# TALLER SR – PRÁCTICA 9 – Servizo DHCP – MS Windows – Logs

| NÚMERO DE GRUPO | FUNCIÓNS | Apelidos, Nome |
|---|---|---|
| | Coordinador/a: | |
| | Responsable Limpeza: | |
| | Responsable Documentación: | |

**ESCENARIO: Servizo DHCP (Microsoft Windows)**

**Portátil:**
Rede Local
MAC filtrada (sen/con acceso)
Cliente DHCP

**USB**
Live Kali amd64

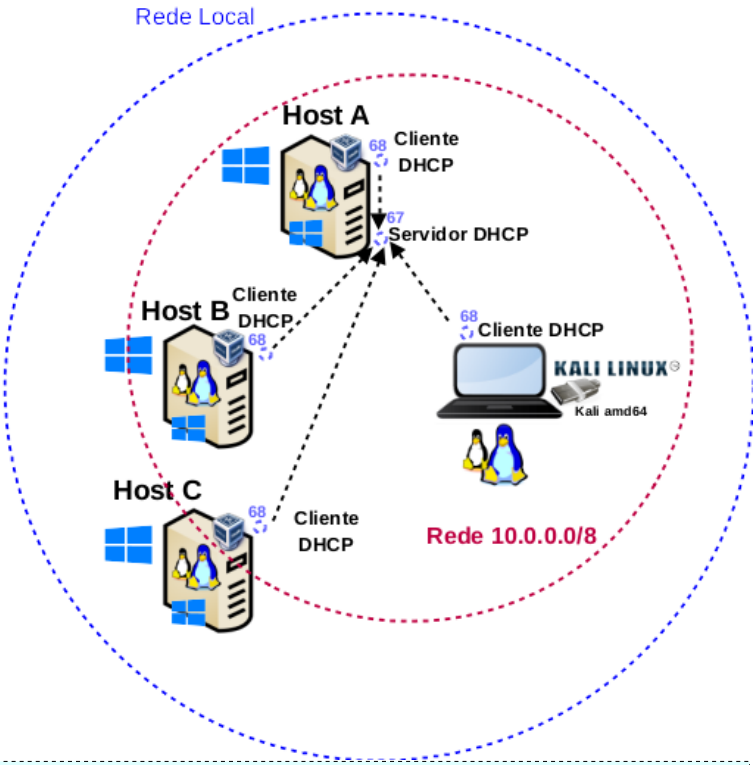
**Hosts A, B, C:**
⊂ Rede Local
⊃ Máquina virtual

**Máquinas virtuais:**
⊂ Host
RAM ≤ 2048MB CPU ≤ 2 PAE/NX habilitado
Rede: 10.10.10.0/8
Rede: Bridge

**Máquinas virtuais GNU/Linux:**
ISO: Kali Live amd64
Cliente DHCP
BIOS: Permite arranque dispositivo extraíble: CD/DVD, USB

**Máquinas virtuais Microsoft Windows:**
Disco duro: Windows amd64
Cliente DHCP

**Máquina virtual Microsoft Windows Server:**
IP/MS: 10.10.10.10/8




**LIMITACIÓN DE RESPONSABILIDADE** O autor do presente documento declina calquera responsabilidade asociada ao uso incorrecto e/ou malicioso que puidese realizarse coa información exposta no mesmo. Por tanto, non se fai responsable en ningún caso, nin pode ser considerado legalmente responsable en ningún caso, das consecuencias que poidan derivarse da información contida nel ou que esté enlazada dende ou hacia el, incluíndo os posibles erros e información incorrecta existentes, información difamatoria, así como das consecuencias que se poidan derivar sobre a súa aplicación en sistemas de información reais e/ou virtuais. Este documento foi xerado para uso didáctico e debe ser empregado en contornas privadas e virtuais controladas co permiso correspondente do administrador desas contornas.

| Material necesario | Práctica: Servizo DHCP – MS Windows – Logs |
|---|---|
| ■ Portátil<br>■ Regleta<br>■ Switch 5-Port Gigabit<br>■ Máquina virtual Windows Server 2019<br>■ Hosts alumnado<br>■ Cableado de rede,<br>■ [1] Protocolo DHCP<br>■ [2] DHCP Windows Server<br>■ [3] Administrador de servidores<br>■ [4] Práctica 1<br>■ [5] Práctica 6<br>■ [6] Rexistros de eventos<br>■ [7] Análisis archivos rexistro DHCP-Server<br>■ [8] APIPA | (1) Prerrequisito: Práctica 1 [4] e Práctica6 [5]<br>(2) Conectar portátil e hosts do alumnado ao switch.<br>(3) HostA alumnado:<br>a) Arrancar máquina virtual Windows Server 2019<br>b) Configurar a rede según o escenario.<br>c) Instalar e configurar o servidor DHCP<br>(4) Portátil:<br>a) Arrancar co USB Live Kali amd64<br>b) Cliente DHCP<br>(5) Hosts alumnado:<br>a) Crear e arrancar máquinas virtuais coa rede en modo “bridge” e especificacións según escenario.<br>b) Cliente DHCP: Recibir a configuración de rede concedida polo servidor DHCP<br>(6) Servidor DHCP: Verificar rexistros [6] [7] |

**Procedemento:**

(1) Conectar no mesmo segmento de rede o portátil e os hosts do alumnado.

a) Conectar a regleta á corrente eléctrica na vosa zona de traballo.

b) Conectar o switch á regleta.

c) Conectar o portátil ao switch.

d) Conectar co cableado de rede creado na Práctica 1 os vosos equipos de alumnado ao switch.

e) Non conectar o switch á roseta da aula.

(2) HostA alumnado: Arrancar a máquina virtual Microsoft Windows Server 2019 [5]

a) Configurar a rede según o escenario. Abrir unha consola e executar:

```
> systeminfo #Amosar información de configuración detallada sobre o equipo e o seu sistema operativo
> ipconfig /all #Amosar a configuración TCP/IP completa de todas as interfaces de rede.
```

b) Realizar a instalación e configuración do servidor DHCP en Microsoft Windows [1][2][3] según [5], é dicir, realizar o procedemento comentado no apartado (2.c) da Práctica 6.

c) Avisar ao docente para a revisión ☐1

(3) Portátil:

a) Arrancar co USB Live Kali amd64.

b) Configurar a rede para a NIC eth0. Executar nunha consola:

```
$ setxkbmap es #Configurar teclado en español
$ sudo su - #Acceder á consola de root(administrador) a través dos permisos configurados co comando sudo (/etc/sudoers, visudo)
# /etc/init.d/avahi-daemon stop #Parar o demo avahi-daemon(control resolución de nomes) para poder configurar de forma manual a configuración de rede e non ter conflicto con este demo.
# /etc/init.d/network-manager stop || pkill NetworkManager #Parar o demo network-manager(xestor de rede) ou o script NetworkManager (executado sen ser demo) para poder configurar doutro xeito (co comando ip(ifconfig) de forma manual ou mediante networking (ficheiros /etc/init.d/networking, /etc/init.d/networking.d) a configuración de rede e non ter conflicto con este xestor.
# ip addr show eth0 #Amosar información sobre a NIC eth0.
# dhclient -v eth0 #Solicitar configuración de rede para a NIC eth0. Como agora temos a MAC Address con permisos podemos obter a configuración de rede para o portátil.
# ip addr show eth0 #Amosar información sobre a NIC eth0.
# ip route #Amosar a táboa de enrutamento.
# cat /etc/resolv.conf #Ver o contido do ficheiro /etc/resolv.conf, o cal contén a configuración os servidores DNS a empregar para a resolución de nomes.
```

c) Avisar ao docente para revisión. ☐2

(4) Servidor DHCP: Visualizar os rexistros do servizo DHCP.

