RESUMEN TEMA 2. Configuración y administración de servidores Web.

Albert Einstein: "Se debe hacer todo tan sencillo como sea posible, pero no más sencillo."

## 1.- Funcionamiento de un servidor Web

## 1.1.- Servicio de ficheros estáticos

Debemos diferenciar cuando accedemos a una página web entre código ejecutable en el lado del servidor y en el lado del cliente.

Si al acceder a una página web no es necesaria la intervención de código en el lado del servidor, entonces entenderemos que la página es estática, si por el contrario la intervención en el lado servidor y/o en el lado del cliente entenderemos que la página es dinámica.

Ofrecer páginas estáticas es simple, puesto que solamente se necesita que el servidor web disponga de soporte html/xhtml/css o solo html/xhtml.

La configuración y administración del servidor es simple: soporte mínimo base de instalación del servidor Apache.

El rendimiento del servidor, es bajo, como no se ejecuta código en el lado servidor, el coste de CPU y memoria es bajo y se traduce en mayor rapidez.

Para ofrecer páginas estáticas mediante el servidor Apache simplemente copias la página en la ruta correspondiente donde quieres.

Estructura de ficheros de Apache:



En la instalación de Apache se crea una página web en **/var/www/html/index.html** referenciada a través del archivo **/etc/apache2/sites-avaliable/000-default.conf** (contiene la configuración por defecto.

Ejercicio:

Copiar el archivo .zip al servidor ubuntuserver en el directorio raíz del usuario Ubuntu.

Scp ruta.zip ubuntu@dirip-server:/home/usuario

El fichero nuevo, descomprimimos y copiamos el contenido del directorio web-estatica al directorio **/var/www/html.**

Comprobar el despliegue desde el navegador.

## 1.2.- Contenido dinámico

Una página dinámica, necesita más recursos del servidor web que una página estática, ya que consume más tiempo de CPU y más memoria.

La configuración y administración del servidor web será más compleja, cuantos más módulos tengamos que soportar, más tendremos que configurar y actualizar.

Repercusión en la seguridad del servidor web, cuántos más módulos más posibilidades de problemas de seguridad. Algunos módulos son: *mod\_actions, mod\_cgi\_ mod\_cgid, mod\_ext\_filter, mod\_include, mod\_ldap, mod\_perl, mod\_php, mod\_python.*

***ACTIVAR O DESACTIVAR MODULOS****:* a2enmod , a2ensite, a2dismod, a2dissite

Debemos controlar que es lo que se ejecuta en el servidor.

Ejercicio:

Copiar y descomprimir el fichero .zip en el directorio raíz.

Copiar el contenido de la web dinámica al directorio /var/www/html.

Comprobamos el funcionamiento accediendo desde un navegador a la URL.

*Composer: es una herramienta de administración de dependencias para PHP que facilita la gestión de bibliotecas y paquetes en tus proyectos utilizado por los desarrolladores PHP.*

* *Instalación de dependencias: permite definir las bibliotecas y paquetes que tu proyecto necesita y los instala automáticamente a partir de registros de paquetes en línea.*
* *Autocarga de clases: genera un archivo de autocarga que simplifica la inclusión de clases en tu código eliminando la necesidad de incluir manualmente archivos de clase.*
* *Resolución de conflictos: resuelve automáticamente conflictos entre diferentes versiones de dependencias para garantizar la compatibilidad de las bibliotecas en tu proyecto.*
* *Actualización de dependencias: puedes actualizar las dependencias de tu proyecto fácilmente con Composer, lo que te permite mantener tu código actualizado con las últimas versiones de las bibliotecas.*
* *Creación de paquetes personalizados: te permite crear y distribuir tus propias bibliotecas y paquetes PHP de manera sencilla.*
* [*https://packagist.org/*](https://packagist.org/)

|  |
| --- |
| * sudo apt update * sudo apt install php-cli unzip * cd ~ * curl -sS [https://getcomposer.org/installer -o /tmp/composer-setup.php](https://getcomposer.org/installer%20-o%20/tmp/composer-setup.php) * HASH=`curl -sS [https://composer.github.io/installer.sig`](https://composer.github.io/installer.sig%60) * echo $HASH * php -r "if (hash\_file('SHA384', '/tmp/composer-setup.php') === '$HASH') { echo 'Installer verified'; } else { echo 'Installer corrupt'; unlink('composer-setup.php'); } echo PHP\_EOL;" * sudo php /tmp/composer-setup.php --install-dir=/usr/local/bin --filename=composer * composer |

## 1.3.- Protocolo Httpy Https

<https://howhttps.works/es/>

El protocolo de Tranferencia de Hipertexto (**http**) es un protocolo de comunicación utilizado en la WWW para la transferencia de datos entre un cliente y un servidor web. Consta de dos tipos principales:

**Solicitud (Request):** este mensaje es enviado por el cliente al servidor para solicitar un recurso web. Una solicitud http generalmente incluye métodos:

* Get: recuperar datos
* Post: enviar datos al servidor
* Put: actualizar recursos
* Delete: eliminar recursos

Además, contiene la URL del recurso solicitado y una serie de cabeceras que proporcionan información adicional.

**Respuesta (response):** el servidor responde a una solicitud http con un mensaje de respuesta que incluye un código de estado (200 OK, 404 Not Found), el tipo de contenido y el contenido real solicitado. También puede incluir cabeceras adicionales para proporcionar información adicional sobre la respuesta.

Estos mensajes http son la base de la comunicación entre los navegadores web y los servidores web, permitiendo la transferencia de datos y recursos a través de la WWW.

El protocolo https permite que la información viaje de forma segura entre el cliente y el servidor.

El protocolo **http** envía la información en texto claro, esto es, cualquiera que accediese a la información transferida entre el cliente y el servidor puede ver el contenido exacto y textual de la información.

El protocolo **https** requiere de certificados y siempre y cuando sean validados la información será transferida cifrada. Pero cifrar la información requiere un tiempo de computación, por lo que será perjudicado el rendimiento del servidor web.

Un servidor web, como Apache, puede emitir certificados, pero puede que en algún navegador sea interpretado como peligroso, esto suele ser debido a que los navegadores poseen en su configuración una lista de Entidades Certificadoras que verifican, autentican y dan validez a los certificados.

Eso no quiere decir que no puedes crear tus certificados en un servidor web, de hecho muchas empresas lo hacen, sobre todo para sitios internos o externos en lo que solamente puede acceder personal autorizado por la propia empresa.

El protocolo https utiliza cifrado sobre SSL/TLS que proporciona autenticación y privacidad. Entonces, si necesitas que la información viaje cifrada debes emplear el protocolo https, en caso contrario el protocolo http. Hay que dejar claro que la utilización del protocolo https no excluye ni impide el protocolo http, los dos pueden convivir en un mismo dominio.

Bien, pero ¿Cómo funciona?

En el protocolo http cuando escribes una dirección url en el navegador, antes de ver la página en el este existe todo un juego de protocolos, sin profundizar en todos ellos básicamente lo que ocurre es lo siguiente:

* Se traduce el dominio dns por una ip, una vez obtenida la ip se busca en ella si un servidor web aloja la página solicitada en el puerto 80, puerto tcp asignado por defecto al protocolo http. Si el servidor web aloja la página ésta será transferida a tu navegador.

Sin embargo, cuando escribes en el navegador una dirección url con llamada al protocolo https, el procedimiento es similar al anterior pero un poco más complejo:

* Así se traduce el dominio dns con una ip, con la ip se busca el servidor web que aloja la página solicitada en el puerto 443, puerto tcp asignado por defecto al protocolo https, pero ahora antes de transferir la página a tu navegador se inicia una negociación ssl, en la que entre otras cosas el servidor envía su certificado. Si el certificado es firmado por una Entidad Certificadora de confianza se acepta el certificado y se cifra la comunicación con él, transfiriendo así la página web de forma cifrada.

## 1.4.- Tips MIME

El estándar Extensiones Multipropósito de Correo de Internet o MIME (Multipurpose Internet Mail Extensions), especifica como un programa debe transferir archivos de texto, imagen, audio, vídeo o cualquier archivo que no esté codificado en US\_ASCII. MIME está especificado en seis RFC (Request for Commentes)

¿Cómo funciona?

Cuando un navegador intenta abrir un archivo el estándar MIME le permite saber con qué tipo de archivo está trabajando para que el programa asociado pueda abrirlo correctamente. Si el archivo no tiene un tipo de MIME especificado el programa asociado puede suponer el tipo de archivo mediante la extensión del mismo.

