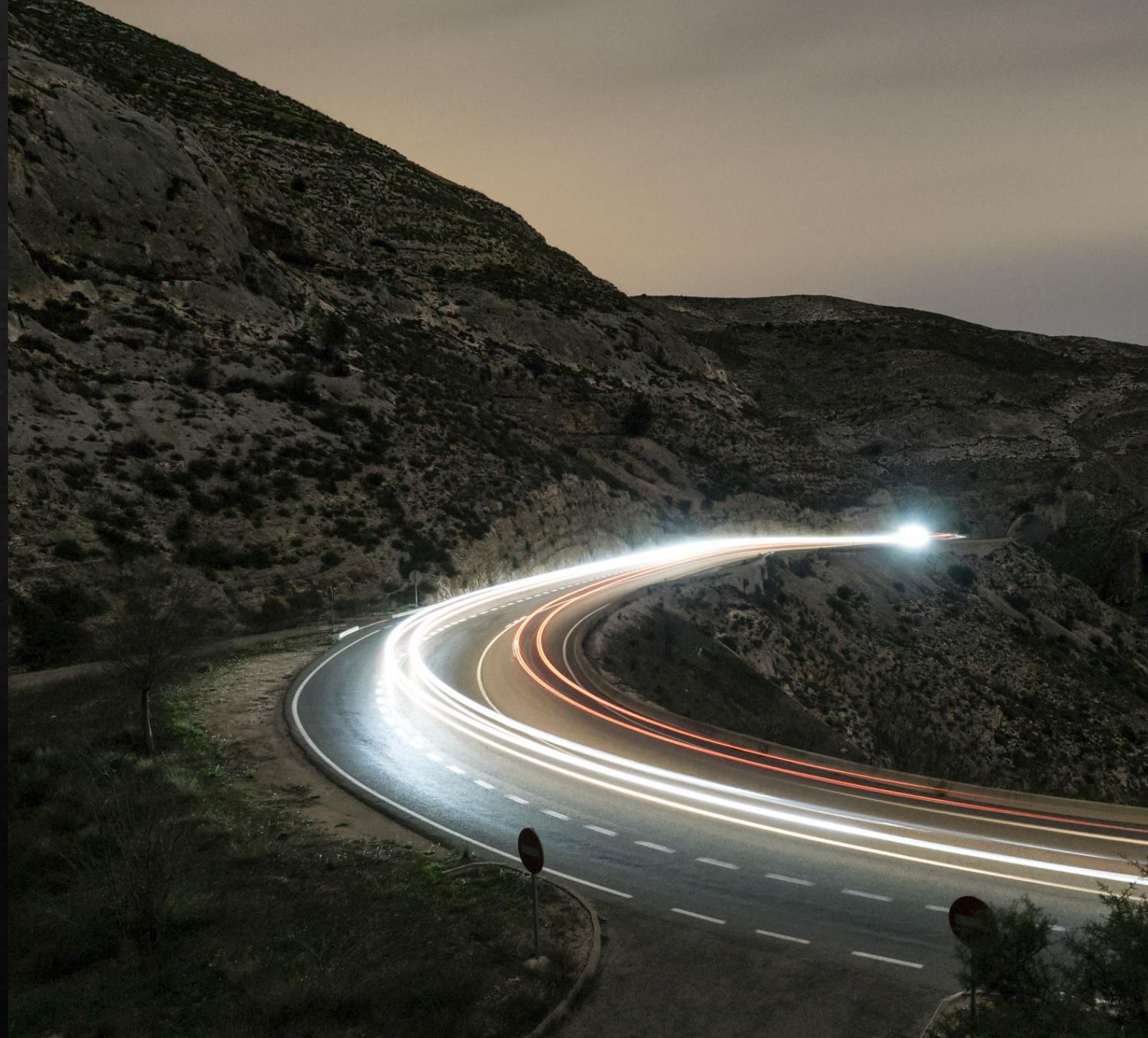
PROTOCOLO DE TRANSFERENCIA DE ARCHIVOS. Enjaular usuarios con SSH

UNIDAD 3

DESPLIEGUE DE APLICACIONES WEB



SSH File Transfer Protocol

SFTP permite una serie de operaciones sobre archivos remotos.

