Departameto de informatica y Comunicaciones
Administración de Sistemas Operativos (ASO)

IES Las Fuentezuelas
Jaén

Ciclo formativo de Grado Superior

ADMINISTRACIÓN DE SISTEMAS INFORMÁTICOS EN RED

Tema 5: Administración remota del sistema

Navarrete Secaduras, Jorge
Martínez Chacón, Emilio José
Bueno Castro, Jesús

Curso 2021-2022

Contenidos:

1. Introducción

Como administradores de sistemas, trabajamos día a día remotamente sobre máquinas o servidores, sean Windows o Linux, por lo que es uno de los aspectos que debemos controlar y manejar sin problema alguno. En esta documentación se tratará de forma general el acceso remoto a sistemas, los protocolos usados, las herramientas que nos podemos encontrar, y por último nos centraremos en Windows Server 2012 R2.

2. Administración remota del sistema

a. Definición

En lugar de acceder a la configuración de nuestro servidor físicamente, teniendo que desplazarnos hasta las instalaciones seguras donde debería encontrarse y entrar en ellas, los administradores de sistemas solemos trabajar de forma remota. Es en ese caso, cuando un sistema permite su acceso remoto desde otro equipo cliente, y desde él podemos configurar y mantener sus servicios desde aplicaciones de administración, sea de forma gráfica o no, cuando nos referimos a la Administración remota del sistema.

Figura 1: Esquema de conexión remota

b. Ventajas de la administración remota

- Poder realizar mantenimiento preventivo y correctivo a distancia.
- Hacer copias de seguridad de la información a otro PC.
- Transferencia de archivos.
- Más barato que una administración física.
- Brindar ayuda sin necesidad de esperar horas o días para que el técnico se desplace.

c. Desventajas de la administración remota

- Si se pierde la conexión, obviamente perdemos el acceso remoto.
- En caso de una filtración de credenciales de usuarios con privilegios, se podría acceder al servidor sin autorización.
- La administración remota sólo es efectiva en caso de la existencia de conexión a una red, si esta falla o no existe, no se podría realizar.
- Si nos conectamos de forma no segura (sin cifrado) la información entre los 2 hosts podrá ser accesible por cualquier que intercepte los paquetes que viajan en la red.
- Aún con cifrado, nuestro sistema puede verse expuesto ante un atacante.

d. La administración remota en las empresas

Figura 2: Logo Tripp Lite

A día de hoy la administración remota nos la podremos encontrar en cualquier situación, pero por especificar un caso real, esta empresa incorpora soluciones de **administración remota** en sus **equipos, servidores y sistemas de respaldo**.

Esto permite administrar sucursales ubicadas en distintas localidades, algunas muy distantes entre sí; rentabilizando al máximo la operación de la compañía.

Además de disminuir costes y mejorar el tiempo de respuesta al no requerir personal especializado en cada sucursal, ni tener que esperar la llegada de un técnico en caso de fallar las soluciones de **administración remota** de los equipos, permiten a los administradores responder de manera inmediata ante cualquier contingencia. Los sistemas de este tipo, tienen la capacidad de encender o apagar vía remota cada contacto, y de notificar los niveles de carga y consumo de los equipos.

En los UPS (sistemas de respaldo de energía eléctrica), la **administración remota** permite apagar y encender los dispositivos conectados a la red. Esto es especialmente útil durante un corte de energía, para mantener encendidos únicamente los dispositivos críticos como el servidor principal o el enlace de internet. Estos sistemas además envían alertas sobre voltaje, batería, temperatura, humedad y alarmas de incendio.

Asimismo, estos sistemas permiten controlar y administrar **servidores**, **equipos** o **Workstations** con una conexión IP segura.

3. Protocolos para acceso remoto

a. Telnet

Como sabemos, el protocolo Telnet proporciona un método estándar para que dos dispositivos intercambien información a través de sus terminales.

De por sí, el protocolo proporciona una serie de reglas básicas que permiten vincular el sistema cliente al sistema servidor mediante un intérprete de comandos, esto lo hace mediante una conexión TCP para enviar los datos en formato ASCII codificados en 8 bits, con orientación bidireccional, y con un aspecto muy importante: Sin ningún tipo de cifrado.

Es por esta característica por la que no es recomendable usar nunca Telnet, menos aún teniendo otras opciones como las que se expondrán a continuación. Incluso en una red privada, un intruso en la red con un sniffer podría analizar toda la información comunicada a través del Telnet.

El puerto 23 es el asignado a este protocolo por defecto, y a través de él se transmitirán esos datos en el flujo TCP. Los susodichos datos, además, deben agruparse en un buffer antes de enviarse, y hasta que no se transmite el byte 255, el receptor no interpreta el comando. Por ello, al byte 255 se le denomina IAC (Interpretar como comando).

Aunque sea inseguro y actualmente no lo usemos, cuando surgió Internet fue útil gracias a que el protocolo Telnet permite a cualquier host comunicarse con otro sin conocer sus características, por muy diferentes que sean entre sí, gracias a unas reglas sencillas de control y de estado.

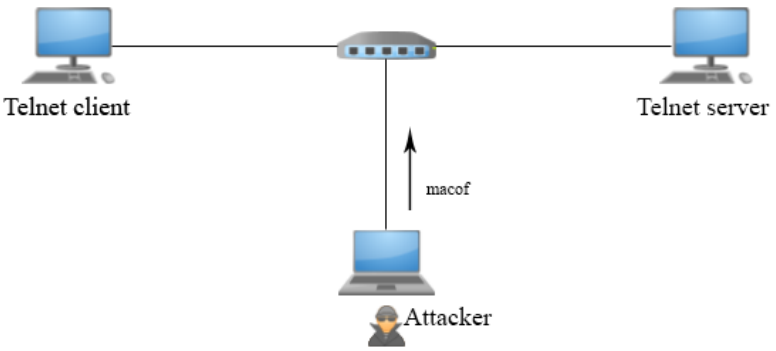

Figura 3: Esquema de conexión Telnet comprometida.

b. SSH

Debido a los enormes problemas de seguridad que conlleva usar Telnet y que, en caso de que como administradores creemos una conexión Telnet con el servidor, comprometeremos gravemente el sistema, SSH o Secure Shell es su alternativa segura.

Siguiendo el mismo concepto, este protocolo proporciona una autenticación segura, y, por supuesto, implementa técnicas criptográficas que hacen más complicado que un individuo pueda comprometer nuestro sistema, ya que las comunicaciones se transfieren de manera encriptada a 128 bits.

Su funcionamiento se basa en que, una vez se lanza en el sistema cliente la petición de abrir una conexión de Secure Shell, dependiendo del sistema de cifrado el proceso será de una forma u otra.

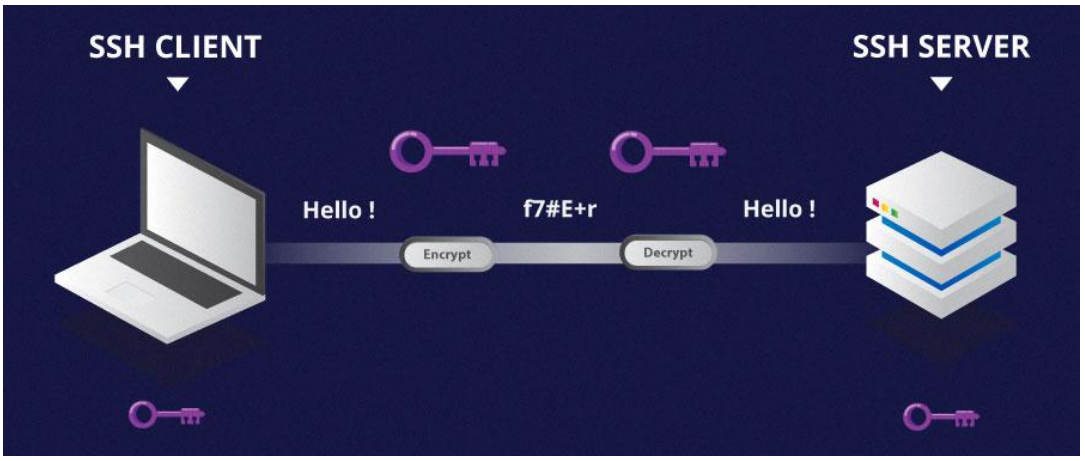

Figura 4: SSH con clave simétrica.

Con un **cifrado simétrico**, se utiliza una llave o clave secreta tanto para el cifrado como para el descifrado. Cliente y servidor deben tener esta clave y es por ello que se conoce como “shared key”.

Esa clave simétrica y compartida se lleva a cabo mediante un algoritmo de intercambio de claves, esto proporciona un método mediante el cual la clave nunca se transmite entre ellos para evitar ser interceptada, sino que los equipos comparten datos públicos y los manipulan de forma independiente para calcular la clave; aunque se intercepten esos datos públicos, otra máquina intrusa no tendrá fácil el cálculo de la clave, ya que no conocerá el algoritmo. Así mismo, también se usará un código de cifrado u otro según ambas máquinas (AES 128, CAST 128, Blowfish...).

Por otro lado, con un **cifrado asimétrico**, se usan dos claves diferentes. Una clave pública y otra privada; una forma muy popular de explicarlo es compararlo con la situación de tener un candado y una llave: El candado es la clave pública, y puede estar en cualquier lado, ya que solo nuestra llave privada lo podrá abrir.

Por obvias razones de seguridad, por tanto, no es posible calcular la clave privada a partir de conocer la pública, y la relación entre ambas es muy compleja, siendo muy complicado descifrar la clave pública sin conocer en su totalidad la clave privada.

Estas claves únicamente se utilizan durante el algoritmo de intercambio de claves, es decir esas claves no son las que cifran toda la comunicación SSH. Antes de comenzar la sesión SSH, se generan otro par de claves para producir la clave secreta de la comunicación.

