atlantic.net
Secure Cloud Services

CELEBRATING 30 YEARS OF EXCELLENCE

BEST PRACTICE FOR CREATING A HIPAA-COMPLIANT LEMP STACK

A LEMP stack is a collection of applications that work seamlessly together to create a powerful open-source web server. Unlike a LAMP Stack, which uses Apache, a LEMP Stack is powered by Nginx (pronounced `Engine-Ex`, hence the E in LEMP).

Nginx is about 2.5x faster than Apache for high traffic websites with static content, so if you have a popular website that serves multiple concurrent connections, then Nginx is what you need. The stack is completely free, and Nginx has many additional modules built-in, including the popular reverse proxy.

Did You Know?

Atlantic.Net has a 1-click application that spins up an Ubuntu LEMP stack in under 30 seconds.

BEST PRACTICE TO SECURE A HIPAA-COMPLIANT LEMP STACK

Any LEMP 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.

Did You Know?

You can automatically deploy a LEMP stack on the Atlantic Cloud Platform in less than 30 seconds using our `1-Click Applications`. Visit https://cloud.atlantic.net for further information.

LINUX - HARDENING THE OPERATING SYSTEM

If you are a relative newcomer to Linux, Atlantic.Net recommends you let our one-click LEMP 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 within the LEMP 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

440 West Kennedy Blvd, Suite 3,
Orlando, FL 32810, USA
www.atlantic.net

sales@atlantic.net
888-618-DATA (3282)
Int'l +1-321-206-3734

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

atlantic.net
Secure Cloud Services

CELEBRATING 30 YEARS OF EXCELLENCE

BEST PRACTICE FOR CREATING A HIPAA-COMPLIANT LEMP 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.

NGINX BEST-PRACTICE TIPS

- Ensure Nginx is updated regularly
- Obfuscate Nginx server information from the public

Did You Know?

You can mask server information on Nginx by adding this to the `Nginx.conf` file:

```
server_tokens off;
```

- Enforce HTTP Strict Transport Security (HSTS on TLS) to add a layer of encryption in communications

Did You Know?

Enforcing HTTP Strict Transport Security means using HTTPS. You can enforce it by adding this to your `ssl.conf`:

```
add_header Strict-Transport-Security "max-age=63072000; includeSubdomains; preload";
```

- Disable deprecated SSL standards and weak cipher suites
- Disable unwanted modules to reduce the attack surface
- Enforce cross-site scripting (XSS) protection

Did You Know?

XSS protection can be implemented by updating your `ssl.conf` file

```
add_header X-XSS-Protection "1; mode=block";
```

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

440 West Kennedy Blvd, Suite 3,
Orlando, FL 32810, USA
www.atlantic.net

sales@atlantic.net
888-618-DATA (3282)
Int'l +1-321-206-3734

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

atlantic.net
Secure Cloud Services

CELEBRATING 30 YEARS OF EXCELLENCE

BEST PRACTICE FOR CREATING A HIPAA-COMPLIANT LEMP 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?

Purekit for MariaDB is perfect for encrypting data at rest; it uses record layer encryption of the database, per-user encryption, and a zero-trust KMS.

- 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 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.

- Use PHP to enforce a user registration system and prevent access to unauthorized users
- Use PHP to protect against Cross-site scripting (XSS) and Request Forgery XSFR

Did You Know?

You can protect against XSS and XSFR by sanitizing data input. The *htmlspecialchars()* and *htmlentities* functions prevent special characters that can hijack PHP code.

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.

440 West Kennedy Blvd, Suite 3,
Orlando, FL 32810, USA
www.atlantic.net

sales@atlantic.net
888-618-DATA (3282)
Int'l +1-321-206-3734

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