Servidores WEB (Apache) en Debian

Simple, SSL, PHP5, MySQL y Páginas Personales

UNIVERSIDAD VERACRUZANA

October 21, 2013

Autor: M.I. Alberto Pedro Lorandi Medina

Contenido

Figuras

Tablas

Servidor HTTP

Apache2

Instalación

root@server:~# aptitude install apache2 apache2-doc

Verificación

En un navegador web, debemos escribir la dirección del servidor (http://192.168.1.100):

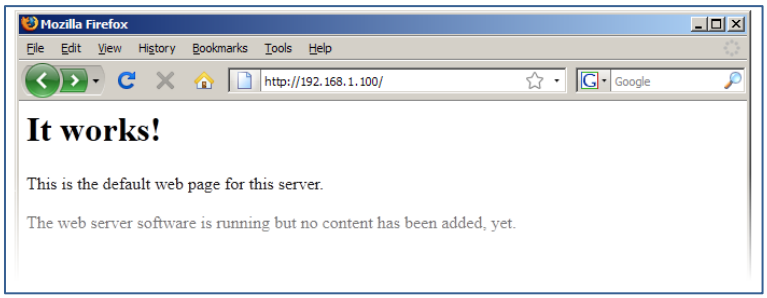

Ilustración 1 Servidor WEB Funcionado

Apache2 + Ssl

Objetivo

La adición del soporte ssl al servidor web permite establecer conexiones seguras y encriptadas entre el servidor y el cliente. De este modo, es posible cambiar contraseñas, con la certeza de que éstas no podrán ser interceptadas por terceros.

De esta forma, es posible usar conexiones seguras como base para la implementación de otros servicios como, por ejemplo, un servidor webmail.

Configuración

Durante la instalación de apache2 se crea una configuración para acceso seguro (https). Por tanto, esta configuración debe ser modificada para incluir los certificados auto-firmados generados previamente.

Esta configuración se almacena en el archivo */etc/apache2/sites-available/default-ssl:*

```
#   SSL Engine Switch:
#   Enable/Disable SSL for this virtual host.
 SSLEngine on
#   A self-signed (snakeoil) certificate can be created by installing
#   the ssl-cert package. See
#   /usr/share/doc/apache2.2-common/README.Debian.gz for more info.
 #   If both key and certificate are stored in the same file, only the
#   SSLCertificateFile directive is needed.
 SSLCertificateFile    /etc/ssl/certs/server.crt
SSLCertificateKeyFile  /etc/ssl/private/server.key.insecure
```

Después, debe activarse el módulo ssl:

Enabling module ssl.

root@server:~# a2enmod ssl

See /usr/share/doc/apache2.2-common/README.Debian.gz on how to configure SSL and create self-signed certificates.

Run '/etc/init.d/apache2 restart' to activate new configuration!

Y el nuevo site también debe activarse:

root@server:~# a2ensite default-ssl
Enabling site default-ssl.
Run '/etc/init.d/apache2 reload' to activate new configuration!

Finalmente, debe reiniciar el servicio:

root@server:~# /etc/init.d/apache2 restart

Verificación

En un navegador de internet, inserte la dirección del servidor (https://192.168.1.100). Después aparecerá el aviso del certificado auto-firmado:

