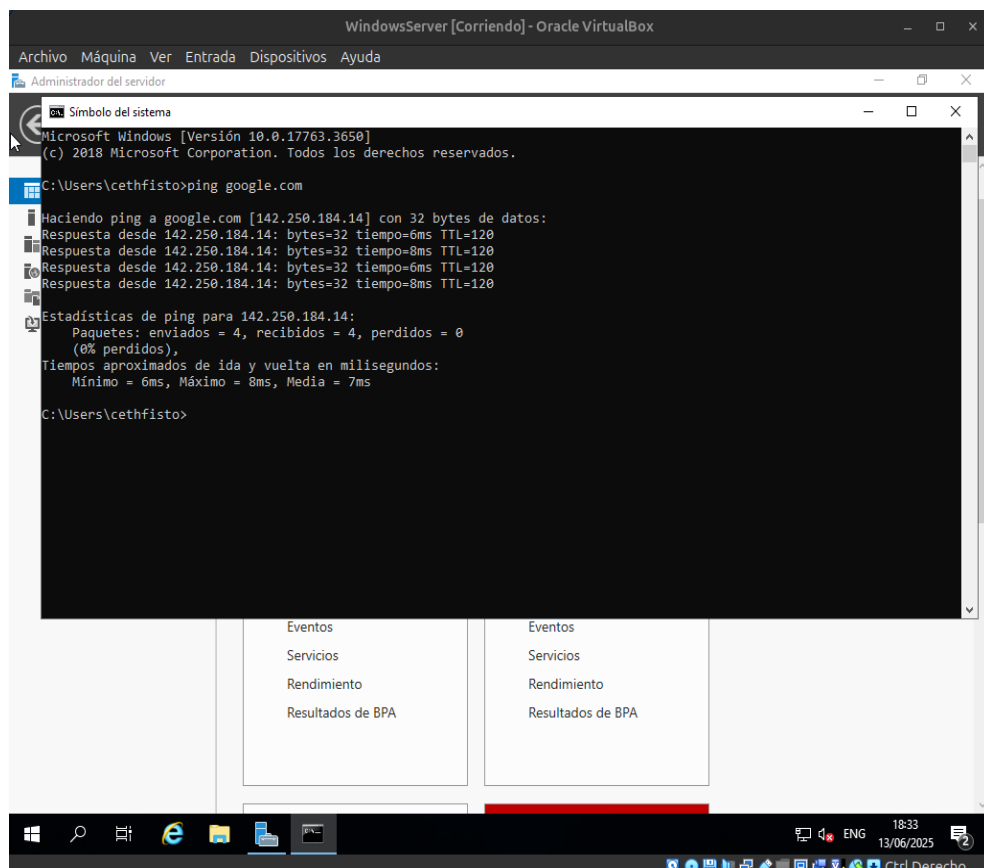
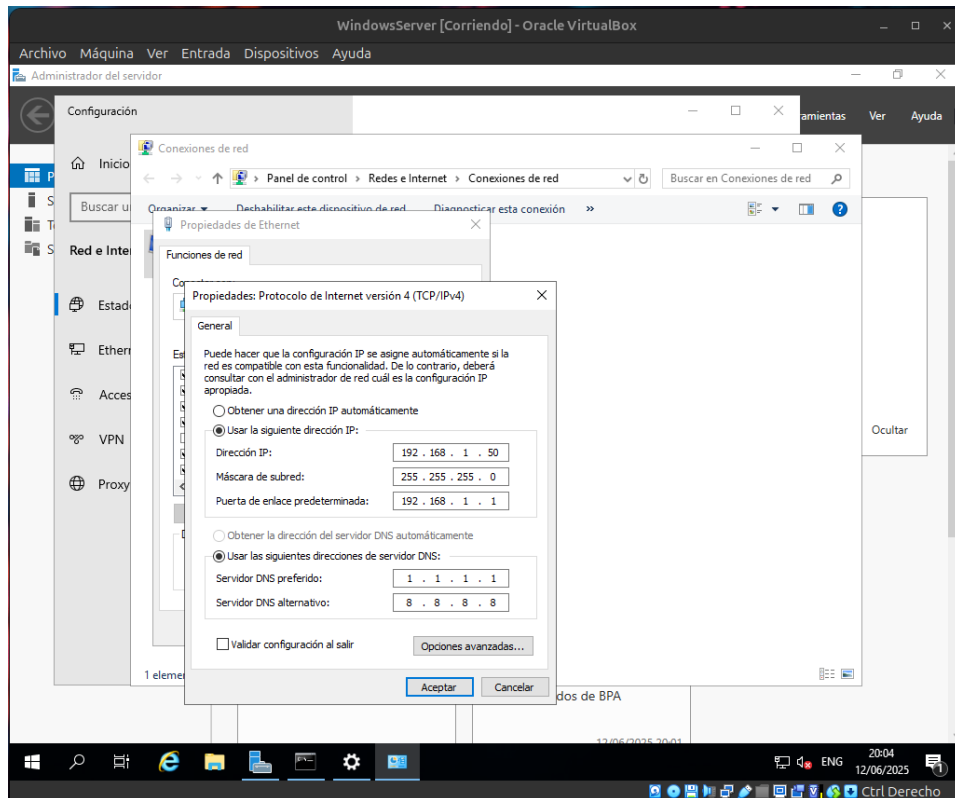
