

¡Hospeda tu propio blog!

Cómo montar y mantener tu servidor bajo linux

- ¿por qué hospedar mi blog?

Instalación LAMP.

Configuración del servidor y herramientas.

Mejorando la seguridad de tu servidor.

Introducción

- ¿por qué hospedar mi blog?
- Instalación LAMP.
- Configuración del servidor y herramientas.
- Mejorando la seguridad de tu servidor.
- Preguntas y dudas.

- *¿por qué hospedar mi blog?*

Instalación LAMP.

Configuración del servidor y herramientas.

Mejorando la seguridad de tu servidor.

¿por qué hospedar mi propio blog?

- Mayor control sobre los servicios del servidor.
- Mayor control y seguridad sobre el contenido.
- Más rápido en actualizaciones.
- ¡¡Para aprender!!

- *¿por qué hospedar mi blog?*

Instalación LAMP.

Configuración del servidor y herramientas.

Mejorando la seguridad de tu servidor.

¿Que necesito?

- Un ordenador (¡no importa que sea viejo!)
- A priori un servidor web con soporte para PHP y bases de datos.
- Un gestor de contenidos (CMS) que fijará nuestros requisitos.

- *¿por qué hospedar mi blog?*

Instalación LAMP.

Configuración del servidor y herramientas.

Mejorando la seguridad de tu servidor.

¿Qué CMS uso?

- Opciones:
 - Wordpress
 - Joomla!
 - Drupal
 - CMS Made Simple
 - Zope
 - El tuyo propio (vLog ? xD)
- Hemos elegido Wordpress



¿Qué CMS uso?

- Ventajas de Wordpress
 - Muy extendido.
 - Facilidad de uso.
 - Mucha documentación y soporte.
 - Infinidad de plugins.
 - Compatibilidad.
- Inconvenientes de Wordpress
 - Seguridad (más extendido = más investigado)

LAMP Vs. WAMP

- ¿por qué usar una solución LAMP?
 - Es una solución libre. Es una solución gratuita.
 - Administración remota mucho más sencilla y eficaz.
 - Rendimiento y requisitos hardware de la máquina.
 - Aplicaciones originalmente pensadas para entornos UNIX.
 - Familiarizarte con un sistema linux.
 - Existen decenas de sistemas instalables LAMP ya configurados y listos para ejecutar.

¿Cómo instalo un paquete en linux?

- Gestor de paquetes de nuestra distribución

Apt (y hermanitos), portage, rpm, pacman, ...

- 'A pelo'

```
$ wget url/package.tar.gz
```

```
$ tar zxvf package.tar.gz
```

```
$ cd package
```

```
$ ./configure
```

```
$ make
```

```
$ sudo make install
```

CampusBlog

- ¿por qué hospedar mi blog?

Instalación LAMP.

Configuración del servidor y herramientas.

Mejorando la seguridad de tu servidor.



- ¿por qué hospedar mi blog?

Instalación LAMP.

Configuración del servidor y herramientas.

Mejorando la seguridad de tu servidor.

Instalación de Apache



- Podemos usar nuestro gestor de paquetes (recomendado) u obtenerlo de <http://httpd.apache.org/> e instalarlo a mano.
- Tenemos que instalar el soporte para PHP y MySQL.

- ¿por qué hospedar mi blog?

Instalación LAMP.

Configuración del servidor y herramientas.

Mejorando la seguridad de tu servidor.

Instalación de Apache

- Editar archivos (pueden variar de sitio!!!)

- /etc/apache2/vhosts.d/00_default_vhost.conf:
(si no en /etc/apache2/httpd.conf)

- Listen 80 (443 para SSL)
 - ServerName midominio.com
 - DocumentRoot /var/www/localhost

- /etc/conf.d/apache2:

```
APACHE2_OPTS="-D DEFAULT_VHOST -D INFO -D LANGUAGE  
-D SSL -D SSL_DEFAULT_VHOST -D USERDIR -D  
PHP5"APACHE2_OPTS="-D DEFAULT_VHOST -D INFO -D  
LANGUAGE -D SSL -D SSL_DEFAULT_VHOST -D USERDIR -D  
PHP5"
```

- ¿por qué hospedar mi blog?

