Compás
capacitación e investigación

2025

Administración de Servicios de Red con Windows Server 2022:

De la instalación a la gestión de DHCP, DNS, IIS, Proxy y Active Directory

Nancy Loja Mora
Fausto Loja Mora
Ivanna Álvarez Valarezo

Administración de Servicios de Red con Windows Server 2022:

De la instalación a la gestión de DHCP, DNS, IIS, Proxy y Active Directory

Nancy Loja Mora
Fausto Loja Mora
Ivanna Álvarez Valarezo

ISBN: 978-9942-33-953-9 DOI: http://doi.org/10.48190/9789942339539

Compás
capacitación e investigación

© Editorial Grupo Compás, 2025
Guayaqui, Ecuador
www.grupocompas.com
http://repositorio.grupocompas.com

Primera edición, 2025-10-24

ISBN: 978-9942-33-953-9
DOI: http://doi.org/10.48190/9789942339539
Distribución online
Acceso abierto

Cita
Loja, N., Loja, F., Álvarez, I. (2025) Administración de Servicios de Red con Windows Server 2022: De la instalación a la gestión de DHCP, DNS, IIS, Proxy y Active Directory. Editorial Grupo Compás

Prefacio

En el contexto actual, donde la digitalización marca el ritmo del desarrollo empresarial y tecnológico, la administración eficiente de infraestructuras de red y servidores se ha convertido en una competencia esencial para profesionales y estudiantes del área de Tecnologías de la Información. Este libro nace como una guía integral que articula el conocimiento teórico con la aplicación práctica, orientada al fortalecimiento de habilidades clave en la configuración, gestión y optimización de entornos informáticos.

A lo largo de sus capítulos, la obra aborda de manera progresiva y estructurada los principales servicios y herramientas que componen el ecosistema de un sistema operativo moderno, con énfasis en entornos Windows Server. Se abordan servicios como DHCP, indispensable para la asignación dinámica de direcciones IP; DNS, esencial para la resolución de nombres de dominio; e IIS, herramienta fundamental para la publicación de sitios web y aplicaciones. Asimismo, se analiza el uso de servidores proxy, destacando su rol en la regulación del tráfico, la mejora del rendimiento y la seguridad de las redes. Se dedica un capítulo completo a Active Directory, abordando su importancia en la gestión centralizada de usuarios, políticas y recursos en entornos corporativos.

Este libro no solo pretende instruir en el manejo técnico de herramientas específicas, sino también fomentar una comprensión global del entorno operativo, promoviendo el pensamiento crítico, la resolución de problemas y la adopción de buenas prácticas. Su enfoque pedagógico está diseñado para ser accesible, dinámico y aplicable, permitiendo a los lectores enfrentarse con confianza a los retos tecnológicos actuales y futuros.

Introducción

En un contexto marcado por la acelerada transformación digital y la creciente dependencia de las Tecnologías de la Información, la correcta administración de sistemas operativos y servicios de red se ha consolidado como una competencia imprescindible para garantizar la eficiencia operativa, la seguridad informática y la escalabilidad de los servicios en cualquier organización. El reto actual no radica únicamente en dominar herramientas específicas, sino en comprender el funcionamiento integral de las infraestructuras tecnológicas para diseñar, implementar y mantener soluciones seguras y adaptables a entornos cambiantes.

Este libro surge como respuesta a una inquietud recurrente en estudiantes y profesionales: ¿Cómo adquirir competencias técnicas para gestionar, los sistemas y servicios de red como: DHCP, DNS, IIS, PROXY y Active Directory, desde su instalación inicial hasta su administración avanzada? Para resolver esta necesidad, se ha adoptado la Metodología Secuencial de Aprendizaje Teórico–Práctico, que articula los fundamentos conceptuales con la práctica aplicada en entornos virtualizados y reales.

La metodología se aplicó mediante un proceso de análisis documental, diseño de prácticas reproducibles, validación académica en escenarios de aula y un enfoque progresivo que conduce al lector desde lo básico hasta lo avanzado. Cada capítulo combina guías paso a paso, ejemplos contextualizados, comandos verificados, casos de estudio y prácticas supervisadas que permiten afianzar el aprendizaje autónomo y el pensamiento crítico, garantizando que el lector no solo aprenda el "cómo", sino también el "por qué" de cada procedimiento.

A lo largo de este libro, se pretenden resolver problemáticas como:

- ✓ Falta de competencias técnicas en el área TI, muchos usuarios saben instalar un servidor, pero carecen de la visión integral para administrarlo de forma segura y eficiente.

- ✓ Dificultad para comprender y aplicar de forma práctica los servicios de red, configuraciones como DHCP, DNS, IIS, Proxy y Active Directory suelen ser complejas y requieren un enfoque progresivo y didáctico que no siempre está disponible en manuales técnicos.

- ✓ Carencia de materiales que integren teoría y práctica en un mismo recurso,
  La mayoría de manuales de Windows Server se enfocan solo en documentación técnica, mientras que este libro integra fundamentos conceptuales, laboratorios prácticos y autoevaluaciones.

La obra aborda situaciones que los administradores de servidores en Windows Server podrían enfrentar en sus tareas diarias, como, por ejemplo:

- ✓ Errores en la resolución de nombres de dominio, que dificultan el acceso a servicios internos, solucionados mediante la correcta configuración de DNS.

- ✓ Publicación insegura de aplicaciones web, que expone vulnerabilidades al no contar con certificados digitales, atendida a través de la implementación segura de IIS con HTTPS.

- ✓ Uso ineficiente del ancho de banda, ocasionado por accesos no controlados a internet, mitigado mediante la gestión de un servidor proxy.

- ✓ Administración descentralizada de usuarios y permisos, que complica la gestión de recursos, resuelta con la centralización que ofrece Active Directory y sus políticas de grupo.

Para una mejor comprensión el libro se ha organizado en cuatro capítulos:

El Capítulo 1 introduce al lector en la instalación y configuración de Windows Server 2022, edición Datacenter, en sus dos modalidades: con Experiencia de Escritorio y Server Core. Se abordan requisitos previos, creación de cuentas, gestión de usuarios y grupos, directivas de seguridad local, configuración de parámetros TCP/IP y pruebas de conectividad, apoyándose en guías visuales y secuencias de comandos.

El Capítulo 2 profundiza en la implementación de servicios esenciales como DHCP, DNS e Internet Information Services (IIS), imprescindibles para la asignación dinámica de direcciones IP, la resolución de nombres de dominio y la publicación de aplicaciones web. Se detallan configuraciones seguras mediante protocolos cifrados como HTTPS, gestión de puertos y administración de certificados digitales.

El Capítulo 3 analiza el uso estratégico de servidores proxy para control de tráfico, filtrado de contenido, protección perimetral y optimización de recursos. Se describen los tipos de proxy más utilizados, sus beneficios y sus aplicaciones, con prácticas basadas en Squid y Nginx que incluyen políticas de acceso, autenticación de usuarios y monitoreo de tráfico.

El Capítulo 4 está dedicado a Active Directory como herramienta centralizada para la administración de recursos y usuarios. Se abordan la creación de dominios, la gestión de cuentas, grupos y unidades organizativas, así como la implementación de directivas

de grupo (GPO) para establecer configuraciones, restricciones y permisos de forma estandarizada.

Más allá de la transferencia de conocimientos, esta obra busca formar profesionales capaces de evaluar, diseñar e implementar infraestructuras informáticas que respondan a las demandas de la era digital. Si bien las herramientas y versiones evolucionan, los fundamentos y buenas prácticas adquiridos aquí constituirán una base para adaptarse a cualquier innovación tecnológica futura.

Objetivo general

Consolidar en estudiantes y profesionales de Tecnologías de la Información competencias para la instalación, configuración y administración de Windows Server 2022 y sus principales servicios de red, mediante una guía estructurada en un enfoque teórico–práctico para la comprensión del aprendizaje desde los fundamentos de la instalación del sistema operativo hasta la gestión avanzada de servicios como DHCP, DNS, IIS, Proxy y Active Directory.

Contenido

CAPÍTULO 1

INSTALACIÓN Y ADMINISTRACIÓN DEL SISTEMA OPERATIVO.

Instalación y Administración de Windows Server 2022

Objetivos

Introducir conceptualmente al sistema operativo Windows Server 2022 en sus opciones con experiencia de escritorio y core.

Desarrollar competencias técnicas para la instalación del sistema operativo Windows Server Datacenter 2022 en sus opciones con experiencia de escritorio y core.

Administrar de forma básica el sistema operativo Windows Server Datacenter 2022 en sus opciones con experiencia de escritorio y core

En el contexto actual de la transformación digital, la infraestructura tecnológica que sostiene a las organizaciones requiere de sistemas operativos robustos, seguros y eficientes. Windows Server 2022 se posiciona como una solución avanzada que ofrece una amplia gama de herramientas para la gestión de redes, servicios y recursos compartidos, con especial atención en la administración centralizada, la seguridad reforzada y la integración con servicios en la nube.

Este capítulo presenta una guía para llevar a cabo la instalación y administración inicial del sistema operativo Windows Server Datacenter 2022 con experiencia de escritorio, se abordan aspectos como: la configuración básica, cuentas, grupos de usuarios, directivas de seguridad local y la configuración del protocolo TCP/IP. Asimismo, con Windows Server Datacenter con la opción Core, se presentan aspectos como: la administración de usuarios, grupos, configuración TCP/IP y administración del servicio

de DHCP. La finalidad es que el lector adquiera no solo conocimientos teóricos, sino también habilidades prácticas que le permitan desenvolverse con solvencia en la administración de sistemas operativos Windows Server en escenarios reales.

Preguntas de enfoque

Preguntas de Inicio

1. ¿Qué es Windows Server 2022 y qué mejoras ofrece con respecto a versiones anteriores del sistema operativo?
2. ¿En qué se diferencia la instalación con experiencia de escritorio de la instalación en modo Server Core?
3. ¿Por qué es importante aplicar directivas de seguridad local y una adecuada gestión de cuentas de usuario tras la instalación del sistema operativo?

Competencias o Problemas a Resolver

Al finalizar este capítulo, los lectores serán capaces de:

- Comprender los conceptos fundamentales relacionados con la instalación y configuración inicial de Windows Server 2022.
- Realizar una instalación limpia del sistema operativo, considerando tanto la edición con entorno gráfico como la edición Server Core.
- Administrar cuentas, grupos de usuarios y directivas de seguridad desde la interfaz gráfica y mediante consola.
- Establecer configuraciones de red de forma manual, incluyendo la asignación de parámetros como: la dirección IP, la máscara de subred, las direcciones de los servidores DNS, entre otros elementos necesarios para el correcto funcionamiento de la red. Por otro lado, también se establecerá la configuración

dinámica a través del protocolo DHCP para la asignación automática de los parámetros de red.

Problemas a Resolver

1. ¿Cómo se configura correctamente una máquina virtual para instalar Windows Server 2022 de forma eficiente?
2. ¿Qué criterios se deben considerar para decidir entre Server Core y la versión con experiencia de escritorio en distintos entornos de red?
3. ¿Cómo se pueden aplicar políticas de seguridad para proteger las cuentas de usuario y restringir el acceso no autorizado?
4. ¿De qué forma puede automatizarse o simplificarse la configuración inicial del servidor utilizando herramientas administrativas o comandos PowerShell?

Windows Server 2022

Windows Server 2022 es un sistema operativo producido por Microsoft para su familia de servidores de Microsoft NT que se lanza bajo la marca Windows Server y está basado en Windows 10. Es similar al sistema operativo Microsoft Windows con la principal diferencia de que está enfocado al área de servidores. Se encuentra disponible es sus versiones: Estándar y Datacenter, para centros de datos y Datacenter Azure para centros de datos que utilicen Azure.

- Windows Server Standard: Se usa para entornos físicos o muy poco virtualizados. La licencia se basa en núcleos del servidor. Admite un máximo de 2 máquinas virtuales y necesita CAL (Client Access Licenses).
- Windows Server Datacenter: Creada para centros de datos y procesamiento en la nube con un alto nivel de virtualización, el número de máquinas virtuales es ilimitado. La licencia se basa en núcleos del servidor y también necesita CAL (Client Access Licenses).
- Windows Server Datacenter Azure: Edición para la nube basada en la Datacenter, ofrece un sistema operativo virtualizado con características avanzadas como SMB, revisión en caliente y redes extendidas de Azure. Ruiz (2023).

Ofrece las opciones de instalación de experiencia de escritorio (interfaz de escritorio completa) y de core (interfaz de usuario mínima).

- Windows Server experiencia de escritorio: esta es una opción completa que incluye la Interfaz gráfica de usuario (GUI).
- Windows Server core: no incluye la interfaz GUI, se puede administrar el servidor desde la línea de comandos, mediante PowerShell, Sconfig o métodos remotos (Microsoft, 2023).

Características de Windows Server 2022

Según (Microsoft, 2023b) entre las características más destacables que nos presenta Windows server 2022 tenemos:

Seguridad: incorpora nuevas funciones de seguridad que se integran con otras ya existentes para ofrecer una protección más sólida y completa. Estas mejoras combinan distintas capas de defensa que trabajan juntas para proteger el sistema frente a amenazas avanzadas. Gracias a este enfoque de seguridad en profundidad, los servidores cuentan con el nivel de protección que necesitan en el entorno actual, cada vez más expuesto a riesgos.

Transporte: HTTPS y TLS 1.3 habilitados de forma predeterminada: Habilita comunicaciones seguras de forma automática con los protocolos HTTPS y TLS 1.3. Esta tecnología cifra los datos para garantizar una conexión segura entre el servidor y los usuarios, protegiendo así la información que se transmite.

Centro de Administración de Windows (Windows Admin Center): Windows Admin Center, ahora incluye nuevas funcionalidades que permiten visualizar de forma clara el estado actual de las principales características de seguridad del sistema, además si alguna de estas funciones no está activada, el administrador puede habilitarlas directamente desde la misma herramienta.

Navegador de internet Microsoft Edge: Se incluye con Windows Server 2022, como reemplazo de Internet Explorer, está respaldado por la seguridad e innovación de Microsoft y se puede utilizar con las opciones de instalación de Servidor con Experiencia de escritorio.

Mejoras en el rendimiento de conexiones UDP: Introduce importantes mejoras que optimizan el rendimiento de las conexiones basadas en UDP, entre ellas la descarga de segmentación UDP (USO), que permite que el trabajo pesado de enviar paquetes se realice directamente desde el adaptador de red, aliviando la carga del procesador. A esto se suma la función de fusión de recepción UDP (UDP RSC), que agrupa paquetes entrantes para reducir aún más el uso de la CPU.

Mejoras en el rendimiento de conexiones TCP: Mejora la eficiencia de las conexiones basadas en TCP, el protocolo más utilizado en Internet. Ahora incluye TCP HyStart++, una tecnología que reduce la pérdida de paquetes cuando una conexión está comenzando, especialmente útil en redes de alta velocidad, además incorpora RACK, una función que disminuye los tiempos de espera cuando es necesario reenviar paquetes, lo que agiliza la comunicación y mejora la estabilidad de las conexiones.

Mejoras en la reversión de Windows Update: Si el problema aparece después de instalar actualizaciones de Windows o nuevos controladores, el sistema detecta esto y elimina automáticamente esas actualizaciones para que el equipo vuelva a funcionar con normalidad y los servidores se recuperen por sí solos del error.

Análisis comparativo entre Windows Server 2022 y su antecesor Windows Server 2019

Windows Server 2022 comparado con su predecesor Windows Server 2019, presenta mejoras importantes como: seguridad, rendimiento y también conectividad en la nube. Además, refuerza la protección contra amenazas modernas mediante múltiples capas de seguridad, incluyendo el uso predeterminado de TLS 1.3 para comunicaciones cifradas. En cuanto a la integración con servicios

en la nube, Windows Server 2022 presenta su compatibilidad mejorada con Azure, permitiendo una administración híbrida más eficiente gracias a herramientas como Azure Arc y Windows Admin Center. También se introduce el soporte para SMB over QUIC, una alternativa segura al VPN tradicional para el acceso remoto a archivos. En el ámbito del rendimiento, Windows Server 2022 optimiza las conexiones TCP y UDP con tecnologías como TCP HyStart++ y UDP RSC, lo que se traduce en una mayor estabilidad y velocidad en redes de alta demanda. Además, se mejora la compatibilidad con contenedores y aplicaciones, facilitando el despliegue en entornos modernos de desarrollo. Ambas versiones mantienen soporte para virtualización con Hyper-V, pero Windows Server 2022 ofrece una experiencia más robusta y segura, especialmente en su edición Datacenter: Azure Edition, que permite actualizaciones sin reinicio mediante Hotpatching. En resumen, Windows Server 2022 no solo conserva las capacidades de Windows Server 2019, sino que las amplía con un enfoque claro en la seguridad, la eficiencia operativa y la conectividad con la nube, posicionándose como una solución más completa para organizaciones que buscan modernizar su infraestructura TI Microsoft. (2021a), Microsoft. (2025a), Microsoft. (2025b).

A continuación, se presenta la Tabla 1 con la comparación entre ambas versiones.

Tabla 1. *Comparación entre Windows Server 2022 y Windows Server 2019*

Característica	Windows Server 2019	Windows Server 2022
Seguridad avanzada	Básica	Multicapa con Secured-core, TLS 1.3
Integración con Azure	Limitada	Mejorada con Azure Arc y Automanage
Hotpatching	No disponible	Disponible en Azure Edition
SMB over QUIC	No disponible	Disponible para acceso remoto seguro
Windows Admin Center	Compatible	Compatible y mejorado
Contenedores y compatibilidad	Compatible	Mejor compatibilidad y menor tamaño de imagen
Rendimiento de red	Estándar	Mejoras con TCP HyStart++, RACK y UDP RSC
Virtualización	Hyper-V	Hyper-V con mejoras de seguridad y rendimiento
Windows Subsystem for Linux	Disponible	Disponible y mejorado

Fuente: Elaboración propia

Instalación de Windows Server 2022 Datacenter con Experiencia de Escritorio en VirtualBox.

Antes de proceder con la instalación de Windows Server 2022 Datacenter con Experiencia de Escritorio, es fundamental asegurarse de que el equipo cumpla con los requisitos mínimos del sistema. Esto garantiza una instalación exitosa y un rendimiento adecuado del sistema operativo. Microsoft. (2023b).

Requisitos previos para instalación

Tabla 2. Requisitos mínimos para la instalación de Windows Server 2022

Componente	Requisito
Procesador	64 bits a 1,4 GHz
Memoria Ram	2 GB
Almacenamiento	36 GB*
Red	Adaptador gigabit ethernet

Fuente: Elaboración propia

* Los equipos con más de 16 GB de RAM necesitarán más espacio en disco para los archivos de paginación, hibernación y volcado.

Proceso de instalación y configuración

Para proceder a la instalación del sistema operativo, accedemos a la página oficial de Microsoft para realizar la descarga del mismo. Escogemos la opción de idioma y arquitectura que se adecué a nuestras necesidades y procedemos a la descarga. En este caso vamos a trabajar con un escenario virtualizado, para ello necesitamos crear una máquina virtual. Esta configuración permite emular un entorno de servidor sin afectar el sistema operativo anfitrión.

Los pasos previos son:

a. Crear nueva máquina virtual y seleccionar el modo típico o personalizado.
b. Seleccionar el archivo ISO correspondiente a la versión de Windows Server 2022.
c. Asignar nombre a la máquina virtual y seleccionar la ubicación de almacenamiento.

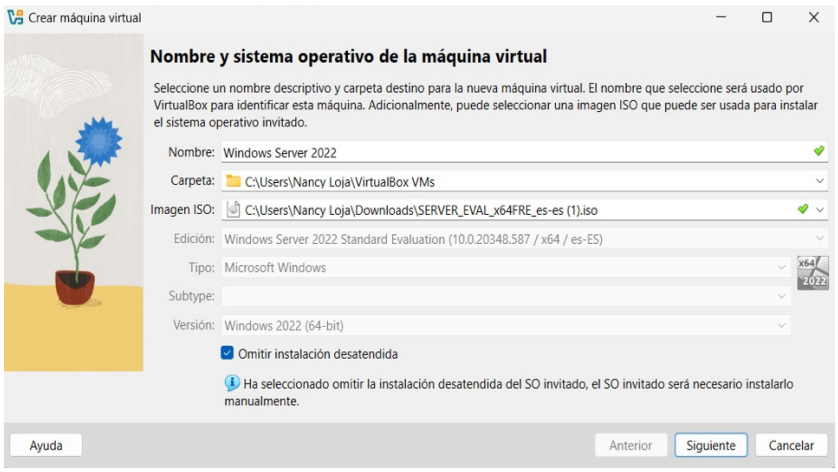


Ilustración 1. Creación de la máquina virtual

Fuente: Elaboración propia

d. Definir las características de hardware, en este caso:

- Memoria RAM: mínimo 4 GB.
- Número de procesadores: 1.
- Disco duro virtual: 60 GB.

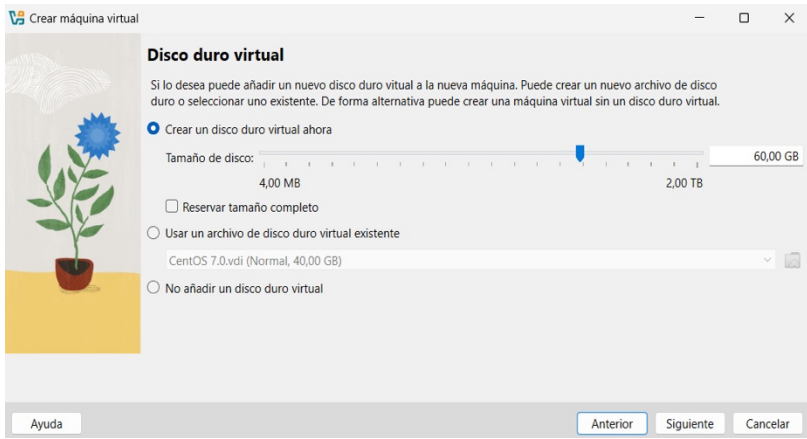


Ilustración 2. Configuración del disco duro virtual

Fuente: Elaboración propia

Inicio de la Máquina Virtual: Para ello se hace clic en "Iniciar" para comenzar el proceso de instalación. Al hacer esto, se inicia el asistente gráfico de instalación. En esta etapa, se seleccionan el idioma, el formato de hora y moneda, y el tipo de teclado. Se procede haciendo clic en "Siguiente" y luego en "Instalar ahora".

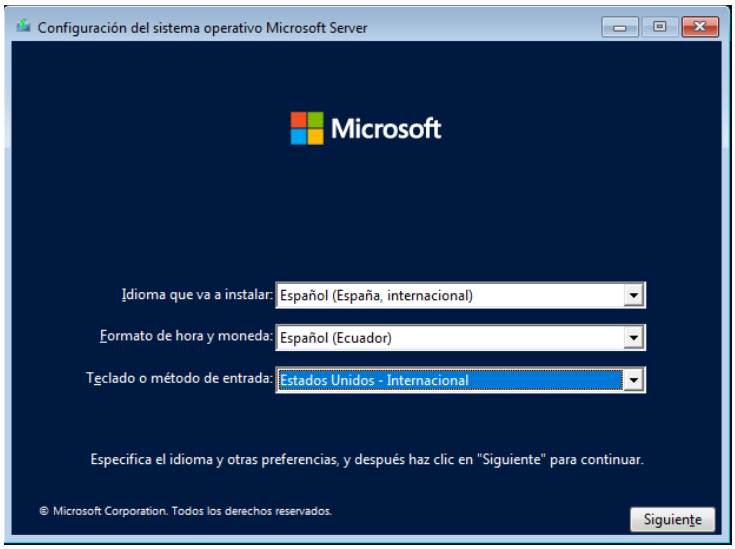
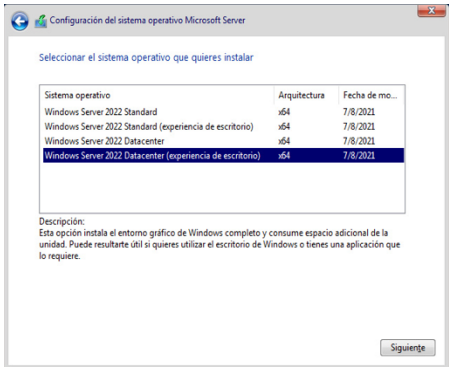


Ilustración 3. Inicio del asistente de instalación

Fuente: Elaboración propia

Se elige la versión del sistema operativo, en este caso "Windows Server 2022 Datacenter (Experiencia de Escritorio)". Esta opción incluye la interfaz gráfica de usuario (GUI), facilitando la administración del servidor. Luego se acepta el acuerdo de licencia marcando la casilla correspondiente, y se hace clic en "Siguiente".



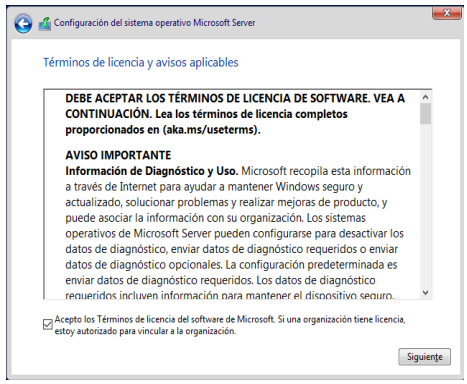


Ilustración 4. Selección de edición del sistema

Fuente: Elaboración propia

Ilustración 5. Aceptación de términos de licencia

Fuente: Elaboración propia

En la siguiente interfaz, se selecciona la opción "Personalizada: instalar solo Windows (avanzado)", ya que se trata de una instalación limpia. En esta pantalla se elige el disco duro virtual o físico en el que se instalará el sistema operativo. En caso de ser necesario, se puede formatear o crear particiones desde esta interfaz.

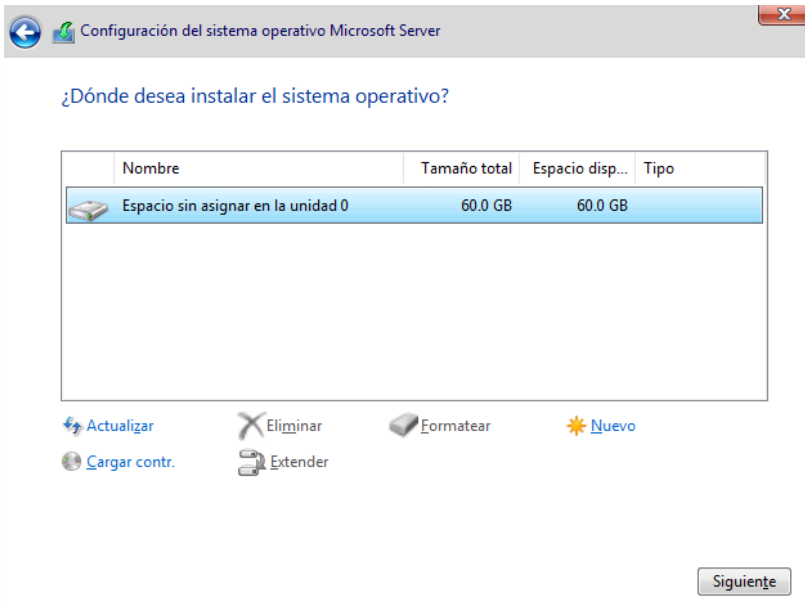


Ilustración 6. Selección del disco de instalación

Fuente: Elaboración propia

El sistema comienza la copia de archivos y la instalación de características. Este proceso puede tardar varios minutos dependiendo del hardware disponible. Una vez finalizado, el sistema se reinicia automáticamente.

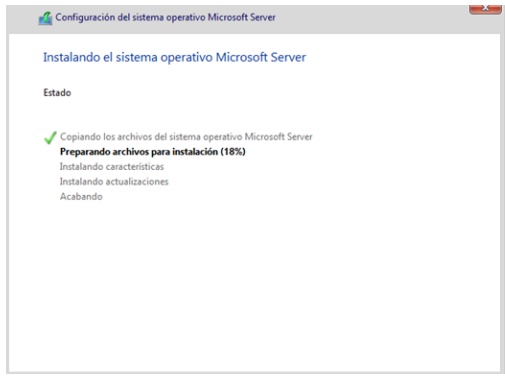


Ilustración 7. Proceso de instalación

Fuente: Elaboración propia

Tras el reinicio, se solicita establecer una contraseña para la cuenta de administrador local. Es importante usar una contraseña robusta conforme a políticas de seguridad mínimas del sistema operativo como: (incluir, mayúsculas, minúsculas, números o signos, que no contenga el nombre del usuario y mínimo 6 caracteres).

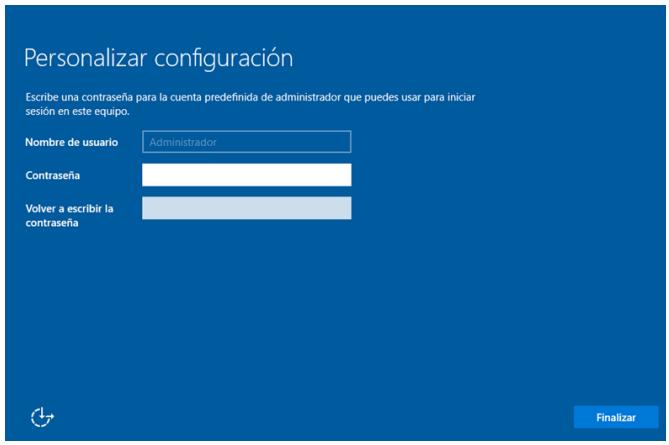


Ilustración 8. Configuración inicial

Fuente: Elaboración propia

Con la contraseña configurada, se accede por primera vez al sistema operativo. Se presenta el entorno gráfico de Windows Server 2022, listo para la instalación de roles y características según los requerimientos del servidor.

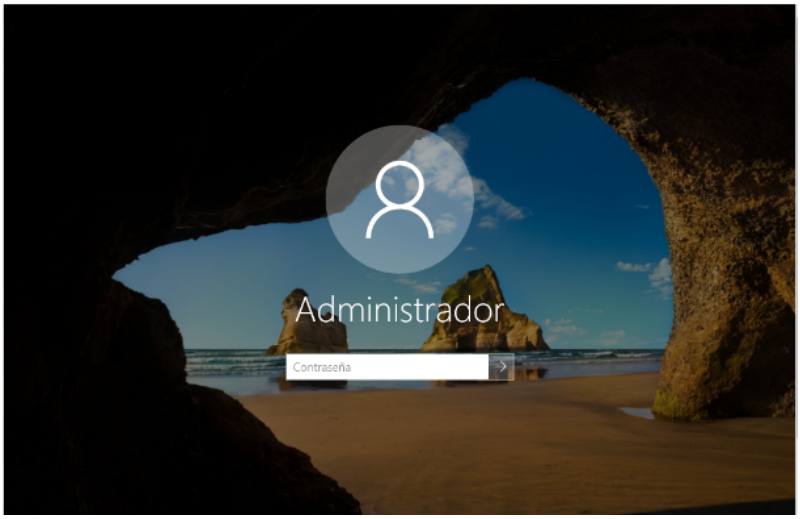


Ilustración 9. Inicio de sesión

Fuente: Elaboración propia

Al ingresar al sistema operativo, nos presenta por defecto la ventana del "Administrador de Servidor" (Server Manager), que es una herramienta centralizada para administrar y configurar servidores locales y remotos.

