

Configuración de agente SNMP en Windows Server

CONFIGURACIÓN DE AGENTE SNMP EN WINDOWS SERVER.....	1
DESARROLLO DE LA GUÍA	3
PRIMERA PARTE. INSTALACIÓN DEL AGENTE SNMP EN WINDOWS 2016.....	3
<i>Paso 1. Configuración de la interfaz de red del servidor Windows 2016</i>	<i>3</i>
<i>Paso 2. Abrir el administrador de servidores</i>	<i>5</i>
<i>Paso 3. Instalación del agente SNMP.....</i>	<i>6</i>
SEGUNDA PARTE. CONFIGURACIÓN DEL AGENTE SNMP	9
<i>Paso 1. Abrir el administrador del Servicio SNMP.....</i>	<i>9</i>
<i>Paso 2. Configurar las opciones del agente SNMP.....</i>	<i>10</i>
TERCERA PARTE: CONFIGURACIÓN DE NM SNMP.....	12
<i>Paso 1 – Verificación de la comunicación IP desde LibreNMS hacia el FreeNAS.....</i>	<i>12</i>
<i>Paso 2 – Comprobación de la comunicación SNMP</i>	<i>12</i>
<i>Paso 3 – Agregar el agente SNMP usando la interfaz Web</i>	<i>13</i>
<i>Paso 4 – Verificar los datos del dispositivo SNMP ds01</i>	<i>15</i>
<i>Paso 5 – Monitoreo de los parámetros “Health”</i>	<i>16</i>
ANEXO – COMO CONFIGURAR WINDOWS 2016 DISMINUIR LA CANTIDAD DE INTERFACES DE RED ACTIVAS.....	19

Conceptos:

Protocolo LLTD Link Layer Discovery Protocol), Asignador de detección de topologías de nivel de vínculo:

LLDP es un Protocolo de Descubrimiento de Vecindario (Neighbor Discovery Protocol NDP), el cual ha sido diseñado para dispositivos de redes Ethernet (como switches y routers), Los NDP se usan para recibir y/o transmitir información relacionada con los dispositivos de otros nodos de la red, también para almacenar la información aprendida acerca de otros dispositivos.

LLDP es un protocolo de “un salto”; es decir que la información LLDP sólo se puede enviar y recibir por medio de dispositivos adyacentes, los cuales están conectados directamente entre sí por el mismo enlace, dichos dispositivos se denominan “vecinos”. La información anunciada nunca se reenvía a otros dispositivos en la red.

LLDP es un Protocolo de Descubrimiento de Vecinos, alternativo a CDP que ha sido diseñado para dispositivos de redes como switches y routers. Dicho protocolo solo trabaja en la Layer-2 modelo OSI.

LLDP, al igual que CDP, es un protocolo de red de nivel 2 utilizado para recibir/transmitir información de los equipos que están conectados (“vecinos”/neighbours). Una de las diferencias que tiene con CDP consiste en que en el caso de LLDP solo pueden recibir o enviar información a dispositivos adyacentes (no trata con direcciones IP), los cuales estén conectados directamente entre sí por el mismo enlace. Esta información nunca se reenvía a otros dispositivos en la red. Además, LLDP permite la comunicación de dicha información entre dispositivos de distintos fabricantes.

De esta manera, por ejemplo, un switch puede descubrir qué dispositivos son vecinos y los puertos por donde se conectan entre sí.

Cada dispositivo tiene su propio agente LLDP, el cual administra la accesibilidad a capas superiores y recoge la información de puntos terminales de los dispositivos adyacentes. Es decir, el agente LLDP se encarga de la recepción, envío y gestión de LLDP.

- Ruta del ejecutable: \Windows\System32\svchost.exe -k LocalService
- Nombre en inglés: Link-Layer Topology Discovery Mapper
- Nombre de Windows: lltdsvc
- Archivos asociados: lltdres.dll

Más información de LLDP se encuentra en <http://segweb.blogspot.com/2011/05/link-layer-discovery-protocol-lltd.html>

Desarrollo de la Guía

El objetivo de esta guía es configurar el Agente SNMP del dispositivo SNMP (FreeNAS) para ser monitoreado por el aplicativo de LibreNMS.

Pasos previos:

1. Instalar Windows Server 2016
2. Tener un AD (opcional)
3. Crear una GPO para conexión de clientes a SNMP

Primera Parte. Instalación del agente SNMP en Windows 2016

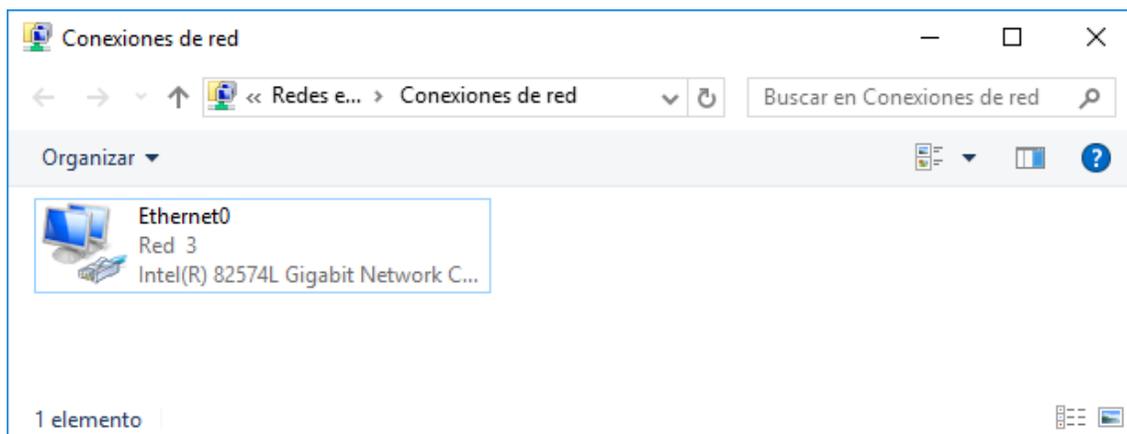
Paso 1. Configuración de la interfaz de red del servidor Windows 2016

1.1 Abrir Panel de control

1.2 Seleccionar Redes e Internet

1.3 Seleccionar Conexiones de red

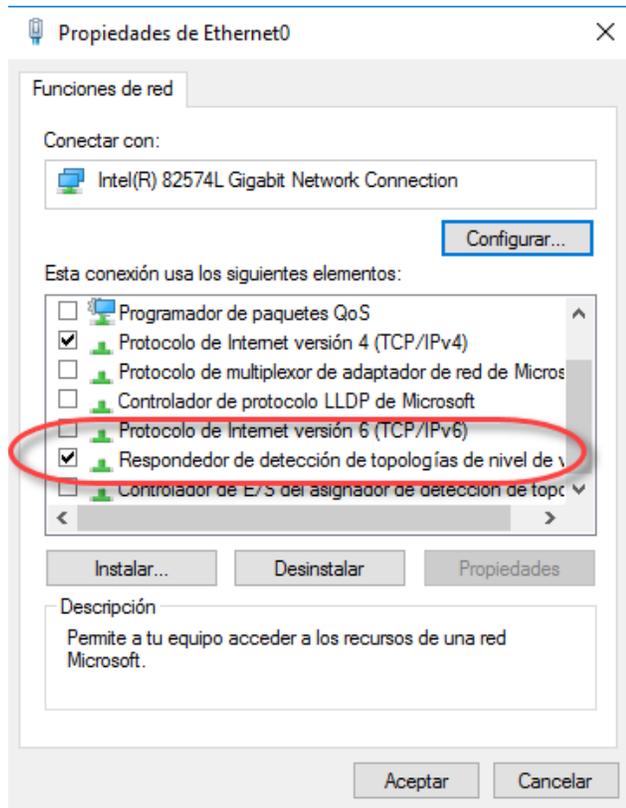
1.4 Seleccionar la interfaz de red a utilizar