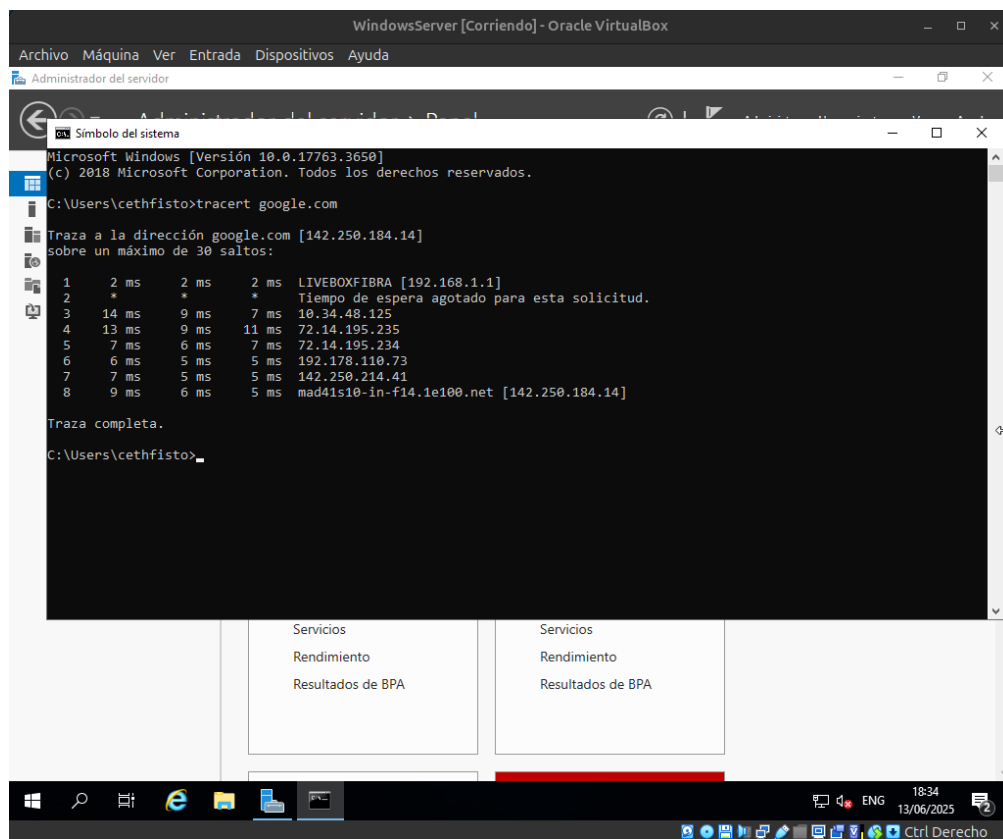


