

# CURSO LINUX ADMINISTRATOR



## Servicio SSH Y FTP

- INSTRUCTOR: RUDY SALVATIERRA  
RODRIGUEZ

LINUXLANDIA

# CONEXIONES REMOTAS



- En la practica uno normalmente no tiene acceso físico a los servidores normalmente se encuentran en un ambiente cerrado y con acceso restringido
- Por tal motivo tenemos que configurar el servidor para que nos de acceso remotamente

# PROGRAMAS DE ACCESO REMOTO



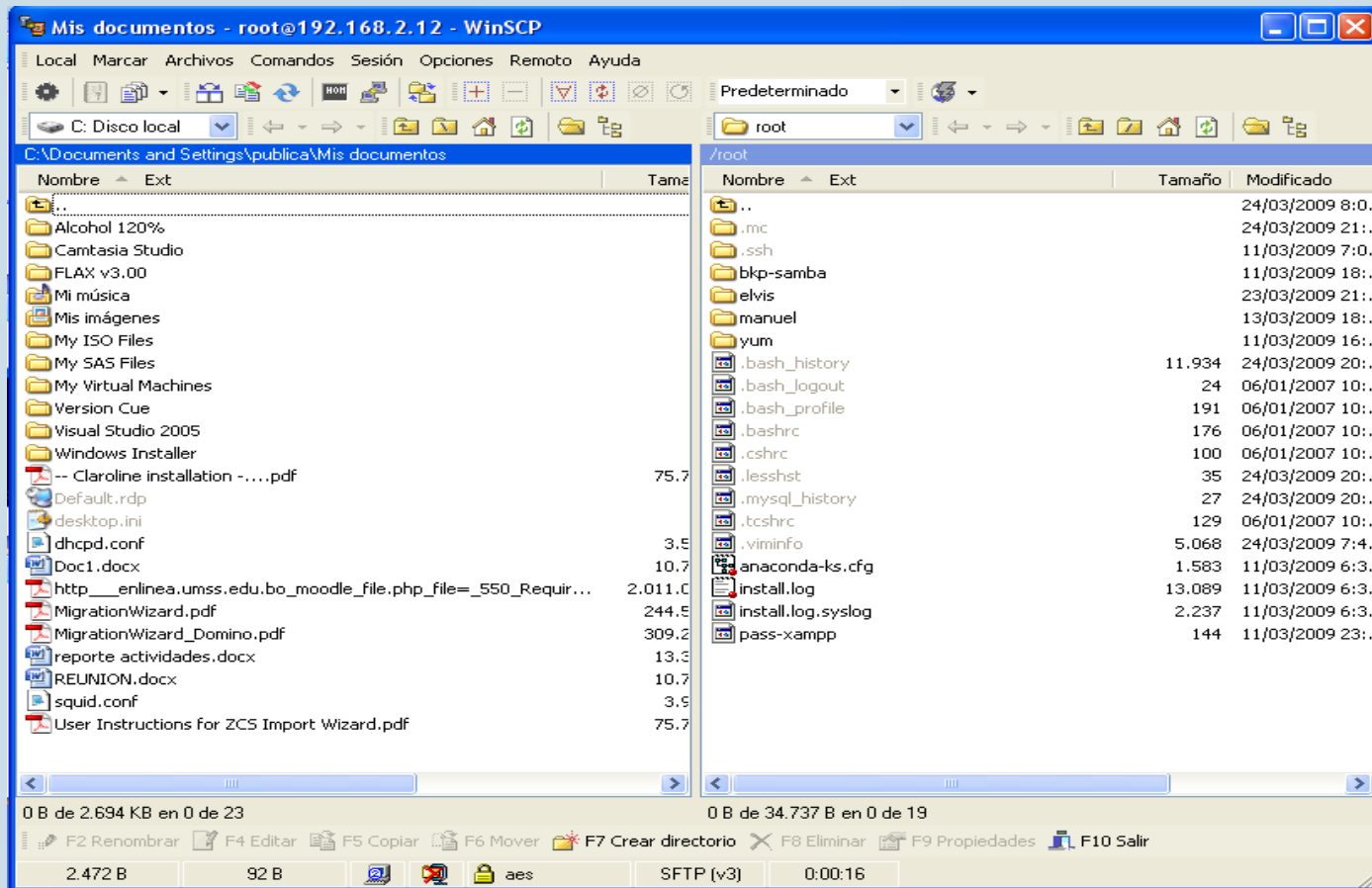
- Uno de los programas de acceso son:
  - telnet y ssh
- Telnet ya no se usa mucho en la actualidad ya que la información transmitida esta en texto plano
- Ssh es lo que se utiliza ya que la información se transmite encriptado.
  - Para ssh podemos usar los siguientes programas
    - ✦ Putty
    - ✦ winscp