1.5 Asignar la dirección IPv4 del servidor

Deberá ser una dirección estática del segmento 192.168.50+Y.0 / 24

1.6 Habilitar el protocolo Respondedor de detección de topologías de nivel de vínculo



Dar un clic en el botón “Aceptar”

1.7 Verificar la comunicación entre equipos

```
C:\Users\Administrador>ping librenms
```

```
Haciendo ping a librenms [192.168.50.7] con 32 bytes de datos:  
Respuesta desde 192.168.50.7: bytes=32 tiempo<1m TTL=64  
Respuesta desde 192.168.50.7: bytes=32 tiempo<1m TTL=64  
Respuesta desde 192.168.50.7: bytes=32 tiempo<1m TTL=64  
Respuesta desde 192.168.50.7: bytes=32 tiempo<1m TTL=64
```

```
Estadísticas de ping para 192.168.50.7:  
Paquetes: enviados = 4, recibidos = 4, perdidos = 0  
(0% perdidos),  
Tiempos aproximados de ida y vuelta en milisegundos:  
Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```

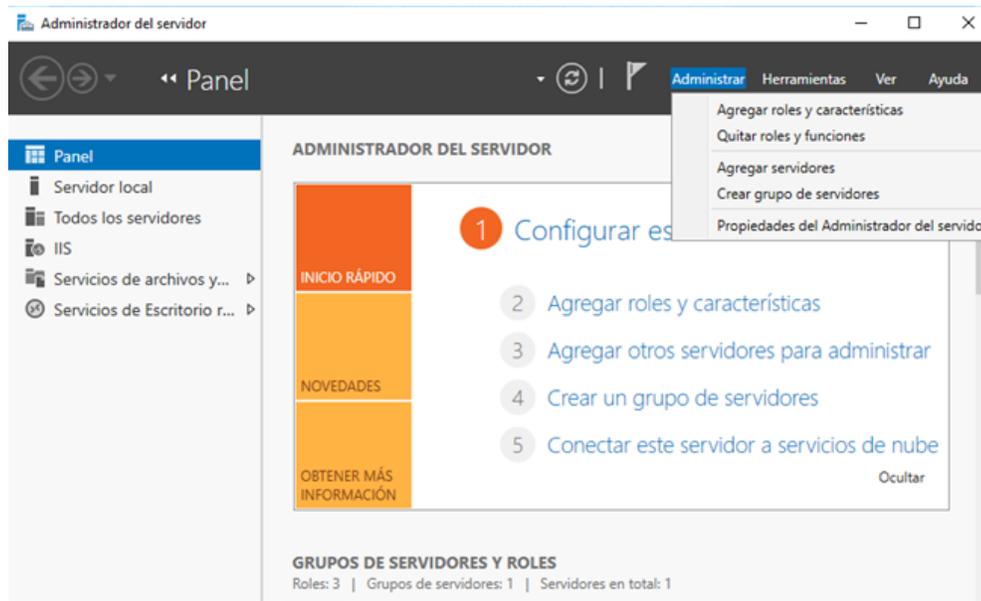
Paso 2. Abrir el administrador de servidores

2.1 Digitar Win + R

2.2 Escribir ServerManager.exe

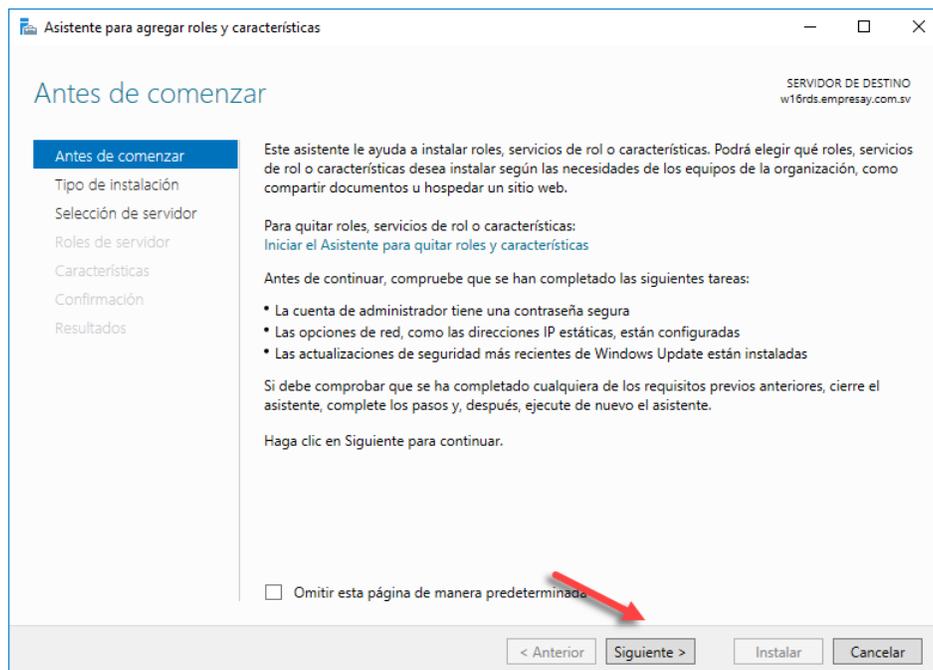
2.3 Presionar tecla enter

2.4 Dar un clic en el botón Administrar



2.5 Dar clic en la opción Agregar roles y características

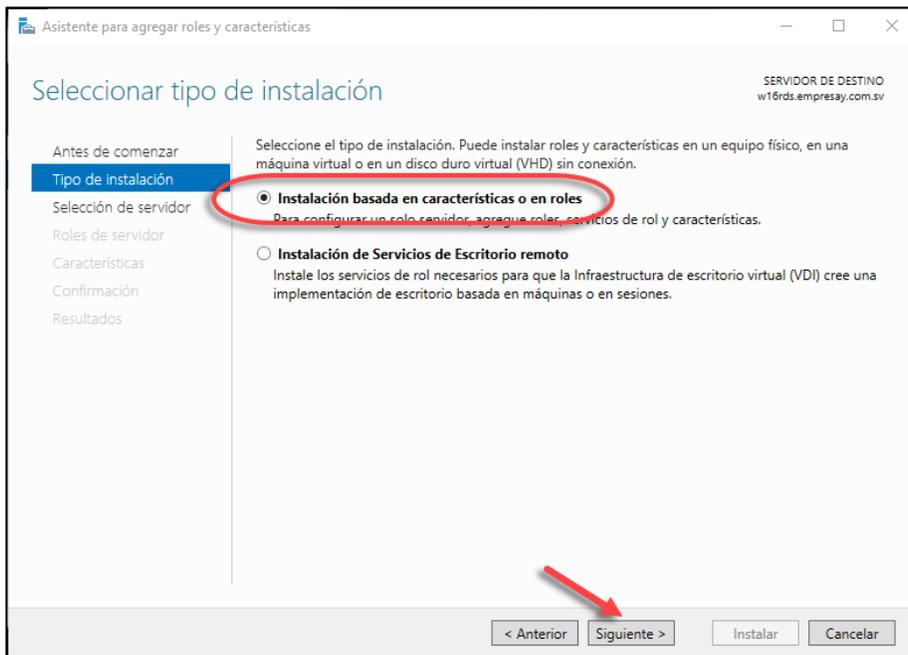
2.6 Confirmar el asistente



Dar clic en el botón siguiente.

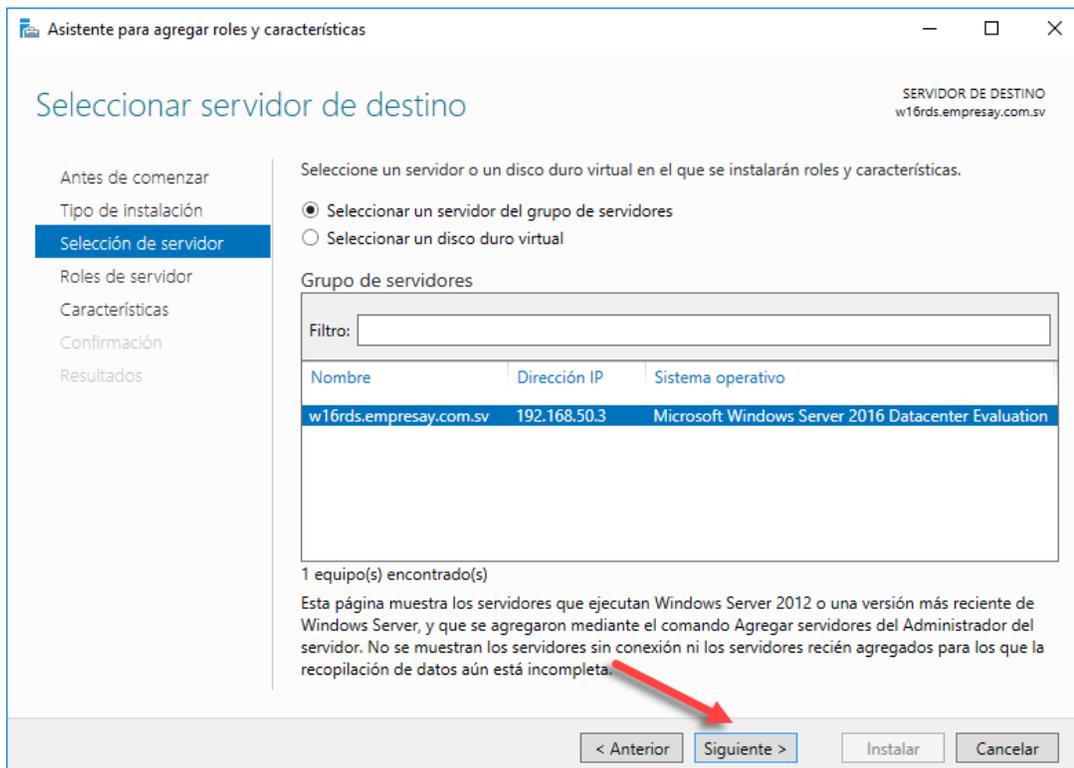
Paso 3. Instalación del agente SNMP

3.1 Seleccionar instalación basada en características



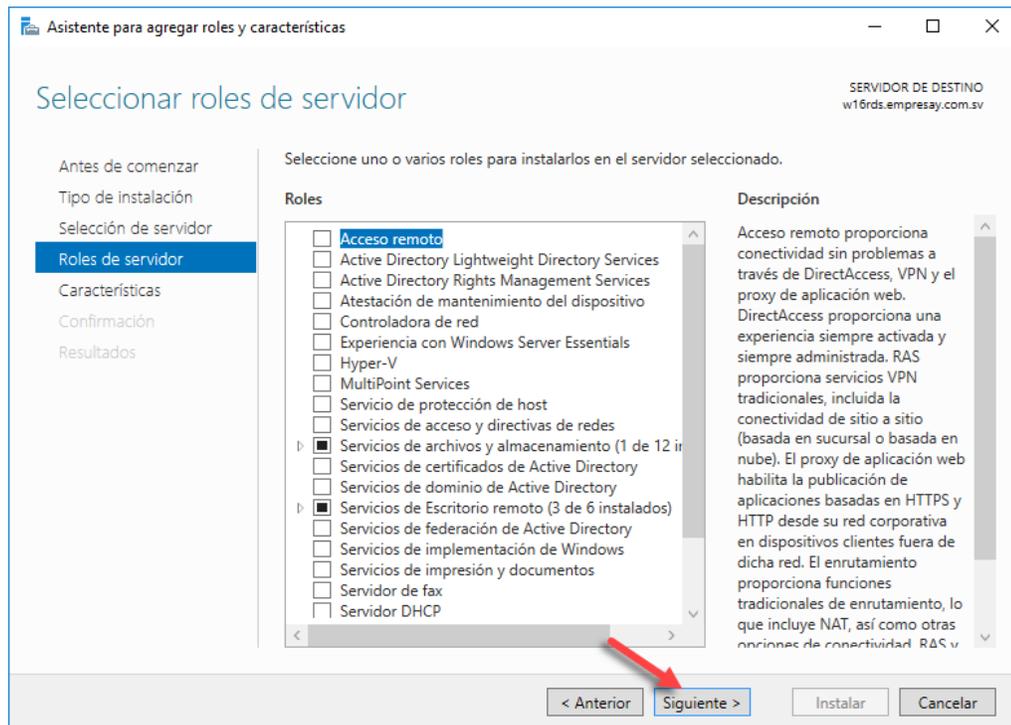
Dar clic en el botón siguiente.

3.2 Seleccionar el servidor a configurar



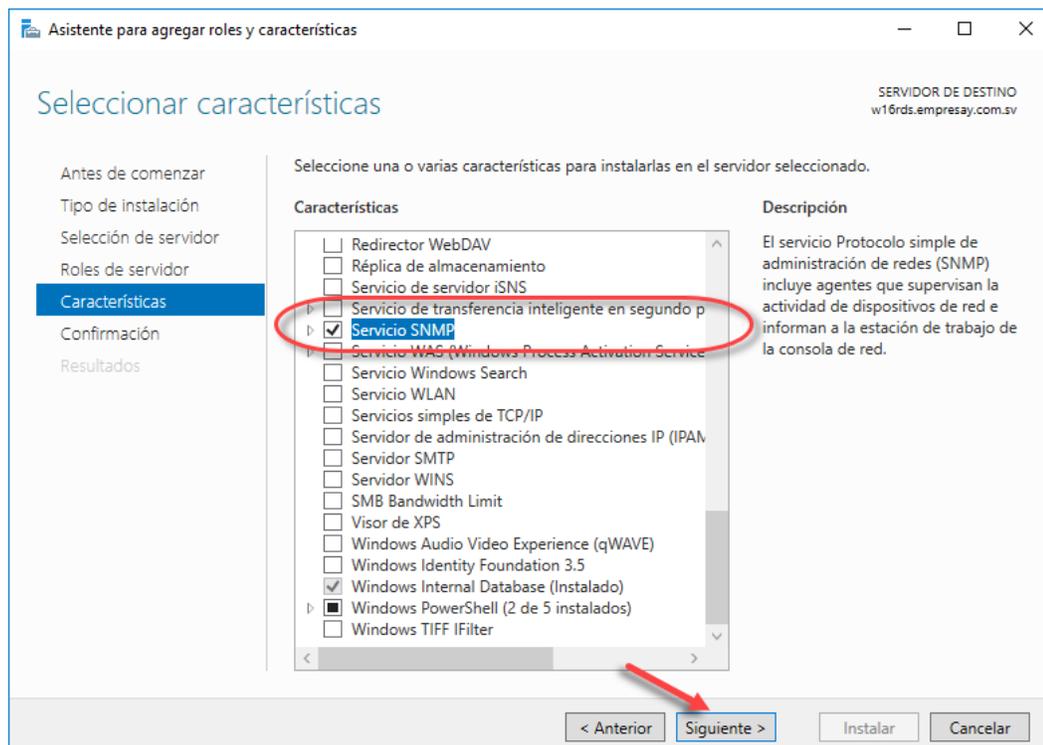
Dar clic en el botón siguiente.

3.3 Omitir selección de Roles



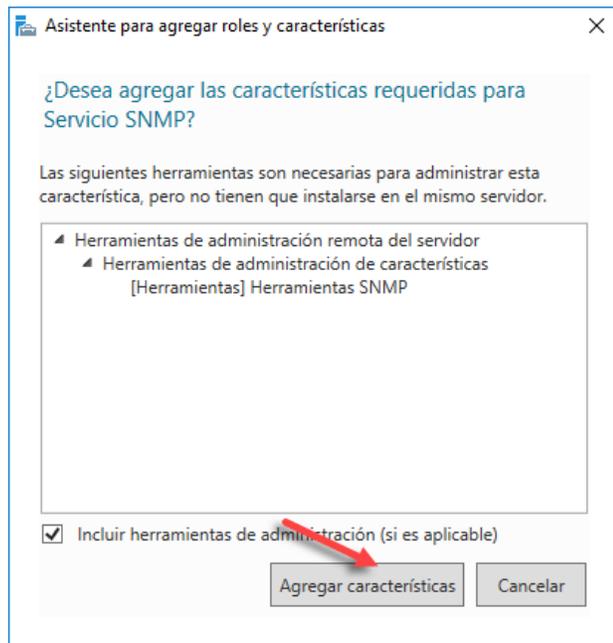
Dar clic en el botón siguiente.

3.4 Seleccionar Servidor SNMP



