



Introducción

UDS Enterprise permite la publicación de diferentes tipos de servicios. Entre ellos, se encuentra la conexión remota con máquinas físicas (ya sea a un pool de máquinas o a una máquina específica). Con anterioridad, cuando una de estas máquinas físicas se encontraba en estado apagado y era necesario arrancarla de forma automática, había que apoyarse en herramientas de terceros tipo OpenGnsys, que permite enviar Wake on LAN (WoL) a los equipos.

El presente documento explica cómo configurar UDS Enterprise para que envíe toda la información necesaria a uno o varios servidores WoL y que sean capaces de iniciar equipos físicos a petición de los usuarios.

Requisitos

A continuación, detallaremos los requisitos más importantes que se han de cumplir para poder utilizar WoL con UDS Enterprise:

- Disponer de un entorno activo de UDS Enterprise en versión 3.5 o superior.
- Las máquinas físicas a las que se les enviará la orden de inicio deben disponer de soporte para WoL
- Los diferentes elementos existentes en la red donde estén conectados los equipos físicos (routers, firewall, switches, etc...) tienen que soportar el envío del WoL
- Es necesario disponer de al menos un servidor WoL (en el presente documento se utiliza un servidor WoL de ejemplo)



Servidor Wake on LAN

Configuraremos un servidor WoL encargado de enviar los “**Magic Paquet**” a los equipos físicos para que se enciendan. Dependiendo de la complejidad de nuestra red y de los diferentes elementos existentes en ella, deberemos configurar un único servidor o varios.

El envío del WoL a través de la red puede ser interrumpido por routers, firewalls, switches y demás elementos existentes en la red. Por eso, es recomendable colocar un servidor WoL por cada red donde se encuentren los equipos físicos a iniciar. También se pueden añadir nuevos interfaces de red al servidor WoL que conecte a los diferentes segmentos de red donde se encuentren dichos equipos.

Para facilitar la tarea de despliegue de este servidor, UDS facilita un Appliance de ejemplo con una serie de recursos muy básicos pero suficientes para esta tarea.

El servidor se puede descargar del siguiente repositorio:

<https://images.udsenderprise.com/files/WoL/Debian-WoL.ova>

Datos del servidor:

- S.O.: Debian 11
- vCPUs: 1
- vRAM: 1024 MB
- Disk: 8 GB
- User: root
- Password: uds

NOTA: El servidor se facilita como Virtual Appliance en formato **.ova**. Si fuera necesario convertirlo a otro formato diferente para su uso en otras plataformas de virtualización, se pueden utilizar herramientas de conversión como **qemu-img** (puede convertir el disco en formato **.vmdk** extraído del **.ova** en cualquier otro formato).

El servidor WoL facilitado por el equipo de UDS Enterprise incluye el software “**etherwake**”, encargado del encendido de los equipos una vez indicada su dirección MAC.



Dentro del servidor, en la ruta: `/usr/lib/cgi-bin/` se encuentra el script **etherwake.py** configurado, a forma de ejemplo, de la siguiente manera:

```
GNU nano 3.2 /usr/lib/cgi-bin/etherwake.py
#!/usr/bin/env python3
import cgi
import subprocess
import ipaddress

IFACE = 'eth0'
ETHERWAKE = '/usr/sbin/etherwake {MAC} -i {IFACE} -b'
SECRET = 'simkem0t'

nets = {
    '192.168.11.0/24': 'eth0',
    '192.168.0.0/20': 'eth0',
    '172.27.0.0/20': 'eth1'
}

args = cgi.FieldStorage()

print('Content-Type: text/plain')
print('')

if 'secret' not in args or 'mac' not in args or args['secret'].value != SECRET:
    print('NOT DONE')
else:
    try:
        iface = IFACE
        if 'ip' in args:
            ip = ipaddress.ip_address(args['ip'].value)
            for net, interface in nets.items():
                if ip in ipaddress.ip_network(net):
                    iface = interface
                    break
        cmd = ETHERWAKE.format(MAC=args['mac'].value, IFACE=iface)
        #print(cmd)
        result = subprocess.run(cmd, shell=True, check=True)
        print('Executed')
    except Exception as e:
        print('Error on WOL: %s' % e)
```

En el script deberemos tener en cuenta los siguientes elementos:

- Apartado “**SECRET**”: Debemos indicar una cadena de caracteres alfanuméricos para dotar de mayor seguridad a la conexión entre el servidor UDS y el servidor WoL. Esta misma cadena la usaremos también cuando configuremos el servidor WoL desde la administración de UDS Enterprise. Es básicamente un parámetro de seguridad, que impide que cualquier persona que conozca el servidor WoL pueda realizar peticiones sin autorización.
- Apartado “**nets**”: Aquí deberemos indicar a través de cuál de los interfaces de red virtuales enviaremos el “**Magic Paquet**” del WoL. El servidor WoL facilitado siempre utilizará la nomenclatura “**ethX**” (eth0, eth1, eth2, etc...).

