



Why we recommend the LAMP Solution Stack

www.jkdesign.com

March 22, 2012

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, can seem 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 V5.2** 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 November 2011, IDC* reported that Linux-based servers now represent 18.6% of all server revenue (this does not represent the number of Web servers running free Linux).

* Reference: <http://www.idc.com/getdoc.jsp?containerId=prUS23179011>

Apache – HTTP/Web Server

Apache has been the most popular Web server on the Internet since April of 1996. The March 2012 Netcraft Web Server Survey* found that over 64% of the Web sites on the Internet are using Apache (versus slightly over 14% who are using IIS). Most of JK Design's Web sites have been built utilizing the Apache HTTP Server.

*Reference: <http://news.netcraft.com/archives/category/web-server-survey/>

MySQL - Database

MySQL is the world's most popular open source database and is used to power high-volume Web sites and other critical business systems. It's used by leading Internet companies including Yahoo, Google, YouTube, Wikipedia, Nokia, Alcatel-Lucent and many others*.

* References: <http://www.mysql.com/about/>
<http://www.mysql.com/why-mysql/marketshare/>

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.

As of March 20 2012, according to W3Techs.com, of the top 1 million Web sites (as reported by Alexa), over 77% of them are using PHP. And Tiobe Software's March 2012 Programming Community Index*

states that PHP is the 6th 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://w3techs.com/technologies/overview/programming_language/all
<http://www.tiobe.com/index.php/content/paperinfo/tpci/index.html>

Developer Tools

Developers may optionally choose to utilize one of many free or inexpensive Integrated Development Environments and editors including open source IDE's such as Aptana, inexpensive commercial options including Sublime Text or more sophisticated offerings from Zend Studio and many others. Version Control can also easily be implemented with additional open source tools, such as Git.

Lower Cost

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

- 1) A plethora of existing quality reusable open source program code
- 2) No server or client software licensing fees
- 3) Costly software development toolsets are not required
- 4) Free technical support found online – no required support contracts
- 5) Wide availability of lower-cost developers

The above open source tools used with LAMP normally do not require commercial licensing fees. However, many commercial software products are built using or on top of open source tools, and professional enterprise support is offered from some vendors such as MySQL (now owned by Oracle). Total Cost of Ownership is normally lower when using open source, as opposed to commercial products such as those from Microsoft which cost thousands of dollars even for a small installation.

Software development would be in addition to the Microsoft 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 (and many others) have sought PHP developers via www.monster.com:

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

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, such as those published by [OWASP](#), the Web is constantly evolving and the software that runs it is changing and will likely never be infallible or 100% secure. Large corporate Web sites, well-known e-Commerce sites and government sites still get hacked on a regular basis.

Thankfully for many companies, their Web sites only contain public marketing material and not confidential data. Some of the most serious security hacks have been beyond the marketing Web site and within actual corporate networks. According to a [2011 survey](#) by Poneman Research, 90% of the 583 companies surveyed, suffered some form of a breach at least once in the past year.

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 Microsoft Windows Server has been the most insecure, though Microsoft has invested heavily to rectify security issues. 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. 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 and 8 have 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: often ASP.net/C#). Code must be written using techniques that help reduce or prevent common Web Application Hacking, such as these top 5 :

- SQL injection
- Cross site scripting
- Broken Authentication and Session Management
- Insecure Direct Object References
- Cross Site Request Forgery

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 a PHP or ASP configuration file, and thus gain access to much of your data, if not all. Database configuration files are typically stored outside the Web root folder, to help mitigate this issue.

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 or secure cloud service (though cloud services have their own set of security issues).

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

Inexpensive Shared Hosting runs a much higher risk that your Web site will be hacked, 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. Although VPS systems are still technically sharing the same physical machine with other Web sites, virtualization tightens security by segregating your Web environment from other companies that may be sharing that same physical machine.

