6.L Servicios Web en Linux (Apache)

- No estudiaremos cómo crear contenido, sino aspectos relativos a:
  - Instalación
  - Configuración
  - Seguridad
  - Administración

6.L Instalación

- `yum install httpd`
- `firewall-cmd --permanent --add-port=80/tcp`
- `firewall-cmd –add-port=443/tcp`
- `firewall-cmd --reload`

6.L Arranque

- Iniciar manualmente

```
systemctl start httpd.service
```

- Para que arranque al iniciar el servidor

```
systemctl enable httpd.service
```

- Para comprobar el status del servicio

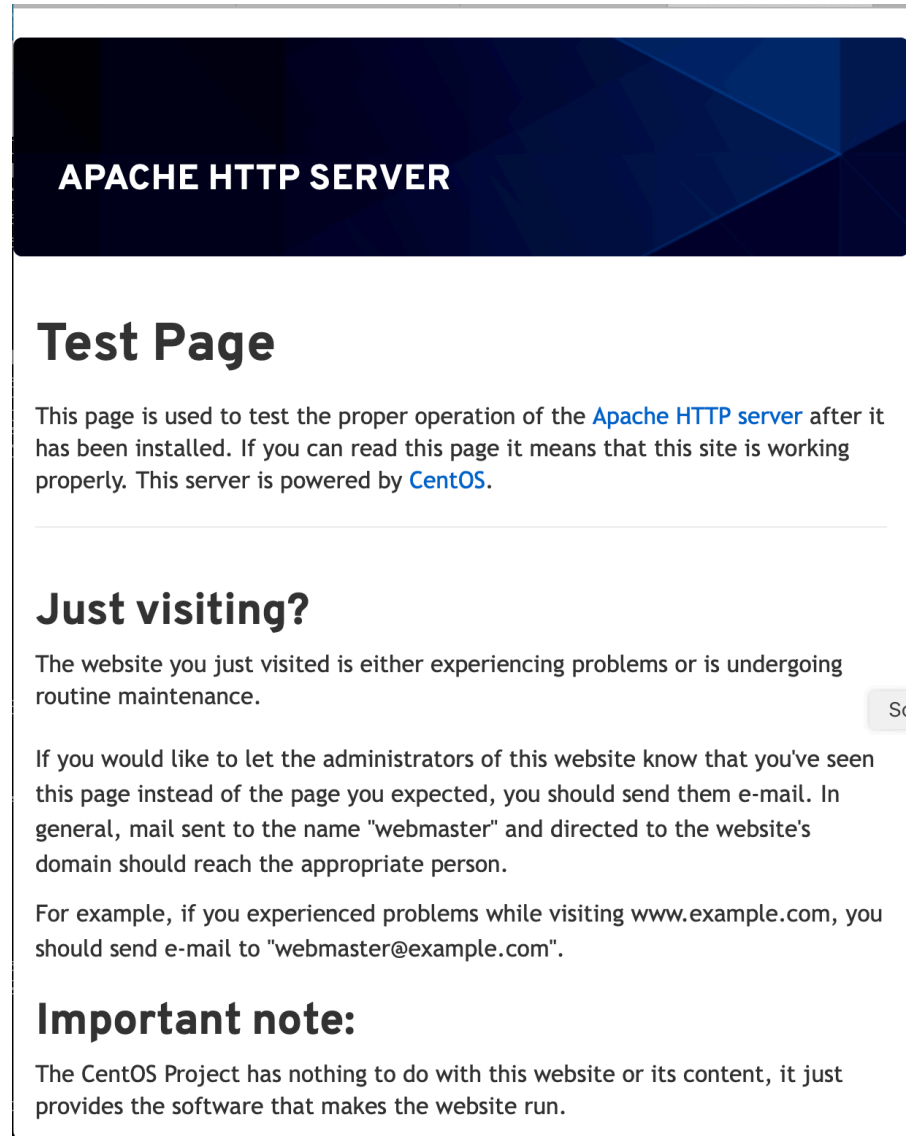
```
systemctl status httpd.service
```

- Para detener el servicio

```
systemctl stop httpd.service
```

6.L Comentarios

- El servicio se llama “httpd”
- No es un único proceso; se lanza una batería de procesos (comprobar con ps | grep httpd)
- El paquete instala un fichero httpd.conf de ejemplo con una configuración mínima. Una vez instalado, al acceder a http://localhost se muestra una página de prueba
- No es necesario que el servidor esté en modo gráfico para servir páginas web



6.L httpd.conf

- El fichero httpd.conf contiene un gran número de directivas que indican dónde se alojan en el filesystem los contenidos, los scripts, los tipos de contenido (estático, activo) que se sirven, las opciones de seguridad, los hosts virtuales (un mismo servidor puede alojar páginas con diferentes direcciones IP), los alias (diferentes directorios en la dirección de la página pueden referirse a localizaciones no relacionadas con esos nombres), el tipo de encriptación, etc.
- También se puede especificar que el servidor sea proxy (redirija las consultas a otras páginas), que haga caché de los contenidos, etc.
- Gran parte de las posibilidades del servidor están disponibles a través de módulos que se cargan dinámicamente

6.L Directivas Básicas de Configuración

- Las directivas básicas son
  - ServerAdmin (email del responsable)
  - ServerName (p.e. www.midominio.com)
  - ServerRoot (directorio donde se almacenan las páginas)
  - ServerType (standalone, en general)
  - Port (generalmente el 80)

6.L Manejo de procesos

- Apache no crea un proceso por cada consulta, para no sobrecargar el sistema. Se lanzan varios procesos independientes y se balancea la carga entre ellos. Hay un límite de transacciones simultáneas.
  - *MinSpareServers*, *MaxSpareServers*: mínimo/máximo número de procesos inactivos
  - *StartServers*: Lanzados inicialmente
  - *MaxRequestWorkers*: Máximo número de conexiones que se procesarán de forma simultánea
  - *MaxConnectionsPerChild*: máximo número de conexiones que un proceso hijo manejará durante su vida

6.L Configuración inicial

1. Backup del archivo de configuración por defecto:

```
cp /etc/httpd/conf/httpd.conf ~/httpd.conf.backup
```

2. Modificar httpd.conf para que apunte al directorio que contiene los datos del servidor web y para que tenga los parámetros deseados de número de procesos

```
DocumentRoot "/var/www/html/example.com/public_html"
...
<IfModule prefork.c>
     StartServers 5
     MinSpareServers 20
     MaxSpareServers 40
     MaxRequestWorkers 256
     MaxConnectionsPerChild 5500
</IfModule>
```

