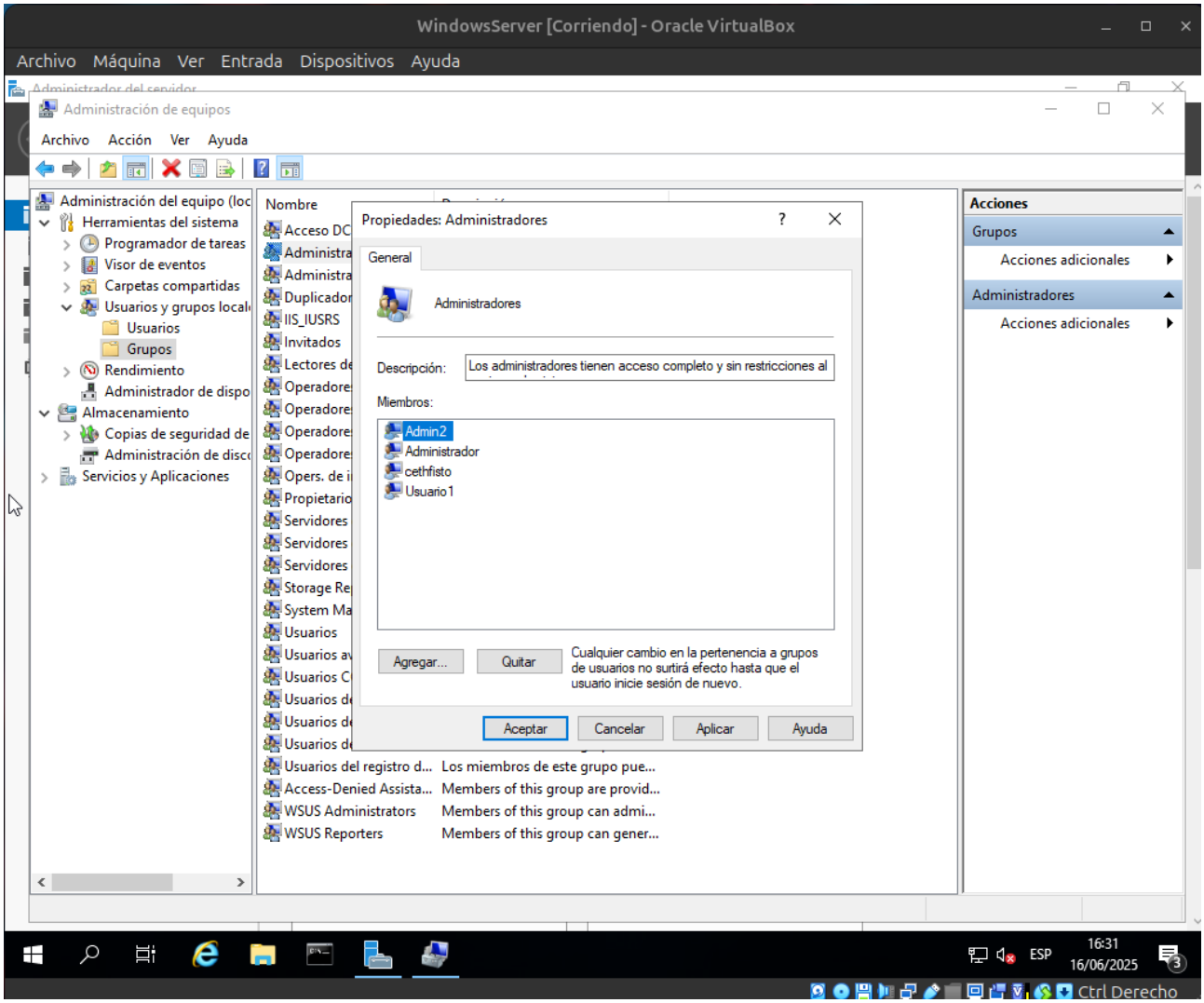
Reto: Bloque 2 día 6

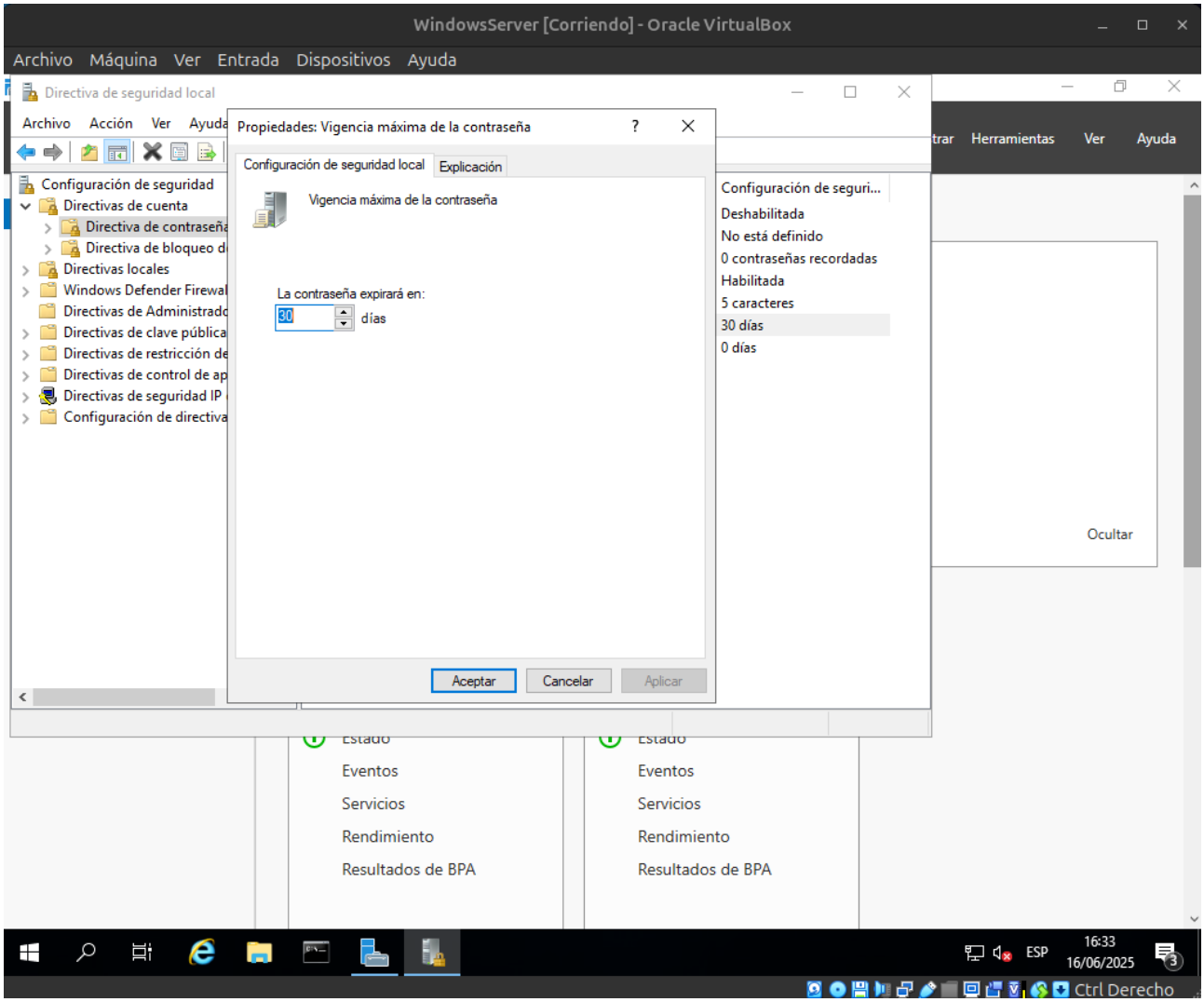
Fase: 1

En esta primera fase del reto crearemos un administrador secundario, cambiaremos las políticas de las contraseñas para que caduquen en 30 días y el Control de Cuentas de Usuario (UAC).

