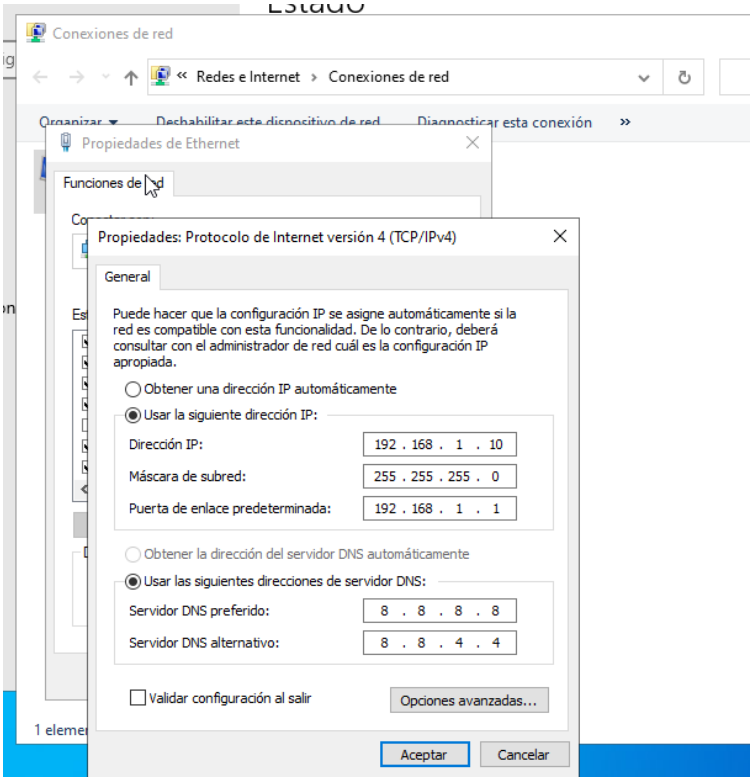
Fase 1: Configuración de red en Windows Server

✅ Asignar una IP estática en la configuración de red.

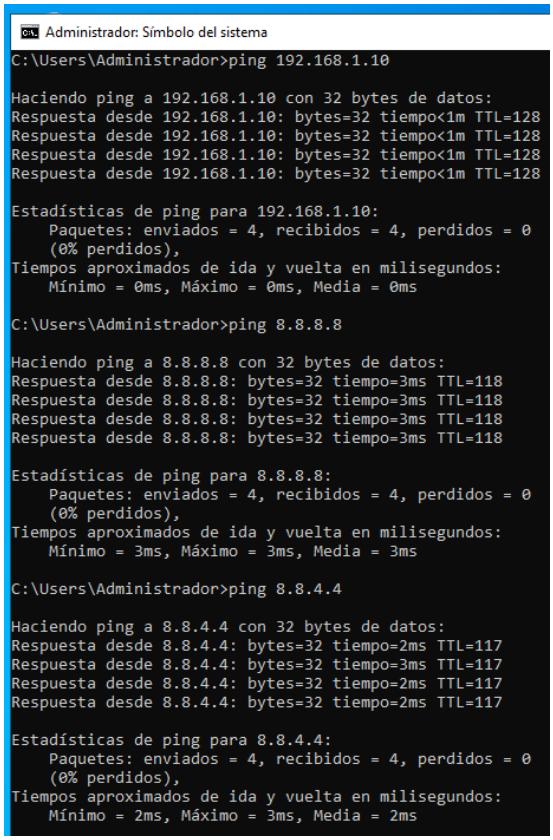
✅ Configurar la puerta de enlace y servidores DNS.

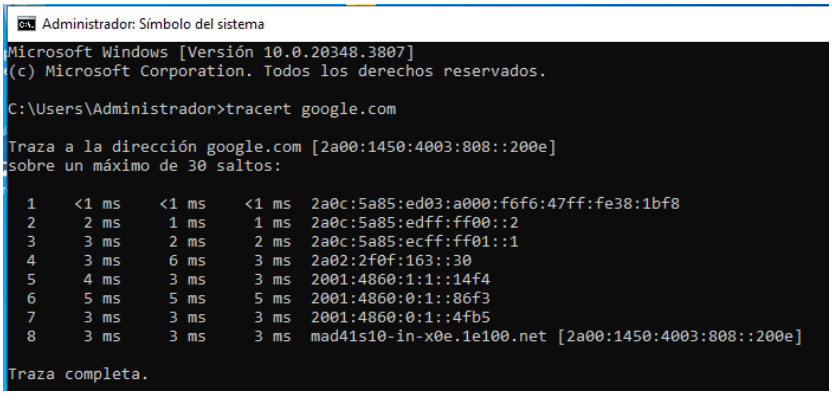
✅ Probar la conectividad con ping y tracert.

Primero asignamos la IP, la puerta de enlace y los DNS:



Probamos la conectividad con el comando ping y tracert:



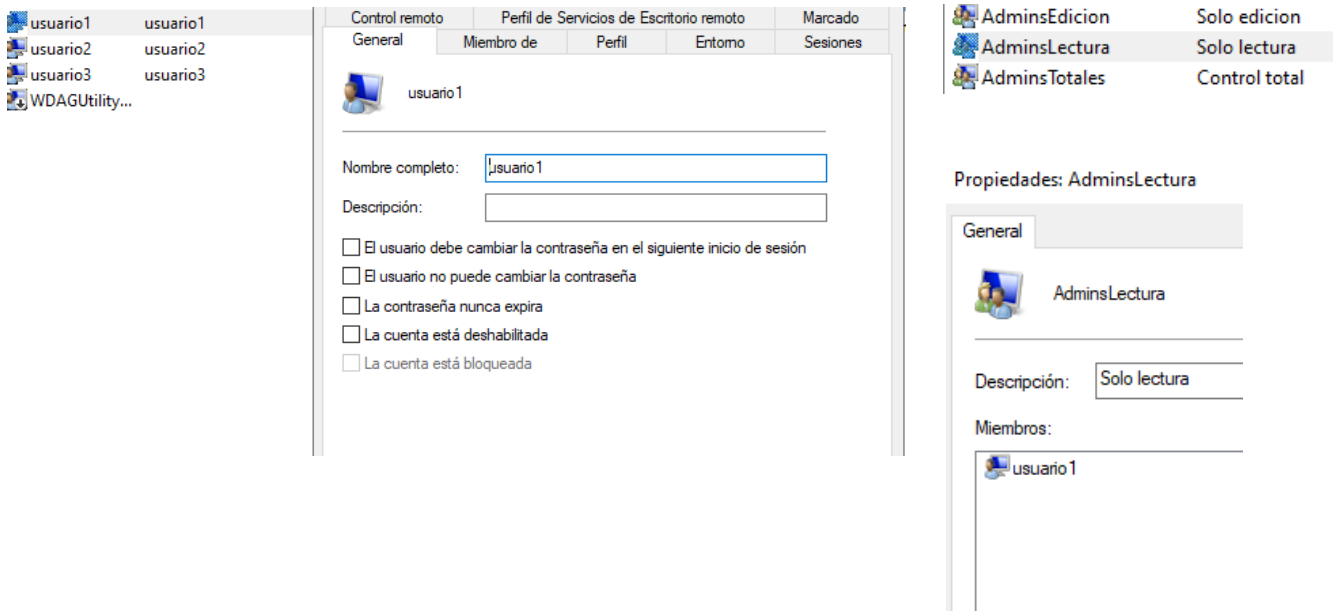


Fase 2: Gestión de usuarios y permisos
✅ Crear tres usuarios estándar con diferentes permisos.
✅ Configurar grupos de seguridad para la administración del servidor.
✅ Aplicar permisos en carpetas compartidas dentro del sistema.

En Administración de equipos, vamos a Usuarios y grupos locales y hacemos clic derecho sobre usuarios, usuario nuevo…

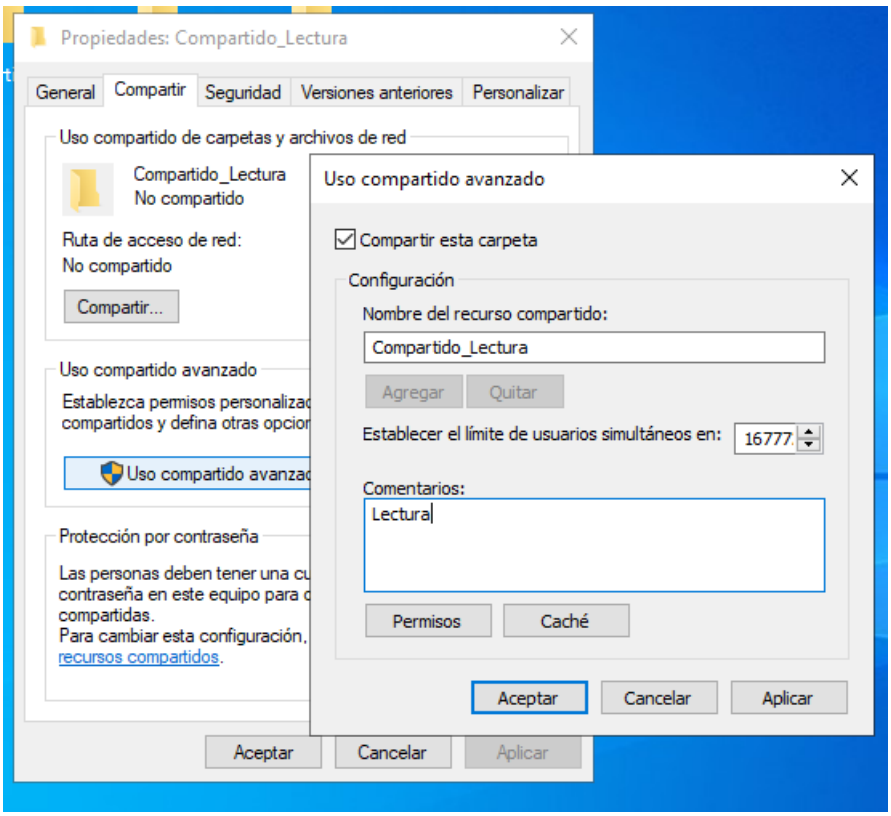
usuario1: Lectura solamente.
usuario2: Lectura y escritura.
usuario3: Control total.

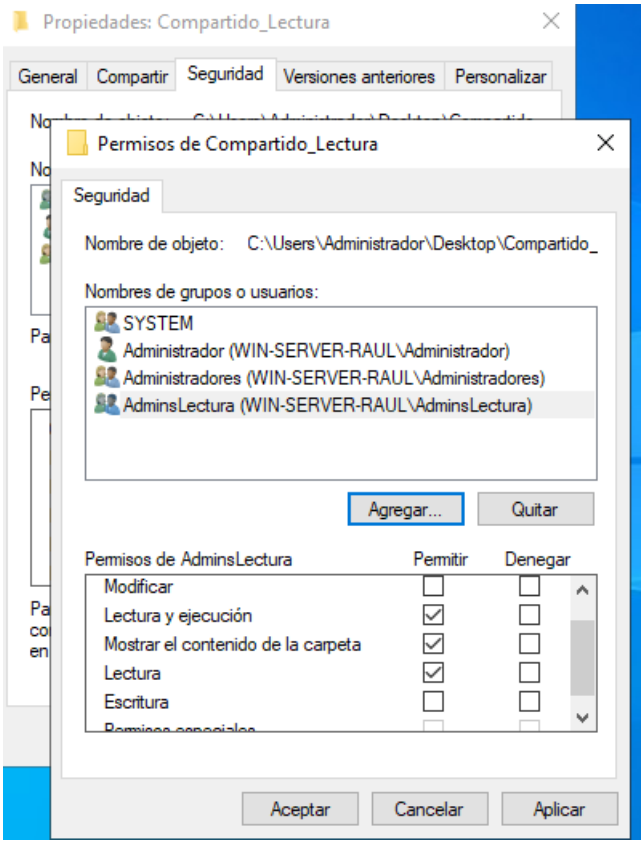
Y creamos tres grupos según sus roles:
usuario1 → AdminsLectura
usuario2 → AdminsEdicion
usuario3 → AdminsTotales



Aplicar permisos en carpetas compartidas dentro del sistema:

Crearemos carpetas:
Compartido\Lectura
Compartido\Edicion
Compartido\ControlTotal
Haz clic derecho sobre cada carpeta > Propiedades > Compartir > Uso compartido avanzado:
Marca Compartir esta carpeta
Asigna un nombre (ej: Lectura)
Ve a la pestaña Seguridad:
Haz clic en Editar > Agregar
Escribe el nombre del grupo de seguridad (ej. AdminsLectura)
Establece los permisos según el grupo:
AdminsLectura: Solo lectura
AdminsEdicion: Modificar
AdminsTotales: Control total





Repetimos el proceso en las dos carpetas restantes dando sus respectivos permisos.