6.L Directivas frecuentes

- La directiva *ServerAdmin* indica la dirección de contacto del administrador
- La directiva *ServerName* indica el nombre del servidor y el puerto en que se establece la comunicación
- La directiva *ServerAlias* indica un nombre alternativo para el servidor (se usa para definir hosts virtuales)
- La directiva *DocumentRoot* define el directorio en que se almacena el árbol de documentos: p.e. DocumentRoot “/var/apache/htdocs”
- La directiva *ErrorLog* define la localización donde se almacenan los mensajes de error (se puede completar con la directiva *ErrorLogFormat*)
- La directiva *CustomLog* define la localización de almacenamiento de los mensajes de traza (en combinación con la directiva *LogFormat*)

6.L Directivas de traza (logging)

- Las directivas de trazado determinan que se almacena ante cada consulta y cada error.
- Se puede hacer que ante ciertos eventos se almacenen mensajes en varios archivos diferentes (p.e. %404{User-agent}i)

```
ErrorLog /var/apache/logs/error_log

LogLevel warn

LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"" combined

LogFormat "%h %l %u %t \"%r\" %>s %b" common

LogFormat "%{Referer}i -> %U" referer

LogFormat "%{User-agent}i" agent

CustomLog /var/apache/logs/access_log common
```

6.L Ejemplo de uso de directivas: Hosts virtuales

1. En el subdirectorio conf.d se crea un archivo /etc/httpd/conf.d/vhost.conf para almacenar las configuraciones de los hosts virtuales:

```
NameVirtualHost *:80

<VirtualHost *:80>
    ServerAdmin webmaster@example.com
    ServerName example.com
    ServerAlias www.example.com
    DocumentRoot /var/www/html/example.com/public_html/
    ErrorLog /var/www/html/example.com/logs/error.log
    CustomLog /var/www/html/example.com/logs/access.log combined
</VirtualHost>
```

6.L Alias

- Un alias asocia un directorio en el nombre de la página con un directorio en el sistema de archivos del servidor

```
Alias /icons/ "/var/apache/icons/"

Alias /manuals/ "/usr/apache/htdocs/manual/"

ScriptAlias /cgi-bin/ "/var/apache/cgi-bin/"
```

6.L Contenedores

- Para aplicar diferentes directivas solamente a un directorio, se crea un contenedor para esas directivas, mediante las órdenes que siguen:
  - <Directory pathname> crea un contenedor con instrucciones hasta el próximo </Directory> (directorios del filesystem)
  - <Location document> crea un contenedor con directivas aplicables a un documento (una página, que puede contener varios archivos)
  - <Files filename> un fichero determinado

6.L Contenedores (II)

- *Order* define cómo se evalúan las reglas de control de acceso
- *Deny/Allow*: hosts prohibidos (por IP). Deny all indica que todos los hosts están prohibidos salvo por las excepciones indicadas después en allow

```
<Directory "/var/apache/htdocs/internal">
    Order deny,allow
    Deny from all
    Allow from hostpermitido.com
</Directory>
```

6.L Opciones de Seguridad

- Las opciones de configuración de seguridad de cada directorio se definen mediante la orden *AccessFileName* *.htaccess*. Si se encuentra el fichero *.htaccess* en un directorio, se puede indicar en ese fichero quién puede acceder a esa página y opcionalmente incluir usuario y contraseña.
- La directiva *AllowOverride* permite que un fichero *.htaccess* altere la configuración de seguridad por defecto de ese directorio

6.L Ejemplo de directiva <Directory>

1. En el ejemplo siguiente, se habilitan los índices en los los archivos del directorio indicado y en sus subdirectorios:

```
<Directory "/usr/local/httpd/htdocs">
    Options Indexes FollowSymLinks
</Directory>
```

6.L Ejemplo de control de acceso de usuarios

```
<Directory "/var/apache/htdocs/internal/accounting">
   AuthName "Accounting"
   AuthType Basic
   AuthUserFile /etc/apache/http.passwords
   AuthGroupFile /etc/apache/http.groups
   Require hdqtrs rec bill pay
   Order deny,allow
   Deny from all
   Allow from Limit>
</Directory>
```

- Contraseñas para acceder a recursos. Con diferentes módulos, se puede combinar la autentificación con la del sistema.

6.L Proxy servers y caching

- Los proxies son servidores intermedios entre los clientes y los servidores web
- Las opciones que controlan el caching son:
  - CacheNegotiatedDocs (permite a un proxy que almacene nuestras páginas)
  - ProxyRequests (poner a on para convertir el servidor en un proxy)
  - CacheRoot, CacheSize: directorio de almacenamiento de cache
  - etc.

6.L squid

- **squid** es un proxy+cache que ofrece control de acceso, autorización y logging. También puede configurarse como un proxy inverso, para redireccionar las conexiones al puerto 80. Cuando actúa como un proxy inverso, el contenido cacheado se sirve desde el servidor proxy al cliente sin exponer el origen de los datos en la red interna.
- Instalación: **sudo dnf install squid**
- Ejecución: **sudo systemctl enable –now squid**

6.L squid

```
#
# Recommended minimum configuration:
#

# Example rule allowing access from your local networks.
# Adapt to list your (internal) IP networks from where browsing
# should be allowed
acl localnet src 0.0.0.1-0.255.255.255  # RFC 1122 "this" network (LAN)
acl localnet src 10.0.0.0/8             # RFC 1918 local private network (LAN)
acl localnet src 100.64.0.0/10          # RFC 6598 shared address space (CGN)
acl localnet src 169.254.0.0/16         # RFC 3927 link-local (directly plugged) machines
acl localnet src 172.16.0.0/12          # RFC 1918 local private network (LAN)
acl localnet src 192.168.0.0/16         # RFC 1918 local private network (LAN)
acl localnet src fc00::/7               # RFC 4193 local private network range
acl localnet src fe80::/10              # RFC 4291 link-local (directly plugged) machines

acl SSL_ports port 443
acl Safe_ports port 80          # http
acl Safe_ports port 21          # ftp
acl Safe_ports port 443         # https
acl Safe_ports port 70          # gopher
acl Safe_ports port 210         # wais
acl Safe_ports port 1025-65535  # unregistered ports
acl Safe_ports port 280         # http-mgmt
acl Safe_ports port 488         # gss-http
acl Safe_ports port 591         # filemaker
acl Safe_ports port 777         # multiling http
acl CONNECT method CONNECT

#
# Recommended minimum Access Permission configuration:
#
# Deny requests to certain unsafe ports
http_access deny !Safe_ports

# Deny CONNECT to other than secure SSL ports
http_access deny CONNECT !SSL_ports

# Only allow cachemgr access from localhost
http_access allow localhost manager
http_access deny manager

# We strongly recommend the following be uncommented to protect innocent
# web applications running on the proxy server who think the only
# one who can access services on "localhost" is a local user
#http_access deny to_localhost

"/etc/squid/squid.conf" 76L, 2553C
```

