



Why we recommend the LAMP Solution Stack

www.jkdesign.com

January 20, 2009

Summary

For companies creating a new small to medium sized Web site, even if they already use Microsoft software tools for other internal purposes, JK Design typically recommends the use of the LAMP Solution Stack due to the reliability, functionality, performance, portability, security and lower cost offered by these open source tools.

The basic idea behind open source is very simple: When programmers can read, redistribute, and modify the source code for a piece of software, the software evolves. People improve it, people adapt it and people fix bugs. And this can happen at a speed that, if one is used to the slow pace of conventional software development, seems astonishing.

LAMP Solution Stack

The following four items form the basis of the LAMP solution stack of **open source** software used to run dynamic Web sites. This is also JK Design's most popular solution stack:

- 1) Linux as the Operating System (or other Unix variants)
- 2) Apache V1.3 or V2 as the HTTP/Web Server
- 3) MySQL V4 or V5 as the Database
- 4) PHP V5 as the Scripting/Programming Language

Linux – Operating System

Linux is a free Unix-type operating system originally created by Linus Torvalds with the assistance of developers around the world. Developed under the GNU General Public License, the source code for Linux is freely available to everyone. Other similar operating systems include FreeBSD and OpenBSD. Several for-profit corporations have created variants of Linux which may also come with certifications and professional support. Examples include Red Hat, Novell SuSE and Canonical Ubuntu. IBM is also a top commercial contributor to Linux. In May 2007, IDC* reported that Linux-based servers now represent 13.7% of all server revenue (this does not represent the number of Web servers running free Linux).

* Reference: <http://www.linux-watch.com/news/NS5369154346.html>

Apache – HTTP/Web Server

Apache has been the most popular Web server on the Internet since April of 1996. The January 2009 Netcraft Web Server Survey* found that over 52% of the Web sites on the Internet are using Apache (versus only 32% are using IIS). Most of JK Design's Web sites have been built utilizing the Apache HTTP Server.

*Reference: http://news.netcraft.com/archives/web_server_survey.html

MySQL - Database

MySQL is the world's most popular open source database. As of February 2008, over eleven million installations* use MySQL to power high-volume Web sites and other critical business systems. It's used by leading Internet companies including Yahoo, Google and YouTube*.

* References: http://www.informationweek.com/news/software/open_source/showArticle.jhtml?articleID=206900327
<http://www.mysql.com/why-mysql>

PHP – Programming Language

PHP (recursive acronym for "PHP: Hypertext Preprocessor") is a widely-used Open Source general-purpose scripting language that is especially suited for Web development and can be embedded into HTML. PHP runs on the Web server, not on the Web browser/client.

According to Nexen.net's PHP Stats Evolution for October 2008*, over 33% of Web sites are running PHP applications. And Tiobe Software's January 2009 Programming Community Index* states that PHP

is the 5th most popular programming language in use. In a nutshell, PHP is widely used for Web site development, which means there are a plentiful number of affordable PHP programmers.

PHP can also run on all major operating systems including Linux, Unix, Windows, Mac OS X, and more. PHP also integrates with major HTTP/Web Server software including Apache, Microsoft IIS, Netscape, iPlanet, and many others.

One of the strongest and most significant features in PHP is its support for a wide range of databases including MySQL, PostgreSQL, Microsoft SQL Server, Oracle, and others.

* References: http://www.nexen.net/chiffres_cles/phpversion/18821-php_stats_evolution_for_october_2008.php
<http://www.tiobe.com/index.php/content/paperinfo/tpci/index.html>

Developer Tools

Developers may optionally choose to utilize a free CVS for Version Control such as SubVersion from Tigris.org - and a tool for entering program code such as TextPad - or other development environments. JK Design prefers using Zend Studio as their IDE.