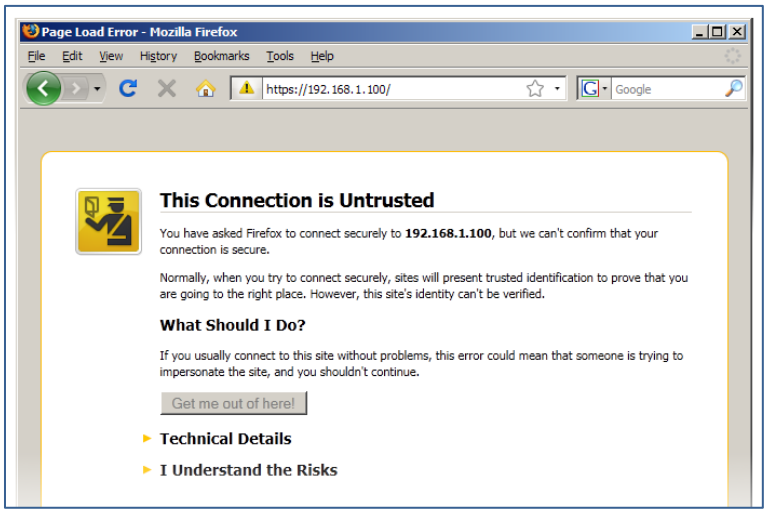

Ilustración 2 Módulo SSL Funcionando

Firefox alertará sobre la existencia de un certificado auto-firmado que, obviamente, no podrá garantizar. Para evitar esta alerta en el futuro, es necesario añadir el certificado a la lista de excepciones de Firefox.

Apache2 + Php5[1]

Objetivo

Expandir la funcionalidad del servidor de internet, activando el soporte php.

Instalación

root@server:~# aptitude install php5 libapache2-mod-php5

Reiniciar el servidor apache2:

root@server:~# /etc/init.d/apache2 restart

Verificación

Para verificar la instalación del soporte php, basta con crear una página de Internet que muestre las características de la instalación php. En este caso, se creará una página en /var/www/phpinfo.php:

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

Con el navegador de Internet y escribiendo la dirección http://192.168.1.100/phpinfo.php, se podrá acceder a la página:

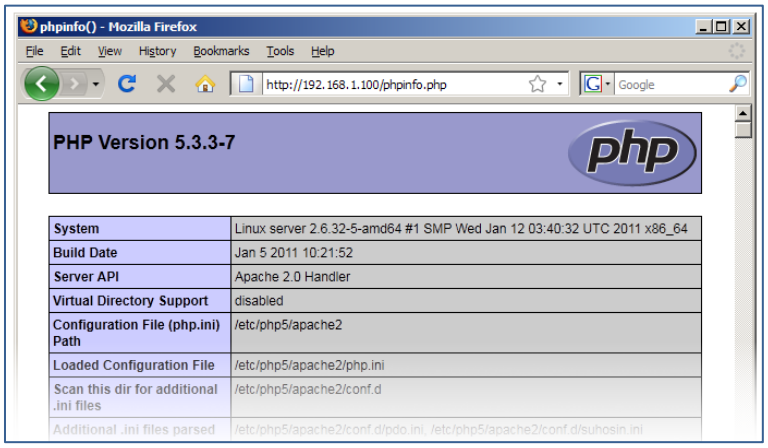

Ilustración 3 PHP5 Habilitado en el Servidor WEB

De la misma manera, también puede ser verificado el acceso seguro a través del protocolo https utilizando la dirección https://192.168.1.100/phpinfo.php.

Una vez verificado el funcionamiento, deberá apagarse la página de pruebas, dado que las informaciones que ésta contiene pueden comprometer la seguridad del servidor:

root@server:~# rm /var/www/phpinfo.php

[1] Antes de proseguir con el siguiente paso ver "Creación de Certificados" al final del documento

Apache2 + Php5 + Mysql

Objetivo

Expandir la funcionalidad del servidor de Internet, activando el soportemySQL del php.

Instalación

root@server:~# aptitude install php5-mysql

Reiniciar el servidor apache:

root@server:~# /etc/init.d/apache2 restart

Verificación

Para verificar la instalación del soportemySQL del php, basta con crear una página de Internet que muestre las características de la instalación php. En este caso, se creará una página en /var/www/phpinfo.php:

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

En seguida puede buscarse la página en un navegador de internet, escribiendo la dirección http://192.168.1.100/phpinfo.php. La información sobre el controlador mysql debe aparecer:

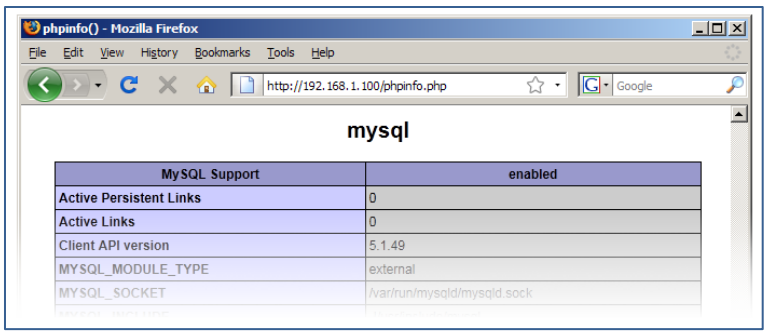

Ilustración 4 MySQL Habilitado en el Servidor

El controlador mysqli también debe aparecer disponible:

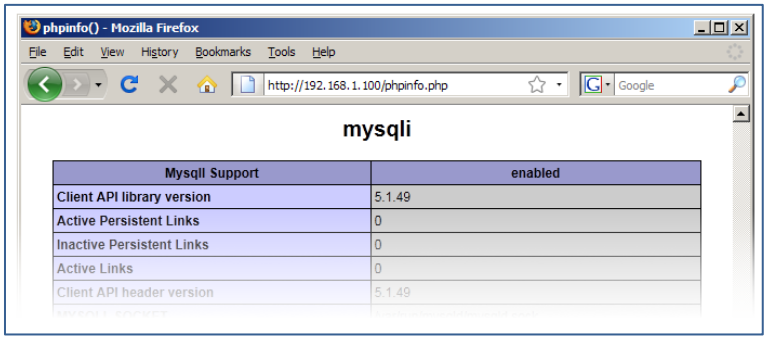

Ilustración 5 MySQLi Habilitado en el Servidor

Una vez realizada la prueba de funcionamiento, se debe apagar esta página de prueba, porque la información que contiene puede comprometer la seguridad del servidor:

```
root@server:~# rm /var/www/phpinfo.php
```

Apache2: Páginas personales

Objetivo

Ofrecerle a cada usuario la posibilidad de crear páginas de Internet personales.

Configuración

Una vez que la instalación del servidor http concluye, la configuración del soporte para crear páginas personales se consigue con la activación del módulo userdir del servidor apache2:

```
root@server:~# a2enmod userdir
Enabling module userdir.
```

Run '/etc/init.d/apache2 restart' to activate new configuration!

Activar soporte PHP

La ejecución de scripts php está desactivada en las páginas personales. Para activarla, se necesita comentar la línea php_admin_value engine Off en el archivo /etc/apache2/mods-available/php5.conf:

```
# To re-enable php in user directories comment the following lines
# (from <IfModule ...> to </IfModule>.) Do NOT set it to On as it
# prevents .htaccess files from disabling it.
<IfModule mod_userdir.c>
    <Directory /home/*/public_html>
        # php_admin_value engine Off
    </Directory>
</IfModule>
```

Luego, reiniciar el servidor apache2:

```
root@server:~# /etc/init.d/apache2 restart
```

De esta manera, queda activado el soporte para páginas personales en el servidor http.

Utilización

Las páginas personales son accesibles a través de una dirección del género "http://servidor/~utilizador". Cuando el servidor recibe un pedido de este género, intenta encontrar el contenido en un directorio específico llamado public_html en la carpeta home del usuario. Por tanto, para que cada usuario pueda crear sus propias páginas, debe primero, crear un directorio llamado "public_html" en su carpeta home, donde ubicará sus contenidos.

```
fribeiro@server:~$ mkdir ~/public_html
```

Una vez creado el directorio, el usuario puede comenzar a crear contenidos.

Verificación

Utilizando un navegador, escriba una url que apunte hacia las páginas personales de un usuario:

Ilustración 6 Páginas Personales Habilitadas en el Servidor WEB

Apache2: Certificados SSL auto-firmados

Objetivo

Para establecer una conexión segura y de confianza es necesario generar certificados que respalden la identidad del servidor. Estos certificados son generalmente emitidos por entidades certificadoras (Certificate Authority) independientes y de confianza reconocida. Sin embargo, para una utilización más casera y económica, es posible crear un certificado "auto-firmado".