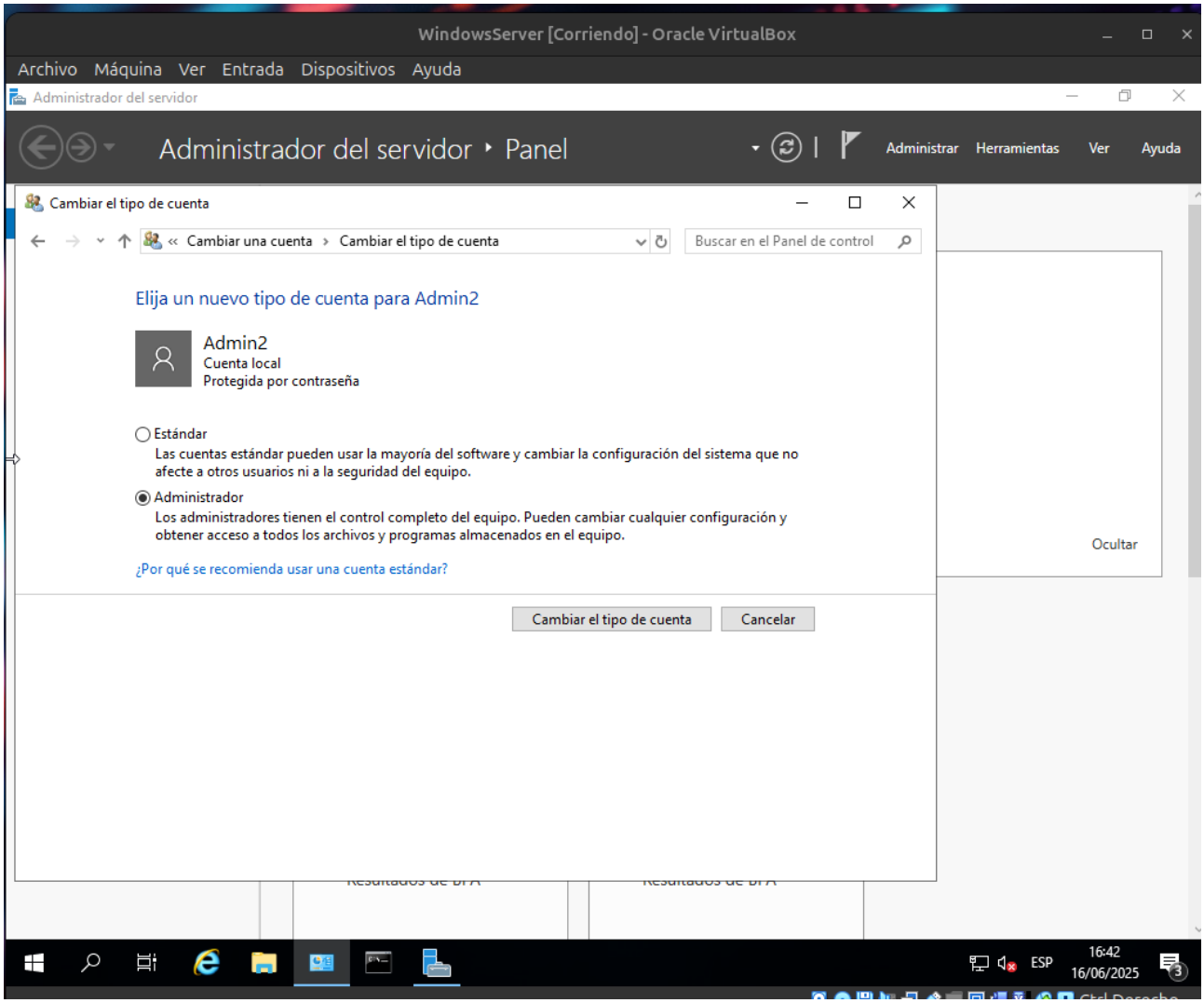
Para crear un Admin secundario, haremos los de siempre. Iremos a Herramienta y a Administración de Equipos. En Usuarios y grupos locales, crearemos el usuario y lo añadimos al grupo de Administradores. Llamaremos al usuario Admin2.



Para cambiar las políticas de contraseñas a la hora crear la contraseña, iremos a Herramientas, Directiva de seguridad local, Directiva de contraseñas. Ahí configuramos la política de contraseñas para que caduquen a los 30 días.



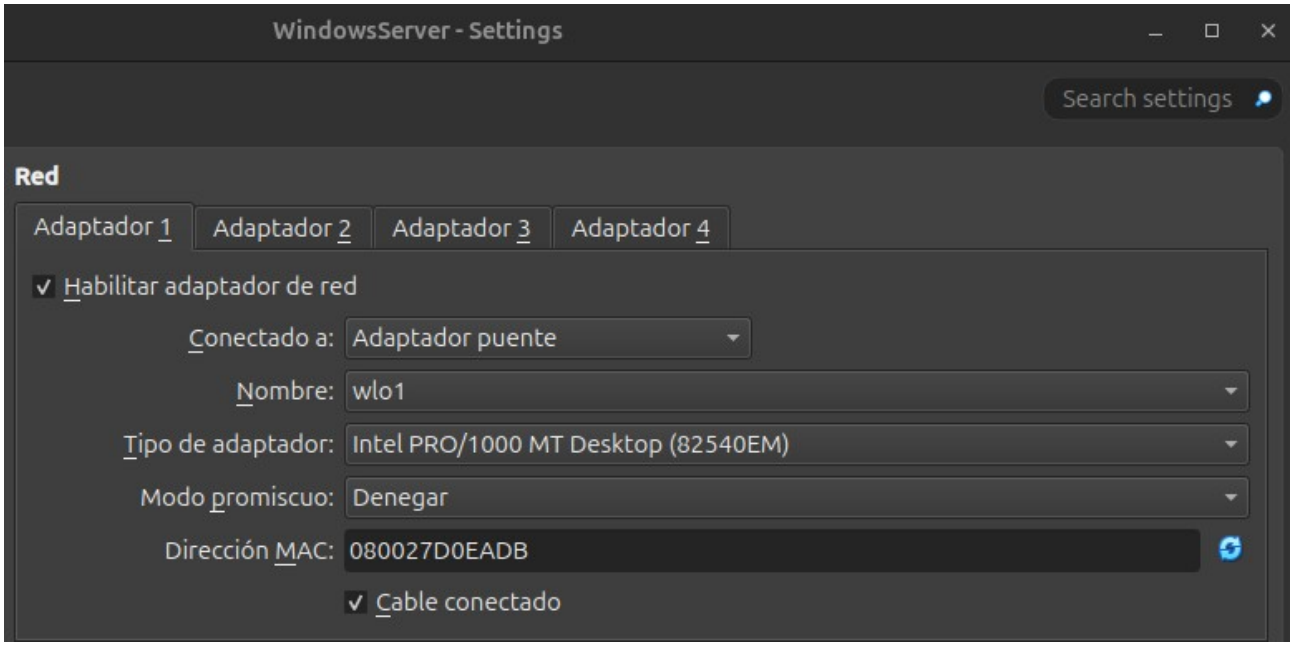
Para cambiar el UAC podemos hacerlo desde la Directiva de seguridad local o por el Panel de Control. Vamos a configurarlo usando el Panel de Control. Iremos a Panel de Control, Cuentas de usuario y Cambiar configuración de cuentas de usuario. Aquí podremos elegir que tipo de cuenta serán lo usuarios, pueden ser Administradores o Estándar. Como queremos que Admin2 sea administrador, cambiaremos la opción.

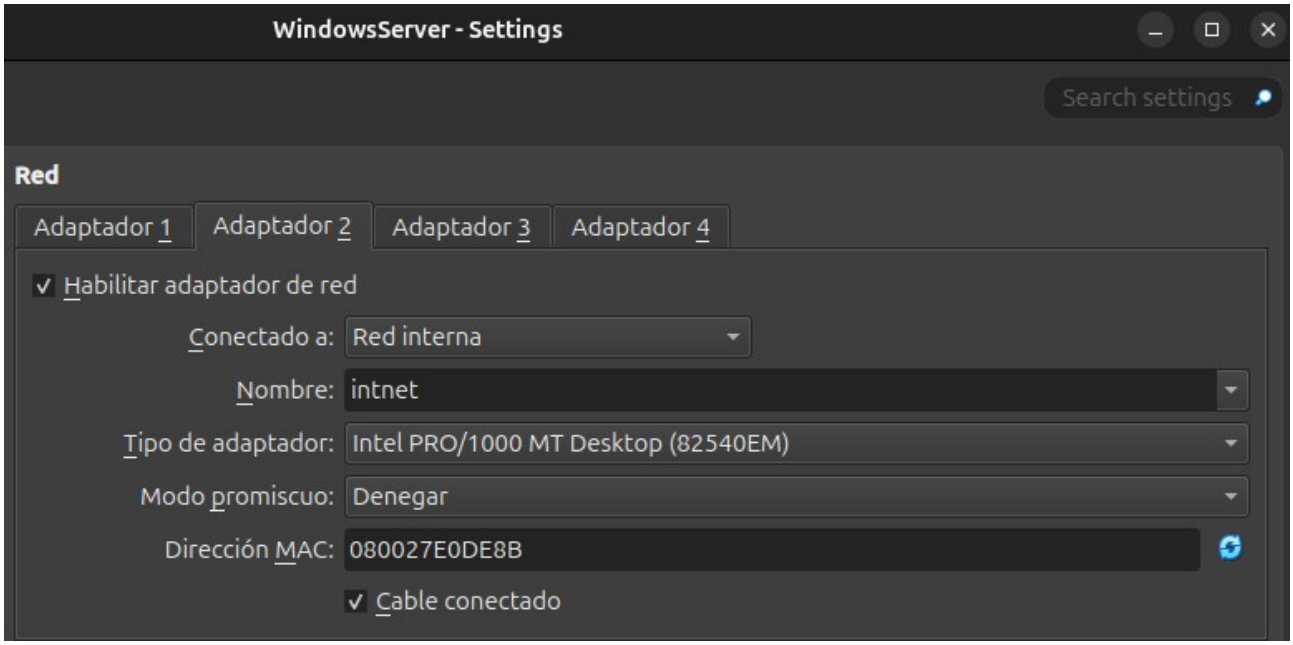


Fase: 2

En la segunda parte simularemos dos tarjetas de red interna y otra externa, configuraremos rutas estáticas en la red interna y crearemos y activaremos un DNS local.