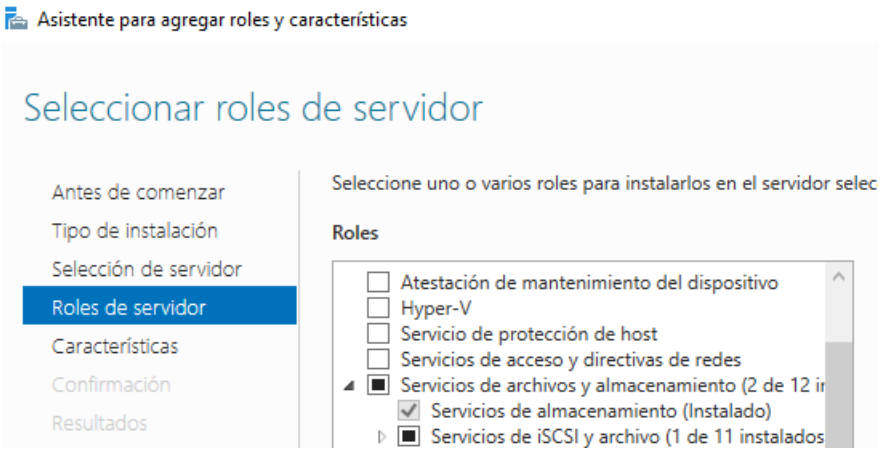
Fase 3: Instalación de roles y herramientas esenciales
✅ Explorar el Administrador del Servidor y su interfaz.
✅ Instalar y configurar herramientas de gestión de archivos y acceso remoto.
✅ Revisar el estado del servidor y monitorear eventos del sistema.

Haz clic en el botón Inicio y abre Administrador del servidor (Server Manager).
Examina los paneles principales:
Dashboard (Panel principal)
Local Server: Configuración y estado del servidor local
All Servers: Lista de servidores que estás gestionando
Tools: Acceso a herramientas administrativas como PowerShell, Event Viewer, etc.

Instalar y configurar herramientas de gestión de
archivos y acceso remoto:

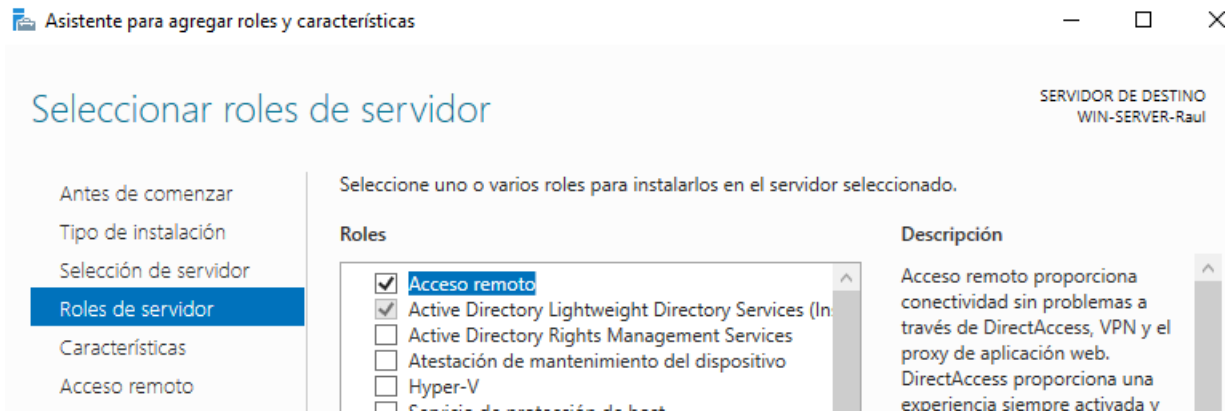
Servidor de Archivos (File Server):
Permite compartir archivos/carpetas y gestionar almacenamiento.

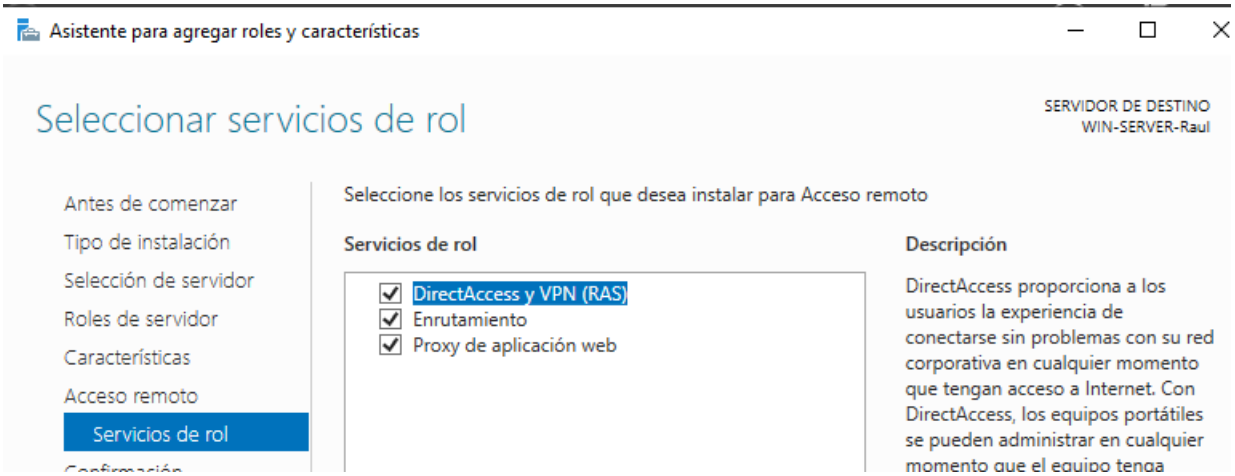
En Administrador del servidor, haz clic en Agregar roles y características.
Tipo de instalación: Basada en funciones o características.
Selecciona el servidor local.
En la sección de Roles, marca:
Servicios de archivo y almacenamiento
Dentro de este, marca Servidor de archivos.



Acceso Remoto (Remote Access):
Permite administrar el servidor desde otros equipos o habilitar VPN, proxy, etc.

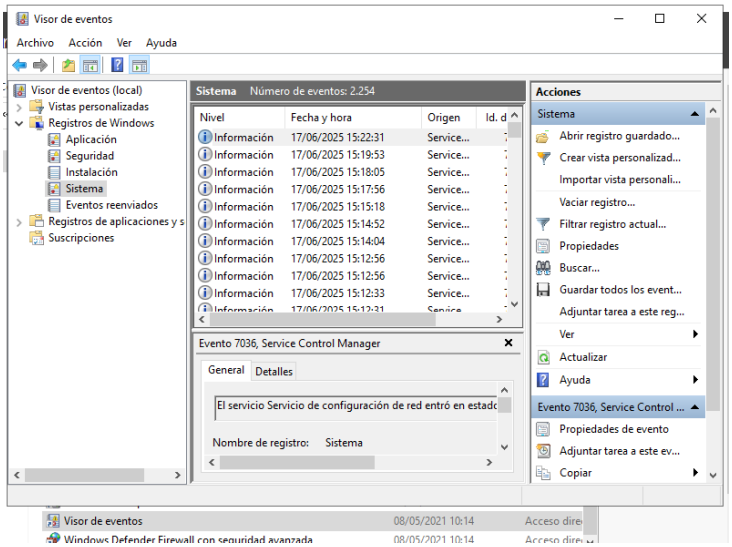
En el asistente de roles, selecciona Acceso remoto.
Dentro de sus subfunciones puedes instalar:
DirectAccess y VPN (RAS) si necesitas acceso remoto completo.
Web Application Proxy, si se gestiona tráfico web.
Finaliza la instalación y reinicia si es necesario.

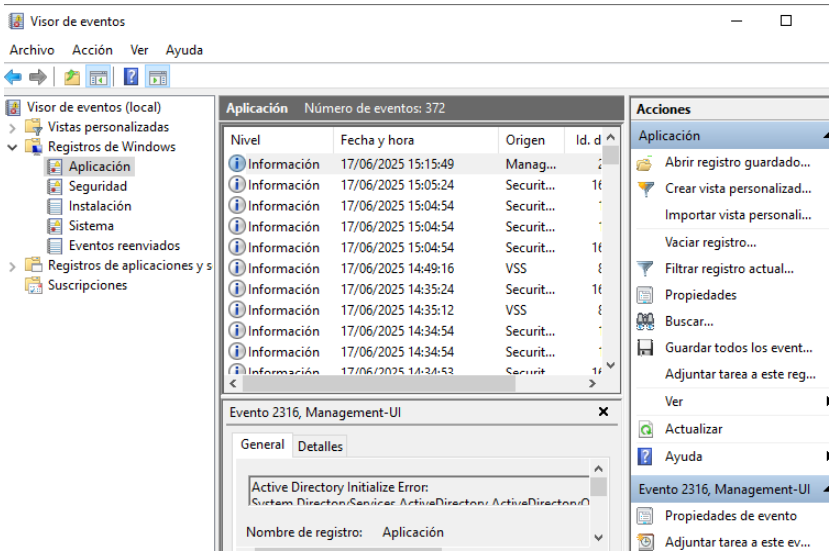


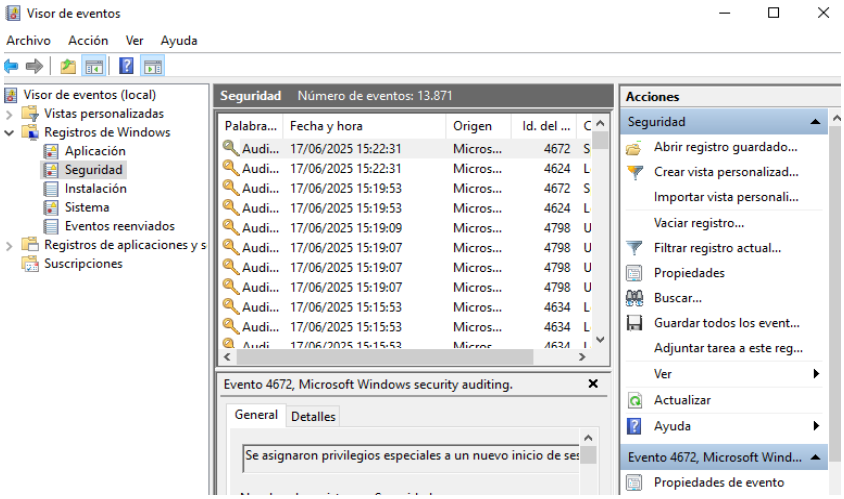


Para monitorear eventos:

Abre Visor de eventos (Event Viewer) desde el menú Herramientas.
Rutas importantes:
Registro de Windows > Sistema: Errores de hardware, servicios, etc.
Registro de Windows > Seguridad: Eventos de inicio de sesión, auditorías
Registro de aplicaciones: Problemas de software