# PUTTY



```
root@matrix:~  
Reloading Squid HTTP Proxy 3.0 configuration files.  
done.  
kronos:~# mcedit /etc/squid3/squid.conf  
  
kronos:~# exit  
logout  
Connection to 192.168.2.1 closed.  
[root@matrix ~]# mcedit /opt/lampp/etc/php.ini  
  
[root@matrix ~]# /opt/lampp/lampp restart  
Stopping XAMPP for Linux 1.7...  
XAMPP: Stopping Apache with SSL...  
XAMPP: Stopping MySQL...  
XAMPP: Stopping ProFTPD...  
XAMPP stopped.  
Starting XAMPP for Linux 1.7...  
XAMPP: Starting Apache with SSL (and PHP5)...  
XAMPP: Starting MySQL...  
XAMPP: Starting ProFTPD...  
XAMPP for Linux started.  
[root@matrix ~]# lv  
lvchange      lvcreate      lvextend      lvmchange      lvmdump      lvmsar      lv  
lvconvert     lvdisplay     lvm           lvmdiskscan    lvmsadc      lvm.static   lv  
[root@matrix ~]# lv
```

# WINSCP



# ADMINISTRACION REMOTA



- Para que podamos usar estas herramientas necesitamos que estén configurados el servicio de SSH en el servidor.

## Servicio SSH

- Es un servicio el cual nos da acceso a un equipo remoto para que podamos usar sus recursos como si estuviésemos usando el equipo directamente.

# SERVICIO SSH



- El nombre del demonio es el “SSHD”, viene por defecto instalado en la mayoría de las distribuciones
- En caso de que no este instalado el paquete que se tiene que instalar es openssh.

## OPENSSSH

- El protocolo ssh (en su versión OpenSSH) provee de un conexión encriptada y comprimida mucho más segura. Todas las distribuciones actuales incorporan el cliente ssh y el servidor sshd por defecto.

# SERVICIO SSH:CLIENTE



**/etc/ssh/ssh\_config:** valores predeterminados del cliente SSH, las entradas mas importantes son:

- ✓ **Protocol:** especifica la versión del protocolo SSH. Valor predeterminado 2
- ✓ **PreferredAuthentications:** Especifica el metodo de autenticación para el cliente SSH2.
- ✓ **ForwardX11:** desactivado por defecto.



# SERVICIO SSH:SERVIDOR



**/etc/ssh/sshd\_config:** valores predeterminados del servidor SSH que los clientes usan para conectarse con la cuenta de este host.

- ✓ **ListenAddress:** especifica las direcciones locales que sshd debe escuchar. Se permiten múltiples opciones.
- ✓ **AllowTcpForwarding:** desactivado por defecto.
- ✓ **X11Forwarding:** desactivado por defecto

# SERVICIO SSH:SERVIDOR



- ✓ **AllowUsers:** Lista de usuarios que se pueden conectar al sistema.
- ✓ **DenyUsers:** Lista de usuarios que no se pueden conectar al sistema.
- ✓ **AllowGroups:** Lista de grupos de usuarios que se pueden conectar
- ✓ **DenyGroups:** Lista de grupos que no se pueden conectar.
- ✓ **PermitRootlogin:** permite que el usuario root acceda mediante ssh.

# SERVICIO SSH:EJEMPLO



Lo siguiente iniciara una conexión ssh desde un cliente:

```
$ ssh prueba@matrix
```

Si quisiéramos dar permisos solamente a ciertos usuarios y a ciertos ips aumentamos la siguiente línea al final del archivo.

```
allowUsers server@192.168.137.70 para limitar el  
acceso a clientes remotos a usuarios específicos
```

# SERVICIO SSH:EJEMPLO



- En el servidor crearse tres usuarios :
  - usuario1, usuario2, usuario3
- Crearse 2 grupos
  - Administración
  - Soporte
- El usuario1 pertenezca al grupo administrador
- El usuario2 pertenezca al grupo soporte
- El usuario3 no pertenezca a ningún grupo
- Permitir solo que se loguee los que pertenezcan al grupo de soporte

