

OSS For Financial Services Sites

Richard Rosa

Debt Resolve Inc.

rich@richrosa.com

rrosa@debtresolve.com

June 15, 2006

Overview

- Introduction
- My Background
- Technology Choices / Tools
- Operational Issues
- Data Transfer / eCommerce
- Security
- Financial Rationale / Acceptance
- Pitfalls and Considerations

Introduction

- Building a Enterprise Quality Financial Services Website using entirely open source tools is an excellent choice and has many advantages
- Financial Services companies either already use open source or want to
- Open source has grown up, is better understood by the mainstream, and is here to stay

My Background

- 9 years of banking in NYC
- President of Consulting Firm
- Director of Online Operations – 1800Flowers.com
- Senior Director of Technology – Scholastic Corp.
- President / Chief Technology Officer – DebtResolve Inc.

Technology Choices

- To build financial services site, there are many development platforms to choose from. Some choices are:
 - .Net
 - Java
 - PHP
 - Perl
 - Others

Platform Considerations

- Ease of development
- Availability of Developers
- Strength of toolset
- Availability of add-ons
- Stability and scalability
- Cost
- Vendor Support

Application Platform Choices

- Each of the major platforms can do the job, but each has specific advantages or disadvantages
- Poor coding defeats the advantages of a good platform
- A platform choice drives the much of the technical strategy

.Net

- Strengths
 - widely used
 - many developers
 - has added OOP features
- Weaknesses
 - vendor lock-in
 - toolset is proprietary
 - price is cheap early, expensive later

Java / J2EE

- Strengths
 - widely used
 - many developers
 - excellent toolset
 - strong OOP
- Weaknesses
 - vendor lock-in
 - high cost of development
 - scale issues if coded improperly
 - platform is generally expensive

PHP

- Strengths –
 - strong, free development tools
 - ease of development
 - vendor neutral
 - OOP in there if you choose to use it
 - even using commercial tools, platform is inexpensive
- Weaknesses –
 - good developers are harder to find
 - less vendor support
 - OOP in PHP4 needed improvement

Perl

- Strengths
 - free development tools
 - ease of development
 - vendor neutral
 - mature
- Weaknesses
 - developers are harder to find
 - less support
 - not enterprise friendly
 - OOP not always implemented

Why we chose PHP

- Ease of development
- Strong toolset, especially prototyping
- Limited budget
- Available expertise
- Negative experiences with other tools
- No immediate need for a significant budget or vendor support

Why we chose PHP

- Availability of commodity hardware
- Platform independence
- Decent development tools and aids
- Well documented online
- “All in” cost to develop was agreeable
- Our clients are losing their technology biases to a “superior platform”

Financial Differences using PHP over rivals

- Application server is free if you want it to be
- Vendor support if required, is much cheaper than alternatives
- Strong development tools are freely or cheaply available
- PHP developers earn less on the average than rivals (is this changing?)

Some PHP pitfalls

- Enterprise integration could be stronger (i.e. Messaging, Web Services)
- As PHP continues to mature, integration with different middleware applications will improve
- XML support is better in other platforms
- Strong, local developers are harder to find