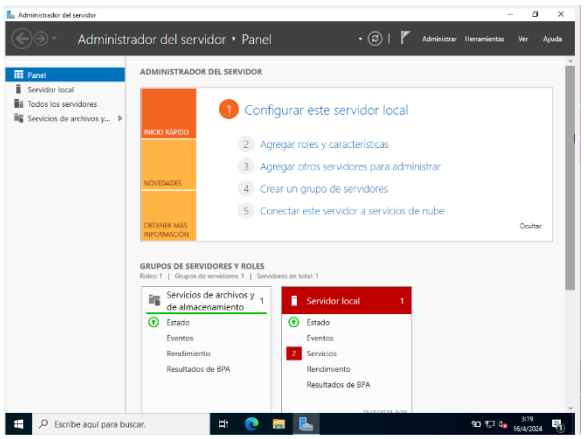


Ilustración 10. Inicio de sesión

Fuente: Elaboración propia

Administración del Sistema Operativo

Cuentas de usuario

Para el manejo de las cuentas de usuario, Windows Server ofrece diversas opciones entre las cuales se encuentran:

- **Agregar una cuenta de usuario**, esta configuración permite la creación de nuevas cuentas de usuario mediante las cuales tendrá accedo ala servidor y sus diferentes recursos de red.
- **Quitar una cuenta de usuario**, esta opción elimina la cuenta seleccionada junto con los permisos que le fueron asignados, esta de ser necesario ser pueden remover los archivos contenidos en la cuenta. Como una alternativa a la eliminación de la cuenta se la puede desactivar dejando inhabilitado el acceso a los equipos.
- **Ver cuentas de usuario**, esta característica permite visualizar las cuentas existentes junto con información adicional de las mismas.

- **Cambiar el nombre para mostrar de la cuenta de usuario**, esta opción permite cambiar el nombre a mostrar de la cuenta. Esto no cambia el nombre propio de la cuenta solo facilita el reconocimiento de usuarios.
- **Activar una cuenta de usuario**, esta característica permite habilitar una cuenta para que pueda acceder a los equipos de la red y sus recursos.
- **Desactivar una cuenta de usuario**, esta configuración deshabilita la cuenta de usuario seleccionada de manera temporal, por lo que el usuario de la cuenta no tendrá ningún acceso. En conjunto con esto, los servicios de Microsoft 365 y otros recursos también serán desactivados al estar asignada una cuenta en línea.

Administración de usuarios

Para realizar una administración de usuarios, se debe realizar las configuraciones desde la herramienta de "Administrador del servidor", la cual solo puede ser ejecutada en la cuenta de administrador. Al abrir la herramienta de administración se selecciona el apartado "Herramientas" y la opción "Administración de equipos".

Ilustración 11. Administrador del servidor

En la ventana de administración de equipos se escoge la opción de "Herramientas del sistema" y realizando un clic derecho sobre "Usuarios y grupos locales" se selecciona "Nuevo usuario".

A continuación, se procederá a realizar la creación de una cuenta de usuario con el permiso de que cambie la contraseña al siguiente inicio de sesión.

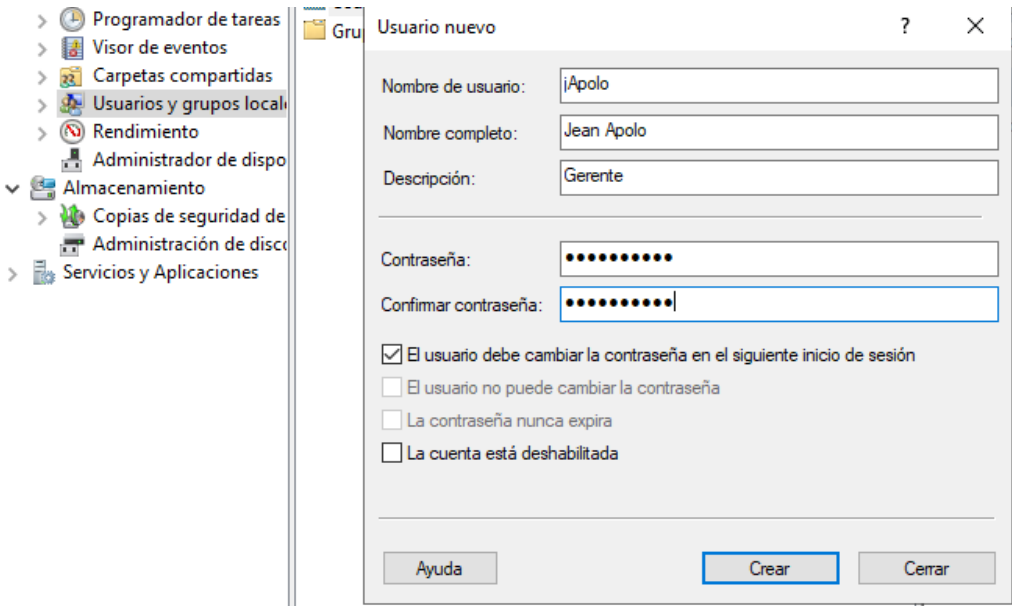


Ilustración 12. El Usuario debe cambiar la contraseña en el siguiente inicio

Fuente: Elaboración propia

Como se puede observar, al iniciar sesión con esta cuenta es necesario realizar el cambio de contraseña para continuar.

Ilustración 13. Permitir que cambie la contraseña al siguiente inicio de sesión

Fuente: Elaboración propia.

Cuentas de usuario locales predeterminadas

Según Microsoft (2023d), Windows Server permite a los usuarios acceder a la información y archivos contenidos dentro del servidor, así como realizar funciones de administración de archivos y configuración. Los usuarios pueden ingresar en los equipos de la red al tener una cuenta de usuario, el inicio de sesión requiere el nombre de usuario y contraseña.

Windows Server tiene algunas cuentas de usuario locales predeterminadas como:

- **Administrador:** es una cuenta especial que se crea automáticamente al instalar Windows. Tiene el control total

sobre el sistema: puede acceder a todos los archivos, configurar servicios, crear otros usuarios y cambiar permisos cuando sea necesario. Aunque esta cuenta no se puede eliminar ni bloquear, sí es posible desactivarla o cambiarle el nombre por seguridad. De hecho, Windows suele desactivarla por defecto y crea otra cuenta de administrador durante la instalación.

- Invitado: La cuenta de invitado, está pensada para personas que necesitan usar un equipo de forma ocasional, sin tener una cuenta propia. Les permite iniciar sesión temporalmente, pero con permisos muy limitados. Por defecto, esta cuenta viene desactivada y sin contraseña, lo que representa un riesgo de seguridad, ya que podría facilitar el acceso anónimo al sistema. Por eso, se recomienda mantenerla deshabilitada, a menos que sea estrictamente necesario activarla.
- HelpAssistant: es una cuenta local que se activa automáticamente cuando alguien solicita ayuda a través de una sesión de asistencia remota en Windows. Esta cuenta permite que otra persona pueda conectarse de forma controlada al equipo para brindar soporte.
- DefaultAccount: La cuenta DefaultAccount es una cuenta estándar, (también llamada *cuenta administrada del sistema predeterminado* o DSMA) es una cuenta especial del sistema en Windows. Está diseñada para ejecutar procesos que no dependen de un usuario específico, y que pueden funcionar con varios usuarios. Por seguridad, esta cuenta viene desactivada por defecto en versiones de escritorio y en servidores con entorno gráfico.

Recomendaciones del manejo de clave de los usuarios

El acceso a la información que contienen los equipos de una organización debe ser altamente restringido, es por eso que se

recomienda seguir ciertas recomendaciones para aumentar la seguridad de los recursos. De esta manera se pretende evitar el acceso indebido por parte de intrusos a los datos y demás información del servidor como lo señala López Pérez (2015). En el sistema operativo Windows Server 2022, la contraseña debe cumplir algunos requisitos de complejidad:

- Longitud de la contraseña, es siempre recomendable optar por una contraseña de larga longitud para maximizar la seguridad, en el caso de Windows Server se recomienda mínimo 6 caracteres.
- Complejidad de la contraseña, de la misma manera se aconseja que se realicen combinaciones de caracteres entre letras mayúsculas y minúsculas (a-z, A-Z), números naturales (0-9) y símbolos (como ;, !, @, #, _ y -). Estas combinaciones son menos predecibles y evitan el acceso no autorizado a diferencia de contraseñas que contengan algún tipo de información personal.
- Duración de la contraseña, es recomendable que el usuario realice continuos cambios de contraseña cada 180 días.

Grupos de usuarios locales

Los grupos de usuarios locales en Windows Server son un conjunto de usuarios y/o grupos de dominio que tienen permisos y derechos específicos para el equipo en el que se definen. Estos grupos se gestionan a través de la herramienta "Usuarios y grupos locales" y se utilizan para controlar el acceso a recursos locales como carpetas compartidas, impresoras, etc. También existen grupos locales predeterminados que se crean automáticamente al instalar el sistema operativo, algunos de ellos son:

- Administradores: Los miembros de este grupo tienen control total del equipo y pueden asignar derechos de usuario y permisos de control a los usuarios según sea necesario.
- Operadores de copia de seguridad: Los miembros de este grupo pueden realizar copias de seguridad y restaurar archivos en un equipo, sin importar los permisos que protejan esos archivos.
- Operadores de configuración de red: Los usuarios de este grupo pueden realizar la administración TCP/IP.
- Operadores criptográficos: Reúne a cuentas autorizadas a realizar operaciones criptográficas.

Administración de grupos

Para realizar la administración de grupos, se debe realizar las configuraciones desde la herramienta de "Administrador del servidor". Al abrir la herramienta de administración se selecciona el apartado "Herramientas" y la opción "Administración de equipos", luego se hace clic en "Usuarios y Grupos Locales". Para agregar usuarios al grupo, se debe seleccionar los usuarios del grupo y la ubicación del grupo local y se establece el nombre y descripción del grupo.

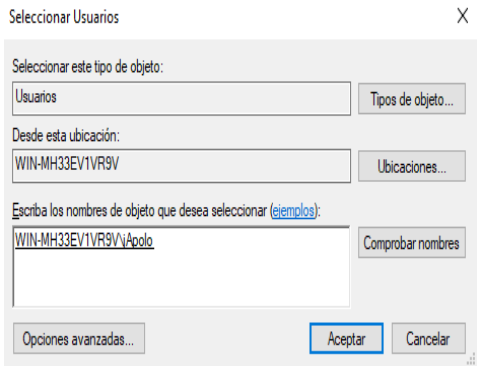


Ilustración 14. Selección de usuarios para un grupo nuevo

Fuente: Elaboración propia

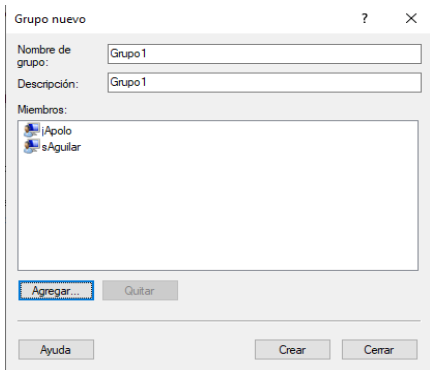


Ilustración 15. Agregar nuevo usuario

Fuente: Elaboración propia

Directivas de seguridad local (Asignación de derechos de usuarios)

Windows Server proporciona algunas directivas de seguridad local, para la asignación de derechos de usuarios. A continuación, se muestran las siguientes:

Tabla 3. Asignación de derechos de usuarios

Directiva	Descripción
Administrar registro de seguridad y auditoría	Indica qué usuarios pueden especificar opciones de auditoría de acceso a objetos para recursos individuales, como archivos, objetos de Active Directory y claves del Registro.

Apagar el sistema	Determina los usuarios que, habiendo iniciado sesión localmente en el equipo, pueden cerrar el sistema con el comando Apagar.
Cambiar la hora del sistema	Determina qué usuarios y grupos pueden cambiar la fecha y hora del reloj interno del equipo.
Cambiar la zona horaria	Determina que los usuarios y grupos que pueden cambiar la zona horaria que usa el equipo para mostrar la hora local, que es la hora del sistema más el desplazamiento de la zona horaria.
Denegar el acceso desde la red a este equipo	Determina qué usuarios no pueden obtener acceso a un equipo a través de la red.
Denegar el inicio de sesión como servicio	Determina qué cuentas de servicio no pueden registrar un proceso como un servicio.
Denegar el inicio de sesión localmente	Esta configuración de seguridad determina qué usuarios no pueden iniciar sesión en el equipo.
Denegar inicio de sesión a través de	Esta configuración de seguridad determina qué usuarios y grupos tienen prohibido iniciar sesión como clientes de Servicios de Escritorio remoto.

Servicios de Escritorio remoto	
Forzar cierre desde un sistema remoto	Indica qué usuarios tienen permiso para apagar un equipo desde una ubicación remota de la red.
Generar auditorías de seguridad	Determina qué cuentas puede usar un proceso para agregar entradas al registro de seguridad. El registro de seguridad se usa para seguir paso a paso el acceso no autorizado al sistema.
Hacer copias de seguridad de archivos y directorios	Este derecho de usuario determina qué usuarios pueden omitir los permisos de archivos y directorios, del Registro y otros permisos de objetos persistentes para hacer una copia de seguridad del sistema.
Permitir el inicio de sesión local	Determina los usuarios que pueden iniciar sesión en el equipo.
Permitir inicio de sesión a través de Servicios de Escritorio remoto	Esta configuración de seguridad determina qué usuarios o grupos tienen permiso para iniciar sesión como un cliente de Servicios de Escritorio remoto.
Restaurar archivos y directorios	Indica qué usuarios pueden omitir los permisos de archivo, directorio, Registro y otros objetos persistentes al restaurar los archivos y directorios de los que se hizo una copia de seguridad, y determina qué usuarios

	pueden establecer cualquier entidad de seguridad válida como propietario del objeto.
Tener acceso a este equipo desde la red	Este derecho de usuario determina qué usuarios y grupos tienen permiso para conectarse al equipo a través de la red. Este derecho de usuario no afecta a Servicios de Escritorio remoto.
Tomar posesión de archivos y otros objetos	Esta configuración de seguridad determina qué usuarios pueden tomar posesión de cualquier objeto del sistema que se pueda proteger, incluidos los objetos de Active Directory, los archivos y carpetas, las impresoras, las claves del Registro, los procesos y los subprocesos.

Fuente: (Microsoft, 2025b).

Administración de asignación de derechos de usuario

Mediante la herramienta de administración del servidor se puede asignar diferentes permisos a las cuentas de usuario estándares. A continuación, se le dará permiso a un usuario para cambiar la hora del sistema y a otro usuario que tenga el permiso de apagar el sistema.

Para asignarle los permisos a los usuarios se debe buscar la ruta en el administrador del servidor (Herramientas > Directiva de seguridad local > Directivas locales > Asignación de derechos de

usuario) en este apartado se encuentran los permisos que se le puede asignar a la cuenta de usuario.

A continuación, vamos a seleccionar un permiso para la cuenta "sAguilar". Para ello, accedemos a "Asignación de derechos de usuario" a través de Herramientas, luego escogemos el permiso necesario, en este caso hacemos doble clic en "Cambiar la hora del sistema".

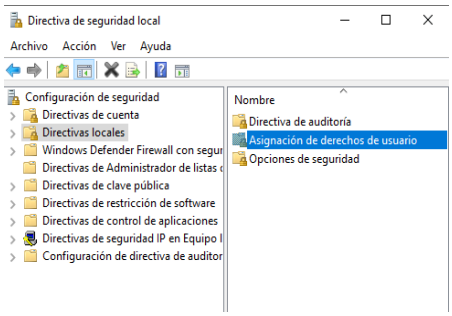


Ilustración 16. Asignación derechos usuario

Fuente: Elaboración propia

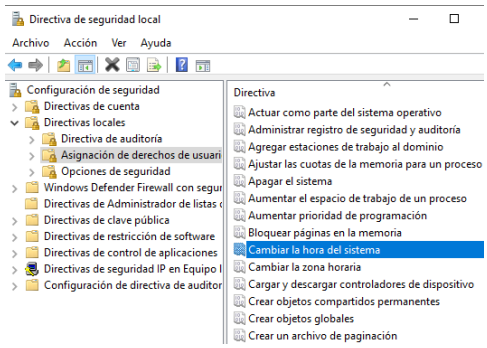


Ilustración 17. Permisos del sistema

Fuente: Elaboración propia

Se muestra la pantalla de "Configuración de seguridad local", aquí se hace clic en "Agregar usuario o grupo", después se muestra la pantalla de "Seleccionar Usuarios o Grupo" en donde se selecciona la cuenta a la que se le va a asignar el mencionado permiso.

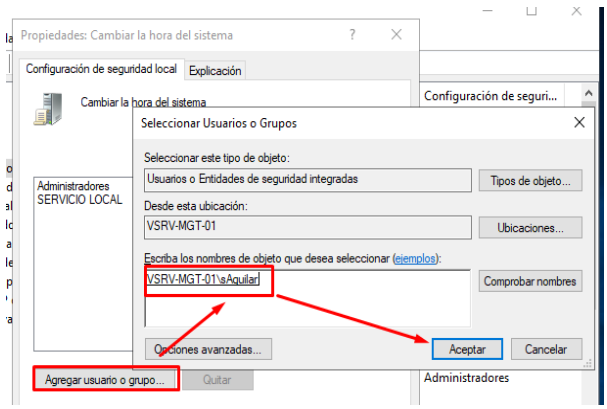


Ilustración 18. Asignación de permisos

Fuente: Elaboración propia

Se puede observar que, al entrar en la configuración del sistema con el usuario sAguilar, el mismo ya tiene el permiso para "Cambiar la hora del sistema".

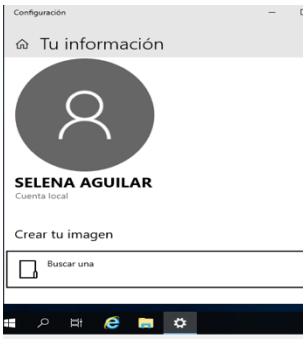


Ilustración 19. Ingreso con el usuario

Fuente: Elaboración propia

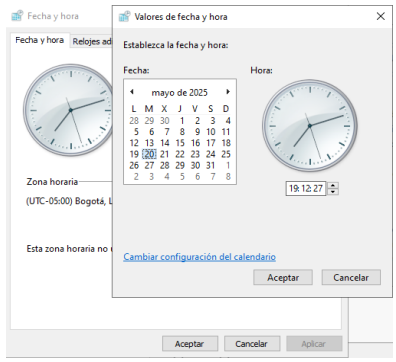


Ilustración 20. Prueba del permiso para la configuración de hora y fecha

Fuente: Elaboración propia

Configuración de red y prueba de conectividad en Windows Server 2022 (GUI)

Una vez finalizada la instalación del sistema operativo y la administración básica de cuentas, es indispensable configurar correctamente la red. Este proceso permite que el servidor se comunique con otros dispositivos, acceda a recursos compartidos y forme parte de una red organizacional o académica. A continuación, se describe la configuración de una dirección IP estática, pruebas de conectividad y comandos esenciales para diagnóstico de red.

Configuración de dirección IP estática

Para establecer una dirección IP manual en el servidor con interfaz gráfica, se accede al Centro de redes y recursos compartidos y se selecciona la opción Cambiar configuración del adaptador. Posteriormente, se accede a las propiedades del adaptador de red activo, se selecciona el protocolo TCP/IPv4 y se define lo siguiente:

- Dirección IP: 10.0.0.3
- Máscara de subred: 255.0.0.0
- Puerta de enlace predeterminada: 10.0.0.1
- Servidor DNS (opcional, si no se gestiona aún)

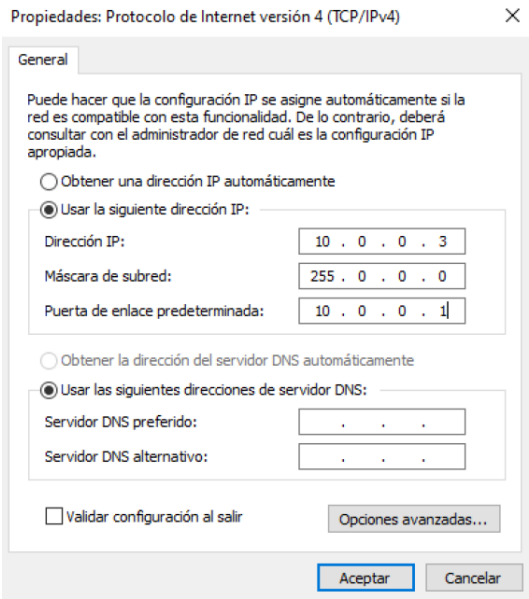


Ilustración 21. Configuración manual de la dirección IP en Windows Server 2022 (GUI).

Fuente: Elaboración propia

Esta asignación garantiza una identificación única en la red local y permite una administración más estable de servicios críticos. Para servidores, se recomienda el uso de direcciones IP estáticas para evitar conflictos.

Verificación de configuración con ipconfig

Una vez aplicada la configuración, se abre la consola CMD o PowerShell y se ejecuta el comando:

```
ipconfig /all
```

Este comando muestra detalles como la dirección física (MAC), la dirección IP asignada, la puerta de enlace y el estado del

arrendamiento si se usa DHCP. En la configuración estática, estos datos se mantienen constantes.

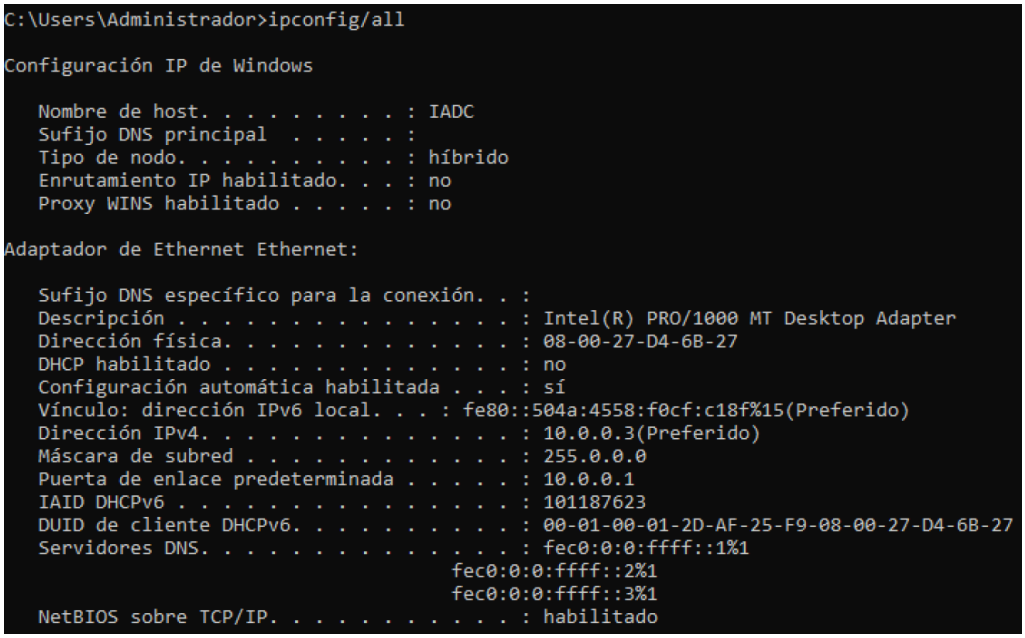


Ilustración 22. Verificación de parámetros de red mediante el comando ipconfig /all.

Fuente: Elaboración propia

Comandos de diagnóstico IP

Se utilizan los siguientes comandos para liberar y renovar la dirección IP del adaptador:

- ipconfig /release: libera la IP actual (aplicable si se usaba DHCP).

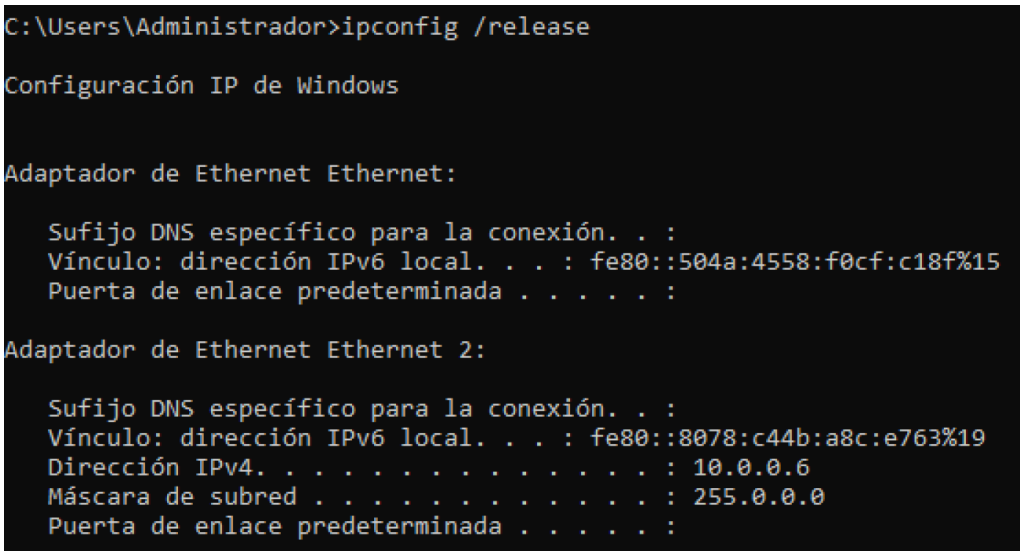


Ilustración 23. Ejecución del comando ipconfig /release para liberar la IP actual.

Fuente: Elaboración propia

- ipconfig /renew: solicita una nueva IP al servidor DHCP.

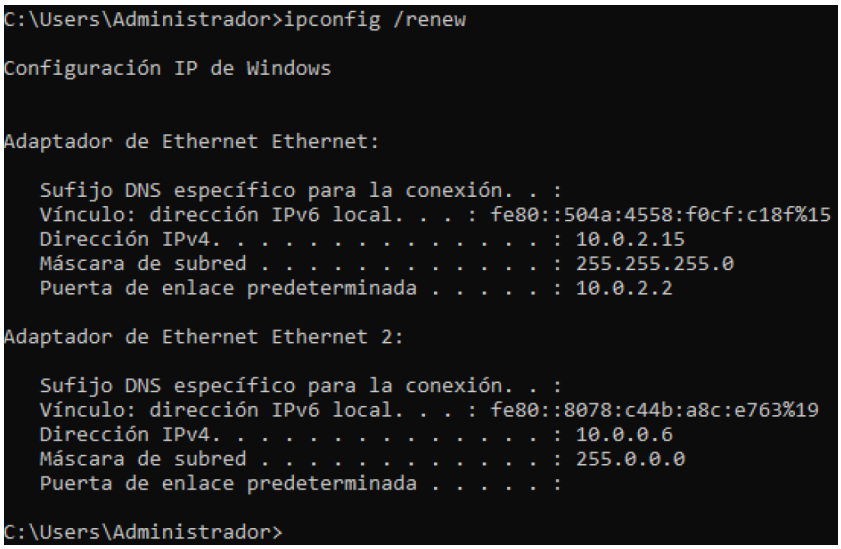


Ilustración 24. Ejecución del comando ipconfig /renew para renovar la dirección IP.

Fuente: Elaboración propia

Estos comandos resultan útiles cuando se requiere reiniciar la conexión con el servidor de direcciones o solucionar conflictos en la red.

Pruebas de conectividad

Para comprobar que el servidor tiene conectividad, se utilizan los siguientes comandos ping:

1. ping 127.0.0.1: Verifica que el protocolo TCP/IP funciona correctamente de forma local.

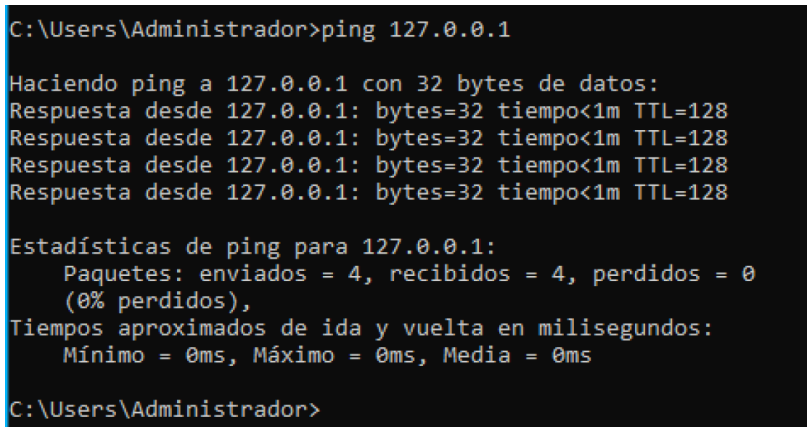


Ilustración 25. Prueba de conectividad local utilizando ping 127.0.0.1.

Fuente: Elaboración propia

2. ping 10.0.0.3: Prueba la comunicación interna del adaptador de red.

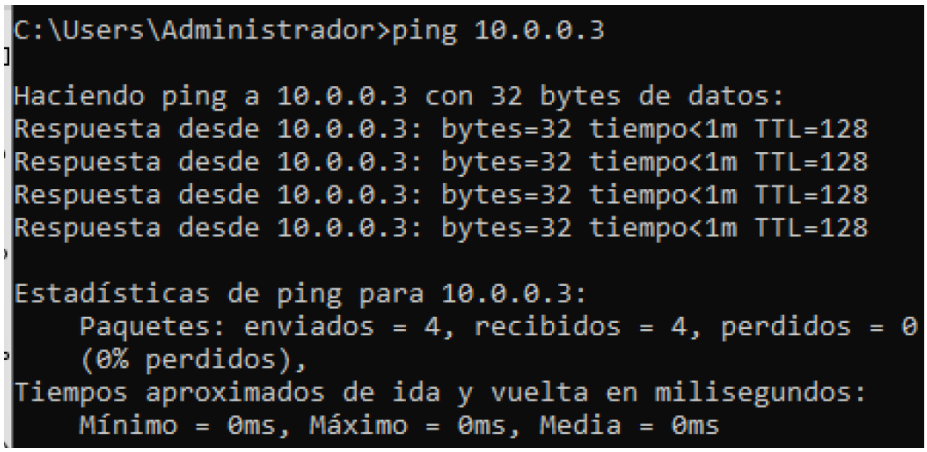


Ilustración 26. Prueba de conectividad entre el servidor y su propia IP estática.

Fuente: Elaboración propia

3. ping [IP del host físico]: Valida la conectividad entre el servidor virtual y la máquina anfitriona.