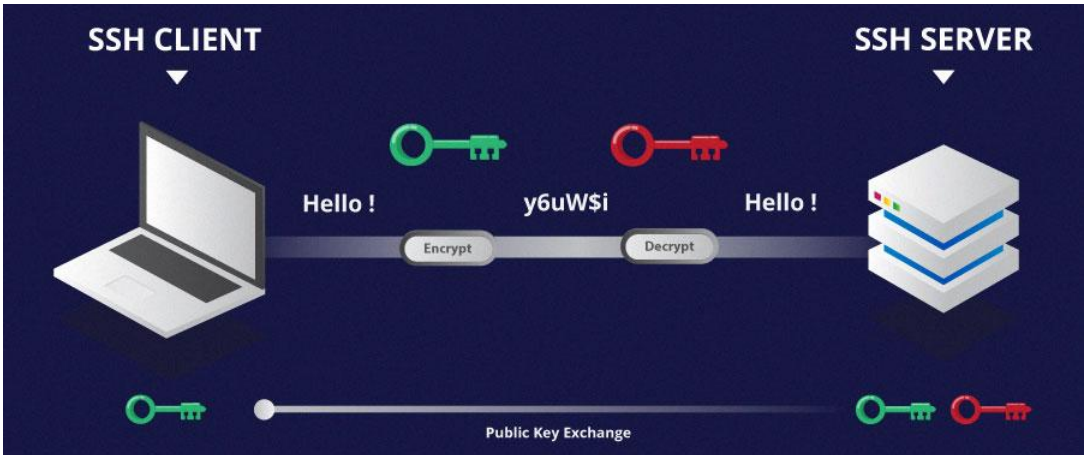

Figura 5: SSH con clave asimétrica.

En este cifrado, el sistema queda comprometido si la clave privada queda expuesta, por lo que los errores humanos, la seguridad física que tenga el equipo con la clave privada a su alrededor etc. son puntos críticos.

Por último, también existe el **hashing unidireccional** en SSH. A partir de una entrada, se genera un valor de una longitud fija (un hash), pero es imposible que al recibir un hash se pueda generar la entrada con la que se generó.

Esto en SSH se usa para verificar la autenticidad de los mensajes, ya que si un cliente tiene la entrada correcta, podrá generar un hash y comprar su valor con el recibido, para verificar la conexión segura.

c. RDP

El protocolo RDP (Protocolo de escritorio remoto) está desarrollado por **Microsoft**, y se encuentra bajo su propiedad. Se basa en los estándares de protocolo T.120, y permite crear canales virtuales independientes cifrados para intercambiar datos. Por defecto se usará el puerto **TCP 3389** para esta conexión.

La comunicación se da a través de la ejecución entre una terminal que muestra la información procesada recibida desde el servidor, y un servidor que recibe la información del cliente mediante los datos que provienen de su teclado y ratón.

Esto se consigue gracias a que, por un lado la información gráfica que genera el servidor, es convertido a un formato propio del protocolo RDP y se envía a través de la red hasta la terminal o cliente, la cual debe interpretar esa información para reconstruir la imagen que mostrará en su pantalla; y, por el otro lado, lo que se haga desde el terminal (teclas pulsadas o movimientos y clicks del ratón) se cifrará y se transmitirá también mediante la red hasta el servidor.

Es destacable comentar, que, aunque Microsoft comente que los datos están “altamente cifrados”, para pentesters reconocidos no es así.

El problema es que es más sencillo para un hacker interceptar información, ya que según pentesters y hackers éticos de la comunidad, **el protocolo RDP expone las conexiones rápidamente**, y mediante buscadores como *Shodan* los atacantes pueden encontrar nuestros sistemas con conexiones RDP abiertas.

Mediante un estudio de *Blumira* con honeypots de servidores con una comunicación RDP, en 5 meses detectaron 1,5 millones de ataques sobre ellos, entre escaneos abusivos e intentos de fuerza bruta; y si consiguen entrar en nuestro sistema a través de este protocolo, lo mínimo que ocurrirá es que tendremos un ransomware como invitado.

Es por ello por lo que **nunca hay que usar RDP a través de Internet**, y aún estando en una VPN con un cifrado decente, será vulnerable hasta que no se configure adecuadamente el NLA (Network Level Authentication) y con 2FA. Es también aconsejable limitar el número de usuarios que puedan acceder mediante RDP a nuestro servidor, así como limitar solo a que ciertas direcciones IP puedan ganar acceso.

d. SOAP

El protocolo simple de acceso a objetos, es un estándar que define cómo dos objetos en diferentes procesos pueden comunicarse datos XML. Es usado sobre todo para implementar servicios web, y se transporta fácilmente a través de HTTP, SMTP o FTP, sin gran importancia para la administración remota o para la comunicación entre servidor y cliente, lo que nos interesa es que en él se basa el WS-Management.

e. WS-Management

Este es un protocolo estándar para la comunicación entre un terminal y un servidor, con el objetivo de su administración remota, siendo multiplataforma y distribuida a través de HTTP y HTTPS, es por ello por lo que se basa en el protocolo mencionado anteriormente.

El protocolo hace uso de un URI, es decir, de un identificador de un recurso específico de una red. La diferencia entre este y una simple URL, es que el recurso al que hace referencia una URL puede variar en el tiempo.

Ese URI identifica un elemento de administración (nuestro servidor), y se le suman unos selectores para identificar una instancia concreta de ese elemento a configurar. El protocolo también cifra levemente la comunicación tras la autenticación inicial, independientemente de si utiliza HTTP o HTTPS.

f. RFB

Por último, entre los protocolos más destacados, el protocolo “Remote Frame Buffer” permite el acceso remoto a interfaces gráficas. A bajo nivel, funcionaba desde el Frame Buffer, que en los inicios de este protocolo, eran los dispositivos que almacenaban la representación de cada uno de los píxeles de la pantalla antes de ser enviados al dispositivo de visualización; hoy en día es obvio que las tarjetas gráficas no funcionan así, ya que han pasado 30 años, pero el concepto sigue siendo que lo que se transmite es la representación de la imagen de la pantalla (en píxeles) del servidor al cliente, siendo esta una gran diferencia con RDP.

Como es de esperar, el nivel de seguridad es muy bajo usando este protocolo, y además, no es lo suficientemente rápido como para ser una opción viable hoy en día.

g. Otros

Aunque no será relevante para nosotros como administradores de un sistema con un Windows Server, Google desarrolló su propio protocolo Chromoting para que los dispositivos con Chrome OS tengan la aplicación Chrome Remote Desktop, siendo muy similar a RDP; y, así mismo, Apple modificó el protocolo RFB con funcionalidades adicionales y seguridad y usabilidad mejoradas para crear Apple Remote Desktop (ARD).

4. Herramientas de Microsoft

a. RSAT

Las herramientas de administración remota del servidor, conocidas como RSAT, nos aportan una posibilidad para mantener y configurar Windows Server desde otro equipo cliente con Windows, iniciando sesión por supuesto como administrador.

Según lo deseado, con el rol activo en Windows Server y con RSAT configurado también en el cliente, tendremos la posibilidad de administrar el servidor mediante consola o mediante la propia interfaz gráfica.

Esta suite usa los protocolos de WS-Man y RDP, pero en un conjunto de herramientas que nos permiten seleccionar la forma de administración deseada.

b. Escritorio Remoto

La aplicación de Escritorio Remoto de Microsoft es una herramienta que nos permite administrar y controlar un equipo desde otro gráficamente, usando el propio protocolo RDP (Remote Desktop Protocol).

RSAT incluye las funciones de este protocolo, pero la propia aplicación tiene como objetivo su uso en los equipos personales, más que los servidores, aunque perfectamente se puede usar para ello.

Actualmente, de hecho, Escritorio Remoto permite que dispositivos con Android e iOS, también puedan conectarse. A pesar de que, por tanto, es una herramienta destinada más bien a los usuarios de Windows, también puede ser una de las opciones que encontraremos en las empresas para la administración de un servidor.

c. WinRM (WS-Man)

Desde la suite de RSAT podemos usar también la administración remota desde Powershell, y esto lo consigue usando WinRM; aunque, al igual que en el caso anterior, también se puede usar por sí misma.

La herramienta es una implementación de Microsoft del protocolo WS-Management, por lo que no es una de las opciones más seguras ni novedosas que tenemos para administrar nuestro servidor, aunque sí fue muy usada en Windows Server 2008.

Al igual que con RSAT, es algo que también hay que habilitar en el equipo cliente que va a administrar el servidor, esto se consigue con el comando "*winrm quickconfig*" desde el **Powershell**; tras su ejecución, se iniciará el servicio, se configurará para que se inicie automáticamente, creará una escucha que acepta solicitudes de cualquier IP, y habilitará las excepciones en el firewall para el tráfico de WS-Man.

Una vez se haya conseguido esa configuración inicial, desde el Powershell y siempre con el comando "*winrm*" inicial, seguido de las opciones principales (get, put, enumeration o invoke) podremos administrar nuestro servidor eso sí, siempre mediante comandos y sin interfaz gráfica.

d. MMC

MMC son las siglas de "Microsoft Management Console", se implementó en Windows 2000, y permite crear, guardar y abrir consolas de administración de hardware, software y red de un sistema Windows.

Debido a las herramientas actuales, a que su seguridad no es la mejor, y que tiene muchas limitaciones, no es una opción muy usada en la actualidad, concretamente desde Windows Server 2003 no la solemos encontrar.

5. Herramientas de terceros

a. VNC Viewer

Web descarga

VNC es un programa que permite tomar el control del ordenador servidor remotamente a través de un cliente multiplataforma. Una vez instalado VNC en el ordenador, es posible acceder a él desde cualquier parte del mundo a través de Internet y desde cualquier dispositivo, como ordenadores o smartphones.

El funcionamiento de VNC a través del protocolo RFB consiste en enviar pequeños rectángulos hacia el dispositivo cliente formando la pantalla que veremos en él.

El método más usado es enviar los datos de los píxeles en orden de izquierda a derecha y una vez formada la pantalla, solo enviar los datos de píxeles que se han modificado. Esto es útil si no vamos a cambiar de pantalla constantemente, de lo contrario requeriría el reenvío completo de la pantalla nuevamente. Con esto conseguimos ahorro en el ancho de banda.

VNC Viewer está disponible para Windows, MacOs, Linux, Raspberry Pi, iOS, Android, Solaris, HP-UX. En Windows no es posible conectar a un escritorio virtual, pero si el servidor lo ejecutamos en un PC con Linux, es posible conectarse a este.