Fase: 1

Hemos asignado una IP estática a nuestro servidor y hemos comprobado si funciona la configuración usando los comandos de ping y tracert. Hemos usado como ejemplo Google para tener un destino para poder ejecutar los comandos.





En estas imágenes podemos comprobar que tenemos una IP estática, el ping hacia Google funciona y que el tracert ha funcionado también. Vemos que ha hecho 8 saltos hasta realizar la trazada completa.

Fase: 2

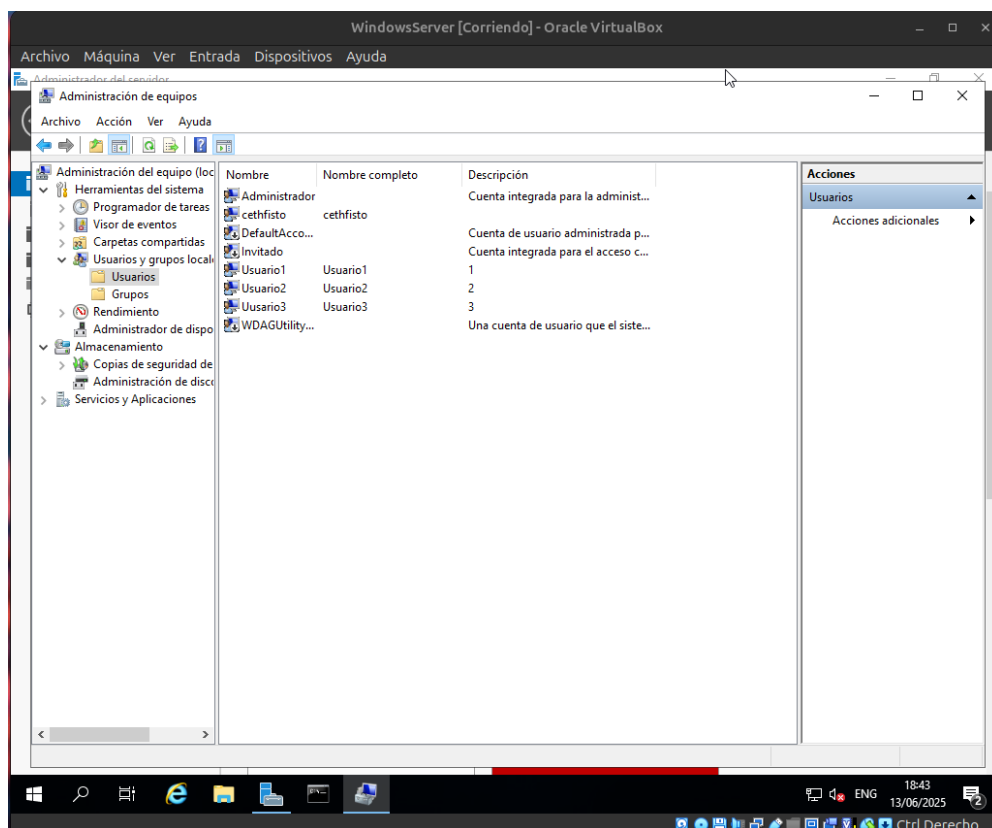
En esta fase, vamos a crear tres usuarios con diferentes permisos, configurar los grupos de seguridad y aplicar dichos permisos en las carpetas compartidas.

Para crear los usuarios haremos los de siempre, vamos a Herramientas, Administración de equipos y Usuarios y grupos locales. Y creamos los tres usuarios.

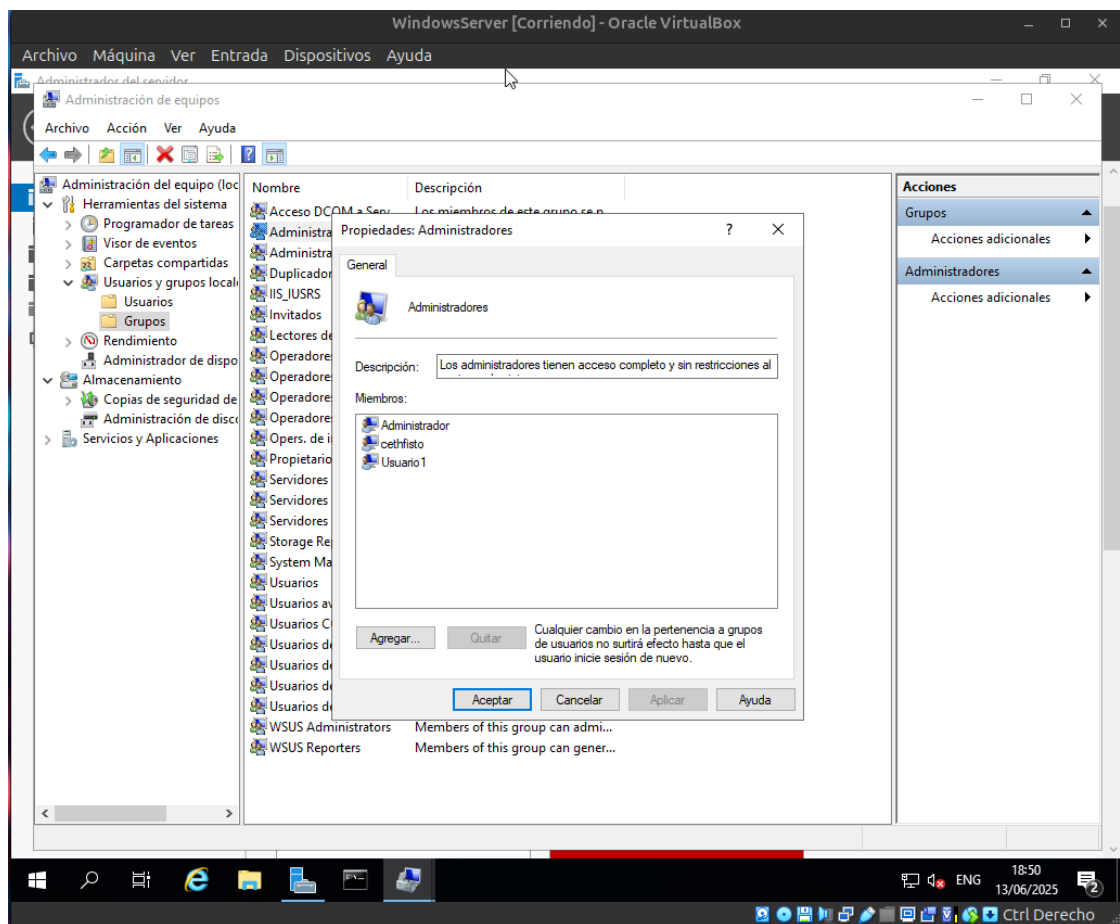
Una vez creados daremos los distintos permisos según el grupo, el Usuario1 será administrados, el Usuario2 será Usuario estándar y el Usuario3 será Invitado. También podemos crear grupos personalizados que podemos dar permisos concretos para se adapten a nuestras necesidades.