¿Cómo lo hace? El navegador solicita la página web y el servidor antes de transferirla confirma que la petición requerida existe y el tipo de datos que contiene. Esto último, mediante referencia al tipo MIME al que corresponde. Este diálogo, oculto al usuario, es parte de las cabeceras http, protocolo que se sigue en la web.

En ese diálogo, en las cabeceras respuestas del servidor existe el campo Content-type donde el servidor avisa del tipo de MIME de la página. Con esta información, el navegador sabe cómo debe presentar los datos que recibe.

**Tres** lugares distintos: el servidor web, la propia página web y el navegador.

* El servidor debe estar capacitado y habilitado para manejar diversos tipos MIME.
* En el código de la página web se referencia tipos MIME constantemente en etiquetas *link, script, object, form, meta, etc.*
* El enlace a un archivo hoja de estilo css.
* El enlace a un archivo código javascript.
* Con las etiquetas meta podemos hacer que la página participe en el diálogo servidor-cliente, especificando datos MIME.
* El navegador del cliente también participa, además de estar capacitado para interpretar el concreto tipo MIME que el servidor le envía, también puede, en el diálogo previo de datos, informar que tipos MIME puede aceptar la cabecera http\_accept.

## 1.4.1.- Configurar el servidor para enviar los tipos MIME correctos

En un servidor web podemos especificar el tipo MIME por defecto para aquellos archivos que el servidor no pueda identificar automáticamente como pertenecientes a un tipo concreto, esto es, para aquellos los cuales no se resuelven según su extensión.

Dos directivas: DefaultType y ForceType

* DefaultType asigna la cabecera Content-Type a cualquier archivo cuya MIME no pueda determinarse desde la extensión del archivo.
* ForceType hace que todos los ficheros cuyos nombres tengan una equivalencia con lo que se especifique sean servidos como contenido del tipo MIME que se establezca.

Ejemplos:

* DefaultType text/plain : Esto significa que cuando el navegador web solicita y recibe ese archivo como respuesta, desplegará el contenido como un archivo de texto.
* DefaultType text/html : Desplegará el contenido como un archivo HTML.
* ForceType image/gif : Desplegará el contenido como un archivo de imagen gif.
* ForceType video/mp4 : Desplegará el contenido como un archivo de vídeo mp4.

En el servidor web Apache existe el archivo **/etc/apache2/mods-available/mime.conf** donde encontrarás una referencia al archivo **/etc/mime.types** el cual contiene la lista de tipos MIME reconocidos por el servidor.

## 2.- Servidores virtuales (VirtualHosts). Creación, configuración y utilización.

Cada servidor virtual es único e independiente de los demás, pero cada servidor virtual que no esté incluido heredará la configuración principal: apache2conf.

Existen dos tipos de servidores virtuales: basados en nombres de dominio del servidor y basados en IP. La diferencia radica en el dato que usa el servidor Apache para enviar las peticiones a uno u otro servidor virtual.

El proceso de creación de un servidor virtual consiste en crear un fichero de configuración en el directorio **/etc/apache2/sites-available.**

Para activar o desactivar los servidores virtuales se usan estos comandos:

* **A2ensite**: habilita el servidor virtual, crea un enlace simbólico desde **/etc/apache2/sites-available** a **/etc/apache2/sites-enabled.**
* A2dissite: deshabilita un servidor virtual. Elimina el enlace simbólico de **/etc/apache2/sites-available** a **/etc/apache2/sites-enabled.**

Linux: el archivo que se debe modificar para la resolución de nombres de dominio en direcciones IP es **/etc/hosts.**

Windows: el archivo que se debe modificar es **C:\Windows\System32\drivers\etc\|hosts.**

## 2.1.- Servidores virtuales basados en nombre.

Ejercicio: gatitos.net

1. Creamos el fichero gatitos.net.conf en la ruta **/etc/apache2/sites-available**
2. Añadimos la configuración para un servidor virtual.
3. **<VirtualHost IP\_Servidor\_Web:puerto>** : IP define el servidor web donde se aloja el sitio web. \* el servidor está escuchando en todos los interfaces que se haya definido en el servidor. Puerto por defecto 80 definido en la directiva **Listen**. Se puede usar varias.
4. **DocumentRoot**: ruta donde está alojada la página web en el servidor.
5. **ServerName**: indica el nombre del dominio que aparece en el URL de acceso al sitio web desde el navegador.
6. **ServerAlias**: permite asociar el servidor virtual a otros nombres de dominio.
7. Descargamos el archivo y habilitamos el sitio web.
8. Y por último comprobamos con un navegador web: [www.gatitos.net](http://www.gatitos.net)

## 2.2.- Servidores virtuales basados en IP.

Ejercicio: buscaminas.net

Ahora vamos a crear un nuevo servidor virtual basado en la IP a la que está asociado en la configuración. La directiva VirtualHost va a especificar la IP de uno de los interfaces con los que está configurado el servidor.