Su objetivo principal es proporcionar la plataforma para realizar presentaciones a distancia o realizar configuraciones en equipos remotamente, esto lo consigue realizando conexiones seguras a través del uso de encriptación de sesión AES de 256 bits, contando además con Control de acceso y Permisos de sesión.

En cuanto a sus precios, disponemos de una prueba gratuita, aunque sus licencias son todas de pago:

Versión	Por dispositivo	Soporte Instantáneo
Professional	2.79€	13.99€
Enterprise	3.99€	27.99€

b. Putty

Web descarga

Putty es un cliente con el que nos podremos conectar a servidores de forma remota a través de conexiones SSH y Telnet.

La principal característica de Putty es que es un software de control a distancia que tendremos que operar en forma de terminal, es decir, se conecta al terminal del servidor, no dispondremos de interfaz gráfica

Putty es compatible tanto para Windows como para Linux, siendo además un software libre y totalmente gratuito. Permite conectarse remotamente a servidores o dispositivos como routers o switches para configurarlos de forma rápida y efectiva.

Al tener la posibilidad de conectarnos mediante SSH, nos encontramos ante una conexión segura gracias a su conexión de cifrado extremo a extremo.

c. Team Viewer

Web descarga

TeamViewer es un programa que permite el acceso remoto rápido y seguro a ordenadores y redes, con el que los usuarios pueden controlar un equipo desde cualquier terminal de escritorio o dispositivo móvil sin necesidad de tener acceso físico a él.

Este es un software que nos permite conectarnos a la interfaz gráfica del dispositivo para su uso a distancia y para llevar a cabo tareas de mantenimiento y configuración de los equipos.

Este software utiliza el protocolo RDP para realizar las conexiones de forma segura y estable, es compatible con Windows, Mac, Linux, Chrome OS, Raspberry Pi, Android e iOS, y presenta una versión gratuita pero viene muy limitada en sus funciones y no se permite su uso profesional o comercial, por ello, tiene varias licencias entre sus opciones de compra:

Versión	Característica	Precio
Usuario único	1 usuario/1 conexión	29.90€
Multiusuario	15 usuarios/1 conexión	59.90€
Para equipos	30 usuarios/ 10 conexiones	129.90€

d. AnyDesk

Web descarga

AnyDesk es una aplicación de control remoto con la que podremos controlar un dispositivo conectado desde otro. Nos encontramos ante una aplicación que nos permite realizar la conexión de forma gráfica.

AnyDesk es compatible con Windows, Mac, Linux, FreeBSD, Chrome OS, Raspberry Pi, Android e iOS, y permite una conexión de forma rápida y sencilla a equipos para poder administrarlos a distancia, conectándose mediante conexiones con cifrado TLS 1.2 y RSA 2048.

Presenta una subscripción gratuita para usuarios individuales que nos permite realizar una única conexión y dos subscripciones de pago para empresas:

Versión	**Precio**
Essentials	9.99€ / mes
Performance	19.99€/mes/usuario

e. OpenSSH

Web Descarga

Figura 10: Logo de OpenSSH

OpenSSH (Open Secure Shell) es un conjunto de aplicaciones que permiten realizar comunicaciones cifradas entre dispositivos a través de una red, usando los protocolos SSH, scp y sftp.

Este método nos permite conectarnos a la consola del servidor para realizar la configuración a través de línea de comandos, aunque es únicamente compatible con dispositivos Windows y Linux, eso sí, es una herramienta de software libre y totalmente gratuita, siendo así una buena opción para la administración de servidores y dispositivos a través de línea de comandos.

f. Tabla comparativa

Con el objetivo de resumir esta información y poder analizarla visualmente, se ha realizado esta pequeña tabla comparativa:

App	Protocolo	Encriptación	Precio uso profesional	Multimedia [2] y funciones
VNC Viewer	RFB	AES 256	2,79€/mes por dispositivo	4 / 5 (Sin grabación)
PuTTy	SSH / Telnet	Base de protocolo	Gratis	1 / 5 (Solo copiar y pegar)
Team Viewer	RDP	AES 256	29,99€/mes por dispositivo [1]	5 / 5 (Todas)
AnyDesk	TLS 1.2	Base de protocolo	9,99/mes por dispositivo [1]	5 / 5 (Todas)
OpenSSH	SSH	Base de protocolo	Gratis	1 / 5 (Solo copiar y pegar)
Remote Desktop *(Microsoft)	RDP	Base de protocolo (56 o 128 bits)	Gratis e instalado en Windows [2]	2 / 5 (Solo audio y copiar y pegar)

- 1: Por dispositivo gestionado con acceso individual a él, solo uso empresarial.
- 2: En Windows 10 no está soportado en versiones Home.
- 3: Se juzgan 5 características: Arrastrar y soltar, transferencia de archivos, copiar y pegar, grabación de sesión y soporte de audio.

6. RSAT en Windows Server 2012 R2

a. Configuración del servidor.

Para poder usar RSAT y administrar nuestro servidor con sus herramientas, primero debemos agregar el correspondiente rol. Como sabemos, para ello, seleccionamos “Agregar roles y características” desde el menú desplegable que se nos abre desde “Administrar”.

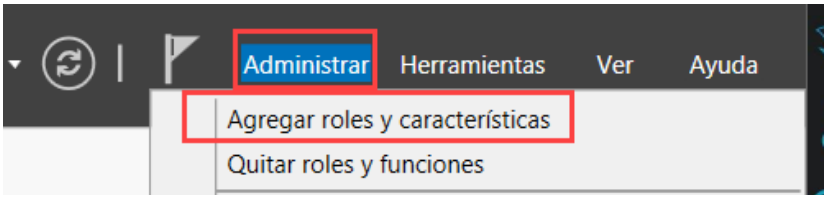

Figura 11: Administrar - Agregar roles y características.

Una vez se nos haya abierto el asistente para agregar roles y características, indicaremos que deseamos hacer una instalación basada en ello.

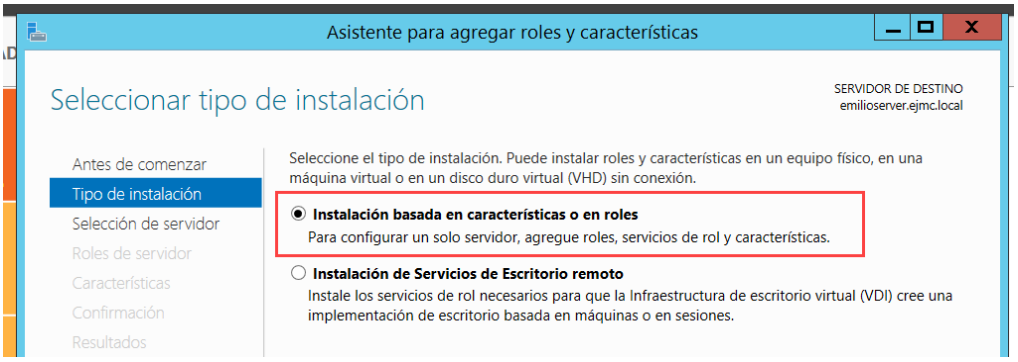

Figura 12: Indicar instalación basada en roles.

En la ventana posterior, seleccionamos nuestro servidor, y acto seguido indicamos que el rol deseado es el de Acceso Remoto.

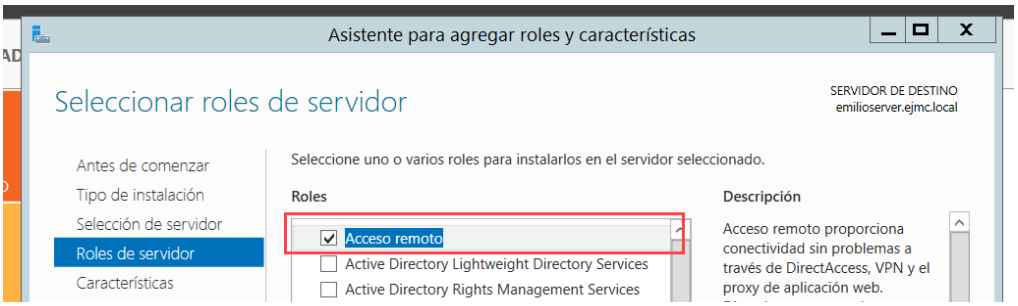

Figura 13: Agregar rol de acceso remoto.

Entre las características que se necesitan instalar para el rol dado, podemos encontrar las Herramientas de Administración Remota del Servidor, las cuales se nos seleccionarán automáticamente.

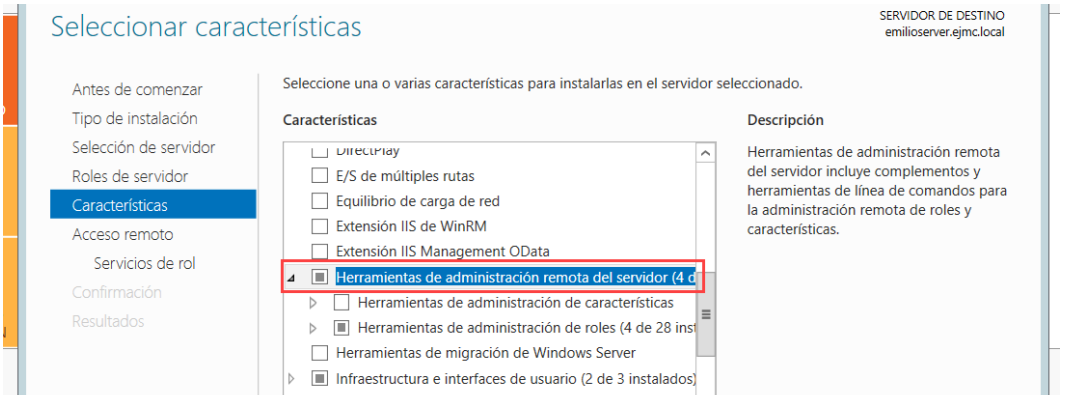

Figura 14: Características del rol.

Seguidamente, debemos elegir los servicios de rol que deseamos instalar según el acceso del equipo cliente a la conexión que permite la administración del servidor. Es decir, tanto como si deseamos que los administradores puedan acceder remotamente al servidor mediante una VPN, o mediante la propia red local o por medio de Internet con DirectAccess (permite un acceso seguro y privado sin necesidad de VPN), seleccionamos la opción de la imagen.