El archivo de configuración es **/etc/squid/squid.conf**

Cada lista de control de acceso (ACL) consiste en un nombre, un tipo y un valor. Por ejemplo, para configurar hosts en el segmento 192.168.10.0/24 se haría:

acl miredlocal src 192.168.10.0/24

Esto crea una ACL llamada miredlocal que especifica los hosts de dicha red

6.L squid

- Una vez se ha definido una ACL, se puede referenciar para permitir o denegar el acceso a una función del cache. Por ejemplo:

  http_access allow miredlocal

- El fichero de configuración se lee de arriba a abajo y el orden de las directivas es relevante
- Para bloquear el acceso a sitios específicos puede crearse un archivo que define los dominios bloqueados, y añadir una ACL indicándolo:

  acl sitiosbloqueados dstdomain "/etc/squid/sitios-bloqueados.squid"

  http_access deny sitiosbloqueados

  http_access allow miredlocal

6.L squid

- También puede denegarse el acceso mediante keywords. Se crea un fichero con palabras prohibidas:

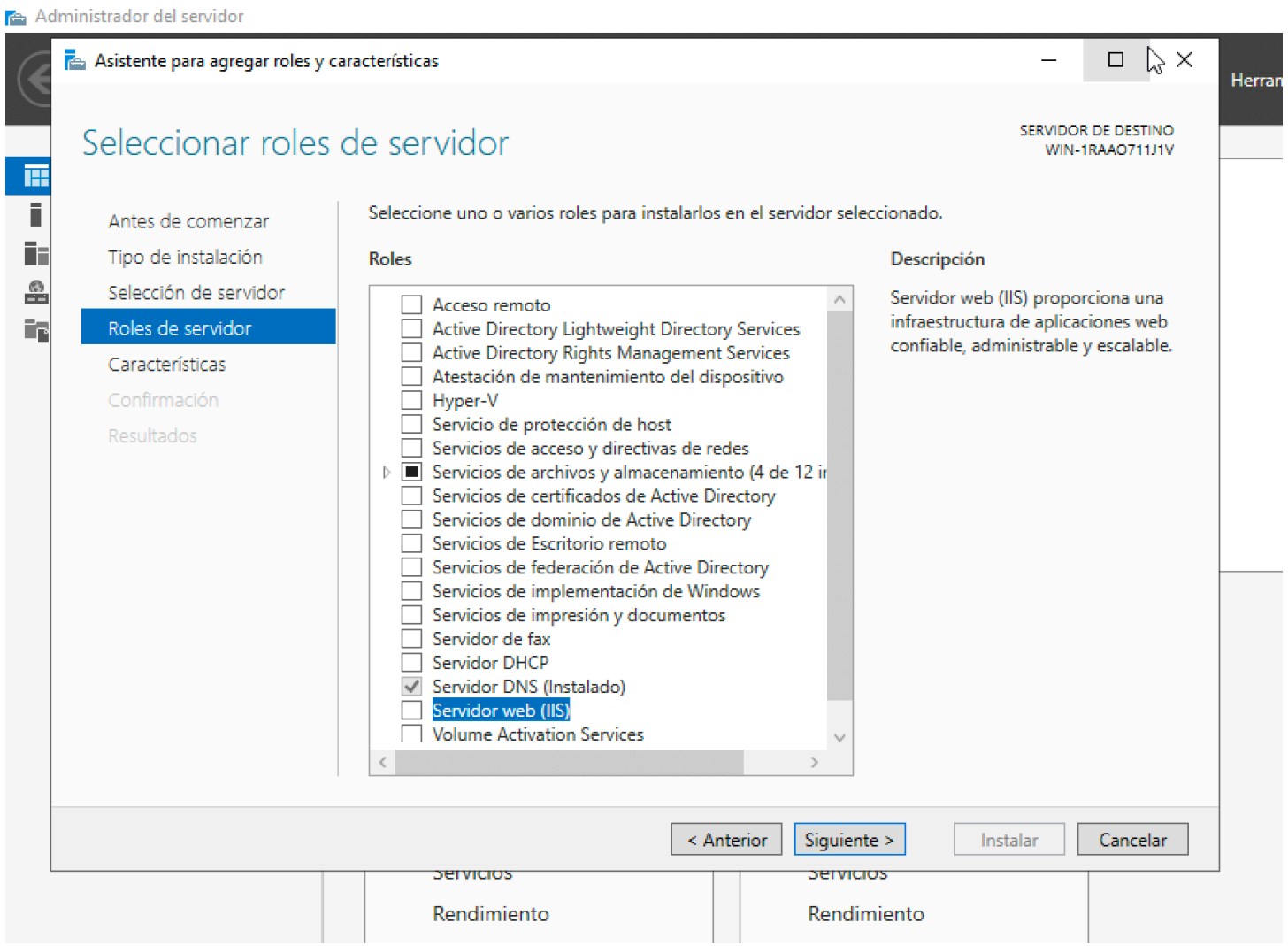
  vi /etc/squid/palabras-prohibidas.squid
  juego
  poker
  apuestas

- y se añade al archivo de configuración:

  acl sitiosbloqueados dstdomain "/etc/squid/sitios-bloqueados.squid"
  http_access deny sitiosbloqueados
  http_access deny palabras-prohibidas
  http_access allow miredlocal

