

Administración de servidores Web (Despliegue de aplicaciones web)

Configuración avanzada del servidor Web

Los servidores web, los gestores de bases de datos, los módulos complementarios, normalmente dan problemas a la hora de instalarlos y se pierde mucho tiempo en arreglar los fallos que dan las instalaciones, para facilitar la vida a los usuarios se han creado herramientas de instalación integrada que reúnen un conjunto de aplicaciones y se instalan sin problemas.

Veamos algunas aplicaciones de instalación integrada:

- **Bitnami** es un proyecto código abierto que desarrolla paquetes de software para aplicaciones web, aparte de instalar Apache, PHP, MySQL también instalan aplicaciones como sistema de gestión de contenidos, foros, wikis, etc.
- **XAMPP** es un paquete de software libre, que consiste principalmente en el sistema de gestión de bases de datos MySQL, el servidor web Apache y los intérpretes para lenguajes de script PHP y Perl. El nombre es en realidad un acrónimo: X, Apache, MariaDB/MySQL, PHP, Perl.

Módulos: instalación, configuración

y uso

En los servidores web podemos configurar cualquier módulo que necesitemos, en general, sólo tenemos que seguir las instrucciones que nos da el desarrollador del módulo sobre cómo instalarlo.

En Windows para instalar un módulo, nos lo descargamos y lo instalamos siguiendo los pasos. Para configurar un módulo en IIS se accede al administrador del IIS, dentro del «Web Site» en el que queremos configurar un módulo accedemos a «Handler Mappings» y finalizamos la configuración del módulo.

La instalación de módulo en Linux se hace como cualquier otra aplicación, descargar el fichero y lo instalamos, puede darse el caso que el nuevo módulo no se añada a la configuración de Apache, entonces hay que añadirlo manualmente.

Hosts virtuales. Creación, configuración y utilización

El término Virtual Host se refiere a la práctica de ejecutar más de un sitio web (como `company1.example.com` y `company2.example.com`) en una sola máquina. Los hosts virtuales pueden estar » basados en IP «, lo que significa que tiene una dirección IP diferente para cada sitio web, o » basados en nombre «, lo que significa que tiene varios nombres que se ejecutan en cada dirección IP. El hecho de que se ejecuten en el mismo servidor físico no es evidente para el usuario final.

Apache fue uno de los primeros servidores en admitir hosts virtuales basados en IP desde el primer momento. Las versiones 1.1 y posteriores de Apache admiten hosts virtuales (vhosts) basados tanto en IP como en nombres. La última variante de hosts virtuales a veces también se denomina hosts virtuales basados en host o no IP .

Autenticación y control de acceso

Autenticación HTTP con PHP

Es posible usar la función `header()` para enviar un mensaje «Authentication Required» al navegador del cliente causando que se abra una ventana para ingresar usuario y password. Una vez se ha llenado el usuario y password, la URL contenida dentro del script PHP será llamada nuevamente con las variables predefinidas `PHP_AUTH_USER`, `PHP_AUTH_PW`, y `AUTH_TYPE` puestas por el nombre del usuario, password y el tipo de autenticación respectivamente. Esas variables predefinidas son encontradas en los arrays `$_SERVER` y `$HTTP_SERVER_VARS`. Ambos métodos de autenticación «Basic» y «Digest» (desde PHP 5.1.0) son soportados.

Autenticación HTTP Basic

En el contexto de una transacción HTTP, la autenticación de acceso básica es un método diseñado para permitir a un navegador web, u otro programa cliente, proveer credenciales en la forma de usuario y contraseña cuando se le solicita una página al servidor.

Autenticación HTTP Digest

Digest access authentication o Autenticación de acceso con resumen es uno de los métodos usados en servidores web para negociar credenciales, tales como nombre de usuario y contraseña, desde el navegador web. El segundo mecanismo es Autenticación de acceso básica. El método «Digest access authentication» es usado para confirmar la identidad de un usuario antes de servir información sensible, como el historial de transacciones de un banco. Se aplica una función hash a la contraseña antes de ser enviada sobre la red, lo que resulta más seguro que enviarla en texto plano como en la autenticación básica.

Autenticación de usuario

Se puede realizar una autenticación de usuario para entrar en una determinada página del siguiente modo utilizando sesiones.

El protocolo HTTPS

Los datos que circulan a través de la red entre aplicaciones son accesibles por terceras personas ajenas a la comunicación, es necesario evitarlo a toda costa mediante el uso de protocolos seguros.

También si importante asegurarse de que los datos no se modifiquen durante el transporte. Los protocolos que aseguran la información a nivel de capa de transporte son SSL y TLS.

El protocolo SSL

Originalmente diseñado por Netscape para establecer comunicaciones seguras con protocolos como HTTP o FTP. Permite negociar qué algoritmos se van a emplear, intercambiar las claves de encriptación y la autenticación de clientes y servidores.

Existen tres versiones del protocolo, la cuarta es una mejora del SSLv3 y se conoce con el nombre de TLS.

El protocolo TLS (Transport Layer Security)

Es una evolución del protocolo SSL (Secure Sockets Layer). La última propuesta de estándar está documentada en la referencia [RFC_2246].

Certificados. Servidores de

certificados

Un certificado de SSL (acrónimo de Secure Sockets Layer) es un tipo de seguridad digital que permite la comunicación cifrada entre un sitio web y un navegador web.

Un certificado SSL pueden usar el protocolo HTTPS para establecer una conexión segura con el servidor. Los certificados SSL/TLS funcionan al vincular digitalmente una clave criptográfica a la información de identificación de una empresa. Esto les permite cifrar las transferencias de datos de tal manera que no puedan ser descifrados por terceros.

El protocolo TLS funciona al tener tanto una clave privada como una pública, así como claves de sesión para cada sesión segura única. Cuando un visitante escribe una dirección con seguridad HTTPS en su navegador web o navega a través de una página segura, el navegador y el servidor web se conectan.

Durante la conexión inicial, las claves pública y privada se utilizarán para crear una clave de sesión, que luego se utilizará para cifrar y descifrar los datos que se transfieren. Esta clave de sesión seguirá siendo válida por un tiempo limitado y solo se utilizará para esa sesión en particular.

Despliegue de aplicaciones sobre servidores Web

Planteamos un despliegue concreto, se trata de un despliegue de un gestor de contenido. Cada gestor de contenidos tiene su propia forma de instalarse aunque en general las instalaciones son parecidas y siempre hay que seguir los mismos pasos.

Es importante indicar que la instalación del gestor de contenidos es independiente del sistema operativo, eso quiere decir que da igual instalar los gestores en sistemas

operativos libres o propietarios, la clave de la instalación está en el lenguaje de programación que se haya utilizado para programar el gestor, esto quiere decir que tenemos que tener instalado en el ordenador el intérprete del lenguaje de programación, por ejemplo si el gestor está desarrollado en PHP necesitamos bajarnos de la página <http://php.net/> la versión recomienda de PHP.

Los pasos generales para instalar y configurar un gestor de contenidos cualquiera son:

1. Tener previamente instalado Apache, MySQL y PHP.
2. Crear una base de datos para el gestor.
3. Descargar una versión actualizada del gestor.
4. Descomprimir el fichero descargado.
5. Acceder desde un navegador a la dirección url donde hemos descomprimido el gestor.
6. Instalar el gestor de contenidos siguiendo los pasos que aparecen en el instalador.