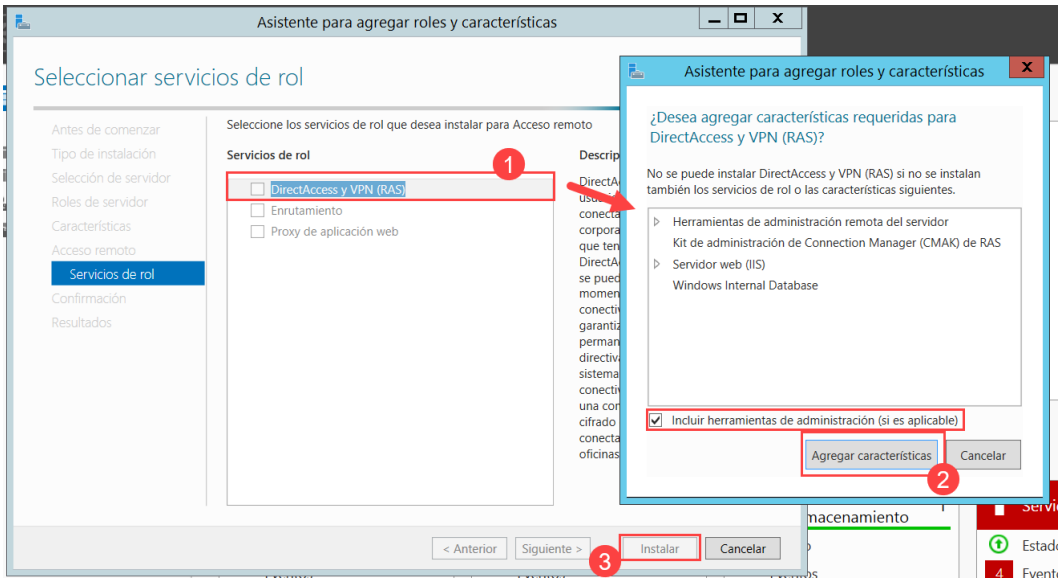

Figura 15: DirectAccess.

Además, el asistente nos pedirá instalar también el rol de servidor web, ya que es necesario para compartir información a través de Internet o de una intranet con seguridad. Una vez haya terminado, la configuración en el servidor para usar RSAT estará completa.

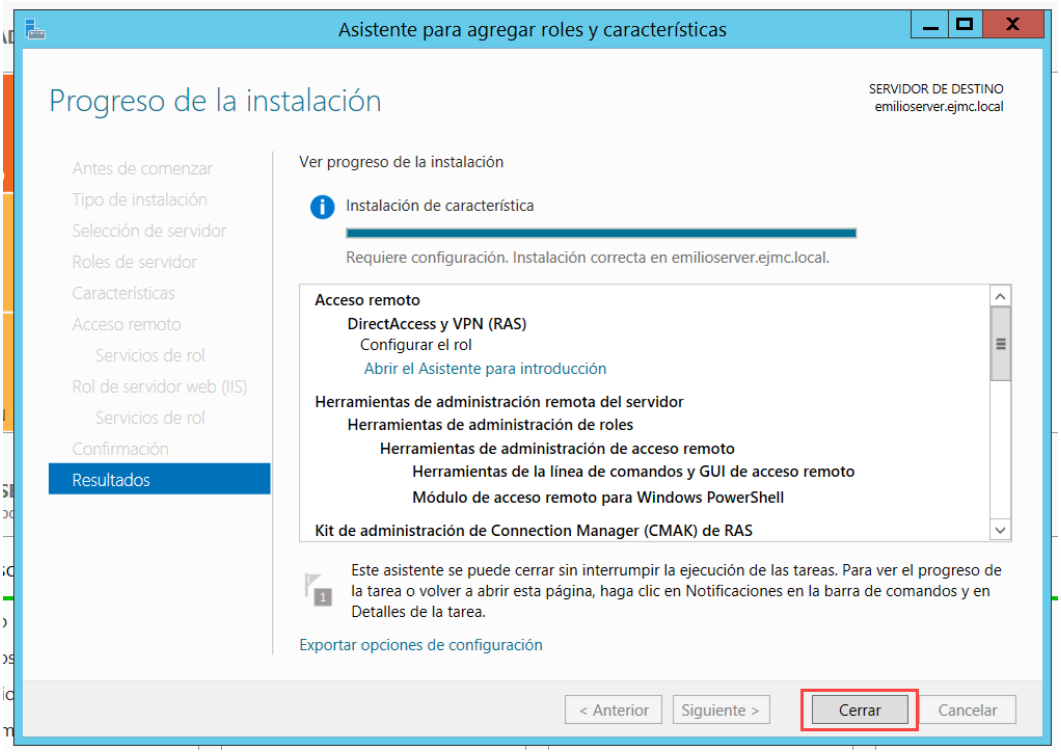

Figura 16: Finalización de instalación de rol.

b. Configuración del cliente.

Desde hace años ya no hace falta descargar RSAT, sino que hay que activarlo desde el menú de características opcionales de Windows 10, esto lo debemos hacer con la sesión iniciada como Administrador del dominio.

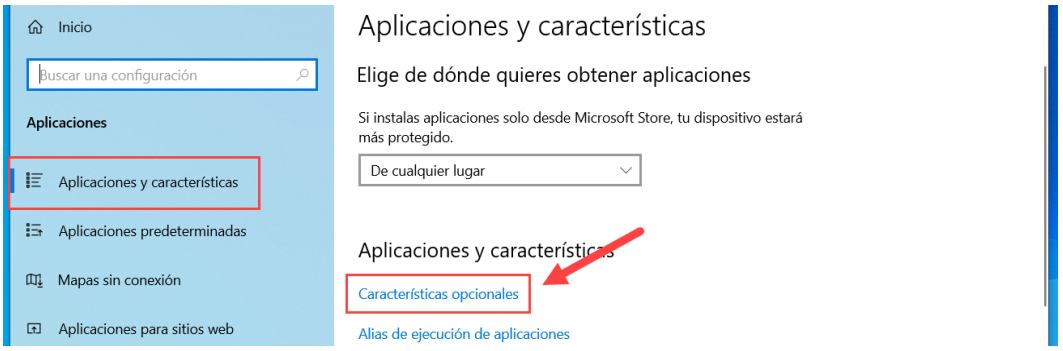

Figura 17: Agregar características opcionales.

Haciendo click sobre “Agregar una característica”, buscaremos “RSAT” y seleccionaremos para instalar la primera opción y la más general. Esta será la opción que nos ofrecerá acceso total a la ventana de Administrador del Servidor de Windows Server 2012 R2. En caso de únicamente querer administrar el servidor DHCP, DNS o cualquier otro, podemos instalar esas herramientas concretas en lugar de la completa.

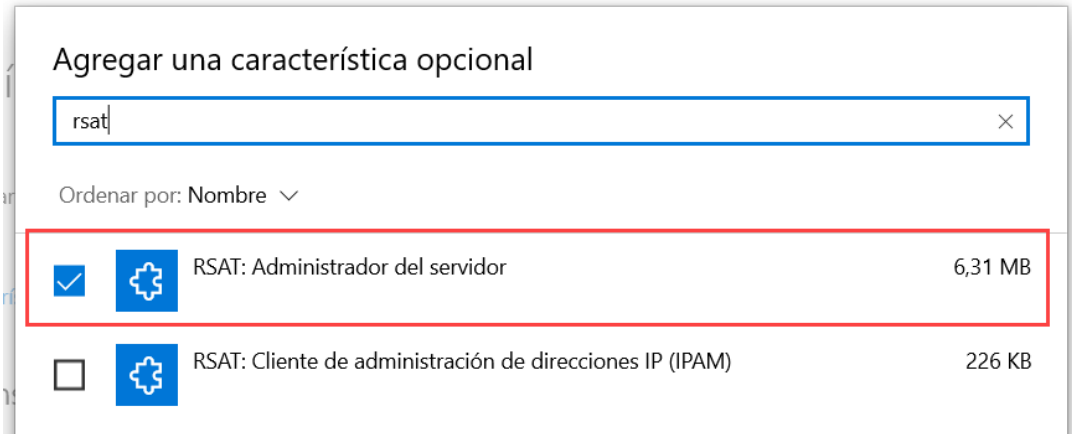

Figura 19: Agregar característica RSAT.

Con esta característica instalada, podemos ejecutarla como administrador para acceder a la ventana de Administración.

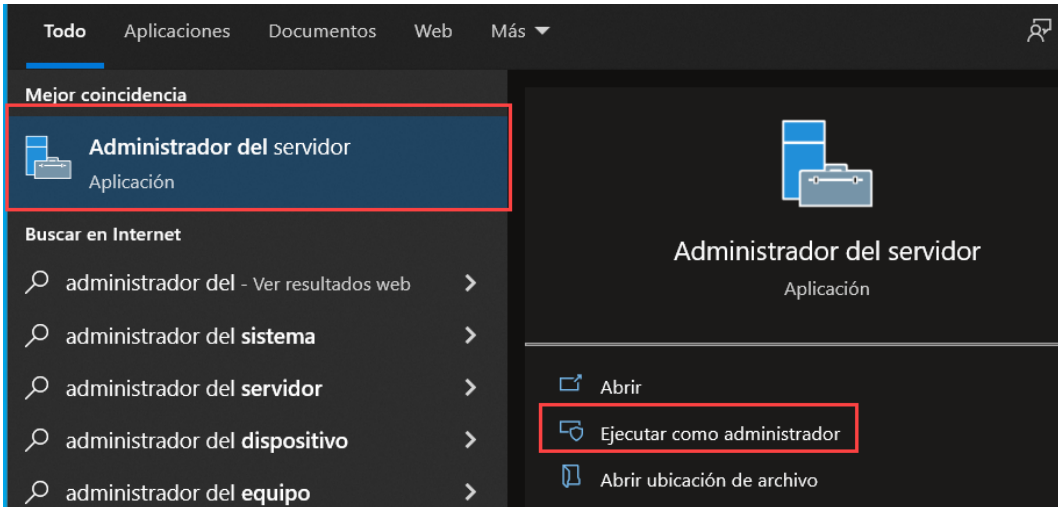

Figura 20: Ejecución Administrador del servidor.