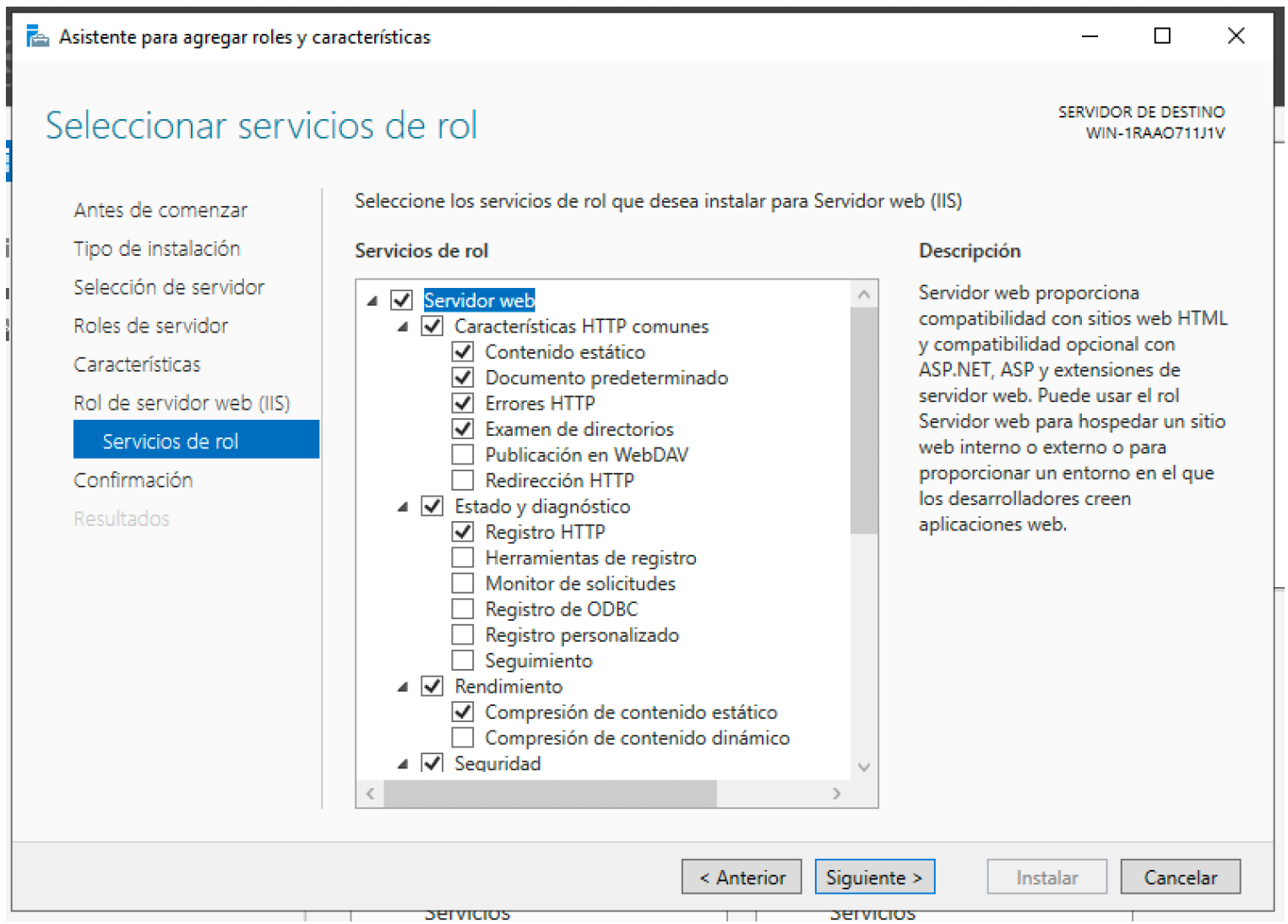
6.W: Internet Information Server

- Se selecciona el rol "Servidor web"