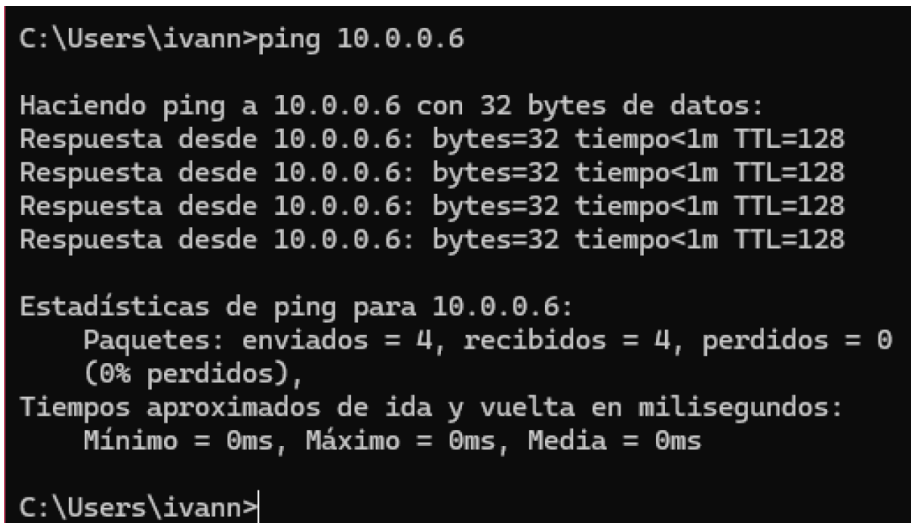


Ilustración 27. Validación de conexión con el equipo cliente desde el servidor.

Fuente: Elaboración propia

Cuando el ping devuelve respuestas exitosas, significa que la comunicación está activa. Si devuelve errores como "tiempo de espera agotado", puede deberse a configuraciones incorrectas, firewalls activos o fallos físicos en la red.

Diagnóstico y recomendaciones

En caso de fallos en la conexión, se recomienda lo siguiente:

- Verificar el estado del adaptador de red.
- Utilizar el asistente de diagnóstico de Windows.
- Confirmar que el firewall no esté bloqueando el tráfico ICMP (usado por el comando ping).
- Revisar que no haya direcciones IP duplicadas en la red.

Asimismo, se deben aplicar buenas prácticas como:

- Asignar direcciones IP estáticas para roles de servidor.
- Usar rangos privados definidos (como 10.0.0.0/8).
- Segmentar la red según las funciones y servicios.
- Documentar toda configuración aplicada para auditoría y replicación.

Windows Server Core

Server Core es una opción de instalación minimalista para Windows Server, que solo incluye los componentes y servicios esenciales para ejecutar roles y características específicos del servidor. Carece de una interfaz gráfica de usuario (GUI) y se administra exclusivamente a través de la línea de comandos, PowerShell o herramientas remotas. Esta opción fue introducida en Windows Server 2008 y ha sido mejorada en versiones posteriores (Hall, Alif C.B, & Selenguende Dzongo, 2016). Durante la instalación de Windows Server, es posible seleccionar únicamente los roles de servidor necesarios, lo cual contribuye a reducir la carga general del sistema operativo. En contraste, la opción de instalación con Experiencia de Escritorio incluye una amplia gama de servicios y componentes adicionales que, en muchos casos, no son indispensables para tareas específicas.

En este contexto, Server Core representa una alternativa optimizada, ya que excluye elementos gráficos y servicios no esenciales, permitiendo un entorno más liviano y seguro para determinados roles de servidor. Por ejemplo, un servidor dedicado a Hyper-V no requiere interfaz gráfica de usuario (GUI), puesto que la mayoría de las tareas pueden llevarse a cabo a través de Windows PowerShell o mediante herramientas de administración remota como el Administrador de Hyper-V (Microsoft, 2025c).

Diferencias clave entre Server Core y Server con Experiencia de Escritorio

Tabla 4. Diferencias entre Server Core y Experiencia de Escritorio.

Componente	Server Core	Servidor con Experiencia de Escritorio
Interfaz de usuario	Mínima, controlada por línea de comandos (PowerShell, SConfig, cmd)	Interfaz gráfica de usuario estándar de Windows
Espacio en disco	El requisito más pequeño	El requisito más grande
Instalación, configuración y desinstalación de roles de servidor localmente	PowerShell	Administrador del servidor o PowerShell
Roles y características	Algunos roles y características no están disponibles. Consulta Roles, servicios de rol y características que no están en Windows Server o	Todos los roles y características están disponibles, incluyendo los de compatibilidad con aplicaciones.

	Server Core. Algunas características de compatibilidad de aplicaciones del Servidor con Experiencia de Escritorio pueden instalarse con la Característica de compatibilidad de aplicaciones a petición (FOD).	
Administración remota	Puede gestionar remotamente usando herramientas de GUI como Windows Admin Center, Herramientas de administración remota del servidor (RSAT), Administrador del servidor o PowerShell.	Se puede gestionar remotamente usando herramientas de GUI como Windows Admin Center, Herramientas de administración remota del servidor (RSAT), Administrador del servidor o PowerShell.

Posible superficie de ataque	Superficie de ataque muy reducida	Sin reducción
Microsoft Management Console	No instalado; se puede agregar con la Característica de compatibilidad de aplicaciones a petición (FOD).	Instalado

Fuente: Microsoft. (2025)

Ventajas de Server Core

Server Core presenta ventajas clave frente a la versión con entorno gráfico, como una menor exposición a vulnerabilidades y menor consumo de recursos del sistema como espacio en disco, memoria y CPU. Al requerir menos actualizaciones y componentes, reduce el mantenimiento, los posibles fallos y el tiempo de inactividad, lo que contribuye a una mayor eficiencia, estabilidad y disponibilidad del servidor. (Hall, Alif C.B, & Selenguende Dzongo, 2016).

Inconvenientes de Server Core

Server Core tiene algunas limitaciones frente a Server con entorno gráfico, como menor compatibilidad con ciertas funciones, herramientas o controladores, y la ausencia de una interfaz visual. Esto implica que su gestión requiere conocimientos más avanzados, ya que se basa en comandos, PowerShell o

herramientas remotas, lo que puede dificultar su uso para algunos administradores (Hall, Alif C.B, & Selenguende Dzongo, 2016).

Administración de un servidor Server Core

Debido a que Server Core no tiene una interfaz gráfica, es necesario utilizar cmdlets de Windows PowerShell, herramientas de línea de comandos o herramientas remotas para su administración. Las secciones siguientes describen los cmdlets y comandos de PowerShell necesarios para realizar tareas básicas. También puedes usar Windows Admin Center, un portal de administración unificado que actualmente está en versión preliminar pública, para gestionar Server Core (Microsoft, 2025e).

Establecer una dirección IP estática

En Server Core, se asigna una dirección DHCP por defecto. Si se necesita configurar una dirección IP estática, se puede ejecutar los siguientes comandos en la Powershell:

Get-NetIPConfiguration para ver la configuración de red actual.

Get-NetIPAddress para ver las direcciones IP en uso.

Para establecer una dirección IP estática:

- Ejecutar Get-NetIPInterface.
- Anotar el número de la columna IfIndex o la cadena InterfaceDescription de la interfaz IP correspondiente.
- Para configurar una dirección IP estática, ejecuta el siguiente

```
New-NetIPAddress -InterfaceIndex 12 -IPAddress 192.0.2.2 -PrefixLength 24 -DefaultGateway 192.0.2.1
```

cmdlet en PowerShell:

- Para establecer la dirección del servidor DNS del cliente, utilizar el siguiente cmdlet:
- Para agregar varios servidores DNS, usar este cmdlet:

```
Set-DNSClientServerAddress -InterfaceIndex 12 -ServerAddresses 192.0.2.4
```

Tareas administrativas desde la línea de comandos

Tabla 5. Tareas administrativas desde la línea de comandos.

Tarea	Comando
Obtener ayuda	Get-Help
Establecer la contraseña del administrador local	net user administrator *
Unir un equipo a un dominio	netdom join %computername% /domain:<dominio> /userd:<dominio\usuario> /passwordd:* Reinicia el equipo y confirma el cambio de dominio usando set
Quitar un equipo de un dominio	netdom remove <nombre del equipo>

Agregar un usuario al grupo de Administradores local	net localgroup Administrators /add <dominio\usuario>
Quitar un usuario del grupo de Administradores local	net localgroup Administrators /delete <dominio\usuario>
Agregar un usuario al equipo local	net user <dominio\usuario> * /add
Cambiar el nombre de un equipo unido a un dominio	netdom renamecomputer %computername% /NewName:<nuevo nombre del equipo> /userd:<dominio\usuario> /passwordd:* Confirma el nuevo nombre del equipo con set
Cambiar el nombre de un equipo en un grupo de trabajo	netdom renamecomputer currentcomputername /NewName:<nuevo nombre del equipo> Reinicia el equipo para aplicar los cambios
Cambiar a una dirección IP estática	netsh interface IPv4 set address <nombre o identificador de la interfaz> source=static address=<dirección IP

	preferida> gateway=<dirección de puerta de enlace> Ejecuta IPconfig /all para confirmar que DHCP está deshabilitado
Establecer una dirección DNS estática	netsh interface IPv4 add DNSserver name=<nombre o identificador de la tarjeta de red> address=<dirección IP del servidor DNS principal> index=1 netsh interface IPv4 add DNSserver name=<nombre del servidor DNS secundario> address=<dirección IP del servidor DNS secundario> index=2 Ejecuta IPconfig /all para confirmar las direcciones
Cambiar una dirección IP estática por una dirección IP proporcionada por DHCP	netsh interface IPv4 set address name=<dirección IP del sistema local> source=DHCP Ejecuta IPconfig /all para confirmar que DHCP está habilitado
Especificar una clave de producto	slmgr.vbs –IPk <clave de producto>
Activar el servidor remotamente	cscrIPt slmgr.vbs –IPk <clave del producto> <nombre del servidor> <nombre de usuario> <contraseña>

cscrIPt slmgr.vbs -ato <nombre del servidor> <nombre de usuario> <contraseña>

Fuente: Microsoft (2025e).

Requisitos de instalación

Tabla 6: Requisitos de instalación

Componente	Mínimo
Procesador	Procesador de 64 bits a 1,4 GHz
RAM	512 MB
Disco	32 GB
Adaptador de red	Adaptador Ethernet
Otros	Unidad de DVD

Fuente: Microsoft (2024).

Topología de Red e Instalación de Windows Server Core

Antes de proceder con la instalación vamos a ver cuál es la topología de red que vamos a utilizar para realizar esta simulación

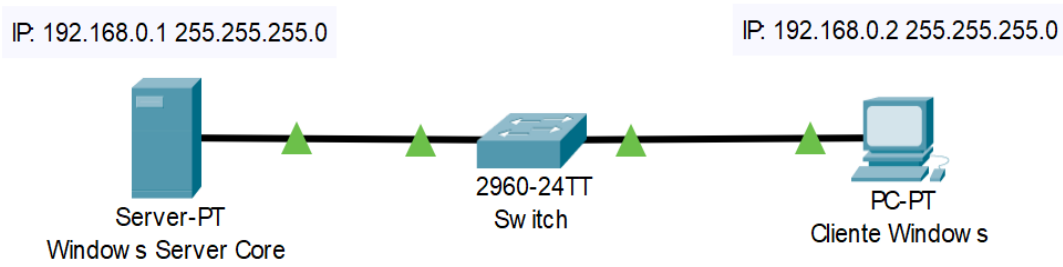


Ilustración 28. Topología de la Red

Fuente: Elaboración propia

Una vez que ya conocemos nuestra topología procedemos a crear una máquina virtual nueva y le asignamos un nombre

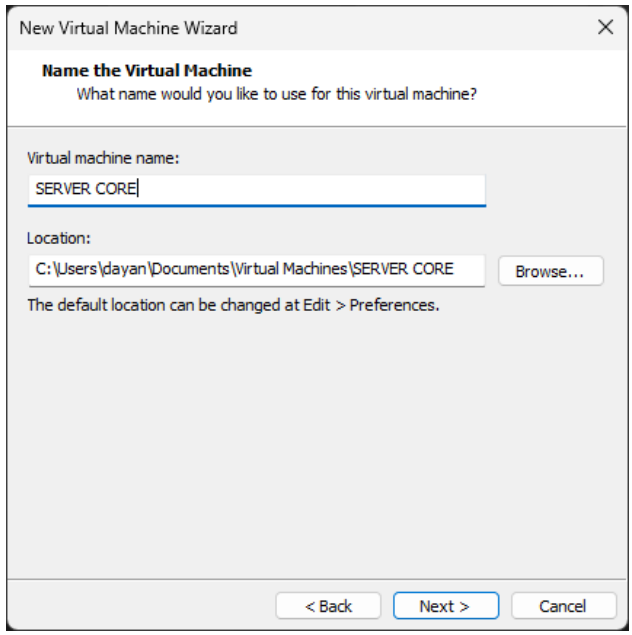


Ilustración 29. Creación de la máquina virtual

Fuente: Elaboración propia

En este caso vamos a poner requisitos básicos como 4GB de Ram, 1 para el procesador y 40Gb de almacenamiento

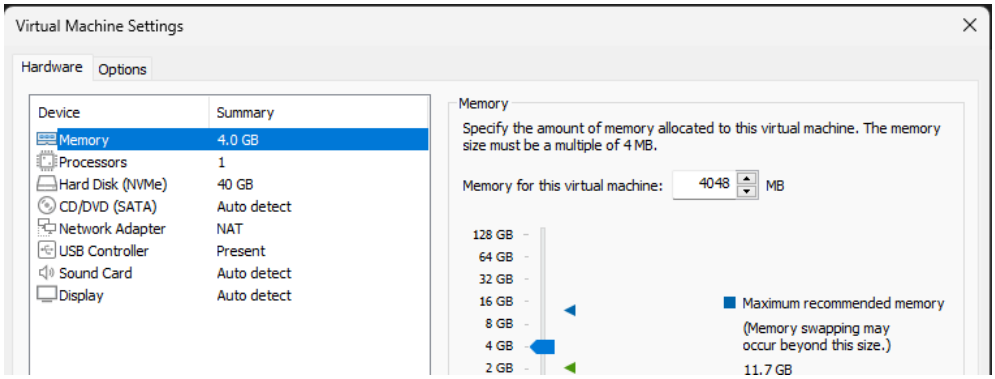


Ilustración 30. Asignación de memoria

Fuente: Elaboración propia

Ahora en la parte del CD buscamos la ISO de Windows Server 2022.

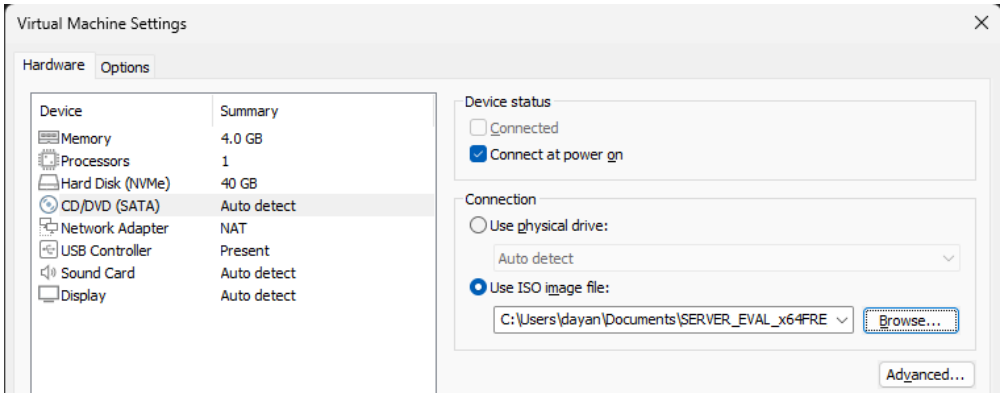


Ilustración 31. Ruta de la imagen ISO

Fuente: Elaboración propia

Ahora vamos a empezar con la instalación de Windows, esto lo podemos cambiar como deseamos o dejarlo por defecto

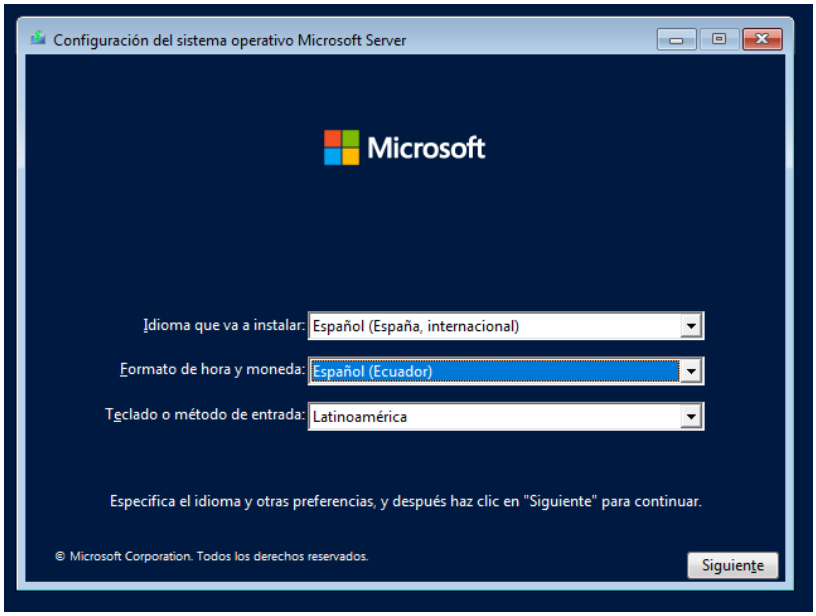


Ilustración 32. Instalación dentro de la máquina virtual

Fuente: Elaboración propia

Aquí seleccionamos la tercera opción, Windows Server Datacenter Evaluation, que es la opción de Windows Server Core

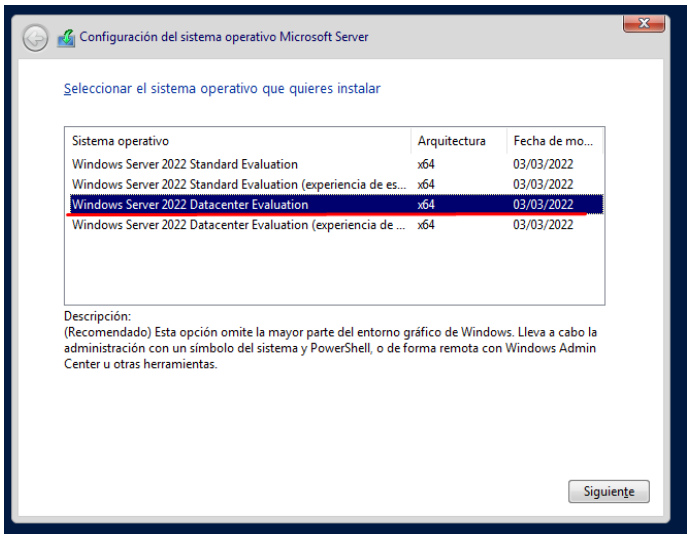


Ilustración 33. Instalación de Windows Server Core

Fuente: Elaboración propia

Ahora aceptamos la licencia

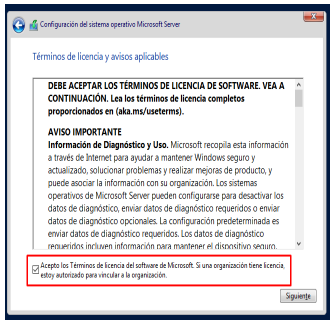


Ilustración 34. Aceptación de términos y condiciones

Aquí seleccionamos la opción personalizar

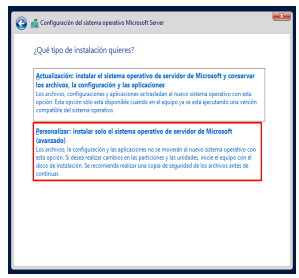


Ilustración 35. Verificación de particiones

Luego, nos aparece una ventana en la que se selecciona el disco duro, en caso de ser necesario se particiona

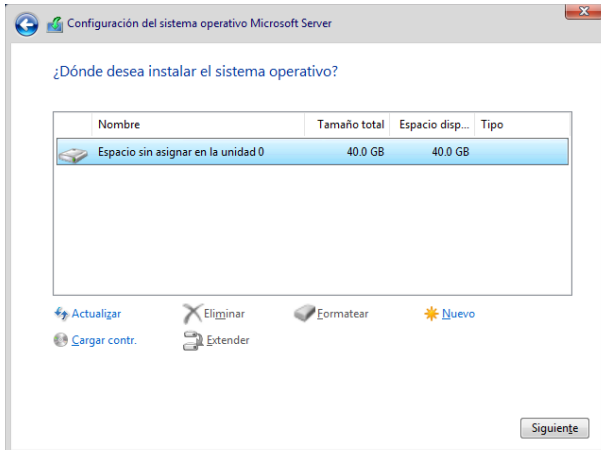


Ilustración 36. Establecer solo una partición

Fuente: Elaboración propia

Finalmente se espera hasta que se concluya en proceso de instalación y se inicie Windows Server Core

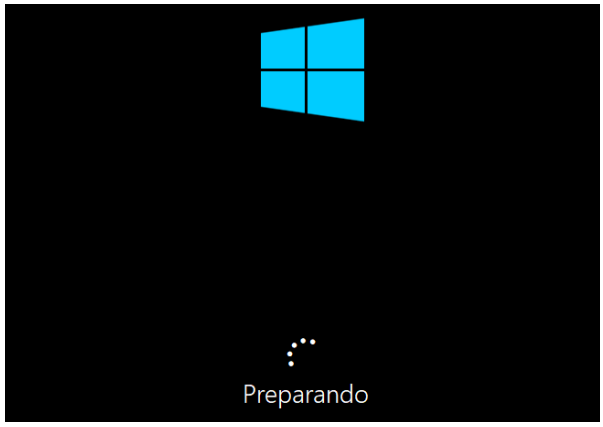


Ilustración 37. Carga de WS Core

Fuente: Elaboración propia

Al momento de ingresar al sistema operativo, se nos pedirá que asignemos una contraseña para el administrador

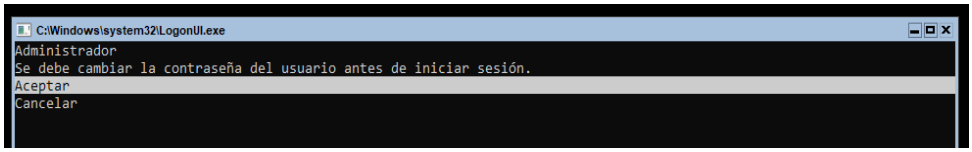


Ilustración 38. Windows Server Core

Fuente: Elaboración propia

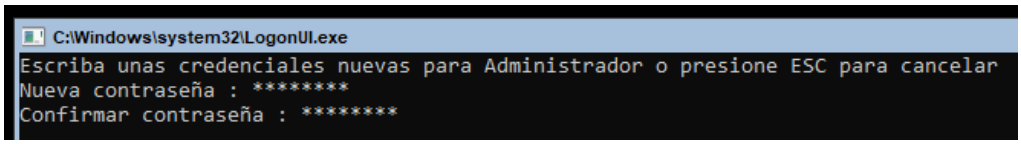


Ilustración 39. Asignación de una contraseña de administrador

Fuente: Elaboración propia

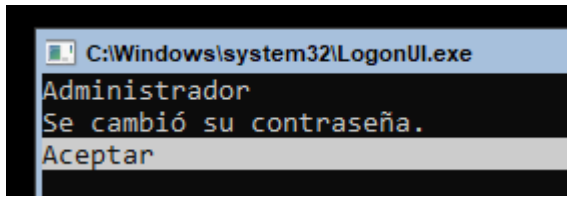


Ilustración 40. Verificación de contraseña creada correctamente

Fuente: Elaboración propia

Aquí podemos acceder a la interfaz principal

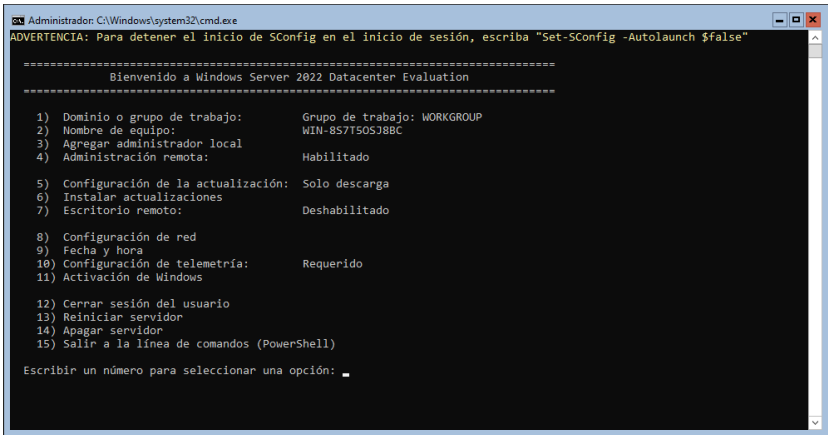


Ilustración 41. Interfaz principal de Server Core

Fuente: Elaboración propia

Configuración de Windows Server Core

Creación de usuarios

Para crear un usuario es necesario usar el comando **New-LocalUser**, este permite crear un usuario en el sistema con los siguientes parámetros: **-Name "NombreUsuario"** para el nombre de inicio de sesión, **-Password (ConvertTo-SecureString "ColocarContraseña" -AsPlainText -Force)** para establecer una contraseña segura, **-FullName "Usercompleto"** para el nombre completo del usuario, y **-Description "AgregarDescripcion"** para una descripción opcional del usuario.

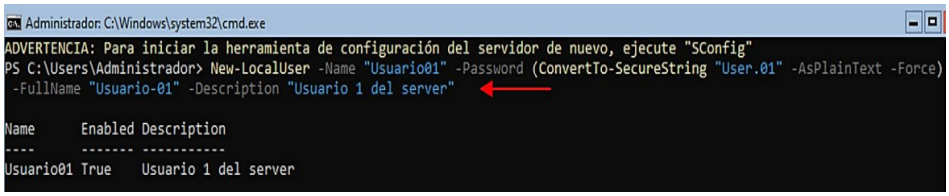


Ilustración 42. Creación de un usuario

Fuente: Elaboración propia

Grupo de usuarios

El comando para crear un nuevo grupo local en el sistema utiliza los siguientes parámetros: **-Name "NombreGrupo"** para especificar el nombre del grupo y **-Description "DescripcionGrupo"** para proporcionar una descripción opcional que detalle el propósito o función del grupo.

Ahora para asignar un usuario al grupo utiliza los siguientes parámetros: **-Group "NombreGrupo"** para especificar el nombre del grupo y **-Member "NombreUsuario"** para indicar el nombre del usuario que se agregará como miembro del grupo.

Ilustración 43. Creación de un grupo e ingreso de un usuario

Fuente: Elaboración propia

Eliminación de usuarios de un grupo

```
Remove-LocalGroupMember -Group "NombreGrupo". -Member "NombreUsuario"
```

Para eliminar un miembro en específico del grupo se usa el comando:

```
PS C:\Users\Administrador> Remove-LocalGroupMember -Group "Grupo01" -Member "Usuario02"
PS C:\Users\Administrador> Get-LocalGroupMember Grupo01

ObjectClass Name                PrincipalSource
----------- ----                ---------------
Usuario     WINSER-01\Usuario01 Local
```

Ilustración 44. Eliminación de un usuario de un grupo

Fuente: Elaboración propia

Cambio de nombre del equipo

Para cambiar el nombre, debemos poner en el cuadro que aparece abajo la opción 2.

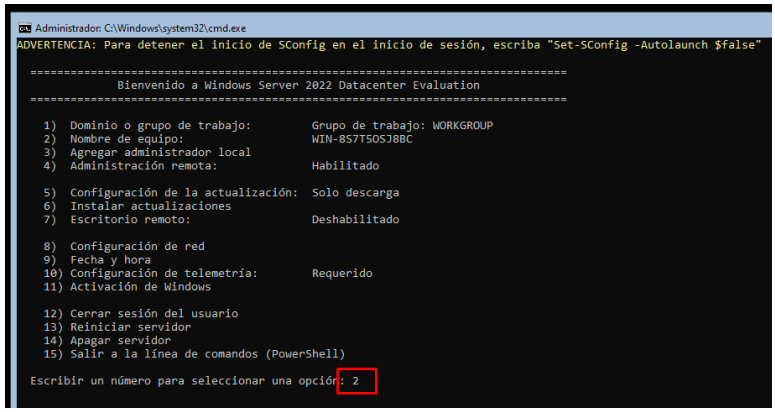


Ilustración 45. Cambio del nombre del equipo

Fuente: Elaboración propia

Esto conduce a otra ventana en donde indique que nombre le queremos aplicar a nuestro servidor, una vez que pongamos el nombre que deseamos tenemos que reiniciar:

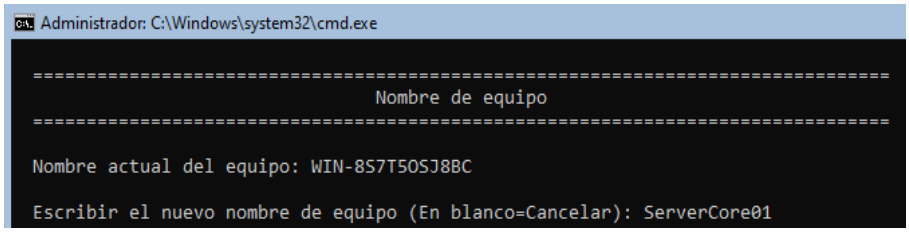


Ilustración 46. Asignación de un nombre

Fuente: Elaboración propia

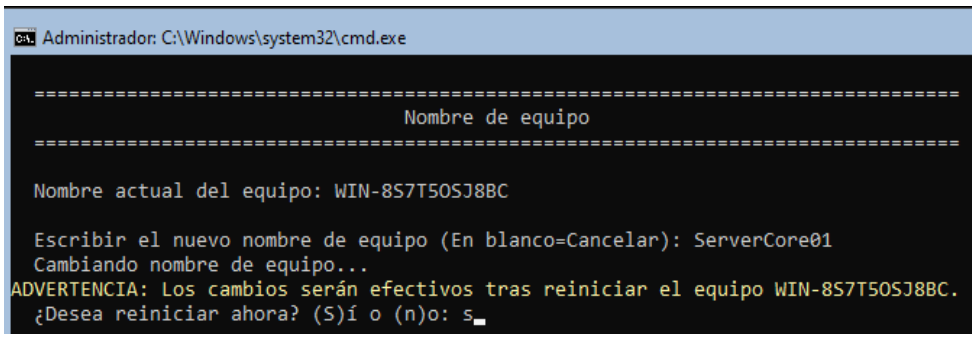


Ilustración 47. Reinicio de WS Core

Fuente: Elaboración propia

Aquí podemos visualizar en la interfaz principal como el nombre que otros asignamos dentro de la configuración ya está puesto.