Aunque antes de poder llegar hasta la configuración de nuestro servidor, debemos agregarlo. Para ello seleccionamos “Agregar servidores” desde el menú desplegable de “Administrar”.

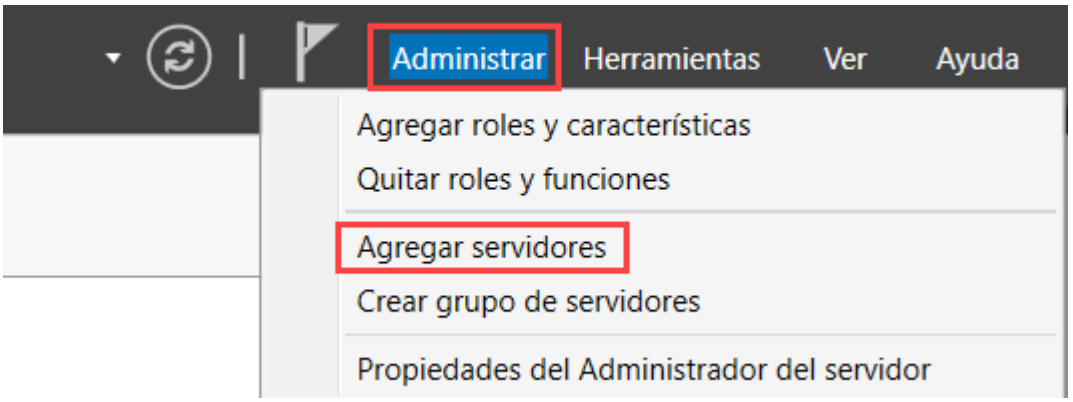

Figura 21: Agregar servidor.

Una vez seleccionado el servidor (que es el único que nos aparecerá en nuestro dominio), ya podremos administrarlo mediante RSAT sin problemas.

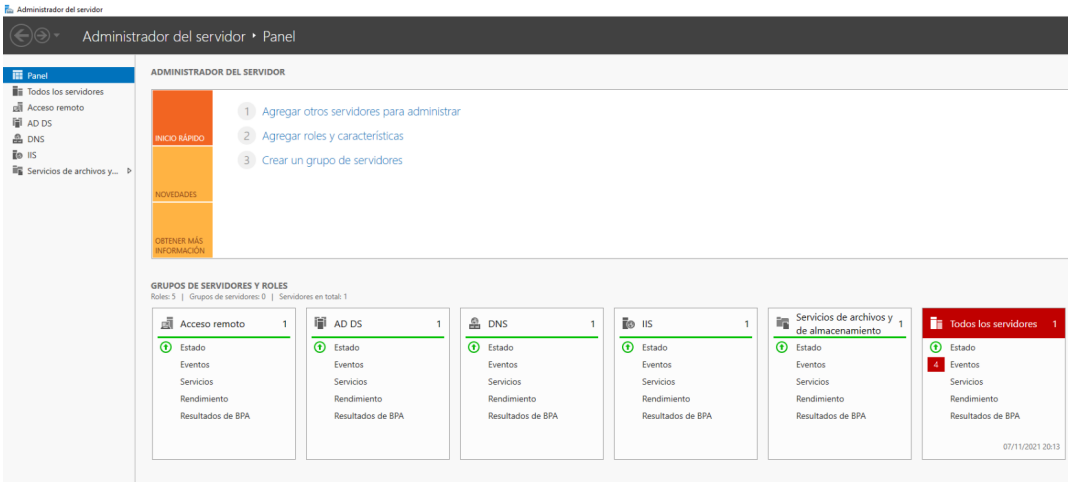

Figura 22: Administrador servidor mediante RSAT.

7. Escritorio Remoto en Windows Server 2012 R2

a. Configuración del servidor.

Como primer paso debemos permitir la conexión remota a nuestro servidor, por lo que, desde la ventana de Sistema del panel de control, accedemos a "Configuración de Acceso remoto".

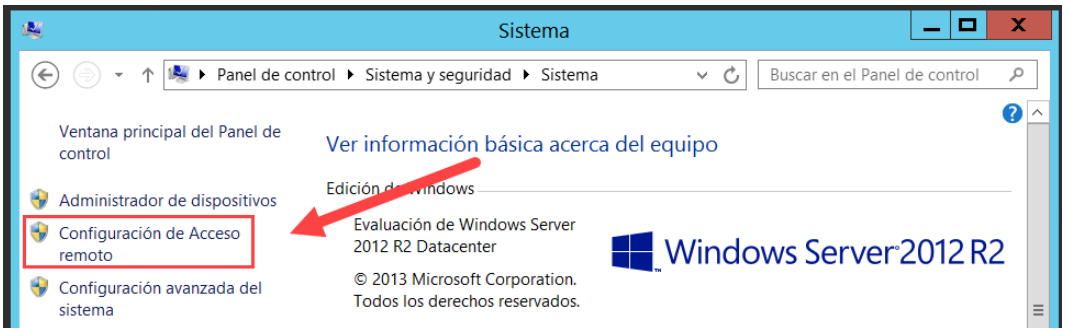

Figura 23: Ventana de Sistema de Servidor.

Lo importante en esta ventana será indicar que queremos permitir las conexiones remotas a este equipo, y es recomendable hacerlo para que solo se permitan conexiones desde equipos con autenticación a nivel de red o mayor. De forma opcional, podemos añadir otros usuarios además del Administrador para que tengan permisos de acceso remoto desde aquí.

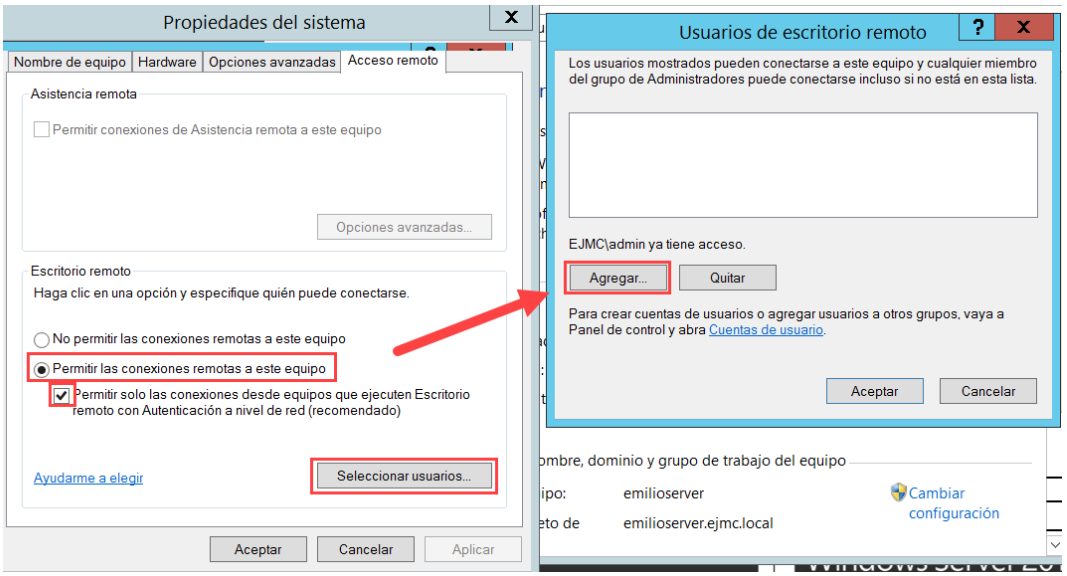

Figura 24: Permitir conexiones remotas al equipo.

El siguiente paso será permitir el acceso a través de Escritorio remoto en el Firewall. También desde el panel de control llegaremos hasta la ventana de configuración básica del cortafuegos, desde la cual podemos llegar hasta la ventana para “Permitir una aplicación o una característica a través de Firewall”.

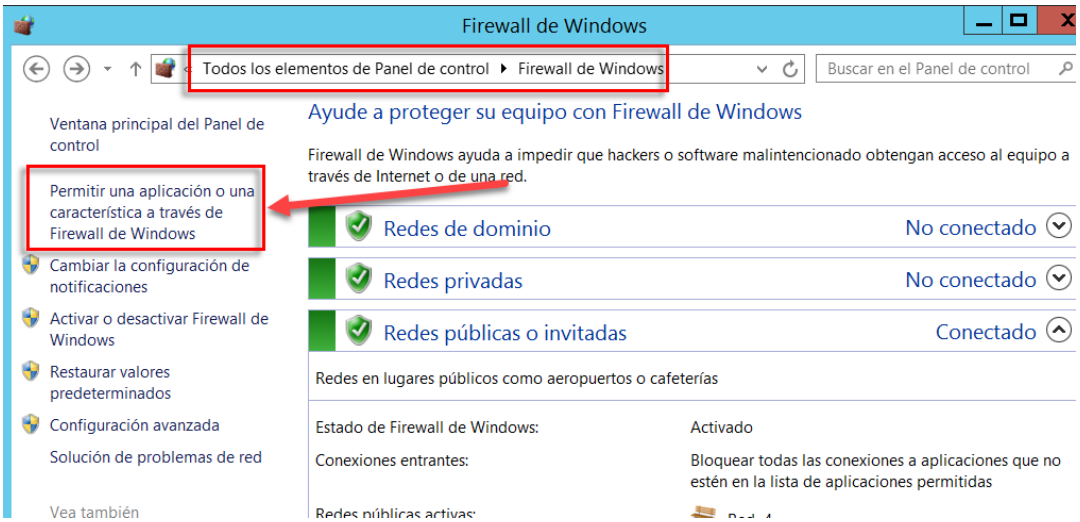

Figura 25: Firewall de Windows.

Desde aquí podremos confirmar que el Escritorio Remoto está permitido en redes privadas y de dominio, pero al estar usando una red pública como es la del instituto para acceder a nuestro servidor, debemos permitirlo también en redes públicas. En caso contrario, no será posible conectarse.

