO
      1.2.2: Send Login page
      2.1: Submit credentials
      2.1.1: Establish global login session
      2.2: Send IP reply to SP 1
      2.2.1: Check auth token
      2.2.2: Perform local login for session
      2.2.3: Serve originally requested resource
   1.2: Show global login page
   2: Insert credentials

3: Show resource
CAS SSO Protocol Details

• **Gateway mode**
  – Login form is not shown to user if SSO session is not established
  – No service ticket returned to SP in this case
  – Useful for SP allowing anonymous access

• **Renew mode**
  – Login form is always shown to user
  – Useful for SP not participating in SSO due sensitive data
Questions & Discussion

?  

Thank you!