a) Visor de sucesos [6]

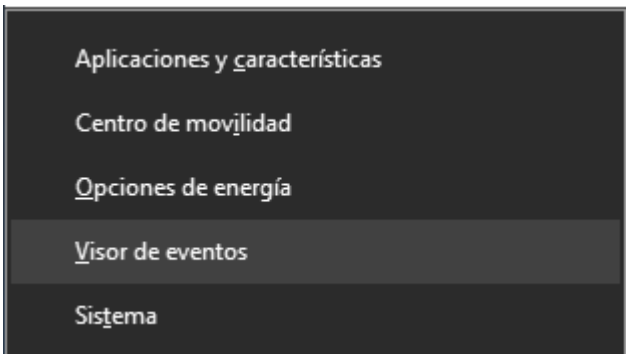



*Figura 1: Windows + x (Atallo de Teclado).*

*Abrir Visor de eventos*

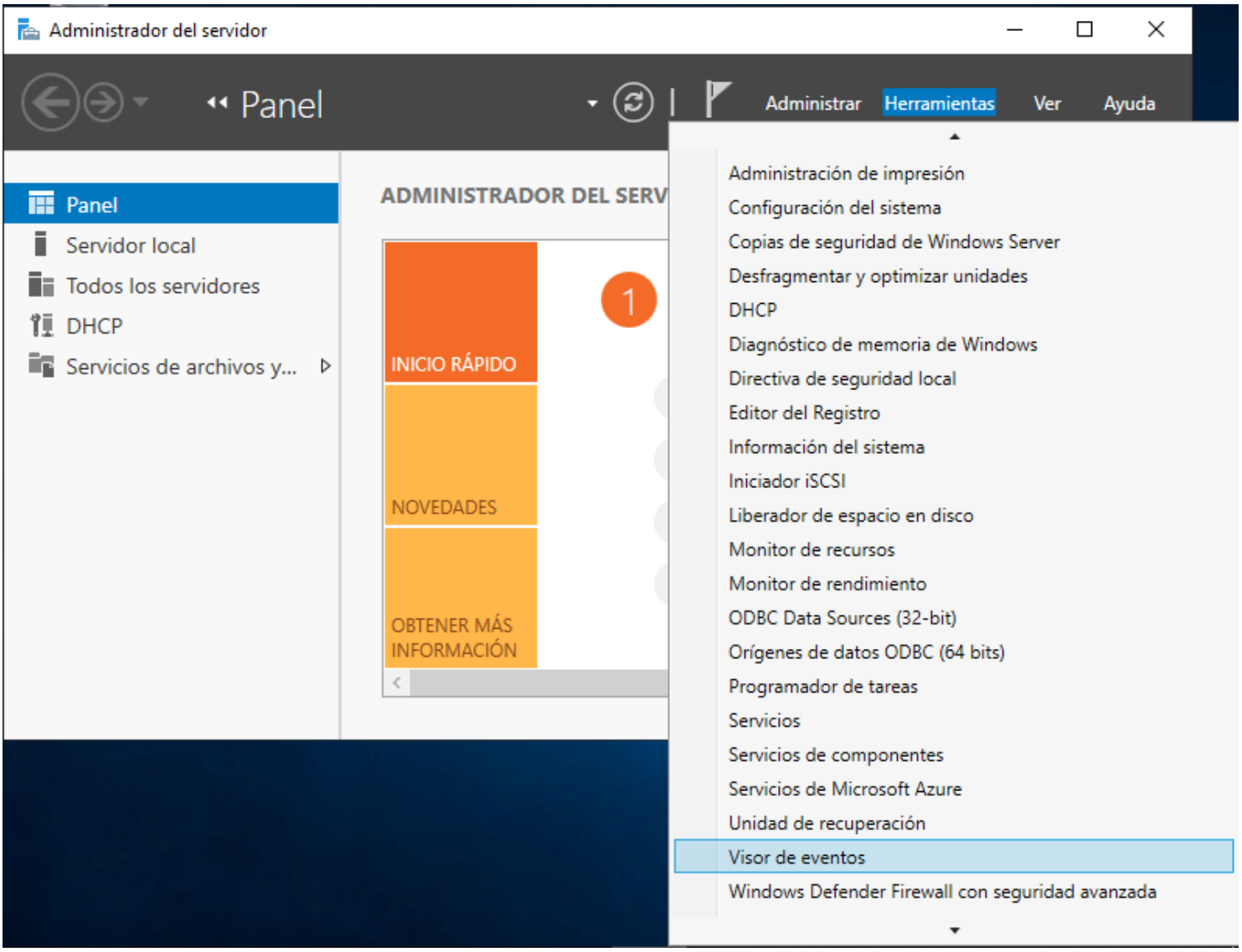



*Figura 2: Administrador de servidor - Herramientas - Abrir Visor de eventos*

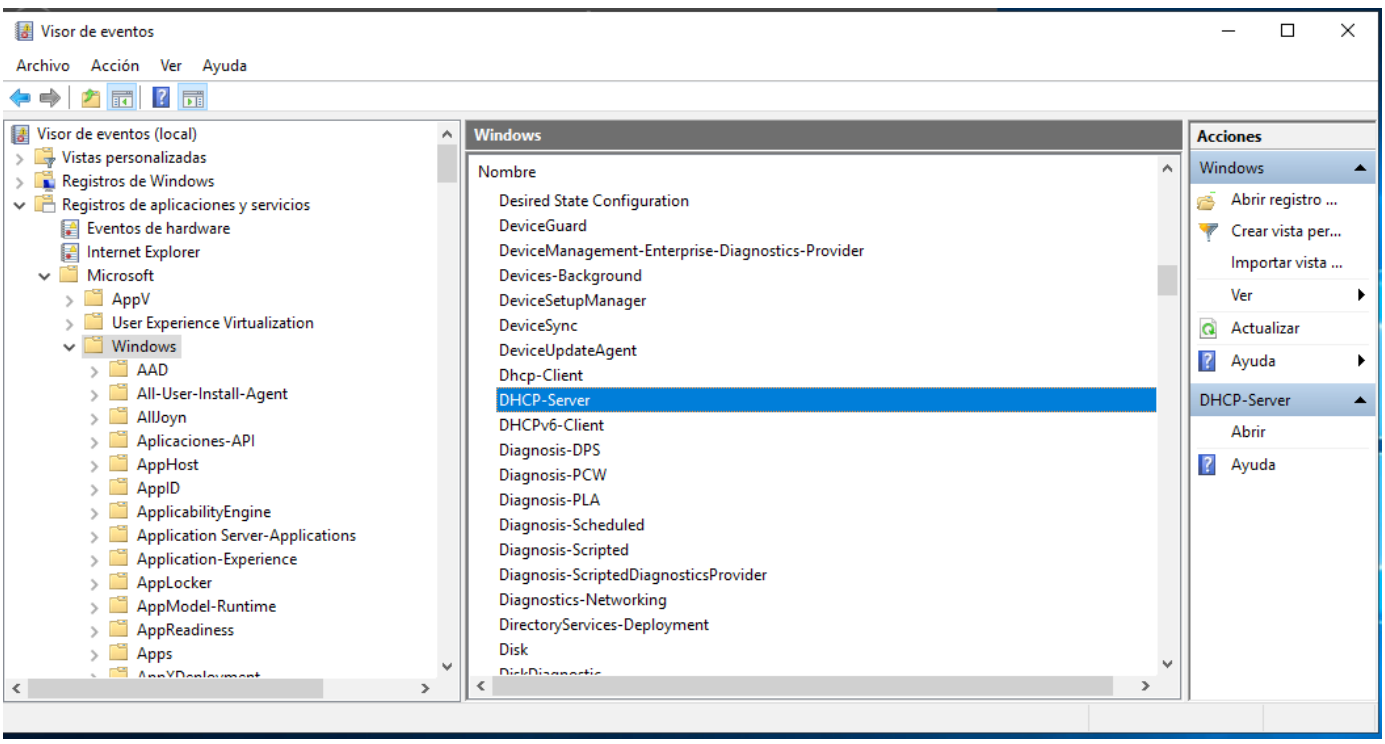



*Figura 3: Registros de aplicaciones y servicios - Microsoft - Windows - DHCP Server*

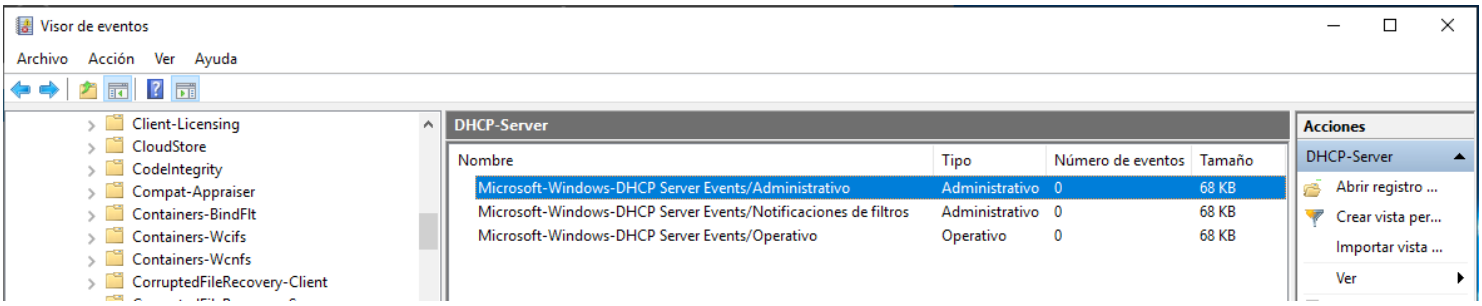



*Figura 4: Registros de aplicaciones y servicios - Microsoft - Windows - DHCP Server - Abrir*

Como podemos observar na *Figura 4* de momento non temos rexistros sobre o servidor DHCP. No voso caso, ao seguir os pasos anteriores indicar que acontece e o por que.

