SSH en Windows

Gustavo García2 28/03/2023.

Basado en <https://www.xataka.com/basics/ssh-windows-11-que-como-configurarlo-paso-a-paso>

# Qué es SSH

El SSH o Secure Shell, es un protocolo que sirve para conectar dos ordenadores entre ellos de forma inalámbrica. Para hacerlo, configura un acceso remoto mediante un canal seguro, donde la información viaja cifrada entre ordenadores. Además del protocolo, SSH también es el nombre del programa que lo implementa.

Además de conectar ordenadores e intercambiar archivos, también te permite copiar datos de forma segura desde un ordenador a un cliente externo que se haya conectado utilizando claves RSA, que son claves más seguras que las contraseñas de inicio de sesión, o simular sesiones FTP cifradas para poder intercambiarlos.

# OpenSSH

Esta es una implementación muy popular. Por ejemplo, viene por defecto en la instalación de Windows. Hay varias aplicaciones que la instalan, porque la necesitan. Pasa que en general no avisan, o no piden permiso, o no lo hacen con claridad. De modo que uno puede terminar con más de una instalación en su PC, sin saber cómo.

# Cliente y servidor

El protocolo necesita un cliente y un servidor. El cliente le solicita al servidor una conexión. Para que la conexión funcione, necesitamos hacer configuraciones, tanto en el servidor como en el cliente.

El servidor, en nuestro caso, será el sitio web de GitHub, donde están alojados nuestros repositorios. En el servidor necesitamos demostrar que nosotros somos quienes decimos ser. Esto lo hacemos por medio de usuario y password. Y necesitamos ponernos de acuerdo en las credenciales con las que nos vamos a identificar en adelante. Para esto subimos una clave SSH,

El cliente es la PC (local) que se conecta al servidor. En el cliente (nuestra PC local) necesitamos crear una clave SSH. Esta clave SSH nos sirve para identificarnos, sin tener que estar poniendo cada vez usuario y password. La subimos una vez al servidor, y nos identificamos con usuario y password. Pero solo la primera vez. De ahí en más, es automático.

# Cómo configurar SHH en Windows 11

De forma predeterminada, el cliente OpenSSH estará ubicado en el directorio:

C:\Windows\System32\OpenSSH

También puede verificar que esté instalado en:

Configuración de Windows> Aplicaciones> Funciones opcionales

Luego busque "OpenSSH" en sus funciones instaladas.

Tecla de Windos. Escribir powersh. Aparece en el menú de inicio la aplicación Windows PowerShell. Ejecutar como Administrador. Esto es lo que se llama una sesión elevada de PowerShell. Tipear

$PSVersionTable PSVersion

y Enter. Aparecerá algo como:

Major Minor Build Revision

----- ----- ----- --------

5 1 22621 963

Tipear

winver.exe

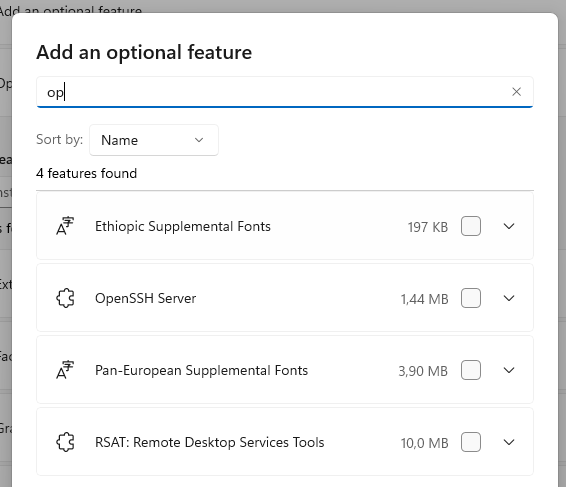
y Enter. Aparecerá algo como

Ejecutar el comando:

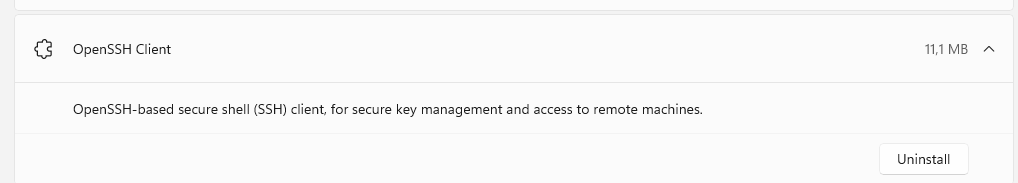
(New-Object Security.Principal.WindowsPrincipal([Security.Principal.WindowsIdentity]::GetCurrent())).IsInRole([Security.Principal.WindowsBuiltInRole]::Administrator)

Aparecerá True, si la cuenta en la que estás loggeado pertenece al grupo de Administrators.

Abrir la aplicación de ajustes de Windows. En el panel izquierdo buscar aplicaciones, características opcionales. En el panel de la derecha buscar SSH. Hay dos entradas posibles para OpenSSH: el servidor y el cliente.

En mi PC, OpenSSh Server está como una característica opcional, pero no está instalado de hecho. Esto es correcto. Este servidor, si está corriendo y correctamente configurado, me permitiría conectarme a mi PC local desde una PC remota. Eso no me interesa. Por eso no lo instalo.

El cliente, por el contrario, está instalado y se ejecuta con el inicio de Windows.



Si no está instalado, hay que instalarlo activando la casilla correspondiente.

Apretar tecla de Windows. Escribir servic. Aparecerá la aplicación de servicios. Ejecutarla. En el panel de detalles buscar OpenSSH Client. Doble click. En la solapa General, en el tipo de inicio, seleccionar Automático. Hecho lo anterior, apretar Start para iniciar inmediatamente el servicio.

**Nota**

La instalación de OpenSSH Server creará y habilitará una regla de firewall llamada OpenSSH-Server-In-TCP. Esto permite el tráfico SSH entrante en el puerto 22. Si esta regla no está habilitada y este puerto no está abierto, las conexiones se rechazarán o se restablecerán.

Para iniciar OpenSSH Client, tipear start-ssh-agent en la consola de Windows. Aparecerá algo como:

Removing old ssh-agent sockets

Starting ssh-agent: done

Identity added: /c/Users/Xxxxxxx/.ssh/id\_rsa (xxxxxx@gmail.com)