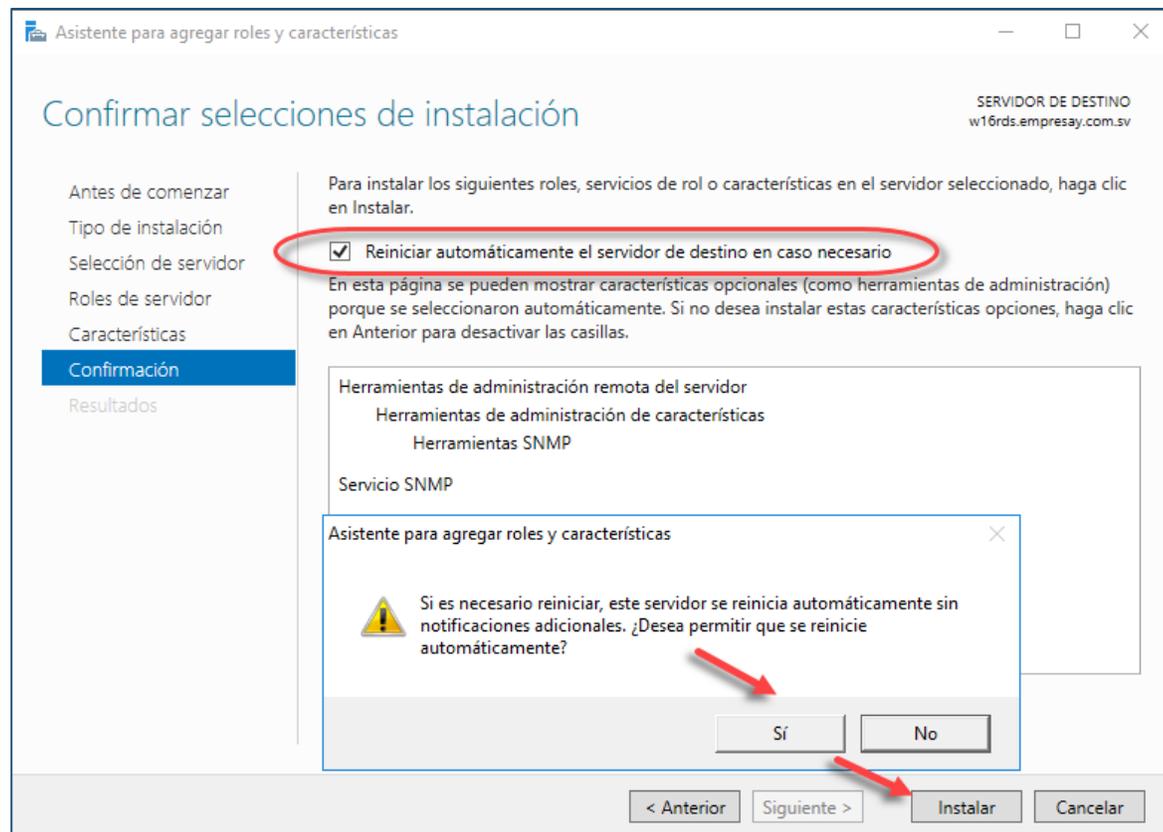
Dar clic en el botón siguiente.

3.5 Aprobar la instalación de los complementos del agente SNMP



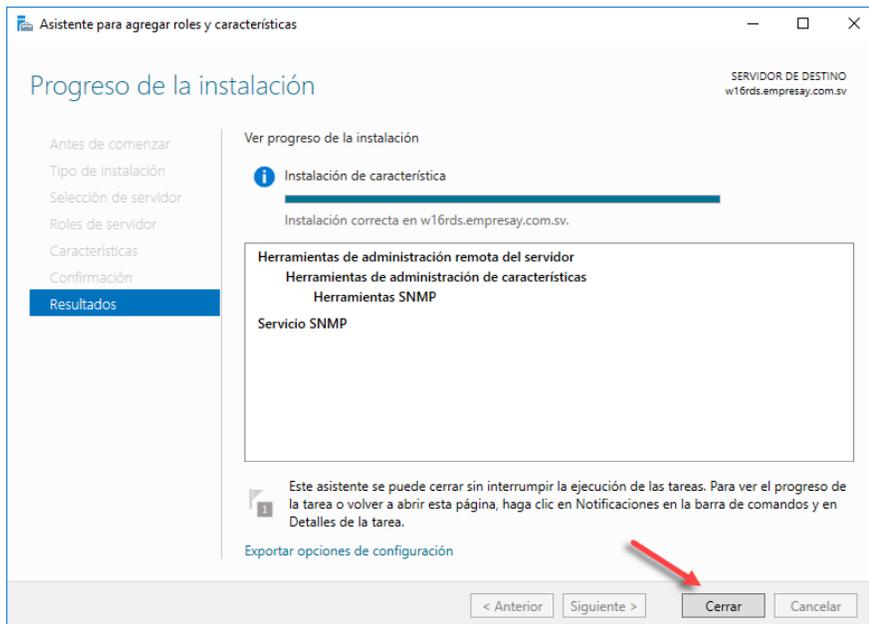
Dar clic en el botón Agregar características

3.6 Confirmar las actualizaciones



Dar clic en el botón Instalar

3.7 Verificar la instalación.



3.8 Reiniciar el equipo.

Segunda Parte. Configuración del agente SNMP

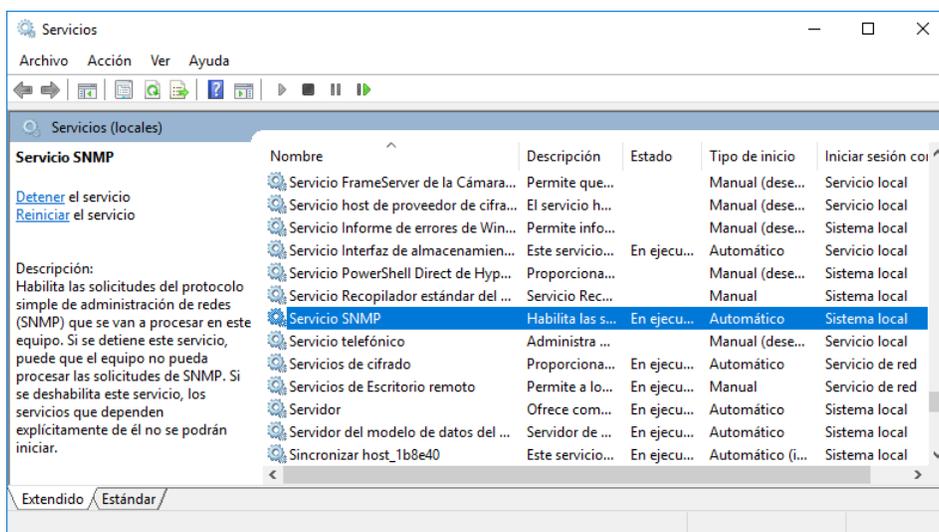
Paso 1. Abrir el administrador del Servicio SNMP

1.1 Digitar Win + R

1.2 Escribir services.msc

1.3 Presionar tecla enter

1.4 Ubicar el servicio SNMP



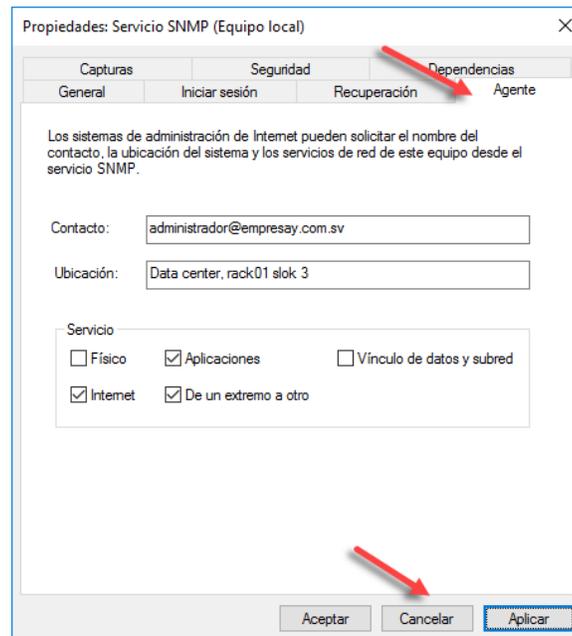
1.5 Dar doble clic en el servicio SNMP

Paso 2. Configurar las opciones del agente SNMP

2.1 Seleccionar la ficha Agente

Digitar las siguientes opciones:

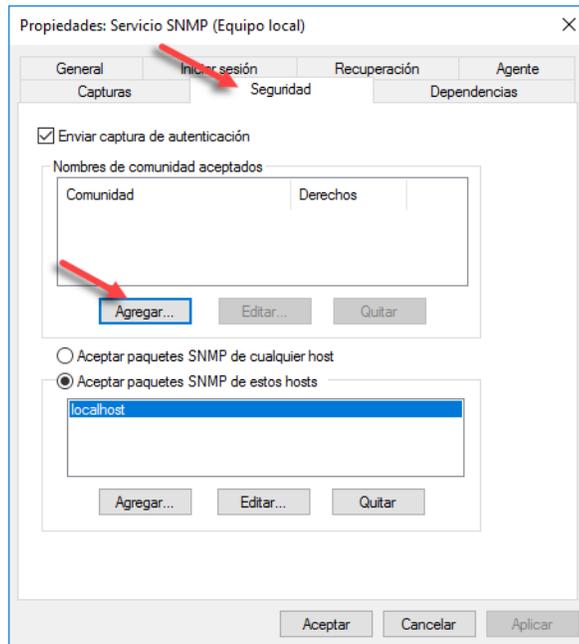