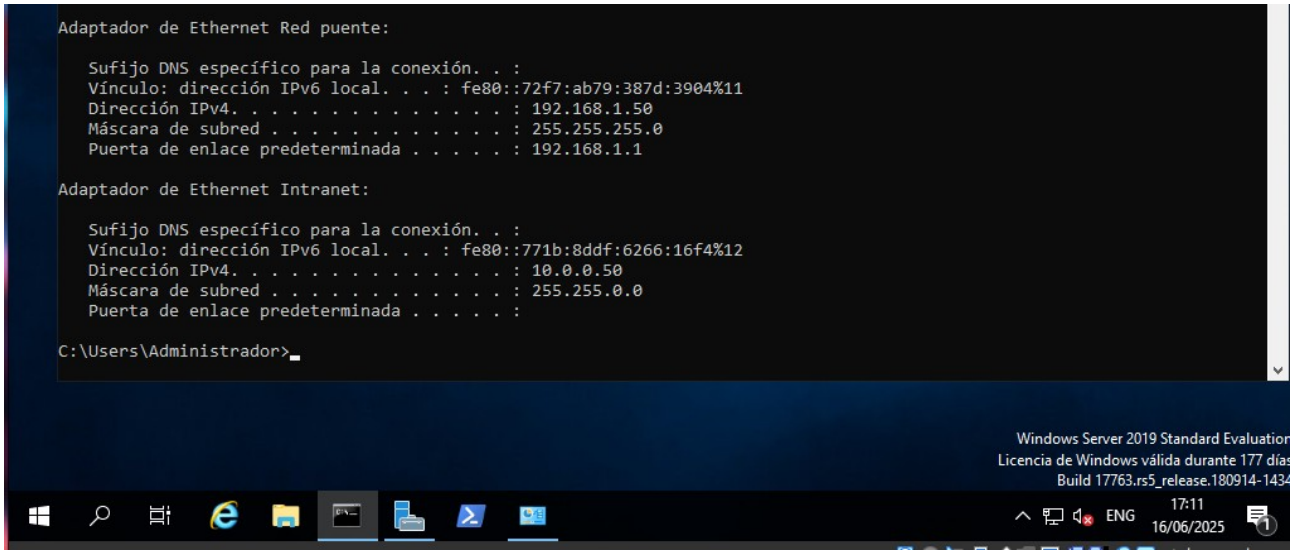
Para configurar las tarjetas de red de la VM iremos a la configuración de la misma en Virtualbox. Ahí pondremos las dos tarjetas de red.