Instalación

root@server:~# aptitude install openssl ca-certificates

Generación de los certificados

La generación de un certificadoSSL requiere de los siguientes pasos: primero es generada una clave privada; en seguida ésta es usada para generar un pedido de certificación (Certificate Signing Request (CSR)). El pedido de certificación es entonces enviado a la entidad certificadora (Certificate Authority (CA)) que devuelve el certificado firmado. Es posible ahorrarse el último paso, generando un certificado auto-firmado (Self-signed Certificate).

Crear una carpeta de trabajo:

root@server:~# mkdir certs
root@server:~# cd certs
root@server:~/certs#

Clave privada

Generar una clave privada(Private Key) encriptada (como root):

Desde el usuario ejecutar:

su – root

Enterar el password correspondiente al superusuario y ejecutar:

~/certs# openssl genrsa -des3 -out server.key 2048
Generating RSA private key, 2048 bit long modulus
.....+++
.....+++
e is 65537 (0x10001)
Enter pass phrase for server.key: (enterar un password complicado)
Verifying - Enter pass phrase for server.key: (enterar un password complicado)

Clave privada sin contraseña

La clave privada está encriptada y protegida por una contraseña, lo que implica que ésta debe escribirse cada vez que un servicio necesite la clave. Como solución, es posible generar una versión de la clave sin la protección de la contraseña:

~/certs# openssl rsa -in server.key -out server.key.insecure

Enter pass phrase for server.key: (enterar un password complicado)

writing RSA key

Esta clave sin contraseña, debe ser almacenada con especial cuidado y sólo debe ser accesible por el usuario root:

~/certs# chmod 600 server.key.insecure

Pedido de certificación

Para generar un pedido de certificación (Certificate Signing Request), debe indicarse en el campo Common Name el nombre del servidor para el cual será generado el certificado. En caso de que un certificado sea requerido por varios servidores del mismo dominio, es posible usar la sintaxis **.home.lan*:

~/certs# openssl req -new -key server.key -out server.csr
Enter pass phrase for server.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.

Country Name (2 letter code) [AU]:MX
State or Province Name (full name) [Some-State]:VERACRUZ
Locality Name (eg, city) []:BOCA DEL RIO
Organization Name (eg, company) [Internet Widgits Pty Ltd]:UNIVERSIDAD VERACRUZANA
Organizational Unit Name (eg, section) []:INSTITUTO DE INGENIERIA
Common Name (e.g. server FQDN or YOUR name) []:.veracruz.intra.uv.mx*
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:(enterar un password complicado)
An optional company name []:

Certificado auto-firmado

El pedido de certificación debería ser enviado a la entidad certificadora, que devolvería el certificado firmado. En este caso, será utilizado para crear un certificado (Self-Signed Certificate), válido por 365 días:

~/certs# openssl x509 -req -days 365 -in server.csr -signkey server.key -out server.crt
Signature ok
Subject=/C=PT/ST=Portugal/O=Home Lan/CN=.home.lan*
Getting Private key
Enter pass phrase for server.key:

El proceso de creación de los certificados concluyó. Al final, fueron generados los siguientes archivos:

Tabla 1 Certificados Creados

Archivo	Descripción
server.key	A chave privada
server.key.insecure	La clave privada sin contraseña
server.csr	El pedido de firma del certificación
server.crt	Al certificado auto-firmado

El certificado auto-firmado es válido por 365 días, pero puede ser renovado en cualquier momento, al regenerar el certificado auto-firmado.

Instalación de la clave privada y del certificado auto-firmado

Para esto, debe copiarse las claves privadas en /etc/ssl/private y el certificado en /etc/ssl/certs:

root@server:~/certs# cp server.key server.key.insecure /etc/ssl/private/
root@server:~/certs# cp server.crt /etc/ssl/certs/

Así, el certificado auto-firmado está listo para utilizarse.

Como se trata de un certificado auto-firmado, su utilización siempre dará origen a un aviso por parte de la aplicación cliente: