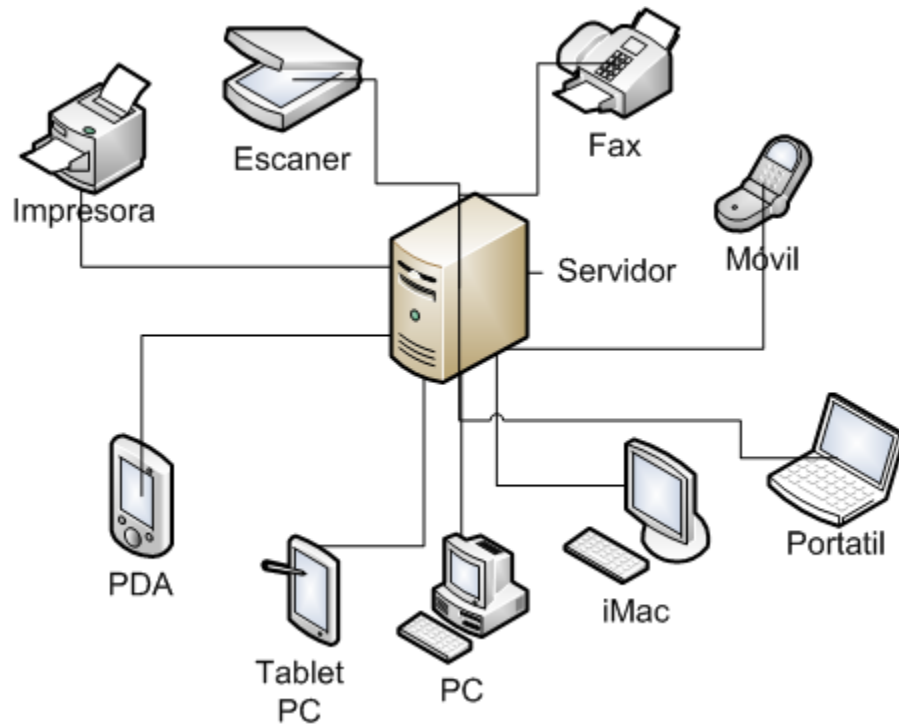


2.1 Clasificación de los servidores

Un servidor es un equipo que forma parte de una red y provee servicios a otros equipos cliente.



Existen muchos tipos de servidores con distintos tipos de funciones algunos tipos son:

Servidores de archivos

Un servidor de ficheros es el encargado de gestionar el uso de un disco duro compartido por parte de varios usuarios y de que en un determinado momento solamente un único usuario pueda estar utilizando un fichero concreto. Cada ordenador trabajará como si su ordenador tuviese un disco duro propio.

Ejemplo: Si tenemos un servidor y tenemos 3 usuarios GAM1, GAM2, y GAM3 como el uso de una PC cada uno de los usuarios no pueden ver los archivos del otro usuario a menos que estén compartidos, en este servidor no se ven los archivos ni los usuarios existente una vez que ya se hizo el inicio de sesión en uno de los 3 usuarios.

Servidores de base de datos

Maneja la administración de una base de datos común. Distribuyen el procesamiento de la información entre una aplicación, que es ejecutada en la estación de trabajo cliente, y el manejador de bases de datos que se ejecuta en el servidor. Con esto se reduce, además de la carga de procesamiento del servidor, el tráfico de la red. Estos servidores pueden manejar

las bases de datos de dos maneras, bases de datos centralizadas y bases de datos distribuidas.

Ejemplo: Dentro de un site en un banco se tiene un servidor de BD para almacenar toda la información de los clientes que se ocupa, este servidor es el encargado además de almacenar de arrojar todas las consultas que realiza el administrador de bases de datos.

Servidores de correo

Son aquellos servidores que se encargan de distribuir los correos electrónicos y guardar todos los mensajes de correo.

Ejemplo: Al enviar un correo los servidores son un intermediario entre el emisor y el receptor del correo debido a que al momento de salir el correo electrónico primero llega o hace una parada al servidor de correos, donde este almacena el correo completo y después envía al destinatario.

Servidores Telnet (Telnet Servers)

Un servidor telnet permite a los usuarios entrar en un ordenador huésped y realizar tareas como si estuviera trabajando directamente en ese ordenador.

Ejemplo: Si necesitamos ayuda de soporte técnico de cualquier empresa o producto estos servidores ayudan al distribuidor del servicio conectarse vía remota a nuestra PC con las configuraciones correspondientes.

Servidores Proxy

Es un programa u ordenador que hace de intermediario entre dos ordenadores.

Ejemplo: Nosotros nos identificamos como “GAM1” y queremos hacer una petición al servidor llamado “GAM2”. Si la petición la hacemos directamente, “GAM2” sabe que “GAM1” le hizo una petición. En cambio, si usamos un proxy que sería un intermediario que por ejemplo podemos llamar “GAM3”, la petición se la haríamos a GAM3 y éste se la haría a GAM2. De esta manera, GAM2 no sabe que quien realmente ha hecho la petición es GAM1. A su vez, el intermediario puede bloquear determinadas peticiones. Por ejemplo, si pedimos a un proxy que tiene bloqueadas las extensiones .xxx, que nos muestre la página web “amanecer.xxx”, dicha página web no se nos mostrará porque el proxy actúa bloqueándola.

Servidores DNS

Son las siglas de Domain Name System. Es un sistema por el que se asocia una información con un nombre de dominio.

Ejemplo: cuando introducimos una ruta url en nuestro navegador de internet del tipo <http://www.aprenderaprogramar.com>. Una vez hemos introducido esta ruta, dicha

información es enviada a un servidor DNS que lo que hace es determinar en qué lugar se encuentra esa página web alojada y nos conecta con

Servidores FTP

Acrónimo de File Transfer Protocol o Protocolo de transferencia de archivos. Es un protocolo utilizado para la transferencia de archivos entre un cliente y un servidor, permitiendo al cliente descargar el archivo desde el servidor o al servidor recibir un archivo enviado desde un cliente. Por defecto FTP no lleva ningún tipo de encriptación permitiendo la máxima velocidad en la transferencia de los archivos.

Servidores Dedicados

Normalmente al ser los servidores equipos más potentes y por tanto más caros, se suelen compartir entre varias personas o empresas, permitiéndoles a todos tener un servicio de gran calidad y a un mínimo precio. En este caso se dice que se trata de un servidor compartido.

Ejemplo: Lo usa exclusivamente una sola persona o empresa si esta puede hacer frente al gasto económico que supone. En este caso se dice que el servidor es “dedicado”

En la siguiente tabla se presentan los servidores más populares o los más usados.

DENOMINACIÓN DEL SERVIDOR	DESCRIPCIÓN
Servidor de Correo	Es el servidor que almacena, envía, recibe y realiza todas las operaciones relacionadas con el e-mail de sus clientes.
Servidor Proxy	Es el servidor que actúa de intermediario de forma que el servidor que recibe una petición no conoce quién es el cliente que verdaderamente está detrás de esa petición.
Servidor Web	Almacena principalmente documentos HTML (son documentos a modo de archivos con un formato especial para la visualización de páginas web en los navegadores de los clientes), imágenes, videos, texto, presentaciones, y en general todo tipo de información. Además se encarga de enviar estas informaciones a los clientes.

Servidor de Base de Datos	Da servicios de almacenamiento y gestión de bases de datos a sus clientes. Una base de datos es un sistema que nos permite almacenar grandes cantidades de información. Por ejemplo, todos los datos de los clientes de un banco y sus movimientos en las cuentas.
Servidores Clúster	Son servidores especializados en el almacenamiento de la información teniendo grandes capacidades de almacenamiento y permitiendo evitar la pérdida de la información por problemas en otros servidores.
Servidores Dedicados	Como ya expresamos anteriormente, hay servidores compartidos si hay varias personas o empresas usando un mismo servidor, o dedicados que son exclusivos para una sola persona o empresa.