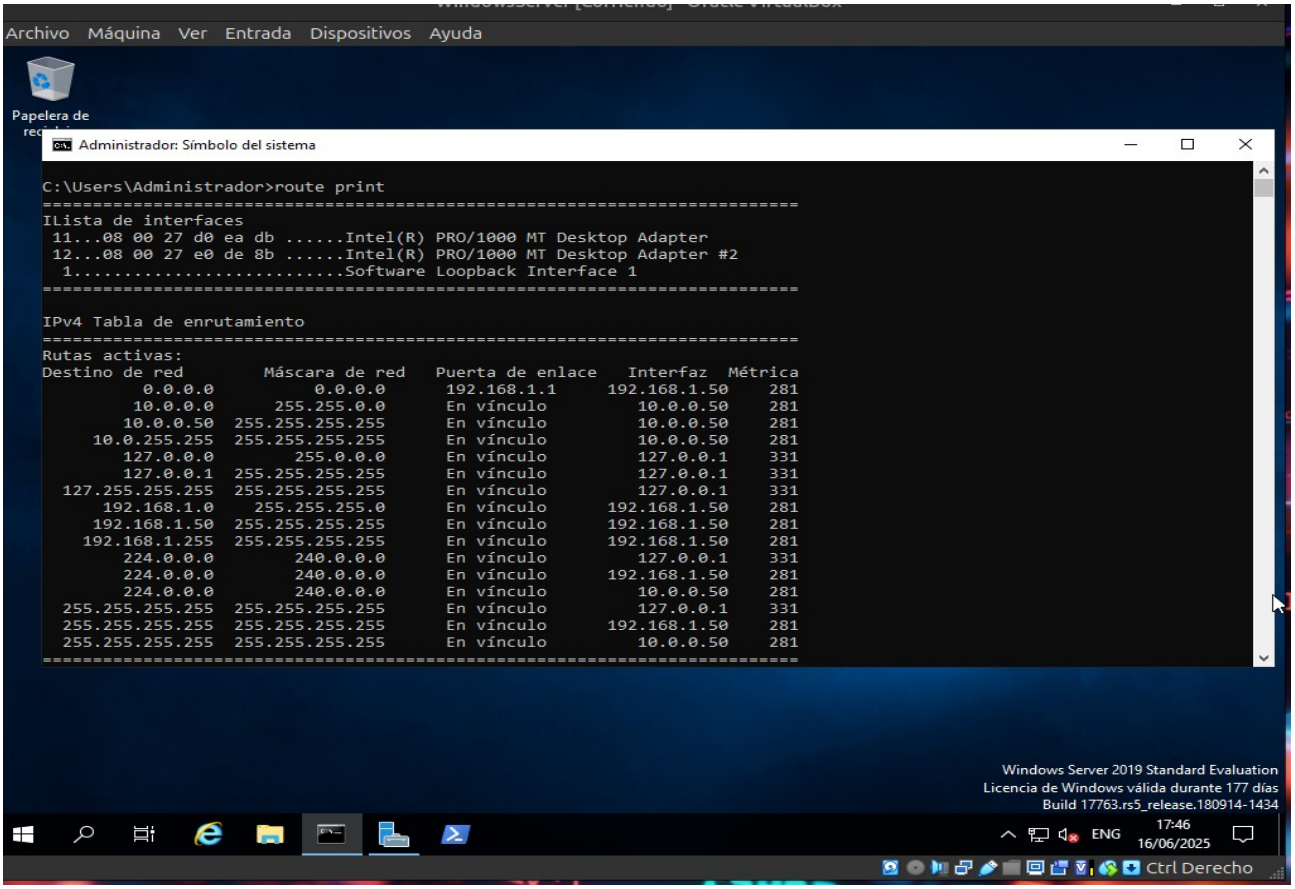




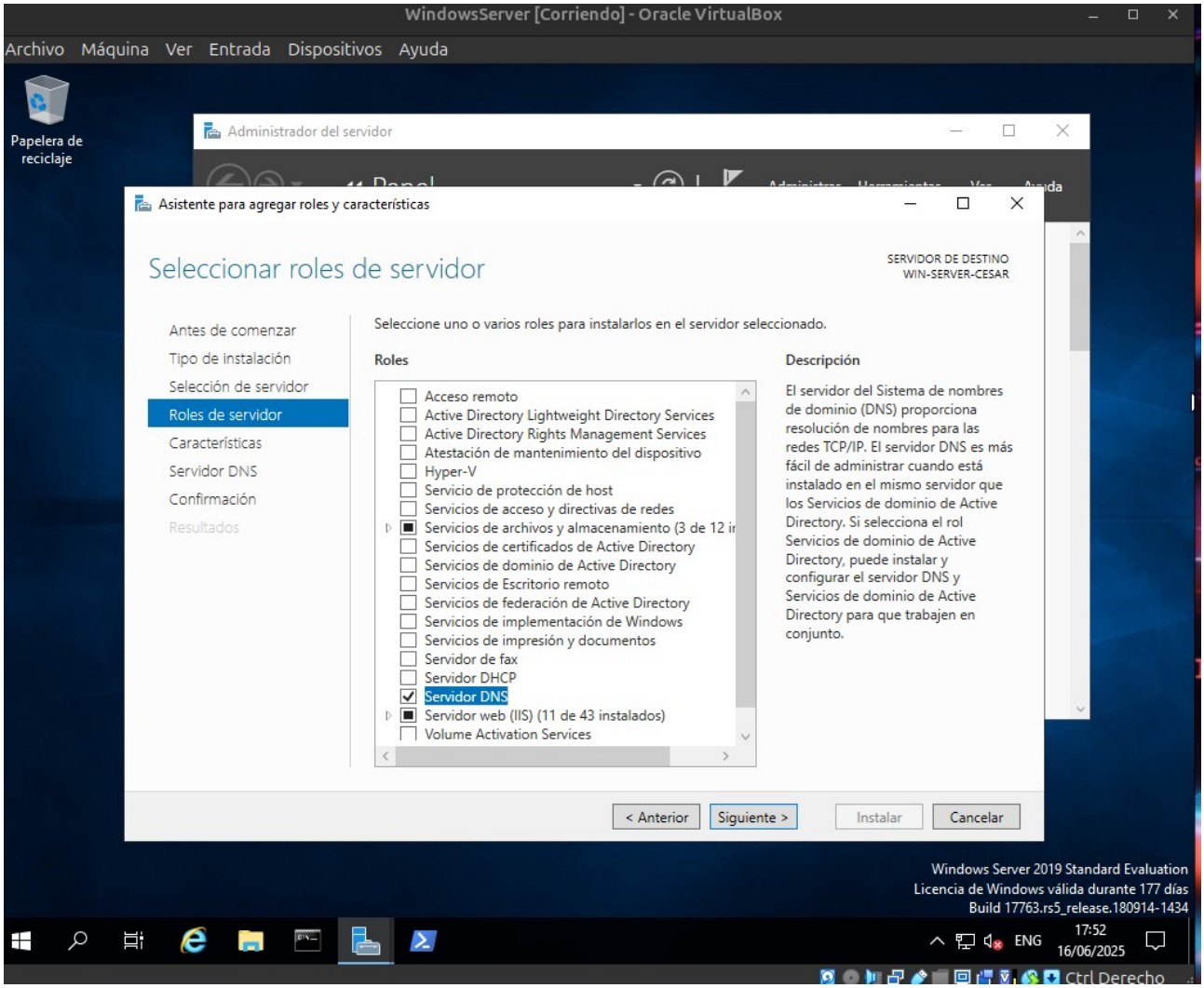
Para configurar las rutas estáticas de la red interna haremos varias cosas. Primero conocer cual es nuestra tarjeta de red, IP y la puerta de enlace. Recomiendo tener una IP estática en la red interna también. Pondremos la IP 10.0.0.50.

Para empezar usaremos los comando ipconfig y route print para verificar que tenemos las IP estáticas y conocer la lista de interfaces. Una vez que conozcamos estos datos deberemos crear las rutas estáticas y permanentes con el comando route -p add, ya que las rutas se eliminan con cada reinicio. Por ejemplo si queremos que todo el tráfico de 10.0.0.0 pase por la red interna y el siguiente salto sea en 10.0.0.49 haremos: route -p add 10.0.0.0 mask 255.255.0.0 10.0.0.49 if 12. Y así sucesivamente hasta configurar las rutas estáticas en su totalidad.

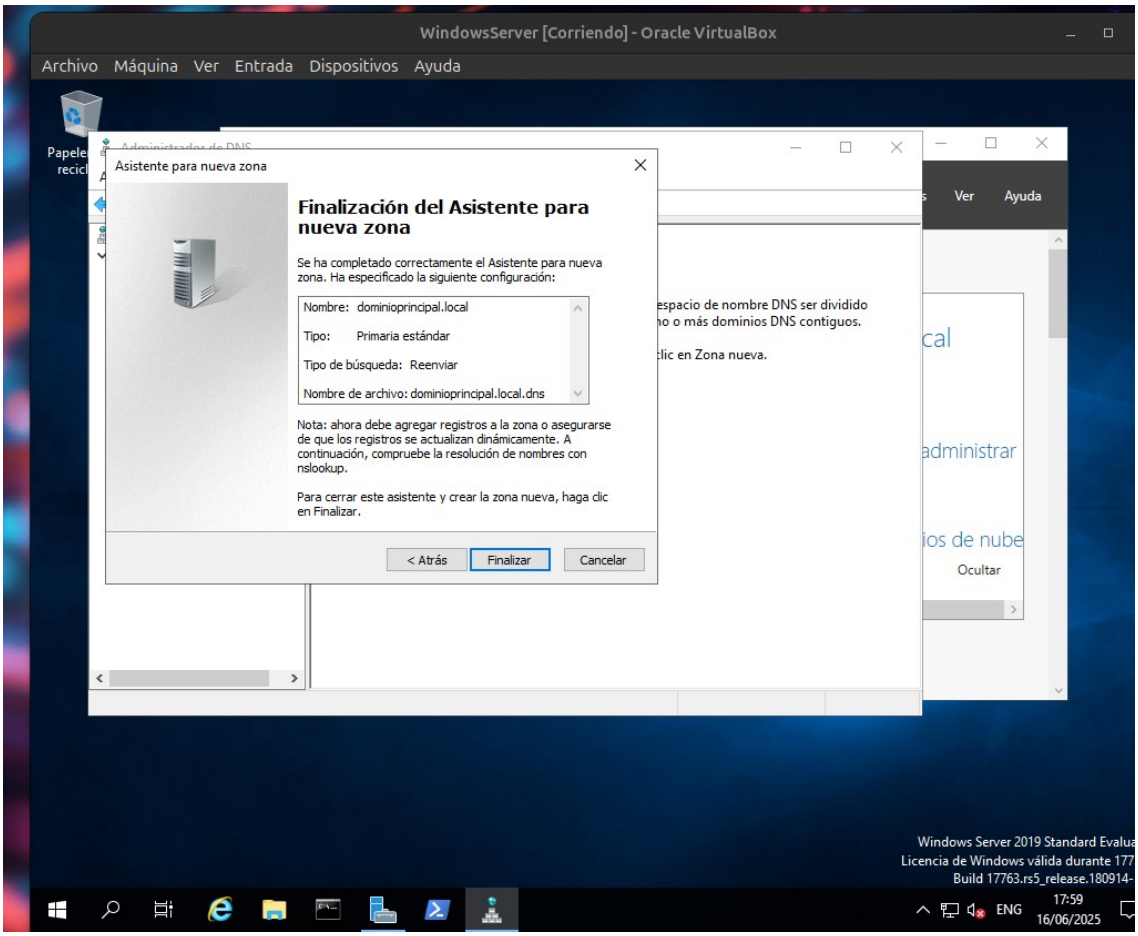


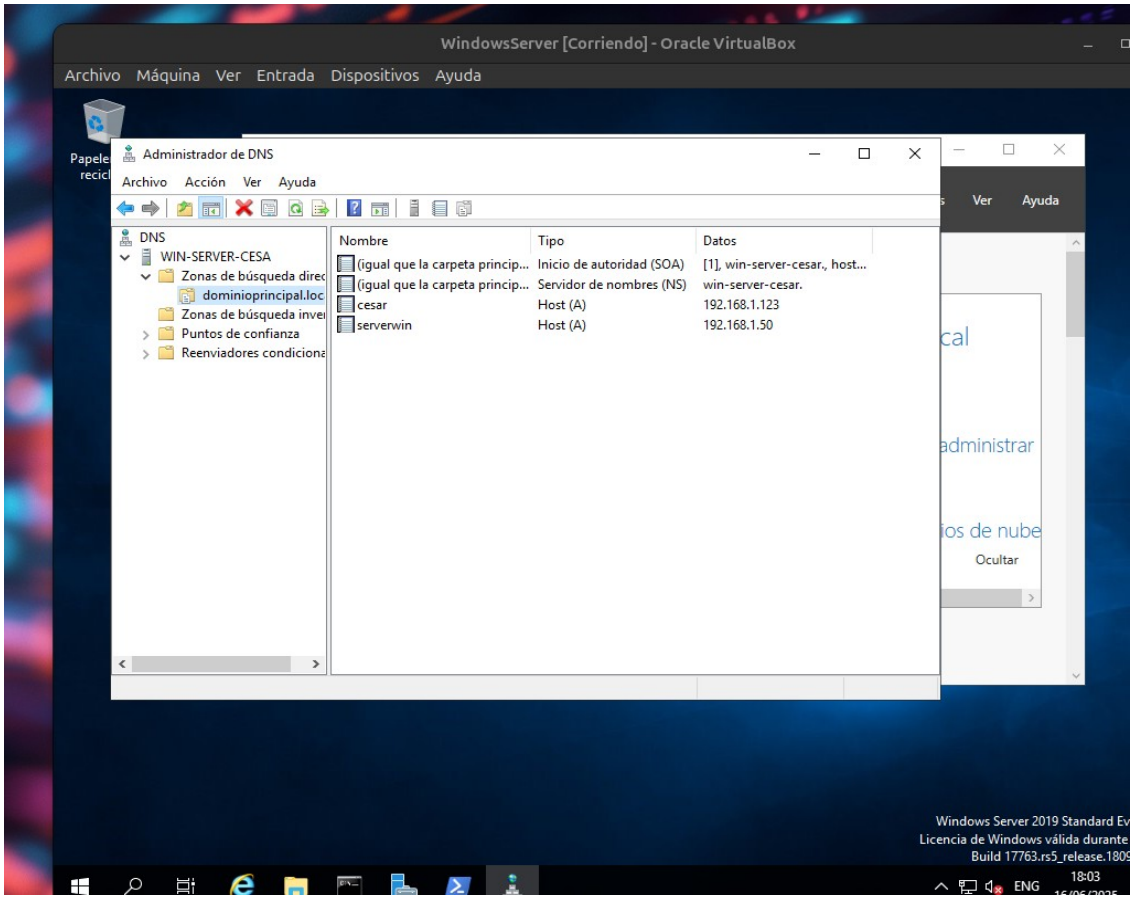


Para crear y activar un DNS local deberemos instalar el rol, para ello iremos a Agregar roles y características y hacemos el proceso de instalación.