b) Administrador DHCP: Concesiones de direcciones

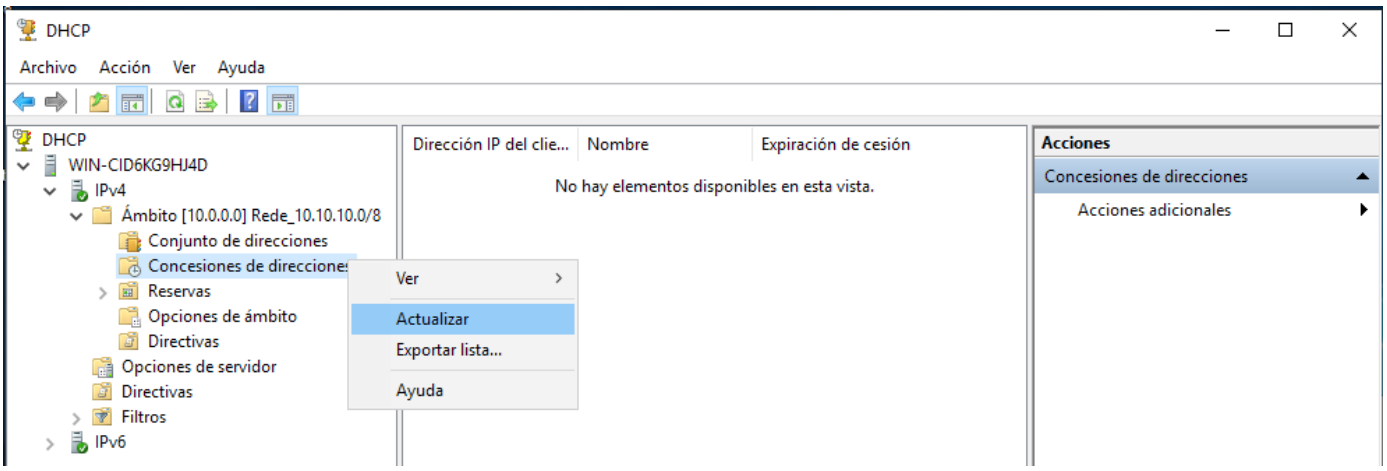



*Figura 5: Administrador DHCP - Concesiones de direcciones - Actualizar*

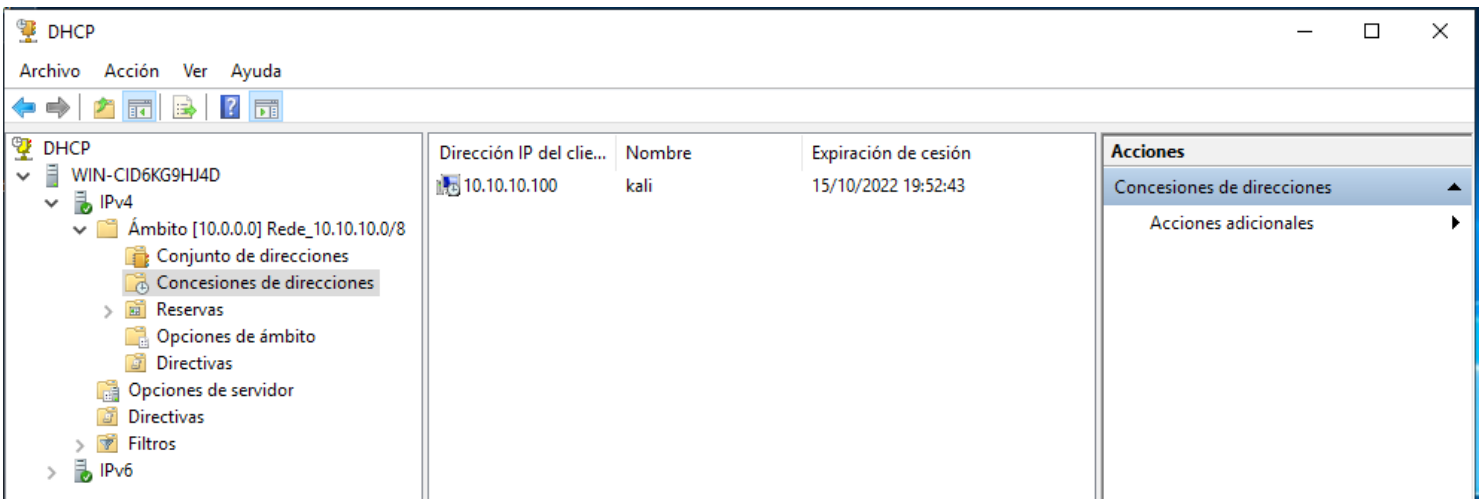



*Figura 6: kali - 10.10.10.100*

Ao actualizar no voso servidor DHCP deberíades obter unha situación similar á da *Figura 6*. No voso caso, ao seguir os pasos anteriores indicade que acontece e o por que.

c) Rexistros depuración servidor DHCP `C:\Windows\System32\dhcp\*.log` [6]

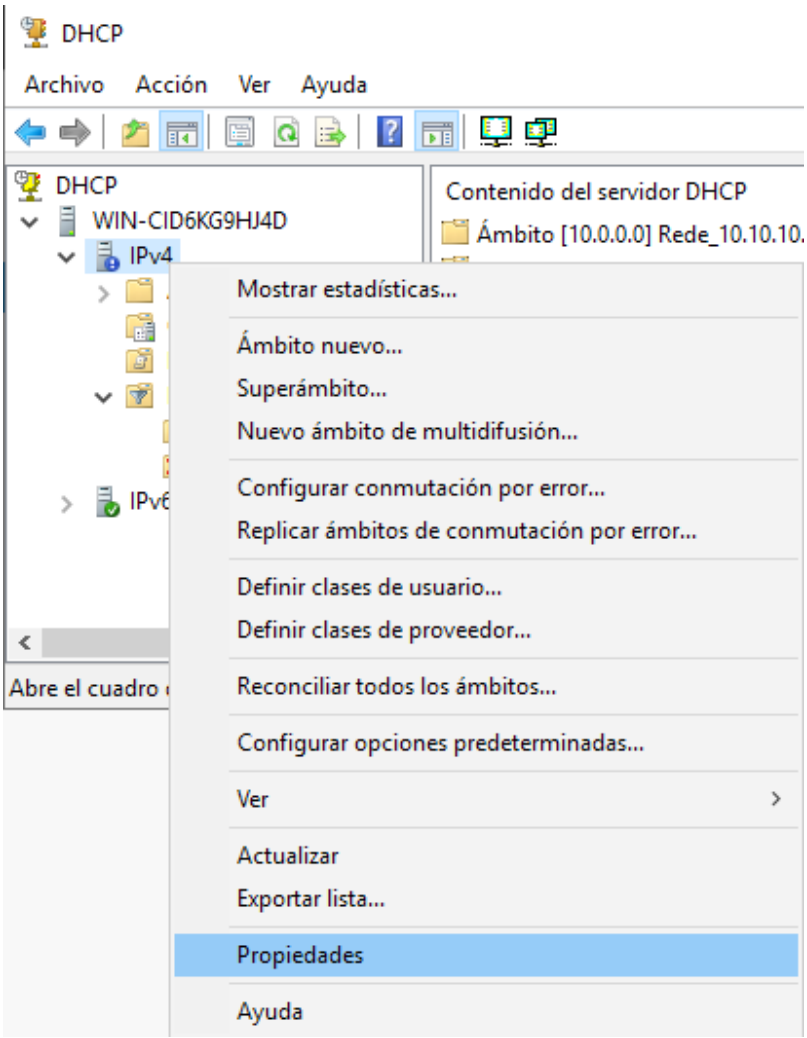



*Figura 7: Administrador DHCP - IPv4 - Propiedades*

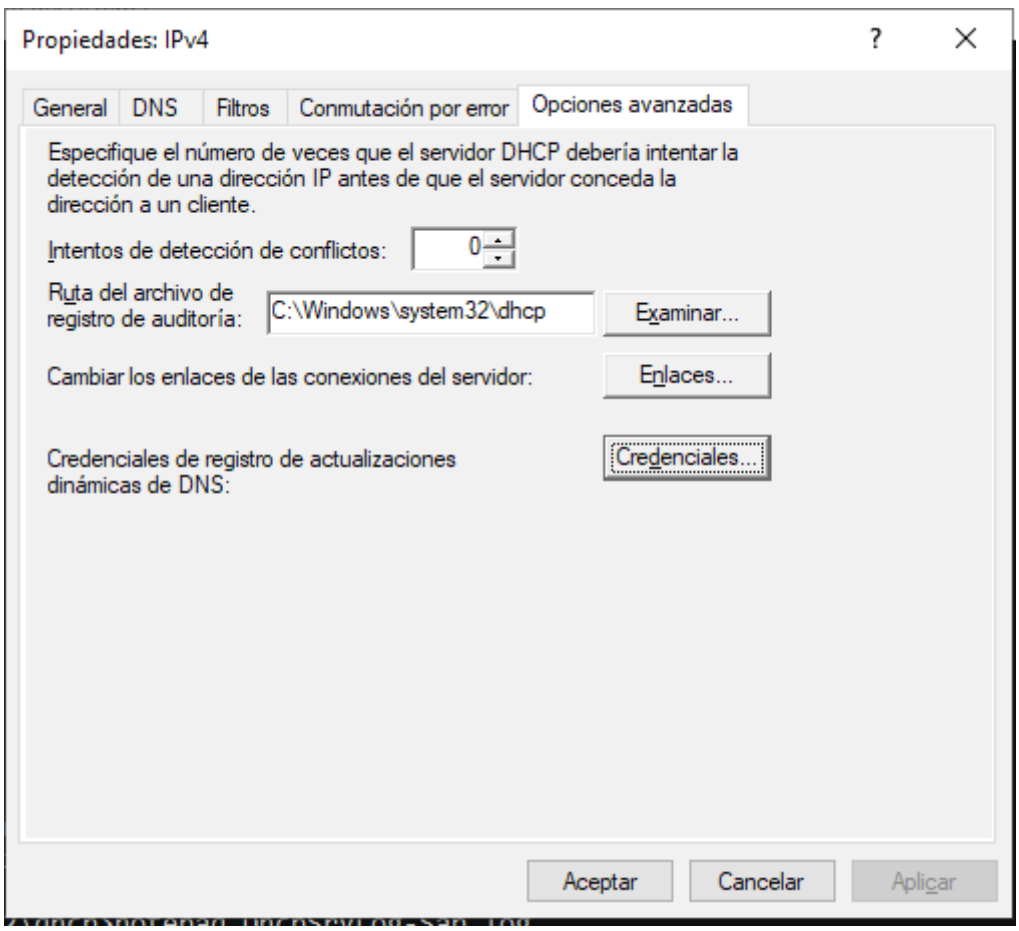



*Figura 8: Ruta archivo de registro de auditoría: C:\Windows\System32\dhcp*

Abrir unha consola powershell e executar:

```
> cd c:\windows\system32\dhcp #Acceder ao directoro c:\windows\system32\dhcp.
> dir #Ver o contido do directorio.
> $dia=get-date -Format "dddd" #Crear a variable dia a cal contén o valor do nome do día da semana na que estás a executar o comando.
> $diaAbrev=$dia.Substring(0,3) #Crear a variable diaAbrev a ca contén como valor os 3 primeiros caracteres do valor da variable dia.
> more DhcpSrvLog-$diaAbrev*.log #Ver de forma paxinada por pantalla o contido do ficheiro do rexistro de auditorái do día de hoxe (do día que estás a executar este comando).
```