# SERVICIO SSH:EJEMPLO



- En el servidor crearse tres usuarios :
  - usuario1, usuario2, usuario3
- Crearse 2 grupos
  - Administración
  - Soporte
- El usuario1 pertenezca al grupo administrador
- El usuario2 pertenezca al grupo soporte
- El usuario3 no pertenezca a ningún grupo
- Permitir solo que se loguee los que pertenezcan al grupo de soporte

# SERVICIO FTP



El Protocolo de transferencia de archivos (FTP) es uno de los protocolos más viejos y populares que se encuentran en la Internet hoy día. Su objetivo es el de transmitir archivos exitosamente entre máquinas en una red sin que el usuario tenga que iniciar una sesión en el host remoto o que requiera tener conocimientos sobre cómo utilizar el sistema remoto. FTP permite a los usuarios acceder a archivos en sistemas remotos usando un conjunto de comandos estándar muy simples.

# SERVICIO FTP



**FTP** requiere de múltiples puertos de red para funcionar correctamente. Cuando una aplicación cliente FTP inicia una conexión a un servidor FTP, abre el puerto 21 en el servidor conocido como el puerto de comandos. Se utiliza este puerto para arrojar todos los comandos al servidor. Cualquier petición de datos desde el servidor se devuelve al cliente a través del puerto de datos. El número de puerto para las conexiones de datos y la forma en la que las conexiones son inicializadas varía dependiendo de si el cliente solicita los datos en modo activo o en modo pasivo.

# SERVICIO FTP:VSFTP



## **VSFTPD (Very Secure FTP Daemon)**

Es un sustento lógico utilizado para implementar servidores de archivos a través del protocolo FTP. Se distingue principalmente porque sus valores por defecto son muy seguros y por su sencillez en la configuración, comparado con otras alternativas como Wu-ftp. Actualmente se presume que VSFTPD es quizá el servidor FTP más seguro del mundo.

VSFTPD está diseñado desde la base para ser rápido, estable y lo más importante, seguro.



# SERVICIO FTP:SEGURIDAD



El modelo de seguridad utilizado por vsftpd tiene tres aspectos principales:

- **Clara separación de procesos privilegiados y sin privilegios** Procesos separados manejan tareas diferentes y cada uno de estos procesos se ejecuta con los privilegios mínimos requeridos para la tarea.
- **La mayoría de los procesos se ejecutan enjaulados en un ambiente chroot** Siempre que sea posible, se cambia la raíz de los procesos al directorio compartido; este directorio se considera luego como la jaula chroot.

# SERVICIO FTP:ARCHIVOS



- **/etc/rc.d/init.d/vsftpd** El script de inicialización utilizado para iniciar, detener o volver a cargar vsftpd.
- **/etc/pam.d/vsftpd** El archivo de configuración de los Pluggable Authentication Modules (PAM) para vsftpd. Este archivo define los requerimientos que debe cumplir un usuario para conectarse a un servidor FTP.
- **/etc/vsftpd/vsftpd.conf** El archivo de configuración para vsftpd.

# SERVICIO FTP:ARCHIVOS



- **/etc/vsftpd.ftpusers** Una lista de los usuarios que no tienen permitido conectarse a vsftpd. Por defecto esta lista incluye a los usuarios root, bin y daemon.
- **/etc/vsftpd.user\_list** Este archivo se puede configurar para negar o permitir el acceso a los usuarios listados, dependiendo de si la directriz userlist\_deny está configurada a YES (por defecto) o a NO en /etc/vsftpd/vsftpd.conf.
- **El directorio /var/ftp/** El directorio que contiene los archivos servidos por vsftpd.

# SERVICIO FTP: CONFIGURACION



- **anonymous\_enable=YES|NO** Para habilitar el acceso anónimo al servidor FTP solo deberá teclear la palabra YES , caso contrario desea tener deshabilitada esta opción solo deberá teclear la palabra NO.
- **local\_enable=YES|NO** Para habilitar o negar los accesos autenticados a los usuario locales.
- **write\_enable=YES|NO** Para habilitar o negar la escritura en el servidor FTP deberá buscar la siguiente línea
- **ftpd\_banner=Bienvenido al Servidor FTP de Linux Para Todos** Para agregar este mensaje al servidor FTP deberá buscar la siguiente linea y editarla.