Para hacer la configuración de la zona directa iremos a Herramientas y seleccionamos DNS. Una vez dentro vamos a Zonas de búsqueda directa y seleccionamos Nueva zona en el menú superior para iniciar el asistente al que llamaremos dominioprincipal.local. Y para añadir los registros, seleccionamos la zona creada y con clic derecho seleccionamos Nuevo host (A o AAAA) para añadir los equipos y su IP.

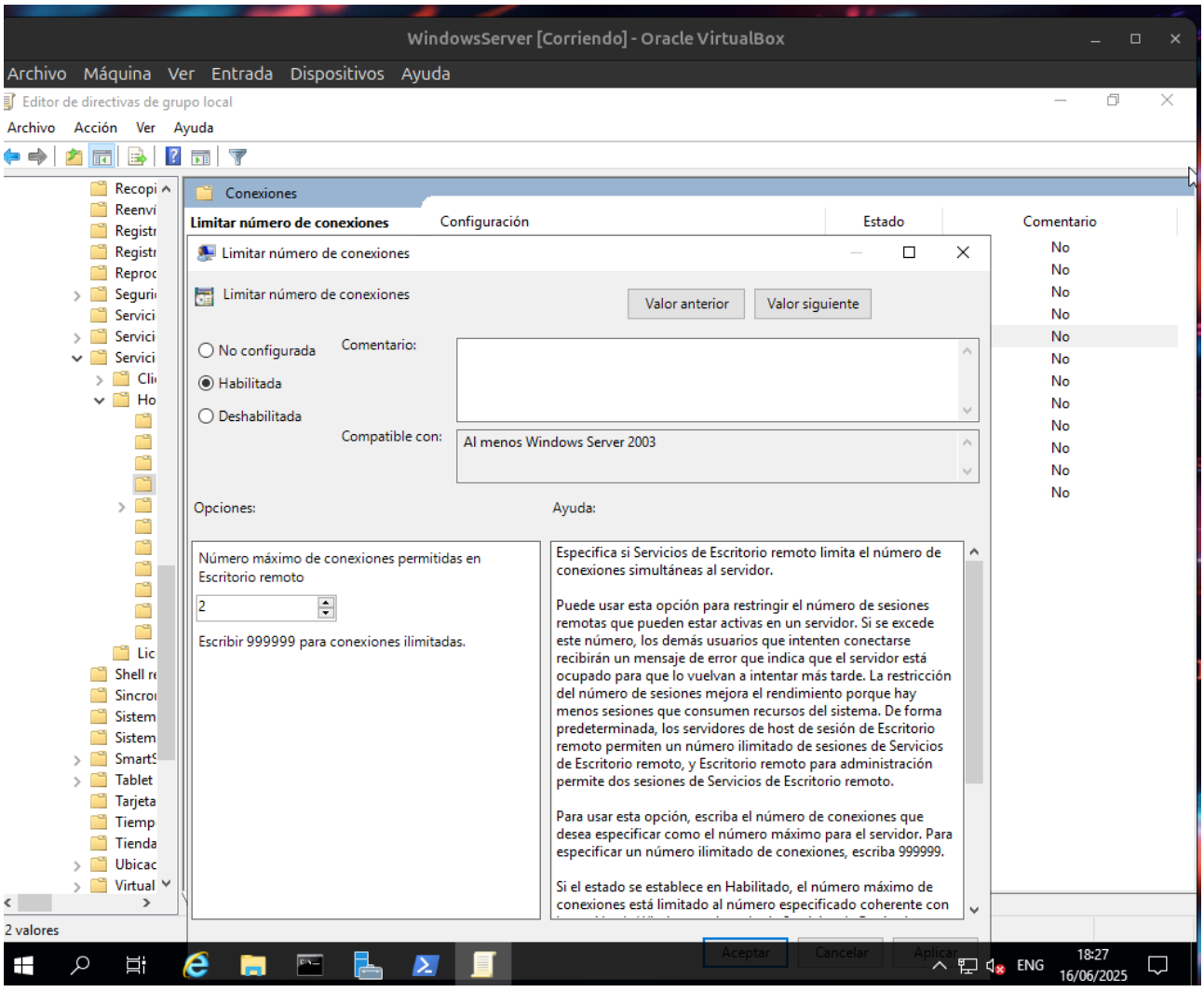

WindowsServer [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Asistente para nueva zona
Finalización del Asistente para nueva zona
Se ha completado correctamente el Asistente para nueva zona. Ha especificado la siguiente configuración:
Nombre: dominioprincipal.local
Tipo: Primaria estándar
Tipo de búsqueda: Reenviar
Nombre de archivo: dominioprincipal.local.dns
Nota: ahora debe agregar registros a la zona o asegurarse de que los registros se actualizan dinámicamente. A continuación, compruebe la resolución de nombres con nslookup.
Para cerrar este asistente y crear la zona nueva, haga clic en Finalizar.
< Atrás
Finalizar
Cancelar
Ver
Ayuda
Ocultar
Windows Server 2019 Standard Evalua
Licencia de Windows válida durante 177
Build 17763.rs5_release.180914-
ENG
17:59
16/06/2025


WindowsServer [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Administrador de DNS
Archivo Acción Ver Ayuda
DNS
WIN-SERVER-CESA
Zonas de búsqueda direc
dominioprincipal.loc
Zonas de búsqueda inver
Puntos de confianza
Reenviadores condiciona
Nombre
Tipo
Datos
(igual que la carpeta princip...
Inicio de autoridad (SOA)
[1], win-server-cesar., host...
(igual que la carpeta princip...
Servidor de nombres (NS)
win-server-cesar.
cesar
Host (A)
192.168.1.123
serverwin
Host (A)
192.168.1.50
Ver
Ayuda
Ocultar
Windows Server 2019 Standard Ev
Licencia de Windows válida durante
Build 17763.rs5_release.1809
ENG
18:03