Consultar [7] e indicar a saída que proporciona este log?

(5) Avisar ao docente para revisión. ☐ 3

(6) Actualizar o visor de eventos.

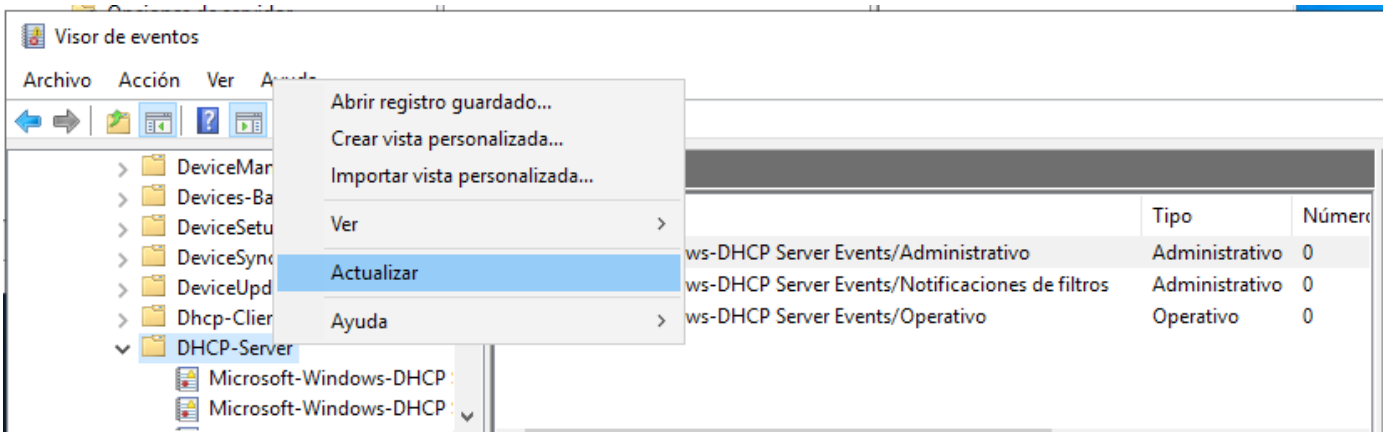



*Figura 9: Visor de eventos - Actualizar*

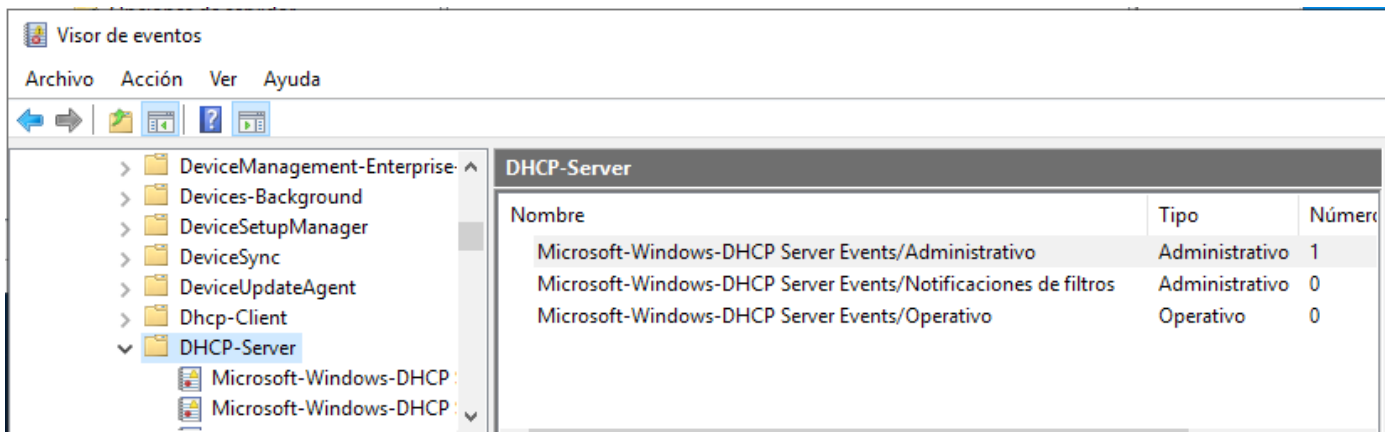



*Figura 10: Visor de eventos - DHCP Server - Administrativo*

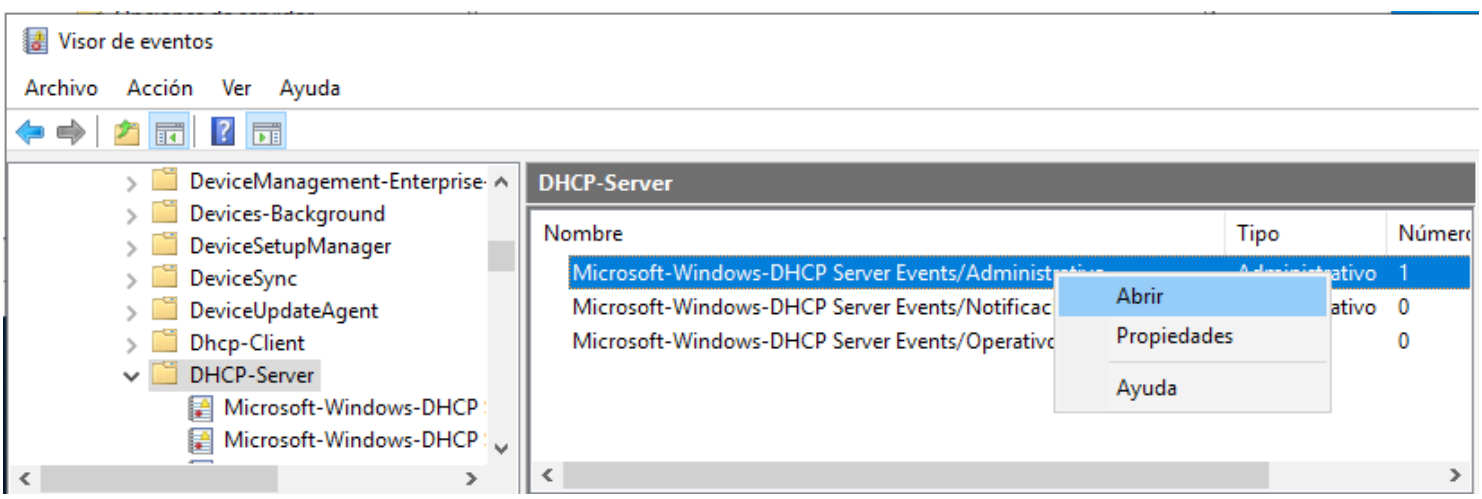



*Figura 11: Visor de eventos - DHCP Server - Administrativo - Abrir*

Que acontece? Podedes ver rexistros novos? En tal caso: cales e que indican?