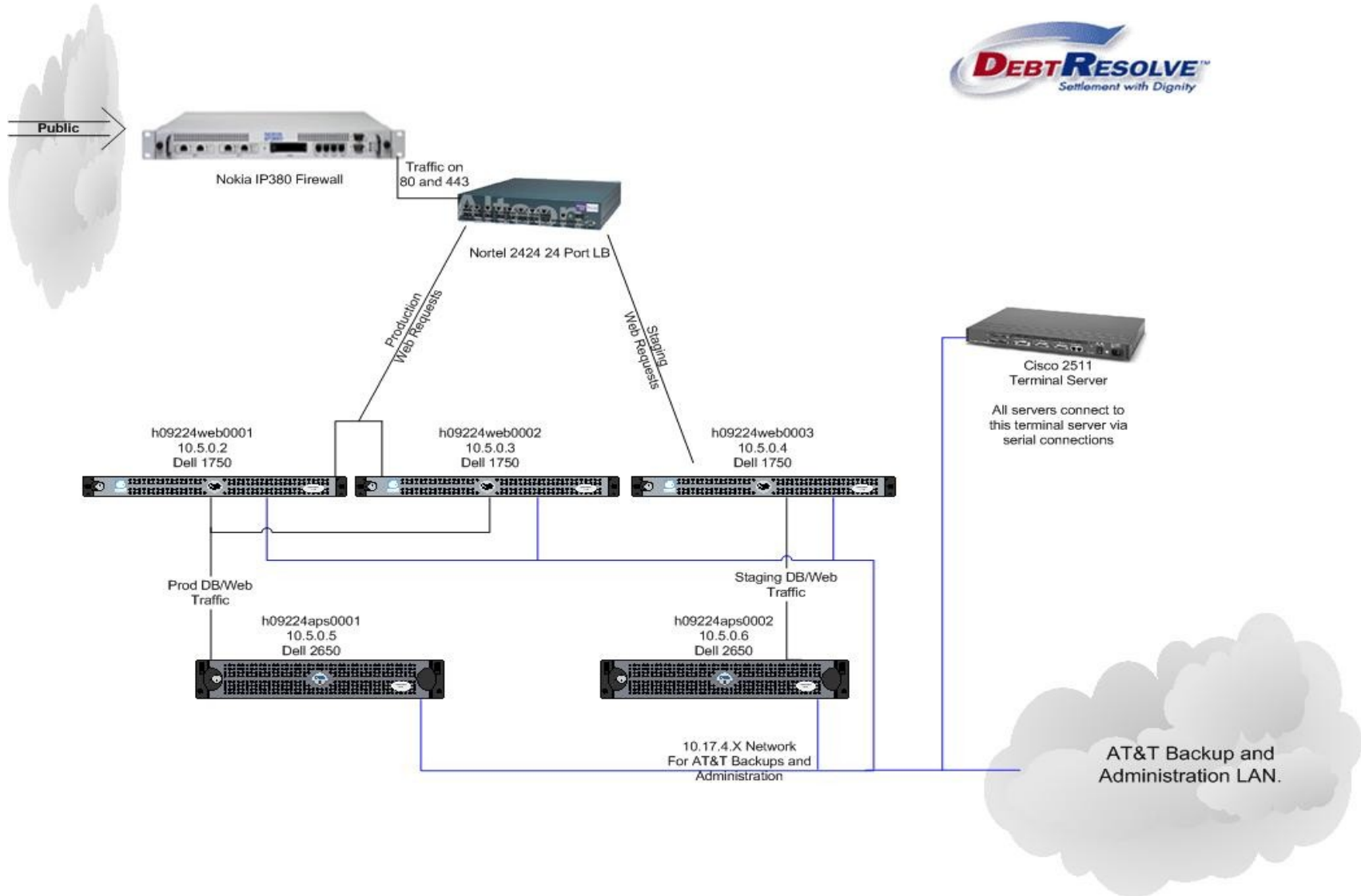
Our Operating Platform

- 100% Linux RedHat Enterprise 4.0
 - Enterprise quality Linux, recognized and used by many financial institutions
- MySQL 4.1.x
 - Perfect for a modest financial services site that does not require the advanced features of better known commercial databases
- PHP 4.4.x
- Apache 2.0.x
 - Recognized as the world-standard web server
- OpenSSL
 - Manages SSL certificates for secure access

What do we need to make PHP/MySQL work?

- Modest hardware
 - Dell 1750's for web servers
 - Dell 2650's for databases
- Persistent load balancing / session management
 - Nortel Alteon 2424 load balancing
 - Persistent load balancing with ADODB and MySql
- Database redundancy
 - Using built-in MySql replication tools
- Monitoring tools
 - Enterprise monitoring tools provided by the hosting provider supplemented by open source home-grown monitoring tools
- Development Site
 - A near-exact replicate of the production site hosted at our White Plains office. A UK site is in the works.

Our infrastructure



PHP Packages in use

- ADODB 4.90
 - Database abstraction layer
- PEAR
 - XML
 - SOAP
- phpMailer
- Smarty
 - Excellent templating engine
- FormGeneral
 - Internally developed MVC package

PHP Development Tools in use

- Zend Studio 5.x
- Mysqlfront 3.2
- Sqlyog 5.14
- Vi
- Crimson Editor

PHP and Enterprise Data Integration

- PHP contains the tools to create a data integration framework
- SOAP and Web Services are fairly easy to setup, but haven't always interoperated perfectly with other platforms
- Other structured data formats can be transported and processed easily
- Integration with Enterprise middleware and messaging needs work (Websphere MQ, JMS)

eCommerce

- There are many tools available to accept and process payments available on the internet
- Nearly every payment platform provides PHP examples or modules to integrate payments
- Many examples are available in other open source packages (ex. osCommerce)

Security Considerations

- Our firewall is managed by hosting provider and follows industry best-practices in change management
- Access is allowed only via backchannel, token-based authentication VPN
- SNORT for intrusion detection
- OS is hardened and locked down for its particular purpose. All non-essential services are disabled.
- Apache with PHP is easiest to secure compared to rivals (IIS, J2EE)

Developer Data Security

- Any developers utilizing production data for development must mount the data on an encrypted drive with TrueCrypt (works on Windows or Linux).
- If the office hardware or laptop gets stolen, the encrypted drive containing the sensitive data cannot be retrieved. This mitigates any potential security incident and reporting.