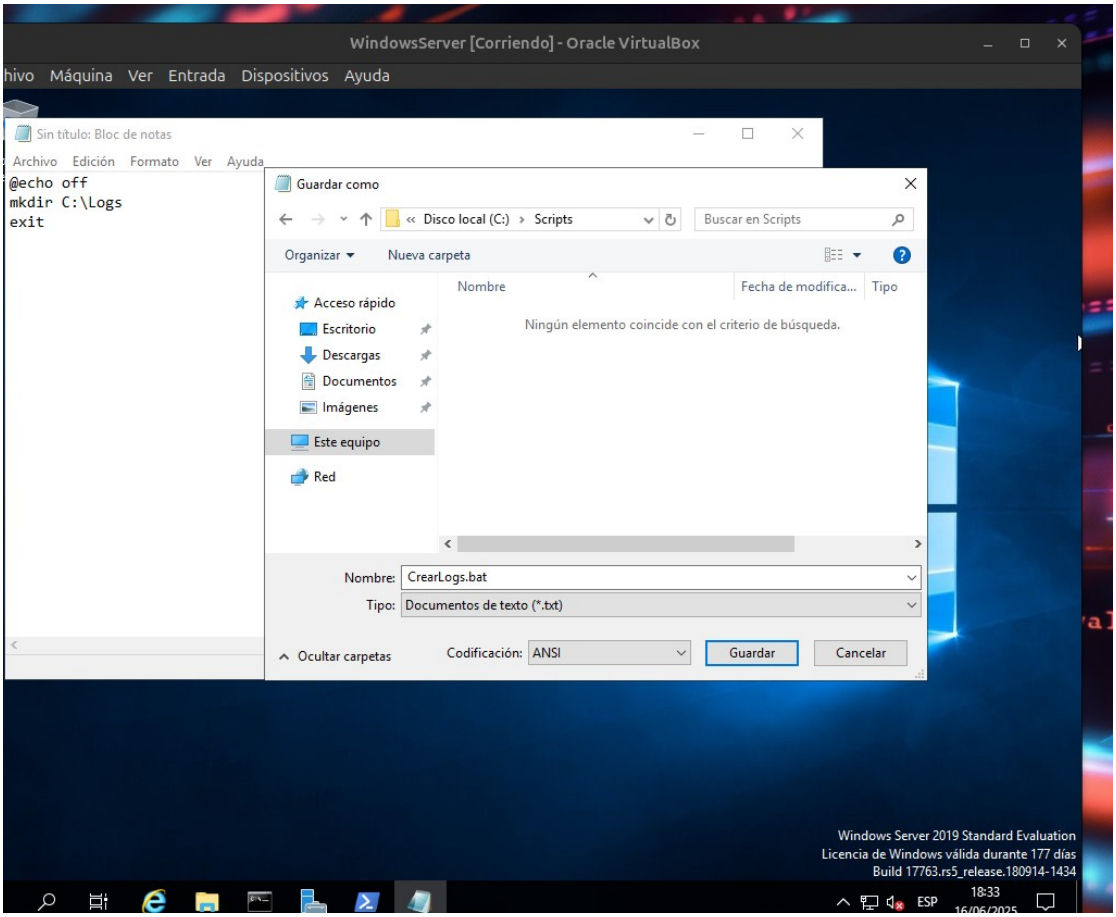
Fase: 3

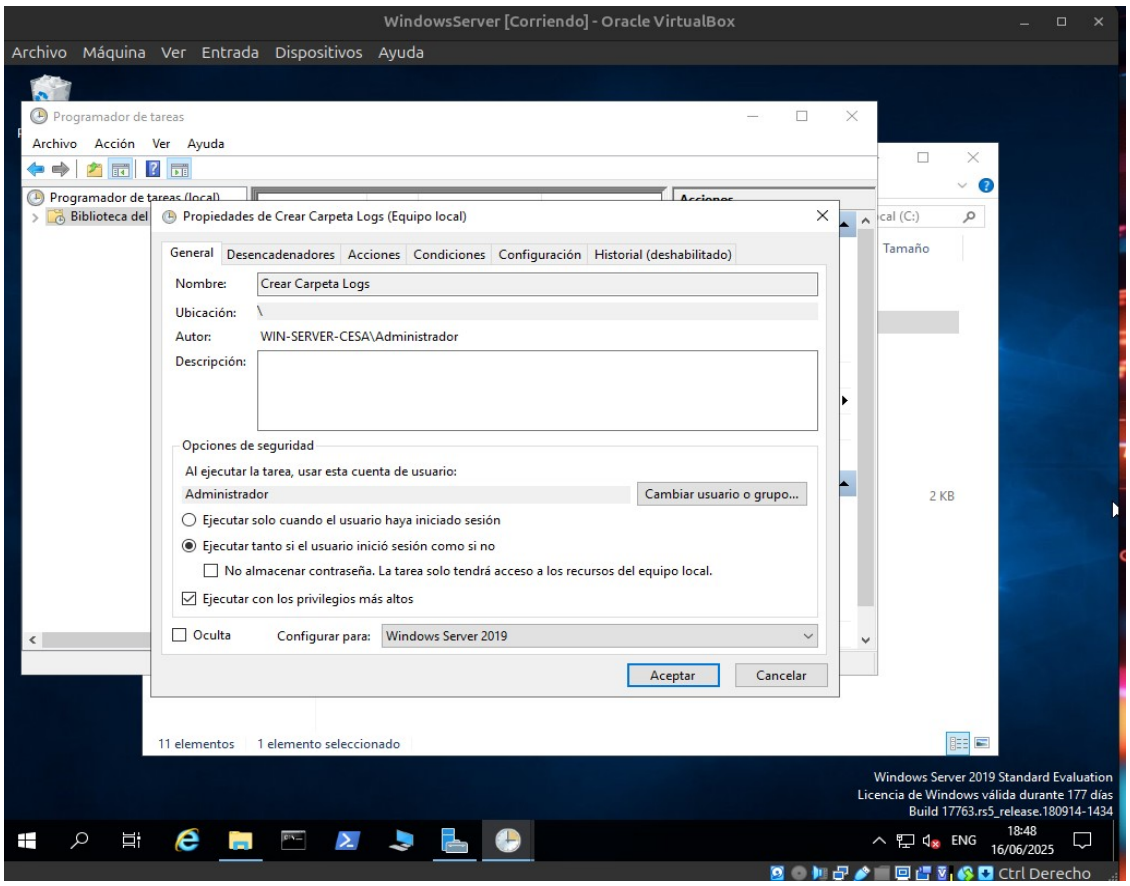
En esta fase habilitaremos en Escritorio Remoto a 2 sesiones, personalizaremos el inicio del sistema con un script en la carpeta Logs y configuraremos el Firewall para que solo permita el RDP y DNS.

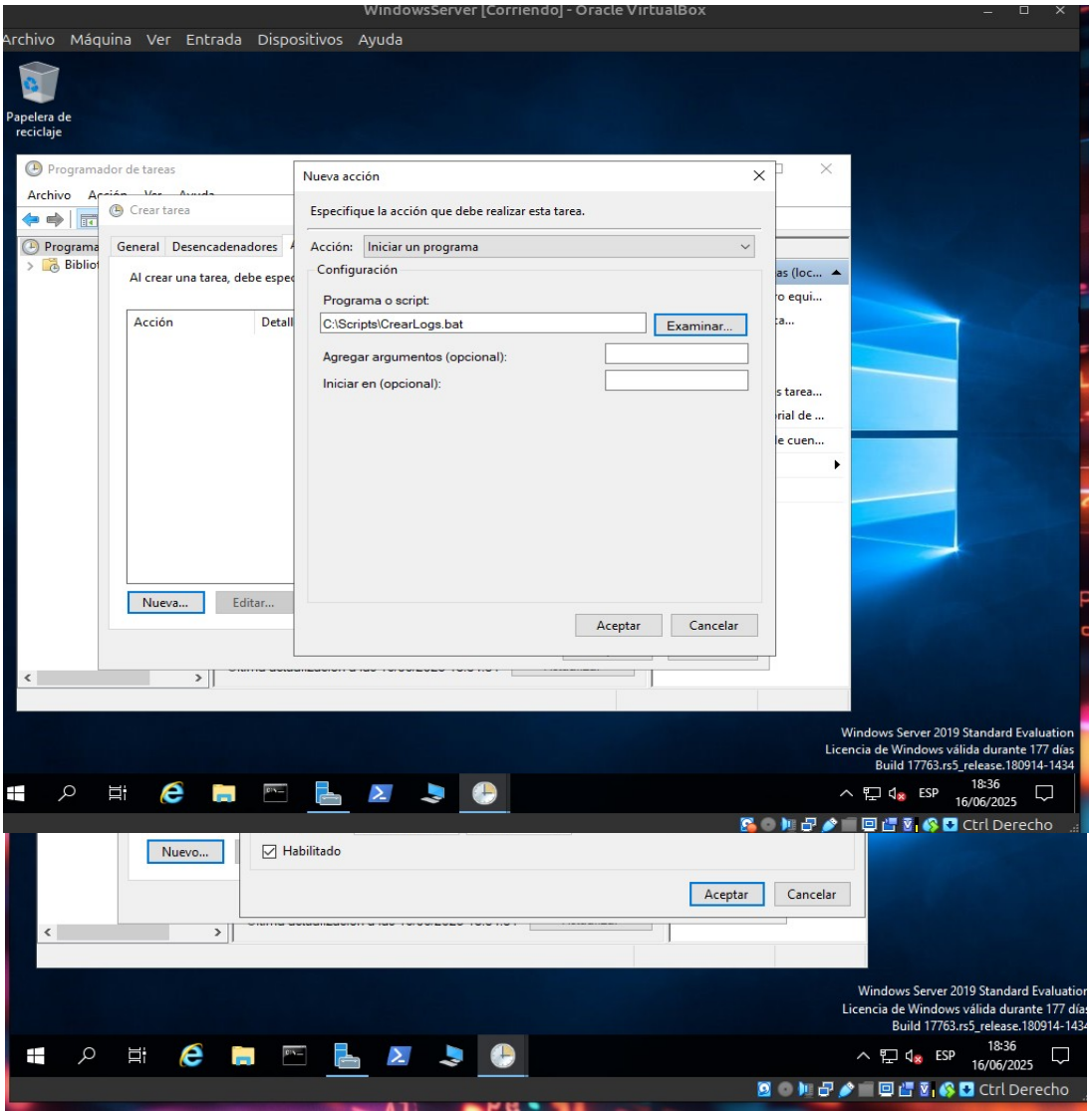
Para limitar el acceso remoto a dos sesiones, primero, deberemos activar el servicio. Ahora para limitar las sesiones, deberemos ir al Editor de directivas de grupo local, podemos acceder con la consola con el comando gpedit.msc. Una vez dentro iremos pasando por Configuración de equipo, Plantillas administrativas, Componentes de Windows, Servicios de Escritorio remoto hasta Conexiones. Dentro de conexiones seleccionamos Limitar número de conexiones y realizamos la configuración pertinente.