Instalación LAMP.

Configuración del servidor y herramientas.

Mejorando la seguridad de tu servidor.

Instalación de MySQL



- Usamos el gestor de paquetes.
- Configuración en `/etc/mysql/my.cnf`
- Establecer una contraseña de root!

```
$ /usr/bin/mysqladmin -u root password 'new-  
password'
```

- `mysql_secure_installation`
- `mysql_setpermission`

- ¿por qué hospedar mi blog?

Instalación LAMP.

Configuración del servidor y herramientas.

Mejorando la seguridad de tu servidor.

Instalación de PHP



- Usamos el gestor de paquetes.
- Hay que activar el soporte para MySQL (debería venir por defecto en el paquete de tu distro).
- Pasarle “-D PHP5” a APACHE_OPTS.

- ¿por qué hospedar mi blog?

Instalación LAMP.

Configuración del servidor y herramientas.

Mejorando la seguridad de tu servidor.

Instalación de PHP

- Editar `/etc/php/apache2-php5/php.ini`
(suelen proporcionar uno recomendado)
 - A gusto del consumidor
 - Tiene muchas opciones. Veremos esto más adelante
- Probamos el funcionamiento de php:

```
<? php
    phpinfo();
php>
```

Instalación de Wordpress



- Requisitos Wordpress
 - PHP version ≥ 4.3
 - MySQL version ≥ 4.0
 - (Opcional) Apache mod_rewrite (para URIs limpias, lo que conocemos como Permalinks)
- JAMÁS usar el gestor de paquetes. Siempre bajar la última versión de www.wordpress.org

```
$ wget http://wordpress.org/latest.tar.gz
```

- ¿por qué hospedar mi blog?

Instalación LAMP.

Configuración del servidor y herramientas.

Mejorando la seguridad de tu servidor.

Instalación de Wordpress

- Lo descomprimimos:

```
$ tar xzvf latest.tar.gz
```

- Creamos las bases de datos:

```
$ mysql -u root -p
```

```
mysql> CREATE DATABASE databasename;
```

```
mysql> GRANT ALL PRIVILEGES ON databasename.* TO  
"wordpressusername"@"hostname" IDENTIFIED BY  
"password";
```

```
mysql> FLUSH PRIVILEGES;
```

```
mysql> EXIT;
```

- ¿por qué hospedar mi blog?

Instalación LAMP.

Configuración del servidor y herramientas.

Mejorando la seguridad de tu servidor.

Instalación de Wordpress

- Editamos wp-config.php
 - DB_NAME
 - DB_USER
 - DB_PASSWORD
 - DB_HOST
 - DB_CHARSET
- Ejecutamos el script de instalación:
<http://example.com/wp-admin/install.php>
y seguimos las sencillas instrucciones.

- ¿por qué hospedar mi blog?

Instalación LAMP.

Configuración del servidor y herramientas.

Mejorando la seguridad de tu servidor.

Instalación de Wordpress

- You got it!!
- Recuerda:
 - Salen vulnerabilidades a menudo y es recomendable usar siempre la última versión.
http://codex.wordpress.org/Upgrading_WordPress
 - Haz backups de tus bases de datos.

CampusBlog

- ¿por qué hospedar mi blog?

Instalación LAMP.

Configuración del servidor y herramientas.

Mejorando la seguridad de tu servidor.



- ¿por qué hospedar mi blog?

Instalación LAMP.

Configuración del servidor y herramientas.

Mejorando la seguridad de tu servidor.

OpenSSH



- OpenSSH te permitirá tener acceso remoto mediante una shell.
- Podremos acceder desde cualquier unix-like mediante el comando ssh o usando putty/winscp desde windows.

- ¿por qué hospedar mi blog?

