

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

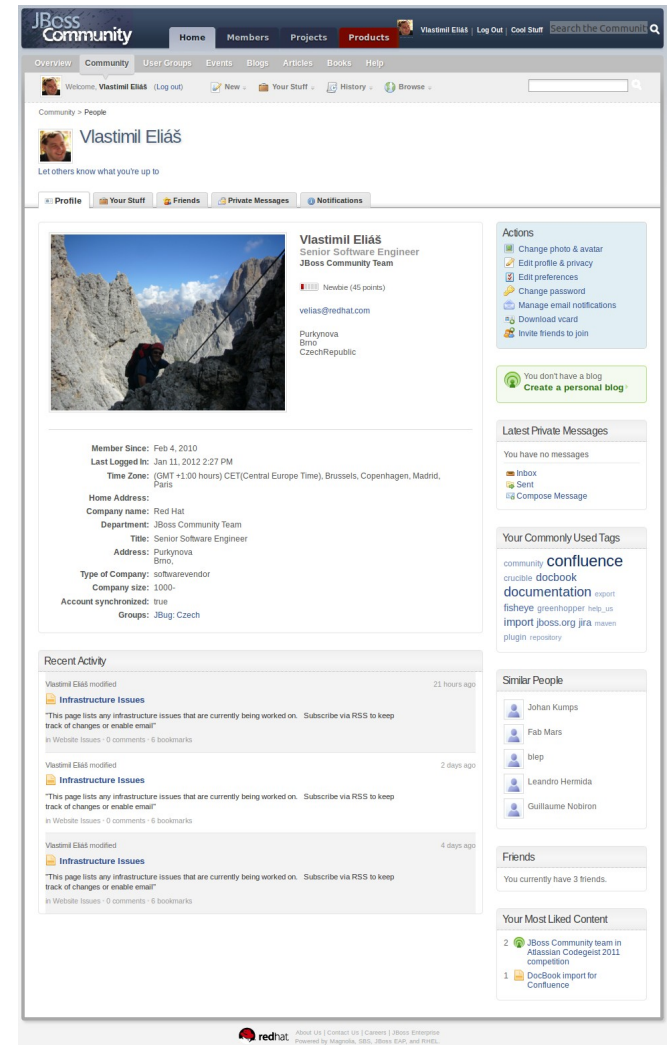
jboss.org User Account

- 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



The screenshot shows a user profile page on the JBoss Community website. The user is Vlastimil Eliáš, a Senior Software Engineer at the JBoss Community Team. The profile includes a profile picture of a person climbing a rock face, a bio, and various statistics like member since (Feb 4, 2010) and last logged in (Jan 11, 2012). There are also sections for recent activity, similar people, friends, and most liked content. The page is cluttered with navigation links and search bars.