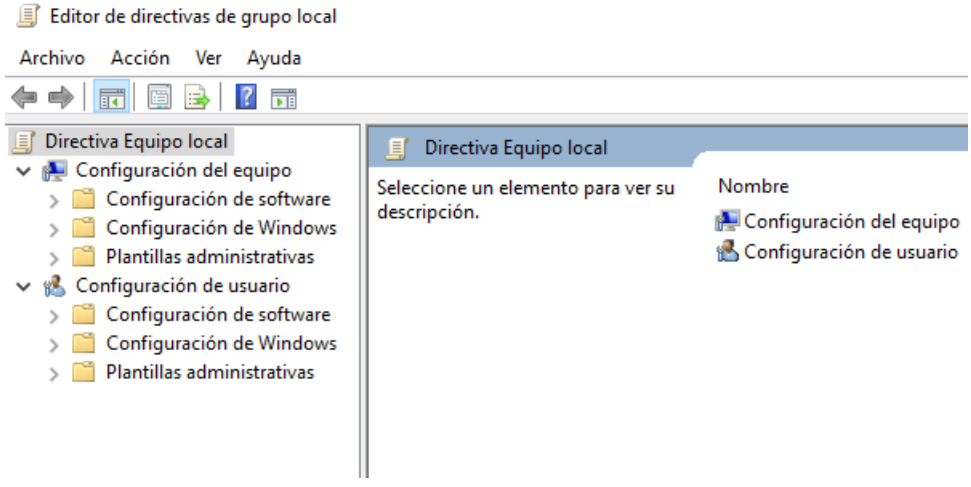




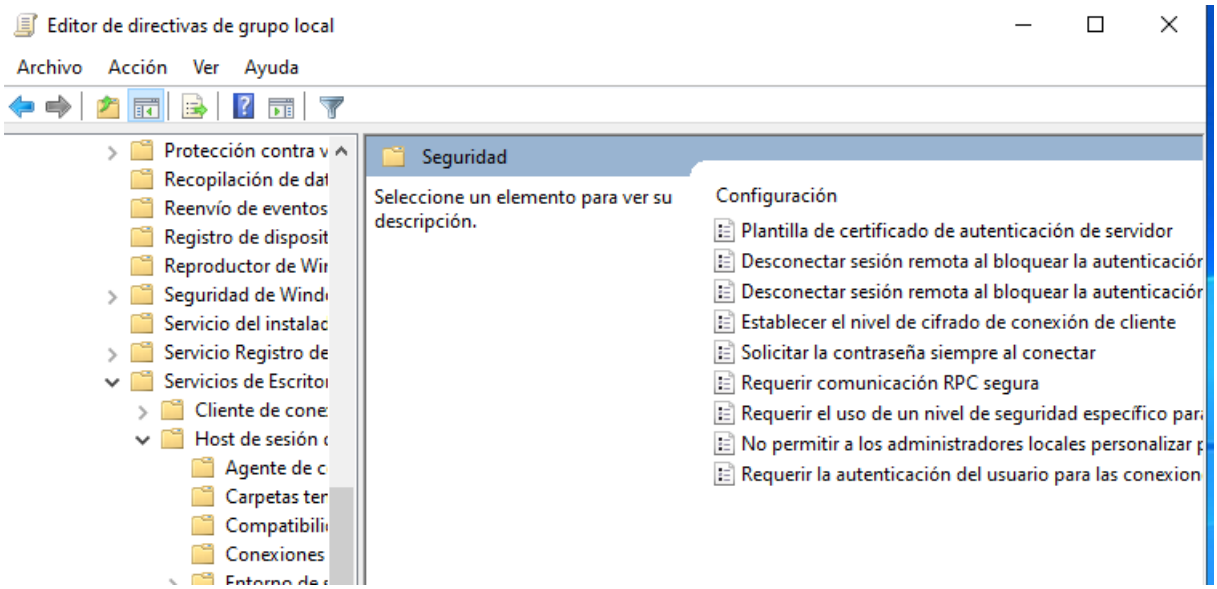
Fase 4: Seguridad y documentación

✅ Implementar políticas de seguridad para accesos remotos.
✅ Configurar reglas en el firewall para bloquear accesos no deseados.
✅ Documentar todas las configuraciones realizadas en un informe técnico.

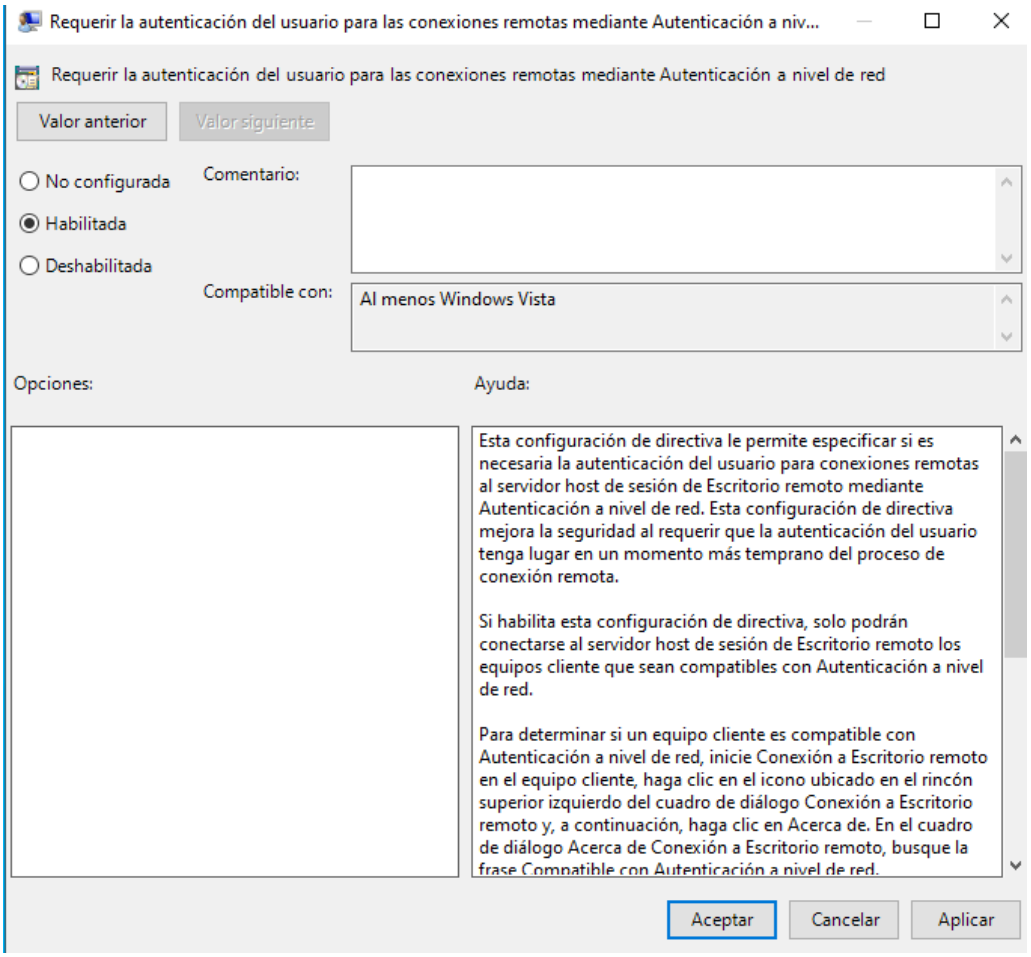
Implementar políticas de seguridad:
Abre gpedit.msc:



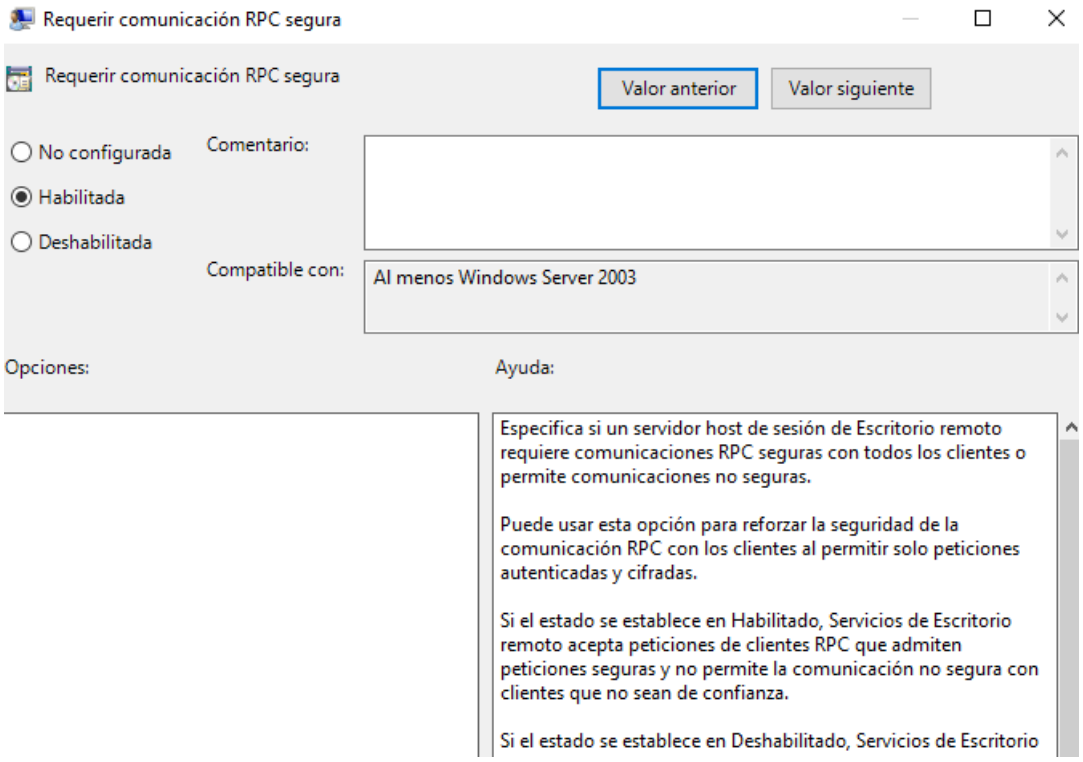
Navega a:
Configuración del equipo > Plantillas administrativas >
Componentes de Windows > Servicios de Escritorio remoto >
Host de sesión de Escritorio remoto > Seguridad



Configura las siguientes opciones:
Requerir autenticación de usuario para conexiones remotas usando NLA: Habilitado



Requerir comunicación RCP segura: Habilitado



Configurar reglas en el firewall para bloquear accesos no deseados:

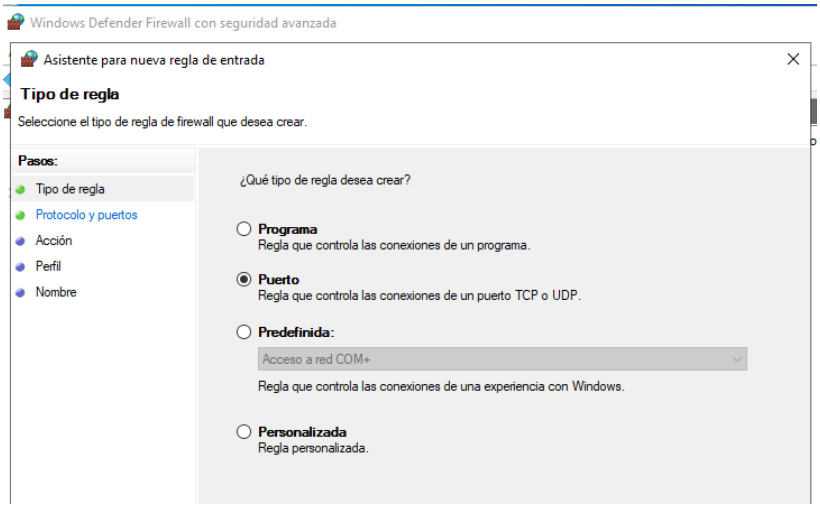
Usar Windows Defender Firewall con seguridad avanzada:

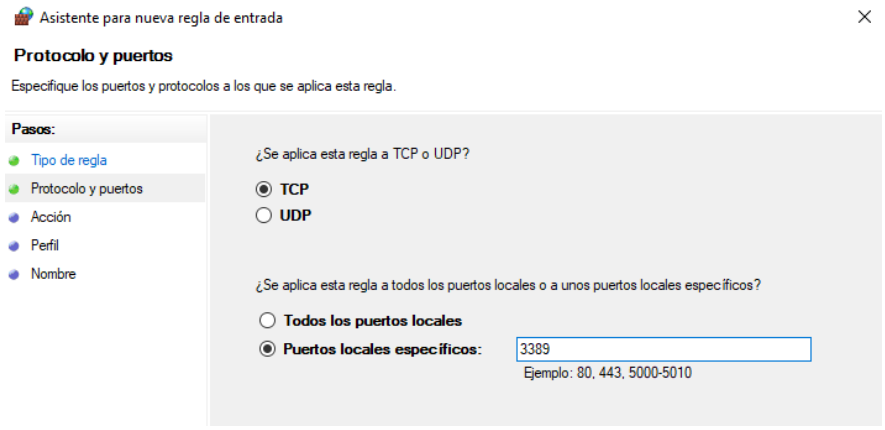
Abrir herramienta:
Ve a: Herramientas > Windows Defender Firewall con seguridad avanzada

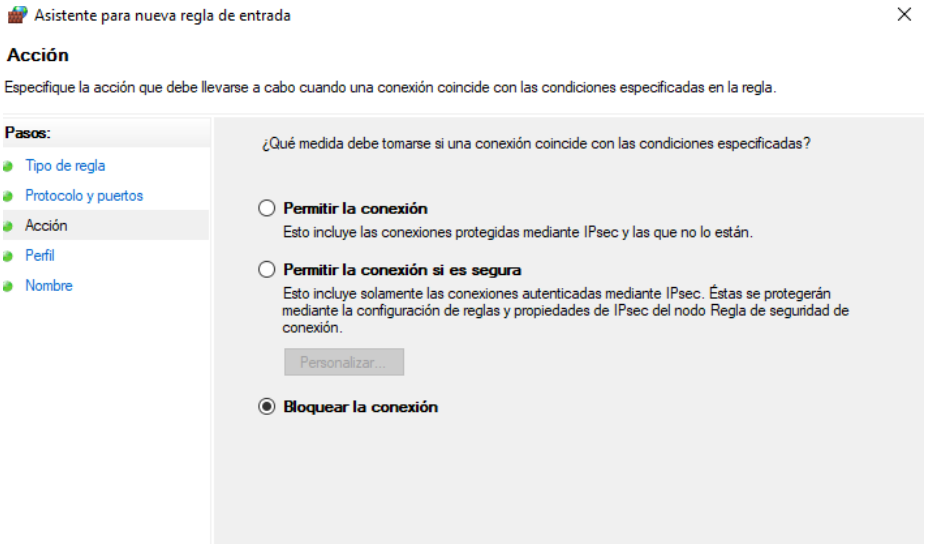
Crear reglas personalizadas:
1. En el panel izquierdo, selecciona Reglas de entrada > Nueva regla.

Tipo de regla: Puerto
Ejemplo: Bloquear el puerto 3389 (RDP) desde ciertas Ips.

Configuración:
Selecciona protocolo (TCP)
Puerto específico: 3389
Acción: Bloquear la conexión
Perfil: Dominio / Privado / Público (según corresponda)
Nombre: “Bloquear RDP desde IPs externas”


Windows Defender Firewall con seguridad avanzada
Asistente para nueva regla de entrada
Tipo de regla
Seleccione el tipo de regla de firewall que desea crear.
Pasos:
Tipo de regla
Protocolo y puertos
Acción
Perfil
Nombre
¿Qué tipo de regla desea crear?
Programa
Regla que controla las conexiones de un programa.
Puerto
Regla que controla las conexiones de un puerto TCP o UDP.
Predefinida:
Acceso a red COM+
Regla que controla las conexiones de una experiencia con Windows.
Personalizada
Regla personalizada.


Asistente para nueva regla de entrada
Protocolo y puertos
Especifique los puertos y protocolos a los que se aplica esta regla.
Pasos:
Tipo de regla
Protocolo y puertos
Acción
Perfil
Nombre
¿Se aplica esta regla a TCP o UDP?
TCP
UDP
¿Se aplica esta regla a todos los puertos locales o a unos puertos locales específicos?
Todos los puertos locales
Puertos locales específicos:
3389
Ejemplo: 80, 443, 5000-5010


Asistente para nueva regla de entrada
Acción
Especifique la acción que debe llevarse a cabo cuando una conexión coincide con las condiciones especificadas en la regla.
Pasos:
Tipo de regla
Protocolo y puertos
Acción
Perfil
Nombre
¿Qué medida debe tomarse si una conexión coincide con las condiciones especificadas?
Permitir la conexión
Esto incluye las conexiones protegidas mediante IPsec y las que no lo están.
Permitir la conexión si es segura
Esto incluye solamente las conexiones autenticadas mediante IPsec. Éstas se protegerán mediante la configuración de reglas y propiedades de IPsec del nodo Regla de seguridad de conexión.
Personalizar...
Bloquear la conexión

Informe Técnico:
1. Datos Generales
• Nombre del servidor: WIN-SERVER-Raul
• Dirección IP: 192.168.1.10
• Fecha de implementación: 17/06/2025
2. Usuarios y Grupos
• usuario1: Lectura (miembro de AdminsLectura)
• usuario2: Edición (miembro de AdminsEdicion)
• usuario3: Control total (miembro de AdminsTotales)
3. Roles y Herramientas Instaladas
• Servidor de archivos
• Acceso remoto (DirectAccess y VPN)
4. Políticas de Seguridad Aplicadas
• Autenticación mediante NLA habilitada
• Solo administradores autorizados pueden acceder por RDP
• Contraseñas seguras forzadas por GPO
5. Reglas de Firewall
Tipo Dirección Puerto Acción Detalles
Entrada TCP 3389 Bloquear Bloquea RDP desde IPs no autorizadas

Justificación de la mejora en seguridad y operatividad
1. Seguridad reforzada mediante control de acceso remoto
• Autenticación por red (NLA): Al requerir autenticación antes de establecer conexión RDP, se evita que atacantes puedan alcanzar la pantalla de inicio de sesión si no están autenticados, reduciendo significativamente los riesgos de ataques de fuerza bruta.
• Restricción de acceso RDP a usuarios autorizados: Minimiza la superficie de ataque, garantizando que solo el personal necesario tenga acceso al servidor.
• Bloqueo por firewall de accesos no deseados: Las reglas personalizadas permiten bloquear el tráfico desde direcciones IP no confiables o puertos innecesarios, previniendo accesos maliciosos.

2. Gestión eficiente mediante organización de usuarios y permisos
• Creación de usuarios estándar con permisos diferenciados: Se aplica el principio de mínimos privilegios, asegurando que cada usuario solo pueda realizar acciones estrictamente necesarias para su rol.
• Uso de grupos de seguridad: Centraliza la asignación de permisos, facilita la administración y reduce errores humanos al otorgar o quitar acceso.

3. Operatividad estable mediante roles esenciales y monitoreo
• Instalación controlada de roles (Servidor de archivos, Acceso remoto): Asegura que solo se implementen servicios necesarios, minimizando vulnerabilidades.
• Monitoreo activo con Event Viewer: Permite detectar rápidamente errores, fallos de hardware o intentos de acceso indebidos, facilitando una respuesta rápida.

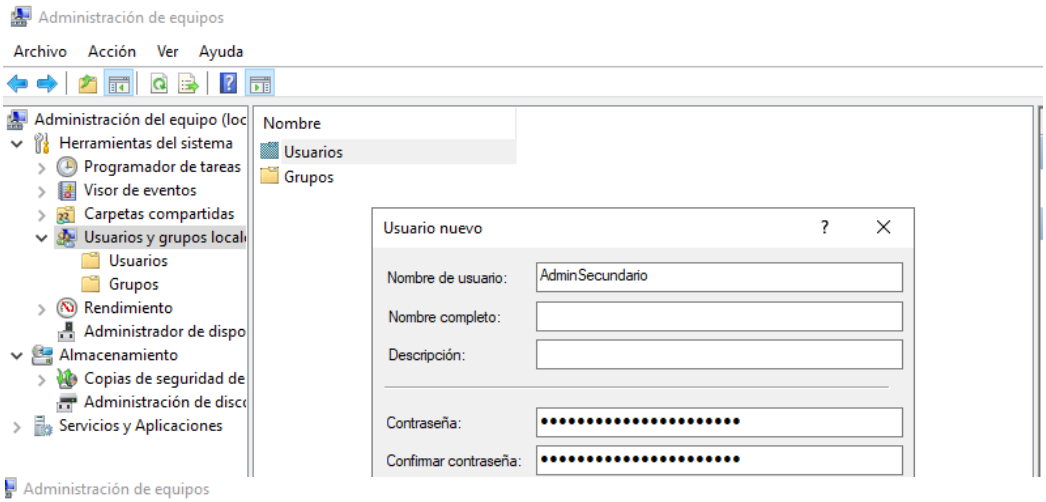
Conclusión
Esta configuración no solo fortalece la seguridad del servidor al reducir puntos vulnerables y controlar el acceso, sino que también mejora la operatividad mediante una gestión más ordenada y controlada, garantizando estabilidad, trazabilidad y facilidad de mantenimiento.

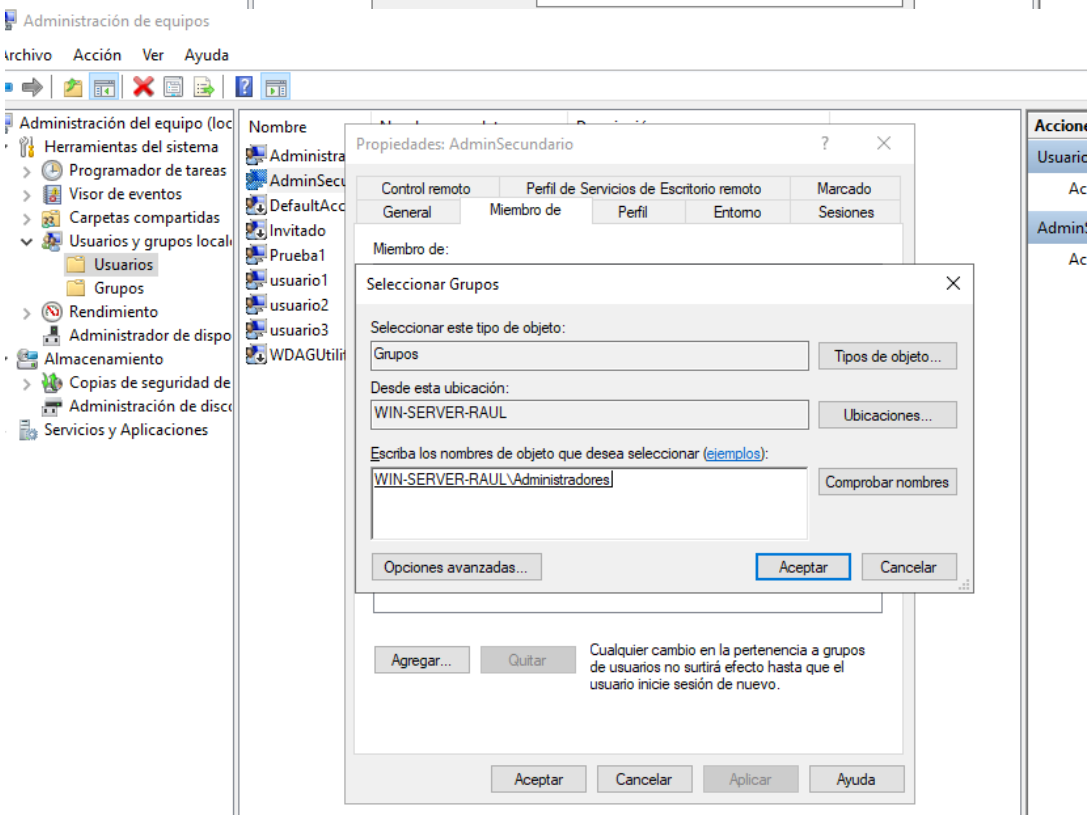
Fase 1: Preparación del entorno y consola administrativa
✅ Crear un usuario administrador secundario con una contraseña compleja.
✅ Configurar una directiva de seguridad local para que las contraseñas caduquen cada 30 días.
✅ Cambiar la configuración del Control de Cuentas de Usuario (UAC) para mayor control de privilegios.

