

Esquema de Permisos

Introducción

Dotar de acceso FTP y SFTP es proporcionar al usuario una herramienta muy completa para la gestión de archivo. Tal y como hemos visto en los apartados *Configuración del servicio: vsftpd* y *Enjaulado SFTP* el acceso se limita al directorio */home* de cada usuario. Mediante la configuración *vsftpd* también hemos restringido el acceso a determinados archivos pero *sftp-server* no dispone de tales opciones.

Aunque los servidores de FTP disponen de estas opciones, es bueno tener una política de permisos para garantizar la seguridad del sistema.

Actuaciones

Se limitan los permisos a los mínimos para garantizar el acceso único de cada usuario y evitar revelar información del sistema.

Esquema de Permisos RH

Para poder trabajar con los usuarios y permitir a apache (usuario httpd) acceder y/o escribir a determinados archivos propongo este esquema, en realidad es el que sugiere red hat.

Por ejemplo supongamos que el grupo de usuarios (tbiada y apache) quieren trabajar en el directorio home para el usuario '/home/tbiada'.

Creamos un grupo de trabajo común, en nuestro caso usamos la siguiente codificación ht IP_SERVIDOR (ULTIMO GRUPO) ID_USUARIO

```
/usr/sbin/groupadd htxxxxxx
```

Para vincular los contenidos del directorio con el grupo

```
chgrp -R htxxxxxx /home/username
```

Ahora agregamos al usuario apache (que podrá gestionar los archivos) al directorio home de este usuario

```
/usr/bin/gpasswd -a apache htxxxxxx
```

Para permitir que todos los usuarios del grupo puedan modificar los archivos debemos asignar los permisos necesarios

```
# Privilegios típicos  
chmod 775 /home/username
```

```
# Privilegios restrictivos  
chmod 660 /home/username (No permite listar directorios)
```

No obstante cuando un usuario crea un archivo el grupo por defecto será el que quede asociado a éste archivo, para lograr que los archivos que cree el usuario apache (grupo por defecto apache) activamos el setgid, que que asigna a todo lo creado en el directorio los mismos permisos de que disponga el directorio (htxxxxxx).

Los bits de permisos espaciales tienen el siguiente significado: sticky (1000), SGID (2000) y SUID (4000).

```
chmod 2775 /home/username
```

At this point, because each user's default umask is 002, all members of the emacs group can create and edit files in the /usr/lib/emacs/site-lisp/ directory without the administrator having to change file permissions every time users write new files.

¿Que es iddover.net?

Iddover Hosting es una iniciativa española en el sector de servidores dedicados. Nace en contraposición de los servicios actuales de hosting . Pretende ofrecer un hosting de alta calidad gestionable a través de un potente panel propio que se adecua a los requisitos de seguridad y que proporciona al cliente potentes herramientas al alcance de un solo click

Desde 69€ dispondrás de un servidor dedicado administrado auditado con todas las medidas de seguridad ya aplicadas.

<http://www.iddover.net>