

# Configuración avanzada de Windows Server

Este documento consta con todos los pasos a seguir para realizar la configuración avanzada de windows con los siguientes parámetros:

## 1. Preparación del entorno y consola administrativa.

- **Creación de un usuario administrador secundario con contraseña compleja.**
- **Directiva de seguridad local:** Las contraseñas caducan a los 30 días.
- **Configuración de Control de Cuentas de Usuario (UAC):** Mayor control de privilegios.

## 2. Ajustes de red y servicios.

- **Dos tarjetas de red:** Una con conexión interna y otra para externa.
- **Configurar rutas estáticas:** Para simular un entorno más complejo.
- **Crear y activar un servidor DNS local:** Con al menos 2 registros.

## 3. Personalización del entorno de trabajo.

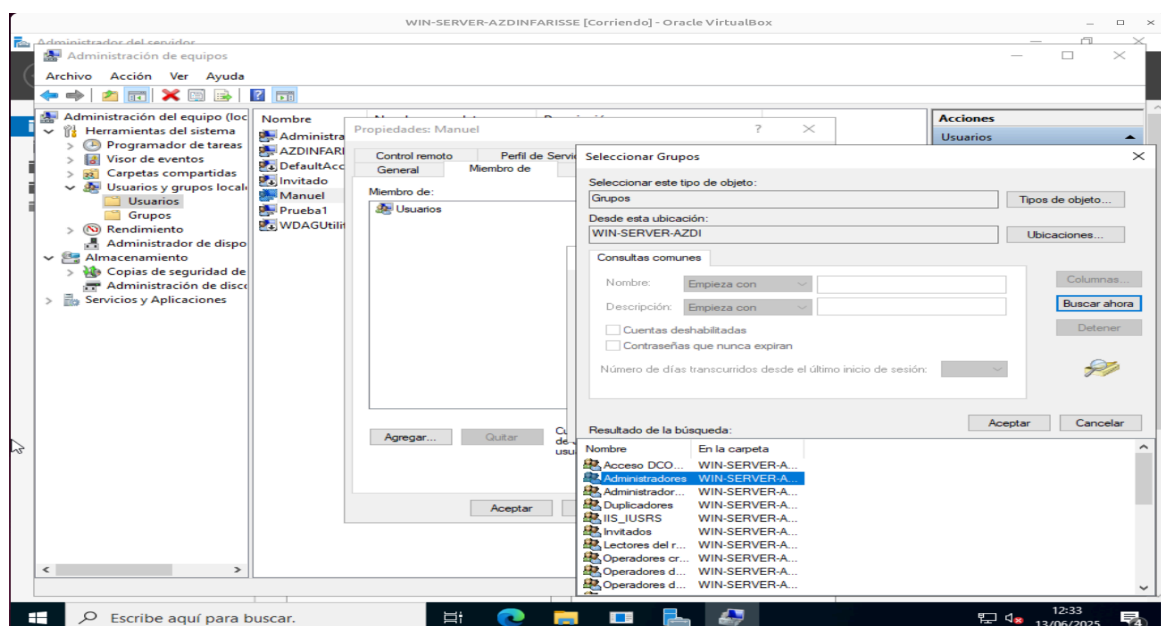
- **Habilitar Escritorio Remoto:** Limitado a 2 sesiones.
- **Personalizar el inicio del sistema:** Añadir un script que cree automáticamente una carpeta de logs en C:/Logs.
- **Configurar firewall:** Solo tráfico RDP Y DNS.

## 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.


Ahora que ya tenemos claros los parámetros, procedemos a la configuración de nuestro Windows Server.

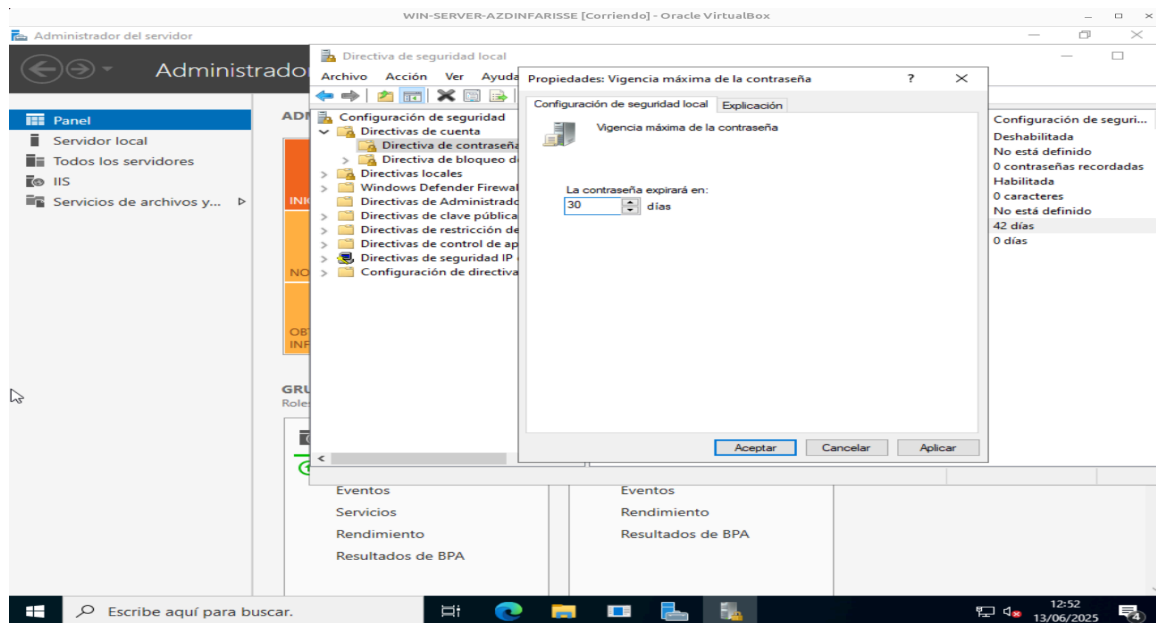
---



Lo siguiente es crear una directiva de seguridad local para que las contraseñas caduquen cada 30 días, por lo que nos dirigiremos a:

**Administrador del servidor→ Herramientas→Directiva de seguridad local→Directivas de cuenta→Directiva de contraseñas.**

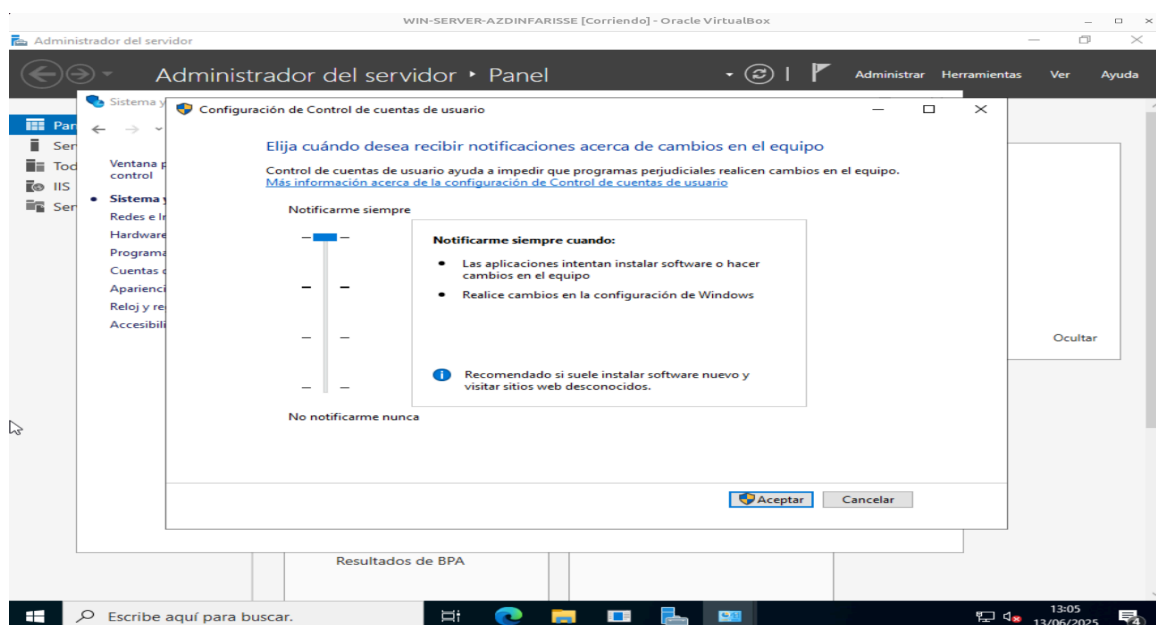
Seleccionamos  **Vigencia máxima de la contraseña** y la modificamos a 30 días.



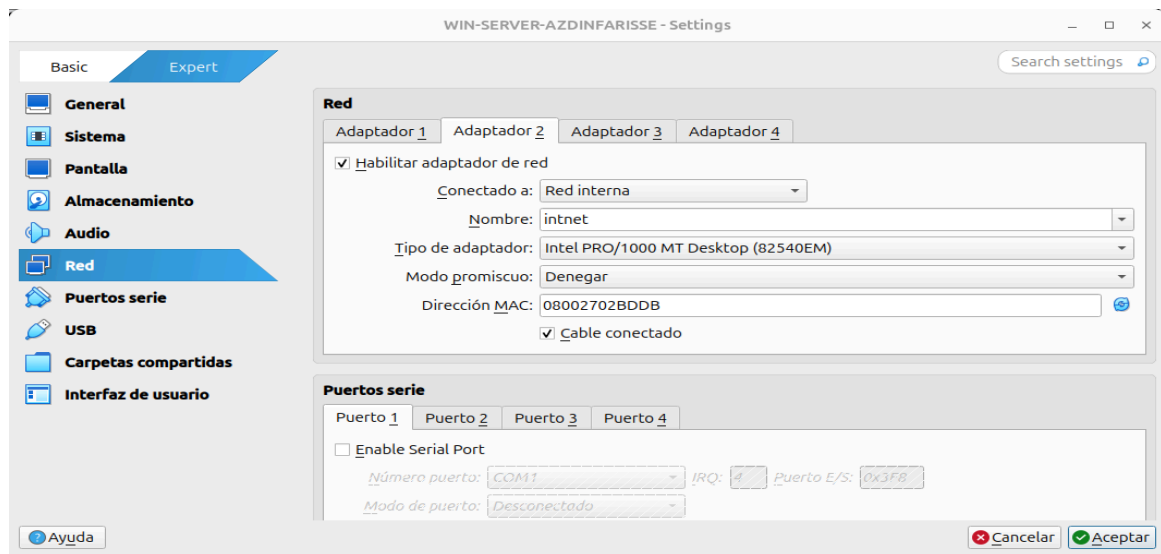
Ahora vamos a cambiar la configuración de Control de Cuentas de Usuario (UAC) dirigiendonos a:

**Panel de control→Sistema y seguridad→Cambiar configuración de Control de cuentas de usuario.**

Ahora podemos aumentar el nivel de control, estableciendo en notificarme siempre, para así tener un control mayor de los privilegios.