Lower Cost

The reason open source tools and related projects are **lower in cost** is due to:

- 1) No server or client software licensing fees
- 2) No proprietary and costly software development toolsets required
- 3) Free technical support found online – no required support contracts
- 4) Wide availability of lower-cost developers
- 5) Reusable open source program code

The above open source tools used with LAMP normally do not require commercial licensing fees. However, professional enterprise support is offered from some vendors such as MySQL (now owned by Sun). Total Cost of Ownership is by and large lower when using open source, as opposed to commercial products such as those from Microsoft. For example, retail licensing fees from Microsoft as of January 20 2009, are summarized below. Note that for every individual Intranet user who will be authenticating on a Microsoft Server or will be uniquely distinguishable, then a Client Access License (CAL) must be purchased for that user, for both the Windows Server in addition to the SQL Server.

Microsoft Windows Server 2008 Standard [per machine] - \$999
Microsoft Windows Server 2008 External Connector License - \$1,999
Microsoft Client Access License (required for each device or user) - \$39 [per user]
Microsoft SQL Server 2008 Standard Edition [per CPU] - \$5,999
Microsoft Visual Studio 2008 Professional w/MSDN Premium [per developer] - \$2,299
Microsoft SourceSafe 2005 [per developer] - \$499
Microsoft 5-Pack Phone Support Contract - \$1,289

Related sources:

<http://www.microsoft.com/windowsserver2008/en/us/pricing.aspx>
<http://www.microsoft.com/sqlserver/2008/en/us/pricing.aspx>
<http://www.newegg.com>

In the above scenario, if your Intranet site has one machine with one CPU running Windows Server 2008 with IIS, in addition to SQL Server 2008, and if you had two developers and 100 employees using your Web site, your **Microsoft license fees alone**, including developer tools, **would be over \$17,000.00!** Add another \$3,900 for every 100 employees accessing your Web site.

Software development would be in addition to the above license fees!

Who uses LAMP?

The following companies have either endorsed the use of LAMP or are running Apache Web server on Unix/Linux based systems.

Many are also using PHP (or Perl/Python) & MySQL.

Yahoo! (PHP/MySQL)	Wikipedia (PHP/MySQL)
Google/YouTube (MySQL)	Sourceforge.org (PHP)
Sony.com	Friendster (PHP)
Oracle (wide PHP integration)	Facebook (PHP)
IBM	Flickr (PHP)
J.P. Morgan Chase	Sabre and Booking.com
Morgan Stanley	Craigslist
HP	Wordpress (PHP)
Apple (PHP)	Digg (PHP)
Adobe	Overstock
Alcatel-Lucent	Zappos
Nokia	StumbleUpon (PHP)

The following well-known companies are also seeking PHP developers via www.monster.com as of January 2009 (there are many others!):

<p>Oracle J&J GE Boeing Northrop Grumman AT&T Apple Tivo PNC Symantec Goodyear Tire Comcast Cable Time Warner Cable</p>	<p>FOX ESPN MTV Networks DeVry University YMCA Playboy SkyWest Air Akamai Netflix eBay WebMD eHarmony L-3</p>
---	---

Security

Today, one of the hot topics in our industry is “security” of a Web site. But security can encompass many levels. Entire books are written on each of the underlined topics below. Thus what you read below is simply a summary of some of our common security recommendations.

Keep in mind that even with putting today’s Best Practices for Security in place, the Web is constantly evolving and the software that runs it is changing and will likely never be bug-free. Large corporate Web sites and well-known e-Commerce sites still get hacked on a regular basis. See the Web Hacking Incidents Database at: <http://www.webappsec.org/projects/whid/>

Many “Security Experts” do exist, who can help define and configure specific security needs. Depending on your needs and budget, either your Web Host or JK Design can implement some or all of these security components. If required, we can have one our Security Consultants work on your specific project.

If you have an Information Technology department, we do recommend that they be involved with determining security requirements and ongoing management thereof.

Operating Systems

HTTP/Web Servers and Database Servers (and sometimes Firewalls) are running on top of an Operating System. *Historically the most secure Operating System has been Unix/Linux. And the most insecure has been Microsoft Windows Server.* The LAMP Solution Stack utilizes Linux as the Operating System.

Web Hosting Providers should regularly apply software patches that are issued for the Operating System used on their HTTP/Web Servers and Databases. These patches may be security updates.