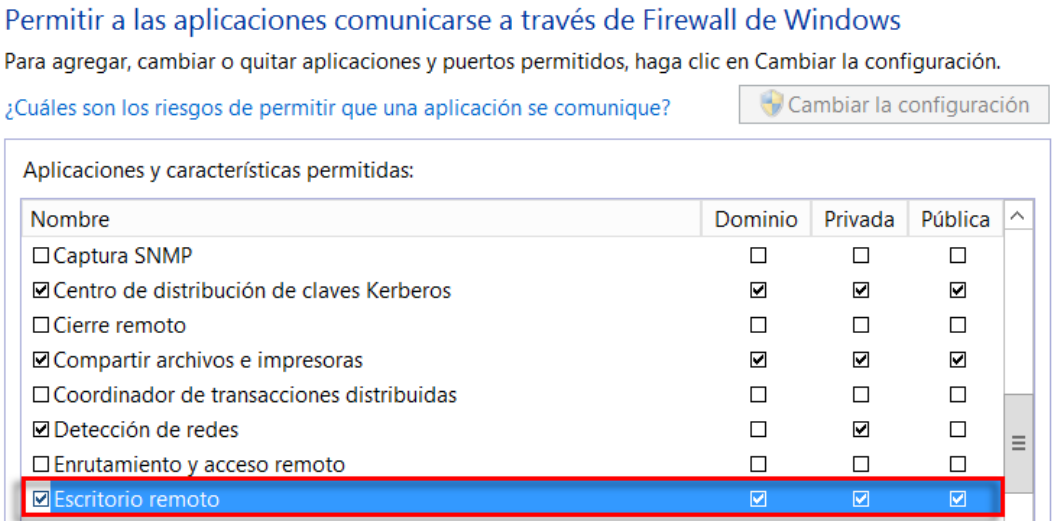

Figura 26: Permitir Escritorio Remoto en Firewall.

b. Acceso desde el cliente.

La aplicación de Escritorio Remoto viene instalado en nuestro Windows 10, por lo que no es necesario descargar la herramienta ni activarlo. Obviamente debemos estar en un equipo conectado al dominio con un usuario del mismo y con derechos de acceso remoto.

Desde la susodicha aplicación, indicaremos la dirección IP o el nombre del servidor, así como el usuario con el que iniciaremos sesión. Tras darle a conectar se nos pedirá la contraseña.

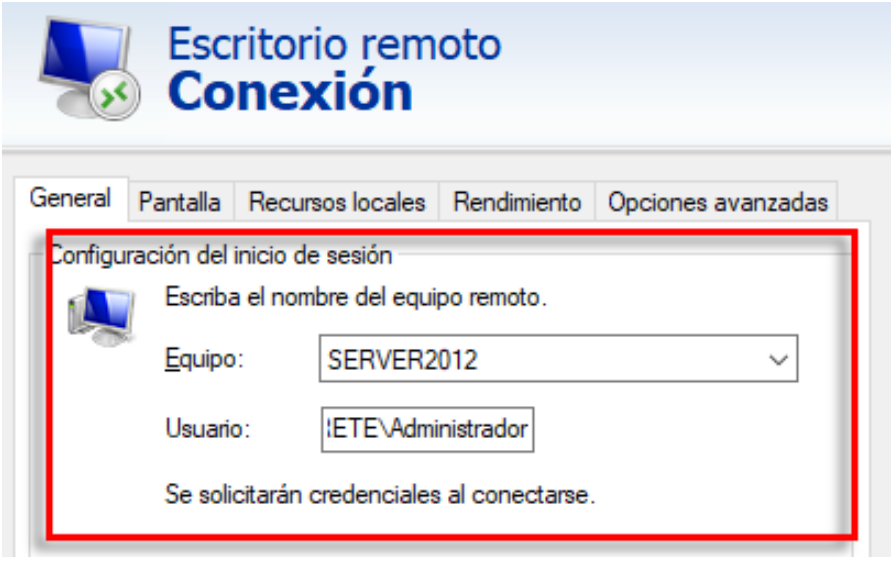

Figura 27: Escritorio Remoto en cliente.

Después de unos segundos, estaremos ante el escritorio del servidor a través de Escritorio Remoto, y podremos administrar nuestro Windows Server sin problema.

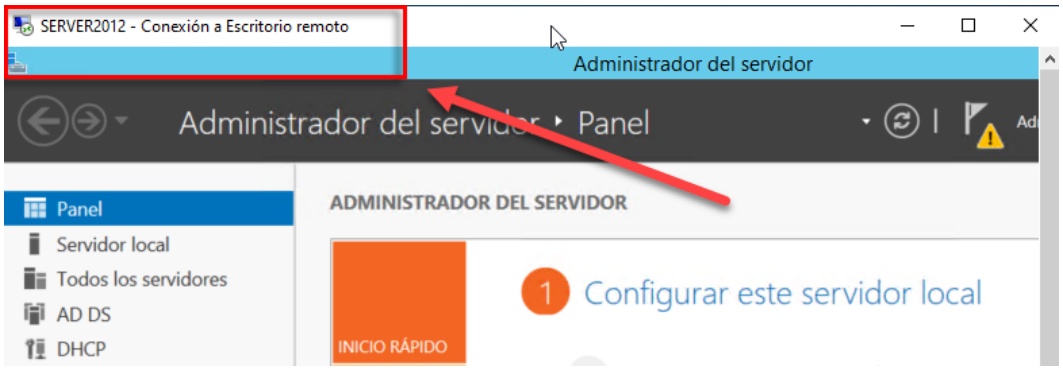

Figura 28: Administrador del servidor en cliente.

8. SSH en Windows Server 2012 R2

a. Configuración en el servidor.

RSAT y RDP son unas grandes opciones para administrar remotamente nuestro servidor, pero, ¿Qué ocurre si debemos trabajar sin modo gráfico? En ese caso es donde debemos buscar otras opciones.

Tanto las opciones de MMC como las de WinRM no las consideramos los suficientemente seguras actualmente, sin embargo, una conexión SSH cifrada a 128 bits y tras una VPN propia de la empresa con cifrado AES 256 o superior sí es aceptable, aportando una funcionalidad correcta.

Hacer esto en un servidor con Linux es más sencillo, pero en el caso de Windows tendremos que descargar freeSSHd o similares para que nos proporcione el servicio para tener nuestro servidor SSH funcional.

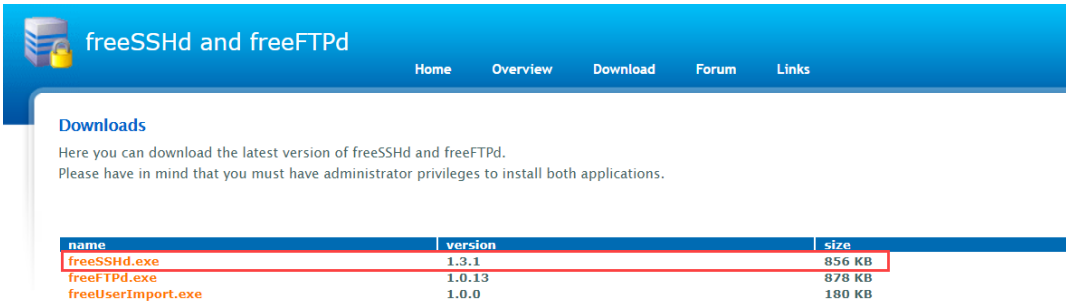

Figura 29: Descarga de freeSSHd.

Ejecutando el .exe del archivo el asistente únicamente nos pedirá la ruta de instalación y si deseamos un icono de escritorio. Tras ello debemos confirmar que queremos que se generen las claves privadas para las conexiones SSH y que FreeSSHd se ejecute como un servicio del sistema.

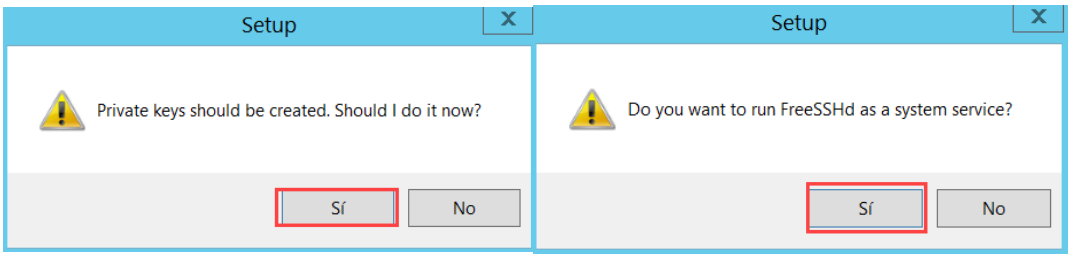

Figura 30: Preguntas en la instalación de freeSSHd.

En sus ajustes, tras su instalación, en la pestaña de SSH, confirmaremos que la dirección IP indicada es la estática del servidor, y le indicaremos un puerto para la conexión. En este caso, para evitar problemas sobre el puerto 22 (el puerto por defecto de SSH), pondremos otro diferente (222 para ser lo más descriptivos posibles), esto también mejorará la seguridad ante un atacante. Desde esta pestaña también podremos limitar aspectos como el número de conexiones máximas simultáneas, o el tiempo de expulsión por inactividad.