El siguiente paso es configurar una segunda tarjeta de red para la conexión interna. Para ello apagamos la máquina y nos dirigimos a la configuración de la misma, en el apartado de red y configuramos el adaptador 2 en red interna.



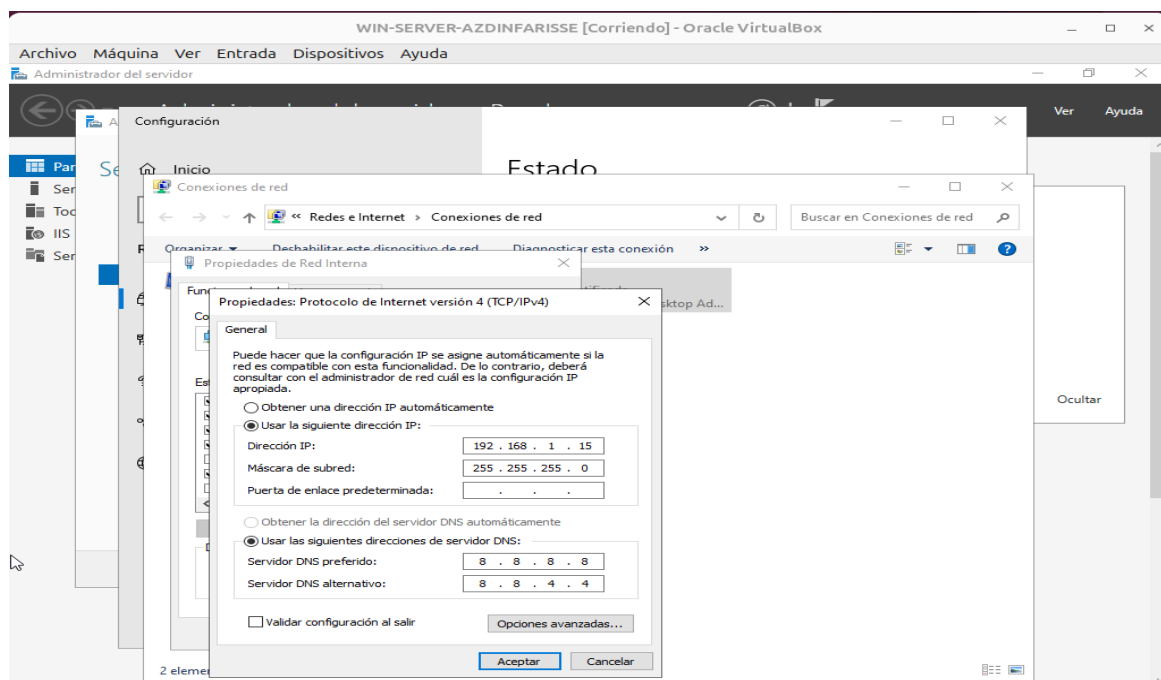
Una vez establecido el segundo adaptador, encendemos la máquina nuevamente y vamos a configurar la ip de la red interna.

**IP:** 192.168.1.15

**Máscara de subred:** 255.255.255.0

**Puerta de enlace predeterminada:** /

**DNS:** 8.8.8.8 / 8.8.4.4



Ahora que ya tenemos nuestra Red Interna configurada, vamos a configurar 2 rutas estáticas en la tabla de red con las siguientes ips:

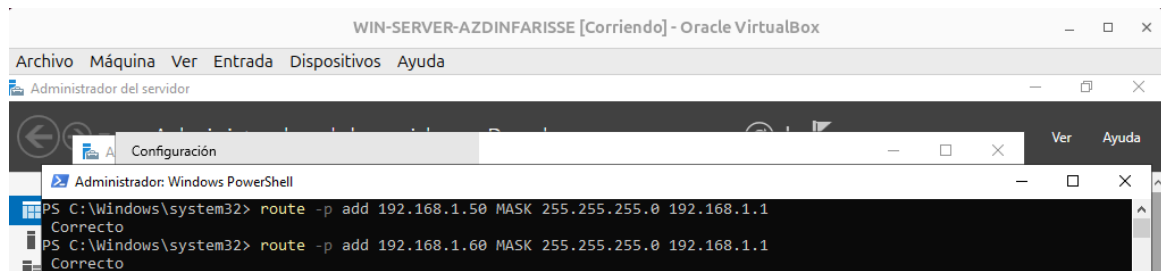
192.168.1.50

192.168.1.60

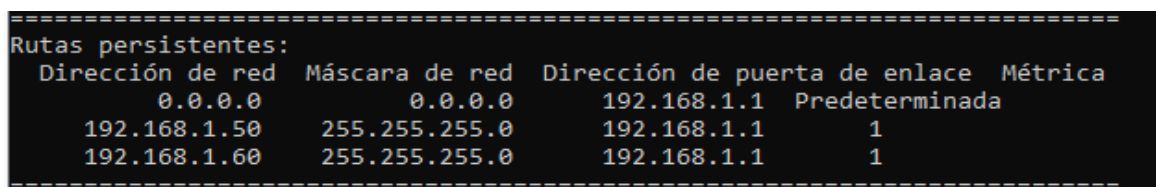
Para ello nos dirigimos al CMD e introducimos los siguientes comandos:

***route -p add 192.168.1.50 MASK 255.255.255.0 192.168.1.1***

***route -p add 192.168.1.60 MASK 255.255.255.0 192.168.1.1***

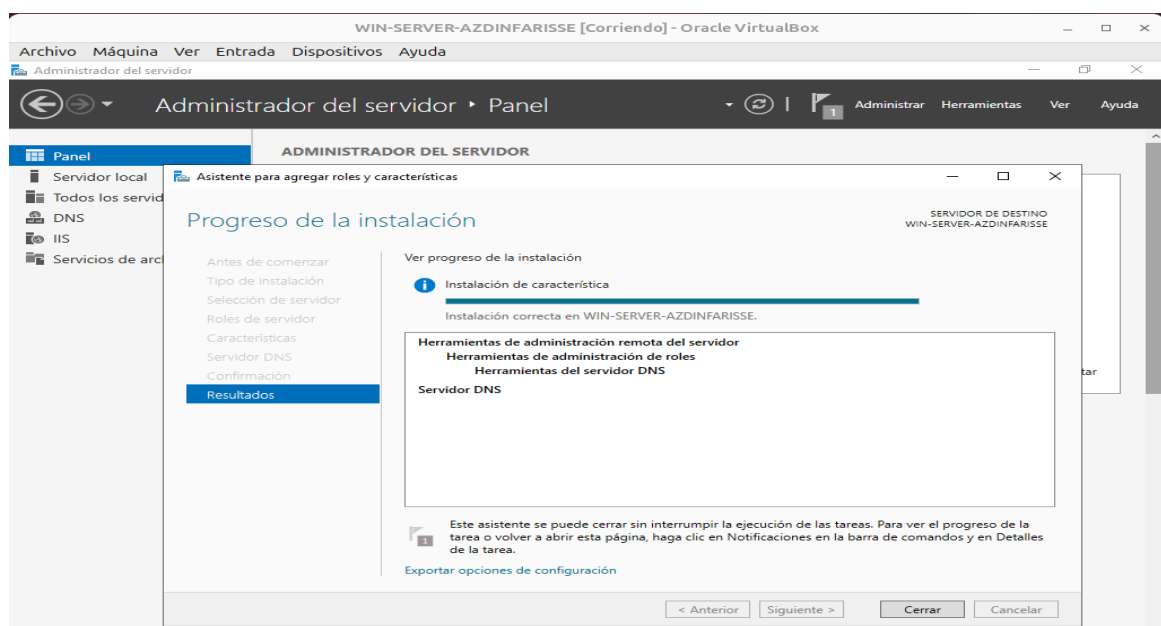


***route print:*** para asegurarnos que se han añadido con éxito.



Ahora crearemos y activaremos un **servidor DNS local** y le añadiremos una zona directa con al menos 2 registros. Para ello nos dirigimos a nuestro **Administrador del servidor** → **Panel** → **Agregar roles y características**.

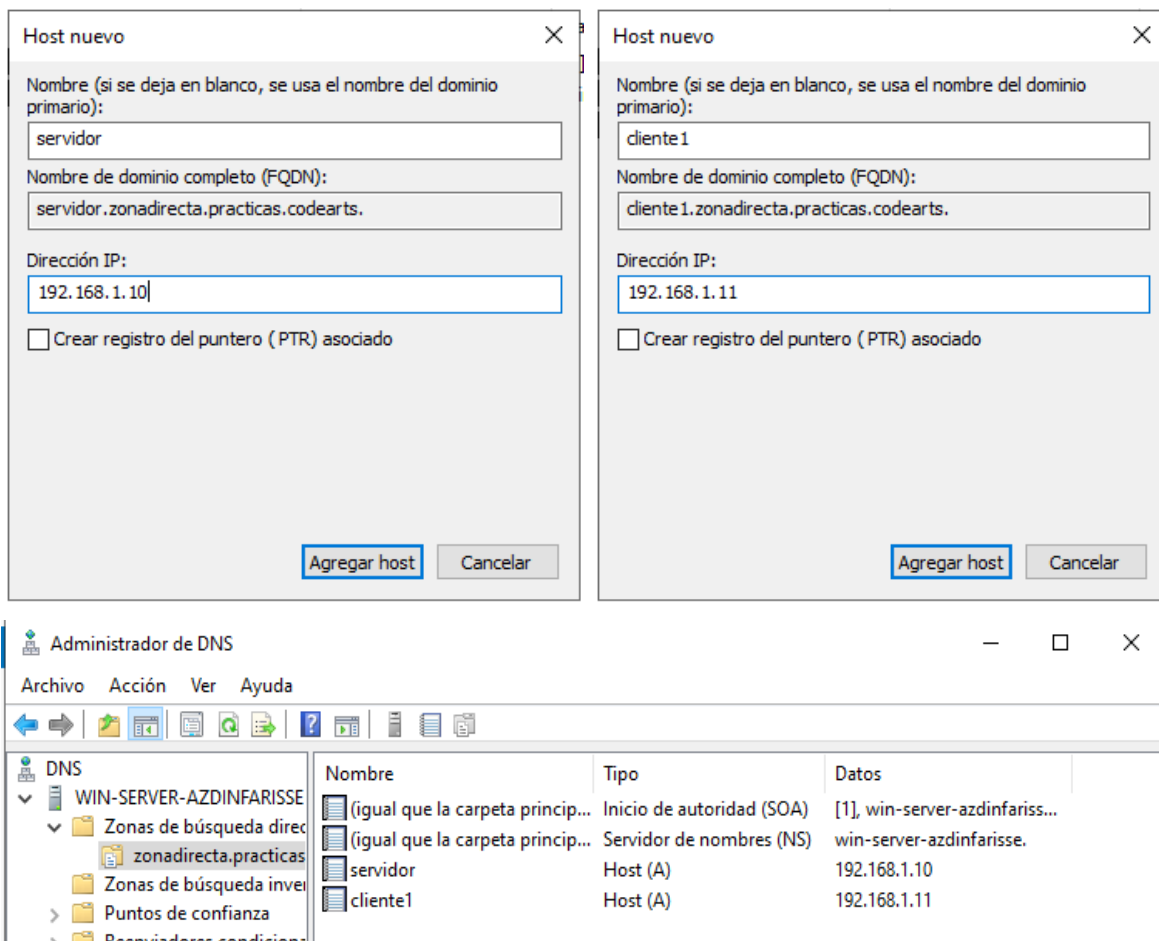
Continuar con la configuración del asistente y en la lista de roles seleccionamos el de **Servidor DNS**.



