

Práctica 2: Servidor web

Objetivo

El objetivo de esta práctica es instalar y configurar el servidor web Apache. Durante estos procesos se prestará especial atención a la seguridad del servidor. También se restringirá el acceso a determinadas páginas ubicadas en el servidor según distintos criterios (dirección IP, dirección de red, contraseña) y se realizarán una serie de pruebas para verificar tales restricciones.

1. Características de Apache

El proyecto servidor HTTP Apache es un esfuerzo para desarrollar y mantener un servidor web de código abierto para sistemas operativos modernos. El objetivo de este proyecto es proporcionar un servidor web seguro, robusto, eficiente y extensible que provea servicio HTTP actualizado al estándar HTTP del momento.

Desde 1996 es el servidor web más utilizado. En la actualidad (marzo de 2014), se estima que más del 60% de los sitios web emplean Apache.

Entre sus características destacan:

- Implementa el protocolo HTTP/1.1 (RFC 2616)
- Multiplataforma: puede ejecutarse sobre UNIX, Microsoft Windows, Mac OS/X y Netware.
- Modular: puede ser adaptado a diferentes entornos y necesidades, con los diferentes módulos de apoyo que proporciona y con la API de programación de módulos para el desarrollo de módulos específicos.
- Es extensible mediante módulos desarrollados por terceros. Como ejemplos pueden citarse *mod_php* que implementa el lenguaje de programación del lado del servidor PHP y *mod_ssl* que dota a Apache de soporte SSL (*Secure Socket Layer*) y TLS (*Transport Layer Security*) para seguridad y cifrado de las comunicaciones.
- Código abierto activamente desarrollado y mantenido
- Incentiva la realimentación de los usuarios, obteniendo nuevas ideas, informes de fallos y parches para la solución de los mismos.
- La versión 2.0 puede ejecutarse en un modo híbrido multiproceso/multithread (sistemas con soporte *POSIX*).

2. Enunciado

La primera tarea es instalar Apache. El paquete de instalación puede descargarse a partir de las siguientes direcciones:

<http://httpd.apache.org/>

Las instrucciones para la compilación e instalación, junto con otra información de utilidad, pueden encontrarse en el siguiente enlace:

<http://httpd.apache.org/docs/>

Durante el proceso de instalación seguir en la medida de lo posible las directrices de seguridad que aparecen en la documentación adjunta (*Guía para asegurar servidores web*).

Repasa los módulos que se instalan por defecto y revisa si es necesario alguno adicional. **Documenta claramente los módulos instalados.** Aunque no es obligatorio, se valorará el servicio HTTPS (módulo *mod_ssl*).

La siguiente tarea es configurar el servidor. Sigue de nuevo en este proceso y en la medida de lo posible, las directrices que aparecen en la documentación adjunta (*Guía para asegurar servidores web*).

3. Pruebas

Una vez verificado el funcionamiento básico de Apache, se realizarán varias pruebas de control de acceso a los contenidos de un servidor web. Para ello, previamente debéis crear un sencillo sitio web con cinco páginas, donde la principal contendrá enlaces a las otras cuatro.

Debéis modificar los ficheros de configuración de Apache para que vuestro sitio web presente el siguiente comportamiento:

- La página principal tiene que ser disponible a todo el mundo.
- El primer enlace será accesible sólo desde una máquina del laboratorio
- El segundo enlace será accesible sólo desde las máquinas de la subred del laboratorio.
- El tercer enlace será de dominio público exceptuando a una máquina del laboratorio.
- El cuarto enlace será accesible tras autenticación mediante usuario y contraseña.

El texto de los enlaces de la página principal debe describir detalladamente su destino (nada de “enlace 1”, “enlace 2” ...).

Se deja abierta la posibilidad de implementar restricciones de acceso adicionales.

4. Memoria de la práctica

La memoria de la práctica, breve pero completa, deberá especificar:

- **Servidor web:** versión, justificación.
- **Instalación:** proceso, módulos instalados y eliminados ...
- **Configuración:** modificaciones/añadidos realizados sobre los ficheros de configuración (explicar brevemente mediante comentarios en los propios ficheros).
- Control de acceso: esquema utilizado, ficheros añadidos/modificados ...
- **Seguridad:** tomar como base el documento “*Guidelines on Securing Public Web Servers*” referenciado en el material auxiliar. Reseñar todas las recomendaciones adoptadas en los procesos de instalación y configuración del servidor.
- Breve análisis de los ficheros de registro (log).

5. Material auxiliar, referencias ...

- Sitio web del proyecto Apache: <http://httpd.apache.org>
- RFC 2616

- *Guidelines on Securing Public Web Servers:*

<http://csrc.nist.gov/publications/nistpubs/800-44-ver2/SP800-44v2.pdf>

- Apache Web Server Security Resources recopilados en el documento anterior.
- OpenSSL: the Open Source Toolkit for SSL/TLS: <http://www.openssl.org>
- mod_SSL: the Apache interface to OpenSSL: <http://www.modssl.org>
- *Authentication, Authorization, and Access Control:*

<http://httpd.apache.org/docs/howto/auth.html>