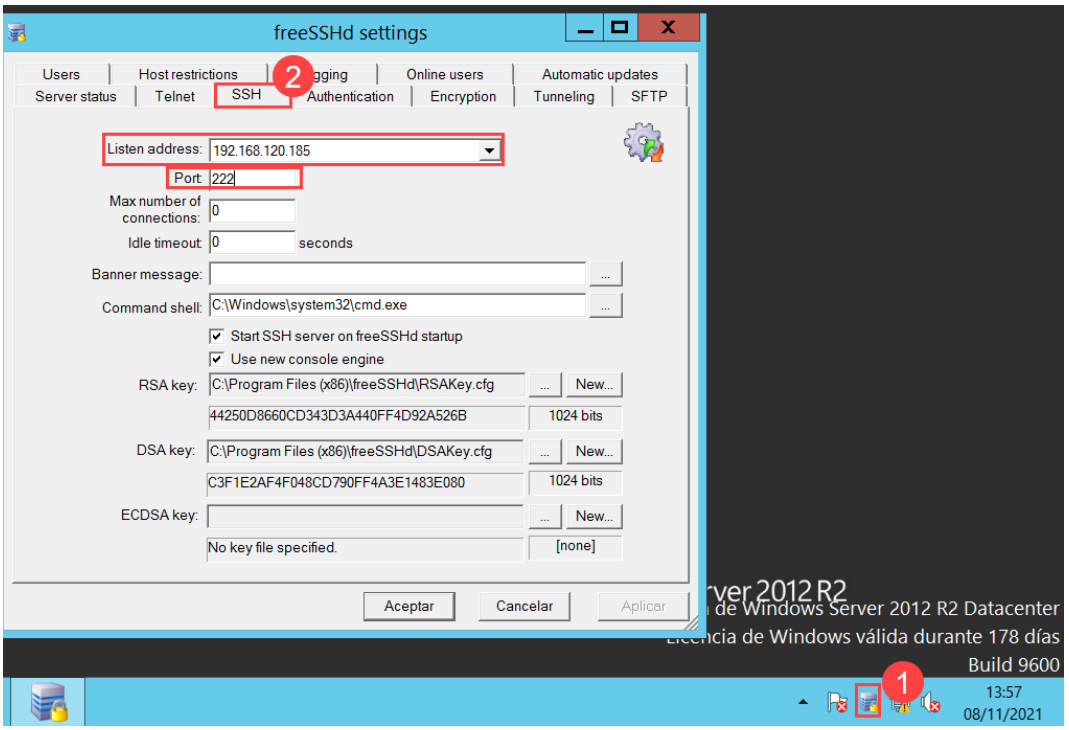

Figura 31: Configuración freeSSHd.

Como ya sabemos, para la conexión con SSH necesitamos generar nuestras claves, pudiendo usar RSA y DSA de forma simultánea para mayor seguridad. Las crearemos desde el botón de “New” y con 2048 bits.

Figura 32: Claves freeSSHd.

Aunque para nuestro caso, accederemos a la conexión SSH con usuario y clave, es útil tener claro cómo generar las claves RSA o DSA para autenticarse desde ciertas aplicaciones. Será desde la pestaña de autenticación, donde haremos obligatorio la autenticación con contraseña, y, de forma recomendable, permitiremos la autenticación con la clave pública.

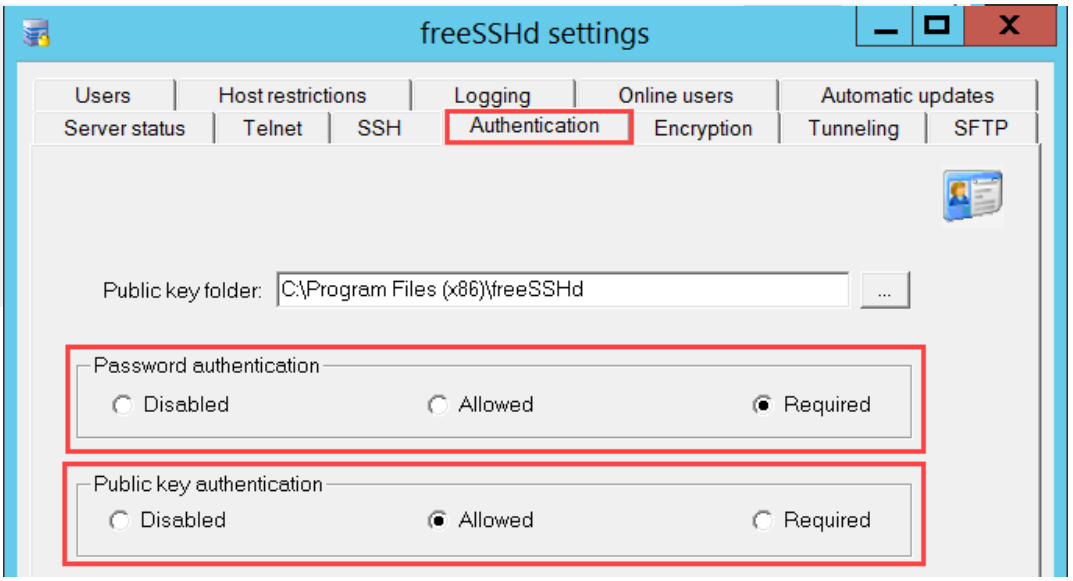

Figura 33: Autenticación en freeSSHd.

Una de las ventajas de usar freeSSHd para nuestro servidor, es que nos permite utilizar AES 256 para encriptar la conexión, por lo que será recomendable usar este método.

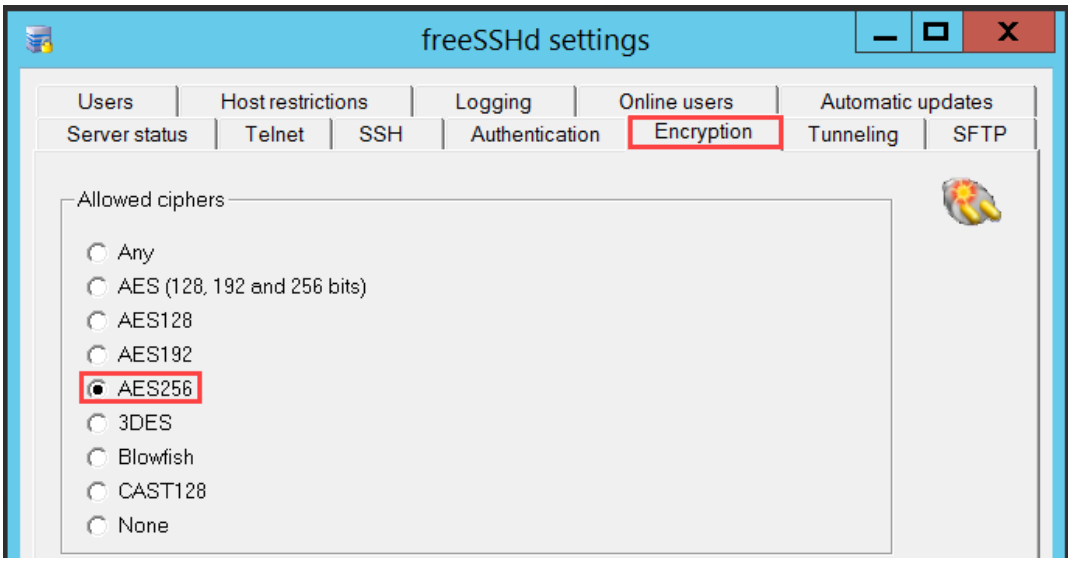

Figura 34: Encriptación en freeSSHd.

En la pestaña “Users” será desde donde añadiremos las propiedades de los usuarios que podrán tener acceso mediante SSH a nuestro servidor. En este caso lo llamaremos “admin” (Algo no recomendable para la seguridad del servidor), indicaremos una contraseña que se almacenará como hash SHA1. En este caso, el usuario podrá usar el Shell, SFTP y Tunneling.

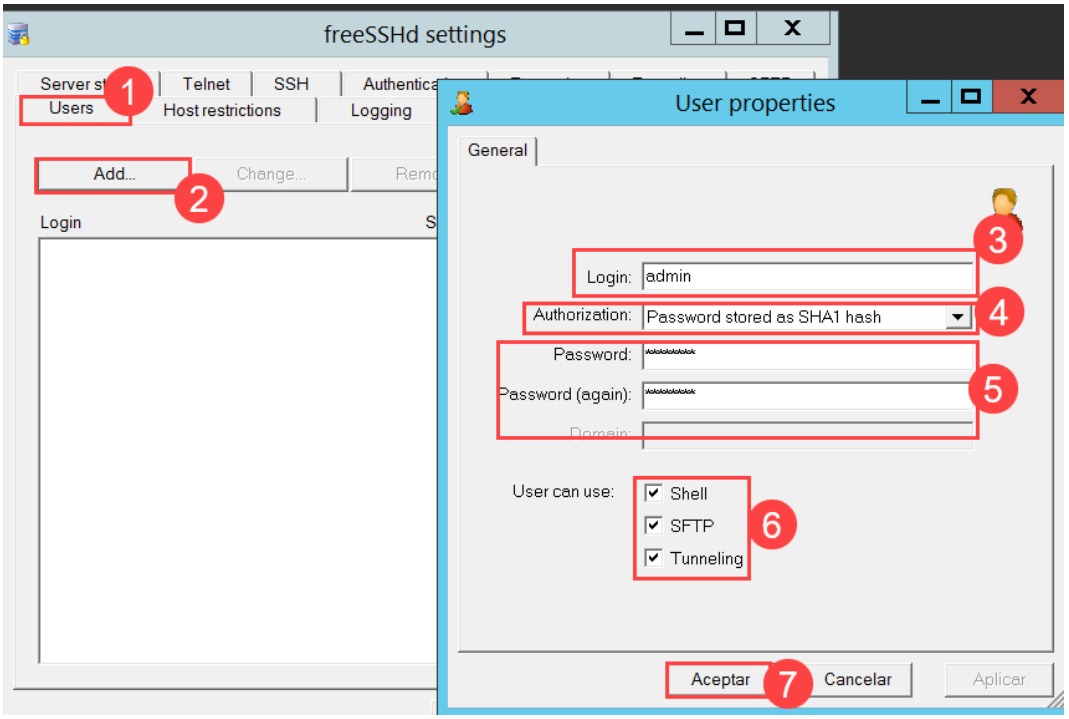

Figura 35: Users en freeSSHd.

En la pestaña Server Status podremos iniciar el servicio tras haber aplicado los cambios con el botón correspondiente.

Figura 36: Users en freeSSHd.

Para evitar problemas con el Firewall de Windows, permitiremos freeSSHd desde el menú de “Aplicaciones permitidas”.