Instalación LAMP.

Configuración del servidor y herramientas.

Mejorando la seguridad de tu servidor.

OpenSSH

- Editamos el `/etc/ssh/sshd_config`
 - Protocol 2
 - Port XXXXX
 - AllowUsers user1 user2
 - PermitRootLogin no
 - StrictModes yes
 - MaxAuthTries
 - PermitEmptyPasswords no
 - PrintLastLog yes

- ¿por qué hospedar mi blog?

Instalación LAMP.

Configuración del servidor y herramientas.

Mejorando la seguridad de tu servidor.

OpenSSH

- Un servidor SSH es una puerta abierta. Tiene que estar vigilada.
- Nivel 1: Denyhosts: lee los logs de autenticación y banea dinámicamente por IP a los atacantes.
- Es simple y efectivo aunque no sofisticado. No requiere de más herramientas para funcionar.
- Herramientas similares: sshdfilter, swatch, fail2ban, blockhosts, ...

- ¿por qué hospedar mi blog?

Instalación LAMP.

Configuración del servidor y herramientas.

Mejorando la seguridad de tu servidor.

Syslog-ng



- Ajustar el syslog-ng a TUS necesidades.
- Configuración en: `/etc/syslog-ng/syslog-ng.conf`
- Logs en `/var/log`
- Importantes a tener en cuenta:
 - `auth.log`, `faillog`, `secure`
 - `apache2/access.log`, `apache2/error_log`
 - `lastlog`
 - `messages`
 - `customizados...`

- ¿por qué hospedar mi blog?

Instalación LAMP.

Configuración del servidor y herramientas.

Mejorando la seguridad de tu servidor.

Syslog-ng

- Existen logs en texto plano y binarios. Los binarios se leen mediante una aplicación:
 - last, lastlog, w, who, faillog,
- Se clasifican según su procedencia y prioridad. se pueden enviar a un fichero de texto plano, a un terminal, a una impresora, a una tubería, ...
- Es recomendable usar logcolorize y logrotate.
- **REGLA DE ORO:** Demasiada información satura. Mantener una política escueta.

- ¿por qué hospedar mi blog?

Instalación LAMP.

Configuración del servidor y herramientas.

Mejorando la seguridad de tu servidor.

Apache

- Ya tenemos un sistema base, ¿se debería quedar así?
- *REGLA DE ORO*: casi siempre la seguridad es el enemigo natural de la usabilidad. Necesitamos mantenernos en un nivel apropiado.
- mod_security para Apache hace las de 'cortafuegos' funcionando como un módulo embebido
- Se activa pasándo la opción -D SECURITY a la variable APACHE_OPTS.

- ¿por qué hospedar mi blog?

Instalación LAMP.

Configuración del servidor y herramientas.

Mejorando la seguridad de tu servidor.

Apache

- Analiza las peticiones http en búsqueda de ataques.
- Es similar a un IDS pero a nivel http.
- Es útil para protegernos de bugs no parcheados y de muchos tipos de ataques.
- Configuración en
`/etc/apache2/modules.d/mod_security/*`
- Vale la pena emplear una configuración 'usable' y no paranoica.

- ¿por qué hospedar mi blog?

Instalación LAMP.

Configuración del servidor y herramientas.

Mejorando la seguridad de tu servidor.

Apache

- Mod_bandwidth: fija el ancho de banda disponible.
- En casa puede parecer poco útil pero simplemente puede que queramos ese ancho de banda.
- mod_evasive: para protegernos de ataque DoS

- ¿por qué hospedar mi blog?

Instalación LAMP.

Configuración del servidor y herramientas.

Mejorando la seguridad de tu servidor.

PHP

- PHP Safe mode. Se configura en el php.ini
- Al igual que ocurre con mod_sec puede llegar a dar más incordios que soluciones. Se pueden encontrar incompatibilidades con plugins de WP.
- Establecer restricciones para ejecutar funciones, chequeos estrictos, proteger variables de entorno, ...
- Desactivar mostrar errores, uploads, etc.

- ¿por qué hospedar mi blog?

Instalación LAMP.

Configuración del servidor y herramientas.

Mejorando la seguridad de tu servidor.

MySQL

- Recomendación: cuanto más aprendas mejor, usa la línea de comandos.
- phpMyAdmin: administración gráfica. Muy importante usar la ÚLTIMA versión siempre. Suelen salir vulnerabilidades.

- ¿por qué hospedar mi blog?

Instalación LAMP.

Configuración del servidor y herramientas.

Mejorando la seguridad de tu servidor.

Monitorización

- Monitorización: cacti y mrtg (famosas pero demasiado completas), webalizer (razonable).
- htop, apachetop, mytop
- netstat, nload, iftop, trafshow, iptraf, ...
- ntop (interfaz web)
- Rootkits: rkhunter, chkrootkit.

- ¿por qué hospedar mi blog?

Instalación LAMP.

Configuración del servidor y herramientas.

Mejorando la seguridad de tu servidor.

Límites

- Ninguna aplicación debe saturar el servidor.
- `/etc/security/limits.conf`
 - Por usuario/grupo (tu_usuario, apache, mysql)
 - Modo estricto o relajado
 - Por tiempo de CPU
 - Por uso de memoria
 - Por número de procesos
 - ...
- Evitar forkbombs.

CampusBlog

- ¿por qué hospedar mi blog?

Instalación LAMP.

Configuración del servidor y herramientas.

Mejorando la seguridad de tu servidor.



Iptables

- ¿Quién trabaja en Windows sin cortafuegos?
- Para gran parte de los usos domésticos el cortafuegos bajo linux podría ser evitable...
(ahora algunos se llevarán las manos a la cabeza y me maldecirán)
- Pero no está de más en algo serio!! ;)
- Iptables es más incómodo de configurar que uno de típico cortafuegos de windows
- KMyFirewall

- ¿por qué hospedar mi blog?

Instalación LAMP.

Configuración del servidor y herramientas.

Mejorando la seguridad de tu servidor.

El kernel

- Las aplicaciones que se corran en nuestro servidor pueden tener vulnerabilidades
- Mediante kernels modificados puedes protegerte de overflows y otros.
 - Pilas y zonas de memoria no ejecutables
 - Mayor entropía
 - Chroots más restringidos
 - Sistemas RSBAC, RBAC

- ¿por qué hospedar mi blog?

Instalación LAMP.

Configuración del servidor y herramientas.

Mejorando la seguridad de tu servidor.

El kernel

- PaX
- GRSecurity
- PIE/SSP
- Control de acceso
- SELinux, RSBAC, aprendizaje de uso.

IDS

- Sistemas de detección de intrusos. Existen soluciones activas y pasivas.
- Tripwire
 - Verifica la integridad de los ficheros/info
 - Checksums
 - Discernir entre un ataque y la actividad normal
- Aide
 - Es un reemplazo más avanzado para Tripwire

- ¿por qué hospedar mi blog?

Instalación LAMP.

Configuración del servidor y herramientas.

Mejorando la seguridad de tu servidor.

IDS

- Snort
 - Posiblemente el más famoso.
 - Existen HIDS, NIDS, DIDS. Snort es un NIDS.
 - Es como un sniffer crecido a más.
 - Tiene varios módulos: sniffer, preprocesador, sistema detector y sistema de salida.
 - Requiere muchos recursos.
 - Analiza muchos tipos de tráfico.
 - Modo in-line => IPS en tiempo real, muy interesante pero necesita más recursos!

- ¿por qué hospedar mi blog?

Instalación LAMP.

Configuración del servidor y herramientas.

Mejorando la seguridad de tu servidor.

Preguntas y dudas

- **Javi Moreno,**

vai <vierito5@gmail.com>

<http://vierito.es/wordpress>

- **Beatriz Cabrera,**

kuasar <kuasar@gmail.com>

<http://kuasar.es/wordpress>