Es más difícil de mantener si las IP del servidor web se modifican con cierta frecuencia.

Para el despliegue seguimos el procedimiento similar utilizado para el servidor virtual basado en nombre.

Pero en vez de un asterisco colocaremos la dirección IP de nuestro servidor. Dicha configuración permite al servidor Apache redirigir todas las peticiones que llegan hacia esa dirección IP a este servidor virtual.

Copiamos y subimos el fichero de buscaminas al servidor.

Habilitamos el sitio y damos los permisos necesarios.

Comprobamos con un buscador el sitio dirigiéndonos a: [www.buscaminas.net](http://www.buscaminas.net)

## 2.3.- Directivas de configuración

Vamos a presentar algunas directivas de configuración adicionales que se pueden usar en a definición de los servidores web.

* **Directory**: se utiliza para aplicar configuraciones específicas a un directorio en el servidor web. Esta directiva permite definir reglas y restricciones para ese directorio, como opciones de autorización, límites de acceso, configuraciones de seguimiento de enlaces simbólicos y más.
* **DirectoryIndex**. Especifica el nombre del archivo que se debe buscar cuando se accede a un directorio. Por lo general, se establece en index.html, index.php, u otros archivos de índice.
* **Options**. Establecer varias opciones de configuración para un directorio o un servidor virtual específico. Estas opciones controlan el comportamiento y las características del servidor web para las solicitudes que se manejan en ese contexto. La directiva Options puede tener múltiples valores que se pueden combinar para personalizar la configuración.
  + **Indexes**: Permite o prohíbe la generación automática de listados de directorios cuando no se encuentra un archivo de índice en unndirectorio. Si se habilita, se mostrará una lista de archivos en el directorio si no hay un archivo de índice presente.
  + **FollowSymLinks**: Permite la navegación simbólica, lo que permite a los usuarios seguir enlaces simbólicos dentro del sistema de archivos. Esto habilita la capacidad de seguir enlaces simbólicos para acceder a recursos en otros directorios.
  + **MultiViews**: Habilita la búsqueda de archivos con nombres similares si no se encuentra un archivo con el nombre exacto en una solicitud. Por ejemplo, si se solicita "archivo" y no se encuentra, Apache buscará "archivo.html" o "archivo.php", si están presentes.
* **AllowOverride**. controla qué configuraciones se pueden anular o sobrescribir mediante archivos ` .htaccess` en un directorio específico. Los archivos `.htaccess` son archivos de configuración que permiten a los administradores de sitios web modificar la configuración de Apacheen un directorio determinado, lo que brinda flexibilidad para ajustar la configuración en un nivel más local. La directiva `AllowOverride` acepta varios valores para determinar qué configuraciones pueden ser anuladas en un directorio. Algunos de los valores más comunes incluyen:
  + **None**: No se permiten anulaciones en ningún nivel. Los archivos `.htaccess` se ignoran completamente.
  + **All**: Se permiten todas las anulaciones. Los archivos `.htaccess` pueden sobrescribir prácticamente todas las configuraciones de Apache, incluyendo la mayoría de las opciones de configuración.
  + **AuthConfig**: Permite la anulación de configuraciones relacionadas con la autenticación y la autorización de usuarios, como AuthType, AuthName, AuthUserFile, etc.
  + **FileInfo**: Permite la anulación de configuraciones relacionadas con la información del archivo, como AddType, AddOutputFilter, DefaultType, etc.
  + **Indexes**: Permite la anulación de configuraciones relacionadas con la generación de listados de directorios, como Options +Indexes, IndexOptions, etc.
  + **Limit**: Permite la anulación de configuraciones relacionadas con la limitación de acceso a través de directivas como Order, Deny,Allow, etc.
  + **Options**: Permite la anulación de configuraciones relacionadas con las opciones del servidor web, como Options, DirectoryIndex,AddHandler, etc.