Optimizar Apache

Para optimizar apache deberiamos entre otras cosas cambiar los siguientes parámetros:

- Timeout
- KeepAlive
- MaxKeepAliveRequests
- KeepAliveTimeout

Además cambiar los siguientes parámetros que dan información sobre el servidor:

- ServerSignature On → poner en off
- ServerTokens OS → cambiar OS por prod

http://www.trucoslinux.es/reiniciar-apache-y-mysql-cuando-la-memoria-se-agota/

Página por defecto

Para modificar la web que carga por defecto hay que modificar el fichero httpd.conf y modificar el path a DocumentRoot

```
# This should be changed to whatever you set DocumentRoot to.
#
<Directory "/var/www/html/joomla">
y recargar la configuración para que se apliquen los cambios
```

Acceso a páginas mediante contraseña

Para restringir el acceso a ciertas páginas por medio de contraseñas hay que hacer los siguiente: * modificar el fichero /etc/apache/access.conf indicando que el directorio tendrá acceso controlado por contraseñas.Por ejemplo vamos a proteger un directorio llamado privado

```
<Directory /var/www/privado>
AllowOverride AuthConfig
</Directory>
```

- Crear un fichero llamado .htaccess dentro del directorio a proteger, en nuestro caso /var/www/privado , indicando el método de protección y el fichero con la lista de usuarios autorizados a entrar.

```
AuthName "Usuarios Registrados"
AuthType Basic
AuthUserFile /etc/usuarios_registrados
require valid-user
```

Solo se aceptarán usuarios que estén identificados en el fichero

/etc/usuarios_registrados

Para crear el fichero /etc/usuarios_registrados

```
htpasswd -c /etc/usuarios_registrados
```

Si queremos crear más usuarios, no debemos usar la opción -c, ya que esta crea un nuevo fichero, sobreescribiendo el anterior. Para el segundo y siguientes usuarios, usaremos

```
htpasswd /etc/usuarios_registrados usuario2
```

Si queremos borrar un usuario, podemos editar el fichero o usar la opción -D mayúscula.

Reiniciamos el servidor apache

```
/etc/init.d/httpd restart
```

para aplicar los cambios

SSL

Para general certificados para apache podemos hacerlo de dos formas:

Mediante Genkey

Genkey es un instalador que nos permite crear facilmente los certificados para ello primero necesitamos instalar el paquete crypto-utils

```
yum install crypto-utils
```

Una vez instalado basta con hacer

```
 genkey --days 365 www.miservidor.com
```

y seguir los pasos del asistente

una vez creados los certificados debemos editar el fichero /etc/httpd/conf.d/ssl.conf y cambiar las variables SSLCertificateFile y SSLCertificateKeyFile por el nombre de los nuevos certificados

Guardamos los cambios y reiniciamos el demonio httpd

```
/etc/init.d/httpd restart
```

Openssl

La otra forma de hacer los certificados es manualmente Lo primero que debemos hacer es instalar mod_ssl y openssl para activar el soporte SSL en Apache (podemos hacerlo con yum, apt...):

```
yum install mod_ssl openssl
```

Una vez instalados los módulos, procederemos con la creación del certificado. En primera instancia generamos la llave privada(private-key):

```
openssl genrsa -out cert.key 1024
```

Ahora generamos el CSR (Certificate Signing Request), usando la key generada antes:

```
openssl req -new -key cert.key -out cert.csr
```

Y ahora generamos el certificado en sí utilizando la key y el CSR:

```
openssl x509 -req -days 365 -in cert.csr -signkey cert.key -out cert.crt
```

Ahora para mayor comodidad podéis mover los tres ficheros (cert.csr, cert.crt y cert.key) a la ruta donde guardéis los SSL, por ejemplo /etc/ssl/

Solamente falta configurar el sitio web o el servidor web entero para que utilice el SSL, si es solo para un sitio web bajo virtualhost, añadir lo siguiente dentro del <virtualhost>, son las rutas al certificado y su key correspondiente:

```
SSLCertificateFile /etc/ssl/cert.crt
SSLCertificateKeyFile /etc/ssl/cert.key
```

Si fuerais a hacerlo para todo el servidor web, lo normal es cambiar los valores indicados anteriormente en el fichero de configuración general del ssl, que suele ser:

```
/etc/httpd/conf.d/ssl.conf
```

Una vez hecho esto, reiniciad apache y ya deberíais navegar correctamente bajo SSL, tened en cuenta que navegadores como firefox o explorer no reconocerán el SSL ya que está firmado por nosotros mismos y no una firma autorizada, no obstante, aceptad el certificado y trabajad normalmente.

Para más información sobre OpenSSL, opciones de comando y personalización del certificado:

- http://www.openssl.org/docs/apps/openssl.html
- http://rm-rf.es/generar-un-certificado-ssl-propio-con-openssl/

Comandos para Apache

http://rm-rf.es/categoria/apache/

mod_status

http://systemadmin.es/2009/02/instalacion-del-server-status-mod_status-de-apache

Solucionar problemas de rendimiento

http://systemadmin.es/2010/04/encontrar-la-raiz-del-problema-en-un-entorno-lamp-i

Cambiar Apache de puerto

http://codigounix.blogspot.com.es/2011/11/red-hat-centos-running-apache-with.html

Asegurar Apache

http://blogofsysadmins.com/20-consejos-para-securizar-apache
http://blogofsysadmins.com/creacion-de-virtualhost-falso-en-apache-para-mejorar-la-seguridad
http://elladodelmal.blogspot.com/2007/09/fortificando-un-servidor-apache-i-de-iv.html
http://www.osmosislatina.com/apache/modulos.htm
http://httpd.apache.org/docs/2.0/es/mod/core.html

Referencias

http://blogofsysadmins.com/category/apache