- Contacto: administrador@empresay.com.sv
- Ubicación: Data center, rack01, slot 3



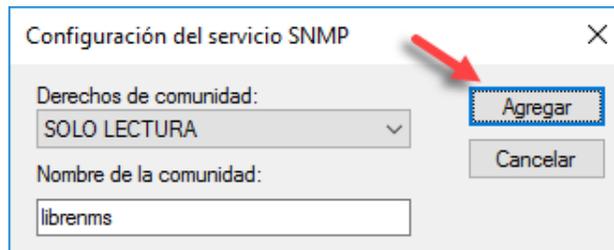
Dar clic en el botón Aplicar

2.2 Configurar la ficha seguridad

- A. Seleccionar la opción Enviar captura de autenticación

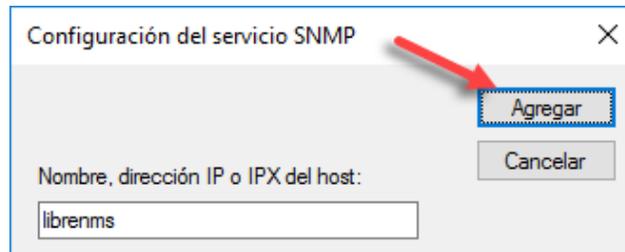


- B. Dar un clic en el botón **Agregar...**
Definir las siguientes opciones:
- Derecho de la comunidad: Solo lectura
 - Nombre de la comunidad: librenms



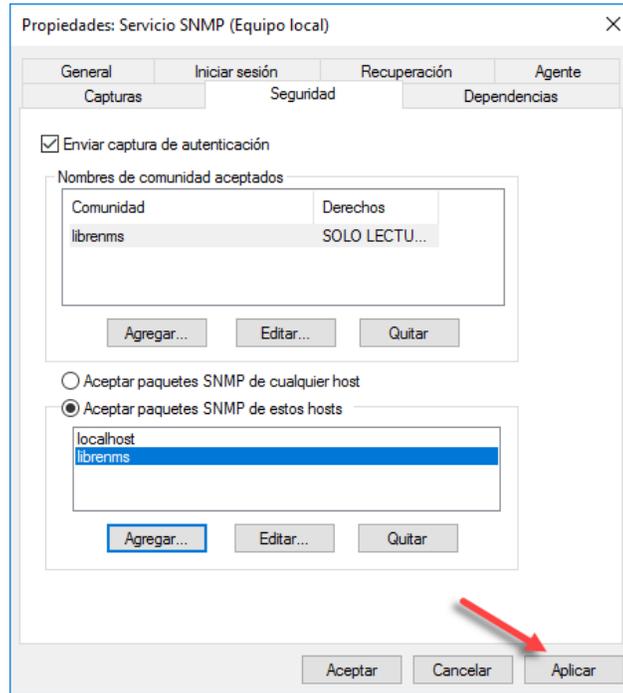
Dar clic en el botón **Agregar**.

- C. Seleccionar la opción: **Aceptar paquetes SNMP de estos hosts**
Digite el nombre o FQDN o Dirección IP del equipo que ejecuta LibreNMS



Dar clic en el botón **Agregar**.

- D. Dar clic en el botón **Aplicar** y **Aceptar**



Tercera parte: Configuración de NM SNMP

Paso 1 – Verificación de la comunicación IP desde LibreNMS hacia el FreeNAS