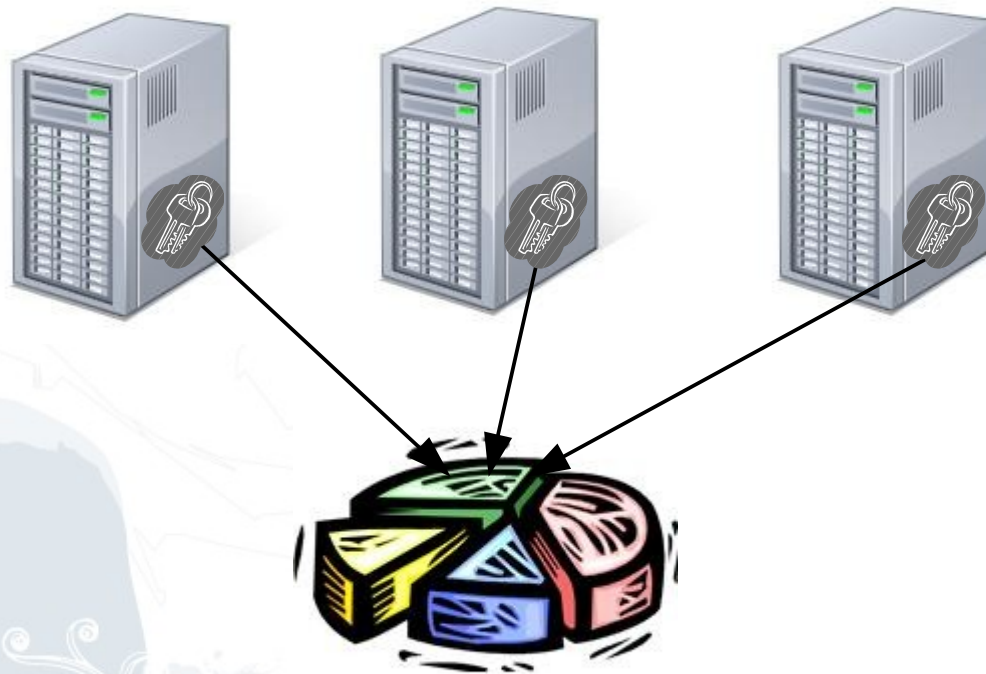
Authorization

- 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

JBoss Community Login

Username:

Password:

Remember me

Don't have an account?

Having trouble logging in? [I forgot my password.](#) | [I forgot my username.](#)

If using a public computer please Log Out and Close your browser when you've finished.

SSO Login System Admin GUI

- Audit log browser
- System informations

Manage Services View Statistics **Audit Log View**

Audit Log View

Date from: Date to:

Action:

- AUTHENTICATION_SUCCESS
- AUTHENTICATION_FAILED
- TICKET_GRANTING_TICKET_CREATED
- TICKET_GRANTING_TICKET_NOT_CREATED
- TICKET_GRANTING_TICKET_DESTROYED
- SERVICE_TICKET_CREATED
- SERVICE_TICKET_NOT_CREATED
- SERVICE_TICKET_VALIDATED
- SERVICE_TICKET_VALIDATE_FAILED

Service:

- JBoss.org JIRA (<https://issues.jboss.org/>)
- JBoss.org Confluence (<https://docs.jboss.org/author/>)
- JBoss.org FishEye (<https://source.jboss.org/>)
- JBoss.org SBS (<http://community.jboss.org/>)
- JBoss.org SBS <https://community.jboss.org/>)
- JBoss.org SSO server management application (https://sso.jboss.org/services/fj_acegi_cas_security_check)
- JBoss.org Planet (<http://planet.jboss.org/>)
- JBoss.org Planet <https://planet.jboss.org/>)
- JBoss.org website (<http://www.jboss.org/>)
- JBoss.org website <https://www.jboss.org/>)
- Hibernate website (<http://www.hibernate.org/>)
- Hibernate website <https://www.hibernate.org/>)

Username: Ticket:



Number of records found: 521

Date	Action	Username	Service
16.2.2012 4:46:18	SERVICE_TICKET_NOT_CREATED		https://community.jboss.org/message/595813
16.2.2012 4:46:11	TICKET_GRANTING_TICKET_NOT_CREATED	maeste	
16.2.2012 4:46:11	AUTHENTICATION_FAILED	maeste	
16.2.2012 4:45:56	TICKET_GRANTING_TICKET_NOT_CREATED	maeste	
16.2.2012 4:45:56	AUTHENTICATION_FAILED	maeste	
16.2.2012 4:45:51	TICKET_GRANTING_TICKET_NOT_CREATED	markus.feber	

View Statistics

Current cluster node: sso01 at sso.jboss.org (sso.jboss.org) running on Apache Tomcat/6.0.35

Runtime Statistics

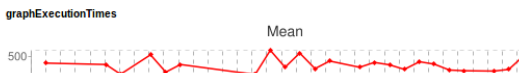
Property	sso01	sso02
Cluster node	sso01	sso02
Deployed version	1.4 (based on CAS 3.4.11)	1.4 (based on CAS 3.4.11)
CAS Ticket Suffix	jboss-org-sso	jboss-org-sso
Server Start Time	Wed Feb 15 06:52:46 EST 2012	Wed Feb 15 06:57:18 EST 2012
Uptime	0 days 21 hours 51 minutes 8 seconds 292 milliseconds	0 days 21 hours 46 minutes 41 seconds 487 milliseconds
Memory	68 MB free  130 MB total	75 MB free  128 MB total
Maximum Memory	227 MB	227 MB
Available Processors	2	2