Usernames/Passwords

All Operating Systems and HTTP/Web Servers and Databases utilize Usernames and Passwords to login. Each Username can be assigned certain access or privileges. The highest privilege level is referred to as “Root” on a Linux Operating System and “Administrator” on Microsoft Windows Server; this account level should not be issued unless absolutely necessary.

Extreme care should be taken to create strong passwords that are not easily decrypted, for any type of Username. In addition, Usernames and Passwords should not be written down on post-it notes next to a person’s desk. They should be treated as confidential information.

Firewall

Firewalls are typically implemented and managed by the Web Hosting Providers. Firewalls can be a separate hardware device that sits in front of the Web server. Firewalls can also be software based, running directly on the Web server. We recommend a separate hardware based Firewall.

Firewalls typically block ports that should not be in use. Firewalls also monitor open ports (such as Port 80, used by Web servers and the HTTP protocol), looking for suspicious activity. Stateful Packet Inspection is a common technique used on Firewalls.

Notifications can be sent to your Web Host Tech Support staff when suspicious activity occurs. Or depending on the functionality of the Firewall, it may shut down certain services to a specific client or IP address, if it detects suspicious activity.

HTTP/Web Server

Historically the most secure HTTP Server, has been Apache HTTP Server. And the most insecure has been Microsoft Internet Information Server (IIS). However IIS Version 7 has been reported as being much more secure than its predecessors. The LAMP Solution Stack utilizes Apache HTTP Server.

HTTP Servers should be configured by your Web Host Provider to minimize hacking attempts. It is also important that they regularly apply software patches that are issued for the HTTP/Web Server. These patches may be security updates.

Secure Certificate

A Secure Certificate can be purchased for a Web Server. When you see a URL in your Web browser's Address bar that starts with "https://", you are on a secure encrypted connection, often referred to as SSL (Secure Sockets Layer).

A Secure Certificate simply allows an encrypted connection between the Web Server and the Web Browser. Typically this is implemented during an online order process, on the page that is accepting the Credit Card information. They are also used for Web Servers that are displaying confidential information.

Note that just because a Web Server is using a Secure Certificate, does not guarantee that your collected data is also being handled and stored in a secure manner. See other sections below.

Application Code

Web Application Code normally resides and executes on the HTTP/Web Server. For the LAMP platform, code is normally written using PHP (for Microsoft platforms: ASP.net/C#). Code must be written using techniques that help reduce or prevent common Web Application Hacking including:

- SQL injection
- Directory Traversal
- Cross site scripting
- Authentication Hacking

Database Server

Databases must be supplied a Username and Password to access data – even if it's PHP software code accessing the database. Thus, if the Web Server is hacked, then chances are high that a hacker will be able to find the Database Username/Password that exists in the PHP or ASP code itself, and thus gain access to much of your data, if not all.

Username's used by the PHP or ASP software code, should not have Administrative privileges to either the machine running the Database or the Database itself. These usernames should only have the functionality or level of access that is needed for the application to interact with the database.

The data in the Database itself can be encrypted, however in order to display the data unencrypted to a Web user, it must be unencrypted by the PHP or ASP code. Thus the same issue can occur - if the Web Server is hacked, the hacker can then unencrypt the data the same way the code would. Some data such as User Passwords can be encrypted in such a way that it cannot be unencrypted by the PHP or ASP software code. However encrypting other data may not serve a useful function.

For very sensitive data, the Database can also be placed on a separate physical machine/server (not on the HTTP/Web Server), which would also be operating behind a second Firewall. The Firewall would need to be configured by a Security Expert to look for certain suspicious activities

Configuring Databases to support any of the above or other options can be complex, yet not infallible.

Backup

Your Web hosting provider and IT department should ensure that your database is backed up on a nightly or regular basis. Note that some databases cannot be backed up properly unless it is exported to a flat file. This flat file should not reside in an area accessible to the public or a hacker. If it must be written to a shared combination Web and Database server, it should be securely deleted after external backup is complete.

In addition to the database, all other files and code on the Web server should be backed up to an external tape storage device.

If your data is backed up to tape, and your Web site is hacked, you can still retrieve your data from your last point of backup.