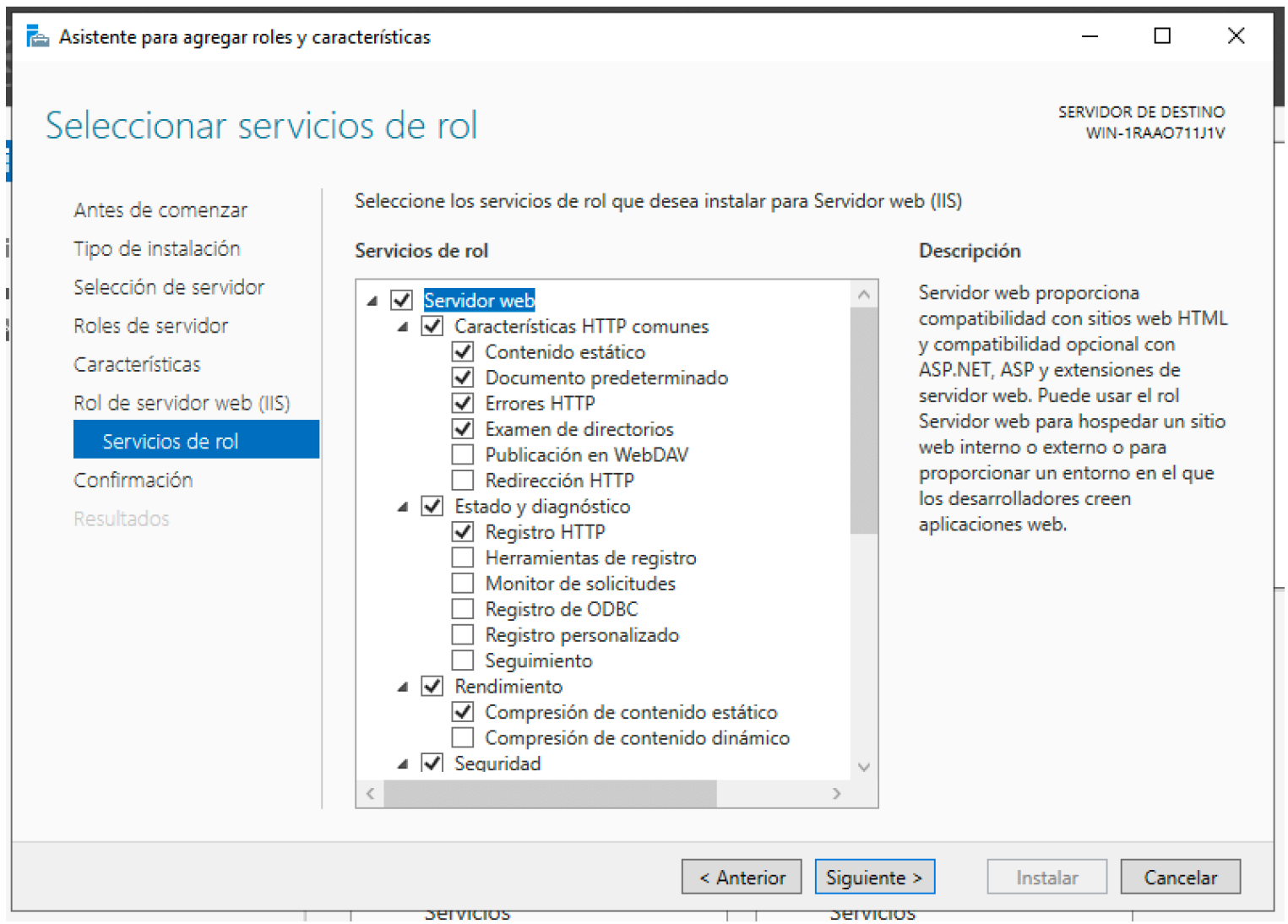
6.W: Internet Information Server

- Se seleccionan los servicios de rol deseados



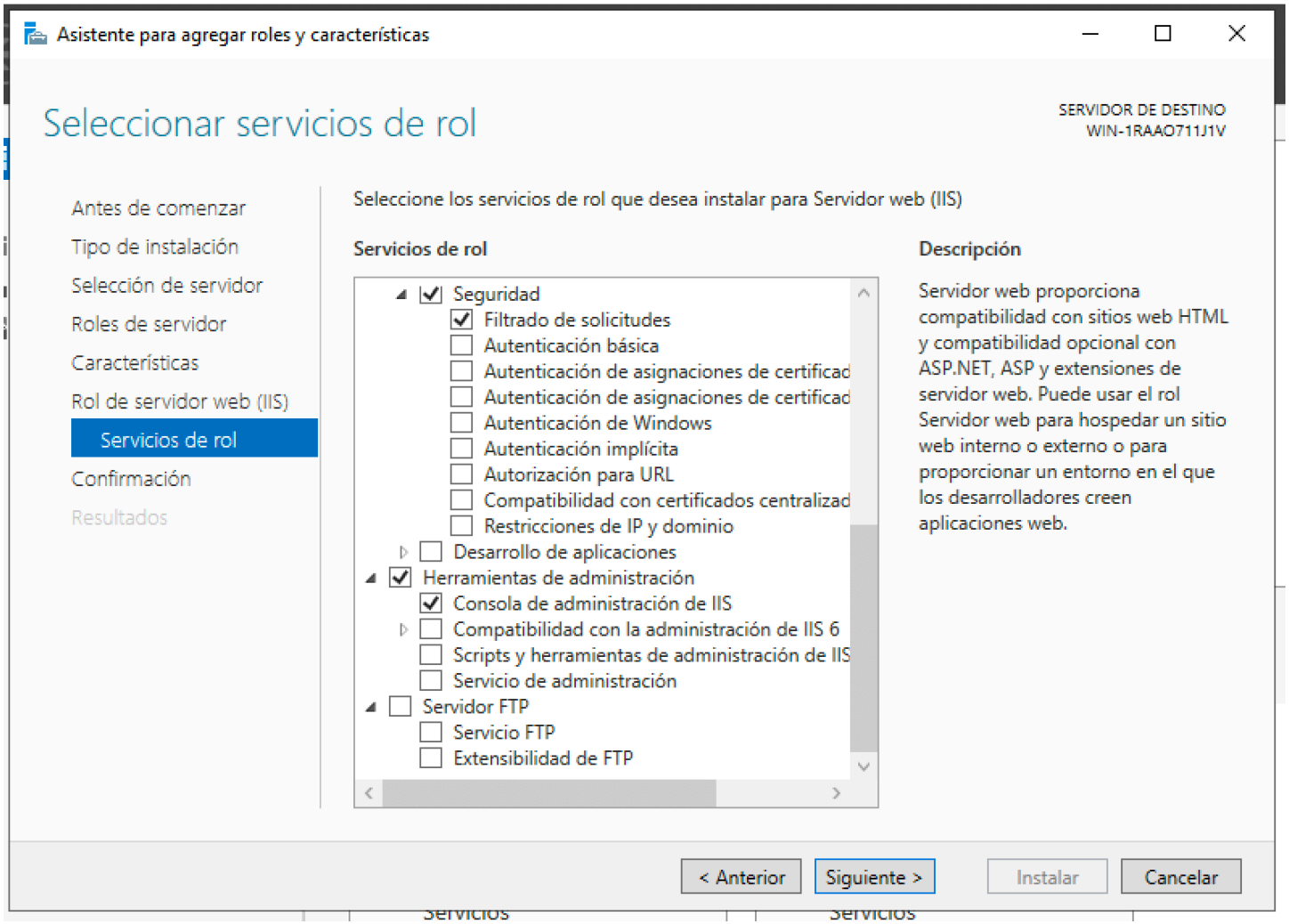
6.W: Internet Information Server

- Se seleccionan los servicios de rol deseados



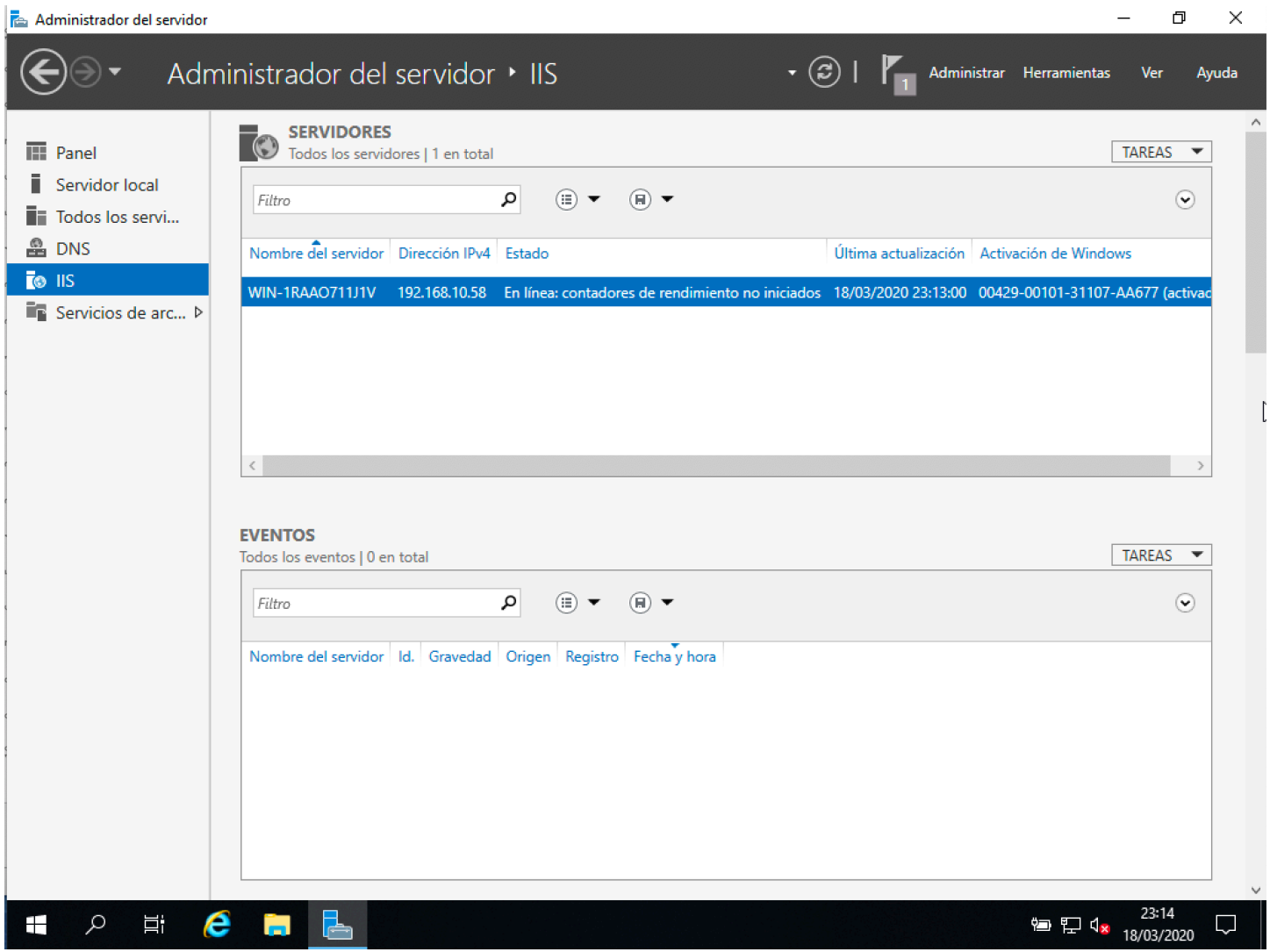
6.W: Internet Information Server

