



PALAMIDA™

Application Security for Open Source Software

The Hot 25: Proven Open Source Projects to Cut Development Costs Today

Theresa Bui Friday, Palamida
Joshua Drake, PostgreSQL
Rick Hillegas, Apache Derby
Greg Olson, Olliance Group

January 29, 2009

Agenda

- **Palamida, Theresa Bui Friday**
 - Open Source Survey
 - Top 25 Open Source Projects
- **PostgreSQL, Joshua Drake**
 - About PostgreSQL
 - Community and Contributors
 - Development Process and Contributors
 - Use Case
- **Apache Derby, Rick Hillegas**
 - About Apache Derby
 - Community and Contributors
 - Development and Release Process
 - Use Case
- **Olliance Group, Greg Olson**
 - Best Practices for Expanding Your Open Source Use

Theresa Bui Friday
VP, Product Marketing - Palamida
theresa@palamida.com

Survey: 2009 IT Spending Outlook - Impact on Open Source and Security

- **Survey was conducted online to check “pulse” of the impact of the economy on possible open source use in 2009**
 - Online survey
 - Not meant to be comprehensive study
- **Sent to medium to large organizations across multiple industries**
- **Survey respondents were executive-level managers in the area of IT, engineering and security**
- **~3600 surveys sent with a an almost 5% response rate**
 - Multiple industries, heavy response in financial services and insurance

Key Findings

- **73% of organizations expect their IT budgets to decrease either moderately or significantly in 2009.**
- **Organizations are still somewhat reluctant to adopt open source in 2009 even in the face of cutbacks: 54.8% say they will not and 45.1% say they “absolutely will” or considering.**
- **78.7% of organizations cite “cost” as the #1 perceived benefit of open source software use, with time savings and flexibility a distant 2nd and 3rd.**
- **62.7% of organizations believe that open source software quality and functionality are either the same or almost the same as commercial counterparts.**
- **50% of respondents cite “security” as #1 concern around open source use, with support costs and intellectual property risks rounding out the top 3.**

Top 25 Open Source Projects to Use for 2009

25 Hot Open Source Projects You Should Be Using Now to Save Money

- **Development Tools**

- NetBeans
- Eclipse
- JUnit
- httpunit
- PMD
- Valgrind
- FindBugs

- **Database/Mapping Tools**

- Hibernate
- SQLite
- Apache Derby
- PostgreSQL
- *MySQL*

*(open source **product** run by Sun Microsystems)*

- **Utility Classes**

- zlib
- libpng
- FFmpeg
- Freetype

- **Reporting and Charting**

- JFreeChart
- Velocity
- Pentaho Reporting
- JasperReports

- **Web 2.0**

- Prototype
- script.aculo.us
- Direct Web Remoting
- Yahoo! User Interface
- jQuery



Joshua Drake
President, US PostgreSQL
Director in the Public Interest
jdrake@postgresql.org

History and Community

- **Initiated as a research project at University of California, Berkeley.**
- **Founded in 1986 by Michael Stonebraker as postgres (after Ingres)**
- **In 1995 became Postgres95**
- **Shortly thereafter became PostgreSQL which started at v6.0**
- **Community is meritocracy based (the work you do, not the money you pay is the qualifier)**



Development process

- **Distributed development**
 - Developers all over the world
 - Approximately a dozen committers
 - Hundreds of contributors
 - Anyone can submit a patch, not all are accepted
 - Meritocratic model ensures contributors push direction and quality of project
- **Quality is job 1.**
 - Averages .041 bugs per 1000 lines of code (has 990k lines of code)



Version updates and security

- Major updates released ever ~ 18 months
- Major releases are supported for ~ 5 years
- Current major release is 8.3 (8.4 is about to go Beta)
- New features do not go into past release, stability first.
- Security releases are handled by security team (verify, fix, pass to packagers). Packagers handle delivery of product.



Use Case: Skype

- Internet collaboration and telecommunications (VOIP)
- <http://www.skype.com/>
- Primary database
- Highly distributed
- Plans on reaching 1 billion users



Use Case: The General Why

- **Quality Code**
 - Coverity shows .041 errors per 1000 lines of code over 990,000 lines of code
- **Longevity**
 - Developed in one fashion or another since 1986
- **Community**
 - Large and international community
- **No primary commercial controller**
- **License: BSD**



Rick Hillegas

Java DB Technical Team Lead - Sun Microsystems

Apache Derby

richard.hillegas@sun.com

Agenda

- **History and Community**
- **Development Process**
- **Security and Updates**
- **Use Case**



History and Community

- **Overview**
- **History**
- **Community**



Overview

- **Full-featured, compact RDBMS**
- **Easy to setup**
- **Runs embedded or client/server**
- **Free via the Apache license**
- **Widely distributed:**
 - Java 6 JDK
 - Glassfish app server
 - Ubuntu component



History

- **Began as Cloudscape (1996)**
- **Acquired by Informix (1999) then IBM (2001)**
- **Open-sourced as Apache Derby in 2004**