Administración de servidores: aspectos importantes a considerar

En la actualidad es bastante fácil montar una instalación para un servidor dedicado basado en Linux y ponerlo en línea. Ya sea para montar un sitio web, una aplicación o cualquier otra necesidad relacionada, montar un servidor dedicado basado en Linux puede ser una tarea que nos lleve solo unas cuantas horas realizar incluso para un desarrollador que no tenga tanta experiencia en hacerlo siguiendo las muchísimas guías que al respecto existen en internet. Incluso existen también muchas compañías que rentan servidores dedicados con las que podemos tener un servidor corriendo en unas cuantas horas.

En cambio, la facilidad de instalar un servidor y comenzar a utilizarlo contrasta mucho con la necesidad de mantenerlo y estarlo vigilando constantemente para asegurarse de que el sistema es estable y tiene lo necesario para mantenerse en línea en un futuro cercano. El éxito de mantener un servidor activo y en línea en el corto plazo depende directamente de la previsión que tengamos por adelantado.

El problema de la falta de previsión respecto al mantenimiento de un servidor web es que uno se puede “salir con la suya” durante meses o años, con lo que pareciera que nuestro servidor corre perfectamente, pero esta falta de previsión puede volverse una situación crítica durante los peores momentos por los que atraviesa nuestro sistema, como los impactos de un tráfico elevado repentino, un disco duro que falla o un intento de hackeo.

Algunos de los aspectos principales que debemos de cuidar en la administración de nuestro servidor dedicado son los siguientes:

Backups o respaldos: el corazón de nuestra previsión

Un aspecto que puede parecer bastante obvio y que probablemente la mayoría de los administradores de sistemas cuidan, al menos en parte, es el de la realización de respaldos de la información. Si no tenemos un esquema sólido de respaldos, simplemente hay que hacerlo ya. No hay otra manera de estar seguros que nuestra información está a salvo más que teniéndola respaldada de tal forma que si algo catastrófico sucede con nuestro servidor, nosotros podemos recuperar al menos la mayor parte de nuestra información desde nuestra fuente de respaldos. Existen ciertas tecnologías a explorar para apoyarnos a elaborar nuestra estrategia de backups como lo son rsync, tar y similares. También debemos de tener cuidado de como respaldamos otro tipo de información como son las bases de datos de MySQL. Dependiendo de nuestros requerimientos podremos elaborar nuestra propia estrategia de backup, pero en general debemos de pensar en que esta debe considerar las siguientes condiciones:

- Debe correr con suficiente regularidad (diaria, cada dos días, etc.)
- Debe mantener varias versiones de nuestro respaldo (a veces es conveniente mantener un respaldo diario, uno semanal y uno mensual)

- Debe de limpiar los respaldos viejos
- Debe realizarse en localidades físicas externas a dónde se encuentra nuestro servidor o infraestructura principal (¿que tal si se incendia el centro de datos donde se encuentra el servidor principal y también el de backup?)
- La información debe estar muy segura en nuestra infraestructura de respaldo también, no solo en la principal.
- Hay que verificar que se están incluyendo todos los datos críticos para poder recuperar nuestro sistema.

En alguna publicación futura profundizaremos sobre las estrategias de backup adecuadas para mantener nuestra infraestructura a flote.

Probar nuestros backups: si ya hicimos respaldos, hay que verificar que funcionen

Una vez que ya tenemos una excelente (o por lo menos suficiente) estrategia de respaldos para nuestro servidor, es importantísimo que verifiquemos que los respaldos automatizados se están haciendo correctamente y que los archivos producidos por nuestros respaldos son válidos (no están corruptos) y se pueden utilizar efectivamente para restaurar nuestro sistema en caso de una catástrofe de datos.

Rotación de logs: que no se coman tu espacio

Un aspecto secundario, pero no por eso menos importante, es verificar que los logs o registros de actividad que nuestro servidor web genera de forma automáticamente están siendo limpiados cada cierto tiempo, esto para prevenir que sigan creciendo y creciendo sin parar y eventualmente terminen por acabarse todo nuestro espacio disponible en el peor momento posible y sin que nos hayamos podido prevenir.