Secure FTP

Your Web server should not allow connections via FTP (port 21), since FTP is an insecure protocol that can easily be exploited by hackers. Web vendors (including JK Design) should connect to your Web server using an encrypted method such as SSH for remote login and file transfers. Your Web server should also be configured to not allow "root" access except to those who absolutely need it.

Shared Hosting versus VPS versus Dedicated

In order to lower costs, Clients often opt to host their Web site on a Shared Server. However when you are running your Web site on a Shared Server, the risk is higher that your Web site will be hacked. This risk is higher due to the other Web sites that may be running on the machine, which may have application code or other security issues, that make it easier for a hacker to gain access to the Server via their Web site. If a hacker obtains Root access to a Web Server from any Web site running on the server, they will have full access to the entire machine and any Web sites running on it.

Virtual Private Servers (VPS) take Shared Hosting one level higher, with regards to the security aspects. However, VPS systems are still technically sharing the Web Server with other Web sites.

Dedicated Servers can provide better security than Shared or VPS, due to the fact that other Web sites would not be running on the Dedicated Server.

Security Testing

Other security programs such as network security audits, network discovery and penetration testing are optional and may also be purchased by the client. Third party companies are contracted for this, who can attempt to hack the Web site, after coding and testing has been completed. Security holes that are found during the Security Testing can then be closed by JK Design's developers.

Physical Security

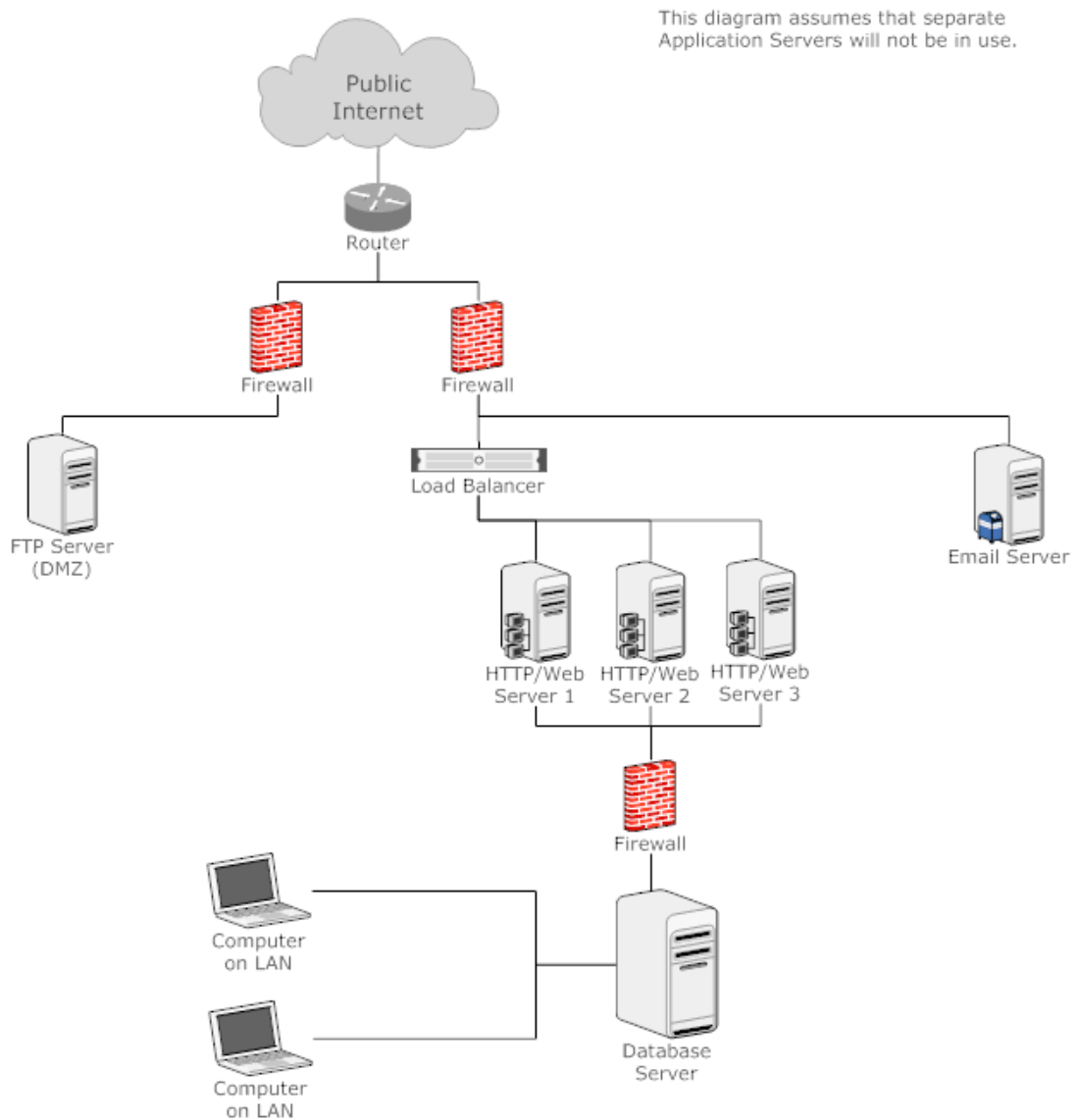
All of the above Security aspects are relating to virtual security. They assume that access to the servers and applications are via the Internet or LAN. However, another security issue to be concerned about, is physical access to the server. Whether you are using a Shared Hosting Server, a VPS or Dedicated – you should understand how your Web Server's machine is protected at the Web Hosting Provider. Is it in a locked cage, with the power button, keyboard, mouse and floppy disk or CD-ROM not accessible to a passer-by? If a machine itself is not secure, a passer-by could technically boot the machine from a hacker CD, obtaining the Root or Administrator Password and thus gaining access to full rights to the machine.