```
librenms@librenms:~$ ping -c 3 w16rds
```

```
PING w16rds.emresay.com.sv (192.168.50.3) 56(84) bytes of data.
64 bytes from w16rds.emresay.com.sv (192.168.50.3): icmp_seq=1 ttl=128 time=0.898 ms
64 bytes from w16rds.emresay.com.sv (192.168.50.3): icmp_seq=2 ttl=128 time=0.438 ms
64 bytes from w16rds.emresay.com.sv (192.168.50.3): icmp_seq=3 ttl=128 time=0.275 ms
```

```
--- w16rds.emresay.com.sv ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2001ms
rtt min/avg/max/mdev = 0.275/0.537/0.898/0.263 ms
```

Nota: si el DNS no estuviera configurado, agregue en el archivo `/etc/hosts` los registros de los servidores de la red.

```
librenms@librenms:~$ cat /etc/hosts
```

```
127.0.0.1      localhost.localdomain  localhost
127.0.1.1      librenms
::1           localhost ip6-localhost ip6-loopback
ff02::1       ip6-allnodes
ff02::2       ip6-allrouters

192.168.50.2   ds01.empresay.com.sv   ds01
192.168.50.2   ds01.empresay.com.sv   ds01
192.168.50.7   librenms.empresay.com.sv librenms
```

Paso 2 – Comprobación de la comunicación SNMP

Para el NM SNMP (Network Monitor), se ha configurado como comunidad SNMP la palabra “librenms”
 Configuración de agente SNMP en Windows Server 2016 – Víctor Cuchillac (padre) – Página 12 de 22

2.1 Verificar el estado del agente SNMP en el servidor Windows 2016

```
librenms@librenms:~$ snmpstatus -c librenms -v2c w16rds
```

```
[UDP: [192.168.50.3]:161->[0.0.0.0]:51942]=>[Hardware: Intel64 Family 6 Model 142 Stepping 9 AT/AT COMPATIBLE - Software: Windows Version 6.3 (Build 14393 Multiprocessor Free)] Up: 5:32:07.68  
Interfaces: 16, Recv/Trans packets: 19077/12956 | IP: 6296/3609
```

2.2 Comprobar comunicación con el agente en ds01

```
librenms@librenms:~$ /usr/bin/snmpbulkwalk -v2c -c librenms w16rds:161 |head
```