Si hemos decidido colocar un servidor WoL por cada una de las redes de los equipos físicos, únicamente utilizaremos el interfaz “**eth0**”. Debemos indicar la subred a la que pertenecen los equipos.



Si en el servidor WoL tenemos diferentes interfaces de red (para utilizar el mismo servidor para varias subredes), deberemos indicar la subred y el interfaz (en el script de ejemplo se indica que en todos los equipos físicos que pertenezcan a la subred: 192.168.11.0/24 y a la subred 192.168.0.0/20, el envío del WoL se realice por el interfaz “eth0”. Todos los equipos que pertenezcan a la subred: 172.27.0.0/20 lo harán por el interfaz “eth1”). Es posible añadir tantas redes (en formato CIDR) e interfaces como sea necesario.

- Apartado “**IFACE**”: Si algunas de las direcciones IP de los equipos físicos sobre los que se quiere enviar el WoL no están definidas en el apartado “**nets**”, se utilizará el interfaz de red indicada en esta variable. Por ejemplo, si se quiere enviar un WoL a la 172.26.0.5 con el script que se proporciona, al no estar definida su red en el apartado “**nets**”, irá por el interfaz “**eth0**”.

Si queremos comprobar manualmente que los servidores WoL funcionan correctamente sobre un equipo específico, podemos usar el siguiente comando:

```
/usr/sbin/etherwake [MAC] -i [INTEFACE] -b
```

Si las conexiones de red son correctas, y la máquina soporta WoL, debería arrancarse al ejecutar este comando.

Si queremos comprobar si el equipo definido desde el broker UDS está recibiendo el WoL y qué datos se están enviando, podemos acceder al siguiente fichero de log del equipo para verificarlo: **/var/log/nginx/access.log**

```
192.168.11.71 - - [24/Mar/2021:17:33:52 +0100] "GET /cgi-bin/etherwake.py?mac=00:24:22:20:E3:C9&secret=simkem0t&ip=192.168.11.19 HTTP/1.1" 200 19 "-" "python-requests/2.25.1"
```

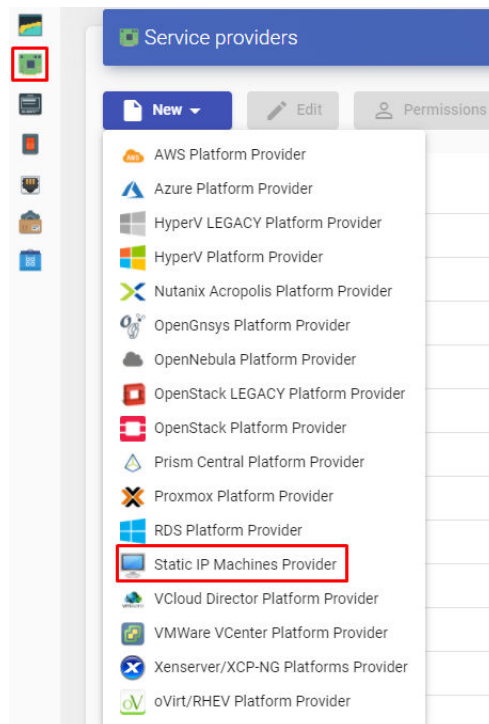
La primera dirección IP corresponderá al servidor desde donde se envía la petición WOL, normalmente el propio servidor UDS (en el ejemplo: 192.168.11.71). Después se indica la ejecución del script de **etherwake** descrito anteriormente, seguido de la dirección MAC del equipo, la cadena “**SECRET**” y la dirección IP del equipo físico a iniciar (en el ejemplo: 192.168.11.19). Los datos de la MAC e IP serán los indicados en la administración de UDS Enterprise.



Administración de UDS Enterprise

Deberemos disponer de los datos de MAC y dirección IP (o nombre dns) de los equipos físicos a los que queramos realizar el envío del WoL. Una vez dispongamos de estos datos, deberemos indicarlos en la administración de UDS Enterprise.