Community

- **20 committers**
 - mostly from Sun and IBM
 - a couple wildcats
- **Courteous, consensus-based decision making**
- **All code donated to the community: no forks**
- **Active user list, rich user docs and wiki**



Development Process

- **Releases**
- **Tests**



Releases

- **Users**
 - Log issues
 - Script reproducible cases
 - Lobby for features
- **Functional specs written for big features**
- **Cadence**
 - Feature releases about once every 9-12 months
 - Maintenance release 3-6 months later
 - Patch releases as needed
 - By community
 - By Sun and IBM



Tests

- **Per check-in**
 - Minimum check-in barrier of regression, stress, and upgrade tests
 - New tests for all bug fixes and feature increments
- **Nightly: performance tests**
- **Weekly: large data volume tests**
- **Per release: long-running tests**



Security and Updates

- **Security overview**
- **Focus**



Security Overview

- **Java Security**
- **Pluggable authentication**
- **Coarse-grained authorization levels**
- **Fine-grained SQL access controls**
- **Database encryption**
- **SSL/TLS encrypted network traffic**
- **See whitepaper:**
 - *<http://developers.sun.com/javadb/reference/whitepapers/index.jsp>*



Focus

- **Past several releases invested heavily in**
 - Performance
 - Security
- **Data integrity issues get quick community action**
- **For serious problems**
 - Community produces an emergency release
 - Sun and IBM roll up bug fixes into patch releases
- **Security problems are chiefly usability issues**
- **Private mailing list for sensitive matters**



Use Case: Paper Cut NG

- **Printer management: <http://www.papercut.com/>**
- **Monitors/enforces usage and quotas**
- **Commercial software**
 - 10,000s of schools, universities, and businesses
 - 60+ countries
- **90% of customers stick with Derby**
 - 7% to SQL Server, 2% to Postgres, 1% to Oracle
- **100s of concurrent connections per server**
 - Live backups
- **See <http://www.papercut.com/anonftp/pub/open-source/apache-derby/ApacheDerbyAJUGPresentation.pdf>**



Summary

- **Full-featured, compact RDBMS**
- **Easy to setup**
- **Free via the Apache license**
- **Broad array of defences against security threats**
- **Courteous, consensus-based community**
- **Feature releases about once every 9-12 months**



olliance

group

Greg Olson

Partner

Olliance Group

golson@olliancegroup.com

Olliance Group

- **The leading independent open source business and strategy consulting firm whose mission is to help clients capitalize on the strategic, technological, and financial benefits of open source software.**
- **Our Open Source IP Management Practice helps clients understand the value and impact of open source software and develop strategies and policies that realize the productivity benefits while managing potential risks.**
 - Extensive research into industry best practices
 - Real world experience addressing open source management issues with scores of firms from small to large
 - Open source software use and licensing strategies
 - Policies
 - Processes

olliance

group

Open Source Saves Money

- **Multiple dimensions of proven savings**
 - The software is free
 - Working code speeds development and time to market
 - Code tested by communities and broad use reduces problems throughout the whole software lifecycle
 - Open approach improves security
 - Ability to modify and participate in a community eliminates roadblocks and impasses

olliance

group

But There Are Also New Perils

- **Several dimensions of OSS use can elevate risk and lifecycle costs**
 - Unmanaged acquisition
 - Not all OSS is high quality
 - Not all OSS is supported by an active community
 - Multiple groups acquiring the similar code from multiple sources
 - Combinatorics
 - OSS stacks come from different sources
 - Coordination of versions and dependencies is critical
 - The self-service support model
 - How do you stay on top of fixes?
 - Bug fixes
 - Security vulnerabilities
 - Is maintenance shared across all users in the company?
 - License compliance (for re-distributors)
 - Knowing what must be done to comply and doing it efficiently
 - Legal exposures
 - Documenting OSS and compliance requirements for customers
 - Lack of indemnification
 - Some code is risky, some is not
 - Where is it cost effective to acquire?

olliance

group

Managing OSS

- **Proven techniques and tools are available to manage open source to maximize savings and minimize risk**
 - A clear, succinct policy that matches your business objectives
 - A well defined process that fits your existing development practice
 - An implementation that facilitates productivity (instead of just adding bureaucratic overhead)
 - Education for developers on how to use OSS to advantage
- **Good tools are critical**
 - Finding and qualifying OSS
 - Functionality and documentation
 - Community health
 - License information
 - Know what OSS you are using
 - Code scanning
 - Auditing
 - Automatically check for security vulnerabilities
 - Security vulnerability scanning
 - Facilitate implementation of the policy and process
 - Flexible web-based workflow

olliance

group

Taking Advantage

- **Open Source can save Engineering expense and time**
- **... but its use entails new issues that must be managed**
- **By employing proven tools and practices you can**
 - Maximize productivity
 - Reduce engineering expense
 - Manage risk

olliance

group

Q&A

Thank You!

Today's Speakers:

Theresa Bui Friday, Palamida, theresa@palamida.com

Joshua Drake, PostgreSQL, jdrake@postgresql.org

Rick Hillegas, Apache Derby, richard.hillegas@sun.com

Greg Olson, Olliance Group, golson@olliancegroup.com