

## 1. Instalación de servicios y configuraciones

**Cuestión 1. Liste los argumentos de yum y apt necesarios para instalar, buscar y eliminar paquetes.**

Para instalar paquetes:

```
yum install <paquete>
apt-get install <paquete>
```

Para buscar paquetes:

```
yum search <información>
apt-cache search <información>
```

\*El orden depende del número de coincidencias.

Para eliminar paquetes:

```
yum remove|erase <paquete>
apt-get remove <paquete>      *Desinstalar
apt-get --purge <paquete>     *Eliminar ficheros de configuración
```

**Cuestión 2. Cree un repositorio local en CentOS desde la imagen .iso con la que instaló CentOS.**

Establecemos la .iso como disco.

Creamos un fichero al que llamaremos local.repo y escribimos lo siguiente:

```
[local]
name=local repository
baseurl=file:///etc/yum.repos.d/repoCd
gpgcheck=1
```

Creamos el repositorio con el siguiente comando:

```
sudo createrepo /etc/yum.repos.d/repoCd
```

## 2. Gestión de los cortafuegos (Firewalls)

**Cuestión 3. ¿Cómo se denominan y por quién pueden ser usados los puertos comprendidos entre 1024 y 65535?**

Los puertos comprendidos entre 1024 y 49151 se denominan puertos registrados y pueden ser usados por cualquier aplicación.

Los puertos comprendidos entre 49152 y 65535 se denominan puertos dinámicos o privados y pueden ser usados por aplicaciones con conexiones P2P.

**Cuestión 4. Pruebe a abrir y cerrar varios puertos en CentOS y Windows Server. Ilústrelolo con capturas de pantalla. Asegúrese de abrir el puerto 21, 22 y 80 a los servicios asociados por defecto.**

CentOS.

Abrimos la aplicación Aplicaciones/Varios/Cortafuego.



Marcamos la zona “public”.



Abrimos la pestaña Puertos.



Pulsamos Añadir.

**Puerto y Protocolo**


Por favor ingrese el puerto y protocolo.

Puerto / Rango de puertos:


Protocolo: tcp ▾

Cancelar
Aceptar

Introducimos el número de puerto que vamos a abrir y pulsamos Aceptar.

 **Se necesita autenticación**

System policy prevents to change the firewall configuration

 **Víctor Monserrat Villatoro**

Contraseña:

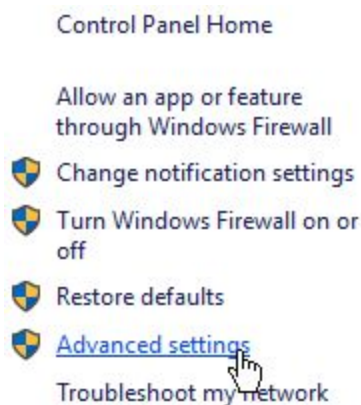
Cancelar
Autenticar

Autenticamos y tras añadir los tres puertos nos quedará algo parecido a lo siguiente:

Puerto	Protocolo
21	tcp
22	tcp
80	tcp

Windows Server.

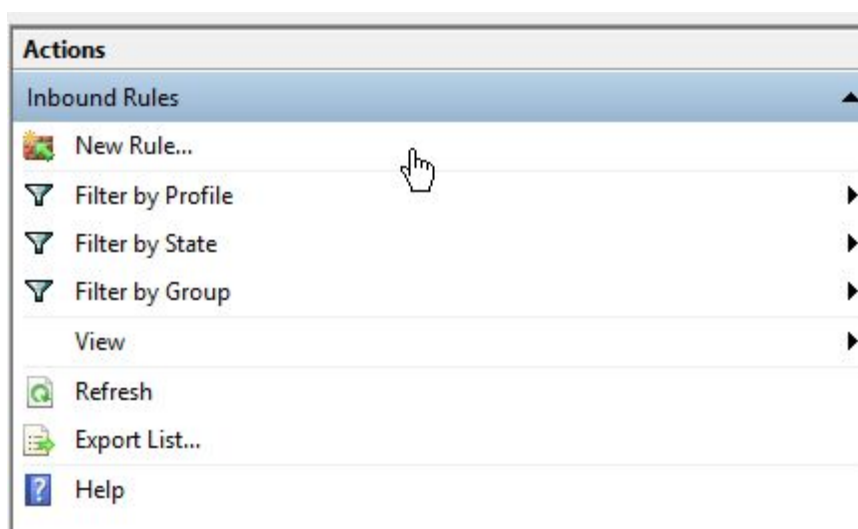
Abrimos Windows Firewall.



Seleccionamos Advanced settings.



Seleccionamos Inbound Rules.



Seleccionamos New Rule...

What type of rule would you like to create?

☐ **Program**  
Rule that controls connections for a program.

☒ **Port**  
Rule that controls connections for a TCP or UDP port.

☐ **Predefined:**  
Active Directory Domain Services  
Rule that controls connections for a Windows experience.

☐ **Custom**  
Custom rule.

Seleccionamos Port.

Does this rule apply to TCP or UDP?

☒ **TCP**

☐ **UDP**

Does this rule apply to all local ports or specific local ports?

☐ **All local ports**

☒ **Specific local ports:**   
Example: 80, 443, 5000-5010

Seleccionamos TCP y especificamos los puertos.

What action should be taken when a connection matches the specified conditions?

☒ **Allow the connection**  
This includes connections that are protected with IPsec as well as those are not.

☐ **Allow the connection if it is secure**  
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.

☐ **Block the connection**

Seleccionamos Allow the connection.

When does this rule apply?

☒ **Domain**  
 Applies when a computer is connected to its corporate domain.

☒ **Private**  
 Applies when a computer is connected to a private network location, such as a home or work place.

☒ **Public**  
 Applies when a computer is connected to a public network location.

Dejamos seleccionado todas las opciones.

Name:

Description (optional):

Elegimos un nombre para nuestra nueva regla y una descripción opcionalmente.

### 3. Configuración del servicio de acceso remoto a la consola (Secure Shell) - Ubuntu y CentOS

**Cuestión 5. ¿Para qué sirve la opción -X? ¿Qué ocurre si ejecutamos el comando gedit?**

La opción -X sirve para poder usar de manera gráfica el servicio.  
 Si ejecutamos el comando gedit abrimos la aplicación gedit en la máquina desde la que accedemos remotamente pero la actividad quedará almacenada en la máquina que accedemos, así si guardamos el fichero, quedará guardado en esta.

**Cuestión 6. Muestre la secuencia de comandos y las modificaciones a los archivos correspondientes para permitir acceder a la consola remota sin introducir la contraseña.**

Generamos la clave pública con el comando:

```
ssh-keygen -t rsa
```

Pasamos esta clave a nuestra máquina virtual con el comando:

```
ssh-copy-id i32moviv@192.168.1.9
```

Ahora conectamos a nuestra máquina remotamente sin usar contraseña.

```
ssh i32moviv@192.168.1.9
```

**Cuestión 7. ¿Qué archivo es el que contiene la configuración de sshd?**

El fichero que contiene la configuración de sshd es el /etc/ssh/sshd\_config.

**Cuestión 8. Indique si es necesario reiniciar el servicio ¿Cómo se reinicia un servicio en Ubuntu? ¿y en CentOS? Muestre la secuencia de comandos para hacerlo.**

Para que estas acciones tengan efecto debemos reiniciar el servicio, para ello usamos el comando:

```
service sshd restart
```

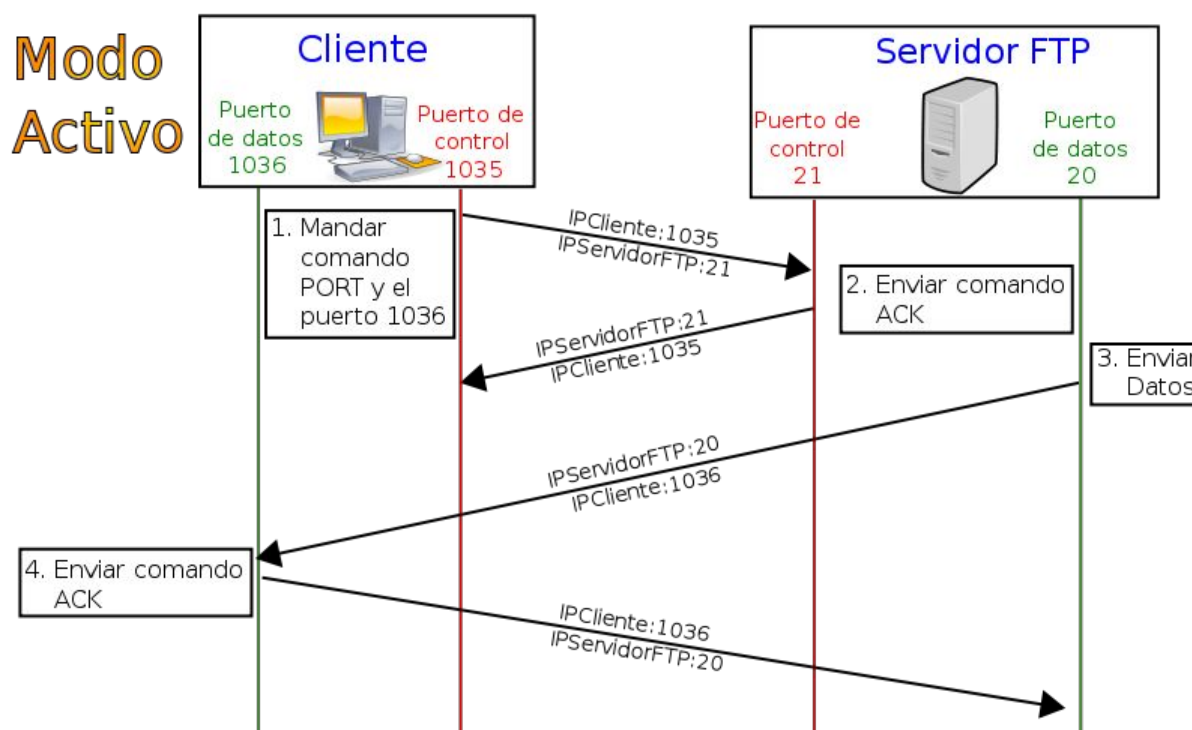
#### **4. Configuración del servicio FTP - CentOS y Windows**

**Cuestión 9. Existen dos modos de conexión FTP, detalle el funcionamiento de cada uno y sus diferencias.**

FTP admite dos modos de conexión del cliente. Estos modos se denominan activo (o Estándar, o PORT, debido a que el cliente envía comandos tipo PORT al servidor por el canal de control al establecer la conexión) y pasivo (o PASV, porque en este caso envía comandos tipo PASV). Tanto en el modo Activo como en el modo Pasivo, el cliente establece una conexión con el servidor mediante el puerto 21, que establece el canal de control.



Modo activo.

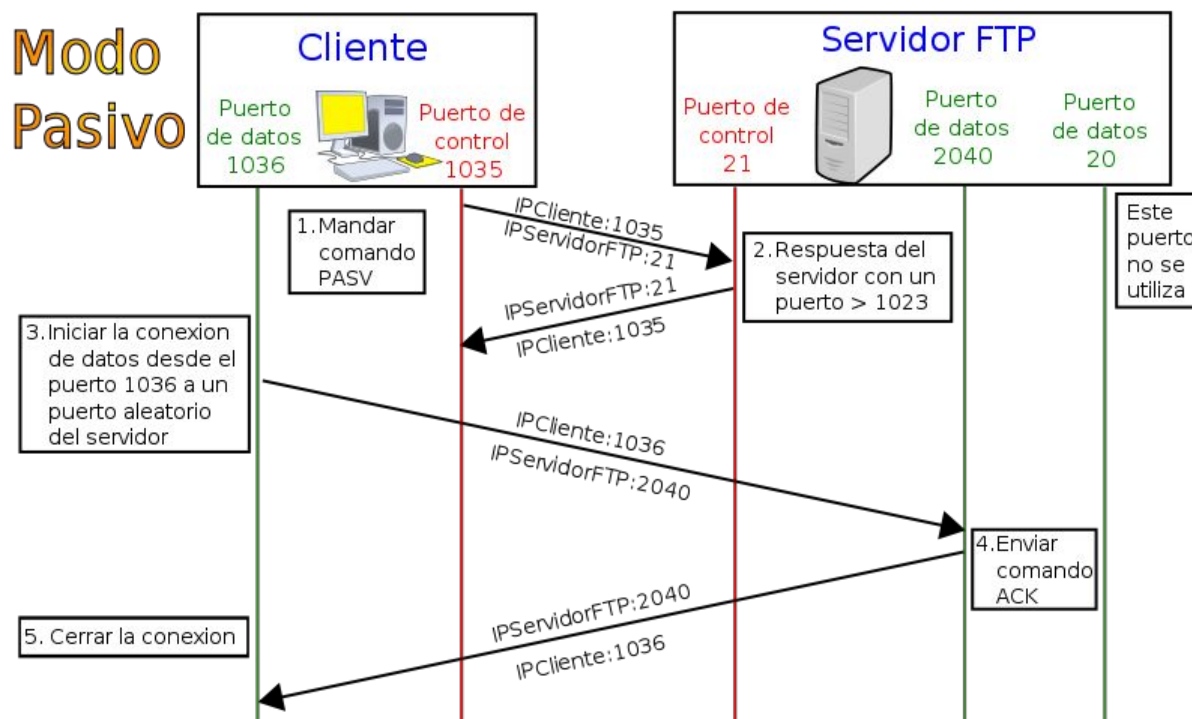


En modo Activo, el servidor siempre crea el canal de datos en su puerto 20, mientras que en el lado del cliente el canal de datos se asocia a un puerto aleatorio mayor que el 1024. Para ello, el cliente manda un comando PORT al servidor por el canal de control indicándole ese número de puerto, de manera que el servidor pueda abrirle una conexión de datos por donde se transferirán los archivos y los listados, en el puerto especificado.

Lo anterior tiene un grave problema de seguridad, y es que la máquina cliente debe estar dispuesta a aceptar cualquier conexión de entrada en un puerto superior al 1024, con los problemas que ello implica si tenemos el equipo conectado a una red insegura como Internet. De hecho, los cortafuegos que se instalen en el equipo para evitar ataques seguramente rechazarán esas conexiones aleatorias. Para solucionar esto se desarrolló el modo pasivo.



Modo pasivo.



Cuando el cliente envía un comando PASV sobre el canal de control, el servidor FTP le indica por el canal de control, el puerto (mayor a 1023 del servidor. Ejemplo: 2040) al que debe conectarse el cliente. El cliente inicia una conexión desde el puerto siguiente al puerto de control (Ejemplo: 1036) hacia el puerto del servidor especificado anteriormente (Ejemplo: 2040).

Antes de cada nueva transferencia tanto en el modo Activo como en el Pasivo, el cliente debe enviar otra vez un comando de control (PORT o PASV, según el modo en el que haya conectado), y el servidor recibirá esa conexión de datos en un nuevo puerto aleatorio (si está en modo pasivo) o por el puerto 20 (si está en modo activo). En el protocolo FTP existen 2 tipos de transferencia en ASCII y en binarios.

**Cuestión 10. ¿Qué es SELinux y qué funcionalidad tiene? Realice las modificaciones necesarias para que el servicio vsftpd proporcione la funcionalidad mencionada en el punto anterior.**

SELinux (Security-Enhanced Linux ) es un módulo de seguridad para el kernel de Linux para controlar los accesos. También se incluye el control de acceso obligatorio del departamento de defensa de los Estados Unidos de América.

Las modificaciones las hacemos todas en /etc/vsftpd/vsftpd.conf

Para permitir el acceso utilizando los usuarios del anfitrión:  
local\_enable=YES

Para no permitir la conexión a usuarios anónimos:  
anonymous\_enable=NOT

Para establecer mensaje de bienvenida:  
ftpd\_banner=MENSAJE DE BIENVENIDA

Para activar los registros:  
dual\_log\_enable = YES

**Cuestión 11. Muestre la secuencia de comandos que utilizaría para subir una imagen al directorio /home/usuario/practica3 del servidor ftp de CentOS desde la máquina anfitriona. Muestre también el log que ha registrado el servicio al realizar las operaciones anteriores.**

Activamos el servicio ftp en la máquina virtual para que permita el acceso y usamos el siguiente usuario desde la máquina que estamos usando:

```
ftp 192.168.1.9
```

Autenticamos y ya estamos conectados. Ahora accedemos al directorio que queramos y subimos la imagen con:

```
put img.png
```

Ya hemos subido nuestra imagen. El log registra lo siguiente:

El día de la semana, mes, día del mes, hora, minutos, segundos y año que se ha realizado la operación.

La dirección desde la que se ha realizado esta.

La dirección de destino de la operación.

El usuario de la máquina virtual al que va dirigido.

**Cuestión 12. Muestre la secuencia de comandos que utilizaría para subir una imagen al directorio /usuario/practica3 del servidor ftp de Windows desde la máquina anfitriona.**

Creamos un sitio FTP y lo instalamos.

Nos dirigimos al Internet Information Services y seleccionamos la opción de agregar un sitio FTP...

Le damos un nombre y le asignamos un directorio.

Configuramos entre otros parámetros la dirección ip y puerto.

Ahora hacemos ftp y la ip de nuestro servidor y el proceso es como siempre.

#### **5. Configuración de un Servidor Web Básico - CentOS, Ubuntu y Windows**

**Cuestión 13. Enumere otros servidores web (mínimo 3 servidores sin considerar Apache, IIS ni nginx)**

BitNami, Cherokee, AOLserver, DroidPHP, NAWWS...

**Cuestión 14. Muestre la secuencia de comandos y configuraciones que usaría para configurar el servidor apache instalado en CentOS para que sirva la página web alojada en el directorio practica3.**

Modificamos /etc/httpd/conf/httpd.conf y escribimos nuestro usuario y grupo en User y Group en lugar de apache. En <Directory ... cambiamos el directorio por "/home/i32moviv/practica3"

Ejecutamos: `setsebool -P httpd_read_user_content 1`

y reiniciamos apache con: `systemctl restart httpd`

**Cuestión 15. Muestre la secuencia de comandos y configuraciones que usaría para configurar el servidor apache instalado en Ubuntu para que sirva la página web alojada en el directorio practica3.**

Modificamos /etc/httpd/conf/httpd.conf y escribimos nuestro usuario y grupo en User y Group en lugar de apache. En <Directory ... cambiamos el directorio por "/home/i32moviv/practica3"