Accederemos a la administración de UDS Enterprise (con un usuario con permisos) y nos situaremos en el apartado “**Services**”. Ahí daremos de alta un nuevo “**Service provider**” de tipo “**Static IP Machine**”:



Indicaremos un nombre descriptivo como nombre del proveedor:

New provider

Main

Advanced

Tags

Tags for this element

Name *

Physical Desktops

Comments

Comments for this element

Test

Discard & close

Save



En la pestaña “**Advanced**” deberemos indicar la opción **[wol]**. Debajo añadiremos las reglas de envío del WoL a los servidores configurados para este propósito.

Ejemplo:

```
[wol]
*=http://xxx.xxx.xxx.xxx/cgi-bin/etherwake.py?mac={MAC}&secret=xxxxxxx&ip={IP}
```

Edit provider

Main **Advanced**

Advanced configuration *

[wol]
*=http://192.168.11.111/cgi-bin/etherwake.py?mac={MAC}&secret=simkem0t&ip={IP}

Test Discard & close Save

El formato de las reglas será el siguiente:

1. Primero indicaremos la subred, rango de red o IP a la que pertenecerán los equipos físicos. Si introducimos un asterisco se incluirán todas.

En el siguiente ejemplo podemos comprobar lo siguiente:

- Todos los equipos que pertenezcan a la subred 192.168.0.0/24 se enviarán al servidor WoL 192.168.11.111
- El equipo con IP 192.168.1.121 se enviará al servidor WoL 192.168.11.112
- Todos los equipos que pertenezcan a la subred 172.27.0.0/20 se enviarán al servidor WoL 192.168.11.113
- El resto de equipos, que no pertenezcan a las subredes o IP indicados antes, se enviarán al servidor WoL 192.168.11.111

Edit provider

Main **Advanced**

Advanced configuration *

[wol]
192.168.0.0/24=http://192.168.11.111/cgi-bin/etherwake.py?mac={MAC}&secret=simkem0t&ip={IP}
192.168.1.121=http://192.168.11.112/cgi-bin/etherwake.py?mac={MAC}&secret=simkem0t&ip={IP}
172.27.0.1/20=http://192.168.11.113/cgi-bin/etherwake.py?mac={MAC}&secret=simkem0t&ip={IP}
*=http://192.168.11.111/cgi-bin/etherwake.py?mac={MAC}&secret=simkem0t&ip={IP}

Test Discard & close Save



UDS Enterprise

Wake on LAN de máquinas físicas con UDS Enterprise 3.5

www.udsenderprise.com

- Una vez definidas las redes a las que pertenecen los equipos físicos, indicaremos los datos de conexión con el servidor WoL que enviará los **"Magic Paquet"**.

En el siguiente ejemplo, se puede ver una configuración para que dependiendo de la IP a la que pertenezca el equipo físico, se le envíe a un servidor WoL concreto.

Edit provider

Main Advanced

Advanced configuration *

```
[wol]
192.168.0.0/24=http://192.168.11.111/cgi-bin/etherwake.py?mac={MAC}&secret=simkem0t&ip={IP}
192.168.1.121=http://192.168.11.112/cgi-bin/etherwake.py?mac={MAC}&secret=simkem0t&ip={IP}
172.27.0.1/20=http://192.168.11.113/cgi-bin/etherwake.py?mac={MAC}&secret=simkem0t&ip={IP}
*=http://192.168.11.111/cgi-bin/etherwake.py?mac={MAC}&secret=simkem0t&ip={IP}
```

- En todas las peticiones de WoL a los servidores, tendremos que enviar la dirección MAC y la dirección IP. UDS Enterprise recoge este dato automáticamente cuando se define el equipo en el servicio base **"Static Multiple IP"** y se envía con las variables: **{MAC}** e **{IP}**.

Edit provider

Main Advanced

Advanced configuration *

```
[wol]
*=http://192.168.11.111/cgi-bin/etherwake.py?mac={MAC}&secret=simkem0t&ip={IP}
```

- Por último deberemos indicar el **"SECRET"**, que será una cadena de caracteres definida en el script (**etherwake.py**) del servidor WoL.