Dedicated Servers can provide better security than Shared and a step beyond 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

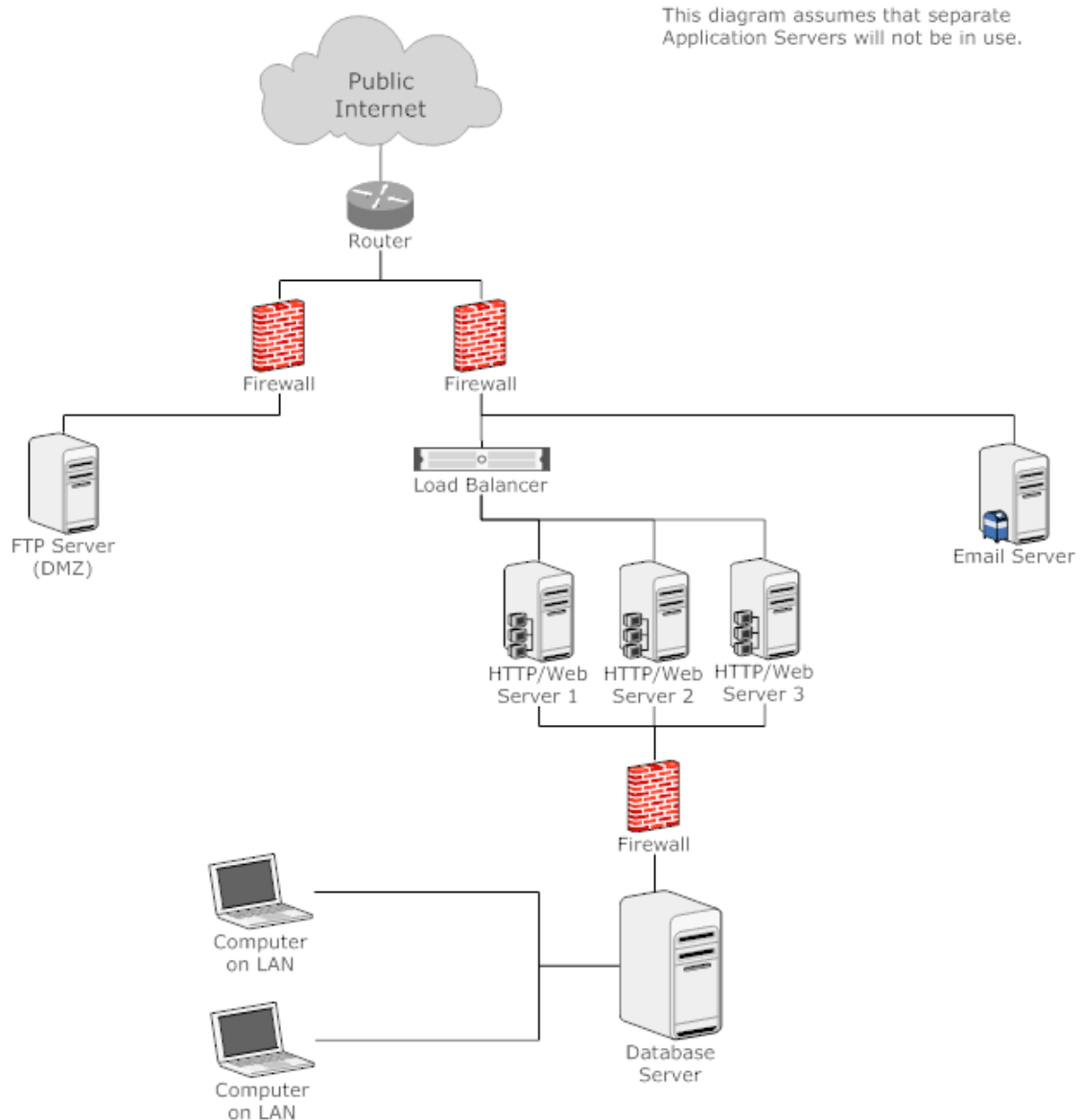
All of the above Security aspects are relating to virtual security. They assume that access to the servers and applications are via the Internet or LAN. However, another security issue to be concerned about, is physical access to the server. Whether you are using a VPS or Dedicated – you should understand 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, floppy disk, USB 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, Internet Information Server (IIS) and Microsoft SQL Server. 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 can work with the following Windows Solution Stacks:

WIMP = Windows Server 2008 R2, IIS 7.5, MySQL 5.5, PHP 5.3

WISP = Windows Server 2008 R2, IIS 7.5, Microsoft SQL Server 2008, PHP 5.3

WIOP = Windows Server 2008 R2, IIS 7.5, Oracle Database 11g, PHP 5.3

For lower cost and quicker development, and when utilizing the JK Design CMS or other open source CMS systems, we recommend the WIMP Solution Stack.

Version 7.5 of IIS includes native support for PHP FastCGI and URL Rewriting. For more information, see: <http://www.microsoft.com/en-us/server-cloud/windows-server/internet-information-services-iis-overview.aspx>

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 7.5 alternative to Apache's "mod_rewrite" is utilized.