Ticket Registry Statistics

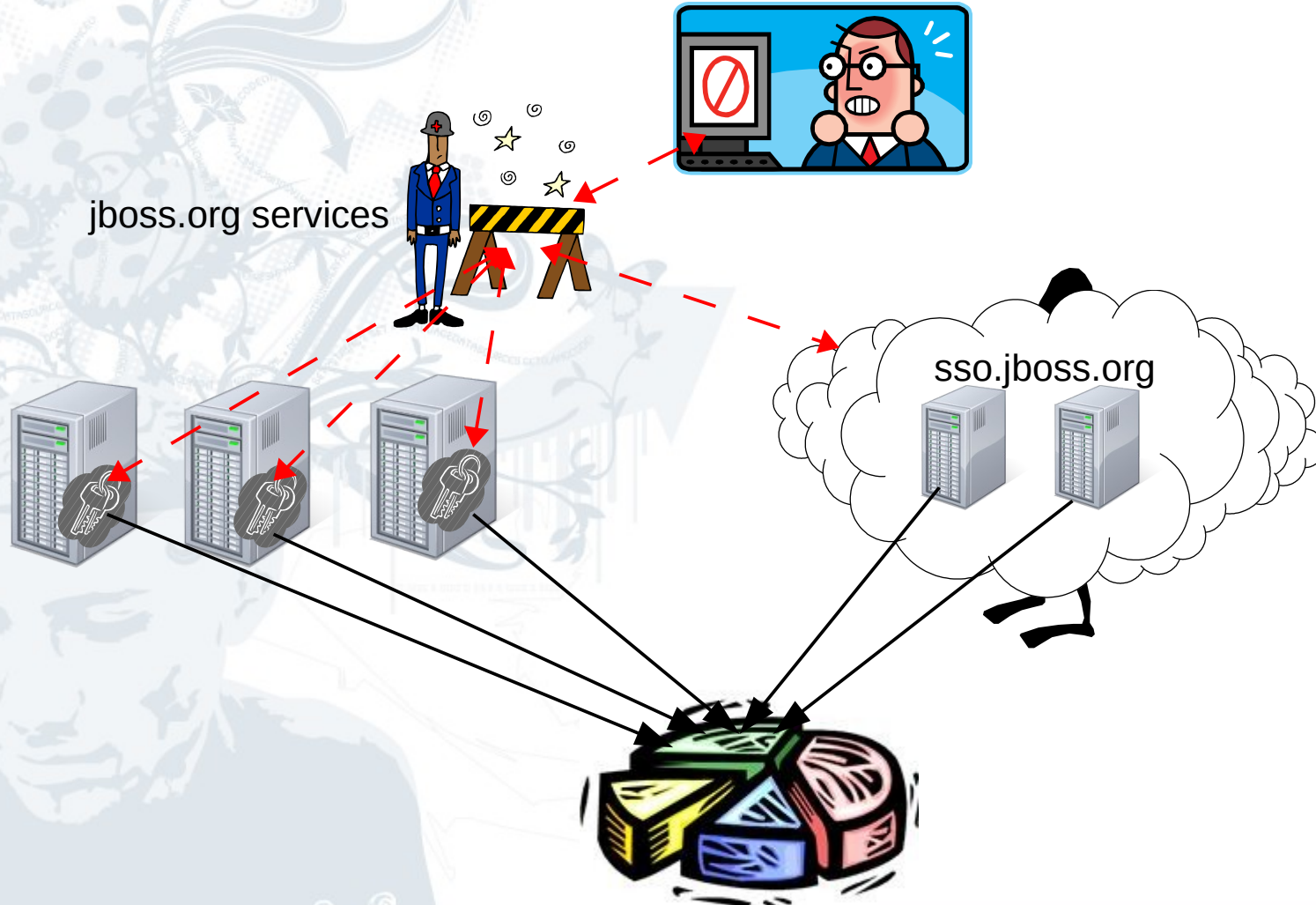
Property	Value
Unexpired TGTs	322
Unexpired STs	0
Expired TGTs	4
Expired STs	0