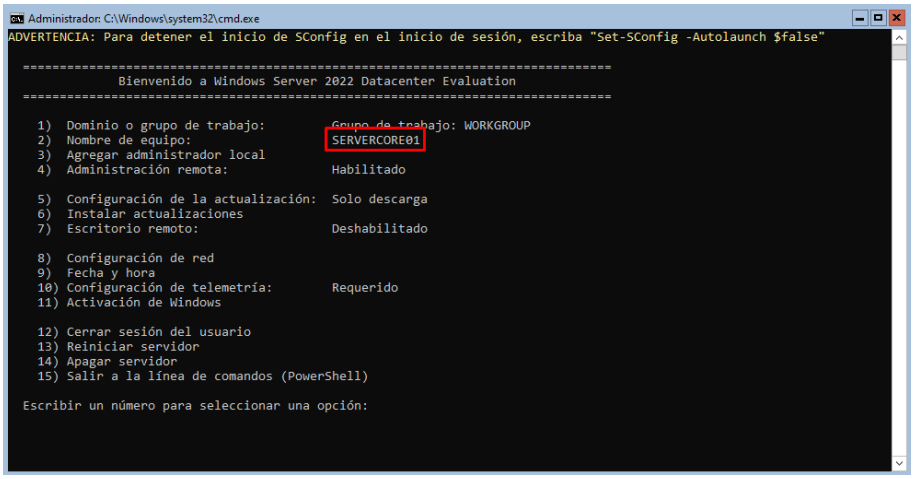


Ilustración 48. Verificación del cambio de nombre

Fuente: Elaboración propia

Asignación de direcciones IP

Para asignar una dirección IP, tenemos que colocar la opción 8

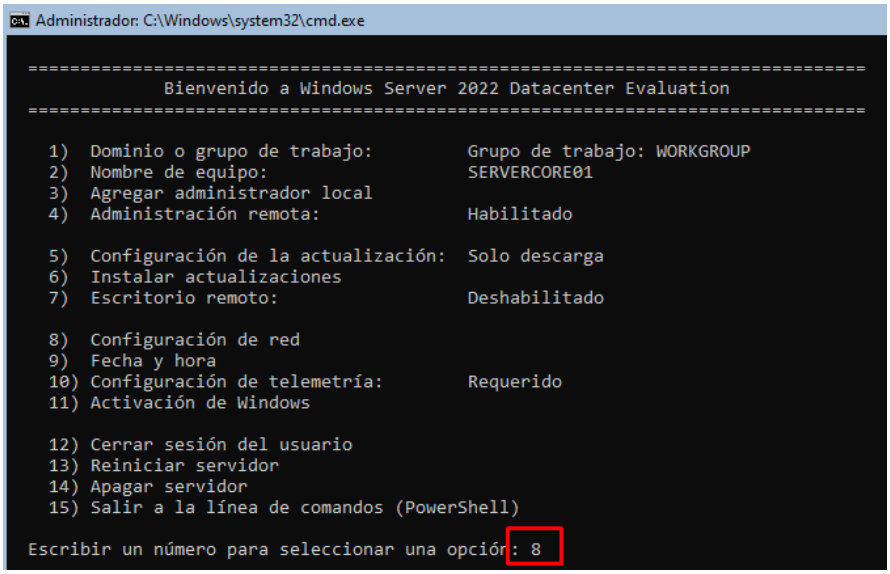


Ilustración 49. Configuración IP en el servidor

Fuente: Elaboración propia

Una vez que colocamos esa opción, seleccionaremos uno de los adaptadores disponibles

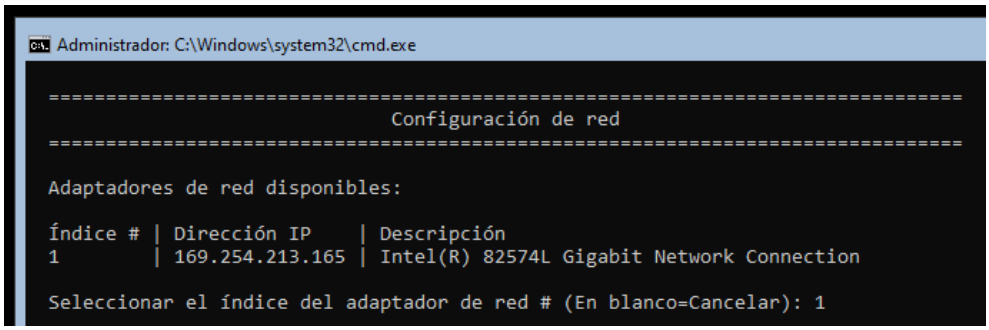


Ilustración 50. Selección del adaptador de red

Fuente: Elaboración propia

Ahora, seleccionamos la opción 1 para asignar una dirección IP.

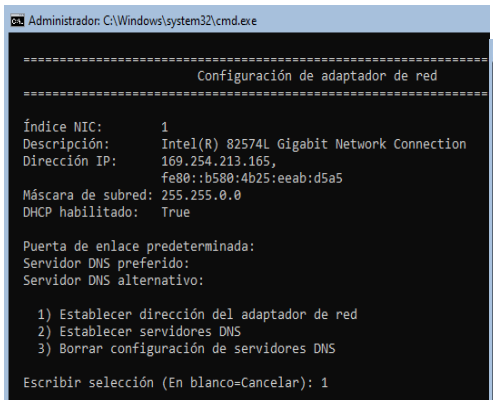


Ilustración 51. Opción 1 para establecer una IP

Fuente: Elaboración propia

Después, presionamos letra S, que significa que realizaremos una asignación estática.

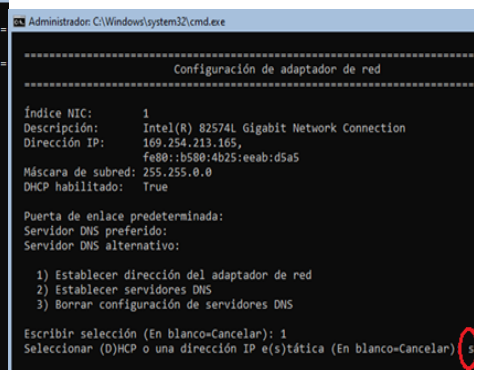


Ilustración 52. Selección de una IP estática

Fuente: Elaboración propia

En este ejemplo, asignamos la IP 192.168.0.1 con mascara de 255.255.255.0

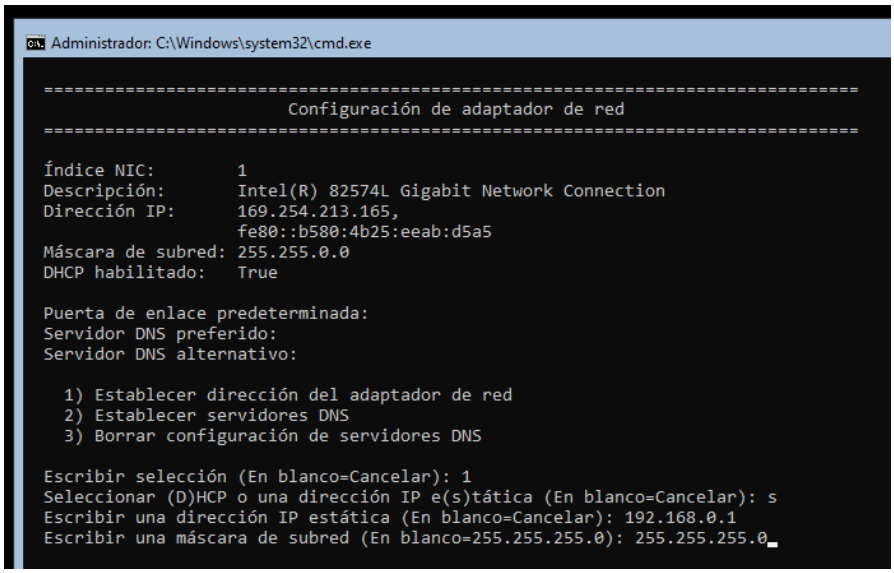


Ilustración 53. Asignación de la IP y mascara de subred

Fuente: Elaboración propia

Una vez asignada la configuración TCP/IP, podremos verficarla

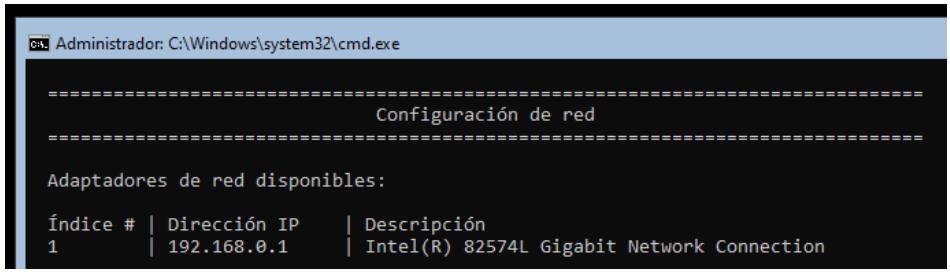


Ilustración 54. Verificación del cambio de IP del adaptador

Fuente: Elaboración propia

Para comprobar el funcionamiento de la configuración TCP/IP, realizamos la asignación en el cliente, en este caso la IP 192.168.0.2

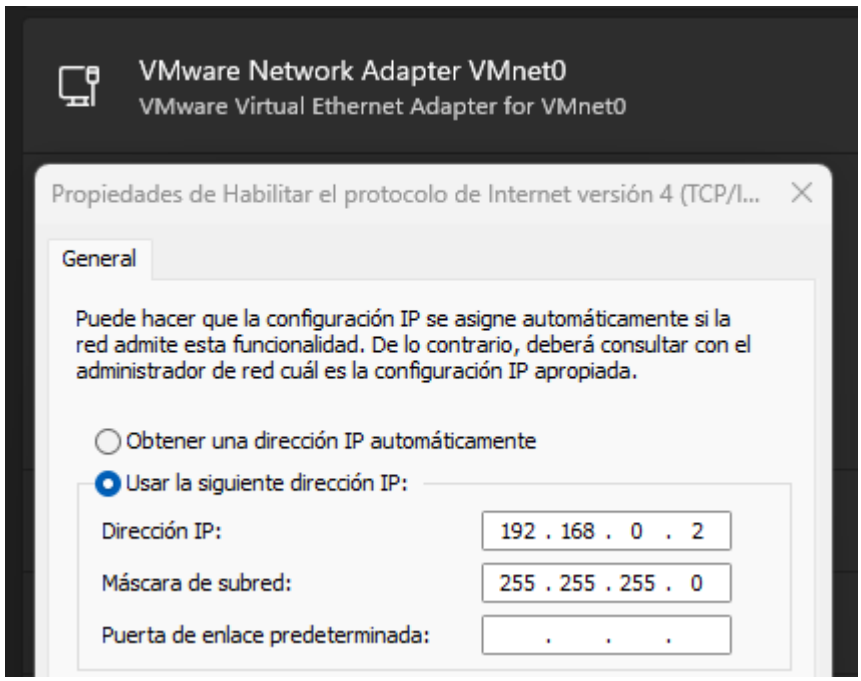


Ilustración 55. Configuración IP en cliente

Fuente: Elaboración propia

En nuestro caso, el cliente es una máquina con Windows. Luego de aplicar los cambios en la configuración TCP/IP, realizamos un diagnóstico accediendo al símbolo del sistema (Command Prompt) y utilizando el comando *ping* para verificar la existencia de comunicación entre el cliente y la máquina servidor (Windows Server Core). Podemos observar en la siguiente Ilustración que si existe dicha comunicación.

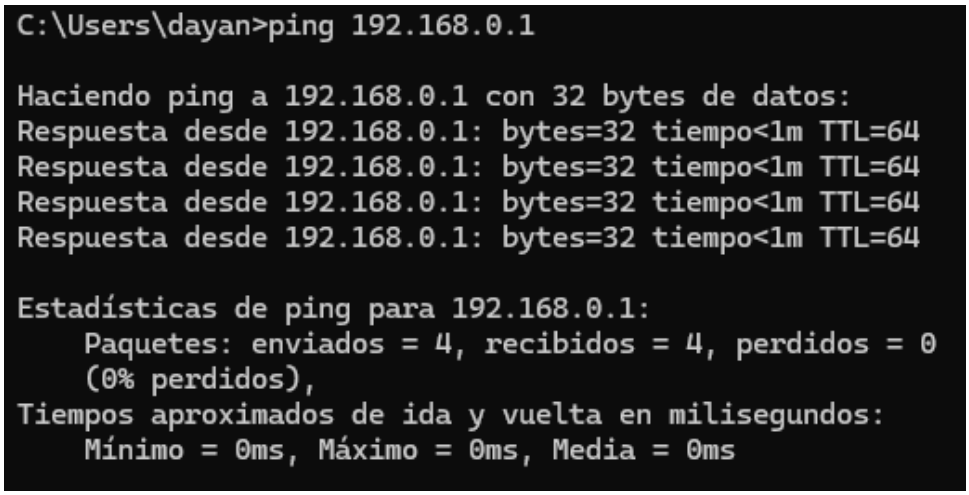


Ilustración 56. Verificación de ping de cliente a servidor

Fuente: Elaboración propia

Para comprobar que también se puede hacer ping al cliente, desde el servidor, accedemos a la opción 15, que significa Salir a la línea de comandos (PowerShell).

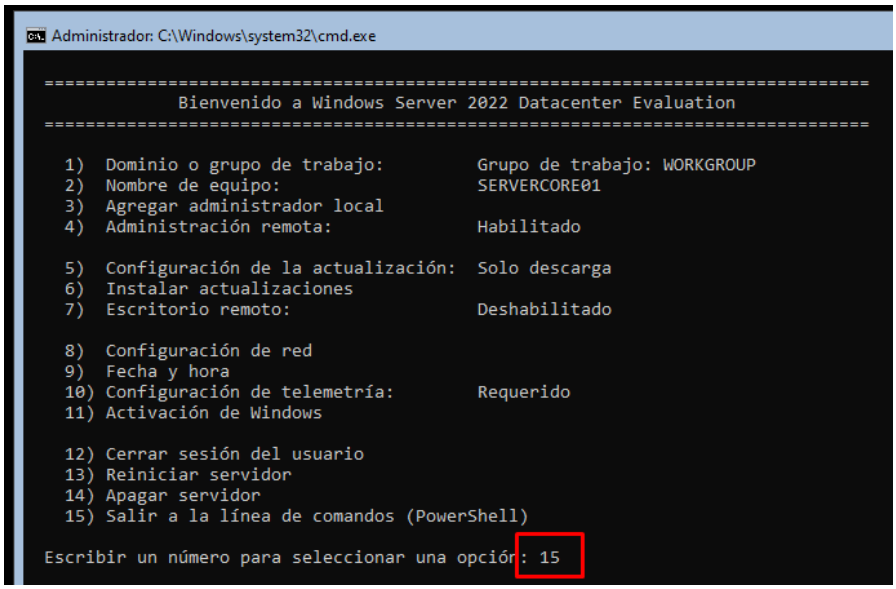


Ilustración 57. Línea de comandos de Server Core

Fuente: Elaboración propia

Una vez en la consola de PowerShell, se ejecuta el comando ping dirigido a la dirección IP del cliente. La respuesta obtenida indica que la conectividad de red es satisfactoria, evidenciando que el cliente está accesible desde el host.

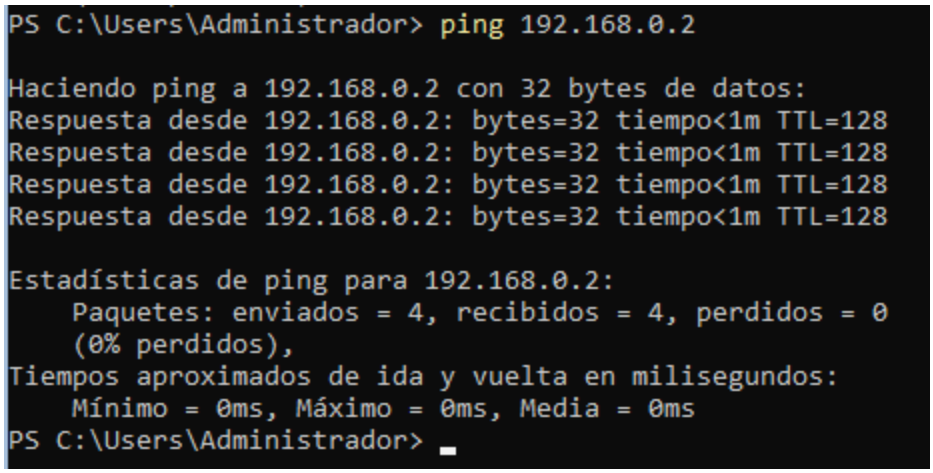


Ilustración 58. Verificación de ping de servidor a cliente

Fuente: Elaboración propia

En caso de que no exista comunicación, puede ser debido a la configuración del firewall. Para diagnosticar, podremos deshabilitar el firewall desde la PowerShell del servidor con el siguiente comando:

```
netsh advfirewall set allprofiles state off
```

Para verificar que está deshabilitado usamos el mismo comando solo cambiando el set por show y quitando el off, quedando de la siguiente manera:

```
netsh advfirewall show allprofiles state
```

Cambio de Fecha/Hora

Para cambiar la fecha y hora del equipo, tenemos que ingresar a la opción 9.

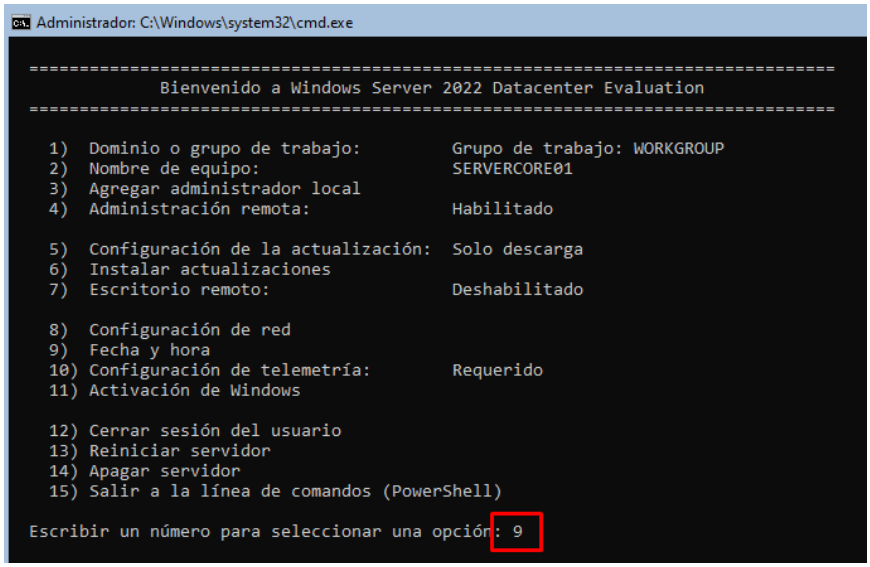


Ilustración 59. Configuración de Hora y Fecha

Fuente: Elaboración propia

A continuación, se muestra la ventana de configuración de Fecha y hora del sistema operativo Windows. Esta interfaz permite al usuario visualizar y modificar parámetros relacionados con la hora del sistema

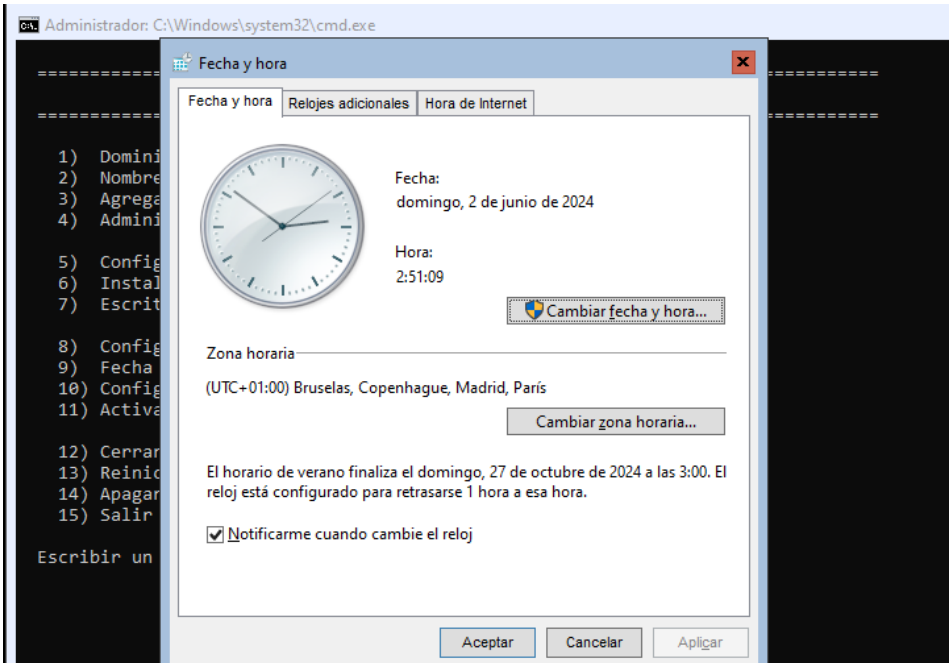


Ilustración 60. Interfaz de Fecha y Hora en WS Core

Fuente: Elaboración propia

Configuración del servicio de DHCP

A continuación, se plantea una topología en la que se muestra que el servidor va a tener asignada de forma estática una IP: 192.168.10.2/24, el servidor de DHCP va a tener un rango de direcciones asignables desde: 192.168.10.10 hasta 192.168.10.20 y un rango de direcciones excluidas de: desde 192.168.10.10 hasta 192.168.10.15. Esto implica que solo estarán disponibles para asignación dinámica las direcciones 192.168.10.16 a 192.168.10.20.

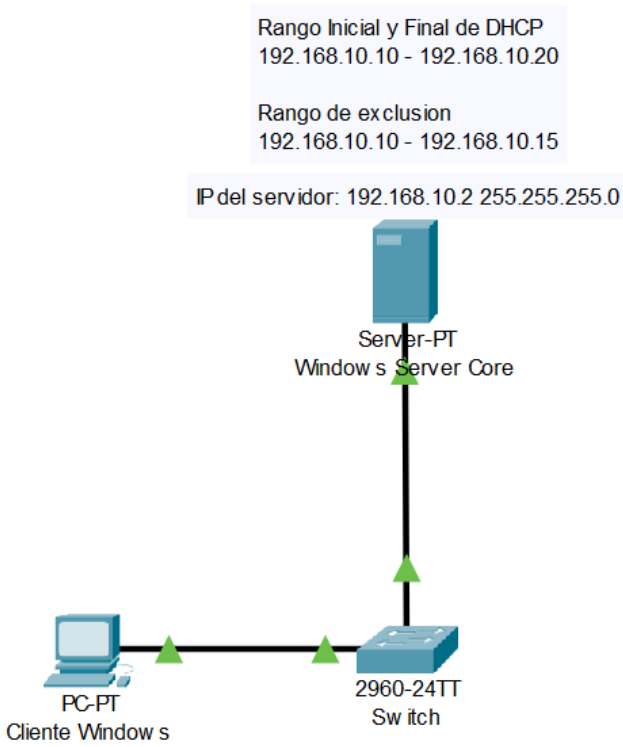


Ilustración 61. Topología de red para el servicio DHCP

Fuente: Elaboración propia

Para realizar esta configuración tenemos que instalar el DHCP que esto solo se puede hacer desde la línea de comandos, a continuación, el comando para que se realice la instalación es la siguiente:

```
Install-WindowsFeature -Name DHCP -
IncludeManagementTools
```

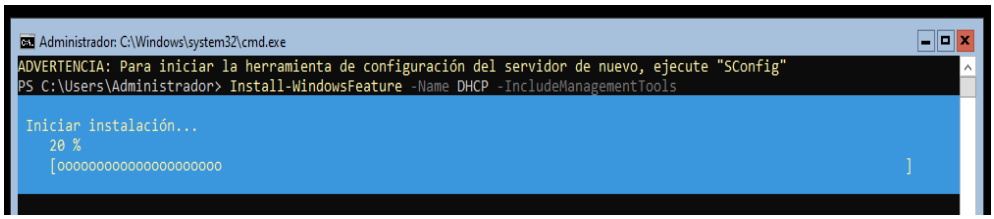


Ilustración 62. Instalación de DHCP

Fuente: Elaboración propia

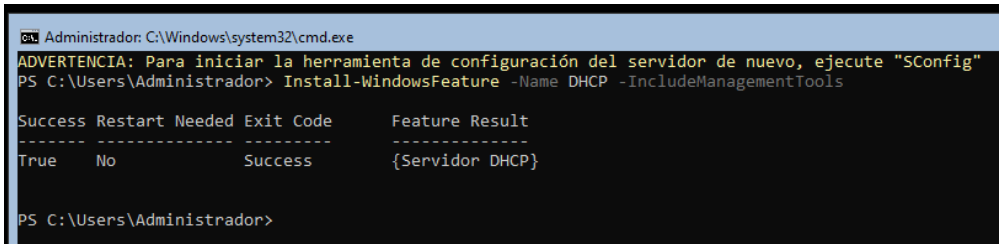


Ilustración 63. Instalación correcta del DHCP

Fuente: Elaboración propia

Una vez que hemos instalado procedemos a realizar una configuración de un nuevo ámbito, en donde tenemos que establecer el rango de inicio y el rango final, con el siguiente comando se puede realizar esta configuración:

```
Add-DhcpServerv4Scope -Name "NombreRed" - StartRange
"RangoIPInicial" -EndRange "RangoIPFinal -SubnetMask
"MascaraSubRed" -LeaseDuration "DuracionConcesionesIP"
```

```
Add-DhcpServerv4Scope -Name "ServerCore" -StartRange 192.168.10.10 -EndRange 192.168.10.20 -Subnet
Mask 255.255.255.0 -LeaseDuration 1.00:00:00
```

Ilustración 64. Configuración DHCP

Fuente: Elaboración propia

Una vez que hemos creado ese ámbito utilizamos el comando **Set -DhcpServerv4OptionValue** para establecer valores de opciones específicas para un ámbito (scope) en un servidor DHCP

```
Set-DhcpServerv4OptionValue -ScopeId 192.168.10.0 -OptionId 3 -Value 192.168.10.1
Set-DhcpServerv4Scope -ScopeId 192.168.10.0 -State Active
```

Ilustración 65. Configuración DHCP – 2

Fuente: Elaboración propia

Para ver los ámbitos que tenemos creados, utilizamos el siguiente comando:

```
PS C:\Users\Administrador> Get-DhcpServerv4Scope

ScopeId         SubnetMask      Name          State    StartRange      EndRange        LeaseDuration
-------         ----------      ----          -----    ----------      --------        -------------
192.168.10.0    255.255.255.0   ServerCore    Active   192.168.10.10   192.168.10.20   1.00:00:00


PS C:\Users\Administrador> Get-Service Dhcp

Status   Name               DisplayName
------   ----               -----------
Running  Dhcp               Cliente DHCP
```

Ilustración 66. Verificación de la configuración del DHCP

Fuente: Elaboración propia

Ahora vamos al cliente y al adaptador veremos que se asignó una dirección IP de forma automática

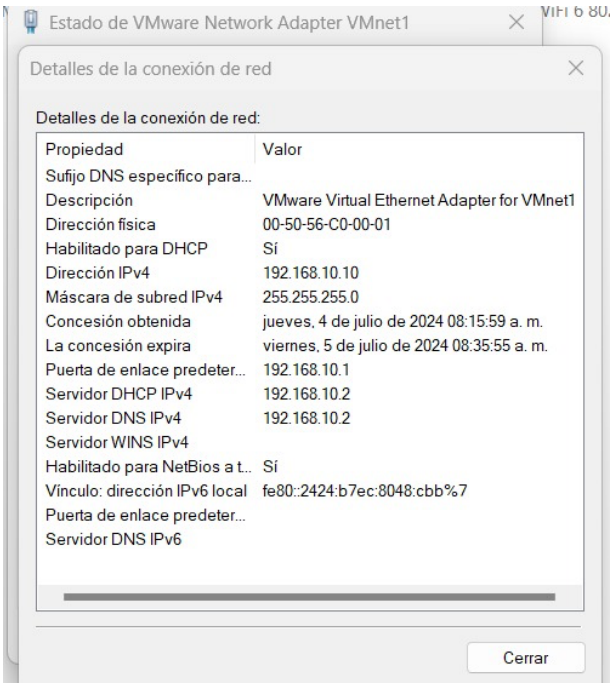


Ilustración 67. Verificación de configuración DHCP en cliente

Fuente: Elaboración propia

DHCP exclusión de rango

Para realizar la exclusión de rango usamos el comando **Add-DhcpServerv4ExclusionRange** agrega un rango de exclusión de direcciones IP en un ámbito DHCP específico, evitando que el servidor DHCP asigne esas IP a dispositivos clientes. Utiliza **-ScopeId 192.168.10.0** para especificar el ámbito, **-StartRange 192.168.10.10** para la dirección IP de inicio del rango de exclusión,

y **-EndRange 192.168.10.15** para la dirección IP de fin del rango de exclusión.

```
Add-DhcpServerv4ExclusionRange -ScopeId 192.168.10.0 -StartRange 192.168.10.10
-EndRange 192.168.10.15
```

Ilustración 68. Configuración DHCP con exclusión de rango

Fuente: Elaboración propia

Ahora verificamos si se realizó la respectiva configuración usando el siguiente comando

```
PS C:\Users\Administrador> Get-DhcpServerv4ExclusionRange

ScopeId            StartRange          EndRange
-------            ----------          --------
192.168.10.0       192.168.10.10       192.168.10.15
```

Ilustración 69. Visualización de la configuración de exclusión de rango

Fuente: Elaboración propia

Activamos para que funcione la configuración que realizamos para poder excluir las direcciones IP

```
Set-DhcpServerv4Scope -ScopeId 192.168.10.0 -State Active
```

Ilustración 70. Activación de la configuración DHCP de exclusión de rango

Fuente: Elaboración propia

Vamos al adaptador de red, lo deshabilitamos y lo volvemos habilitar para que se ponga la nueva dirección IP

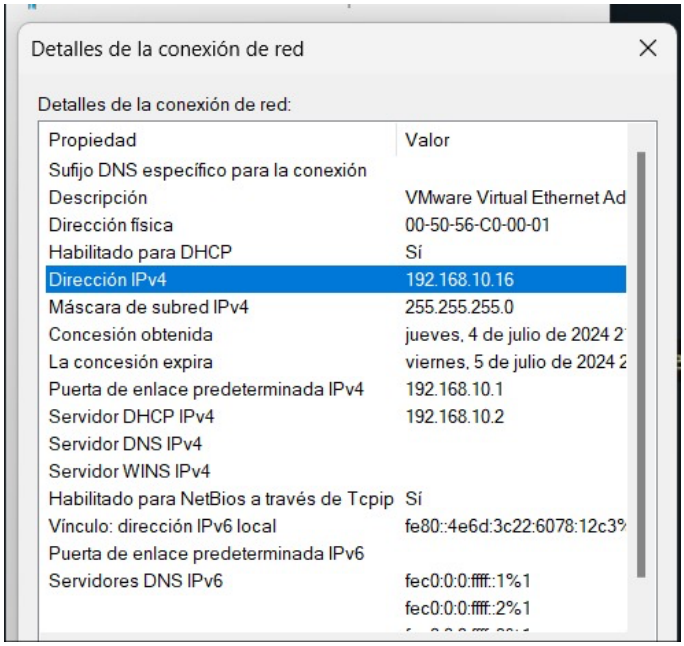


Ilustración 71. Verificación de configuración de DHCP de exclusión de rango en el cliente

Fuente: Elaboración propia

Resumen del Capítulo I

El capítulo I de este libro, ofrece una visión integral de Windows Server 2022, el sistema operativo de la Microsoft orientado para entornos de servidores, aquí se realiza una introducción al mismo, se destaca sus ediciones como la: estándar, datacenter y datacenter azure; así como sus opciones de instalación, con experiencia de escritorio y core. Se analizan las características más relevantes del sistema operativo, así como las mejoras del mismo en seguridad, rendimiento, administración y la inclusión del navegador Microsoft Edge. Además, se detallan los requisitos mínimos y el proceso completo para instalar Windows Server 2022 Datacenter con Experiencia de Escritorio y core en un entorno virtualizado usando VirtualBox.