Monitorear los recursos: el “check-up” de la salud de nuestro servidor

Importantísimo: debemos de monitorear con regularidad las cargas de nuestro CPU, el uso de la memoria, el espacio en disco disponible, el ancho de banda usado. Esto es importantísimo para saber la salud de nuestro sistema y detectar posibles upgrades que debamos realizar antes de que el hardware de nuestro servidor se vea rebasado por la demanda del mismo y se nos vaya a “caer” un tiempo antes de que podamos hacer un upgrade no previsto.

Monitoreo de procesos y servicios: ¿está todo funcionando en éste momento?

Mantener Apache, MySQL, los servicios de e-mail (pop, smtp, imap) y otros servicios corriendo puede ser crucial para el funcionamiento de nuestro servidor. Es muy recomendable apoyarnos en alguna herramienta que automatice el proceso de monitoreo de

servicios para que no nos enteremos que algún servicio de nuestro servidor no está en línea hasta que un usuario se queja amargamente con nosotros.

Endurecer nuestro servidor (Hardening): Solo los servidores rudos sobreviven

El proceso de hardening o endurecimiento consiste en muchas acciones distintas que se pueden tomar para fortalecer la seguridad de nuestro servidor. Para comenzar, es muy importante que sepamos qué procesos están corriendo en nuestro servidor, qué puertos tenemos abiertos, si tenemos o no habilitada alguna herramienta de prevención de intrusiones, etc. Es importantísimo investigar un poco más y llevar la vanguardia en cuanto a los procedimientos de seguridad que podemos llevar en nuestro servidor previniendo cualquier tipo de ataque.

Actualizaciones de seguridad: a veces tedioso pero muy importante

Muchos de los creadores de los programas que utilizamos en nuestro servidor, regularmente liberan nuevos parches y actualizaciones de seguridad que desarrollan al descubrirse nuevas vulnerabilidades en sus sistemas. El proceso de aplicar estos parches y actualizaciones es muchas veces olvidado y/o pasado por alto por algunos administradores de sistemas, sin embargo el ignorar estas actualizaciones de seguridad es una de las principales rutas por las que los atacantes pueden ingresar a un sistema (ya que en general estas vulnerabilidades de los programas son bien conocidas y publicadas en internet y son relativamente fáciles de emplear para vulnerar un sistema).

CONCLUSIONES

Conclusión García Perrusquia Luis Antonio:

Tener un servidor hoy en día es algo indispensable para el uso de las Tic's, dentro de la rana de redes y de cualquier tipo de rama.

Tener el servidor para realizar la tarea apropiada es algo que se debe tener en cuenta a la hora de montar dicha red, además de tener buen controlado los accesos y los recursos, debido a que una mala administración nos puede generar pérdida de información valiosa.

Conclusión Hernández Moreno Cesar Adrián:

En la exposición dada en clase se explicó los diferentes tipos de servidores que existen como su funcionalidad de cada uno, también los más usados, los más seguros y los porque se usan esos, así como su clasificación de los mismos.

También se explicaron las recomendaciones que se pueden hacer cuando se está trabajando en un servidor como lo que se explicó que fueron los respaldos, Backups, etc.

Conclusión Reyes Jiménez Marco Yazu-a:

Un servidor también puede ser un proceso que entrega información o sirve a otro proceso. El modelo Cliente-servidor no necesariamente implica tener dos ordenadores, ya que un proceso cliente puede solicitar algo como una impresión a un proceso servidor en un mismo ordenador.

Conclusión Romero Silva Manuel Alejandro:

Con el tema abordado en la pasada presentación, dimos un panorama base sobre los servidores y su administración, se vieron temas como la clasificación de servidores y su administración.

En la clasificación se dio información acerca de los servidores más usados en la actualidad.

Referente a la administración se habló acerca de los puntos considerados más importantes para tener un servidor estable.