SFTP Transfer Protocol

- Transferencia de archivos entre sistemas remotos
- Conexión segura sobre SSH
- Comprobación autenticación del servidor
- Comunicación segura, se cifran los datos intercambiados.
- TCP/22
- Autenticación por clave pública y privada
- Autenticación usuario / contraseña

Clientes SFTP/SCP

- Clientes en línea de comandos:
  - SFTP
  - SCP
  - Conexión a un equipo remoto con SSH podemos usar comandos get, put, mput, mget para transferir archivos.
- Clientes gráficos
  - WinSCP, Filezilla,…
  - Editores de texto, NotePad++
  - Integración en IDE (Netbeans, Eclipse, PHPStorm, …

SFTP enjaulado

- ¿Qué es enjaular a un usuario?
  - Aislar o enjaular a los usuarios dentro de un directorio, y no puede acceder al resto de directorios del sistemas de ficheros del servidor remoto.
  - Es una técnica mediante la que proporciona al usuario un acceso limitado al sistema de ficheros Linux.
- Pasos a seguir:
  - Crear el grupo de usuario
  - Modificar el fichero de configuración del servicio /etc/ssh/sshd_config
  - Reiniciar SSH

Vamos a enjaular al usuario operadorweb, DAW201, DAW202,..

REQUISITOS

El home del usuario donde se enjaula pertenece al usuario root del grupo root

No tiene permisos de escritura

Es necesario, crear una carpeta con permisos de escritura y que pertenezca al usuario creado.

Creación de usuario

Comandos Linux para creación del usuario

- Creación del grupo
  - sudo groupadd ftpusers
- Creación del usuario y cambio de password
  - sudo useradd –g www-data –G ftpusers -m –d /var/www/nombredeusuario nombredeusuario
- Cambiar la constraseña
  - sudo passwd nombredeusuario

Comandos Linux carpeta home del usuario

- El propietario del directorio jaula y los directorios sobre este, debe ser root.
- El home del usuario pertenece al root
  - sudo chown root:root /var/www/nombredeusuario
- Eliminar el permiso de escritura
  - sudo chmod –w /var/www/nombredeusuario

  - Por lo tanto, el usuario no tendría privilegios de escritura sobre su directorio. Para evitar ese problema se crea un directorio ‘public_html’, dentro de la jaula, que sea de propiedad y es allí donde él pueda escribir como leer archivos.

Crear carpeta public_html

- Creación de la carpeta public_html
  - sudo mkdir /var/www/nombredeusuario/public_html
- Permisos de public_html
  - sudo chmod 2775 –R /var/www/nombredeusuario/public_html
- Propietarios de public_html
  - sudo chown nombredeusuario:www-data –R /var/www/nombredeusuario/public_html

SFTP enjaulado

- Crear un grupo que pertenecen los usuarios que vamos a enjaular.

```
miadmin@DAW-USED:~$ cat /etc/group |grep sftp
sftpusers:x:1001:operadorweb,SMR1,PROFESOR1,PROFESOR2,PROFESOR3,PROFESOR4,PROFESOR5,DAW218,DAW201,DAW202,D
AW203,DAW204,DAW205,DAW206,DAW207,DAW208,DAW209,DAW210,DAW211,DAW212,DAW213,DAW214,DAW215,DAW216,DAW217,CO
MUN1,COMUN2,COMUN3,COMUN4,COMUN5,COMUN6,COMUN7,COMUN8,COMUN9,COMUN10,COMUN11,COMUN12,COMUN13,COMUN14,COMUN
15,COMUN16,COMUN17,COMUN18
```

Editar /etc/ssh/sshd_config

Servicio SFTP restringido usando las directivas: ForceCommand y ChrootDirectory

Editar /etc/ssh/sshd_config

```
# Subsystem sftp /usr/lib/openssh/sftp-server

Subsystem sftp internal-sftp
```

miadmin@DAW-USED: ~

```
 GNU nano 2.5.3                  Archivo: /etc/ssh/sshd_config


Match Group sftpusers
ChrootDirectory %h
ForceCommand internal-sftp -u 2
AllowTcpForwarding yes
PermitTunnel no
X11Forwarding no
```

Control de acceso al servicio SFTP

Directivas permitir el acceso:

- AllowUsers
- AllowGroups

Directivas para denegar el acceso

- DenyUsers
- DenyGroups

https://www.openssh.com/

DOCUMENTACIÓN