El capítulo también incluye la administración de cuentas de usuario y grupos locales, incluyendo la administración de cuentas, así como la asignación de permisos mediante directivas de seguridad local. Se destacan las cuentas predeterminadas del sistema y se ofrecen recomendaciones para el manejo seguro de contraseñas. Se presenta la configuración de red, desde la asignación de direcciones IP estáticas hasta pruebas de conectividad mediante comandos como ping e ipconfig, para verificar la comunicación efectiva entre el servidor y los clientes. En cuanto a Windows Server Core, la versión optimizada del sistema operativo sin interfaz gráfica, ideal para entornos que requieren mayor seguridad y eficiencia. Se comparan sus ventajas e inconvenientes frente a la versión con Experiencia de Escritorio, y se detallan comandos esenciales para su administración desde la línea de comandos y PowerShell. Finalmente, se explica la configuración del servicio DHCP, incluyendo la creación de ámbitos, exclusión de rangos de IP y verificación de asignaciones dinámicas, todo dentro de una topología de red simulada que refuerza el aprendizaje práctico.

Este capítulo combina teoría y práctica, brindando al lector una base para instalar y administrar Windows Server 2022 en distintos entornos.

Preguntas de Revisión

Evaluación de Conocimientos Adquiridos

- Entendimiento de Conceptos Básicos:
    - Defina con claridad qué es Windows Server 2022 y explique en qué se diferencia de versiones anteriores del sistema operativo. Si no puede hacerlo con seguridad, investigue más sobre el tema y elabore un resumen comparativo.
    - Describa al menos tres ventajas de instalar Windows Server 2022 en modo Server Core frente a la instalación con experiencia de escritorio. Considere realizar una tabla que resuma sus características, ventajas y limitaciones.
- Habilidades Prácticas:
- Evalúe su capacidad para instalar Windows Server 2022 desde una imagen ISO en una máquina virtual. Si encontró dificultades, indique qué pasos le resultaron más complejos y qué aspectos necesita reforzar.
- Analice un caso práctico donde haya configurado servicios básicos como la IP estática o el nombre del equipo desde el entorno Server Core. Redacte un breve informe sobre su experiencia.
- Aplicación de Políticas de Seguridad:
- Explique cómo aplica buenas prácticas de seguridad iniciales tras la instalación del sistema operativo, como la gestión de

contraseñas, la creación de cuentas de usuario limitadas y la configuración de directivas locales.

- Discuta cómo verifica que la configuración de seguridad cumple con los requisitos de un entorno empresarial. Cree una lista de verificación con puntos clave como la desactivación de cuentas por defecto, asignación de derechos y control de acceso.

- Resolución de Problemas:

- Diagnostique y resuelva un problema común tras la instalación de Windows Server, como errores en la red, conflictos de configuración o imposibilidad de acceder a la consola de administración. Documente el proceso y reflexione sobre las lecciones aprendidas.

- Realice una tarea de mantenimiento, como la actualización del sistema operativo o la aplicación de parches de seguridad. Describa el procedimiento y evalúe su efectividad en términos de estabilidad y protección del sistema.

- Autoevaluación Personal

- Reflexión sobre el Aprendizaje:

- Identifique los aspectos de la instalación, administración o configuración inicial de Windows Server 2022 que le resultaron más desafiantes. Explique por qué y proponga formas efectivas de superar esas dificultades.

- Determine qué recursos adicionales (tutoriales, laboratorios virtuales, documentación oficial) necesita para mejorar su

comprensión de la administración básica del sistema operativo.

- Plan de Mejora Continua:

- Establezca los próximos pasos en su plan de aprendizaje para dominar Windows Server 2022. Esto puede incluir el desarrollo de entornos de prueba, la automatización de tareas administrativas o la práctica con Server Core.

- Investigue qué certificaciones o cursos están disponibles sobre administración de Windows Server (como Microsoft Certified: Windows Server Hybrid Administrator Associate). Elabore una lista de opciones e incluya metas concretas para alcanzarlas.

Referencias

Hall, W., Alif C.B, J., & Selenguende Dzongo, Y. (2016). ¿Cuáles son las ventajas y desventajas de usar Server Core frente a Server with Desktop Experience? *LinkedIn*. https://www.linkedin.com/advice/1/what-benefits-drawbacks-using-server

López Pérez, M. (2015). *Administración de directivas de grupo para la configuración segura de sistemas corporativos basados en Windows Server 2012* [Trabajo de fin de máster, Universitat Politècnica de València]. Repositorio institucional RiuNet. https://riunet.upv.es/handle/10251/55391

Microsoft. (2023a). ¿Qué es Server Core? *Microsoft Learn*. https://learn.microsoft.com/es-es/windows-server/administration/server-core/what-is-server-core

Microsoft. (2023b). Novedades en Windows Server 2022. *Microsoft Learn*. https://learn.microsoft.com/es-es/windows-server/get-started/whats-new-in-windows-server-2022

Microsoft. (2021a). Windows Server 2022 Comparison Guide. Microsoft Corporation. https://download.microsoft.com/download/4/4/5/445bb987-de1e-4ad7-a085-342da48c0179/Windows_Server_2022_Comparison_Guide.pdf

Microsoft. (2025a). Comparison of Windows Server editions. Microsoft Learn. https://learn.microsoft.com/en-us/windows-server/get-started/editions-comparison

Microsoft. (2025b). What's new in Windows Server 2022. Microsoft Learn. https://learn.microsoft.com/en-us/windows-server/get-started/whats-new-in-windows-server-2022

Microsoft. (2023b). Requisitos de hardware para Windows Server. *Microsoft Learn*. https://learn.microsoft.com/es-es/windows-server/get-started/hardware-requirements

Microsoft. (2023c). Local accounts. *Microsoft Learn*. https://learn.microsoft.com/es-es/windows/security/identity-protection/access-control/local-accounts

Microsoft. (2024). Hardware requirements for Windows Server. *Microsoft Learn*. https://learn.microsoft.com/en-us/windows-server/get-started/hardware-requirements?tabs=cpu&pivots=windows-server-2025

Microsoft. (2025b). Policy CSP - UserRights. *Microsoft Learn*. https://learn.microsoft.com/es-es/windows/client-management/mdm/policy-csp-userrights

Microsoft. (2025c). ¿Qué es Server Core? *Microsoft Learn*. https://learn.microsoft.com/es-es/windows-server/administration/server-core/what-is-server-core

Microsoft. (2025d). Opciones de instalación de Windows Server: Server Core y Desktop Experience. *Microsoft Learn*. https://learn.microsoft.com/es-es/windows-server/get-started/install-options-server-core-desktop-experience

Microsoft. (2025e). Administrar Server Core. *Microsoft Learn*. https://learn.microsoft.com/es-es/windows-server/administration/server-core/server-core-administer

Ruiz, P. (2023, 4 septiembre). Windows Server 2022: Ediciones y licencias. *SomeBooks.es*. https://somebooks.es/windows-server-2022-ediciones-y-licencias/

CAPÍTULO 2

ADMINISTRACIÓN DE LOS SERVICIOS DE: DHCP, DNS Y WEB.

Administración de los Servicios de Red: DHCP, DNS e IIS

Objetivos

Instalar y Configurar el servicio DHCP para la asignación dinámica de los elementos TCP/IP

Instalar y Configurar el servicio DNS para la resolución de nombres de dominio.

Implementar zonas directas e inversas en DNS, asegurando la disponibilidad y confiabilidad en la resolución de nombres dentro de redes locales o globales.

Instalar y configurar Internet Information Services (IIS) como plataforma para el alojamiento de sitios web.

El Protocolo de Configuración Dinámica de Host (DHCP) automatiza la asignación de direcciones IP y otros parámetros de red, facilitando la administración y reduciendo errores en redes con múltiples dispositivos. Permite definir ámbitos de direcciones, establecer reservas para equipos específicos mediante su dirección MAC, aplicar exclusiones y configurar filtros para controlar el acceso al servicio, mejorando así la eficiencia y seguridad de la red.

A la par del DHCP, el Sistema de Nombres de Dominio (DNS) y el servicio Internet Information Services (IIS) constituyen pilares fundamentales dentro de una infraestructura de red moderna. El DNS actúa como una especie de guía telefónica de Internet: traduce nombres de dominio fáciles de recordar, como

www.ejemplo.com, en direcciones IP que las computadoras pueden entender. Esta función es esencial para la navegación web, el envío de correos electrónicos y la comunicación entre dispositivos.

Por su parte, IIS es la plataforma de servidor web de Microsoft, que convierte un sistema Windows en un entorno para alojar sitios y aplicaciones web. Gestiona eficazmente las solicitudes entrantes, distribuyéndolas mediante subprocesos para optimizar el rendimiento. Además, incluye importantes mecanismos de seguridad, como el uso de cifrado SSL/TLS y la gestión de los puertos estándar HTTP y HTTPS, lo cual garantiza comunicaciones seguras entre los usuarios y los servicios web.

Este capítulo ofrece una visión completa de estos tres servicios. En el caso de DHCP, se profundiza en la creación y gestión de ámbitos, reservas, exclusiones y filtros. Para DNS, se analiza su funcionamiento interno, los diferentes tipos de servidores, las zonas directas e inversas, y los registros más comunes. En cuanto a IIS, se estudian sus componentes principales, la administración de solicitudes HTTP, la implementación de dominios virtuales y los módulos que permiten personalizar su comportamiento. Una correcta configuración de todos estos elementos contribuye de forma significativa a mejorar la disponibilidad, la seguridad y la eficiencia de las redes y aplicaciones, ya sea en contextos empresariales, educativos o personales.

Preguntas de Enfoque

Preguntas de Inicio

1. ¿Qué es el servicio DNS y por qué es fundamental para la navegación web y la resolución de nombres en redes locales o globales?

2. ¿Qué función cumple IIS dentro de una infraestructura de red y cómo facilita el despliegue de aplicaciones web?

3. ¿Cuáles son las principales diferencias entre los servicios ofrecidos por DNS e IIS y cómo se complementan en la gestión de redes empresariales?

Competencias o Problemas a Resolver

Al finalizar este capítulo, los lectores serán capaces de:

- Comprender y explicar los principios fundamentales del servicio DNS, incluyendo zonas directas e inversas, registros y procesos de resolución de nombres.

- Instalar, configurar y administrar Internet Information Services (IIS) en un entorno Windows Server para la gestión de sitios y aplicaciones web.

- Aplicar configuraciones de seguridad en DNS e IIS, como el bloqueo de sitios sospechosos o la implementación de certificados SSL/TLS.

Problemas a Resolver

1. ¿Cómo se puede estructurar correctamente una zona DNS para garantizar la disponibilidad y resolución efectiva de nombres de dominio dentro de una red corporativa?

2. ¿Qué estrategias pueden implementarse en IIS para mejorar la seguridad y el rendimiento de aplicaciones web alojadas en un mismo servidor?

3. ¿Cómo se puede integrar de manera efectiva el uso de DNS e IIS en una infraestructura que requiere servicios confiables, rápidos y protegidos para usuarios internos y externos?

Servidor de DHCP

El servidor DHCP (Protocolo de Configuración Dinámica de Host) en Windows Server facilita de forma automática la asignación y gestión de direcciones IP, así como de otros parámetros de red. Al encargarse centralizadamente de estas funciones, ayuda a disminuir la intervención manual, reduce los errores y optimiza la utilización de las direcciones IP disponibles en la red. Windows Server ofrece el servidor DHCP como un rol de red opcional que puede instalarse para distribuir direcciones IP y configuraciones relacionadas a los dispositivos cliente que utilicen DHCP. Los sistemas operativos cliente de Windows incluyen, por defecto, el cliente DHCP integrado en la pila de TCP/IP. DHCP es un protocolo basado en el modelo cliente-servidor que asigna automáticamente a un equipo una dirección IP y otros datos necesarios para su configuración en la red, como la máscara de subred y la puerta de enlace predeterminada. Está definido en los documentos RFC 2131 y RFC 2132 del IETF como un estándar derivado del protocolo BOOTP, con el cual comparte varias características técnicas. Gracias a DHCP, los dispositivos pueden obtener toda la configuración TCP/IP necesaria directamente desde un servidor (Microsoft, 2025).

Funcionamiento del DHCP

El Protocolo de Configuración Dinámica de Host (DHCP) es un protocolo de red utilizado para asignar automáticamente direcciones IP y otros parámetros de configuración de red a los dispositivos en una red. Esto facilita la administración de la configuración de red sin la intervención manual de los administradores de red.

- DHCP DISCOVERYL: El proceso de DHCP DISCOVERY es el primer paso en el cual un cliente DHCP envía un mensaje de descubrimiento (DHCPDISCOVER) para identificar los servidores DHCP disponibles en la red. Este mensaje se envía como una difusión (broadcast) porque el cliente no tiene conocimiento de la dirección IP del servidor DHCP.
- DHCP OFFER: En respuesta al mensaje de descubrimiento, los servidores DHCP envían un mensaje de oferta (DHCPOFFER). Este mensaje contiene una dirección IP disponible y otros parámetros de configuración de red que el servidor DHCP está dispuesto a asignar al cliente.
- DHCP REQUEST: El cliente responde con un mensaje de solicitud (DHCPREQUEST), indicando que acepta la oferta y solicitando la asignación de la dirección IP propuesta. Este mensaje también se difunde a todos los servidores DHCP para que aquellos que no fueron seleccionados puedan liberar las direcciones IP ofrecidas.
- DHCP ACK: Finalmente, el servidor DHCP seleccionado envía un mensaje de reconocimiento (DHCPACK) al cliente. Este mensaje confirma la asignación de la dirección IP y proporciona cualquier otra configuración de red necesaria. A partir de este punto, el cliente puede usar la dirección IP asignada y los parámetros de configuración para comunicarse en la red (OmniSecu, 2025).

Tipos de Asignación de Direcciones IP

La asignación de direcciones IP es un componente fundamental en la gestión de redes. Permite a los dispositivos conectados a una red recibir una dirección IP que les permite comunicarse entre sí y acceder a otros recursos de la red, incluyendo Internet.

- Asignación Automática: La asignación automática de direcciones IP permite a un servidor DHCP asignar una dirección IP permanente a un dispositivo. Una vez asignada, la dirección IP se guarda y se utiliza cada vez que el dispositivo se conecta a la red. (OmniSecu, OmniSecu)
- Asignación Dinámica: La asignación dinámica implica que el servidor DHCP asigna una dirección IP a un dispositivo por un período de tiempo limitado, conocido como "duración del arrendamiento" (lease time). Esta dirección IP puede cambiar cada vez que el dispositivo se conecta a la red o cuando expira el período de arrendamiento. (Ewing, 2022)
- Asignación Manual o Estática con Reserva: La asignación manual o estática con reserva es cuando el administrador de la red asigna una dirección IP específica a un dispositivo basándose en su dirección MAC. Esta dirección IP es reservada en la base de datos del servidor DHCP y se asigna al dispositivo cada vez que se conecta a la red (De Luz, 2024).

Exclusiones y Reservas en el Servicio DHCP

El Servicio DHCP (Dynamic Host Configuration Protocol) facilita la asignación automática de direcciones IP y otros parámetros de configuración de red a los dispositivos en una red. Este servicio permite la gestión eficiente de direcciones IP, asegurando que no haya conflictos y facilitando la administración de grandes redes. Dentro de las funcionalidades del DHCP, se encuentran las exclusiones y las reservas de direcciones IP, que permiten un control más granular sobre cómo se asignan las direcciones IP a los dispositivos.

- Exclusiones: Las exclusiones en un ámbito DHCP se utilizan para evitar que ciertas direcciones IP dentro de un rango sean asignadas automáticamente a los clientes DHCP. Esto es útil

cuando se necesita reservar direcciones IP específicas para su asignación manual o para dispositivos que requieren configuraciones estáticas.

- Reservas: Las reservas DHCP permiten asignar una dirección IP específica a un dispositivo en función de su dirección MAC. Esto asegura que el dispositivo siempre reciba la misma dirección IP cada vez que se conecta a la red. Esta funcionalidad es especialmente útil para dispositivos que requieren direcciones IP fijas, como servidores, impresoras de red y otros dispositivos críticos (EITCA Academy, 2023).

Beneficios del Uso de DHCP

El uso del Protocolo de Configuración Dinámica de Host (DHCP) ofrece numerosos beneficios en la administración de redes, especialmente en términos de automatización y eficiencia. Aquí se detallan algunos de los principales beneficios:

- Configuración Automática y Centralizada: DHCP automatiza la asignación de direcciones IP y otros parámetros de red (como la máscara de subred, puerta de enlace predeterminada y servidores DNS), lo que elimina la necesidad de configuración manual y reduce el riesgo de errores humanos. Esta automatización simplifica significativamente la administración de redes, permitiendo que incluso usuarios sin conocimientos técnicos puedan conectarse fácilmente a la red (Riveros García, 2023).

- Eficiencia en el Uso de Direcciones IP: DHCP permite una gestión eficiente de las direcciones IP disponibles mediante la asignación dinámica. Esto evita la asignación duplicada de direcciones y minimiza los conflictos, lo cual es esencial en entornos con un gran número de dispositivos que se conectan y desconectan frecuentemente.

- Facilidad de Expansión y Flexibilidad: Con DHCP, añadir nuevos dispositivos a la red es un proceso sencillo y rápido. La red puede crecer y adaptarse a cambios sin la necesidad de reconfigurar manualmente cada dispositivo. Esto es especialmente útil en entornos empresariales y redes públicas como cafeterías y aeropuertos.

- Compatibilidad y Soporte Extenso: DHCP es compatible con una amplia variedad de dispositivos y puede integrarse fácilmente en redes que utilizan otros protocolos como BOOTP. Además, el protocolo puede ser utilizado tanto en redes locales como remotas, facilitando el manejo de redes complejas y distribuidas (García de Zúñiga, 2024).

- Reducción de la Carga Administrativa: La centralización de la configuración TCP/IP reduce significativamente la carga administrativa al permitir a los administradores gestionar la red desde un único punto de control. Esto incluye la capacidad de definir configuraciones desde una ubicación central y aplicar cambios rápidamente en toda la red. (Riveros García, 2023).

Comandos de Diagnóstico de Red

ipconfig /all:

Función: Muestra toda la información detallada de las interfaces de red del equipo, incluyendo direcciones IP, máscara de subred, puerta de enlace predeterminada, servidores DNS, DHCP, y más.

Tabla 7. Comando para mostrar información detallada

cmd
ipconfig /all

Fuente: Elaboración propia

Aplicación: Se utiliza para obtener una visión completa de la configuración de red actual del equipo. Es útil para diagnosticar problemas de configuración y verificar los parámetros asignados por DHCP.

ipconfig /release:

Función: Libera la dirección IP asignada por DHCP, desconectando temporalmente el equipo de la red.

Tabla 8. Libera dirección IP del DHCP asignada

cmd
ipconfig /release

Fuente: Elaboración propia

Aplicación: Se utiliza cuando necesitas liberar la dirección IP actual del equipo, por ejemplo, antes de reasignar una nueva dirección IP o para resolver conflictos de direcciones IP.

ipconfig /renew:

Función: Renueva la dirección IP desde el servidor DHCP, solicitando una nueva dirección IP

Tabla 9. Proporciona una nueva dirección IP con DHCP

cmd
ipconfig / **renew**

Fuente: Elaboración propia

Aplicación: Si un dispositivo no puede conectarse a la red correctamente, este comando puede resolver el problema solicitando una nueva dirección IP del servidor DHCP.

Implementación Práctica del servicio de DHCP

Instalación del servicio de DHCP

Antes de todo debemos instalar el DHCP por lo cual estando en el panel de administrador del servidor damos clic en "Agregar roles y características"

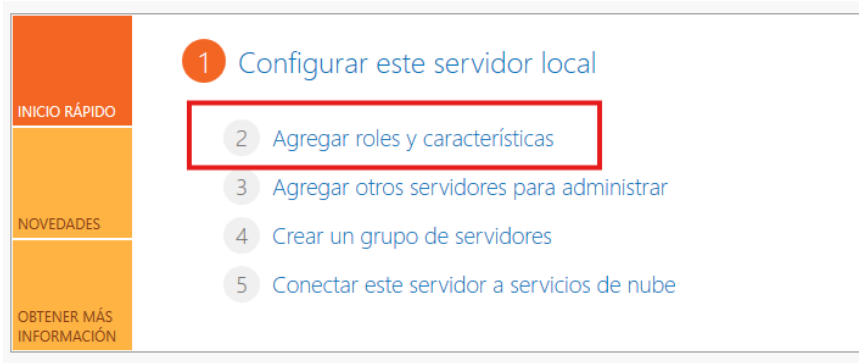


Ilustración 72. Administrador del servidor.

Fuente: Elaboración propia

Se nos abrirá el asistente para agregar roles y características, deberemos dar clic en "siguiente" en el proceso.

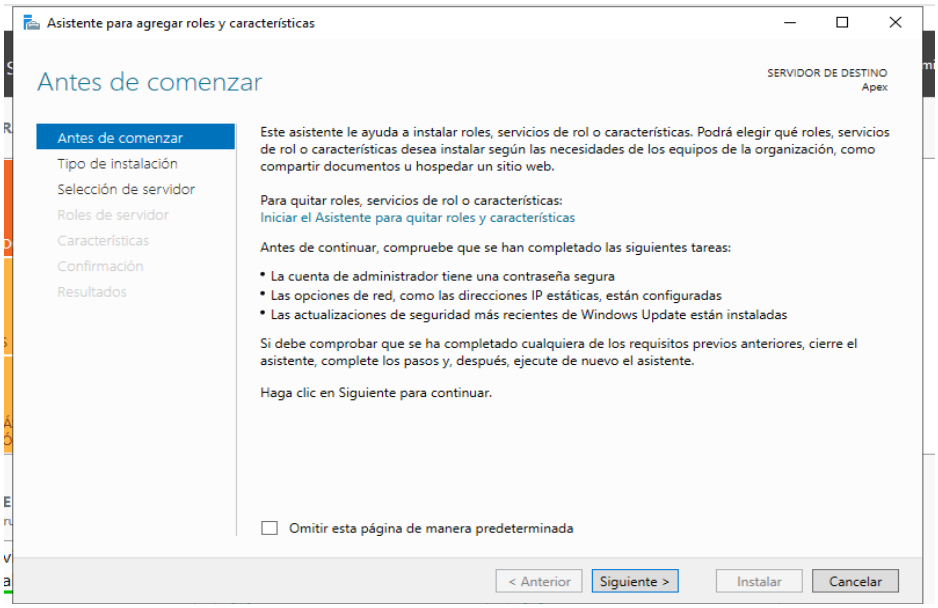


Ilustración 73. Asistente de agregar roles y características

Fuente: Elaboración propia

Escogeremos la instalación deseada, en nuestro caso seleccionaremos "Instalación basada en características o en roles" y damos clic en "siguiente".

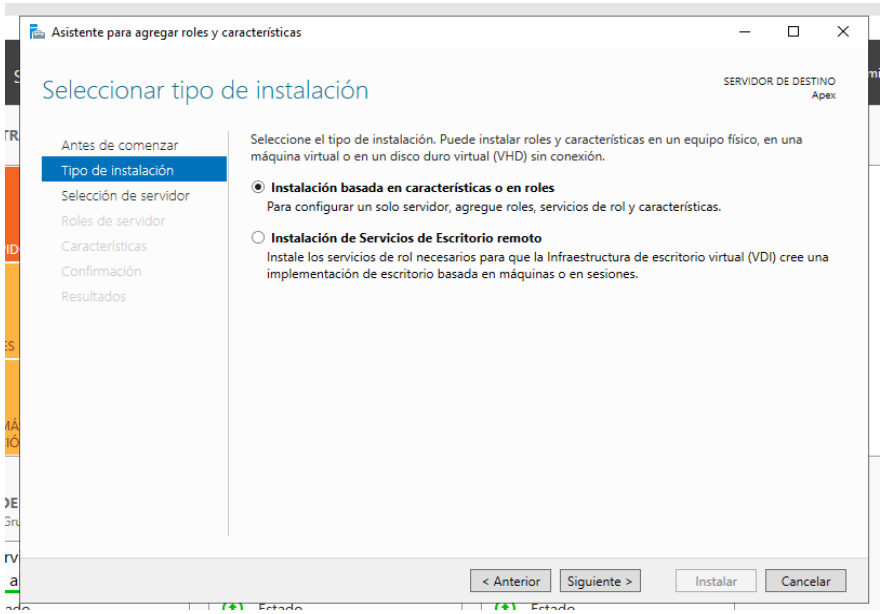


Ilustración 74. Selección de tipo de instalación.

Fuente: Elaboración propia

Ahora nos aparecerá un listado en donde aparecerán nuestros servidores, en este caso solo tendremos nuestro servidor que es llamado "apex" (cada uno tendrá su propio servidor con su propio nombre). Seleccionamos el servidor y damos clic a siguiente.

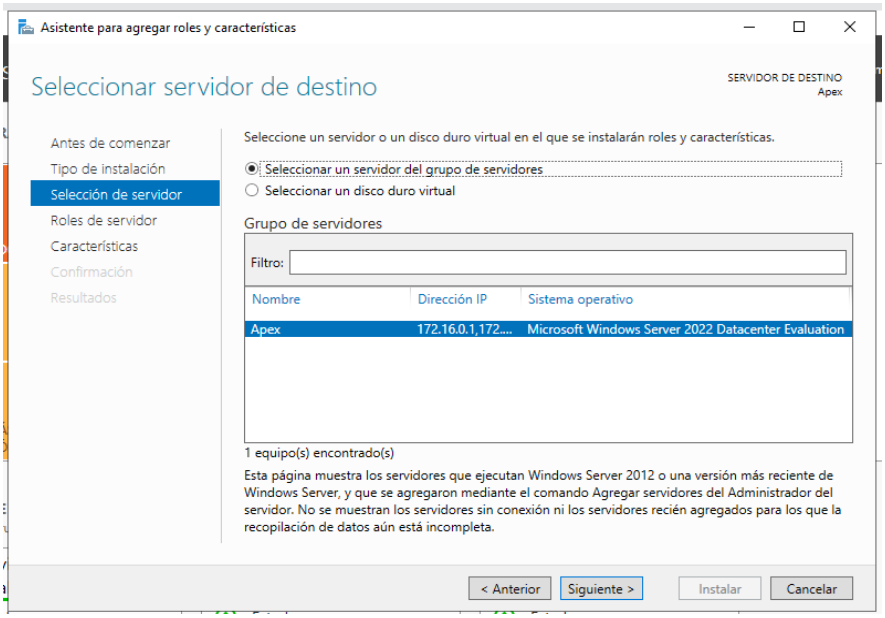


Ilustración 75. Selección del Servidor.

Fuente: Elaboración propia

Buscamos el rol que queremos agregar, en este caso se llama "Servidor DHCP", seleccionamos y nos aparecerá otra ventana en donde damos clic en agregar "agregar características y damos clic a "Siguiente"

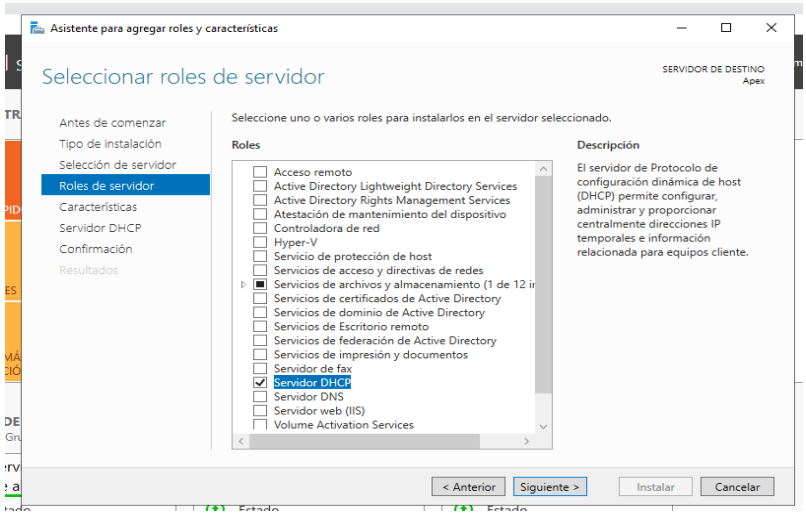


Ilustración 76. Selección de Rol DHCP.

Fuente: Elaboración propia

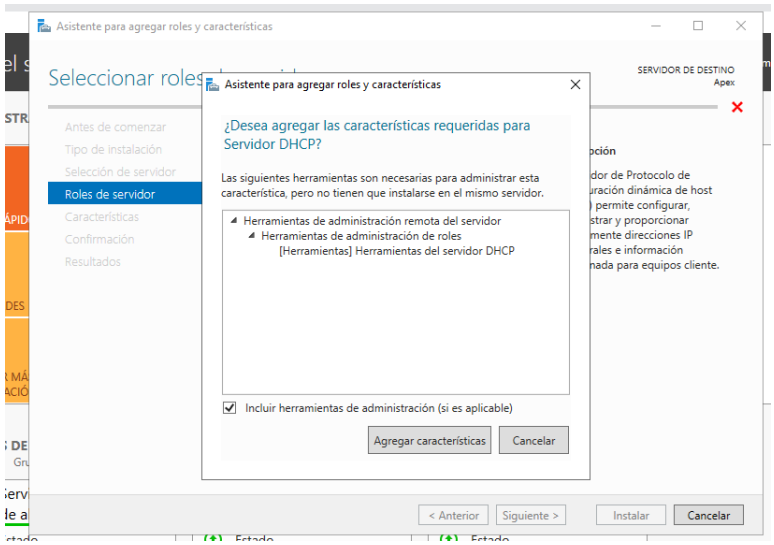


Ilustración 77. Agregar Características del Rol DHCP.