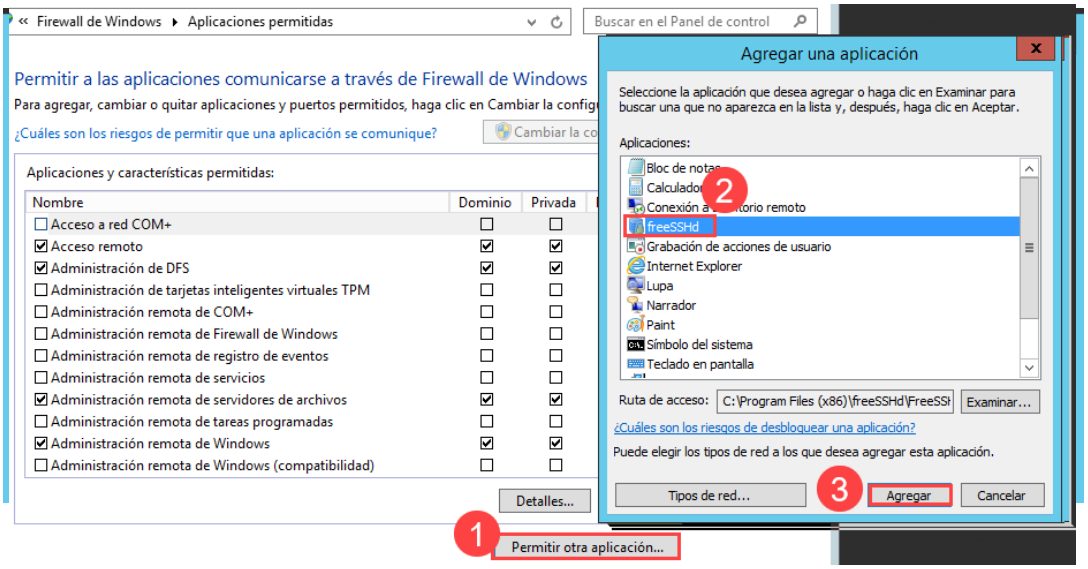

Figura 37: Firewall del servidor para permitir freeSSHd.

b. Configuración en el servidor.

Desde la máquina cliente nos hemos también encontrado problemas con el Firewall, por lo que para evitarlos es recomendable permitir también en él las conexiones SSH.

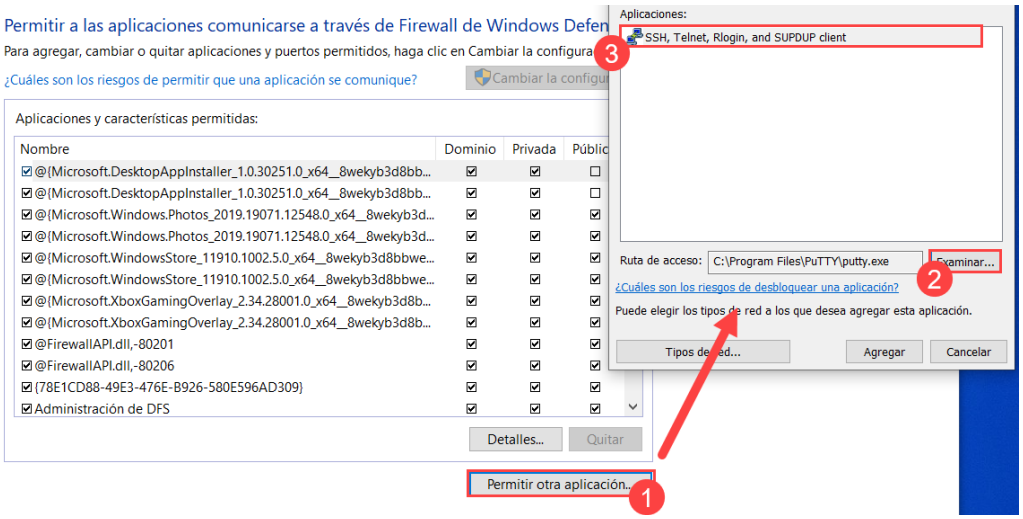

Figura 38: Firewall del cliente para permitir SSH.

Con cualquier aplicación para conectarnos por SSH, ya podremos realizar la conexión, indicando tanto la dirección IP (o el nombre del host) y el puerto.

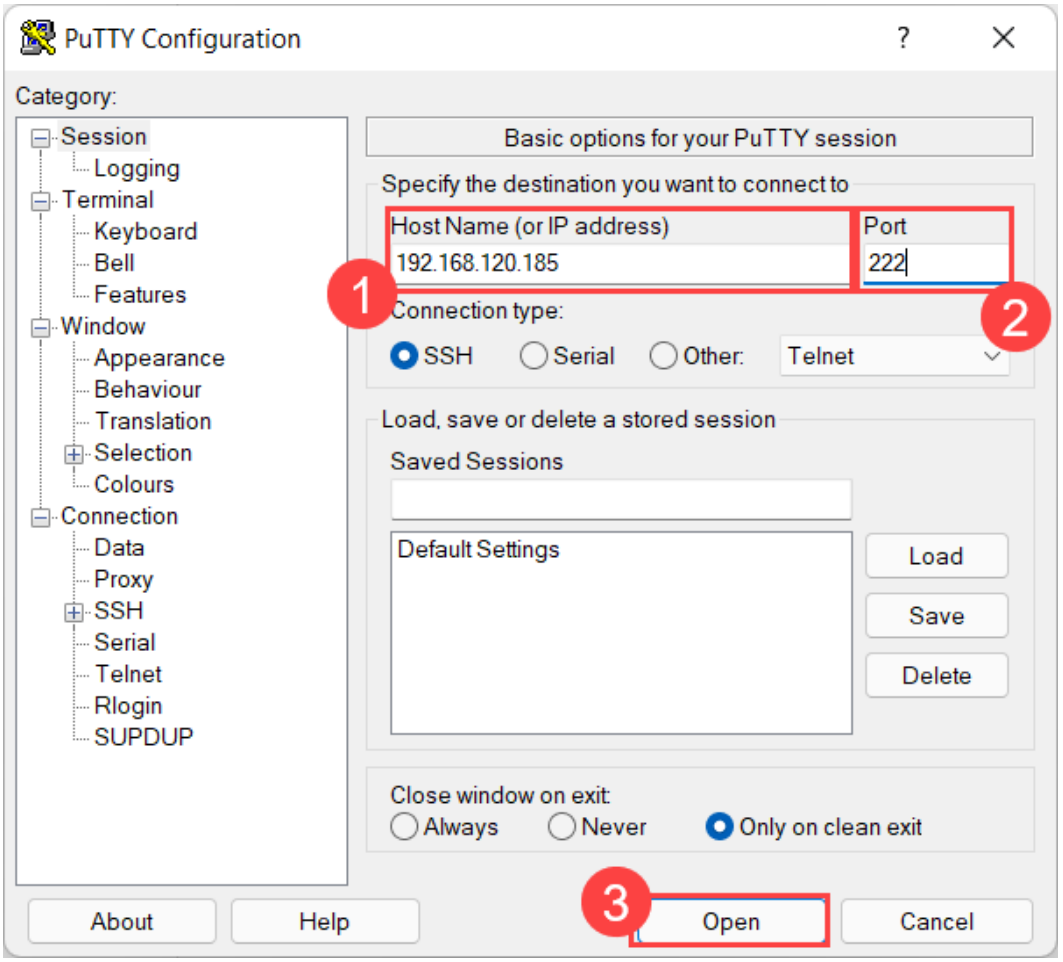

Figura 39: Iniciar conexión SSH.

Por supuesto, antes de iniciar la conexión, debemos iniciar sesión en el usuario que creamos en freeSSHd.

Figura 40: Inicio de sesión SSH.

9. Referencias

BLACKBOX. *Administración remota de ordenadores* <Blackbox.com | Administración remota> [Consulta: 2/11/2021].

PCNAUTAS. *Ventajas e inconvenientes de la Administración remota* <Pcnautas.com | Soporte remoto> [Consulta: 2/11/2021].

THESTANDARCIO. *Infraestructura en una empresa* <Thestandarcio.com | Infraestructura en Tripp Lite> [Consulta: 3/11/2021].

HERSCHELGONZALEZ. *¿Qué es un sistema multiusuario?* <Herschelgonzalez.com | Sistema multiusuario> [Consulta: 3/11/2021].

LAURA FITZGIBBONS. *What is Telnet?* <Techtarget.com | Telnet>. [Consulta: 01/11/2021] .

EXTRAHOP. Teletype Network Protocol? <Extrahop.com | Telnet>. [Consulta: 01/11/2021].

KARTIK THAKRAL. Difference between SSH and Telnet <Geeksforgeeks.com | SSH - Telnet>. [Consulta: 01/11/2021].

JUSTIN ELLINGWOOD. Understanding the SSH Encryption <Digitalocena.com | SSH>. [Consulta: 01/11/2021].

MUDIN MAHESHWARI. Understanding SSH workflow <Medium.com | SSH Workflow>. [Consulta: 02/11/2021].

BEN STOCKTON. What is RDP? <Comparitech.com | What is RDP?>. [Consulta: 02/11/2021].

DELAND- HAND. Descripción del Protocolo de Escritorio remoto <Microsoft.com | Understanding RDP>. [Consulta: 02/11/2021].

ALYSSA WALKER. SOAP Web Services Tutorial. <Guru99.com | Soap Protocol>. [Consulta: 03/11/2021].

GEEKS.MS. Administración de Remota de Win Vista mediante WS-Management <Geeks.ms | WS-Management>. [Consulta: 03/11/2021].

KDE. El protocolo Remote Frame Buffer <KDE.org | What is RFB> [Consulta: 03/11/2021].

OPENSSH. *Portable Realise* <OpenSSH.com | Portable Realease>. [Consulta: 02/11/2021]

OSI. *Herramientas gratuitas* <OSI.es | Herramientas Gratuitas>. [Consulta: 03/11/2021]

TEAMVIEWER. *Soporte remoto rápido* <TeamViewer | Soporte remoto rápido> [Consulta: 03/11/2021]

ANYDESK. *Características de AnyDesk* <AnyDesk | Características> [Consulta: 03/11/2021]

ANYDESK. *¿Por qué AnyDesk?* <AnyDesk | Performace> [Consulta:03/11/2021]

JESÚS RODRÍGUEZ. *Administración remota Windows Server 2012 RSAT* <Administración remota RSAT (cipsa.net)> [Consulta:05/11/2021]

DOCUMENTACIÓN MICROSOFT. *Escritorio remoto: Permitir Acceso* <Escritorio remoto: permitir el acceso al equipo> [Consulta:05/11/2021]

REDESZONE. *FreeSSHd para Windows* <FreeSSHd para windows> [Consulta: 09/11/2021]