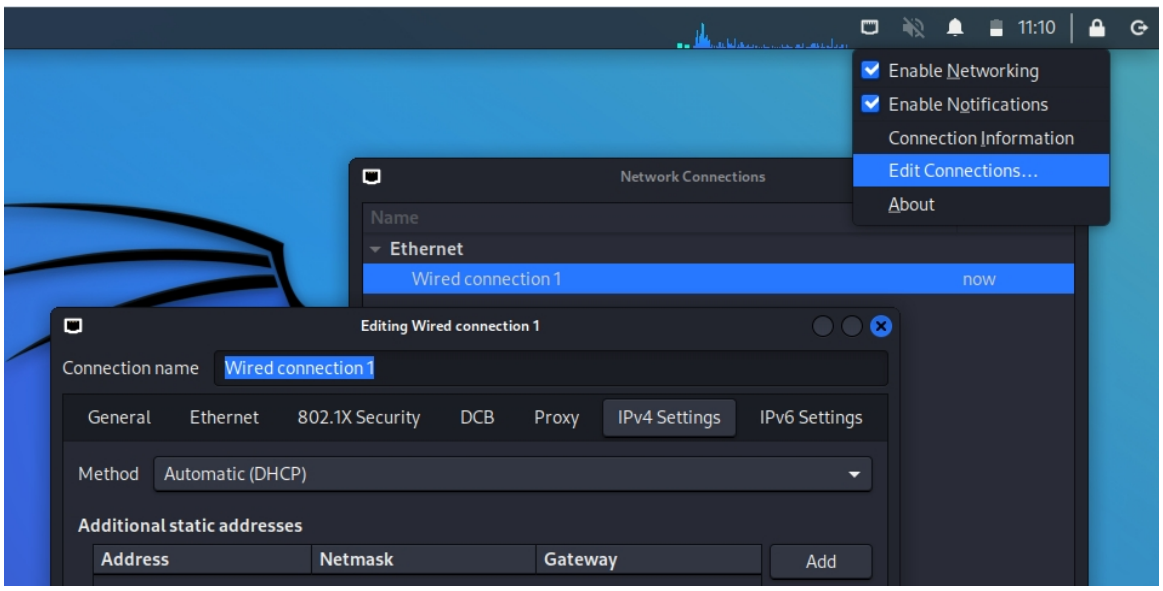
Avisar ao docente para revisión. ☐4

(7) Hosts alumnado:

a) Crear e arrancar unha máquina virtual en cada equipo do alumnado coas seguintes características (ver escenario):

i. RAM ≥ 2048MB
ii. CPU ≥ 2
iii. PAE/NX habilitado
iv. Rede: Soamente unha tarxeta activada en modo bridge (ponte)
v. ISO: Kali Live amd64
vi. Nome: Practica9-Cliente-DHCP

b) O xestor de redes NetworkManager está habilitado. Por defecto, está xerada unha conexión da interface eth0 solicitando a configuración de rede mediante DHCP. Comprobar se isto é correcto, deberiades ver unha imaxe similar á seguinte:




c) Executar nunha consola,

```
$ setxkbmap es #Configurar teclado en español
$ ip addr show eth0 #Amosar información sobre a NIC eth0.
$ ip route #Amosar a táboa de enrutamento.
$ cat /etc/resolv.conf #Ver o contido do ficheiro /etc/resolv.conf, o cal contén a configuración os servidores DNS a empregar para a resolución de nomes.
```

d) Realizar de novo os apartados (4.b), (4,c) e (6) Que acontece? Por que?

e) Avisar ao docente para revisión. ☐5

(8) Hosts alumnado:

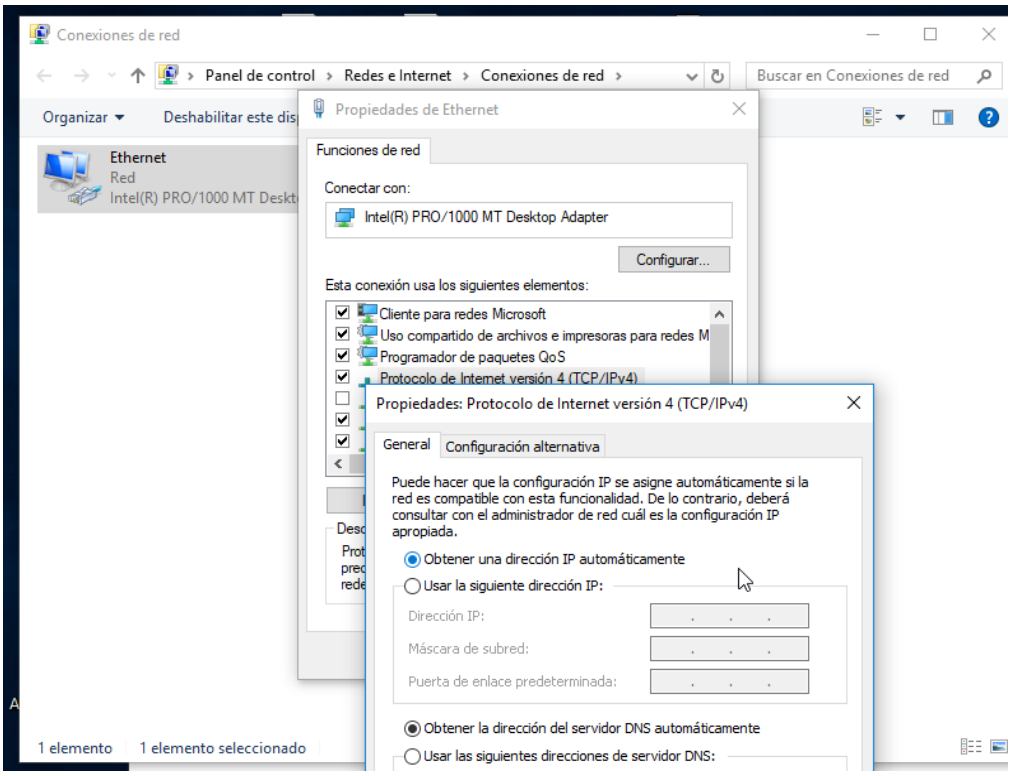
a) Crear unha máquina virtual en cada equipo do alumnado coas seguintes características (ver escenario):

i. RAM ≥ 2048MB
ii. CPU ≥ 2
iii. PAE/NX habilitado
iv. Rede: Soamente unha tarxeta activada en modo bridge (ponte)
v. Sistema operativo instalado: Windows amd64
vi. Nome: Practica9-Cliente-Windows-DHCP

b) Arrancar cada máquina virtual.