Fuente: Elaboración propia

Una vez culminado le damos a Instalar y se nos iniciará una progresión de Instalación de características. Por último, se deberá cerrar.

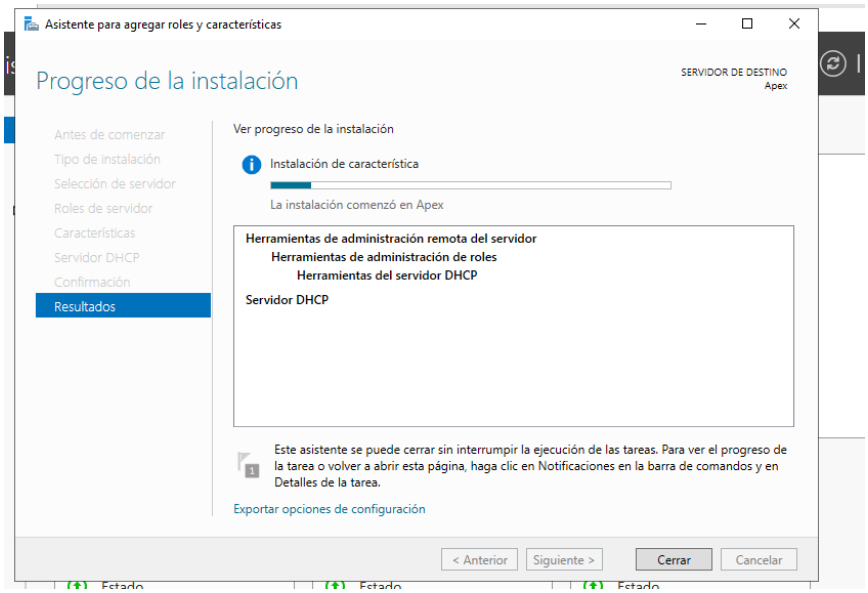


Ilustración 78. Instalación de características del Rol DHCP.

Fuente: Elaboración propia

Configuración servidor DHCP

Primeramente, para poder entrar a la configuración del DHCP nos ubicamos en la parte superior, damos clic en "herramientas" luego en el rol creado, en este caso del "DHCP".

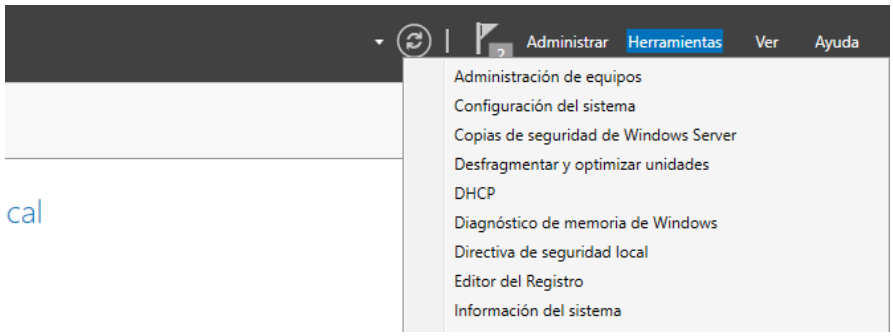


Ilustración 79. Configuración del DHCP.

Fuente: Elaboración propia

Nos saldrá una nueva ventana en donde aparecerá nuestro servidor "apex", en este escogemos ipv4 y damos clic derecho para crear un "Ámbito nuevo…"

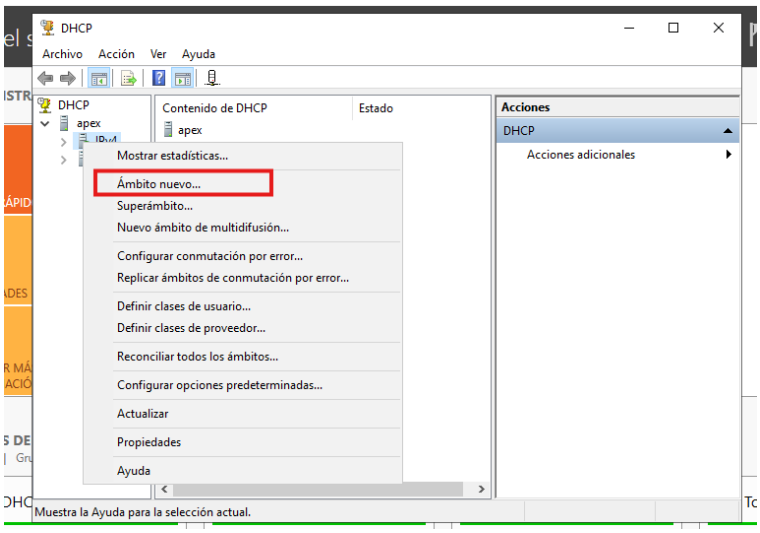


Ilustración 80. Creación de Ámbito nuevo.

Fuente: Elaboración propia

Se abrirá una ventana nueva de "Asistente para ámbito nuevo" y asignaremos el nombre y la descripción.

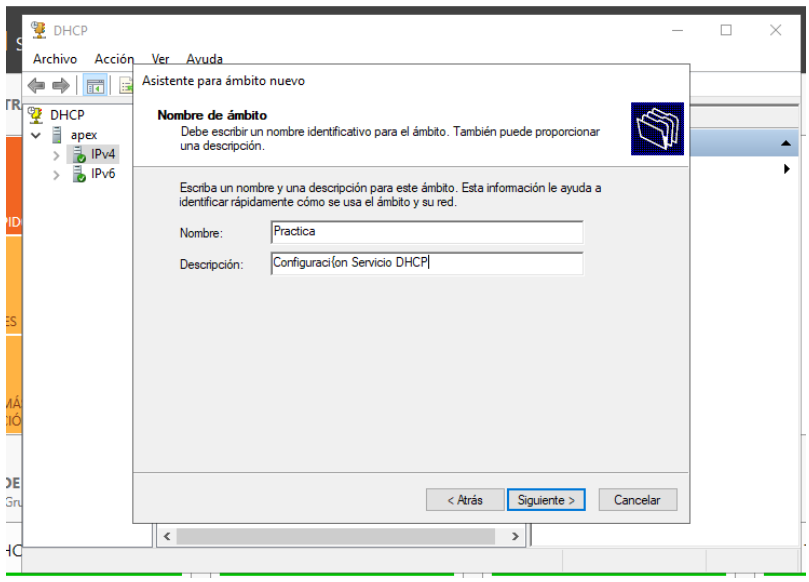


Ilustración 81. Asignación de nombre y descripción

Fuente: Elaboración propia

Ahora asignaremos un intervalo de direcciones IP que utiliza el DHCP para que estos sean asignados a distintos dispositivos.

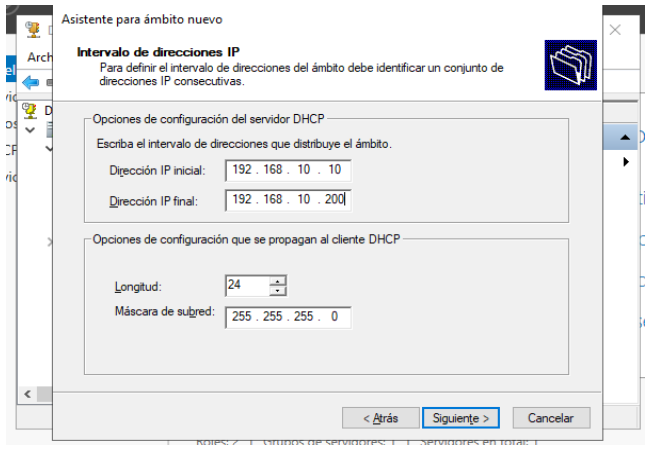


Ilustración 82. Rango de direcciones IP.

Fuente: Elaboración propia

Nos saldrá la siguiente ventana el cual pondremos las exclusiones el cual serán un rango de direcciones IP que el servicio DHCP denegará o no asignará a los clientes.

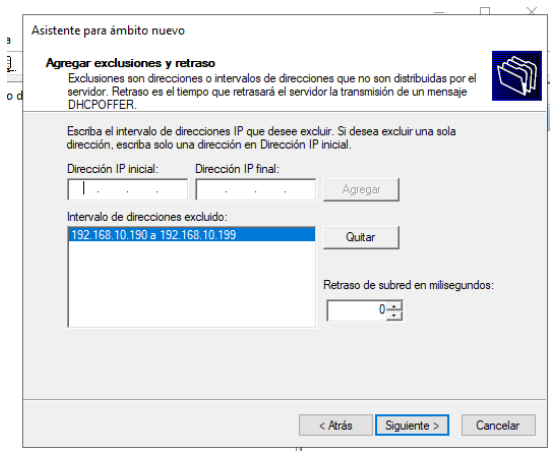


Ilustración 83. Agregación de rango de Exclusiones.

Fuente: Elaboración propia

Ahora podremos configurar el tiempo de concesión el cual el cliente podrá utilizar una dirección IP de dicho ámbito. Por defecto vamos a dejarlo 8 horas.

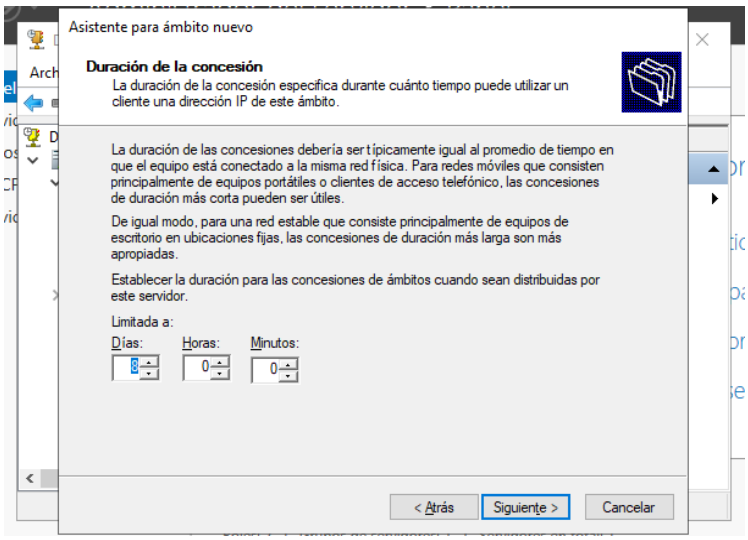


Ilustración 84. Duración de Concesión.

Fuente: Elaboración propia

En la máquina del cliente nos aseguramos que se encuentre activada la opción “Obtener una dirección IP automáticamente".

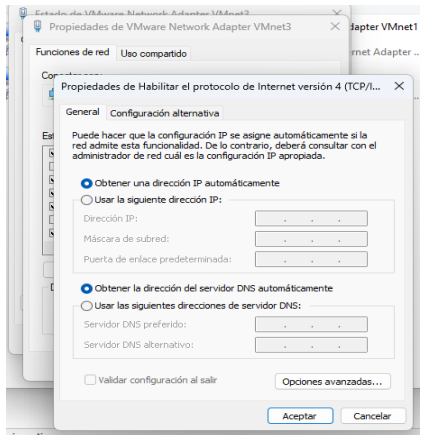


Ilustración 85. Dirección IP automática en propiedades.

Fuente: Autores

Podemos revisar que se ha asignado automáticamente en la máquina del cliente una ip el cual asignamos.

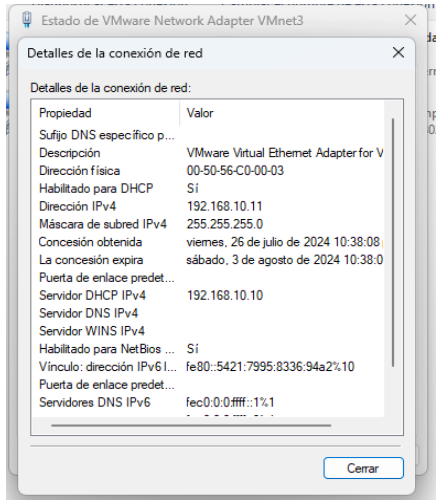


Ilustración 86. Comprobación de asignación de dirección IP.

Fuente: Elaboración propia

Para asignar reservas ya sea para una impresora o algún dispositivo que nosotros deseamos debemos ubicarnos en la ventana del DHCP nuevamente y dar clic derecho en "Reservas" y luego a "Reserva nueva…"

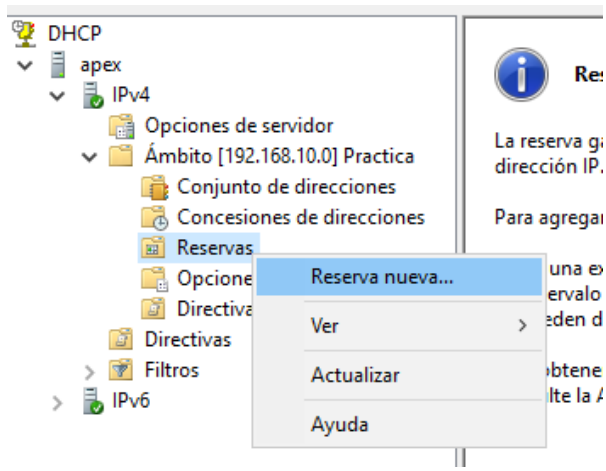


Ilustración 87. Creación de una Reserva.

Fuente: Autores

Asignamos los datos de la máquina el cual queremos reservar, en este ejemplo usaremos los siguiente

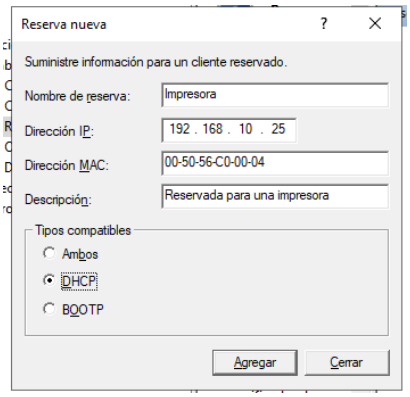


Ilustración 88. Configurar la Reserva.

Fuente: Elaboración propia

Vamos a denegar dispositivos el cuales nosotros no deseamos que estás sean clientes del DHCP

Para esto en la ventana DHCP vamos a filtros y de ahí a "Denegar" clic derecho y "Nuevo filtro…"

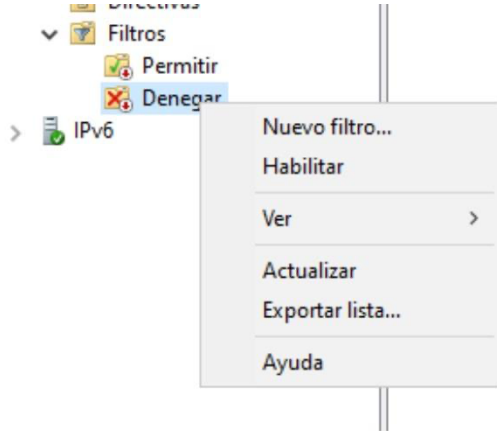


Ilustración 89. Filtro de negación.

Fuente: Elaboración propia

Asignamos la dirección MAC del cual está denegará

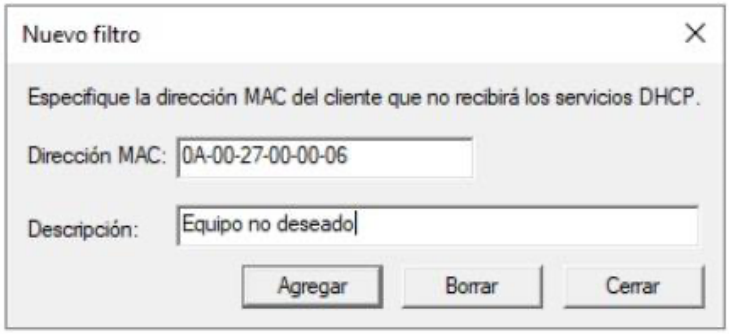


Ilustración 90. Dirección MAC del cual será negado.

Fuente: Elaboración propia

En Concesión de direcciones podremos observar todas las Denegaciones o filtros que poseemos.

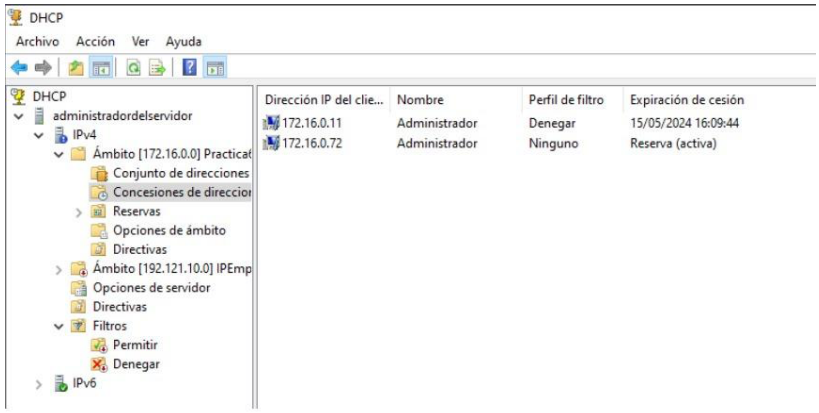


Ilustración 91. Panel de Concesiones de direcciones.

Fuente: Autores

Servidor de DNS

El sistema de nombres de dominio (DNS), es una gran base de datos que relaciona cada nombre de dominio con el número o dirección IP del equipo al que está asociado y viceversa, los nombres de dominio de Internet han pasado a tener una función igualmente importante, como es la de identificar de una manera sencilla a las empresas y organizaciones presentes en Internet, facilitando que los usuarios puedan acceder de manera inmediata a la información y los servicios que éstas ofrecen en la Red. El DNS se apoya en una gran base de datos distribuida por todo Internet construida como una estructura jerárquica (Rodríguez Raposo, 2001).

Funcionamiento del DNS

El funcionamiento del DNS se realiza en un esquema cliente/servidor, siendo el cliente el que requiere la resolución de nombres. Los Servidores DNS utilizan TCP y UDP, en el puerto 53 para responder las consultas. Casi todas las consultas consisten de una sola solicitud UDP desde un Cliente DNS, seguida por una sola respuesta UDP del servidor. Se realiza una conexión TCP cuando el tamaño de los datos de la respuesta excede los 512 bytes, tal como ocurre con tareas como transferencia de zonas (Barbieri, 2023)

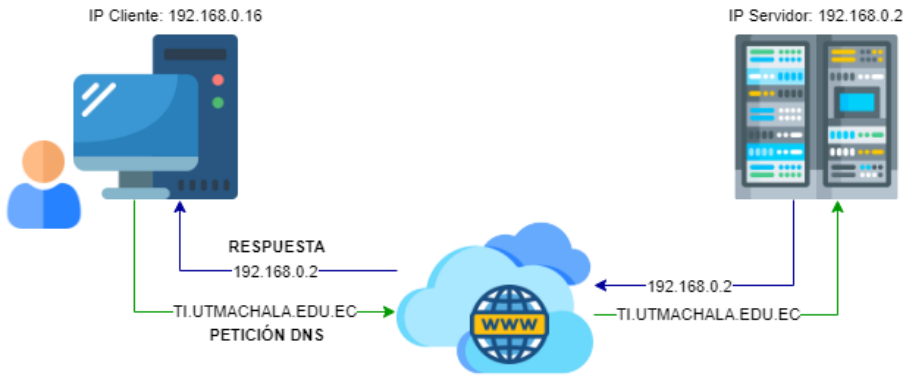


Ilustración 92. Funcionamiento DNS

Fuente: Elaboración propia

En la ilustración se puede observar un ejemplo del funcionamiento del servicio DNS, al ingresar la dirección del sitio web al que se desea acceder en este caso https: //www.ti.utmachala.edu.ec, el equipo realiza una petición para conectarse al servidor DNS. El servidor busca el dominio en su base de datos y devuelve la dirección IP al equipo para que acceda al sitio web.

Puertos DNS

Un puerto DNS es un puerto de comunicación designado por su servidor DNS para poder tener una comunicación con un dispositivo para la resolución de nombres de dominio.

Lista de puertos DNS:

- Puerto UDP 53
- Puerto TCP 53

El DNS emplea protocolos UDP y TCP para la comunicación entre los cliente-servidor. Por lo que, de manera automática, el DNS usa

el puerto UDP 53 y pasa al puerto TCP 53 cuando no puede comunicarse en UDP. Esto sucede cuando se sobrepasa el tamaño establecido para el paquete UDP y el DNS recurre a TCP para que sea más seguro (WPADE, 2024).

Tipos de servidores DNS

Según el tipo de funciones que realicen, existen tres tipos de servidores DNS que son utilizados para diferentes fines, los cuales son los siguientes:

Servidores DNS maestros

Este tipo de servidor DNS tiene permisos autoritativos de una zona, y contiene la información de la misma en sus archivos de configuración, además de permitir la transferencia automática de información de la zona desde otros servidores DNS. Sin embargo, existen algunas limitaciones con la transferencia de datos de la zona, ya que estos archivos pierden su orden y todos sus comentarios.

Servidores DNS esclavos

Este tipo de servidores son utilizados como DNS de respaldo, de manera que son ubicados en diferentes locaciones mejorando la conexión y los tiempos en la solicitud y respuesta del cliente al servidor DNS.

Servidores de DNS de caché

Estos servidores son utilizados para minorizar las tareas de los servidores primarios y secundarios. Al realizar una petición al DNS este devuelve la IP, pero no es óptimo realizar la misma petición a cada momento, por lo que se usa este tipo de DNS que registra los

dominios con sus respectivas direcciones IP que ya han sido solicitadas (IBM Corporation, 2010).

Nombres de dominio

Los nombres de dominio son un conjunto de caracteres que están definidas por etiquetas que se dividen por niveles, los cuales siendo letras, números y guion medio y no se distinguen entre mayúsculas y minúsculas. Estos niveles deben tener menos de 63 caracteres. Es importante aclarar que no pueden iniciar o finalizar en el guion y tener en cuenta que habrá 127 niveles disponibles mientras no se sobrepase el límite de los 255 caracteres [4].

Estos nombres de dominio se organizan mediante árboles que van desde el nivel jerárquico más bajo hasta el más alto llegando hasta su raíz. [4].

Por lo tanto, a cada nivel de la estructura se le asigna un nombre o etiqueta comenzando así:

- Primer nivel: es el Dominio de Nivel Superior es el que se encuentra a la derecha del todo, este puede "ec" o .com, .es, .net.
- Segundo nivel: este nivel especifica el nombre del dominio. Por ejemplo ". edu.ec"
- Tercer nivel: se especifica el nombre de maquia o

subdominio. Por ejemplo “utmachala.edu.ec”.

- **Cuarto nivel:** en este nivel se conforma en su totalidad la estructura del nombre. Por ejemplo “www.utmachala.edu.ec”

Ilustración 93. Funcionamiento DNS

Fuente: Elaboración propia

Registro de recursos

Según Cloudflare (2025), los registros DNS, o archivos de zona, son instrucciones guardadas en servidores DNS autoritativos que indican cómo manejar un dominio. Básicamente, contienen información como la dirección IP asociada a ese dominio y cómo gestionar las solicitudes que se envían a dicho dominio. Estos registros están escritos en un formato especial llamado sintaxis DNS, que es como un conjunto de comandos en texto que le dicen al servidor DNS qué hacer.

Tipos de registros más comunes:

- Registro A: Este registro que contiene la dirección IP de un dominio.
- Registro AAAA: Este registro contiene la dirección IPv6 de un dominio
- Registro CNAME: Este registro reenvía un dominio o subdominio a otro dominio por lo que no utiliza dirección IP

- Registro MX: Este registro dirige el correo a un servidor de correo electrónico.
- Registro TXT: Este registro autoriza que un administrador pueda almacenar notas de texto en el registro. Estos registros se suelen ser de gran ayuda para la seguridad del correo electrónico.
- Registro NS: Este registro almacena el servidor de nombres para una entrada DNS. Registro SOA: Este registro guarda la información del administrador sobre un dominio.
- Registro SRV: Este registro especifica un puerto para servicios específicos.
- Registro PTR: Este registro proporciona un nombre de dominio en búsquedas inversas.

Zonas

Una zona DNS es una parte del espacio de nombres de DNS que está gestionada por una organización o administrador específicos. Una zona DNS es un espacio administrativo que permite un mayor control granular de los componentes de DNS, tales como los servidores de nombres autorizados. Se definen dos secciones de zona para cada dominio o subdominio. El primero contiene los datos de resolución de nombres y el segundo contiene los datos de resolución inversa.

Zona Directa

La zona directa resuelve los nombres de host en direcciones IP y albergan los registros de recursos comunes: A, CNAME, SRV, MX, SOA, TXT y NS.

Zona Inversa

La zona inversa resuelve una dirección IP a un nombre de dominio, y albergan los registros: SOA, NS y PTR. Las funciones de la zona de búsqueda inversa son las mismas que la zona de búsqueda directa, pero la dirección IP es la parte de la consulta y el nombre de host es la información devuelta. Las zonas de búsqueda inversa no siempre se configuran, pero es recomendable que se configure para reducir las advertencias y mensajes de error (InterGrupo, 2013).

Comandos de diagnóstico

Nslookup

Nslookup es una herramienta de línea de comandos práctica y sencilla de usar, cuya función es encontrar la dirección IP de un equipo determinado o realizar una búsqueda DNS inversa (IONOS, 2019).

Ping

Ping está dentro de los paquetes de software TCP/IP y utiliza una serie de mensajes de eco para determinar si un host de destino, identificado con una determina IP, es accesible desde otro host. También se utiliza para detectar el retardo de envió y retorno en la comunicación (Kessler & Shepard, 1997).

Caso Práctico

Topología e Instalación del servicio DNS

Como pueden observar en la topología, se trata de un cliente que realiza las consultas al servidor.

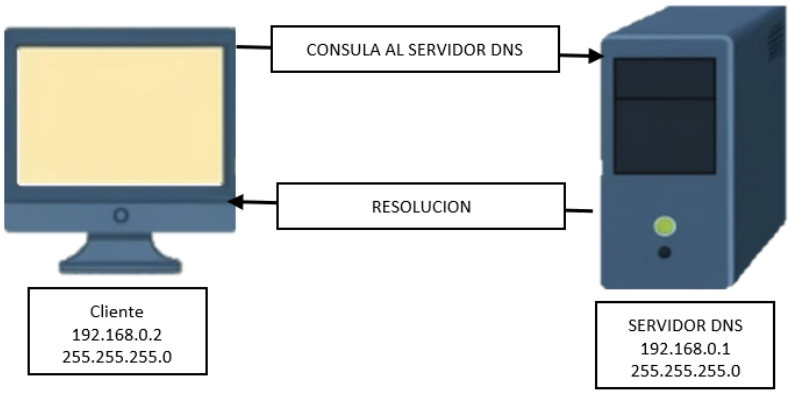


Ilustración 94. Topología del Servidor DNS

Fuente: Elaboración propia

Una vez abierto el Administrador del Servidor, procedemos a instalar el servicio DNS. Para ello, nos dirigimos al Administrador del Servidor y hacemos clic en "Agregar roles y características". Se iniciará el asistente para agregar roles y características y se da clic en “siguiente”.

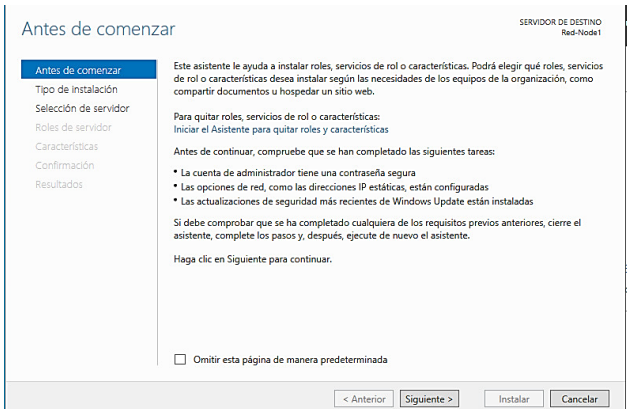


Ilustración 95. Instalación del Servicio DNS

Fuente: Elaboración propia

Seleccionamos el tipo de instalación en este caso se escoge "Instalación basada en características o en roles". Y damos clic en "siguiente".

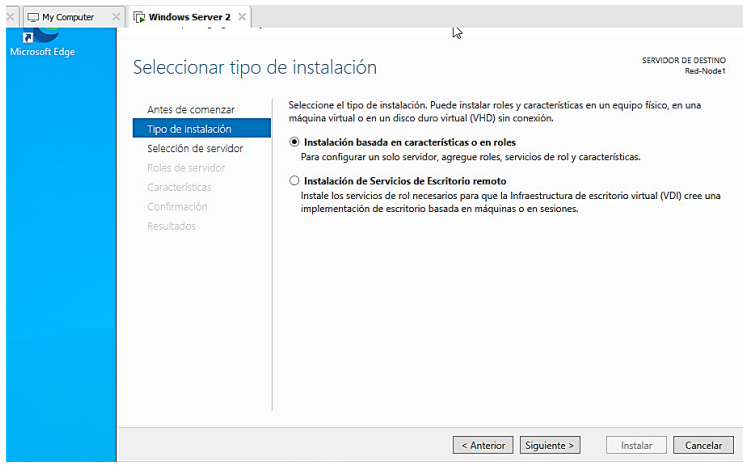


Ilustración 96. Asistente de Instalación del servicio

Fuente: Elaboración propia

Se selecciona un servidor de destino del grupo de servidores y luego clic en “siguiente”

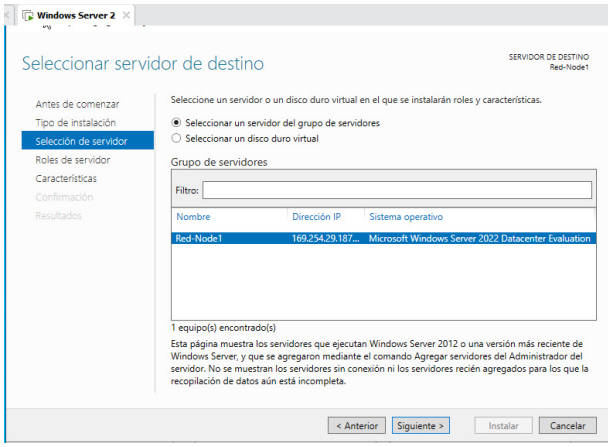


Ilustración 97. Selección del Servidor de Destino

Fuente: Elaboración propia

Una vez completadas las configuraciones necesarias, se selecciona la opción "Instalar" para iniciar el proceso de instalación del servicio DNS. Una vez que la instalación ha concluido satisfactoriamente, se hace clic en "Cerrar" para finalizar el proceso. Con esto, el servicio DNS queda correctamente instalado y listo para su uso.