Crear un usuario administrador secundario con una contraseña compleja:

Inicia sesión con una cuenta de administrador.
Abre Server Manager (Administrador del servidor).
Ve a Herramientas > Administración de equipos.
Herramientas del sistema > Usuarios y grupos locales > Usuarios.
Haz clic derecho en Usuarios y selecciona Nuevo usuario.
Completa los campos:
Nombre de usuario: Ej. AdminSecundario
Contraseña: Compleja
Haz clic en Crear.

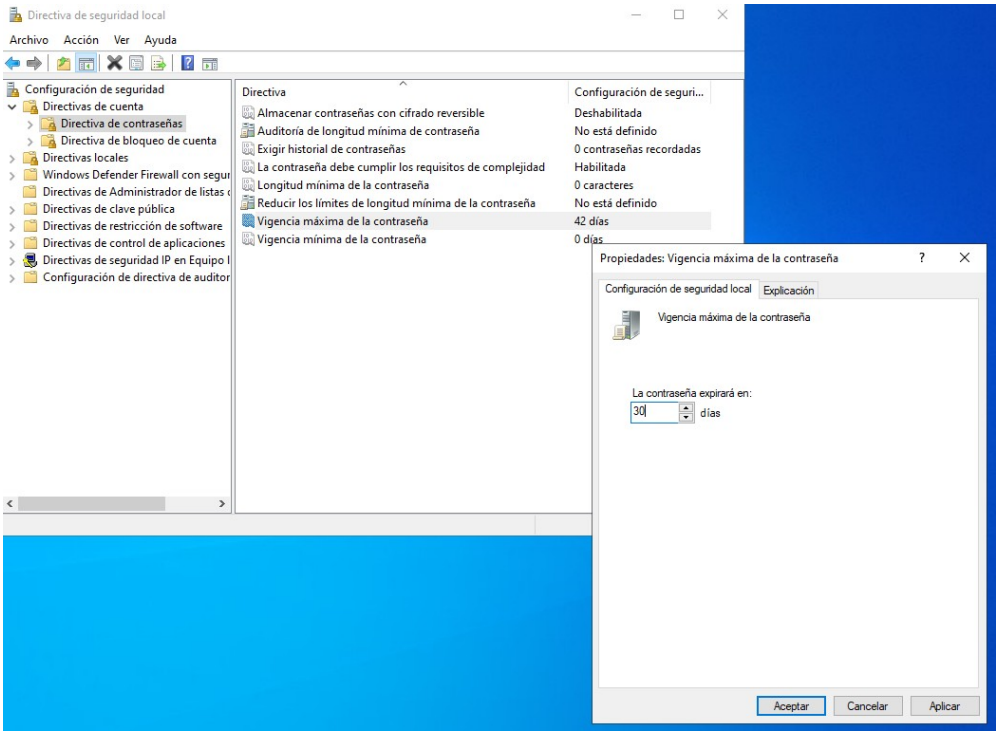
Luego, haz doble clic sobre el nuevo usuario, ve a la pestaña Miembro de, y añade el grupo Administradores para darle privilegios administrativos.





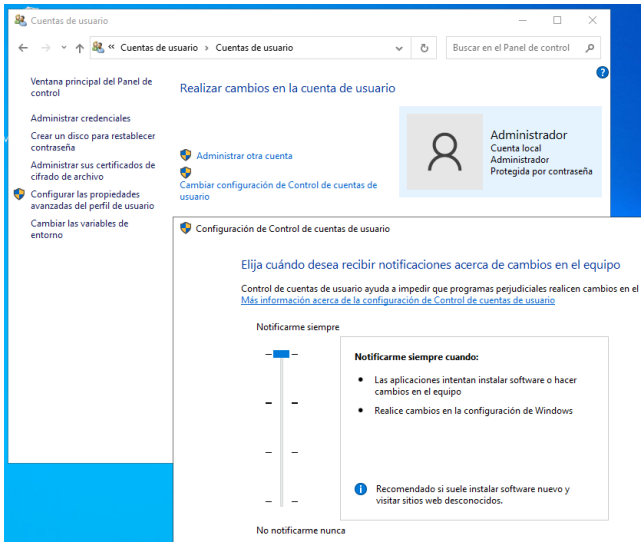
Configurar una directiva de seguridad local para que las contraseñas caduquen cada 30 días:

Abre el Administrador del servidor.
Ve a Herramientas > Directiva de seguridad local.
Directivas de cuenta > Directiva de contraseñas.
Vigencia máxima de la contraseña.
Haz doble clic, establece el valor en 30 días.
Haz clic en Aplicar y Aceptar.



Cambiar la configuración del Control de Cuentas de Usuario (UAC):

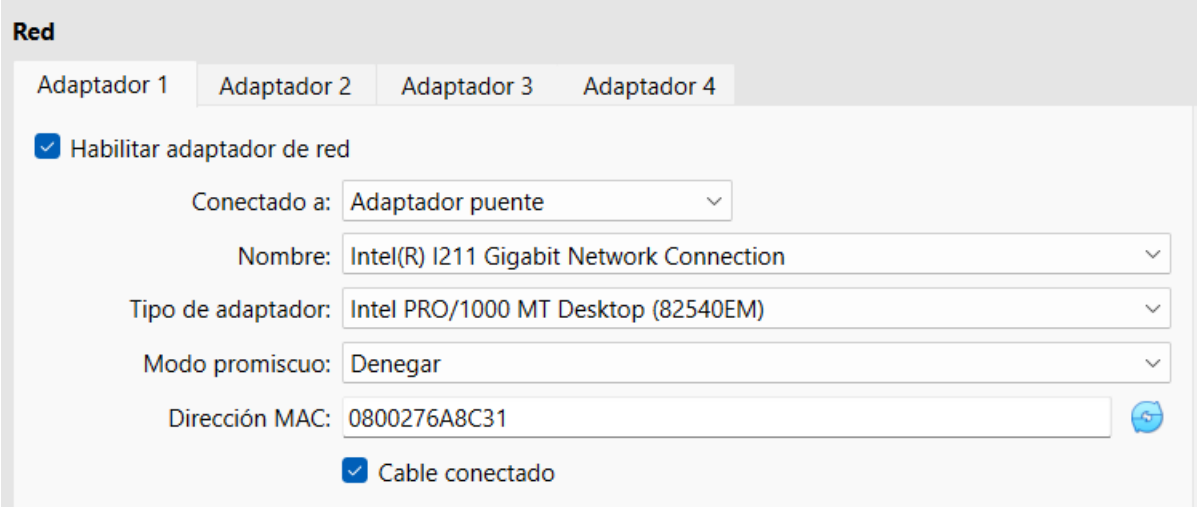
Abre el Panel de control.
Ve a Cuentas de usuario > Cambiar configuración de Control de cuentas de usuario.
Selecciona: Notificar siempre que las aplicaciones intenten instalar software o hacer cambios en el equipo.
Haz clic en Aceptar.

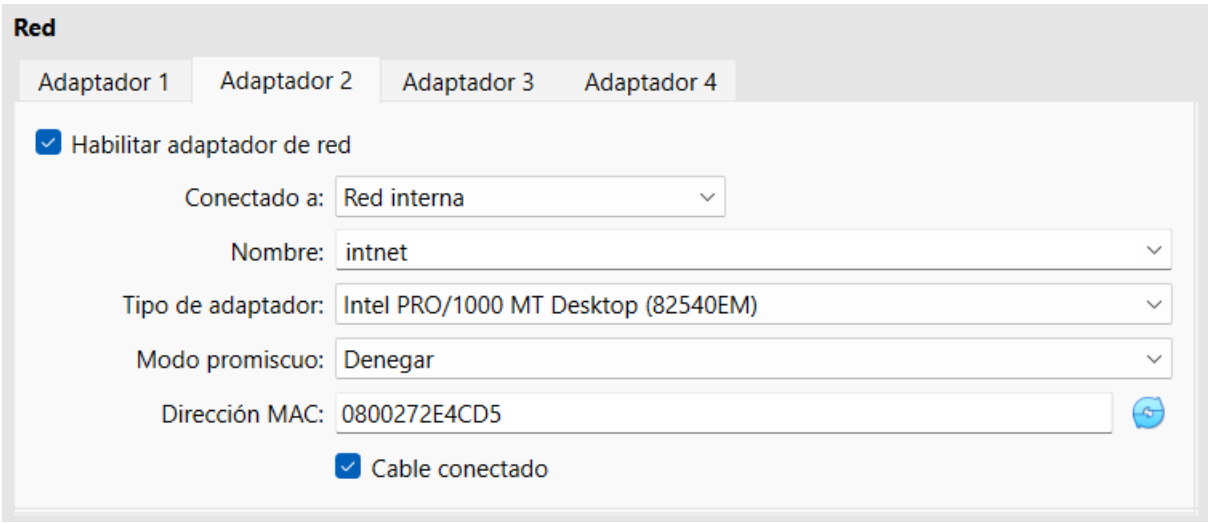


Fase 2: Ajustes de red y servicios
✅ Establecer dos tarjetas de red en la máquina virtual: una para conexión interna, otra para externa.
✅ Configurar rutas estáticas en la tabla de red para simular un entorno más complejo.
✅ Crear y activar un servidor DNS local, añadiendo una zona directa con al menos 2 registros.

Establecer dos tarjetas de red en la máquina virtual:

Tarjeta 1 (Externa): Conectada a una red externa (internet o puente con el host).
Tarjeta 2 (Interna): Conectada a una red interna (sin acceso a internet).



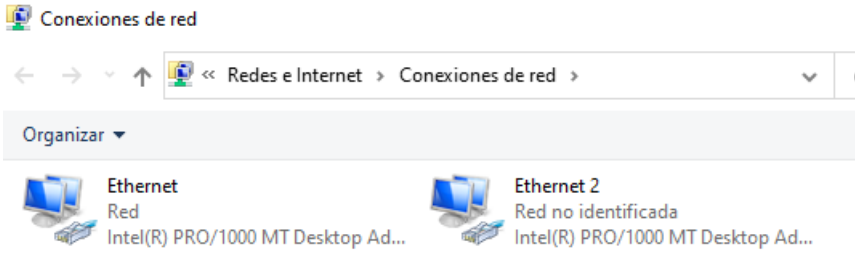


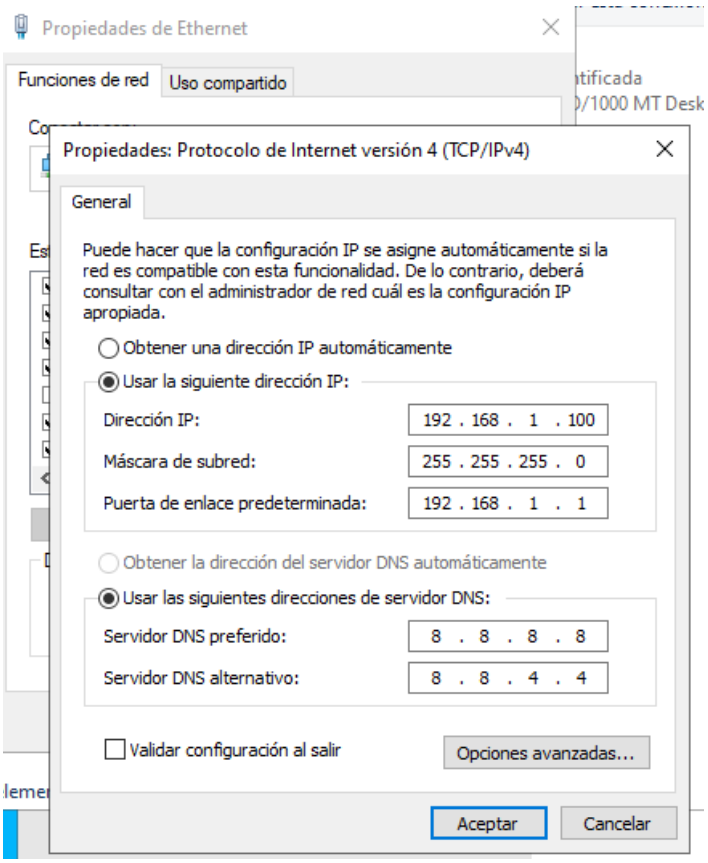
En Windows Server 2022:
Abre "Centro de redes y recursos compartidos" → Cambiar configuración del adaptador.
Verás dos interfaces de red, ej.: Ethernet 0 (externa) y Ethernet 1 (interna).
Asigna IPs manualmente:

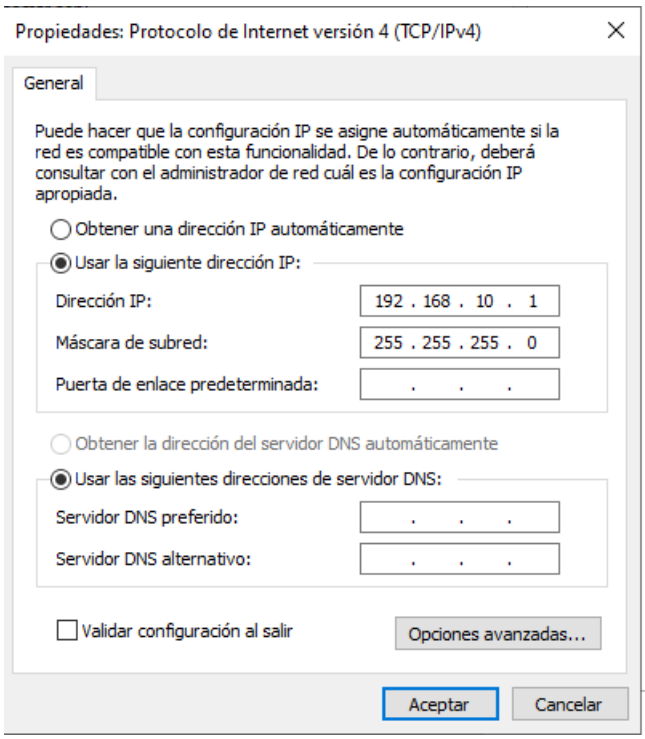
Externa (por DHCP o IP fija si es puenteada):
IP: 192.168.1.100
Máscara: 255.255.255.0
Puerta de enlace: 192.168.1.1

DNS: 8.8.8.8

Interna (IP fija):
IP: 192.168.10.1
Máscara: 255.255.255.0
Puerta de enlace: (dejar en blanco)
DNS: (dejar en blanco)



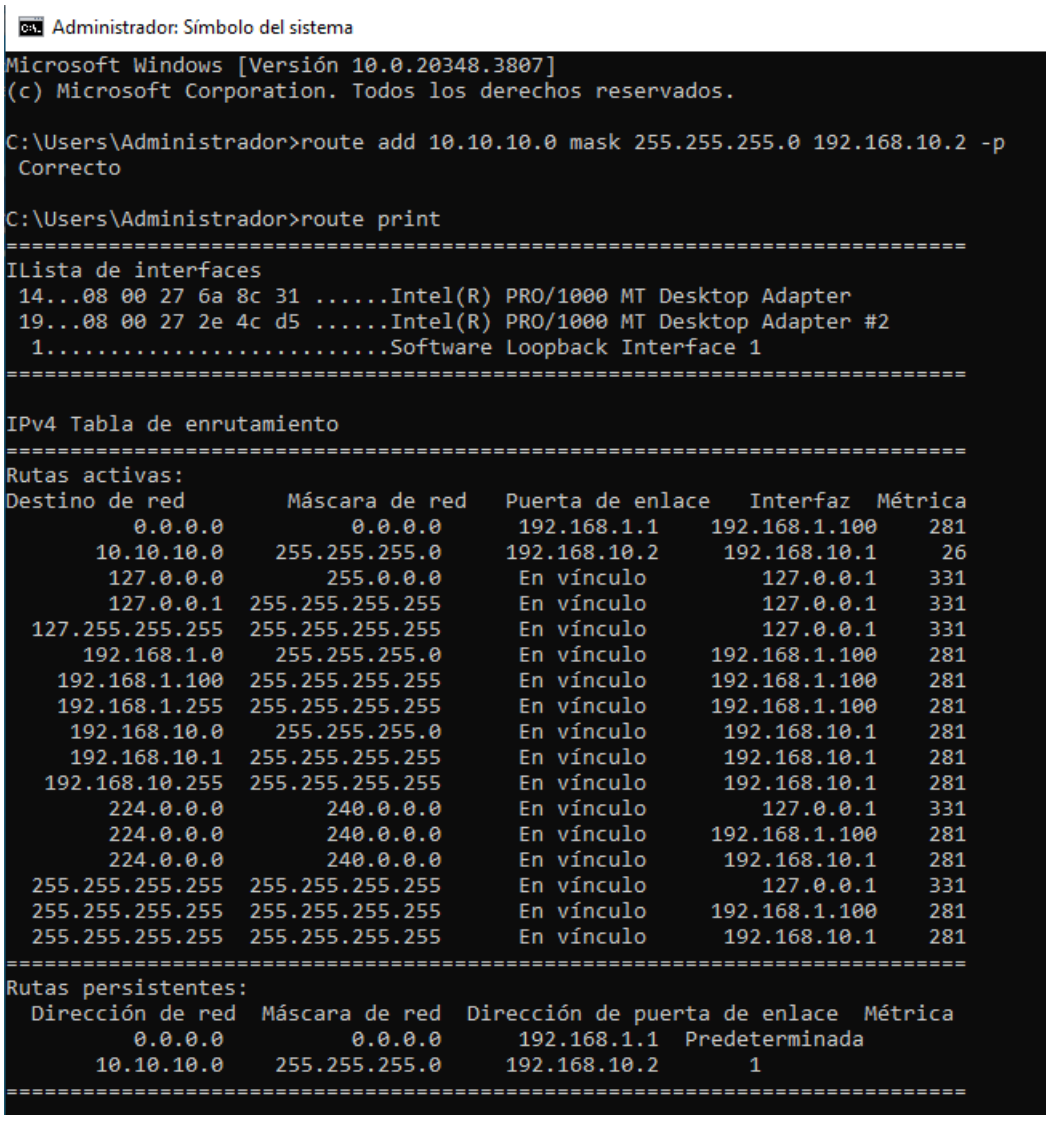




Configurar rutas estáticas:

Abre símbolo del sistema como administrador y usa el comando route add:
route add 10.10.10.0 mask 255.255.255.0 192.168.10.2 -p
Esto indica: "Para llegar a la red 10.10.10.0/24, usa 192.168.10.2 como gateway".
Route print-p hace la ruta persistente tras reinicios.

Para ver la tabla de rutas:
route print



Crear y activar un servidor DNS local con zona directa:

Instalar rol de DNS Server:

Abre Administrador del servidor, Agregar roles y características.
Selecciona:
Rol: Servidor DNS

Crear una zona directa:
Abre DNS Manager (dnsmgmt.msc).
Botón derecho sobre Zonas de búsqueda directa → Nueva zona…

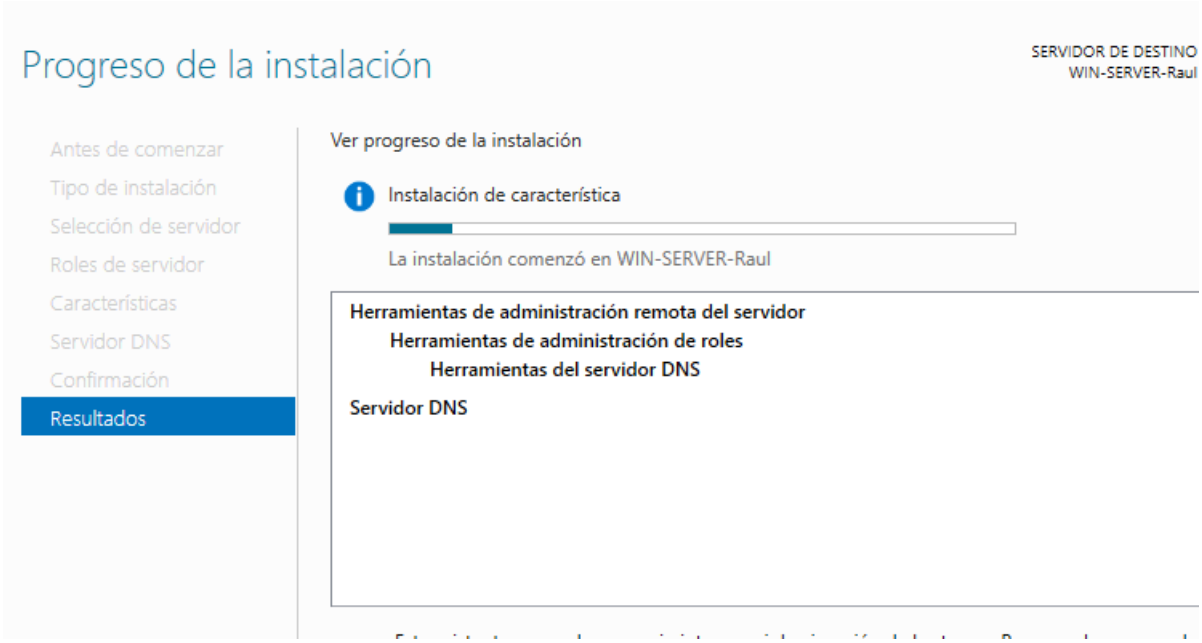
Tipo: Principal
Nombre de zona: por ejemplo, midominio.local
Crear nuevo archivo de zona.
Permitir sólo actualizaciones seguras (si estás en dominio) o no seguras.

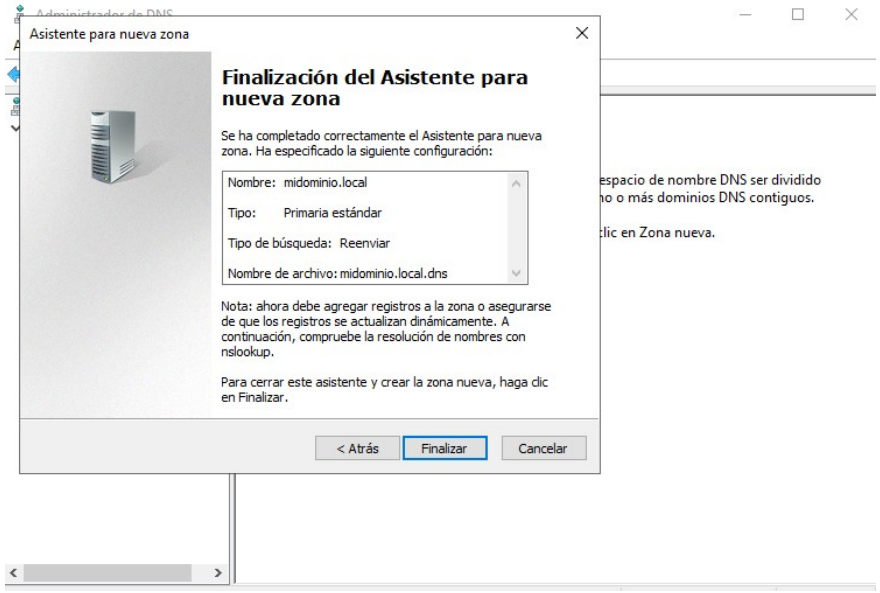
Agregar al menos 2 registros:

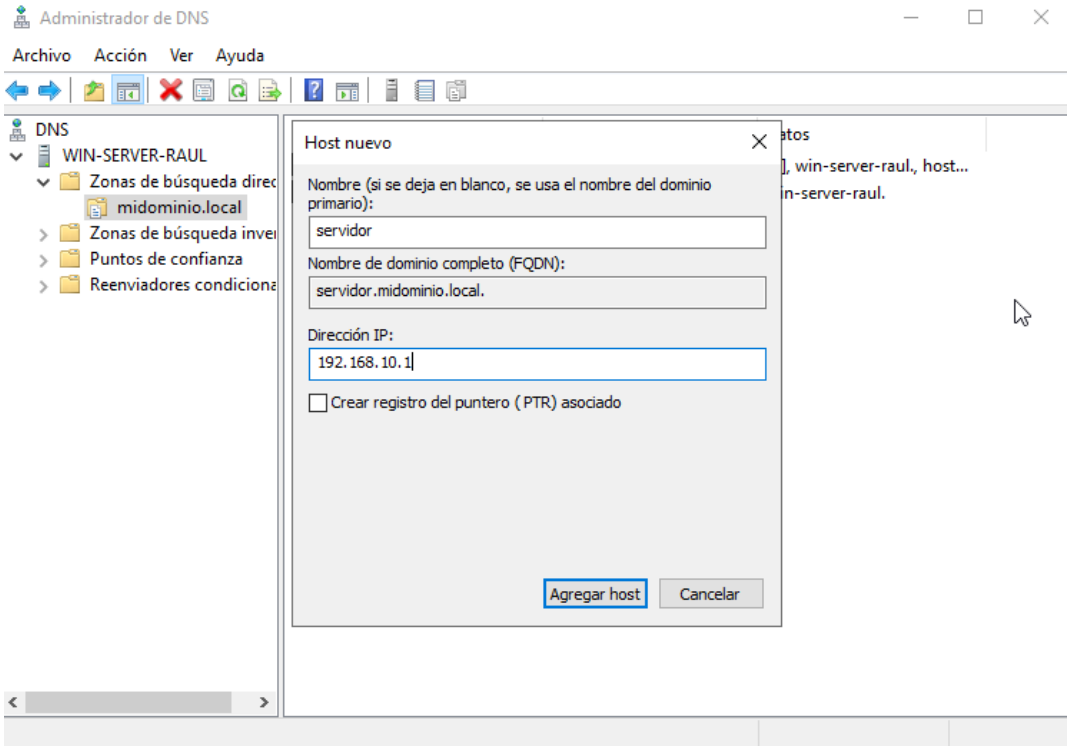
En la zona midominio.local, clic derecho, Nuevo host (A o AAAA)…
Nombre: servidor
IP: 192.168.10.1

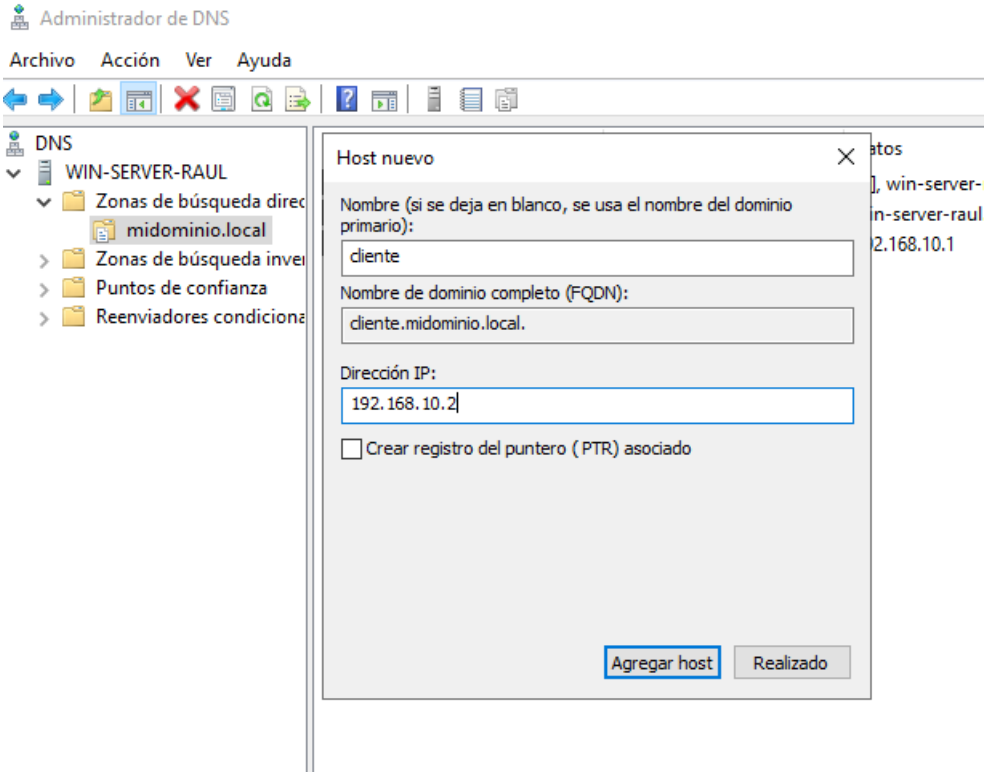
Repite para otro host:
Nombre: cliente
IP: 192.168.10.2

Ahora puedes hacer ping desde otra máquina conectada a la red interna:
ping servidor.midominio.local









Fase 3: Personalización del entorno de trabajo del servidor

✅ Habilitar el Escritorio Remoto y limitar el número de sesiones a 2.

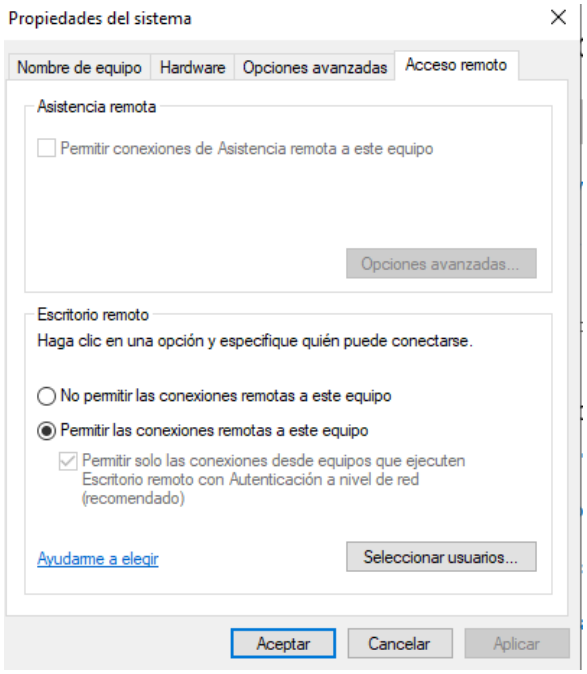
✅ Personalizar el inicio del sistema añadiendo un script que cree automáticamente una carpeta de logs en C:\Logs.

✅ Configurar el firewall para que solo permita el tráfico RDP y DNS.

Habilitar el Escritorio Remoto y limitar a 2 sesiones:

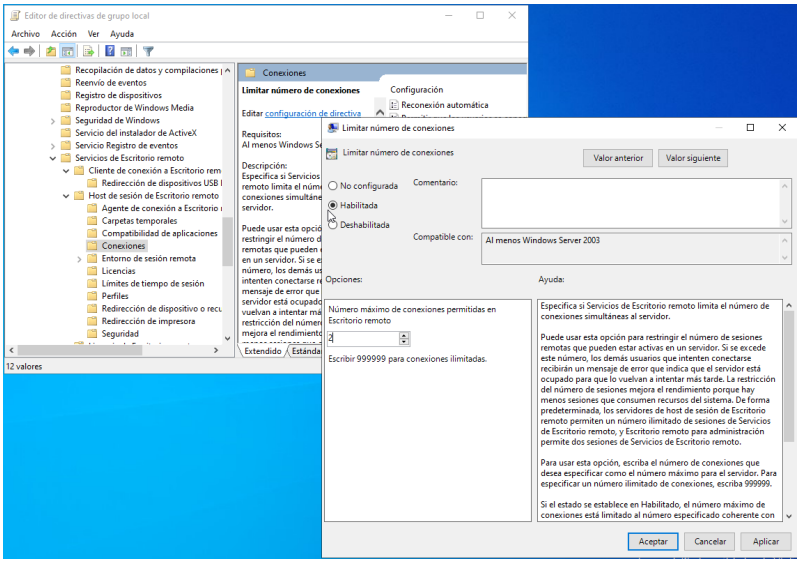
Habilitar Escritorio Remoto:

Ve a Configuración del sistema:
Clic derecho en Este equipo, Propiedades.
Selecciona Configuración remota.
Marca Permitir conexiones remotas a este equipo.



Limitar sesiones RDP a 2:

Abre el Editor de directivas de grupo local: gpedit.msc
Configuración del equipo, Plantillas administrativas, Componentes de Windows, Servicios de Escritorio remoto, Host de sesión de Escritorio remoto, Conexiones
Limitar el número de conexiones: Habilitado, 2 sesiones

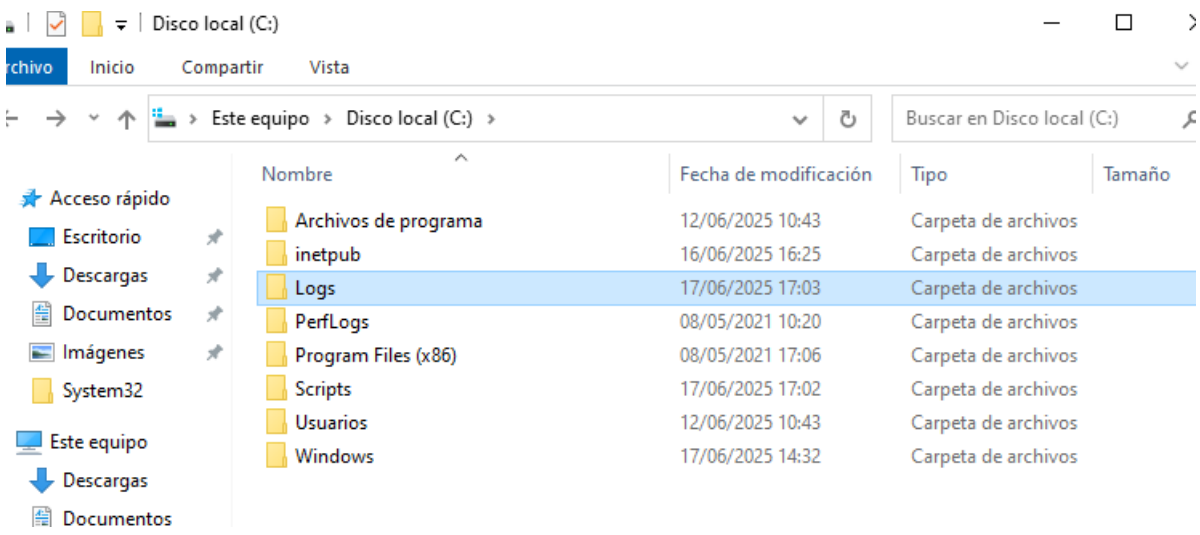


Script de inicio que crea una carpeta de logs en C:\Logs:

Crear el script:

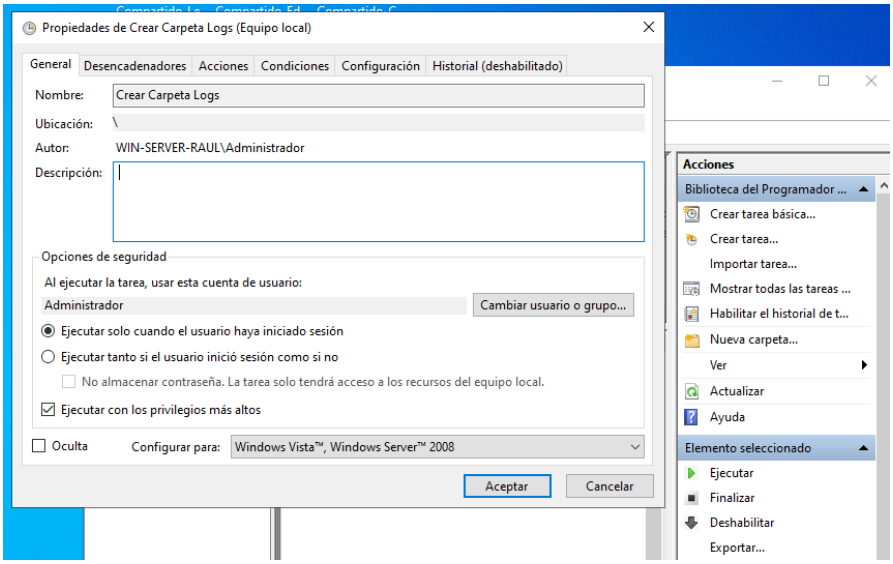
Abre Bloc de notas, escribe lo siguiente:
if (!(Test-Path -Path "C:\Logs")) { New-Item -Path "C:\Logs" -ItemType Directory}

Guarda como: CrearLogs.ps1



Ejecutarlo al inicio del sistema:

Abre el Programador de tareas.
Crea una nueva tarea:
Nombre: Crear Carpeta Logs
Desencadenador: Al iniciar el sistema
Acción: Ejecutar programa: "C:\Scripts\CrearLogs.ps1"
Condiciones: Desactiva "Iniciar solo si está en corriente alterna"
General: Ejecutar con privilegios más altos.