Edit provider

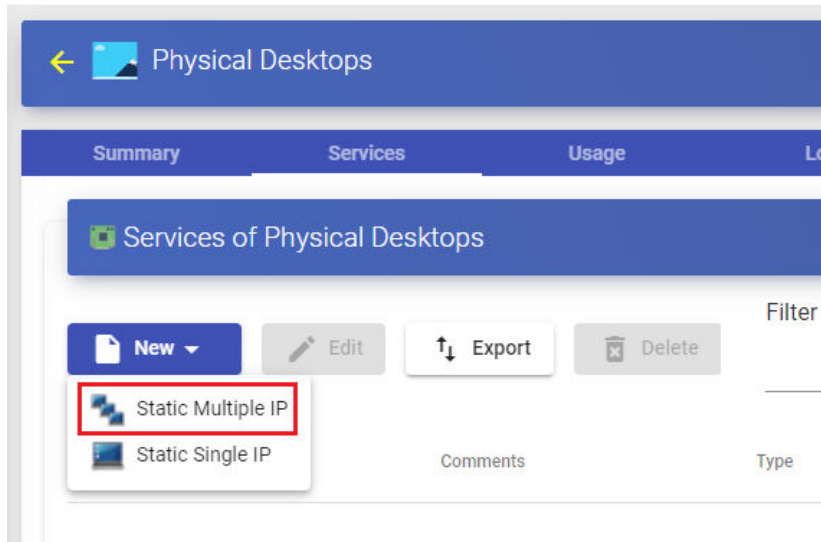
Main Advanced

Advanced configuration *

```
[wol]
*=http://192.168.11.111/cgi-bin/etherwake.py?mac={MAC}&secret=simkem0t&ip={IP}
```

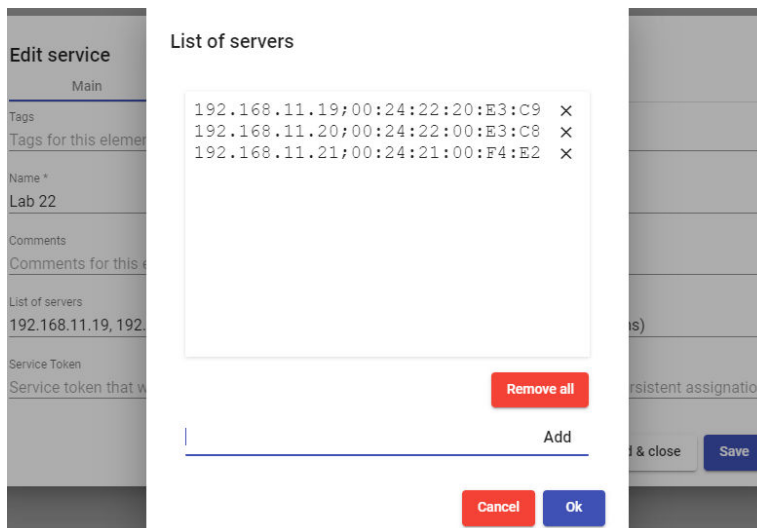


Una vez creado el proveedor de servicios con la configuración de WoL en la pestaña “**Advanced**”, accedemos a él y creamos un nuevo servicio base de tipo “**Static Multiple IP**”:



En este tipo de servicio base, deberemos indicar un nombre identificativo para el servicio. En el apartado “**List of Servers**”, indicaremos las direcciones IP o nombres de los equipos físicos a utilizar. A continuación introduciremos la dirección MAC de la tarjeta del equipo, separada por *punto y coma*. El formato sería:

Direccion_IP;Direccion_MAC





UDS Enterprise

Wake on LAN de máquinas físicas con UDS Enterprise 3.5

www.udsenderprise.com

Si queremos que UDS Enterprise detecte los inicios y cierres de sesión de los usuarios (indispensable si necesitamos que las máquinas se liberen y estén disponibles para otros usuarios), deberemos instalar el actor **“unmanaged”** y podremos utilizar el apartado **“Service Token”**. Si lo que necesitamos es que una máquina esté siempre asignada a un usuario específico, no utilizaremos el **“Service Token”**.

NOTA: Se recomienda utilizar direcciones IPs en lugar de nombres. También es posible usar el nombre DNS de los equipos siempre y cuando exista resolución de nombres tanto desde los servidores de UDS como desde los equipos clientes de conexión que ejecuten conexiones directas. Si utilizamos **“Service Token”**, no es posible utilizar nombres. Solo se soporta el uso de direcciones IP.

NOTA2: Es posible combinar equipos con y sin dirección MAC. A los equipos que no incluyan la dirección, no se les enviará WoL.

En la pestaña **“Advanced”**, es imprescindible que no se compruebe la conexión (es decir, poner **“Check Port”** a cero), puesto que el equipo estará apagado. Tampoco es posible utilizar el valor **“Skip time”**.

Además se podrá configurar un tiempo de sesión máxima por máquina **“Max session per machine”**.