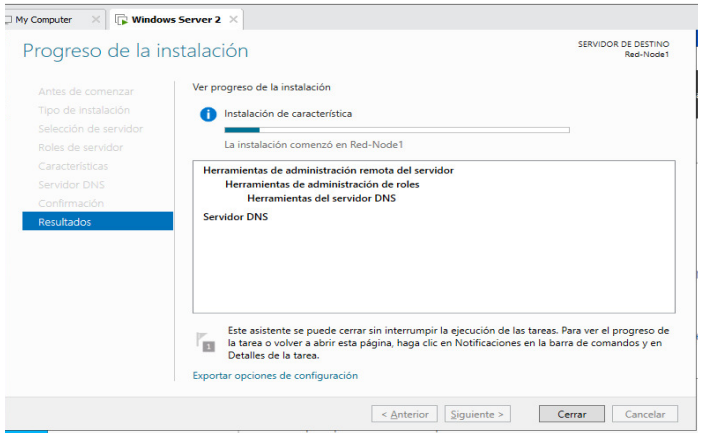


Ilustración 98. Instalación del Servicio DNS

Fuente: Elaboración propia

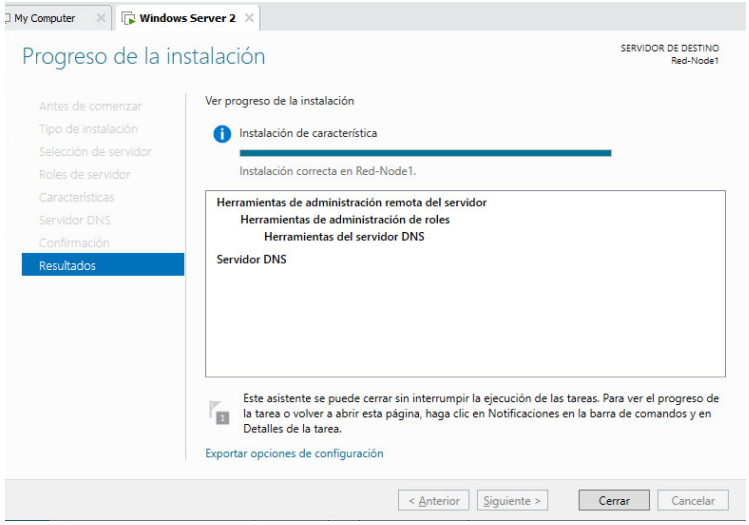


Ilustración 99. Instalación Completa

Fuente: Elaboración propia

Creación zona directa

Desde el Administrador de Servidor DNS crear una zona nueva inversa en zonas de búsqueda inversa.

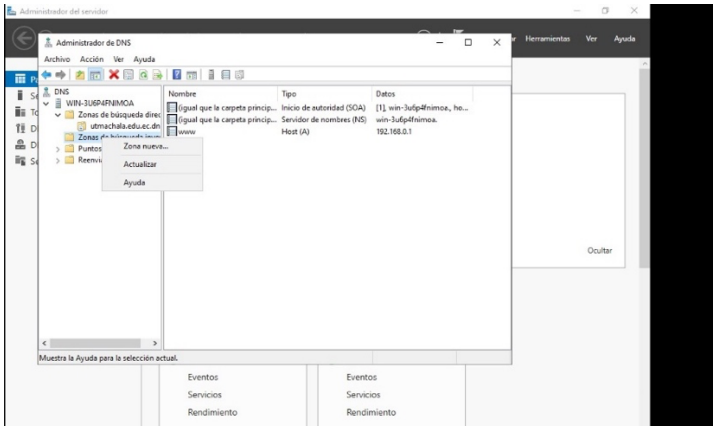


Ilustración 100. Creación de la Nueva zona

Fuente: Elaboración propia

Para crear una nueva zona de búsqueda directa, se puede hacer clic derecho sobre "Zonas de búsqueda directa" y seleccionar la opción "Zona nueva". Este proceso es comúnmente realizado por administradores de sistemas o personas encargadas de la gestión de servidores DNS.

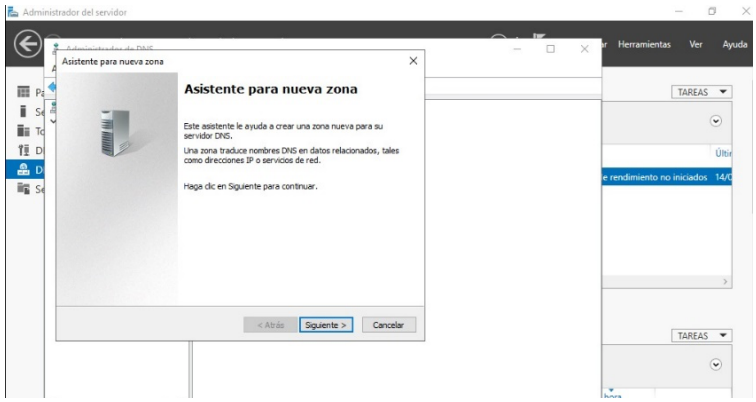


Ilustración 101. Asistente para crear Zona Directa

Fuente: Elaboración propia

La nueva zona se define como "utmachala.edu.ec". Esta designación establece un ámbito específico dentro del Sistema de Nombres de Dominio (DNS) para la Universidad Técnica de Machala en Ecuador.

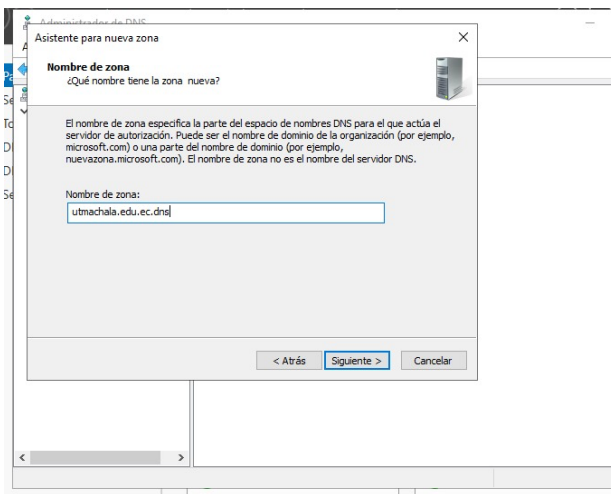


Ilustración 102. Nombre de la Zona nueva

Fuente: Elaboración propia

Se establece un proceso para la obtención de actualizaciones en los registros DNS, lo que implica que estos deben ser gestionados manualmente. Cualquier modificación en la configuración de DNS requerirá intervención manual por parte de los administradores de red. Aunque este enfoque puede resultar me conveniente en términos de administración, ofrece beneficios significativos en cuanto a la seguridad y estabilidad del sistema.

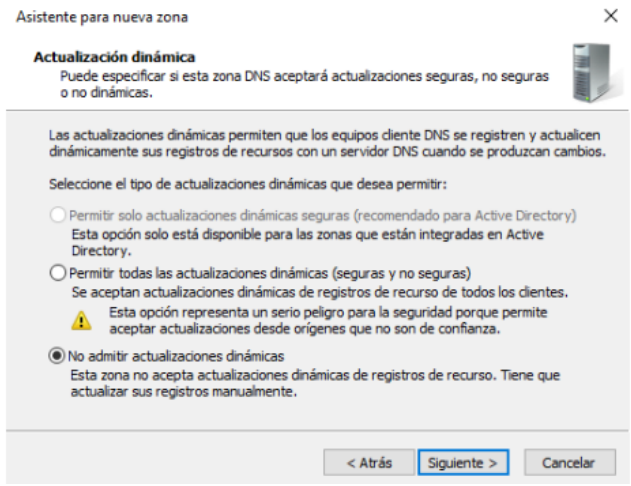


Ilustración 103. Actualización Dinámica

Fuente: Elaboración propia

Finalmente, se hace clic en “Finalizar” para crear la zona directa.

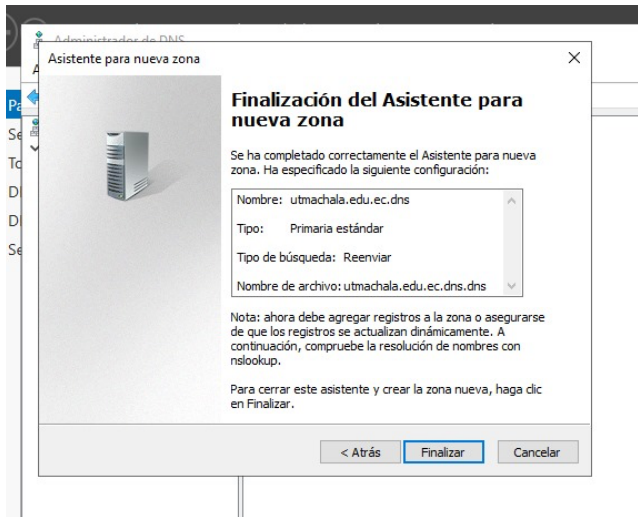


Ilustración 104. Finalización de la creación de la zona directa

Fuente: Elaboración propia

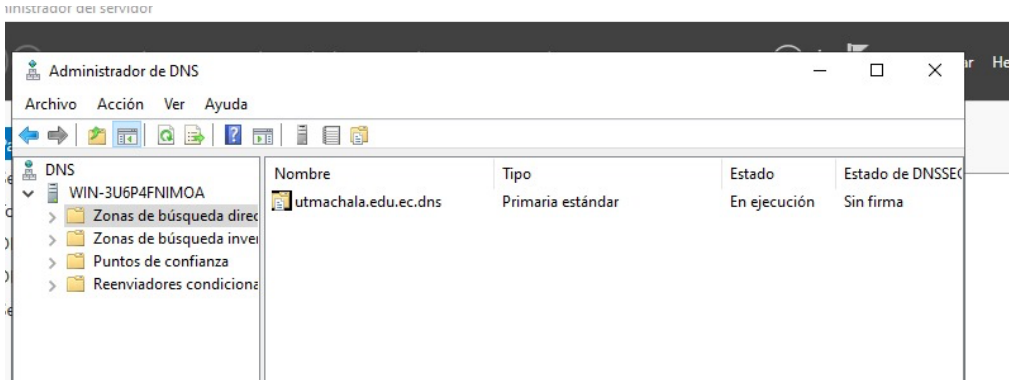


Ilustración 105. Verificación de la nueva zona

Fuente: Elaboración propia

Una vez creada la zona directa, se puede configurar un nuevo host en el servidor DNS accediendo a la configuración de la zona directa y seleccionando la opción “Host Nuevo”.

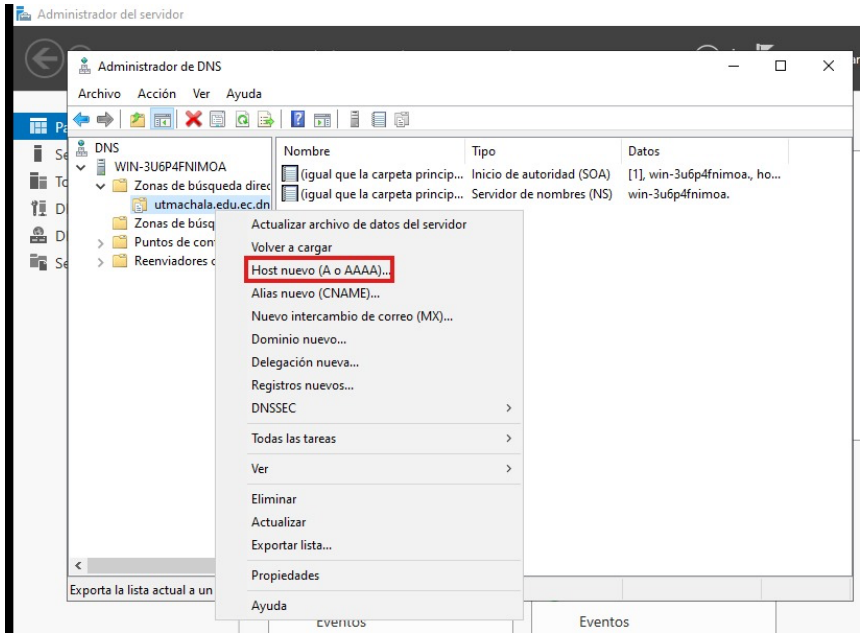


Ilustración 106. Creación del Nuevo Host

Fuente: Elaboración propia

Cuando se muestra la ventana, es necesario asignar un nombre y añadir la dirección IP del servidor, por ejemplo, 192.168.0.1. Por último, se debe activar la opción para crear el registro del puntero (PTR) correspondiente.

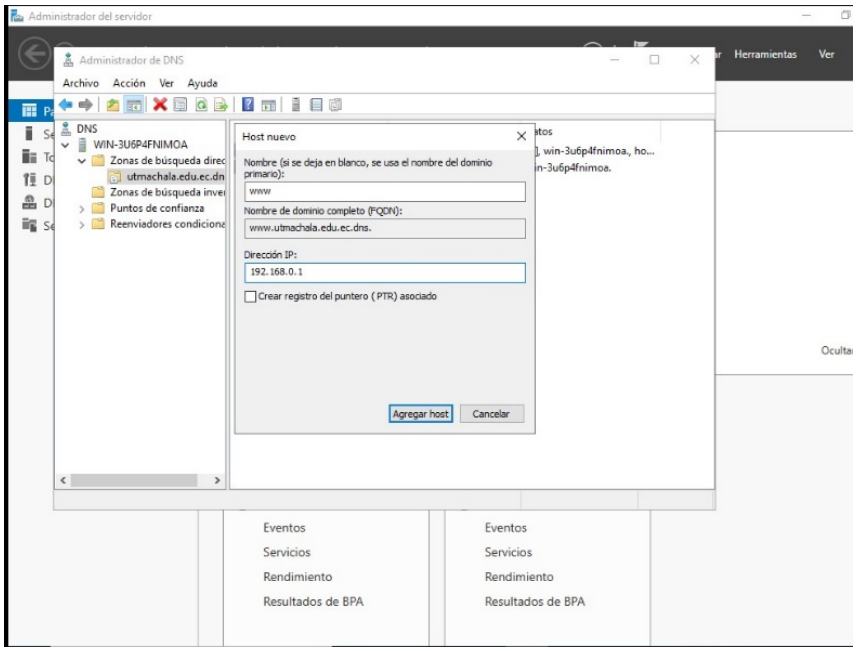


Ilustración 107. Configuración del Host

Fuente: Elaboración propia

Creación zona Inversa

Al hacer clic derecho en "Zonas de búsqueda directa", se ofrece la opción de seleccionar "Zona nueva".

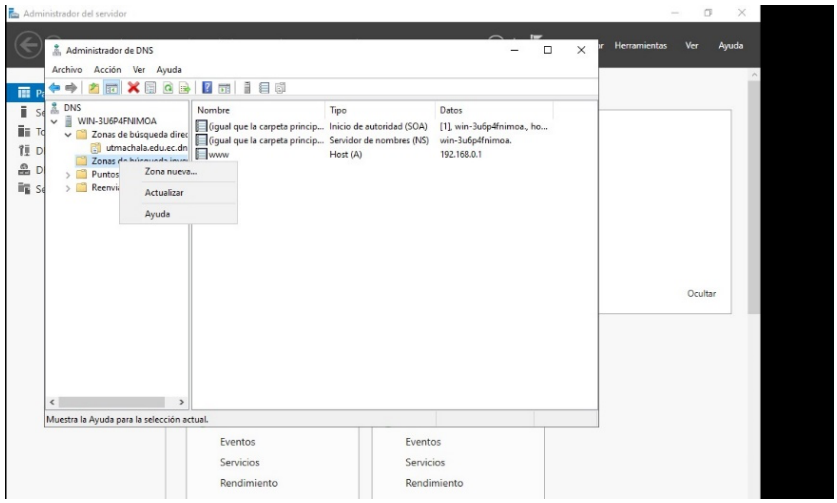


Ilustración 108. Creación Zona Inversa

Fuente: Elaboración propia

En la configuración de replicación de zonas, seleccionamos la opción de Zona Principal.

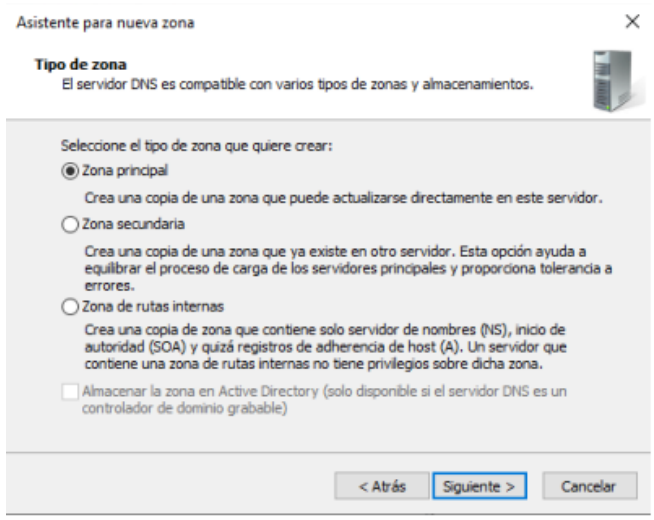


Ilustración 109. Selección de Tipo de Zona

Fuente: Elaboración propia

Se selecciona la "Zona de búsqueda inversa para IPv4" y damos clic en siguiente

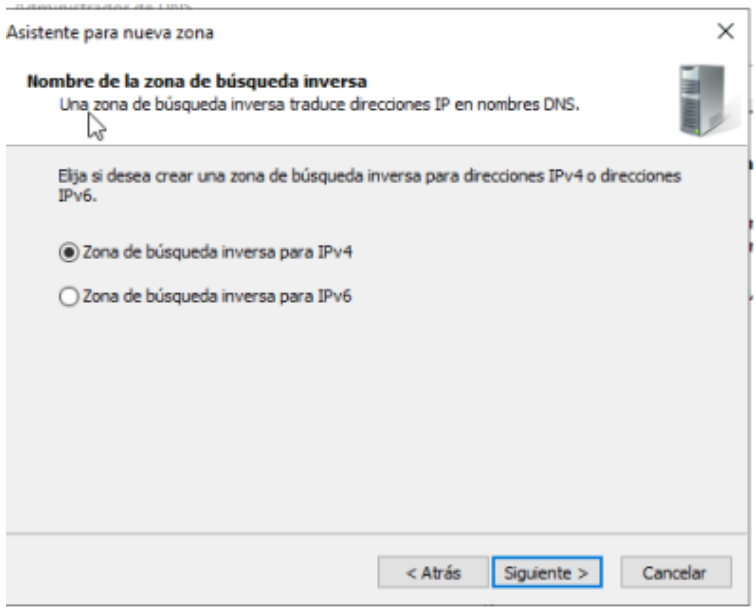


Ilustración 110. Zona de Búsqueda Inversa

Fuente: Elaboración propia

A continuación, ingresamos el Id de red y damos clic en siguiente

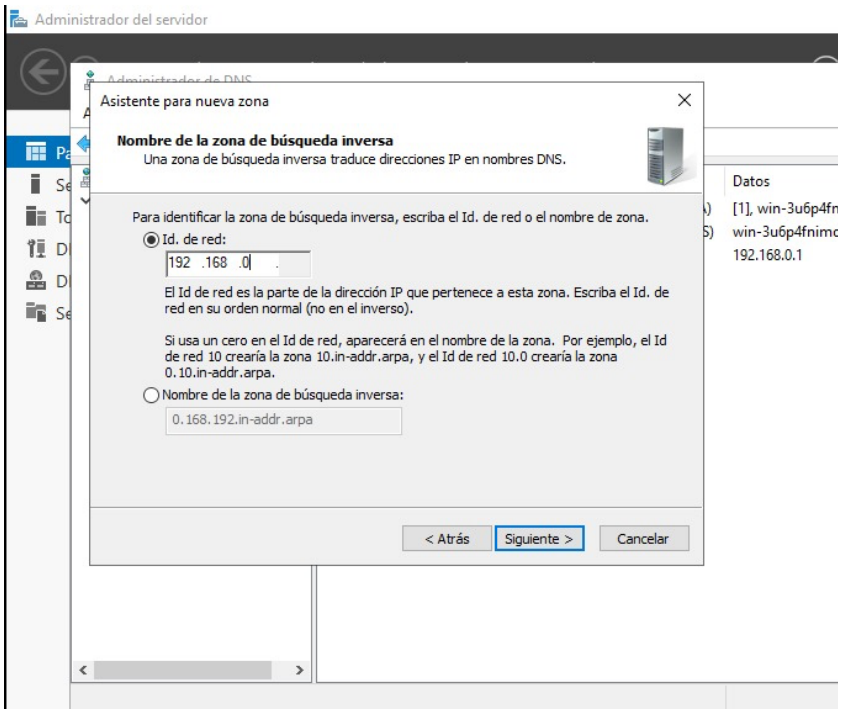


Ilustración 111. Colocación del Id de la red en la zona inversa

Fuente: Elaboración propia

El nombre del archivo se ingresa automática y solamente se da clic en siguiente

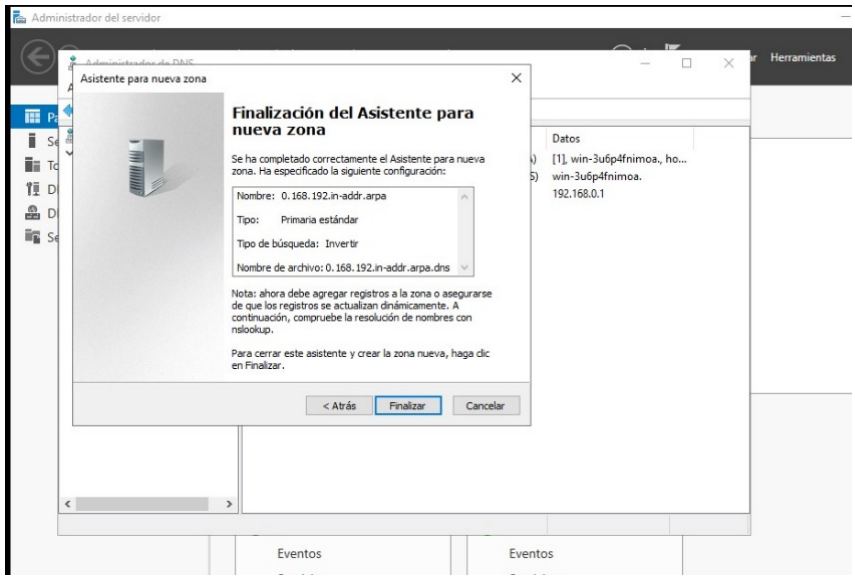


Ilustración 112. Final de la creación de la zona inversa

Fuente: Elaboración propia

Luego de crear la zona inversa, procedemos a crear un nuevo puntero (PTR) dando clic derecho en la zona inversa

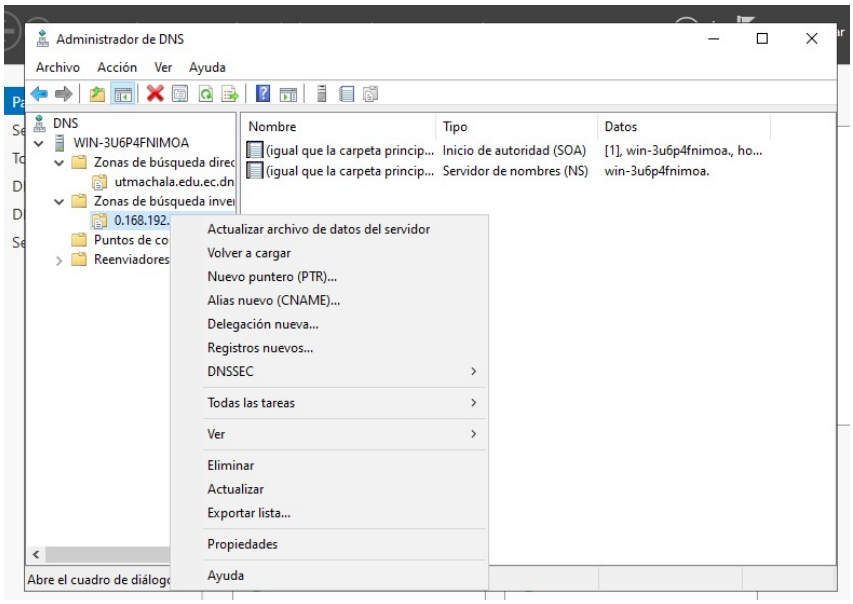


Ilustración 113. Creación del PTR

Fuente: Elaboración propia

Al ingresar la dirección IP del servidor, se debe completar el campo "Nombre de host" con el nombre del host creado en la zona directa, como, por ejemplo, "practica". Luego, se incluye el nombre de la nueva zona creada en la zona directa, en este caso, "utmachala.edu.ec". Esta acción establece la asociación entre la dirección IP del servidor y el nombre del host dentro de la estructura de la zona directa, facilitando así la identificación y resolución de nombres en el entorno DNS.

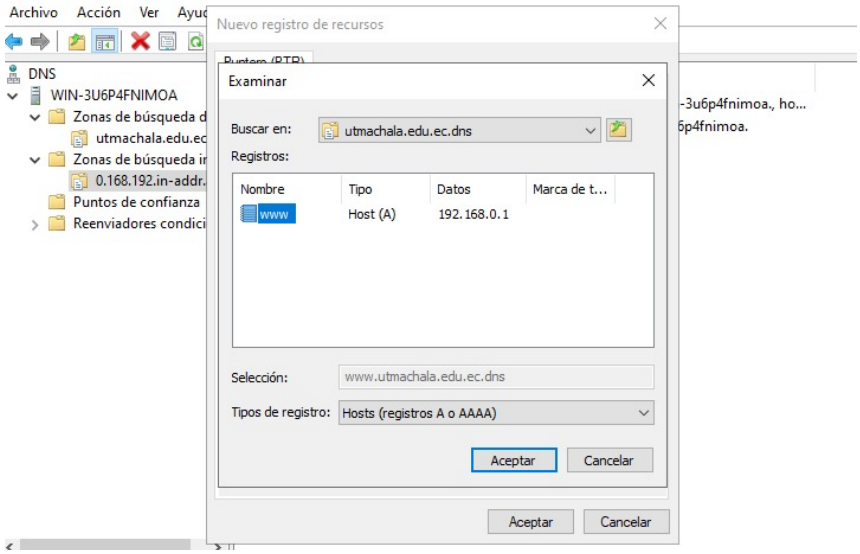


Ilustración 114. Verificación de la zona Inversa

Fuente: Elaboración propia

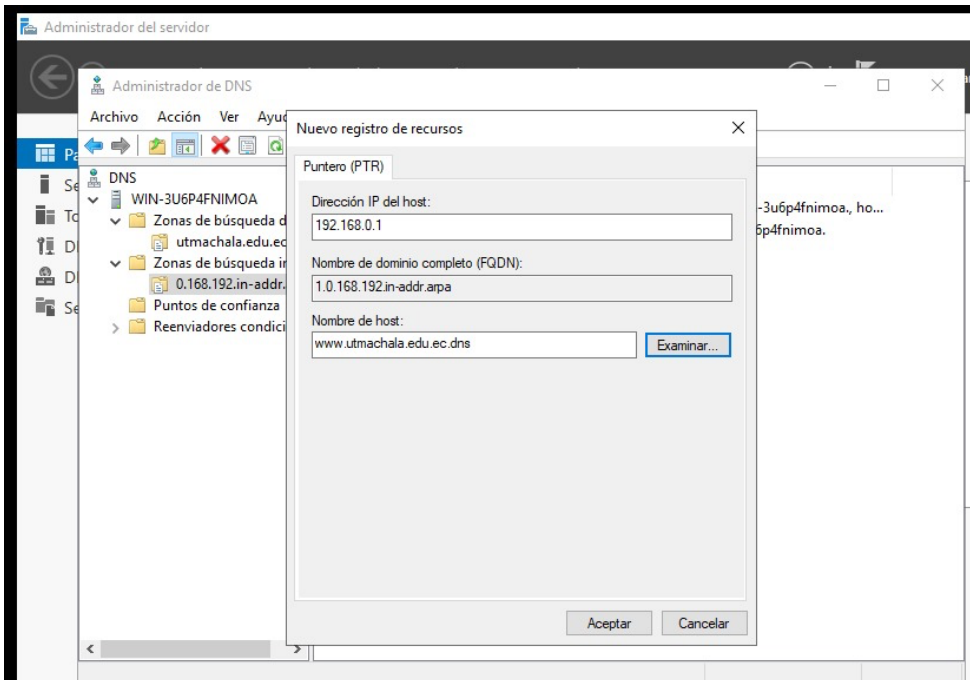


Ilustración 115. Registro del recurso

Fuente: Elaboración propia

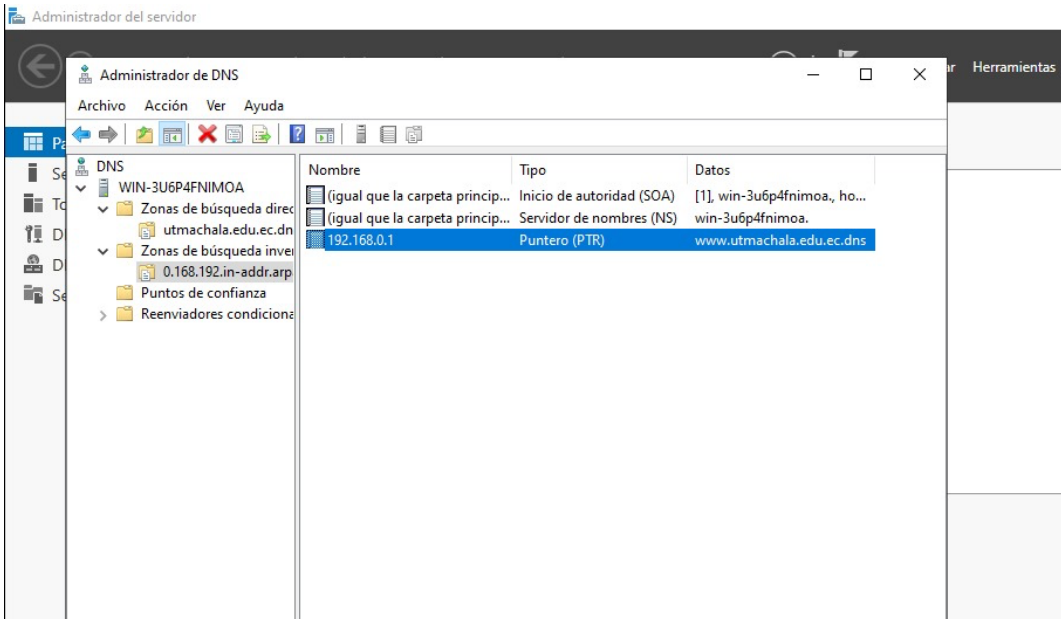


Ilustración 116. Verificación del registro

Fuente: Elaboración propia

Pruebas de Funcionamiento

Antes de proceder con las pruebas de DNS en el cliente, es necesario ingresar la dirección IP del servicio DNS en la configuración del adaptador de red, tal como se indica a continuación.