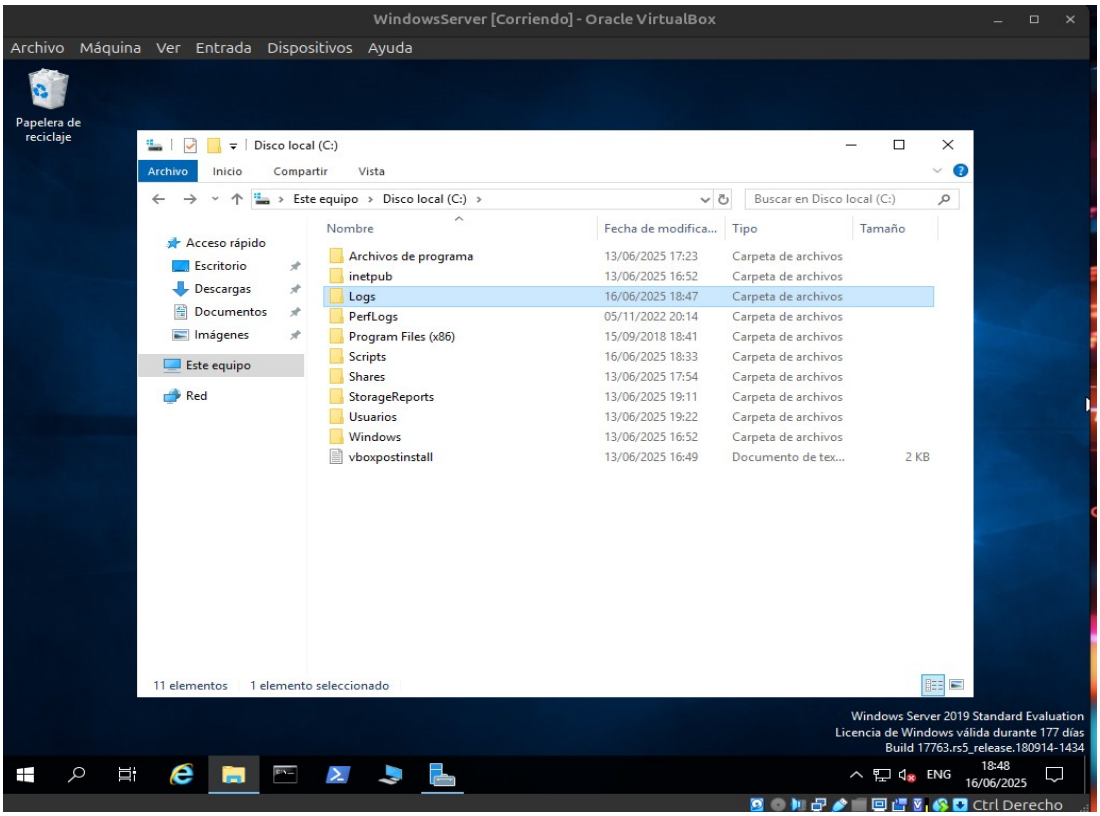


Ahora vamos a crear un script para crear una carpeta en el directorio C:\Logs. Para podemos usar el bloc de notas. Luego para automatizar el script iremos al Programador de tareas en el menú de Inicio, creamos, configuramos y activamos la tarea.

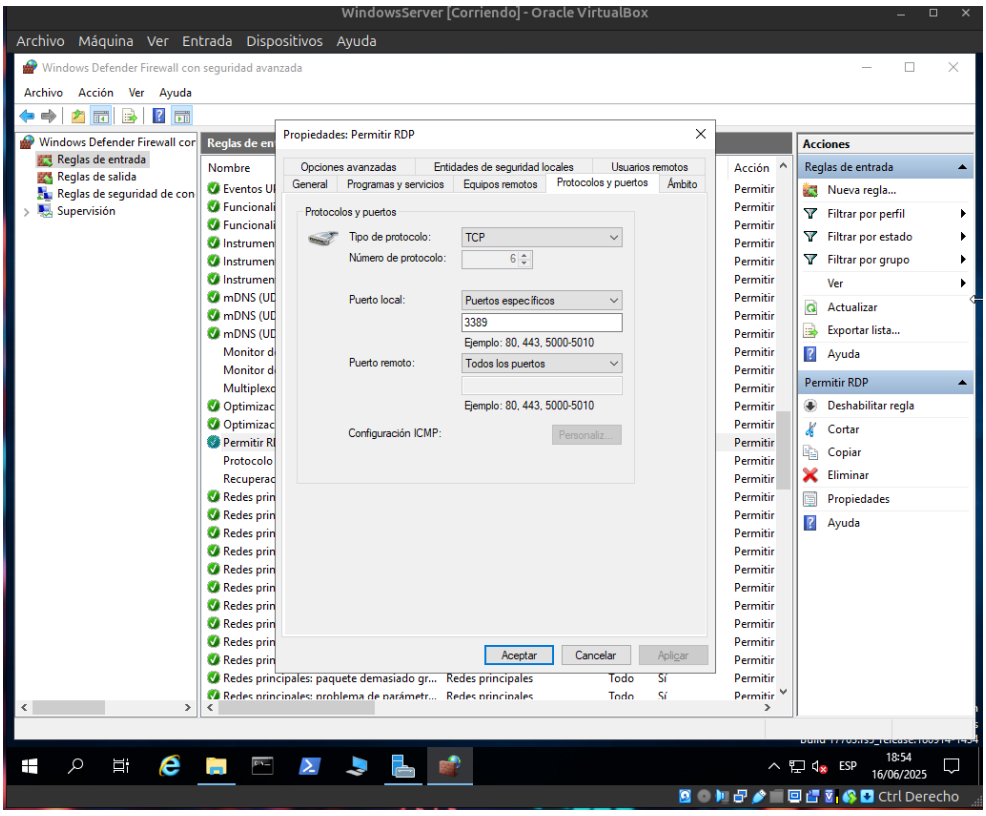


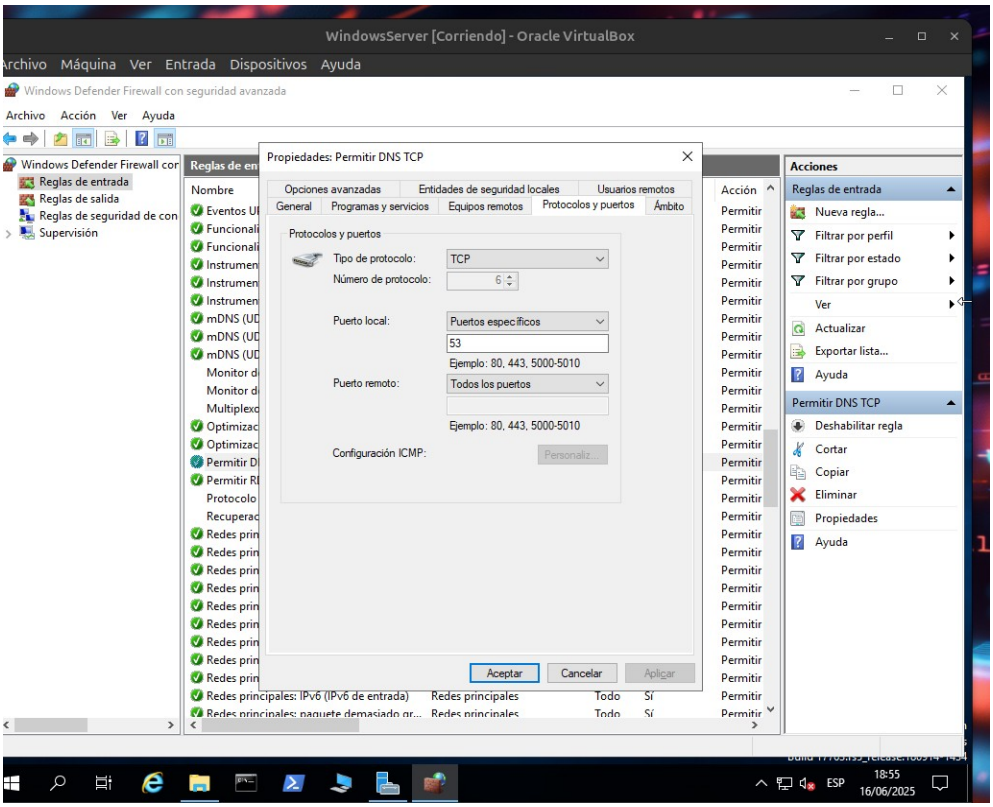

WindowsServer [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Programador de tareas
Archivo Acción Ver Ayuda
Propiedades de Crear Carpeta Logs (Equipo local)
General Desencadenadores Acciones Condiciones Configuración Historial (deshabilitado)
Nombre: Crear Carpeta Logs
Ubicación: \
Autor: WIN-SERVER-CESA\Administrador
Descripción:
Opciones de seguridad
Al ejecutar la tarea, usar esta cuenta de usuario:
Administrador
Cambiar usuario o grupo...
Ejecutar solo cuando el usuario haya iniciado sesión
Ejecutar tanto si el usuario inició sesión como si no
No almacenar contraseña. La tarea solo tendrá acceso a los recursos del equipo local.
Ejecutar con los privilegios más altos
Oculta
Configurar para: Windows Server 2019
Aceptar
Cancelar
11 elementos
1 elemento seleccionado
Tamaño
2 KB
Windows Server 2019 Standard Evaluation
Licencia de Windows válida durante 177 días
Build 17763.rs5_release.180914-1434
ENG
18:48
16/06/2025
Ctrl Derecho