Una vez instalado este rol, abrimos el administrador de DNS introduciendo **dnsmgmt.msc** en nuestra barra de búsqueda del inicio.

En el árbol de la izquierda, expandir el nombre del servidor → clic derecho en **Zonas de búsqueda directa** → **Zona Nueva**.

Añadimos una nueva zona directa con el nombre de *zonadirecta.practicas.codearts*. Ahora que ya la hemos añadido, continuamos con la creación de 2 registros. Para ello en el panel izquierdo le damos clic derecho a nuestra nueva zona directa y vamos a Host Nuevo (A o AAAA)...

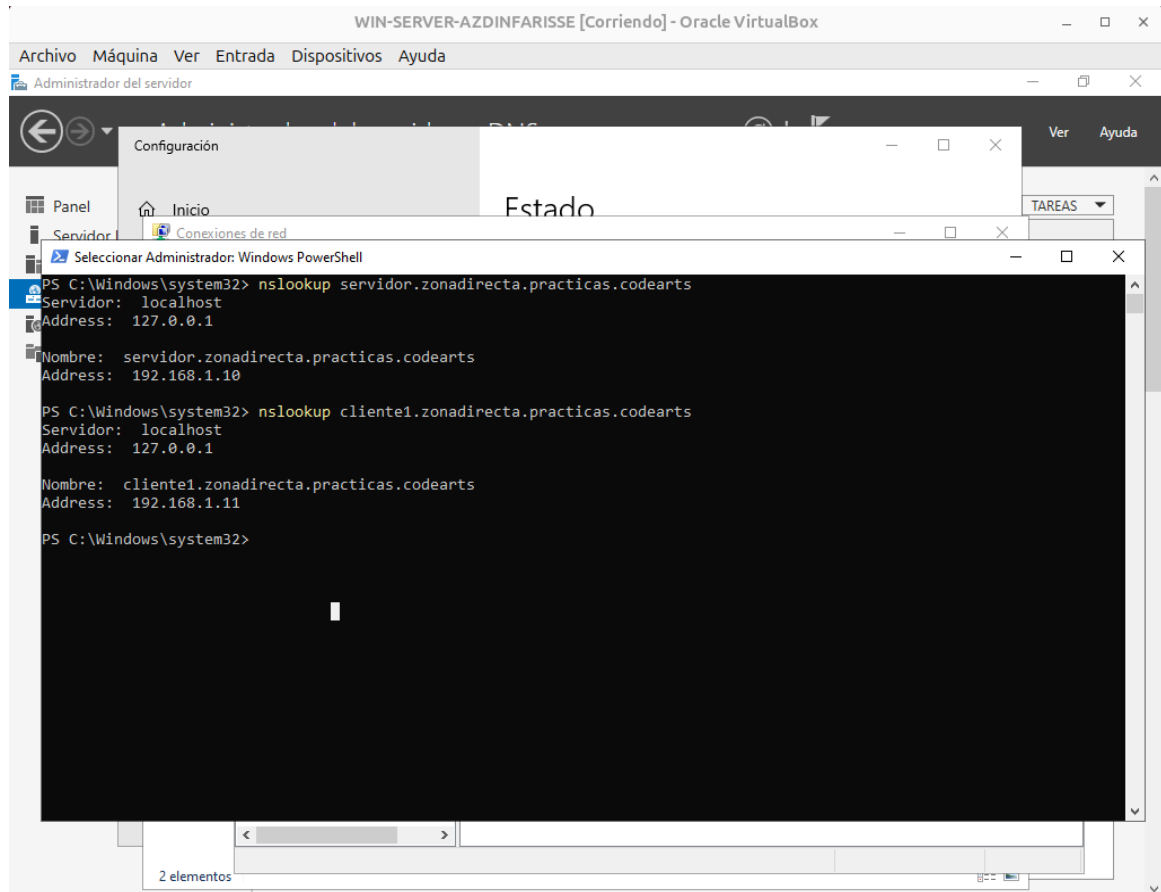


Ahora que ya tenemos los dos registros creados, hemos de ir a la configuración del adaptador de red y cambiar el servidor DNS por el nuestro propio sustituyéndolo por 127.0.0.1 para que apunte a nosotros.

Ahora que ya lo tenemos nos vamos a nuestro CMD y escribimos los siguientes comandos:

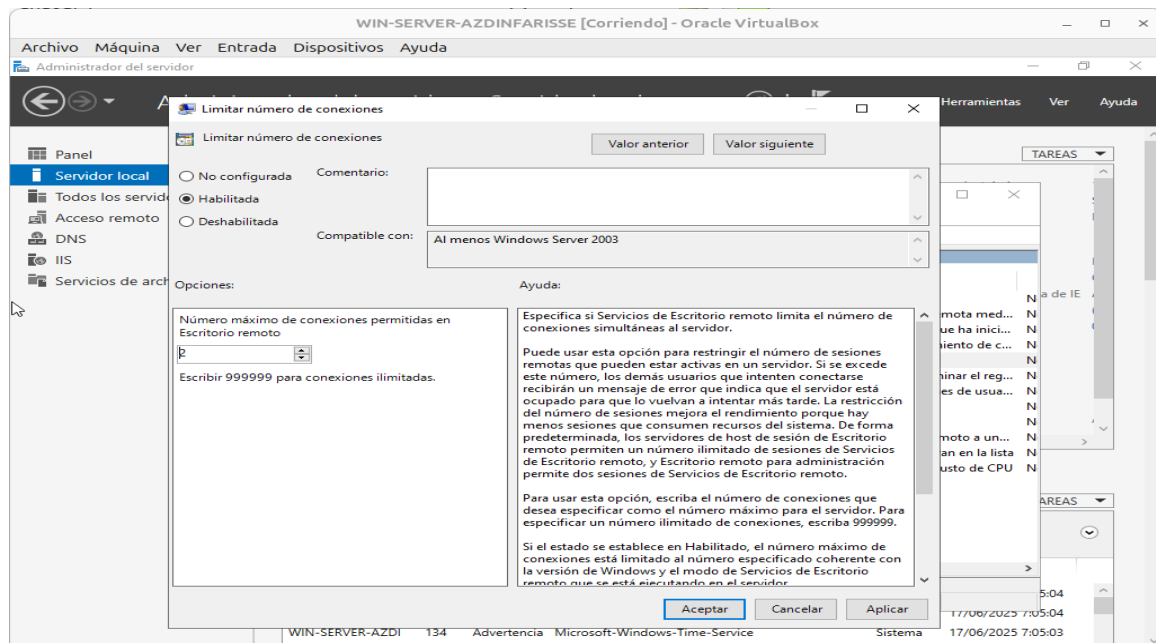
**nslookup servidor.zonadirecta.practicas.codearts**

**nslookup cliente1.zonadirecta.practicas.codearts**



El siguiente paso será habilitar el escritorio remoto y limitar el número de sesiones a 2. Para ello nos dirigimos a nuestro **Administrador del Servidor**→**Panel**→**Agregar roles y características**.

En la lista de roles seleccionamos **Acceso remoto** y lo instalamos. Ahora para limitar el número de sesiones a 2, en nuestra barra de búsqueda introduciremos **gpedit.msc** para abrir el editor de directivas local, y nos dirigimos a: **Configuración del equipo**→**Plantillas administrativas**→**Componentes de windows**→**Servicios de escritorio remoto**→**Host de sesión de escritorio remoto**→**Conexiones**→**Limitar número de conexiones** y establecemos el número de conexiones a 2 y aceptamos.

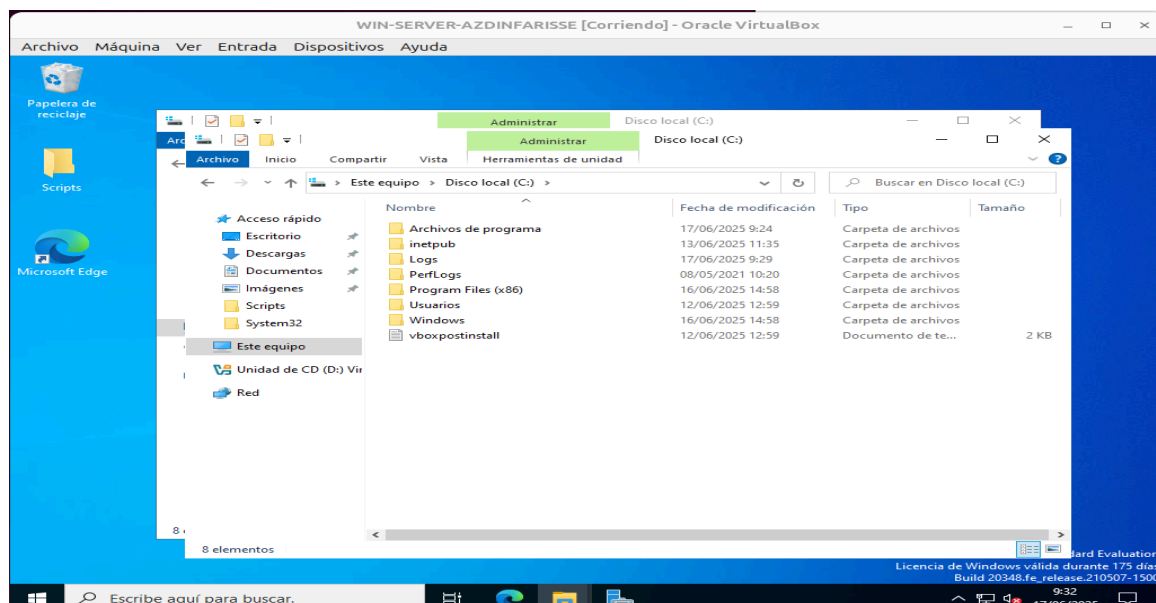


Ahora vamos a crear un script que cree automáticamente una carpeta de logs en C:\Logs. Lo primero será crear el script abriendo el Bloc de notas y escribiendo el siguiente comando:

```
@echo off
if not exist C:\Logs (
    mkdir C:\Logs
)
```

Guardamos el archivo como **crearLogs.bat** en el escritorio en una carpeta llamada Scripts.

Una vez creado el Script, nos dirigimos al editor de directivas de grupo local (gpedit.msc) y entramos en **Configuración del equipo**→**Configuración de Windows**→**Scripts (inicio y apagado)**→**Inicio** y seleccionamos en agregar y buscamos nuestro Script y lo aceptamos. Ahora reiniciamos el servidor para verificar que se ha creado **C:\Logs**.





Lo siguiente es configurar el firewall para que sólo permita el tráfico RDP y DNS.