```
iso.3.6.1.2.1.1.1.0 = STRING: "Hardware: Intel64 Family 6 Model 142 Stepping 9 AT/AT COMPATIBLE - Software: Windows Version 6.3 (Build 14393 Multiprocessor Free)"  
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.311.1.1.3.1.2  
iso.3.6.1.2.1.1.3.0 = Timeticks: (2001318) 5:33:33.18  
iso.3.6.1.2.1.1.4.0 = STRING: "administrador@empresay.com.sv"  
iso.3.6.1.2.1.1.5.0 = STRING: "w16rds.empresay.com.sv"  
iso.3.6.1.2.1.1.6.0 = STRING: "Data center, rack01 slok 3"  
iso.3.6.1.2.1.1.7.0 = INTEGER: 76  
iso.3.6.1.2.1.2.1.0 = INTEGER: 16  
iso.3.6.1.2.1.2.2.1.1.1 = INTEGER: 1  
iso.3.6.1.2.1.2.2.1.1.2 = INTEGER: 2  
iso.3.6.1.2.1.1.9.1.2.2 = OID: iso.3.6.1.6.3.15.2.1.1
```

2.3 Hacer una consulta usando la MIB de DELL que tiene LibreNMS

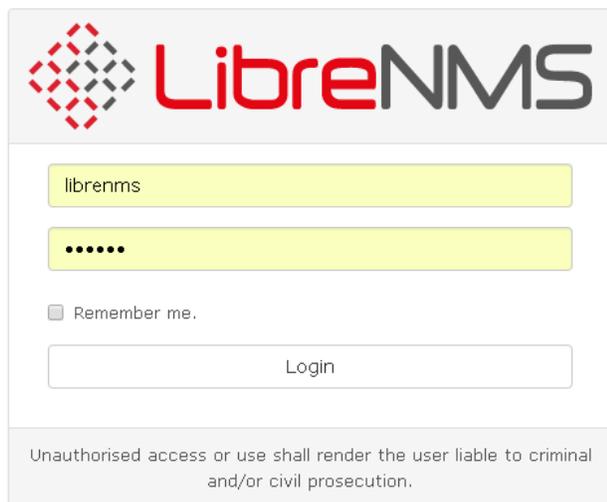
```
librenms@librenms:~$ /usr/bin/snmpget -v2c -c librenms -OqUt -m SNMPv2-MIB -M /opt/librenms/mibs:/opt/librenms/mibs/dell udp:w16rds:161 sysUpTime.0 sysLocation.0 sysContact.0 sysName.0 sysObjectID.0 sysDescr.0
```

```
.1.3.6.1.2.1.1.3.0 = 2701823  
.1.3.6.1.2.1.1.6.0 = Data center, rack01 slok 3  
.1.3.6.1.2.1.1.4.0 = administrador@empresay.com.sv  
.1.3.6.1.2.1.1.5.0 = w16rds.empresay.com.sv  
.1.3.6.1.2.1.1.2.0 = .1.3.6.1.4.1.311.1.1.3.1.2  
.1.3.6.1.2.1.1.1.0 = Hardware: Intel64 Family 6 Model 142 Stepping 9 AT/AT COMPATIBLE - Software: Windows Version 6.3 (Build 14393 Multiprocessor Free)
```

Paso 3 – Agregar el agente SNMP usando la interfaz Web

3.1 Ingresar a la interfaz web del Appliance Librenms

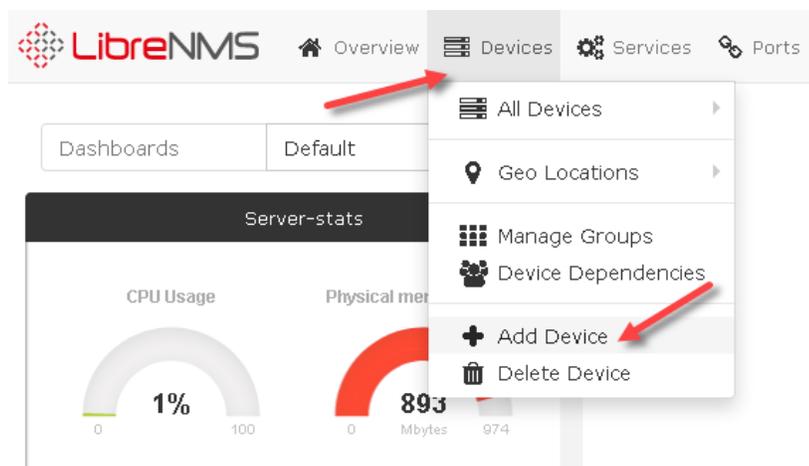
Utilizar el usuario librenms/123456



The image shows the LibreNMS login interface. At the top left is the LibreNMS logo. Below it is a text input field containing 'librenms'. Underneath is a password input field with six dots. A checkbox labeled 'Remember me.' is present. A 'Login' button is at the bottom. At the very bottom, there is a disclaimer: 'Unauthorised access or use shall render the user liable to criminal and/or civil prosecution.'

3.2 Agregar el dispositivo SNMP

- Dar clic en menú “Devices”
- Dar clic en menú “+ Add Device”



3.3 Completar los datos de la pantalla

- Hostname: ds01 (debe existir resolución local o por DNS)
- SNMP: On
- SNMP versión: v2c
- Protocolo: udp
- Puerto: 161
- Comunity: librenms

Add Device

Devices will be checked for Ping/SNMP reachability before being probed.

Hostname

SNMP ON

SNMP Version

Port Association Mode

SNMPv1/2c Configuration

Community

Force add - No ICMP or SNMP checks performed

3.4 Dar clic en botón “Add Device”

3.5 Verificar que se haya agregado correctamente el dispositivo SNMP

✔ Adding host w16rds community librenms port 161 using udp

✔ Device added w16rds (3)

Paso 4 – Verificar los datos del dispositivo SNMP ds01

LibreNMS Overview Devices Services Ports Health Alerts Global Search

Lists: Basic | **Detail** | Graphs: Bits | CPU | Load | Memory | Uptime | Storage | Disk I/O | Poller | Ping | Temperature Agent Remove Search | Remove Header

50

Search All OSes All Versions All Platforms All Featuresets All Locations Server Search Update URL Reset

Vendor	Device	Metrics	Platform	Operating System	Uptime	Location	Actions
	ds01 ds01.empresay.com.sv	4	amd64 GENERIC	FreeBSD Intel(R)	1h 57m 33s	datacenter	
	localhost librenms	2	Generic x86 64-bit Ubuntu 16.04	Linux 4.4.0-130-generic	9h 12m 45s	Rack, Room, Building, City, Coun	
	w16rds w16rds.empresay.com.sv	17	Intel x64 Multiprocessor	Microsoft Windows Server 2016 (NT 6.3)	6h 57m 19s	Data center, rack01 slok 3	

Showing 1 to 3 of 3 entries

Paso 5 – Monitoreo de los parámetros “Health”

5.1 Dar un clic en el botón “Health” “con un corazón”

5.2 Verificar los valores de la memoria

Home Overview Services Ports Health Alerts Global Search

Health » **Memory** | Processor | Storage | Toner Graphs | **No Graphs**

Search w16rds 50

Device	Memory	Used	Usage
w16rds	Physical Memory	1.120GB / 4.000GB 2.880GB	28%
w16rds	Virtual Memory	1.290GB / 4.690GB 3.400GB	27%

Showing 1 to 2 of 2 entries

5.3 Verificar los valores para los procesadores

Health » Memory | **Processor** | Storage | Toner Graphs | **No Graphs**

Search: w16rds Refresh 50 List Icon

Device	Processor	Usage
w16rds	Processor	1% 99%
w16rds	Processor	1% 99%
w16rds	Processor	1% 99%
w16rds	Processor	1% 99%

« < 1 > » Showing 1 to 4 of 4 entries

5.4 Verificar los valores del almacenamiento

Health » Memory | Processor | **Storage** | Toner Graphs | **No Graphs**

Search: w16rds Refresh 50 List Icon

Device	Storage	Used	Usage
w16rds	C:\ Label: Serial Number 52bc3e67	14.190GB / 59.510GB	0.000B 0%

« < 1 > » Showing 1 to 1 of 1 entries

5.5 Verificar otras gráficas

LibreNMS Overview Devices Services Ports Health Alerts Global Search

w16rds
Data center, rack01 slok 3

Memory Usage Processor Usage

Overview Graphs Health Ports Inventory Services Logs Alerts Alert Stats Notes

Hardware: Intel64 Family 6 Model 142 Stepping 9 AT/AT COMPATIBLE - Software: Windows Version 6.3 (Build 14393 Multiprocessor Free)

System Name	w16rds.empresay.com.sv
Hardware	Intel x64
Operating System	Microsoft Windows Server 2016 (NT 6.3) (Multiprocessor)
Object ID	.1.3.6.1.4.1.311.1.1.3.1.2
Contact	administrador@empresay.com.sv
Location	Data center, rack01 slok 3
Lat / Lng	[30.207108,-97.700668] Map
Uptime	7h 2m 20s

Processors

Processor x4 0%

Overall Traffic

Memory Pools

Virtual Memory	27%
Physical Memory	28%

Anexo – Como configurar Windows 2016 disminuir la cantidad de interfaces de red activas.

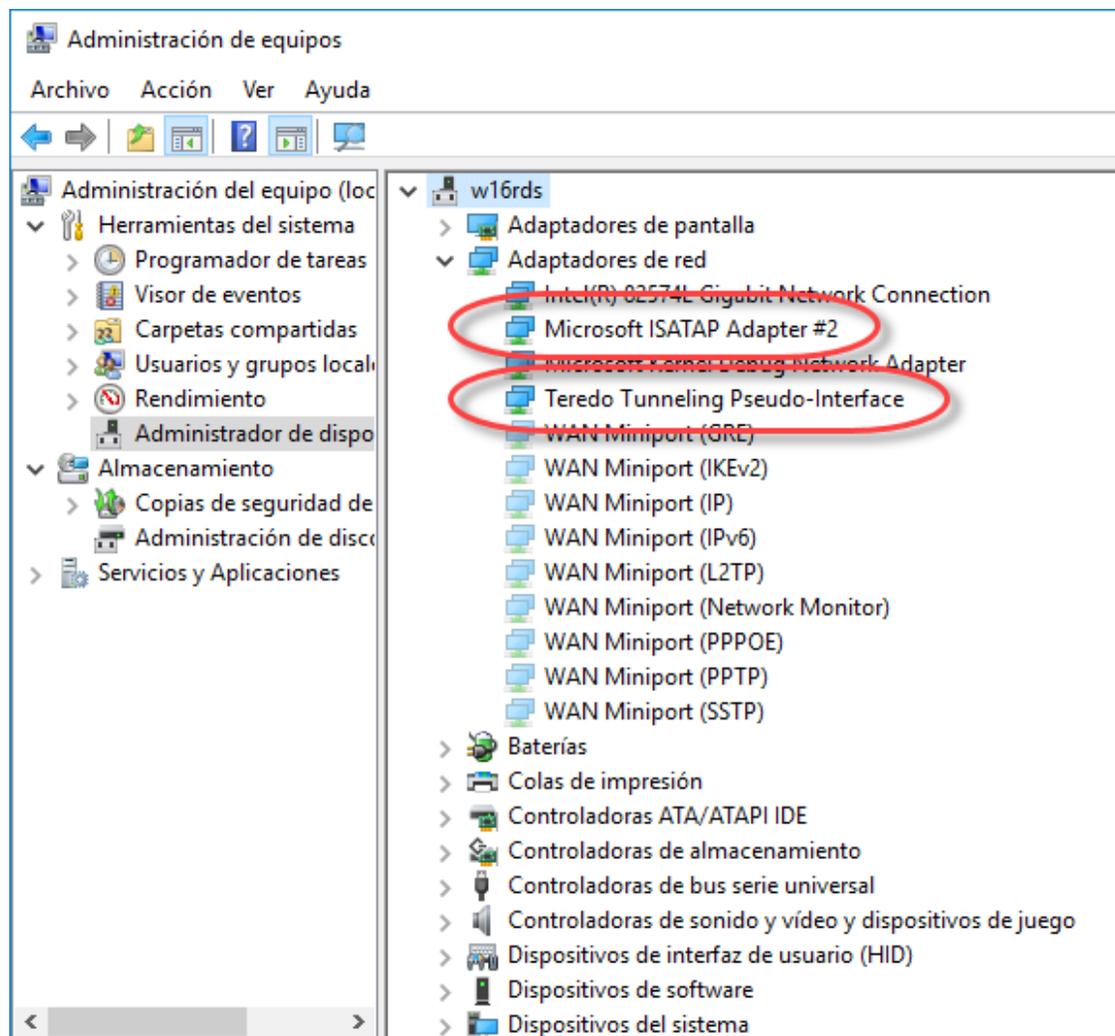
Para identificar la dirección Física y ID en el registro de windows