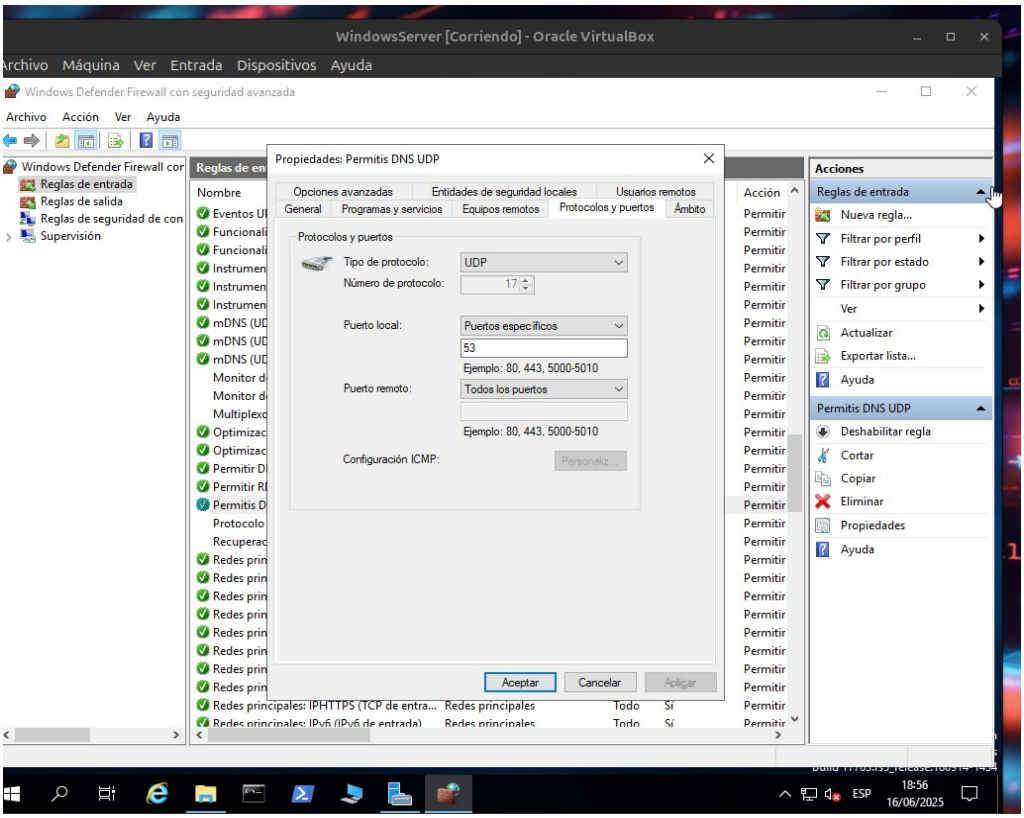

WindowsServer [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Papelera de reciclaje
Programador de tareas
Archivo
Crear tarea
General Desencadenadores
Acción
Nueva...
Editar...
Nueva acción
Especifique la acción que debe realizar esta tarea.
Acción: Iniciar un programa
Configuración
Programa o script:
C:\Scripts\CrearLogs.bat
Examinar...
Agregar argumentos (opcional):
Iniciar en (opcional):
Aceptar
Cancelar
Windows Server 2019 Standard Evaluation
Licencia de Windows válida durante 177 días
Build 17763.rs5_release.180914-1434
ESP
18:36
16/06/2025
Ctrl Derecho
Nuevo...
Habilitado
Aceptar
Cancelar
Windows Server 2019 Standard Evaluation
Licencia de Windows válida durante 177 días
Build 17763.rs5_release.180914-1434
ESP
18:36
16/06/2025
Ctrl Derecho



Por último configuramos el Firewall para que solo permita el RDP y DNS, para ello iremos al Windows Defender Firewall con seguridad avanzada. Iremos a reglas de entrada y creamos las reglas para el RDP y DNS. En el caso del DNS crearemos dos reglas una para el puerto TCP y otra para el puesto UDP.




WindowsServer [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Windows Defender Firewall con seguridad avanzada
Archivo Acción Ver Ayuda
Windows Defender Firewall cor
Reglas de entrada
Reglas de salida
Reglas de seguridad de con
Supervisión
Propiedades: Permitir DNS TCP
Opciones avanzadas
Entidades de seguridad locales
Usuarios remotos
General
Programas y servicios
Equipos remotos
Protocolos y puertos
Ámbito
Protocolos y puertos
Tipo de protocolo: TCP
Número de protocolo: 6
Puerto local: Puertos específicos
53
Ejemplo: 80, 443, 5000-5010
Puerto remoto: Todos los puertos
Ejemplo: 80, 443, 5000-5010
Configuración ICMP:
Personaliz...
Aceptar
Cancelar
Aplicar
Acciones
Reglas de entrada
Nueva regla...
Filtrar por perfil
Filtrar por estado
Filtrar por grupo
Ver
Actualizar
Exportar lista...
Ayuda
Permitir DNS TCP
Deshabilitar regla
Cortar
Copiar
Eliminar
Propiedades
Ayuda
ESP
18:55
16/06/2025


WindowsServer [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Windows Defender Firewall con seguridad avanzada
Archivo Acción Ver Ayuda
Windows Defender Firewall cor
Reglas de entrada
Reglas de salida
Reglas de seguridad de con
Supervisión
Propiedades: Permitis DNS UDP
Opciones avanzadas
Entidades de seguridad locales
Usuarios remotos
General
Programas y servicios
Equipos remotos
Protocolos y puertos
Ámbito
Protocolos y puertos
Tipo de protocolo: UDP
Número de protocolo: 17
Puerto local: Puertos específicos
53
Ejemplo: 80, 443, 5000-5010
Puerto remoto: Todos los puertos
Ejemplo: 80, 443, 5000-5010
Configuración ICMP:
Personaliz...
Aceptar
Cancelar
Aplicar
Acciones
Reglas de entrada
Nueva regla...
Filtrar por perfil
Filtrar por estado
Filtrar por grupo
Ver
Actualizar
Exportar lista...
Ayuda
Permitis DNS UDP
Deshabilitar regla
Cortar
Copiar
Eliminar
Propiedades
Ayuda
ESP
18:56
16/06/2025

Fase: 4 y 5

Aquí, crearemos un script en PowerShell para crear una carpeta con la fecha actual, copie los archivos del escritorio de esa carpeta y genere un log en formato .txt con el resultado de la copia en el directorio creado previamente en C:\Logs.

Por último dejaremos las configuraciones de red, directivas y añadiremos el código de script.

Código del script para crear una carpeta en C:\Logs:

```
@echo off
mkdir C:\Logs
exit
```

Código para el script en PowerShell sería:

```
$fecha = Get-Date -Format "yyyy-MM-dd"

$carpetaDestino = "C:\Backups\$fecha"

# Si no existe la carpeta, la crea
if (!(Test-Path -Path $carpetaDestino)) {
    New-Item -Path $carpetaDestino -ItemType Directory
}

$escritorio = [Environment]::GetFolderPath("Desktop")

$resultado = Copy-Item -Path "$escritorio\*" -Destination $carpetaDestino -Recurse -Force
-ErrorAction SilentlyContinue -PassThru

$logPath = "C:\Logs\log_copia_$fecha.txt"

Add-Content -Path $logPath -Value "==== Log de copia - $fecha ===="
Add-Content -Path $logPath -Value "Archivos copiados desde: $escritorio"
Add-Content -Path $logPath -Value "Copiados a: $carpetaDestino"
Add-Content -Path $logPath -Value "------------------------------"

foreach ($item in $resultado) {
    Add-Content -Path $logPath -Value "Copiado: $($item.FullName)"
}

Add-Content -Path $logPath -Value "==== Fin del log ===="
```

P.D: He tenido que tirar de búsquedas por Intenet e IA, ya que no tengo experiencia previa en Scripts