For more information about PHP on IIS, see: <http://php.iis.net>

For more information on URL Rewrite, see: <http://www.iis.net/download/URLRewrite>

MySQL can be downloaded from: <http://dev.mysql.com/downloads/mysql/#downloads>

Tips for installing MySQL on IIS 7 are available, though steps may differ when using IIS V7.5:

<http://learn.iis.net/page.aspx/353/install-and-configure-mysql-for-php-applications-on-iis-7-and-above/>

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

Open Source Licensing

In order to expedite the creation of Interactive (Website, iPad, Mobile) Projects, JK Design may make use of various Open Source programming code that has previously been created by third parties. As such, all third party software source code may have their own unique software license. In general, JK Design selects tools that we interpret as having “client distribution friendly licenses”, meaning the licenses allow us to redistribute the software tool, and allow clients to use and maintain the code, without having to release the code back to the open source community. Licenses that work in this manner include but may not be limited to the MIT, GNU Lesser General Public License and the New BSD License.

Some licenses require that the software tool be “free” and not “sold”. As such, JK Design is not selling these software libraries, we are only redistributing them to our clients. Our project fees relate to the labor and man-hours that it has taken to design and implement Web sites and mobile applications, which may require modification and configuration of JK Design software tools or service time required to redistribute third party open source tools, to implement client requirements. The GNU General Public License and Apache License 2.0 are “free” software licenses; though free does not imply it must be public domain.

JK Design maintains their own bespoke Web-based Content Management System built on top of CodeIgniter and several other open source tools are supplied to enhance the usage. iPad software programs are typically programmed with Objective C in an Xcode environment. Should any of JK Design’s existing or new software components be utilized for Client projects (as specified in a project proposal or other written means), JK Design will grant the Client a single perpetual, irrevocable, worldwide, non-exclusive, royalty-free license (or, in the case of third-party software, sub-license, where permissible), upon completion of the project and payment of all Project fees. Third-party software redistributed by JK Design for Client Projects may include their own license agreements that the Client must also abide by, including but not limited to the following. Note that actual versions of tools/software were current as of March 2012 – however *newer releases/versions are regularly applied to the JK Design CMS.*

A) CMS (JK Design Bespoke CMS)

Required Platforms (but not distributed):

- PHP 5.2+ <http://www.php.net/license>
- MySQL 5.5 <http://www.mysql.com/downloads/mysql>

Technologies/Specifications:

- JavaScript (EcmaScript 1.4)
- HTML 4.01 / XHTML 1 / HTML 5
- CSS 2.1 / CSS 3
- JSON <http://json.org/>

Packages:

- CodeIgniter v 2.1.0 http://codeigniter.com/user_guide/license.html
- TinyMCE <http://www.tinymce.com/wiki.php/License>
- Ion Auth 2 <https://github.com/benedmunds/CodeIgniter-Ion-Auth>
- Twitter Bootstrap 2.0.1 <http://twitter.github.com/bootstrap>
- jQuery 1.7.1 <http://jquery.org/license>
- jQuery UI 1.8.16 <http://jquery.org/license>
- jQuery nestedSortable 1.3.4 <http://mjsarfatti.com/sandbox/nestedSortable/>
- jQuery serializeTree <http://archive.plugins.jquery.com/project/serializeTree>
- Multiple jQuery CSS Hooks -- All licensed under MIT license
- Valums Upload <https://github.com/valums/file-uploader/>

Third Party CMS Systems:

- WordPress V3 (some blog implementations) <http://codex.wordpress.org/License>

B) iPad

Languages:

- iOS SDK with Objective-C http://en.wikipedia.org/wiki/IOS_SDK

Packages:

- MWFeedParser for parsing RSS Feed <https://github.com/mwaterfall/MWFeedParser>
- FMDatabase <https://github.com/ccgus/fmdb>
- Google Analytics for iOS <http://code.google.com/apis/analytics/docs/mobile/ios.html>
- JK Library (JK Design specific functions/features)
- DragDropKit

Licensed Code:

- FastPdfKit for viewing PDF <http://fastpdfkit.com>

Note that the authors of open source tools, generally require in their license, that copyright notices and existing licenses remain in tact for redistributions, and any modifications to the program code must be noted (generally JK Design does not modify open source libraries that we redistribute). In addition, the authors do not provide a warranty for their work and neither can JK Design – and the authors have no liability and neither does JK Design – this is the nature of using open source tools. We can only warranty our original source code, for the period specified within client Agreements.