```
C:\Users\Administrador>getmac
```

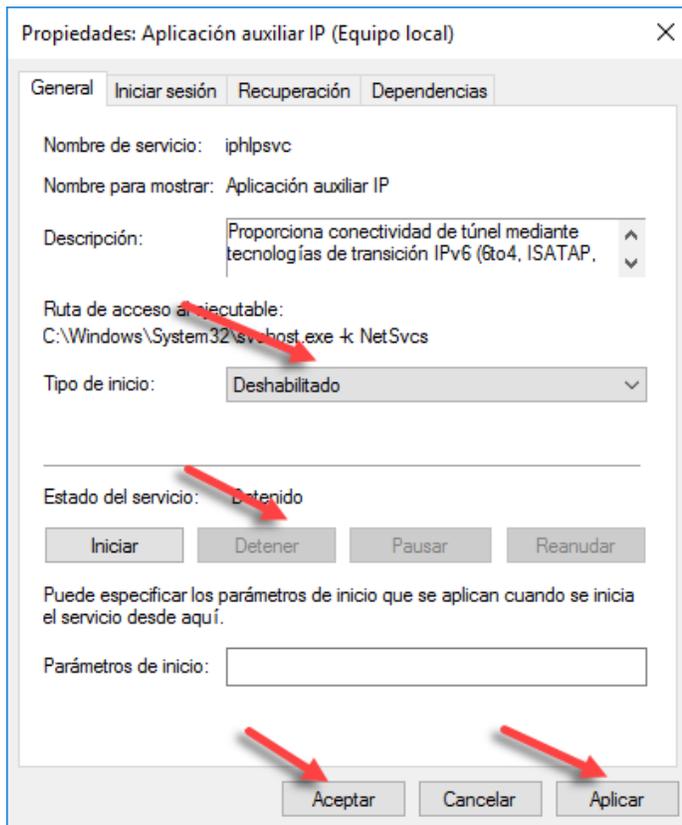
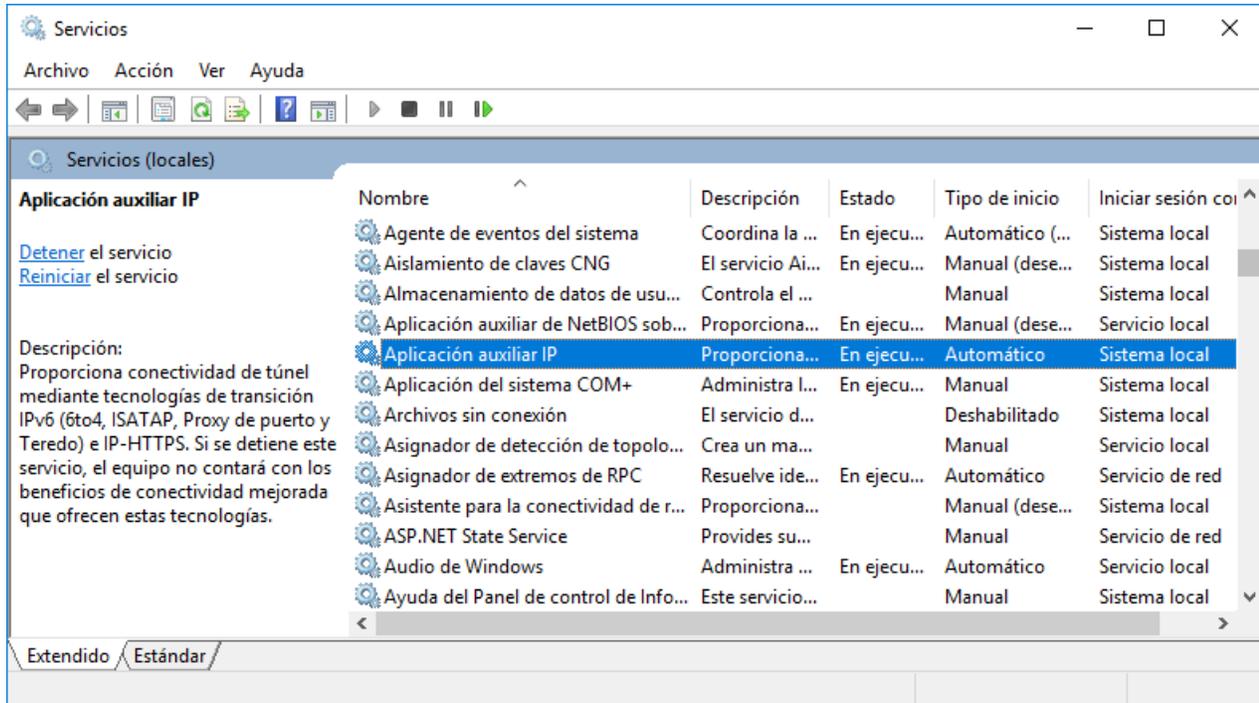
```
Dirección física      Nombre de transporte
=====
00-0C-29-26-07-ED    \Device\Tcpip_{54E55D4E-C805-4C8F-9245-344F9609CED2}
```

Para borrar las interfaces creadas automáticamente

En el administrador de equipos, eliminar las intrfaces, MS ISATAP, Teredo Tunneling Pseudo-interface, IPv6to4

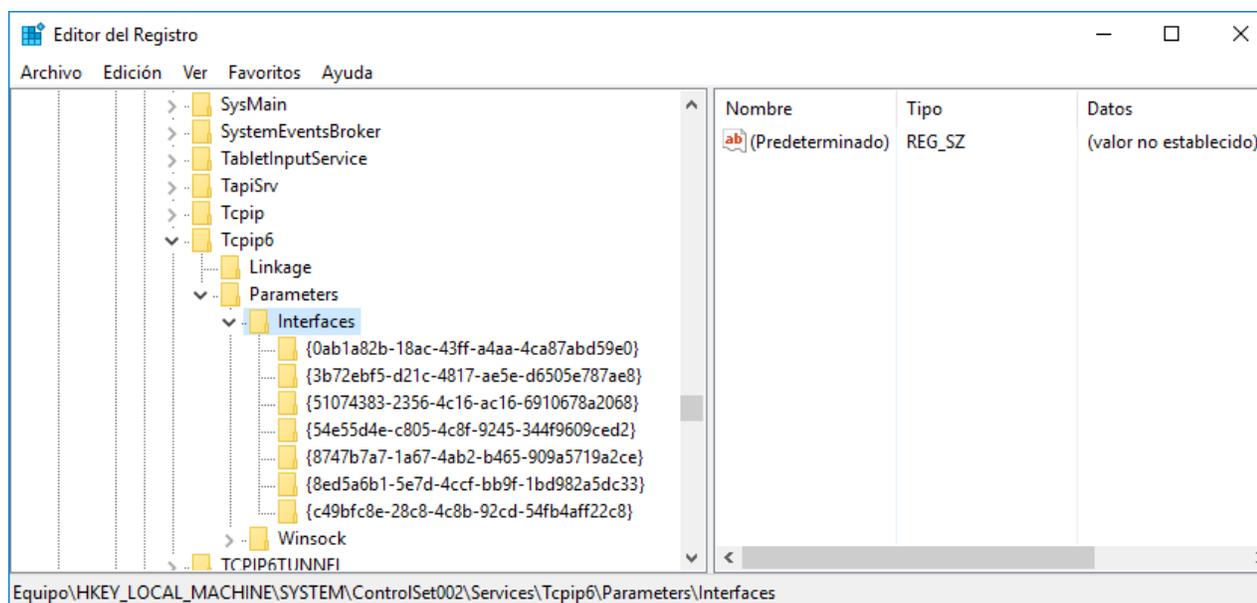
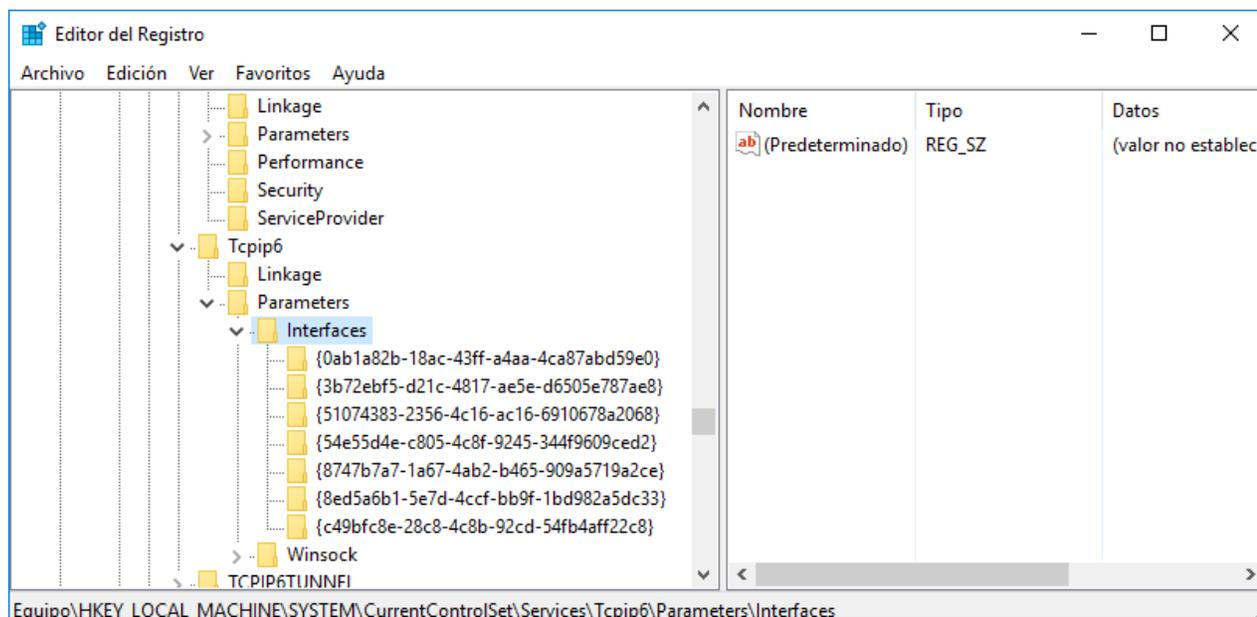


Detener el servicio que crea las interfaces teredo, ISATAP y Ipv6to4



Cadenas del registro que se pueden borrar

Para eliminar las interfaces de red que no se utilicen o que han sido creadas automáticamente.



Comandos para deshabilitar los servicios Teredo e ISATAP

```
C:\>netsh interface teredo show state
```

```
Parámetros de Teredo
```

```
-----  
Tipo : client  
Nombre del servidor : win10.ipv6.microsoft.com.  
Intervalo de actualización del cliente: 30 segundos  
Puerto de cliente : unspecified
```

```
C:\>netsh interface teredo set state disable
```

```
Aceptar
```

```
C:\>netsh interface isatap show
```

Los siguientes comandos están disponibles:

Comandos en este contexto:

```
show router    - Muestra la información del enrutador ISATAP.  
show state    - Muestra el estado de ISATAP.
```

```
C:\>netsh interface isatap show state
```

```
Estado de ISATAP          : default
```

```
C:\>netsh interface isatap set state disable
```

Aceptar

Cómo identificar la interfaz de red real

En LibreNMS no todas las interfaces detectadas corresponden a la verdadera NIC