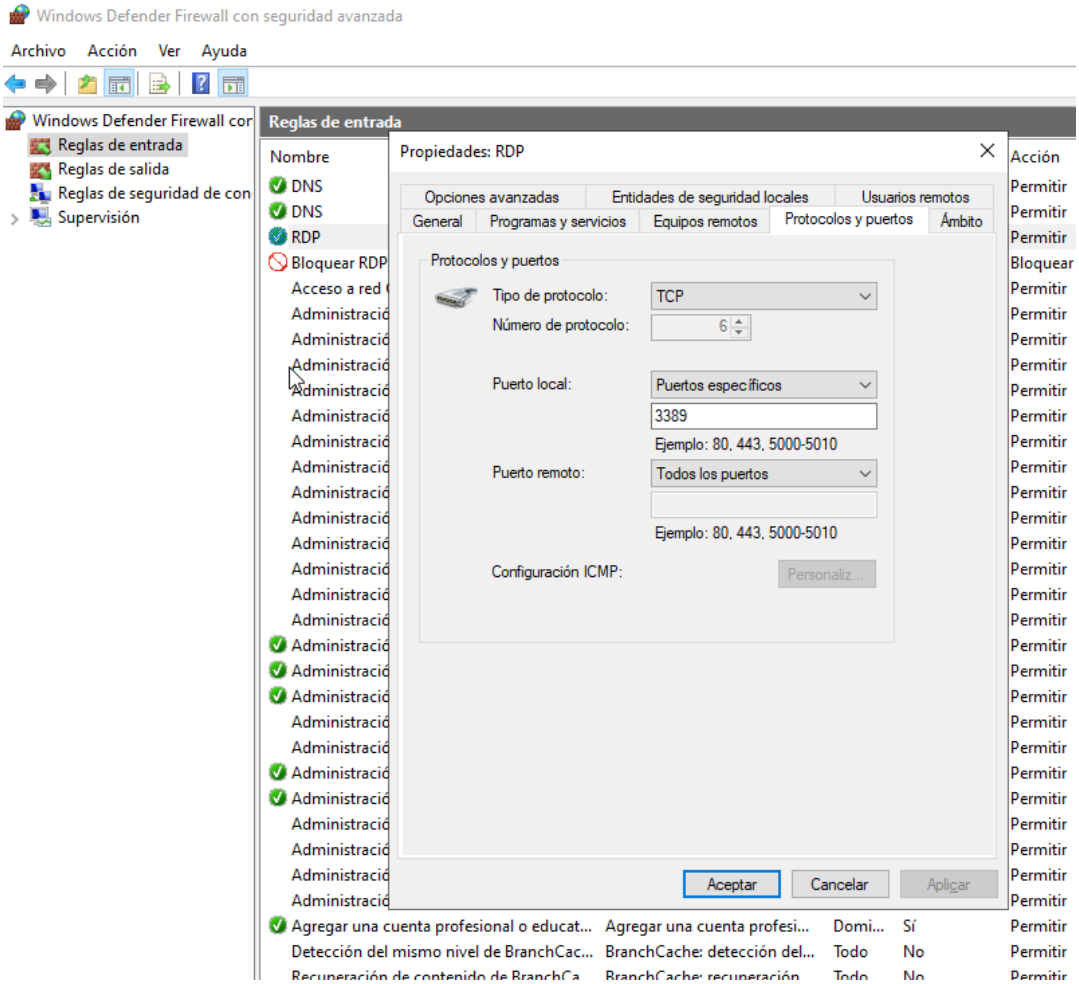


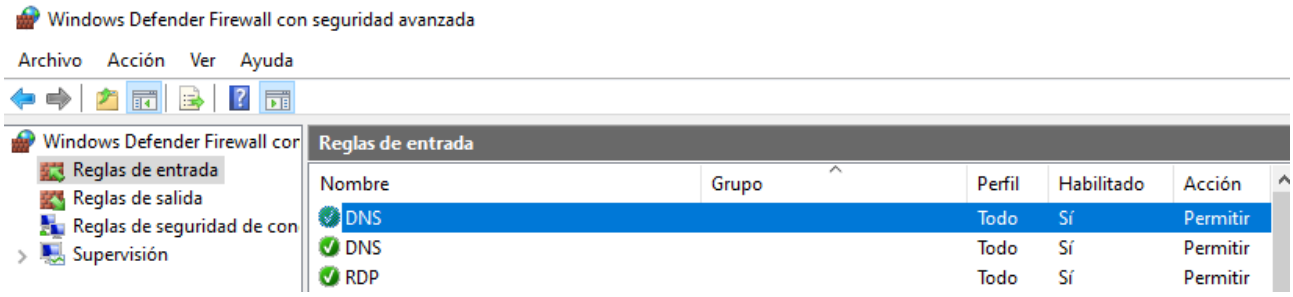
Configurar el firewall para permitir solo RDP y DNS:

Permitir solo RDP y DNS:

Acceder al Firewall de Windows con Seguridad Avanzada:
Busca "Firewall de Windows con seguridad avanzada" en el menú Inicio y ábrelo.

Crear una nueva regla de entrada:
En el panel izquierdo, selecciona "Reglas de entrada".
Haz clic en "Nueva regla..." en el panel derecho.
Seleccionar el tipo de regla:
Elige "Puerto" y haz clic en "Siguiente".
Especificar el protocolo y puerto:
Selecciona "TCP" y luego "Puertos locales específicos".
Introduce "3389" para RDP.
Selecciona "UDP" y luego "Puertos locales específicos".
Introduce "53" para DNS.
Selecciona "TCP" y luego "Puertos locales específicos".
Introduce "53" para DNS.
Haz clic en "Siguiente".
Definir la acción:
Selecciona "Permitir la conexión" y haz clic en "Siguiente".



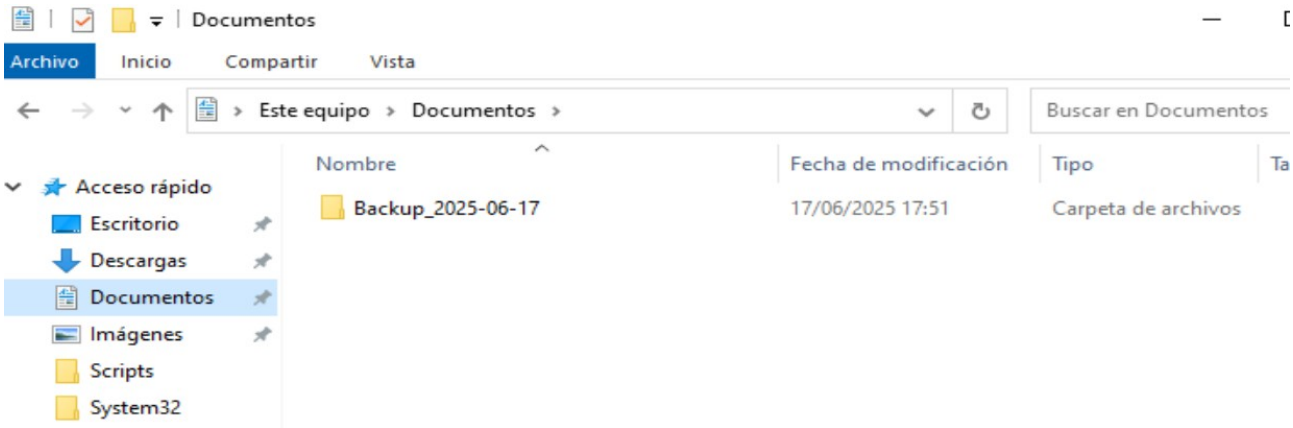


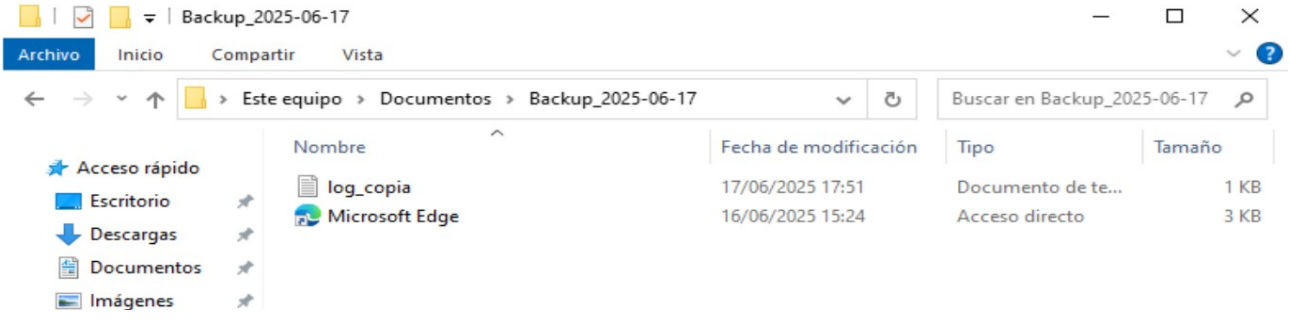
Fase 4: Automatización básica

✅ Crear un script en PowerShell que realice las siguientes tareas:

•Cree una carpeta con la fecha actual.
•Copie archivos del escritorio a esa carpeta.
•Genere un log en .txt con el resultado de la copia.

```
PS C:\Users\Administrador> # Obtener la fecha actual en formato yyyy-MM-dd
>> $fecha = Get-Date -Format "yyyy-MM-dd"
>>
>> # Definir la ruta del escritorio del usuario actual
>> $escritorio = [Environment]::GetFolderPath("Desktop")
>>
>> # Definir la carpeta de destino en Documentos
>> $destinoRaiz = "$HOME\Documents\Backup_$fecha"
>> New-Item -ItemType Directory -Path $destinoRaiz -Force | Out-Null
>>
>> # Definir la ruta del archivo de log
>> $logPath = "$destinoRaiz\log_copia.txt"
>>
>> # Obtener los archivos del escritorio (no carpetas)
>> $archivos = Get-ChildItem -Path $escritorio -File
>>
>> # Inicializar contenido del log
>> Add-Content -Path $logPath -Value "==== LOG DE COPIA - $fecha ===="
>>
>> # Copiar archivos y registrar resultados
>> foreach ($archivo in $archivos) {
>>     try {
>>         Copy-Item -Path $archivo.FullName -Destination $destinoRaiz -Force
>>         Add-Content -Path $logPath -Value "Copiado: $($archivo.Name)"
>>     } catch {
>>         Add-Content -Path $logPath -Value "ERROR al copiar: $($archivo.Name) - $($_.Exception.Message)"
>>     }
>> }
```




Backup_2025-06-17
Archivo
Inicio
Compartir
Vista
Este equipo
Documentos
Backup_2025-06-17
Buscar en Backup_2025-06-17
Acceso rápido
Escritorio
Descargas
Documentos
Imágenes
Nombre
Fecha de modificación
Tipo
Tamaño
log_copia
17/06/2025 17:51
Documento de te...
1 KB
Microsoft Edge
16/06/2025 15:24
Acceso directo
3 KB


log_copia: Bloc de notas
Archivo Edición Formato Ver Ayuda
==== LOG DE COPIA - 2025-06-17 ====
Copiado: dsxfh.txt
Copiado: Microsoft Edge.lnk
==== LOG DE COPIA - 2025-06-17 ====
Copiado: Microsoft Edge.lnk