Security and Privacy Issues of a Financial Services Site

- Sarbanes-Oxley Act of 2002
- SAS-70 audit qualification
- Gramm-Leach-Bliley Act of 1999
- GLBA assessments
- ISO 17799
- PCI Data Security Standard
- Creating a security program

Sarbanes-Oxley Act of 2002

- Protects investors by improving the accuracy and reliability of corporate disclosures
- Corporate responsibility for financial reporting requires certification of financial statements by both the CEO and the CFO
- e-mail messages and attachments as business records that must be retained to achieve regulatory compliance

Effects of Sarbanes-Oxley

- There is increased scrutiny over systems that process financial records to ensure that they are accurate and secure
- This puts an increased emphasis over who has access to data
- System administration and application access policy must be up-to-date and functional

SAS-70

- An internationally recognized auditing standard developed by the American Institute of Certified Public Accountants (AICPA).
- Represents that a service organization has been through an in-depth audit of their control activities.
- Audit includes controls over information technology and related processes.
- Service organizations or service providers must demonstrate that they have adequate controls and safeguards when they host or process data belonging to their customers.

Effects of SAS-70

- Companies who process financial data must ensure that they meet the security and operational standards as required by the SAS-70 audit standard
- This puts the service provider in the position of having to show an audit team that it has standards and procedures in place to protect its security, systems, and data.

Gramm-Leach-Bliley

- Financial institutions have restrictions on when they may disclose a consumer's personal financial information to nonaffiliated third parties.
- Financial institutions are required to provide notices to their customers about their information-collection and information-sharing practices.
- Consumers may decide to "opt out"

GLB Mandates

- The company must appoint an information security plan coordinator
- Conduct a risk assessment of likely security and privacy risks
- Design a safeguard program and detail the plans to monitor it
- Institute a training program for all employees who have access to covered data and information
- Oversee service providers and contracts, and evaluate and adjust the information security program periodically.

Effects of Gramm-Leach-Bliley

- Service providers are now held to a higher standard of security and privacy
- Financial institutions are responsible to assuring that those entities who are entrusted with their customer data are held to the same standards that they hold themselves

What is ISO 17799?

- ISO17799 is "*a comprehensive set of controls comprising best practices in information security*". It is essentially, in part (extended), an internationally recognized generic information security standard.
- It is a guideline for provide security best practices, and is used often for self-assessment.

The 10 sections of ISO 17799

- *Security Policy*
- *System Access Control*
- *Computer & Operations Management*
- *System Development and Maintenance*
- *Physical and Environmental Security*

The 10 sections of ISO 17799 (con't)

- *Compliance*
- *Personnel Security*
- *Security Organization*
- *Asset Classification*
- *Control Business Continuity Management (BCM)*

PCI Data Security Standard

- The new Payment Card Industry (PCI) data security standards are network security and business practice guidelines developed by Visa, MasterCard, American Express and Discover
- These comprise remote vulnerability scans and the completion of self-assessment security questionnaire
- This standard is emerging as quite important for financial institutions

What this all means?

- To work in financial services, you will be held to a far greater standard than before if you possess or impact customer or financial information
- The emphasis on maintaining and auditing security within a financial-based organization is significant and can no longer be overlooked

Where does PHP fit in?

- PHP has to the toolset and maturity to keep data secure.
- A PHP development team must keep abreast of the latest exploits and patches to stay ahead of the security curve.
- Using PHP implies a better security reputation than .Net, but not better than Java.
- With PHP you can build add-on or modules to comply with standards rapidly.

Where does PHP fit in?

- Development best practices and policies should be documented, reviewed and audited on a regular basis.
- PHP is not fully on the radar of financial institutions.
- PHP is accepted by security auditing firms who do most of the outsourced audit work for financial institutions.
- Bottom Line: You can create any platform you like, provided you are security conscious. PHP fits this requirement well.

Financial Institutions and Open Source

- Each institution that we've encountered readily admits to having substantial open-source projects under way internally.
- These institutions view open-source as generally acceptable for usage in a commercial setting.
- They are especially friendly to Apache and Linux
- Once the institution understands where PHP fits in, they readily accept it.

PHP is being embraced by Financial Institutions

- If you are a service provider and can pass the rigorous security requirements, PHP as a programming language will be an afterthought by the institution
- The same institution is looking for ways to declare vendor independence and utilize the same tools that you do.
- Financial institutions adopt new technologies very slowly, however they are recognizing open source rapidly.

Questions

Contact Info

- Richard Rosa

rrosa@debtresolve.com

rich@richrosa.com

President / CTO

Debt Resolve Inc.

707 Westchester Ave Suite L7

White Plains, NY 10604

914-949-5500