Y por último para configurar una carpeta según los permisos de cada usuario, haríamos lo siguiente. Creamos la carpeta que queremos compartir y en las propiedades, seleccionamos Compartir. Y seleccionamos Uso compartido avanzado.

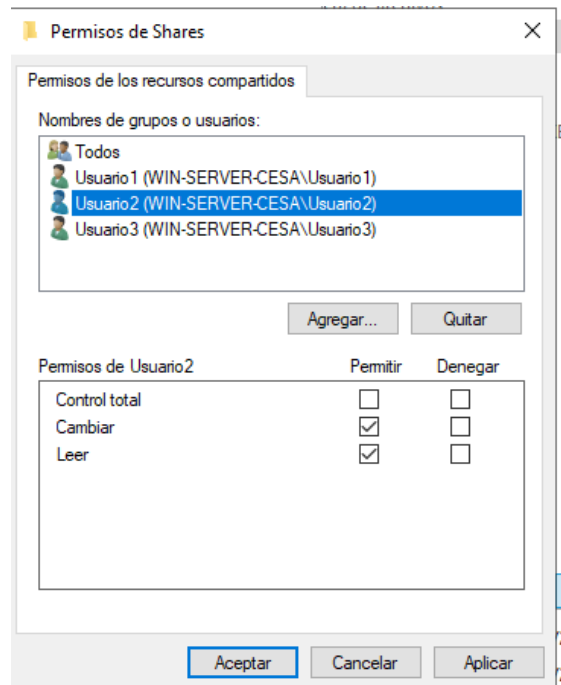
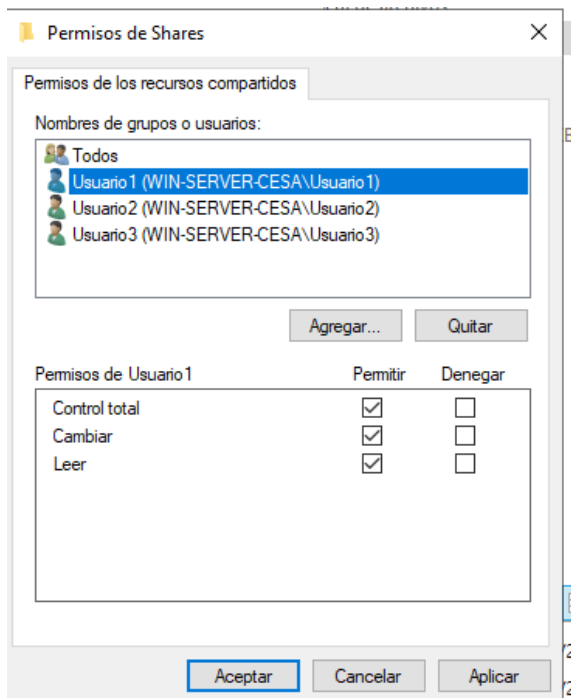
En el caso de Usuario1, le hemos dado control total, ya que es administrador. En el caso de Usuario2, cambiar y leer que es un usuario estándar. Y para el Usuario3, solo leer, ya que es invitado.