Example Network Diagram

Depending on your needs, several of the above Security recommendations may be put in place. Below, is an example of a possible Network Diagram, which can help to illustrate how the above Servers and Firewalls relate to each other.

Note that there are multitudes of ways to configure a network. This is simply an example.

Example Network Diagram for HTTP/Web & Database Servers



Windows Solution Stacks

Although JK Design typically recommends the LAMP Solution Stack, several of our clients host their own Web servers in-house, and they have trained I.T. support staff who know how to Administer Windows Servers and Internet Information Server (IIS). It's understandable that these clients may not want to learn a new Server Operating System such as Linux, or a new HTTP/Web Server such as Apache.

For these instances, JK Design recommends that one of the following Windows Solution Stacks be utilized for the project:

WIMP = Windows Server 2008, IIS 7, MySQL 5, PHP 5

WISP = Windows Server 2008, IIS 7, Microsoft SQL Server 2008, PHP 5

WIOP = Windows Server 2008, IIS 7, Oracle Database 10g/11g, PHP 5

For lower cost and quicker development, we recommend the WIMP Solution Stack.

The secret behind running PHP effectively on Windows Server, is using Microsoft's FastCGI component, which is built-into Windows Server 2008 (it's available for download with Windows Server 2003). IIS 7 also has components to interact with FastCGI.

There **has** been some recent good press regarding the efficient Web server speed found when using IIS 7, FastCGI and PHP and JK Design has successfully worked in these environments. However the costs for development are higher due to the server licensing requirements.

Note that the Apache module "mod_rewrite" is used extensively by JK Design to provide Search Engine Friendly URL's. The use of mod_rewrite is also integrated with our CMS. When using IIS as the HTTP/Web Server, the IIS 7 alternative to Apache's "mod_rewrite" module must be installed:

Microsoft URL Rewrite Module for IIS 7:

x86: <http://www.iis.net/downloads/default.aspx?tabid=34&q=6&i=1691>

x64: <http://www.iis.net/downloads/default.aspx?tabid=34&q=6&i=1692>

Hotfixes: <http://support.microsoft.com/kb/954946>

Database Note: When Microsoft SQL Server or Oracle Database is used, a DBA is typically required to perform installation, setup, configuration and also assist with implementing databases and table structures. When using MySQL, developers can perform these functions for much less cost.