Performance Statistics (from current cluster node only)

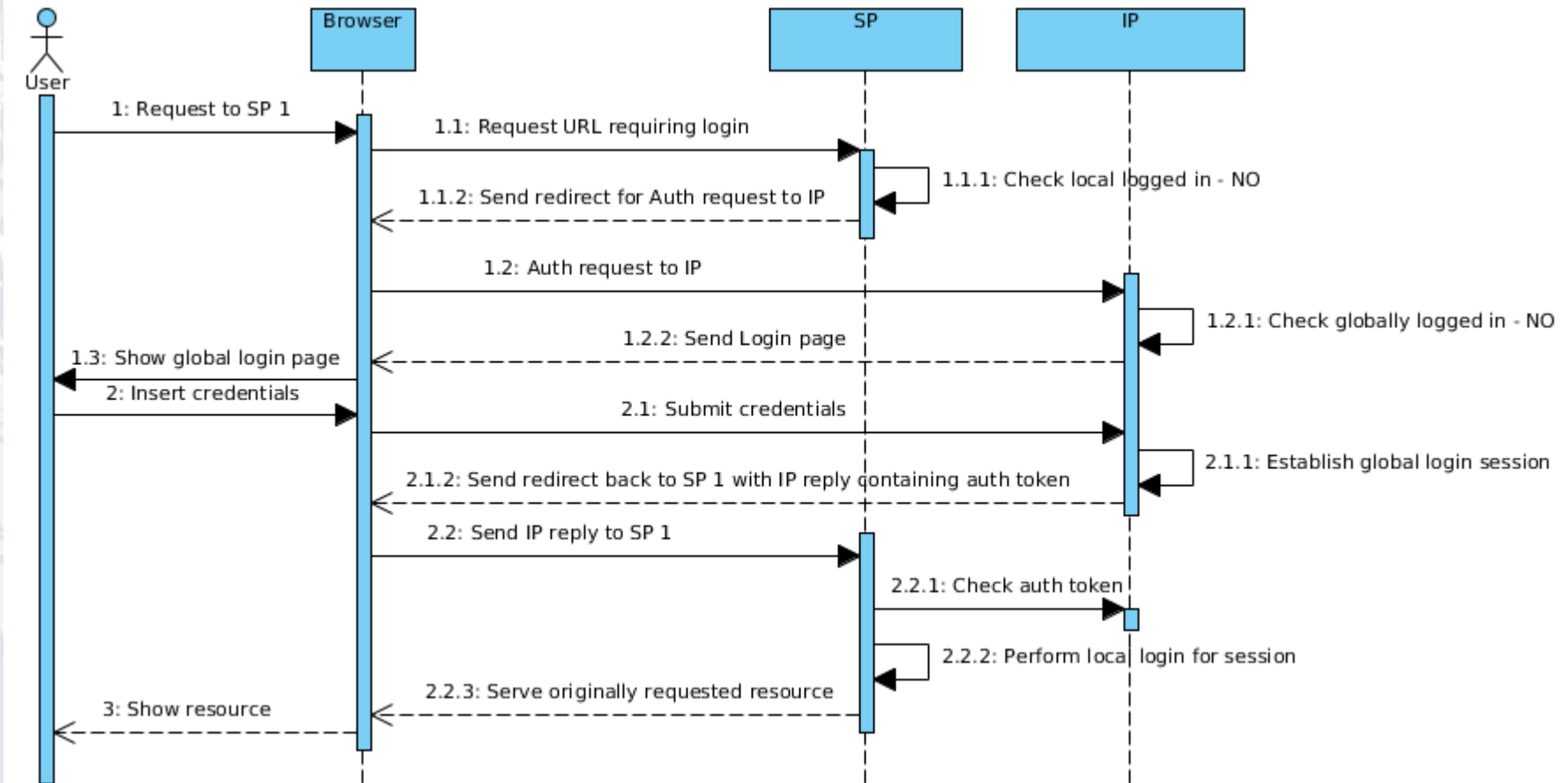
graphExecutionTimes



SSO Login System Architecture



CAS SSO Protocol Details



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!

JBoss Community