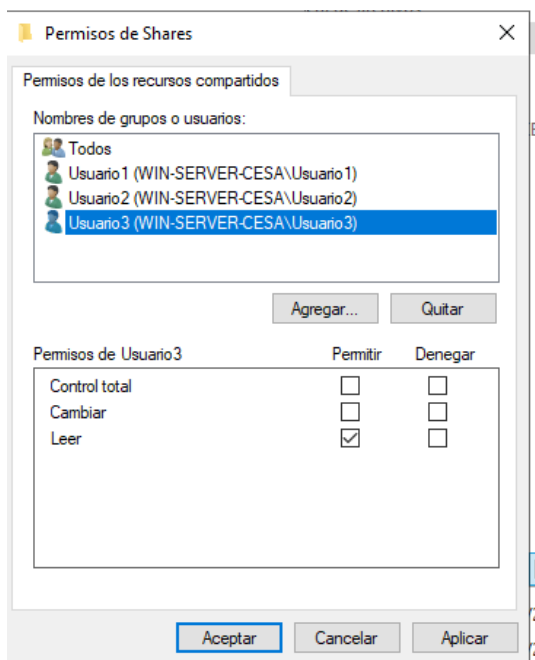


En esta imagen podemos ver a los usuarios ya creados.



Aquí podemos ver que uno de los usuarios está en el grupo que le corresponde.





En estas tres capturas podemos ver que hemos asignado los permisos a cada usuario según el grupo al que pertenece.

Fase: 3

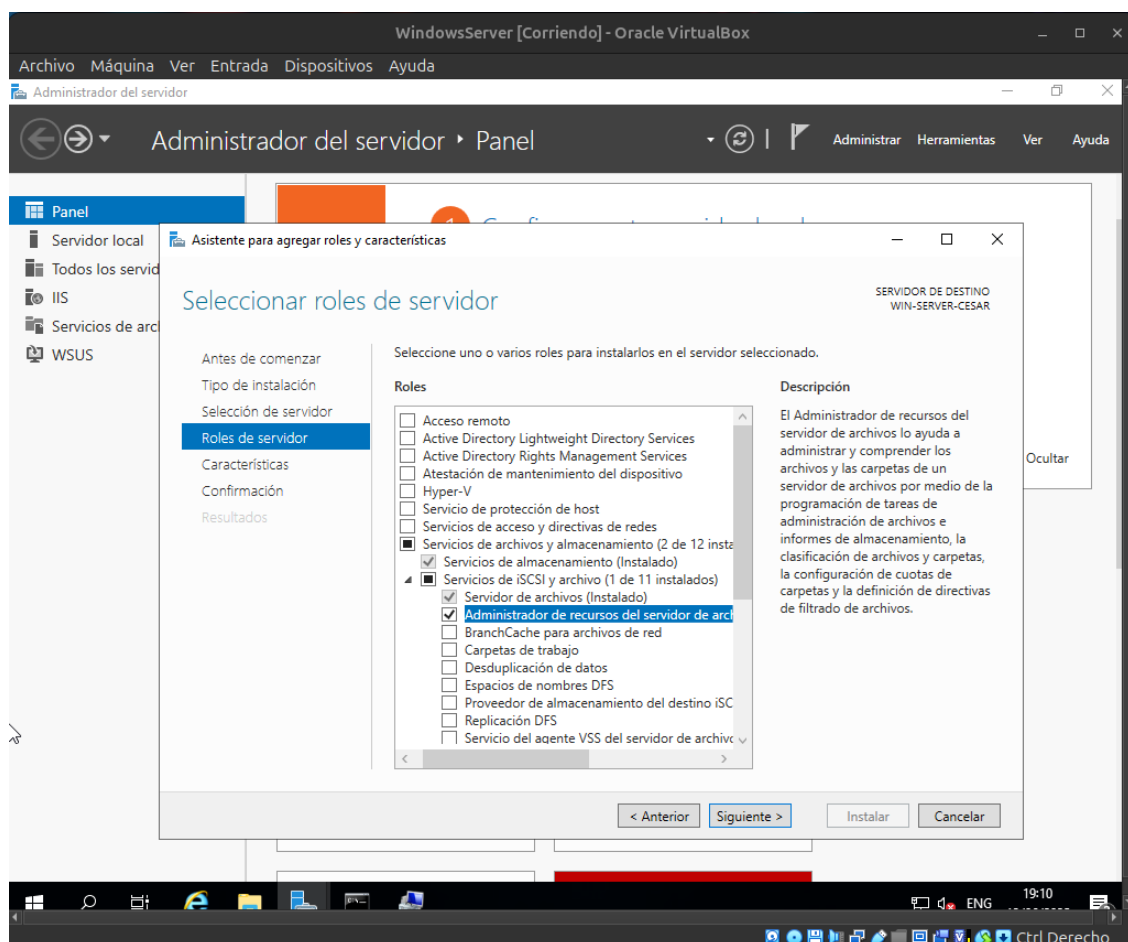
En esta fase, vamos a instalar y configurar herramientas de gestión de archivos y de acceso remoto. Para terminar revisaremos el estado del servidor y veremos los eventos.

