atlantic.net
Secure Cloud Services

CELEBRATING 29 YEARS OF EXCELLENCE

BEST PRACTICE FOR CREATING A HIPAA-COMPLIANT LAMP STACK

A LAMP stack is a collection of applications that work seamlessly together to create a powerful open-source web server. The application stack is not only completely free, but also unbelievably powerful and highly customizable, both of which make it a popular choice for developers.

Why is it called LAMP?

Linux is the base operating system used on the server.
Apache is the most popular web server used today, powering about 37% of all websites.
MySQL (or MariaDB) is a relational database application that is perfect for storing website data.
PHP is a highly adaptable scripting language that is especially suited to web development.

One of the best things about a LAMP stack is its ease of deployment. The one-click application is our recommended deployment method, but if you want to give it a try yourself you can:

Did You Know?

Atlantic.Net has a one-click application that spins up an Ubuntu LAMP stack in under 30 seconds.

HOW TO SECURE A HIPAA-COMPLIANT LAMP STACK

Any LAMP stack that will host or process Protected Health Information (PHI) must adhere to the administrative, physical, and technical safeguards of HIPAA to ensure the confidentiality of data uploaded or made available through a website or application.

LINUX - HARDENING THE OPERATING SYSTEM

If you are a relative newcomer to Linux, Atlantic.Net recommends you let our one-click LAMP application handle the deployment for you. However, if you want to take the plunge and try it yourself, here is what you need to do:

- Update the operating system monthly
- Utilize the built-in hard drive encryption tools

Did You Know?

Two of the best filesystem encryption tools are eCryptfs and EncFS.
Two of the best block level (disk) encryption tools are DMCrypt and VeraCrypt.

- Only use very strong passwords, and never reuse passwords throughout the LAMP stack
- Only use sFTP encryption to transfer files to and from the webserver
- Update file permissions so that no user can change or modify files
- Ensure no system services or applications run as the root user

BEST PRACTICE FOR CREATING A HIPAA-COMPLIANT LAMP STACK

Did You Know?

You can set up a cron job to chown and chmod files every night as a scheduled task. This helps with preventing user error and correcting careless mistakes when updating web server files.

Apache

APACHE SECURITY TIPS

- Keep Apache up-to-date
- Configure Apache to increase DDOS (denial of service) protection level

Did You Know?

Editing the httpd.conf file and reducing the *RequestReadTimeout*, *Timeout*, *KeepAliveTimeout*, and *MaxRequestWorkers* thresholds will greatly improve DDOS protection.

- Set strict chown, chmod, and chggrp permissions on ServerRoot Directories; this will reduce the ability of a hacker to run arbitrary code
- Enforce TLS certificate encryption using mod_ssl, ensuring you use a strong cipher suite and OCSP stapling
- Implement dynamic content security

Did You Know?

The Apache module mod_security can be finely tuned as a HTTP firewall, perfect for dynamic content security.

- Protect system settings with .htaccess restrictions
- Protect access to service files

Did You Know?

To enable this protection, add this to your httpd.conf:

```
<Directory "/"> AllowOverride None </Directory>
<Directory "/"> Require all denied </Directory>
```

MySQL

MYSQL BEST PRACTICE

The database is where many users will save protected health information. There are strict regulatory compliance rules regarding the masking and de-identification of data, as well as encryption.

- Invoke MySQL Enterprise Data Masking and De-identification routines

atlantic.net
Secure Cloud Services

CELEBRATING 29 YEARS OF EXCELLENCE

BEST PRACTICE FOR CREATING A HIPAA-COMPLIANT LAMP STACK

Did You Know?

A server-side plugin called *data_masking* can manage a SQL-Level API to perform masking and de-identification tasks on your data when it is used by an application.

- Data must be encrypted at rest

Did You Know?

Atlantic.Net's Cloud Platform is encrypted at rest with every server deployed by default, saving you time and effort from implementing encryption inside MySQL

- Enable SELinux for mandatory access controls to protect the MySQL daemon
- Implement MySQL plugins to authenticate users and restrict access by user, password, and approved IP address
- Enable MySQL Enterprise Audit plugin to enable standard, policy-based monitoring and logging of connection and query activity executed on the 8MySQL servers

php PHP BEST PRACTICE

PHP is a popular programming language used by websites to display enhanced content. PHP can either run as an Apache plugin or as a standalone CGI binary. No HIPAA legislation relates directly to PHP; instead, PHP must adhere to access and transmission security, and the browser connections must be secure.

- Ensure PHP is kept up-to-date
- Use PHP to hash and verify all passwords entered by users; BCrypt is included with PHP 7 onwards

Did You Know?

Passwords can be hashed using the *password_hash* PHP function.

- Keep Apache up-to-date
- Configure Apache to increase DDOS (denial of service) protection level

Did You Know?

Editing the httpd.conf file and reducing the *RequestReadTimeout*, *Timeout*, *KeepAliveTimeout*, and *MaxRequestWorkers* thresholds will greatly improve DDOS protection.

Find Out More?

Atlantic.Net stands ready to help you attain fast compliance with a range of certifications, such as SOC 2 and SOC 3, HIPAA, and HITECH, all with 24x7x365 support, monitoring, and world-class data center infrastructure. For faster application deployment, free IT architecture design, and assessment, visit us at www.atlantic.net, call 888-618-DATA (3282), or email us at sales@atlantic.net.

ATLANTIC.NET MANAGED & SUPPORTED IN THE USA INVESTING IN AMERICAN JOBS