New service

| Main | Advanced |
|------|--|
| | <p>Skip time *</p> <input type="text" value="0"/> |
| | <p>Check Port *</p> <input type="text" value="0"/> |
| | <p>Max session per machine *</p> <input type="text" value="0"/> |
| | <p>Lock machine by external access</p> <input type="checkbox"/> No |

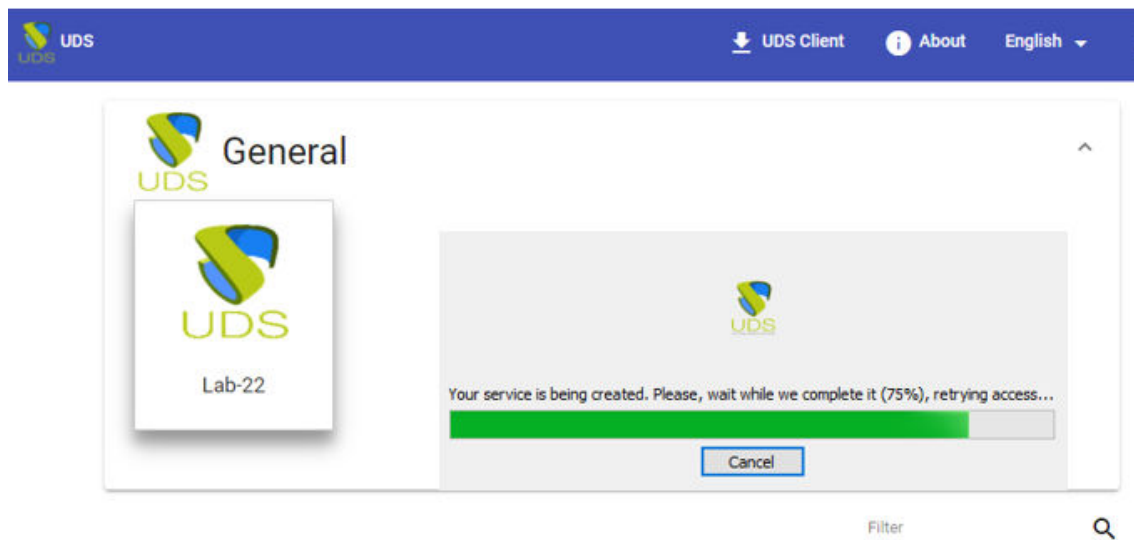
Una vez creado el servicio base de tipo **“Static Multiple IP”** e indicados los equipos a utilizar, ya podremos crear el **“Service Pool”** para el acceso de los usuarios.



Acceso a máquinas

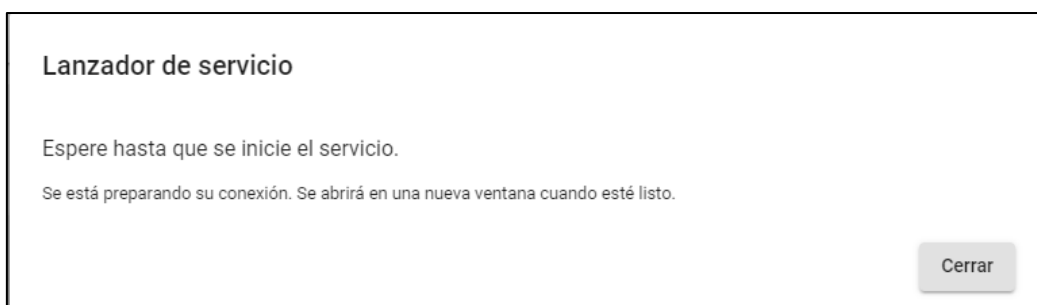
Una vez realizada todas las configuraciones necesarias en los elementos descritos anteriormente y creado el pool de servicios con al menos un grupo de usuarios y un transporte, ya podremos acceder a nuestros equipos físicos.

Cuando realicemos el acceso, el equipo tendrá que iniciarse. Mientras se inicia, en el cuadro de conexiones RDP aparecerá el siguiente aviso:



Una vez iniciado el equipo, UDS Enterprise se conectará automáticamente a él (el tiempo en completar la conexión dependerá de lo que tarde en iniciar el equipo físico y en habilitar el servicio de RDP).

Si estamos usando una conexión de tipo HTML5, el sistema mostrará este aviso:



Una vez lanzada la conexión solo habrá que esperar a que arranque la máquina y esta esté completamente encendida y nos lanzará una nueva pestaña en el navegador.



UDS Enterprise

Wake on LAN de máquinas físicas con UDS Enterprise
3.5

www.udsenderprise.com

Soporte y servicios profesionales

Virtual Cable comercializa UDS Enterprise mediante un modelo de suscripción según el número de usuarios, incluyendo soporte y actualizaciones.

Además, Virtual Cable ofrece servicios profesionales para instalar y configurar UDS Enterprise.

Para más información, visite www.udsenderprise.com o envíenos un email a info@udsenderprise.com