Para instalar el gestor de archivos del servidor iremos al Administrador del servidor y seleccionamos Agregar roles y características. Y en Características seleccionamos, Servicios de archivos y almacenamiento y Administrador de recursos del servidor de archivos. Aquí podemos crear cuotas a usuarios, crear reglas de acceso a archivos o ver informes de almacenamiento.

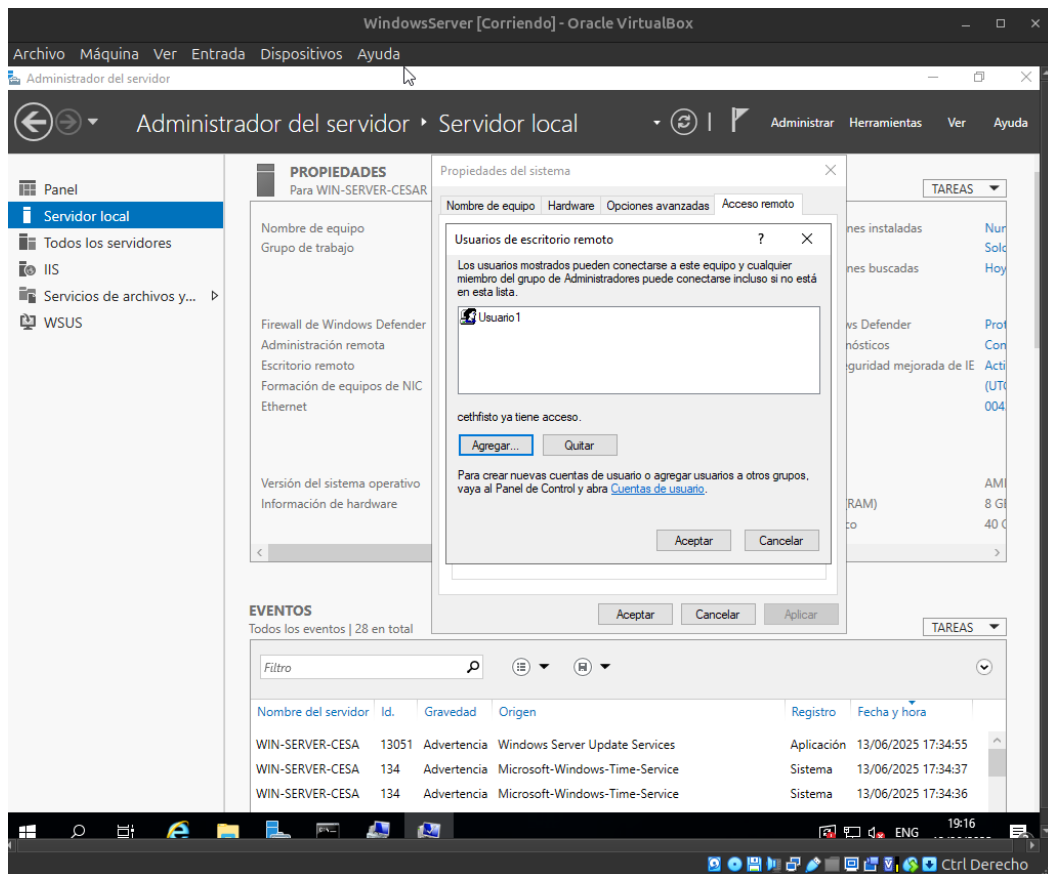
Vamos añadir unas reglas de acceso a una carpeta. Iremos a Herramientas, Administrador de recursos del servidor. Y en este caso seleccionamos Filtros de archivos y elegimos Crear filtro. En la ventana emergente crearemos el filtro, en este caso e bloqueado los archivos ejecutables en la carpeta compartida llamada Prueba1.