(9) Hosts alumnado: Máquinas virtuais Practica9-Cliente-Windows-DHCP

a) Configurar o xestor de redes de Microsoft Windows para que a conexión ethernet solicite a configuración de rede mediante DHCP:




b) Abrir unha consola e comprobar a configuración de rede. Executar:

```
> ipconfig /all #Amosar a configuración TCP/IP completa de todas as interfaces de rede.
>
```

c) Realizar de novo os apartados (4.b), (4.c) e (6) Que acontece? Por que?

(10) **HostA alumnado - Máquina virtual Microsoft Windows Server 2019**:

a) Parar o servizo DHCP. Abrir unha consola e executar:

```
> net start  #Amosar cales son os servizos en execución.
> net stop "servidor dhcp"  #Deter o servizo DHCP.
> net start  #Amosar cales son os servizos en execución.
```

b) Realizar de novo os apartados (4.b), (4.c) e (6) Que acontece? Por que?

c) Realizar de novo o apartado (3). Que configuración de rede obtedes para o portátil? Cubrir a seguinte táboa:

| Host | IP | Máscara Subrede | Gateway | Servidores DNS |
|---|---|---|---|---|
| Portátil | | | | |

d) Realizar de novo os apartados (4.b), (4.c) e (6) Que acontece? Por que?

e) Avisar ao docente para a revisión. ☐6

f) Arrancar o servizo DHCP. Abrir unha consola e executar:

```
> net start "servidor dhcp" #Arrancar o servizo DHCP.
> net start  #Amosar cales son os servizos en execución.
```

g) Realizar de novo os apartados (4.b), (4.c) e (6) Que acontece? Por que?

h) Avisar ao docente para a revisión. ☐7

(11) **HostA alumnado - Máquina virtual Microsoft Windows Server 2019**:

a) Consultar no visor de eventos os rexistros xenéricos de Windows:

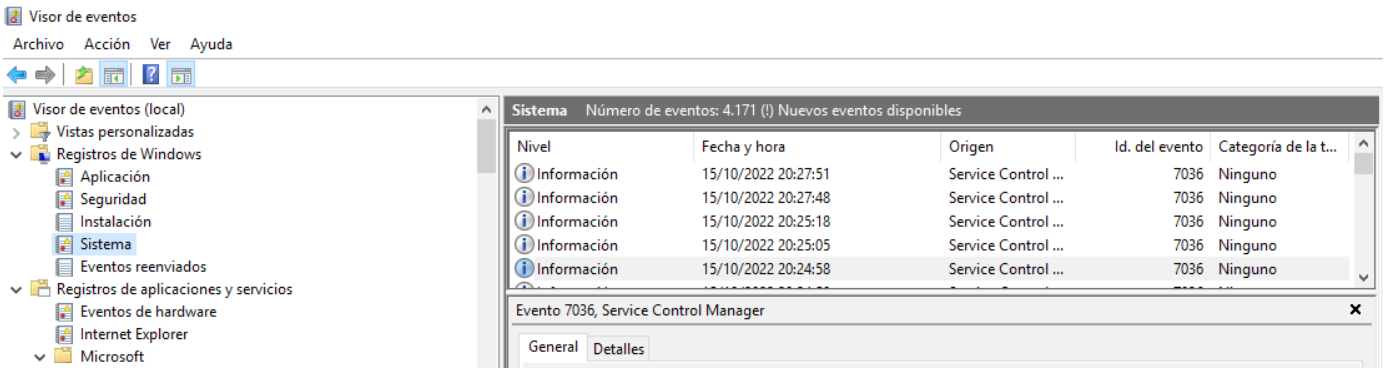



*Figura 12: Visor de eventos – Registros de Windows - Sistema*

b) Buscar no rexistro xenérico Sistema o patrón dhcp:

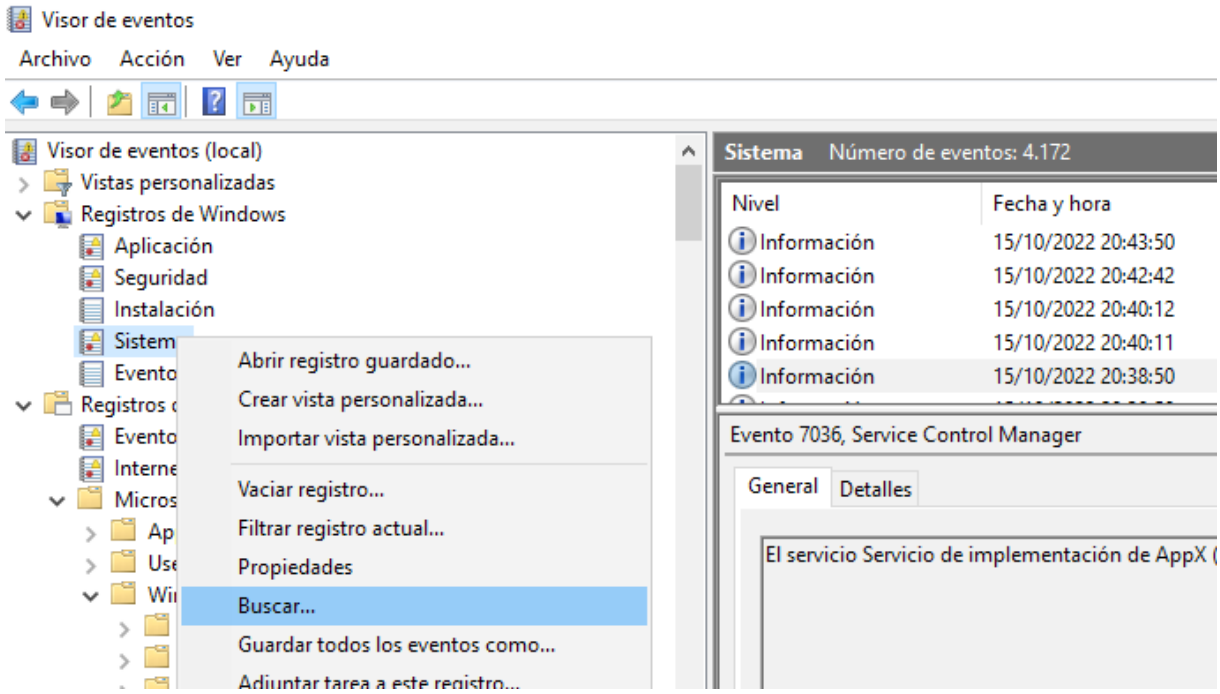



*Figura 13: Sistema - Buscar*

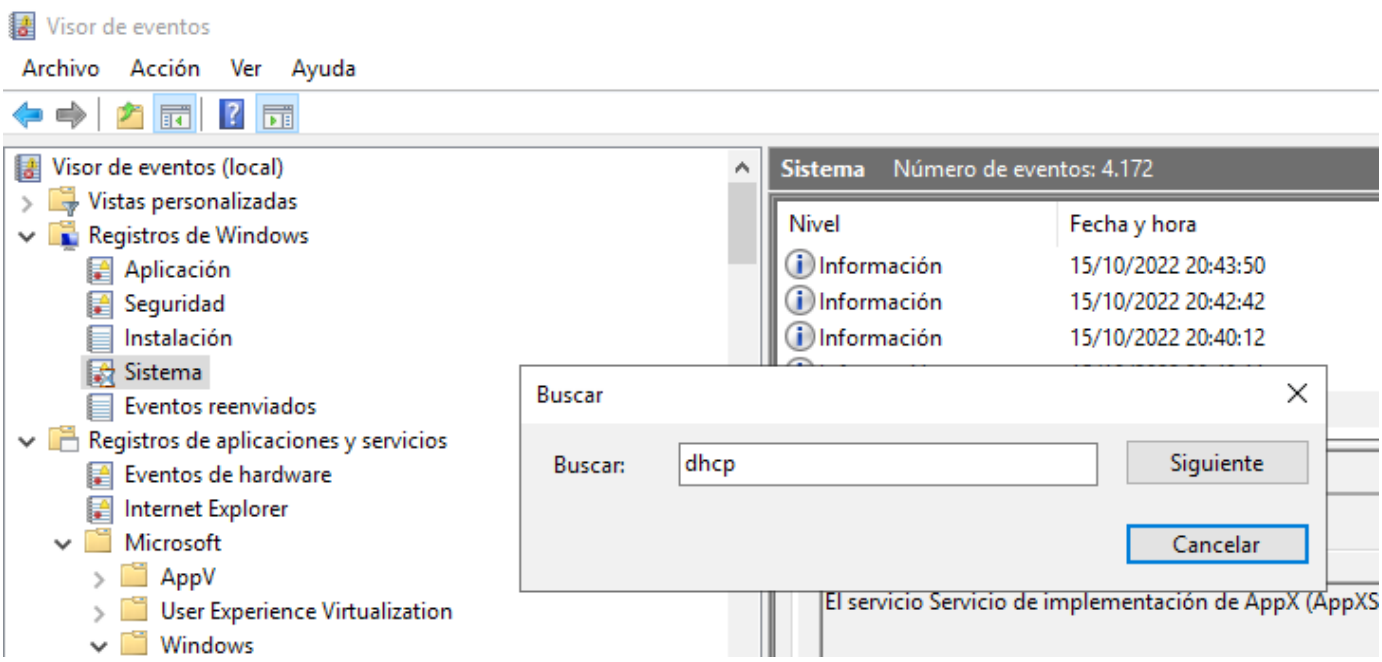



*Figura 14: Buscar - dhcp*

c) Consultar todos os sucesos atopados premendo en Siguiente:

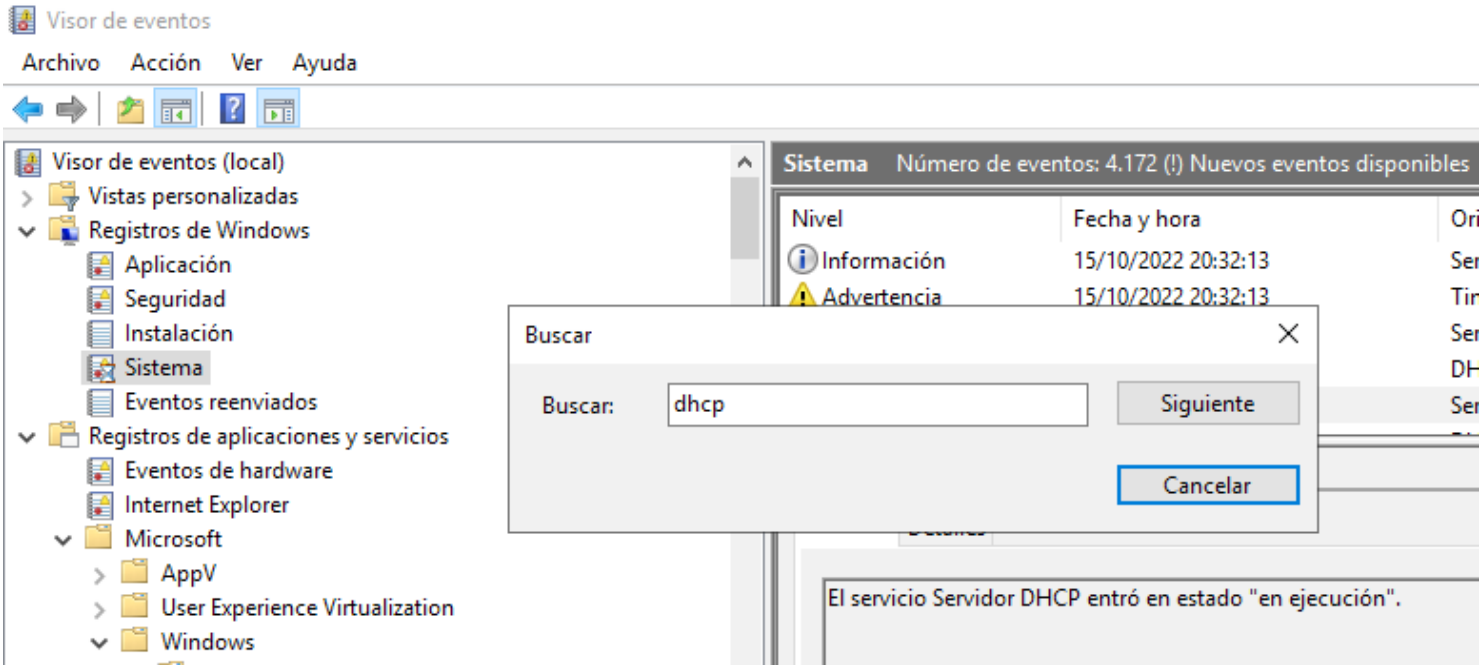



*Figura 15: Buscar dhcp - Siguiente*

d) Indicar se agora sodes quen de atopar os rexistros da parada (stop) e da execución (start) do servidor DHCP realizado no apartado (10). Se é así, cubride cada rexistro start/stop atopado na Táboa Registros de Windows (ver última páxina). Se é preciso xerade máis táboas seguindo este modelo.

e) Avisar ao docente para revisión. ☐ 8

(12) Contesta e razoa brevemente:

a) Nalgún apartado desta práctica os clientes DCHP obtiveron unha IP dentro do seguinte rango: `169.254.0.0–169.254.255.255` [8]. Se é o caso indica onde foi rexistrado ese suceso, ou como pode consultarse.

b) Avisar ao docente para a entrega e revisión da práctica. ☐ 9

## Revisión:

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7 ☐ 8 ☐ 9

| | Registros de Windows - Sistema | | | | | | |
|---|---|---|---|---|---|---|---|
| **Estado DHCP-Server** | **Nivel** | **Fecha y hora** | **Origen** | **Id. del evento** | **Categoría de la tarea** | **General** | **Detalles** |
| start | | | | | | | |
| stop | | | | | | | |