- Se incluye la consola de administración y opcionalmente el servidor FTP

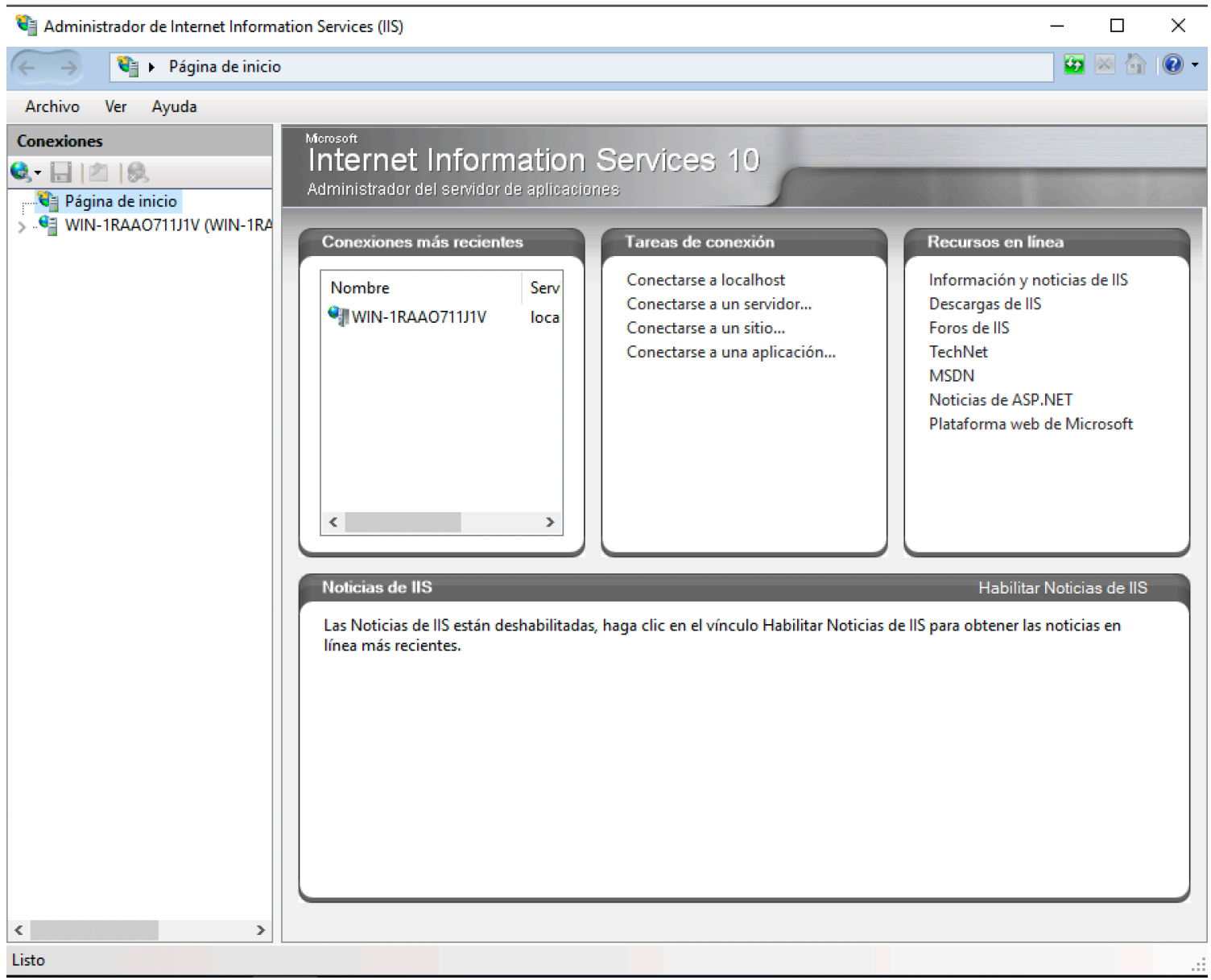


6.W: Internet Information Server

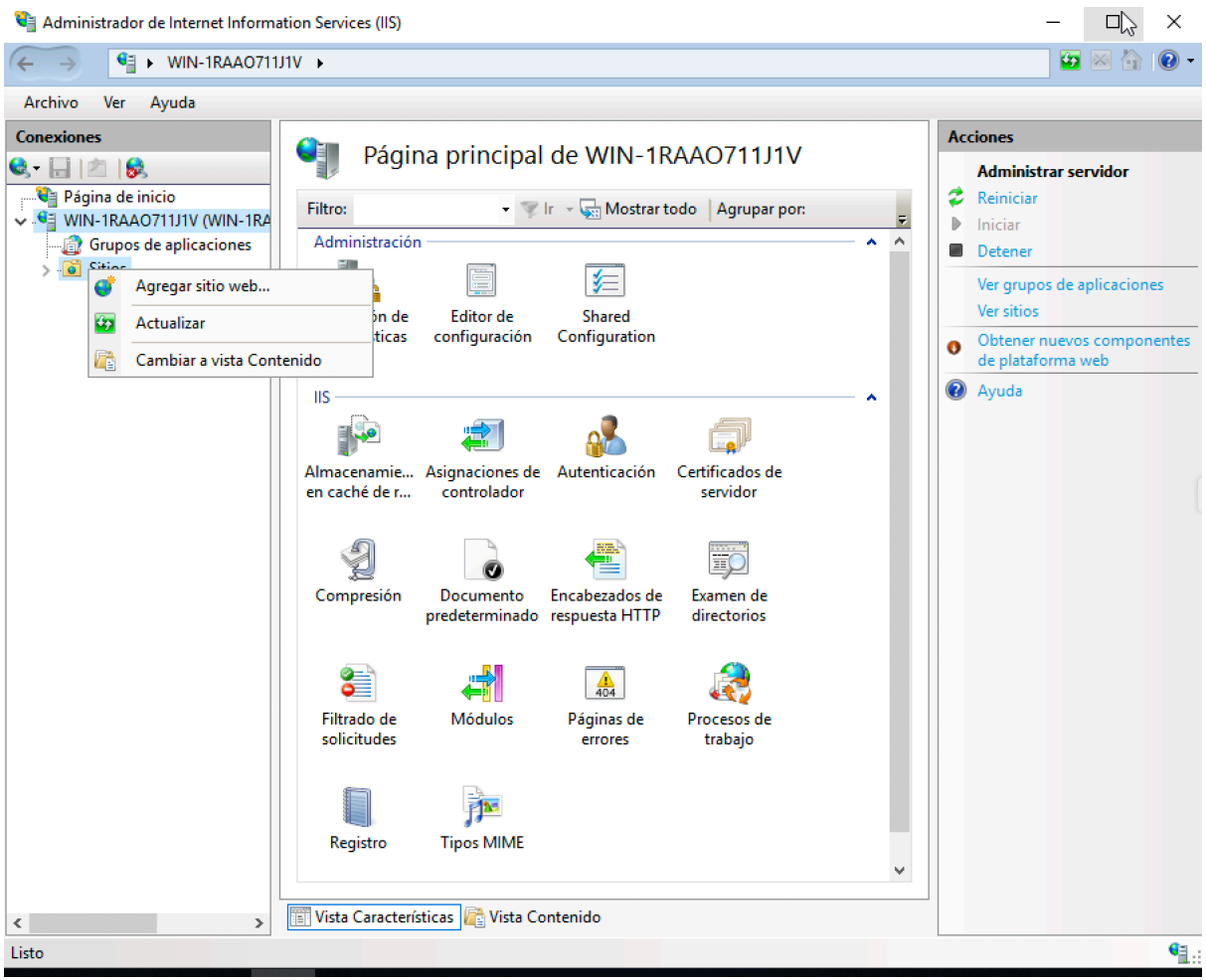
- IIS desde administración del servidor



6.W. Administrador de IIS

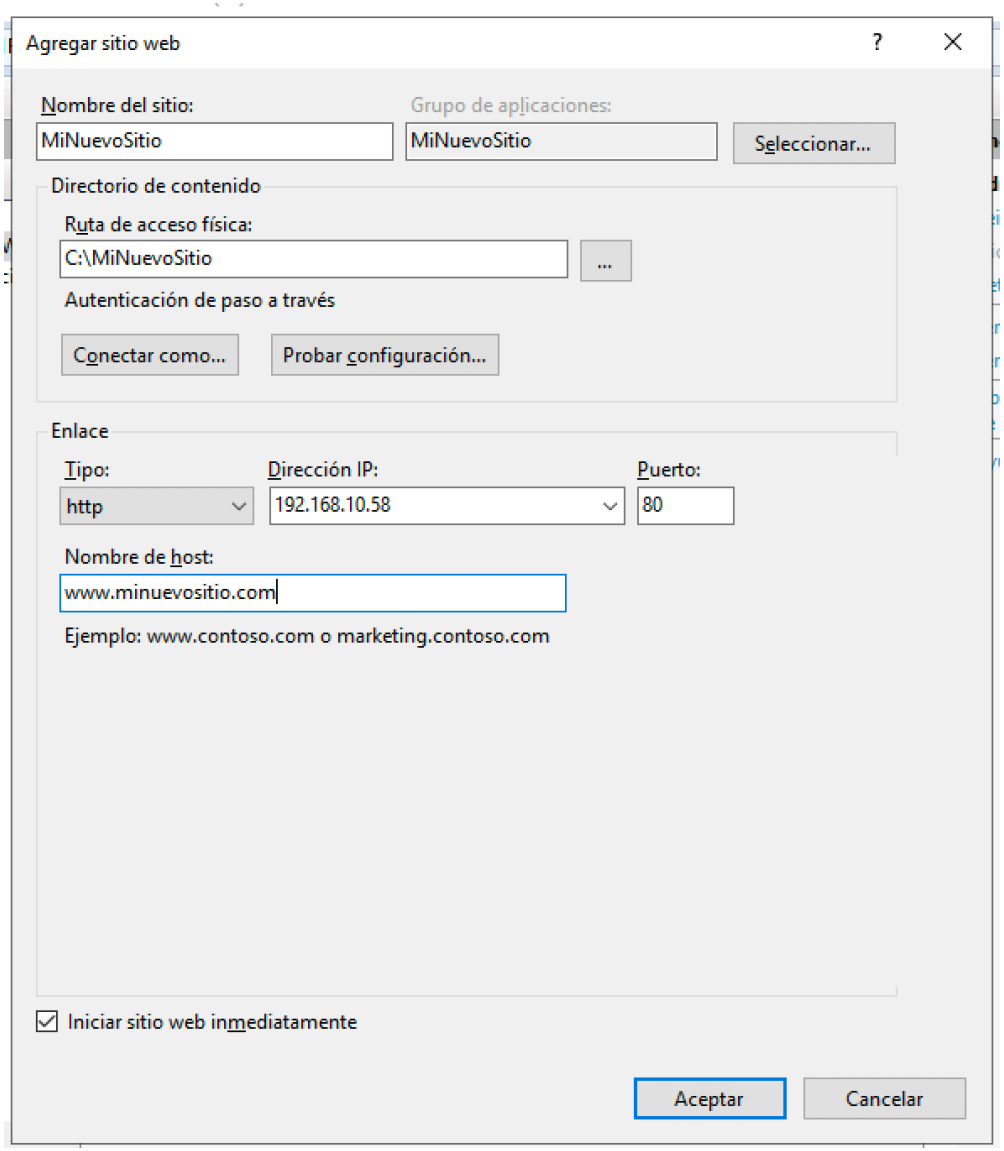


6.W Agregar nuevo sitio