Para el acceso remoto, primero debemos tener el servicio habilitado, lo podemos comprobar en las Propiedades del servidor local. Seleccionamos el servicio y hacemos click en Seleccionar usuarios. Pondremos al Usuario1, ya que es el administrador. Debemos asegurarnos que el firewall esté configurado, sino tendremos que crear una regla de entrada del puerto 3389 TCP.

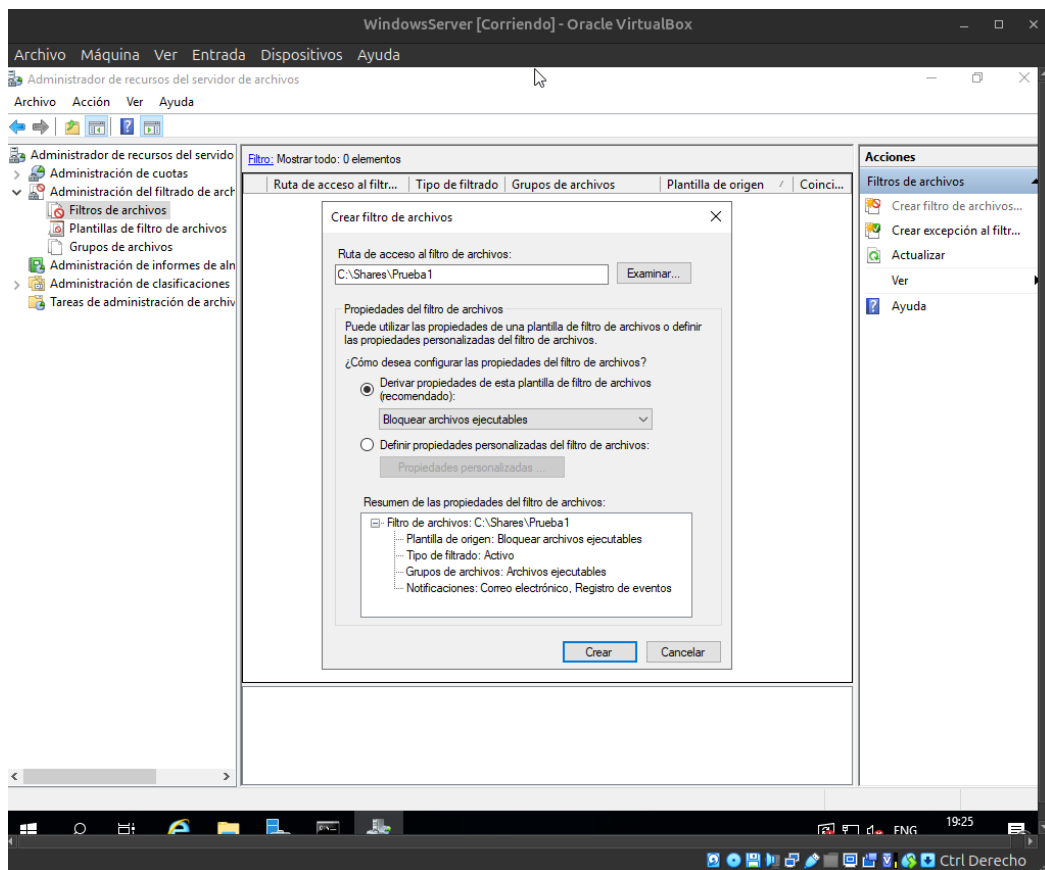
De esta tendríamos una configuración sencilla para una situación hipotética con varios usuarios, permisos y carpetas compartidas.



En esta foto podemos el proceso de instalación del gestor de archivos del servidor.



En la imagen superior podemos ver que hemos añadido el Usuario1 para el acceso remoto.



Y en esta ultima podemos que hemos bloqueado los ejecutable en la carpeta en cuestión.