Añadimos una línea: `ServerName 127.0.0.1`

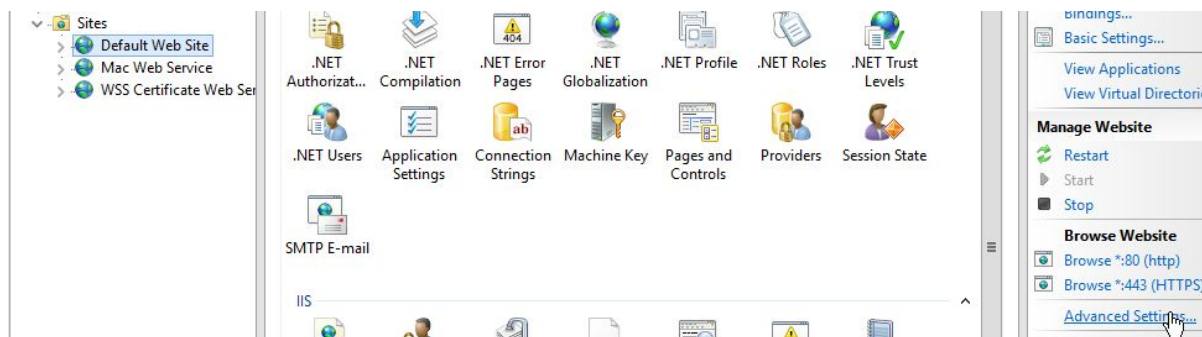
y reiniciamos: `apachectl restart`

**Cuestión 16. Muestre la secuencia de comandos que usaría para ver si el servicio php está instalado y qué versión se ha instalado en CentOS y en Ubuntu.**

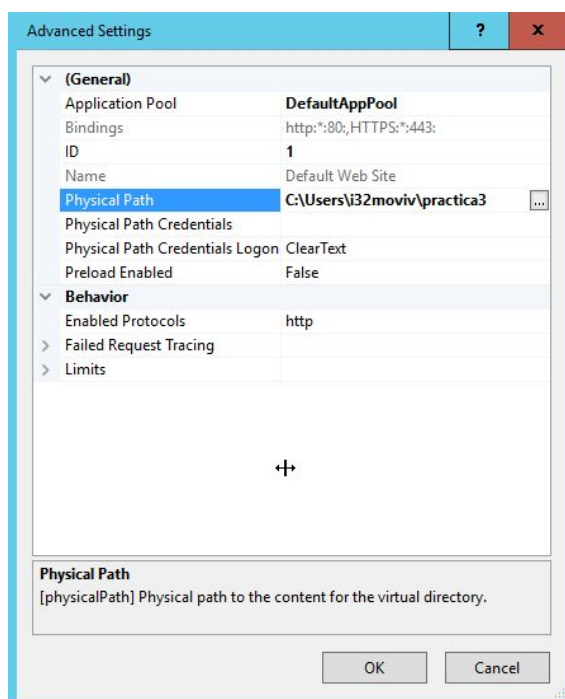
Con `php -v` nos muestra la versión instalada de php en nuestra máquina si este paquete está instalado.

**Cuestión 17. Muestre la secuencia de comandos y configuraciones que usaría para configurar el servidor IIS instalado en Windows Server para que sirva la página web alojada en el directorio practica3.**

Entramos en Internet Information Services Manager.



Seleccionamos Default Web Site y clicamos en Advanced Settings...



Indicamos la ruta y al abrir localhost debemos verla.

## 6. Cuestiones propias.

**Cuestión 18.** Hemos subido archivos por ftp con put <archivo>, pero ¿con qué comando bajamos archivos por ftp?

Con el comando get <archivo>

**Cuestión 19.** ¿Cómo se denominan los puertos del 0 al 1023?

Puertos reservados para el sistema.

**Cuestión 20.** Explique para qué son los puertos 20, 21 y 80.

20/tcp	<a href="#">FTP</a> File Transfer Protocol (Protocolo de Transferencia de Ficheros) - datos
21/tcp	<a href="#">FTP</a> File Transfer Protocol (Protocolo de Transferencia de Ficheros) - control
80/tcp	<a href="#">HTTP</a> HyperText Transfer Protocol (Protocolo de Transferencia de HiperTexto) ( <a href="#">www</a> )