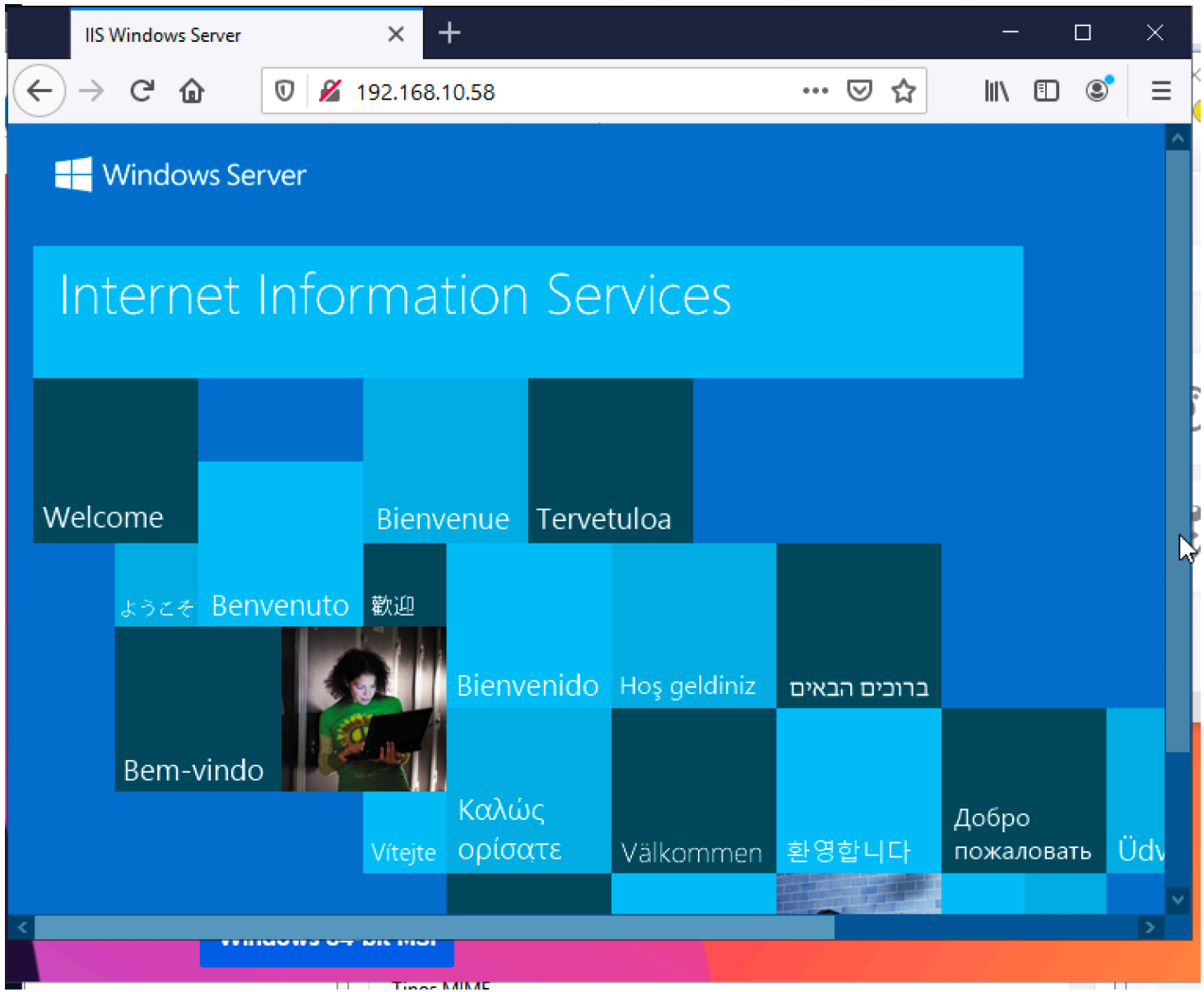
- Botón secundario del ratón en el nodo “Sitios”
- Se indica el directorio donde se almacenan los archivos
- Se indica la dirección IP y el nombre del host

6.W Agregar nuevo sitio

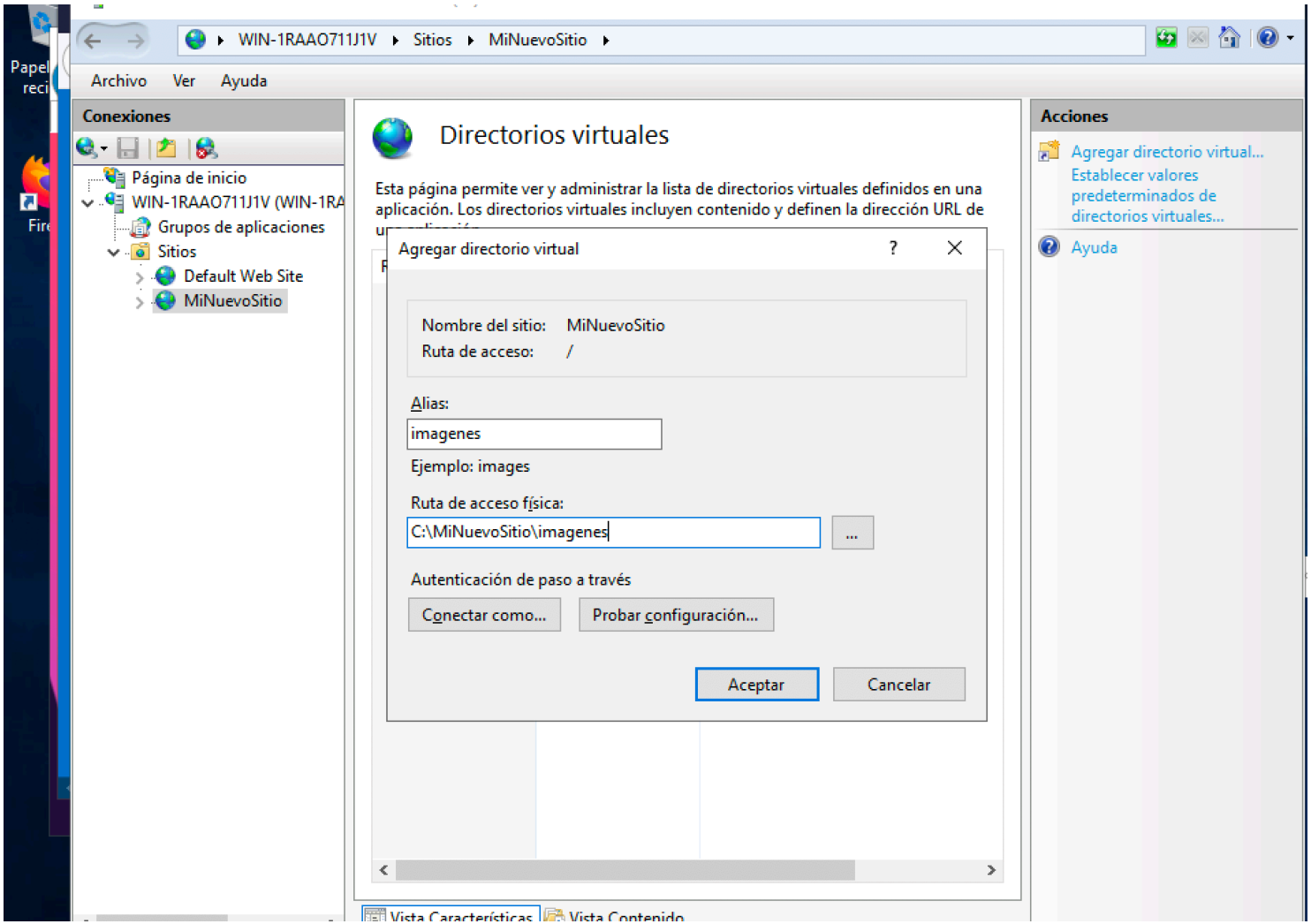


- Botón secundario del ratón en el nodo “Sitios”
- Se indica el directorio donde se almacenan los archivos
- Se indica la dirección IP y el nombre del host

6.W Agregar nuevo sitio



Directorio Virtual



- Los alias (un nombre alternativo para un directorio no contenido en el directorio principal) se crean también desde el nodo sitios (menú contextual, añadir directorio virtual)