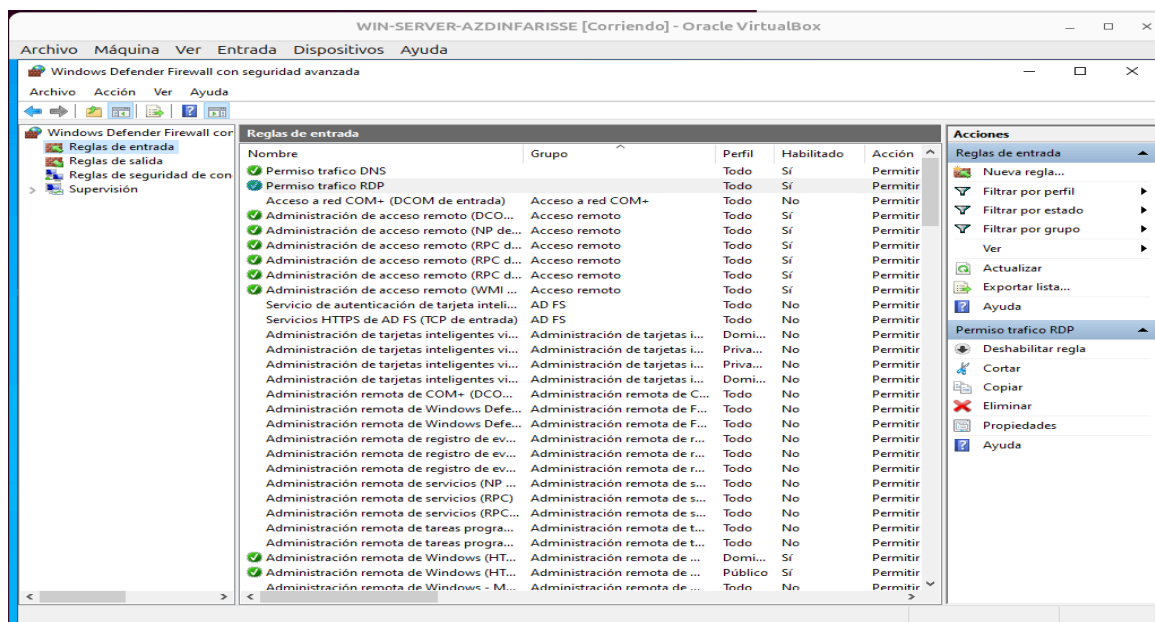
Lo primero que necesitamos saber son los puertos de cada uno. Buscando en Google podemos encontrar que son:

**RDP: 3389**

**DNS: 53**

Ahora que conocemos los puertos, abrimos **Administrador del servidor**→**Herramientas**→**Windows Defender Firewall con seguridad avanzada**→**Reglas de entrada** y añadimos una nueva regla. Seleccionamos la opción de Puerto→TCP→ añadimos el puerto 3389→Permitir la conexión→permitimos a Dominio, Privado y Público→lo nombramos **permiso tráfico RDP**.

Una vez creada esta regla, creamos la otra cambiando el puerto a 53 y nombrandola **permiso tráfico DNS**.



En el panel izquierdo damos clic secundario encima de Windows Defender Firewall y entramos en las propiedades. Una vez aquí hemos de asegurarnos de que cada perfil (privado, público y dominio) estén activados y en las conexiones entrantes esté seleccionado *bloquear*.

Ahora ya tenemos nuestro firewall configurado para que bloquee todo excepto las reglas de entrada incluyendo las de DNS y RDP.

Ahora vamos a crear un script en PowerShell que cree una carpeta con la fecha actual, copie archivos del escritorio en esa carpeta y genere un log en .txt con el resultado de la copia.

Para ello abrimos como administrador nuestro **PowerShell ISE**, y pegamos el siguiente código:

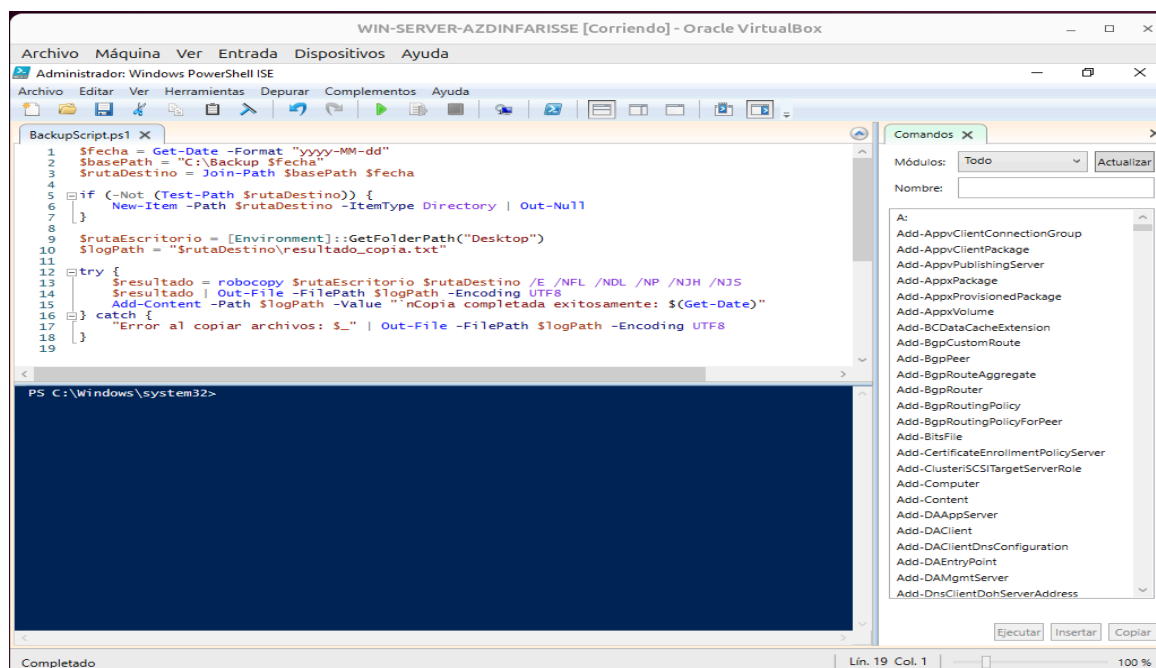
```
$fecha = Get-Date -Format "yyyy-MM-dd"
$basePath = "C:\Backup $fecha"
$rutaDestino = Join-Path $basePath $fecha

if (-Not (Test-Path $rutaDestino)) {
    New-Item -Path $rutaDestino -ItemType Directory | Out-Null
}

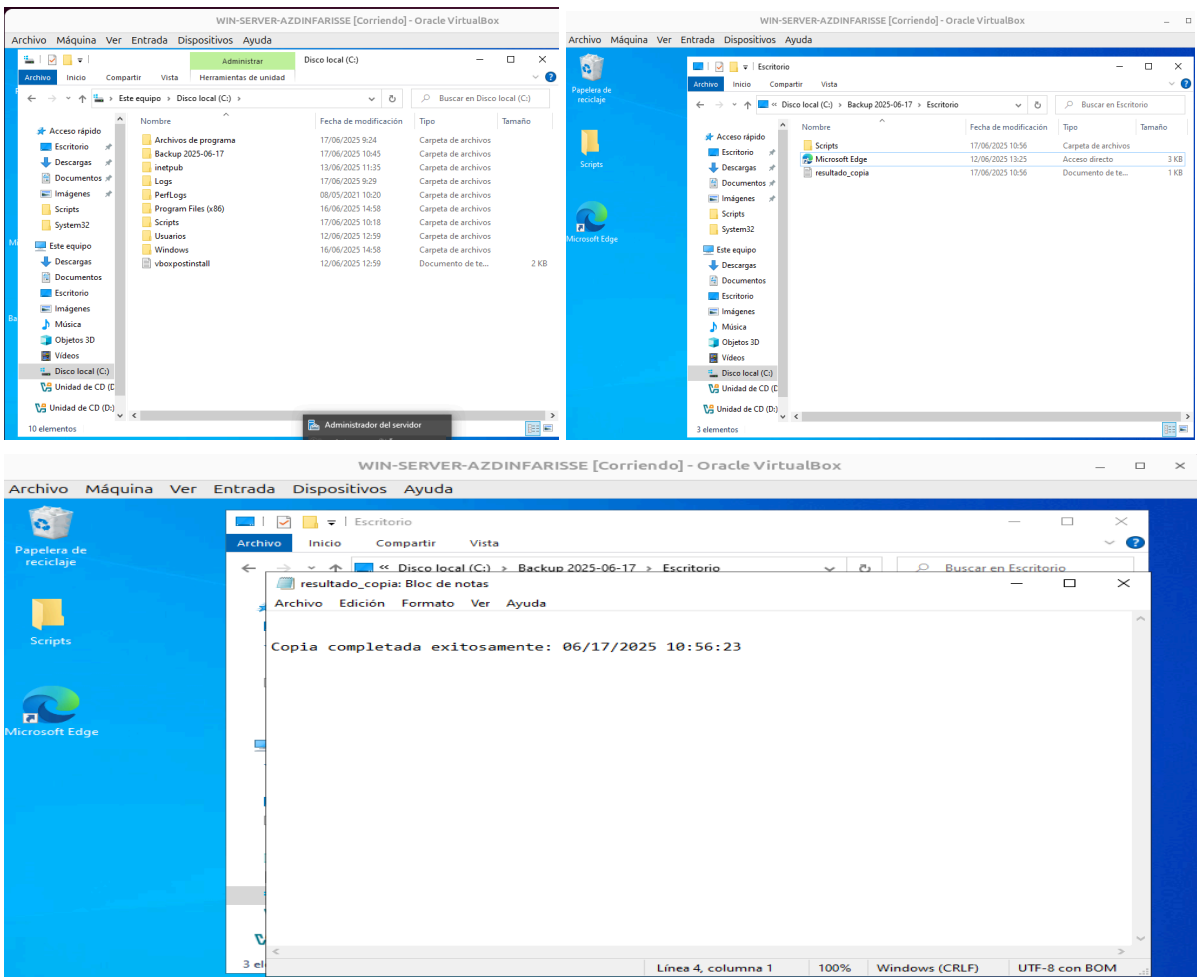
$rutaEscritorio = [Environment]::GetFolderPath("Desktop")
$logPath = "$rutaDestino\resultado_copia.txt"

try {
    $resultado = robocopy $rutaEscritorio $rutaDestino /E /NFL /NDL /NP /NJH /NJS
    $resultado | Out-File -FilePath $logPath -Encoding UTF8
    Add-Content -Path $logPath -Value "`nCopia completada exitosamente: $(Get-Date)"
} catch {
    "Error al copiar archivos: $_" | Out-File -FilePath $logPath -Encoding UTF8
}
```

y lo guardamos en nuestra carpeta de Scripts como BackupScript.ps1



Ahora si ejecutamos nuestro Script, podemos comprobar que la carpeta ha sido creada con éxito, que los archivos del escritorio se han copiado y que ha generado un log con el resultado de la copia.



[Código del script](#)