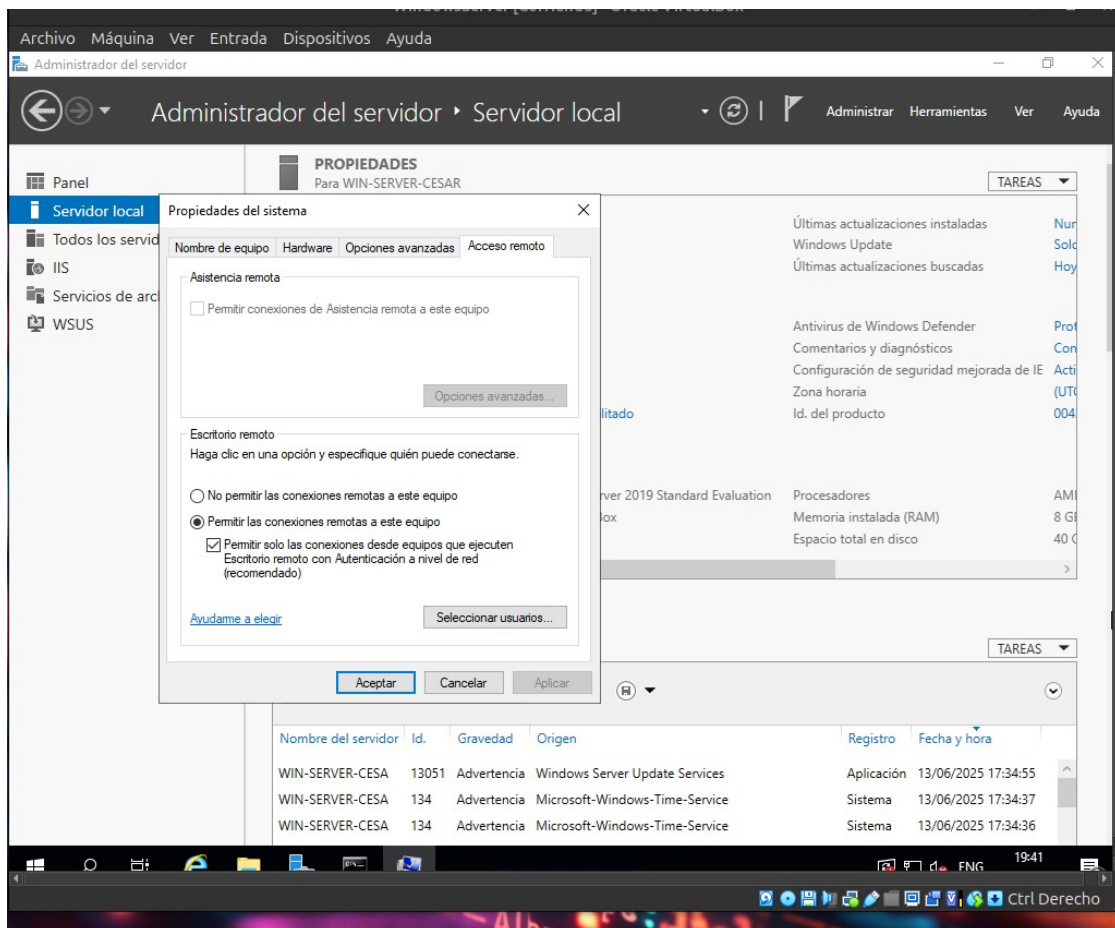
Fase: 4

En esta fase vamos a integrar políticas de seguridad para accesos remotos y configurar el firewall para evitar accesos no deseados.

Para crear una buena política de seguridad en accesos remotos, tan solo debemos añadir a los usuarios que queramos que tengan dicho privilegio y activar la opción de Permitir conexiones solo desde equipos que ejecuten Escritorio remoto con autenticación a nivel de red.

Respecto a la hora de crear reglas de firewall para evitar accesos no deseados, iremos a Herramientas y seleccionamos Firewall de Windows Defender con seguridad avanzada. Una vez allí, podremos bloquear IPs y puertos.

Vamos a bloquear una IP supuestamente sospechosa, para ello seleccionamos Nueva regla, completaremos el usuario y terminaremos con la opción Bloquear conexión. Y ya tendríamos la IP bloqueada en este caso.



En esta imagen podemos apreciar que tenemos activada la opción de Permitir conexiones solo desde equipos que ejecuten Escritorio remoto con autenticación a nivel de red para los accesos remotos.

Fase: 5

Para terminar, hemos hecho configuraciones sencillas y en supuestos prácticos. Estas configuraciones en una situación real, crear una división de permisos entre los usuarios según su categoría para evitar filtraciones o modificaciones no deseadas. A su vez, tenemos acceso remoto por parte de usuarios autorizados. En cuanto al firewall o permisos en carpetas compartidas tenemos, un bloqueo a ciertos archivos que queramos no ejecutar. Y a la modificación o lectura de archivos en carpetas compartidas según el tipo de usuario que quiera acceder o modificar algo.