# SERVICIO FTP: CONFIGURACION



- **chroot\_local\_users=YES** para enjaular a todos los usuarios locales
- **chroot\_list\_enable=YES |NO** Para limitar a los usuarios a trabajar en su propia carpeta de trabajo
- El siguiente parámetro se encuentra en función del anterior, de forma que si usted lo habilito también tendrá
- que habilitar este ultimo, para ello solo deberá borrar el  
caracter                      de                      numero                      (#)  
**chroot\_list\_file=/etc/vsftpd/chroot\_list**

# SERVICIO FTP:USUARIO LOCAL



- **local\_umask** Especifica el valor de umask para la creación de archivos. Observe que el valor por defecto está en forma octal (un sistema numérico con base ocho).
- **passwd\_chroot\_enable** Cuando se activa junto con la directriz `chroot_local_user`, `vsftpd` cambia la raíz de los usuarios locales basado en la ocurrencia de `./.` en el campo del directorio principal dentro de `/etc/passwd`.
- **user\_config\_dir** Especifica la ruta a un directorio que contiene los archivos de configuración con los nombres de los usuarios locales.

# SERVICIO FTP: CONEXION



- **dual\_log\_enable** Cuando se activa en conjunto con `xferlog_enable`, `vsftpd` escribe simultáneamente dos archivos: un registro compatible con `wu-ftp` al archivo especificado en la directriz `xferlog_file` (por defecto `/var/log/xferlog`) y un archivo de registro estándar `vsftpd` especificado en la directriz `vsftpd_log_file` (por defecto `/var/log/vsftpd.log`).
- **log\_ftp\_protocol** Cuando está activado en conjunto con `xferlog_enable` y con `xferlog_std_format` configurada a `NO`, se registran todos los comandos y respuestas.

# SERVICIO FTP:CONEXION



- **syslog\_enable** Cuando se activa en conjunto con `xferlog_enable`, todos los registros que normalmente se escriben al archivo estándar `vsftpd` especificado en la directriz `vsftpd_log_file`.
- **vsftpd\_log\_file** Especifica el archivo de registro de `vsftpd`. Para que se utilice este archivo, `xferlog_enable` debe estar activado y `xferlog_std_format` debe ser bien sea `NO` o, si está en `YES`, entonces `dual_log_enable` debe estar activado.



# SERVICIO FTP:CONEXION



- **xferlog\_enable** Cuando se activa, vsftpd registra las conexiones (solamente formato vsftpd) y la información de transferencia, al archivo de registro especificado en la directriz `vsftpd_log_file` (por defecto es `/var/log/vsftpd.log`).
- **xferlog\_file** Especifica el archivo de registro compatible con `wu-ftp`. Para que se utilice este archivo, `xferlog_enable` debe estar activado y `xferlog_std_format` debe tener el valor de `YES`.

# SERVICIO FTP:FIREWALL



- Luego de instalar el servicio Vsftpd agregamos las reglas de firewall para los puertos 21 y 20 que utiliza ftp.

```
firewall-cmd --add-port=20 /tcp --permanent
```

```
firewall-cmd --add-port=21 /tcp --permanent
```

- Para que los cambios hagan efecto se coloca en siguiente comando que actualiza las reglas de firewall.

```
firewall-cmd --reload
```

# SERVICIO FTP:COMANDOS



- Los comandos generales tanto para servidores como para cliente de FTP por línea de comandos son los siguientes:
  - **get:** Para bajar ficheros
  - **put:** Para subir ficheros
  - **lid:** Especifica el directorio local sobre el que vamos a trabajar,
  - **cd:** se utiliza para moverse a través de los directorios
  - **delete:** borra un fichero del servidor remoto
  - **oppend:** permite reanudar una descarga que haya sido interrumpida,

# SERVICIO FTP:COMANDOS



- **open:** abre una sesión en el FTP
- **close:** termina la sesión con el FTP
- **bye:** cierra la sesión y sale del programa de forma que todas las sesiones abiertas se cierran,
- **ls:** muestra el contenido del servidor remoto
- **mput:** sube varios ficheros al servidor
- **mget:** baja varios ficheros al ordenador local
- **user:** sirve para cambiar el usuario con el que nos hemos conectado al FTP.