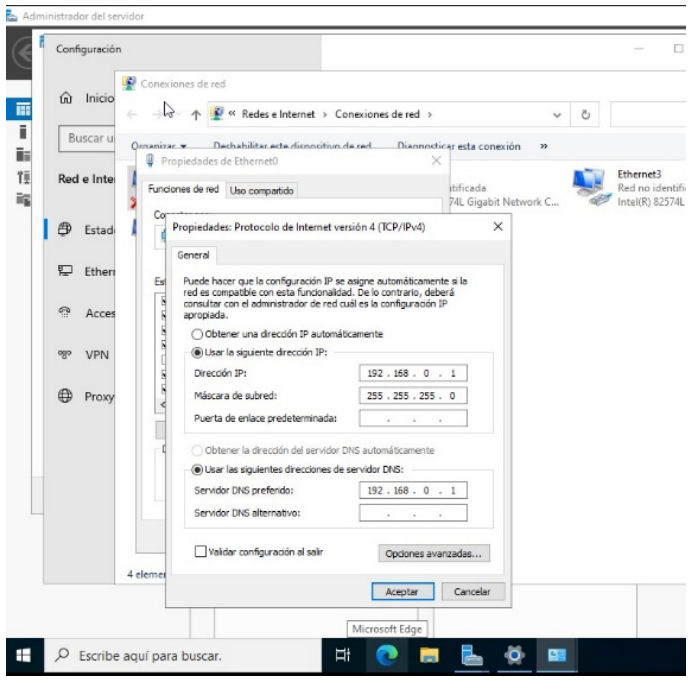


Ilustración 117. Configuración de Dirección IP en el Servidor

Fuente: Elaboración propia

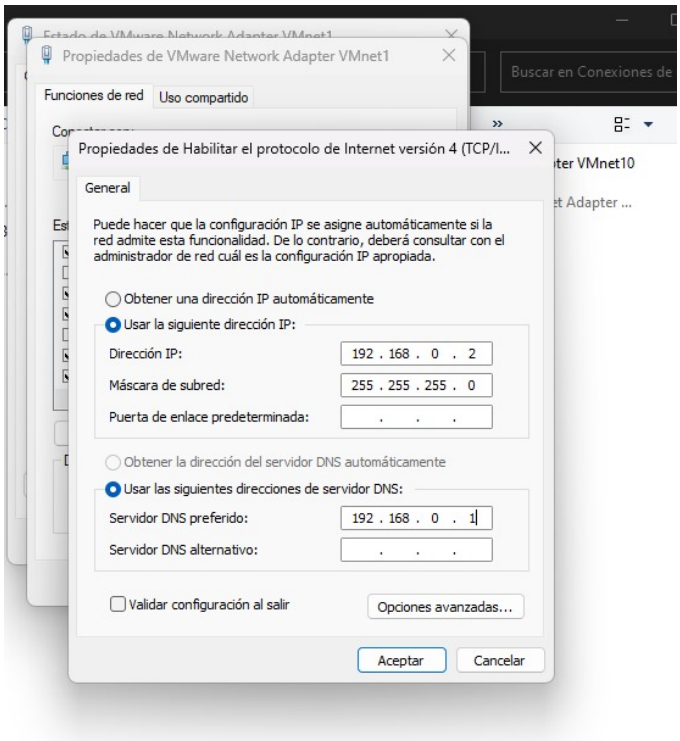


Ilustración 118. Configuración IP y DNS en el Cliente

Fuente: Elaboración propia

Para continuar, una vez agregadas las direcciones IP tanto en el cliente como en el servidor procedemos a realizar lo que son las pruebas de conexión mediante el uso del comando Ping y así verificar si la configuración se ha realizado de manera correcta.

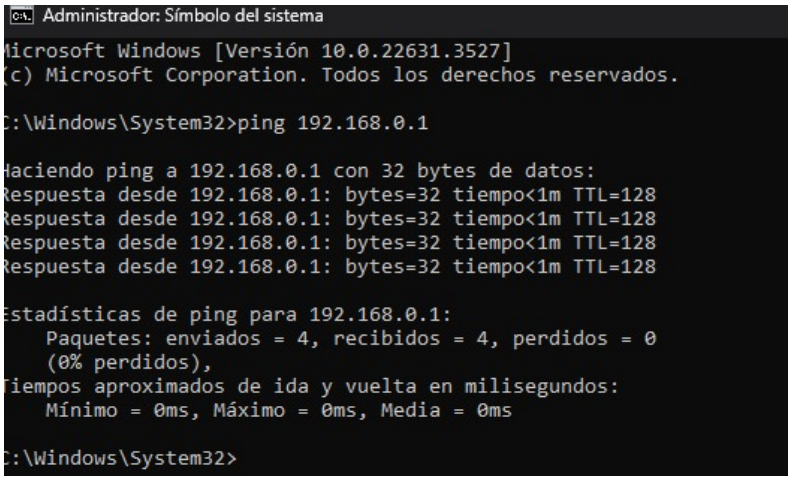


Ilustración 119. Verificación de la Conexión entre Cliente-Servidor

Fuente: Elaboración propia

Para empezar con la verificacion, utilizamos el comando Nslookup, el cual en termi generales es utilizado para poder realizar consultas en el sistema de nombres de dominios, para de esta manera poder resolver nombres de dominio a direcciones IP y viceversa.

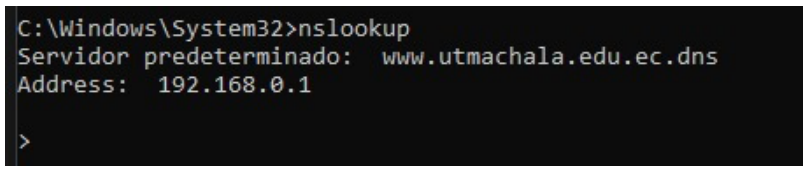


Ilustración 120. Verificación con Comando nslookup

Fuente: Elaboración Propia

El comando ping envía paquetes de datos a una dirección IP o nombre de dominio y mide el tiempo que tardan en recibir una

respuesta, en este caso enviamos paquetes al dominio www.utmachala.edu.ec y verificamos si está configurado el DNS de manera correcta.

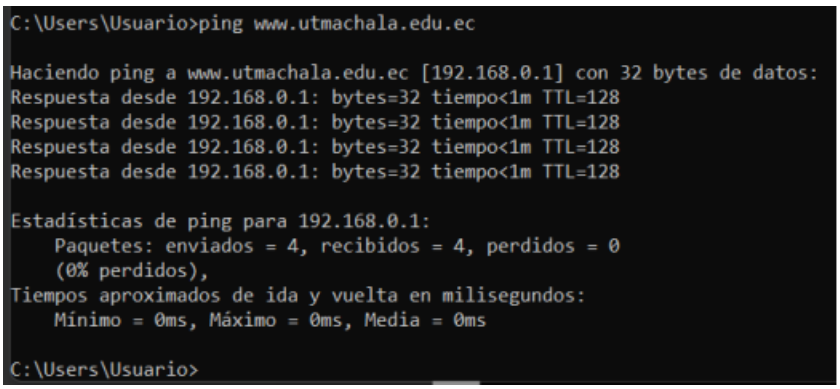


Ilustración 121. Ping a la zona directa

Fuente: Elaboración propia

A diferencia del caso anterior, cuando se quiere realizar un ping a una IP que está configurada a un dominio, utilizamos el comando PING -A y la IP que esta enlazada al dominio que se quiere alcanzar y verificar que existe una conexión.

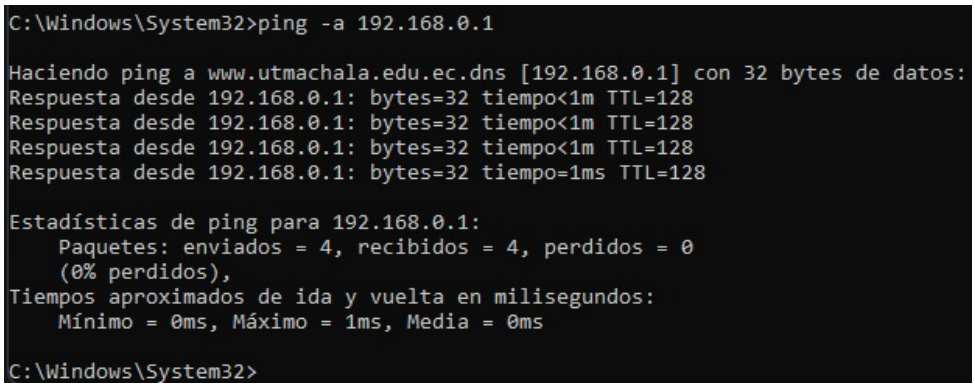


Ilustración 122. Verificación con comando Ping-a

Fuente: Elaboración propia

Por último, cuando se quiere realizar un ping a una IP en este caso inversa que está configurada a un dominio, utilizamos el comando PING -A y la dirección IP invertida que esta enlazada al dominio que se quiere alcanzar y verificar que existe una conexión.

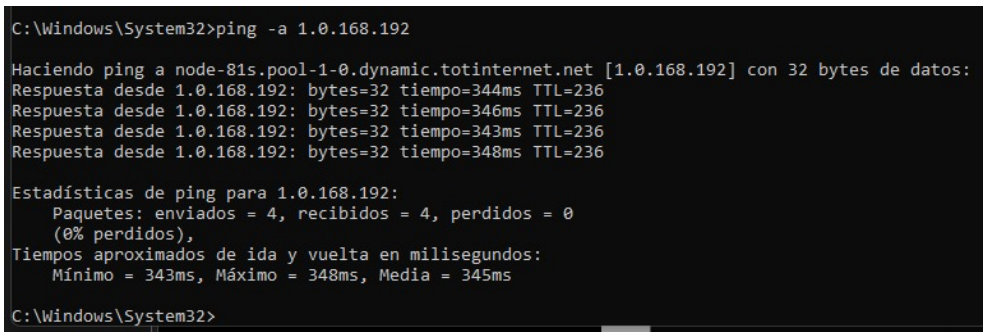


Ilustración 123. Verificación con Ping -a zona inversa

Fuente: Elaboración propia

Configuración del DNS en DHCP

El objetivo principal del servicio DHCP es lograr que los dispositivos obtengan una direccion IP automaticamente de un servidor DNS, implica la asigancion de nombres de dominio en distintas direcciones IP.

Para realizar esta configuracion primero debemos crear un nuevo ambito y configurar sus opciones. Primero, dentro del Administrador de DHCP tenemos la opcion de IPv4 e IPv6, seleccionamos IPv4 para crear un nuevo ámbito.

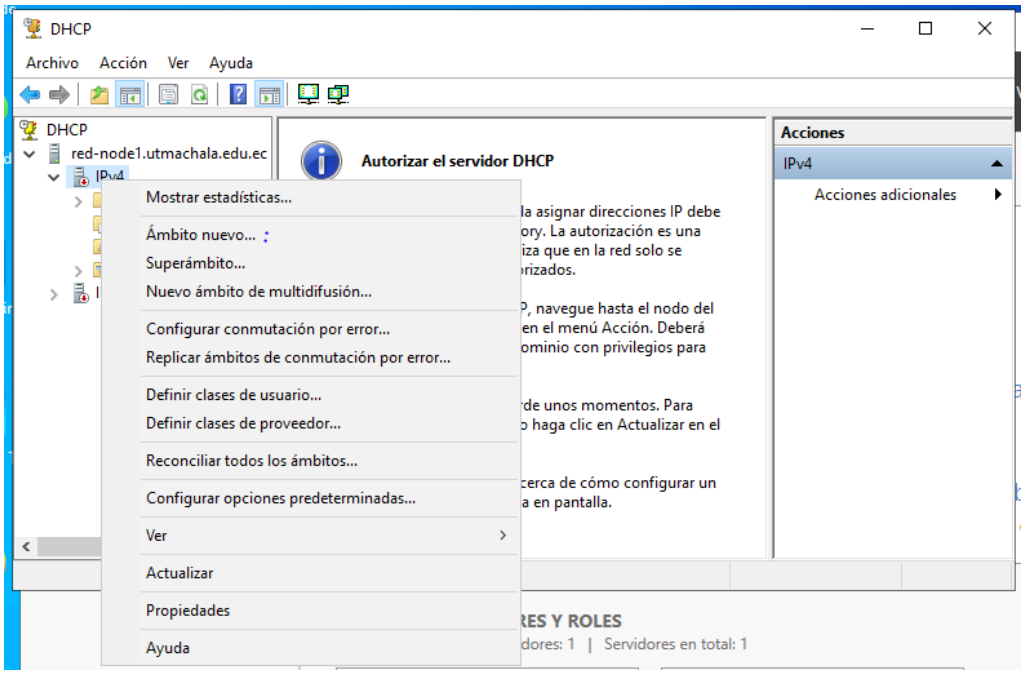


Ilustración 124. Creación de un nuevo ámbito

Fuente: Elaboración propia

Rapidamente tendremos la guia de una Asistente para la creacion de un nuevo ámbito, seguir las instrucciones correctamente, hacer clic en siguiente.

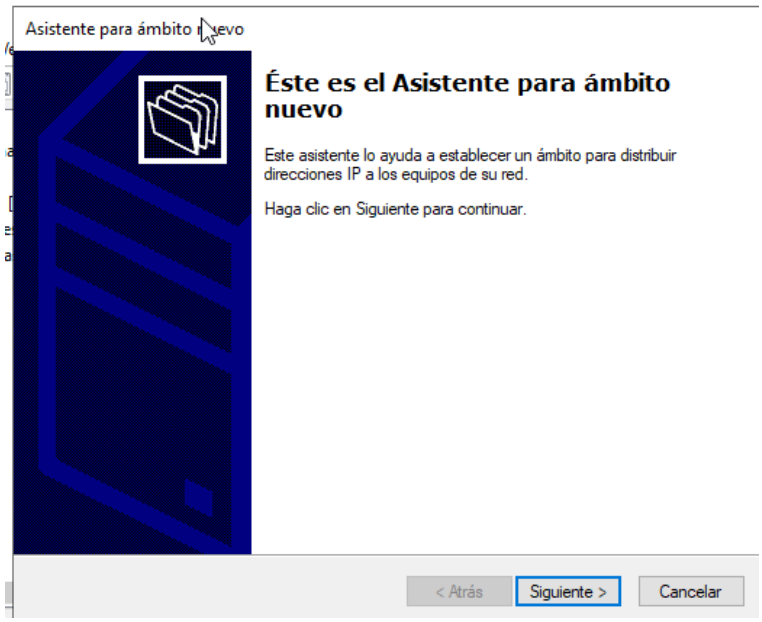


Ilustración 125. Asistente para un nuevo ámbito

Fuente: Elaboración propia

A continuacion se debe establecer un nombre y descripcion al nuevo ámbito.

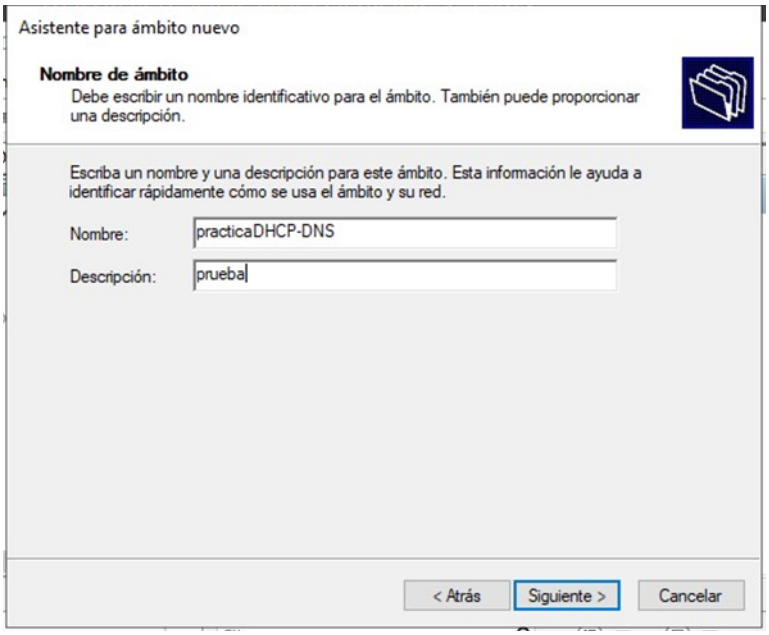


Ilustración 126. Configuración de nombre y descripción del ámbito nuevo

Fuente: Elaboración propia

En este paso se establece un intervalo de direcciones IP, para este proyecto se utilizo una direccion IP de clase C desde el rango 192.168.0.1 hasta 192.168.0.253. Recuerde tomar muy en cuenta el tipo de clase.

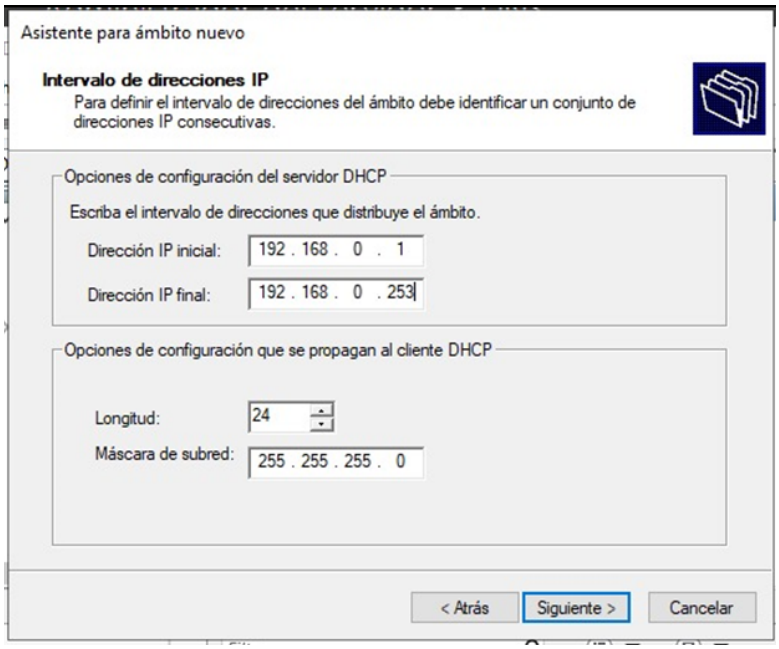


Ilustración 127. Intervalo de direcciones IP

Fuente: Elaboración propia

Podremos observar que podemos excluir ciertos rangos de direcciones IP para distintos equipos como servidores, entre otros. En esta ocasión hemos decidido excluir el rango 192.168.0.1 hasta 192.168.0.20.

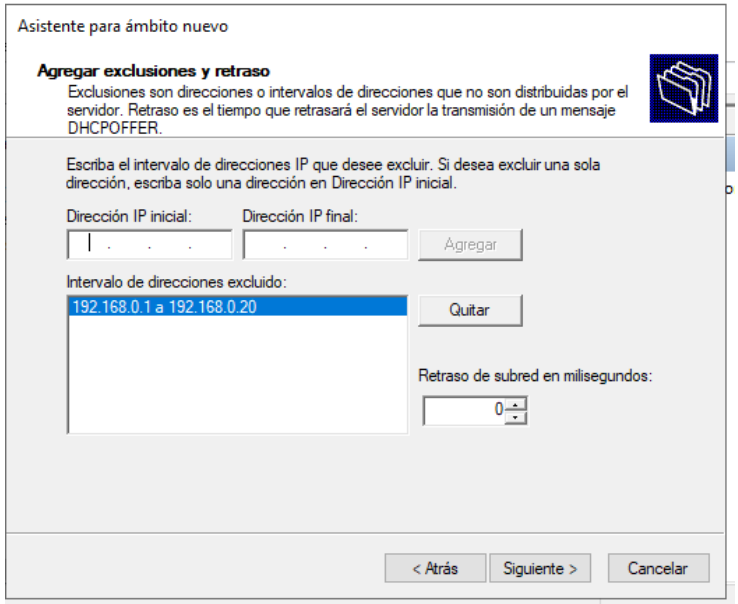


Ilustración 128. Agregar exclusiones y retraso

Fuente: Elaboración propia

Podemos asignar la duración de la concesión que especifica cuanto tiempo puede utilizar un cliente la dirección IP de este ámbito.

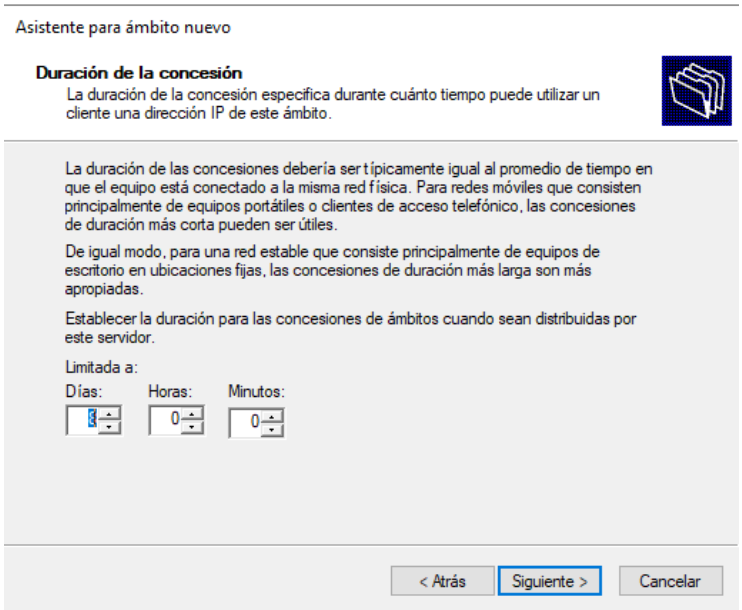


Ilustración 129. Duración de la concesión

Fuente: Elaboración propia

Para que el cliente pueda hacer uso del ámbito debemos configurar las opciones DHCP, seleccionamos "Configurar estas opciones ahora"

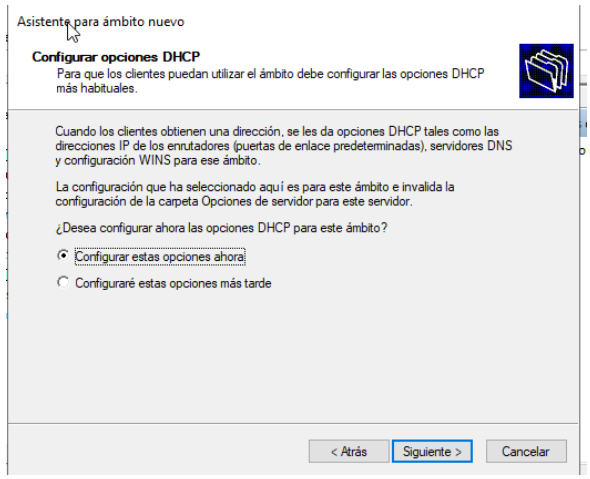


Ilustración 130. Configurar opciones DHCP

Fuente: Elaboración propia

Asignamos la puerta de enlace predeterminada que se distribuirán en el ámbito.

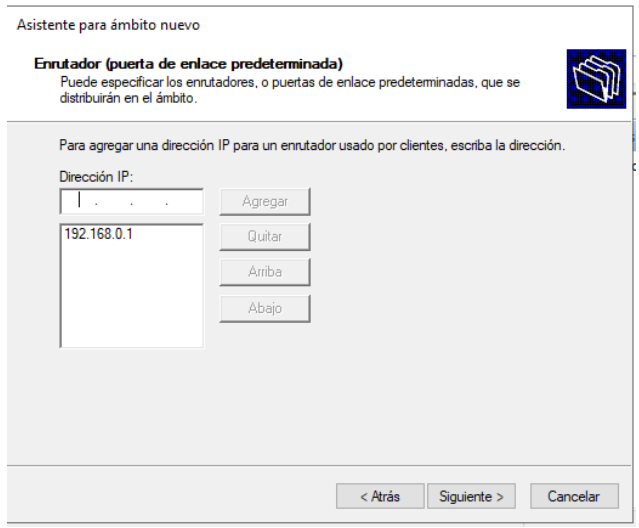


Ilustración 131. Asignación de puerta de enlace predeterminada

Fuente: Elaboración propia

Finalmente clic en "Finalizar" al asistente para culminar con la creación del ámbito nuevo.

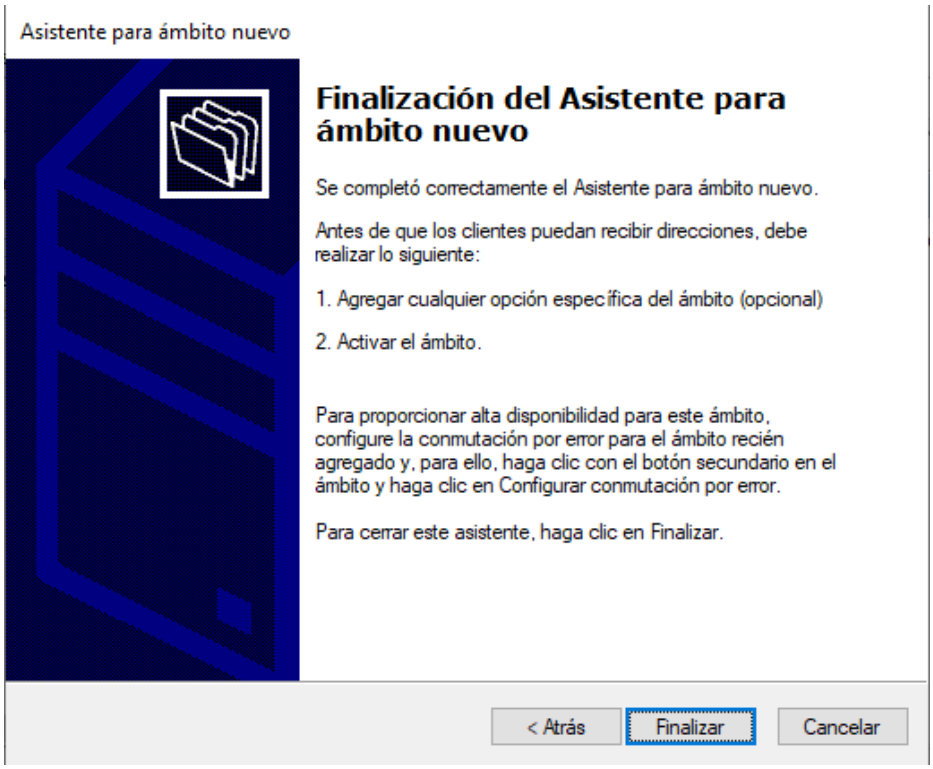


Ilustración 132. Finalización de la creación de un ámbito nuevo

Fuente: Elaboración propia

Una vez dentro del ámbito creado, haciendo clic derecho en Opciones de ámbito, seleccionamos "Configurar Opciones". Ahora nos situamos ahora dentro de las opciones de ámbito y tendremos una serie de opciones generales y avanzadas disponibles.

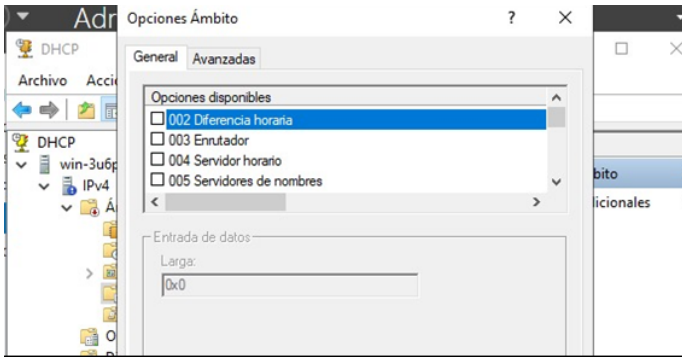


Ilustración 133. Opciones de ámbito

Fuente: Elaboración propia

Dentro de las opciones generales haremos uso de 2 opciones; 006 Servidores DNS para agregar la IP del DNS y activar la asignación automática.

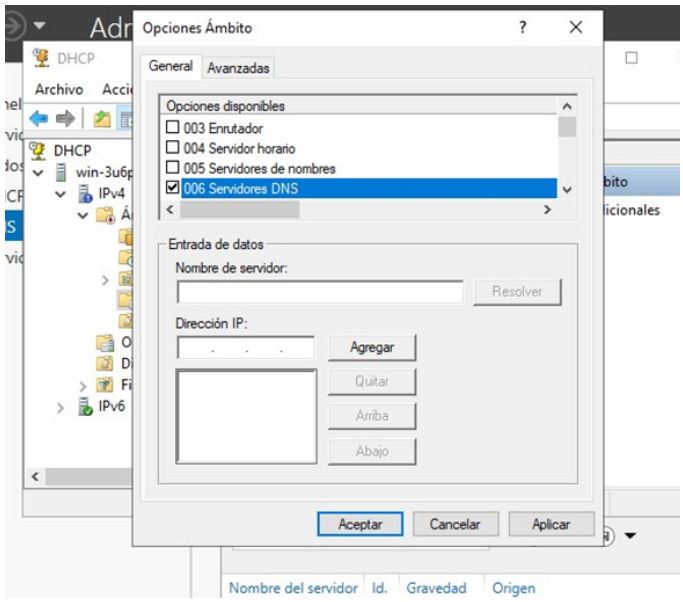


Ilustración 134. Activación Servidores DNS

Fuente: Elaboración propia

Y la opción 015 Nombre de dominio DNS para activar dicho nombre en nuestro servidor.

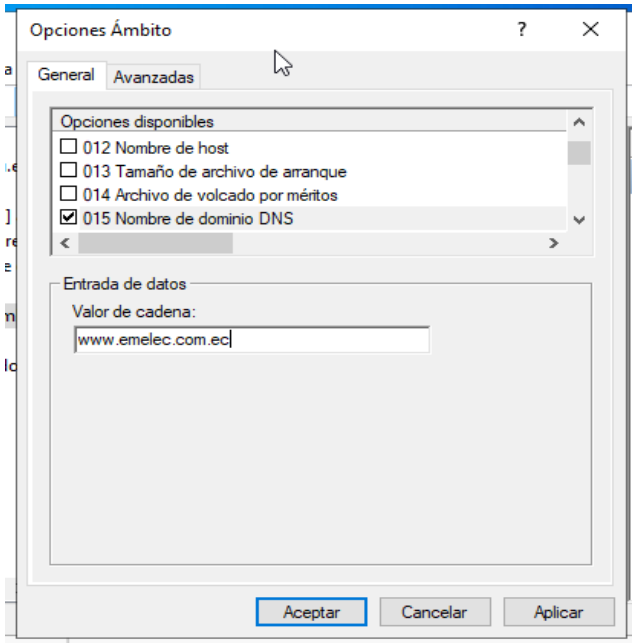


Ilustración 135. Activación de Nombre de dominio DNS

Fuente: Elaboración propia

Para comprobar el funcionamiento correcto de la configuración del DNS utilizando DHCP es necesario primero, activar la configuración automática del TCP/IP en el cliente.

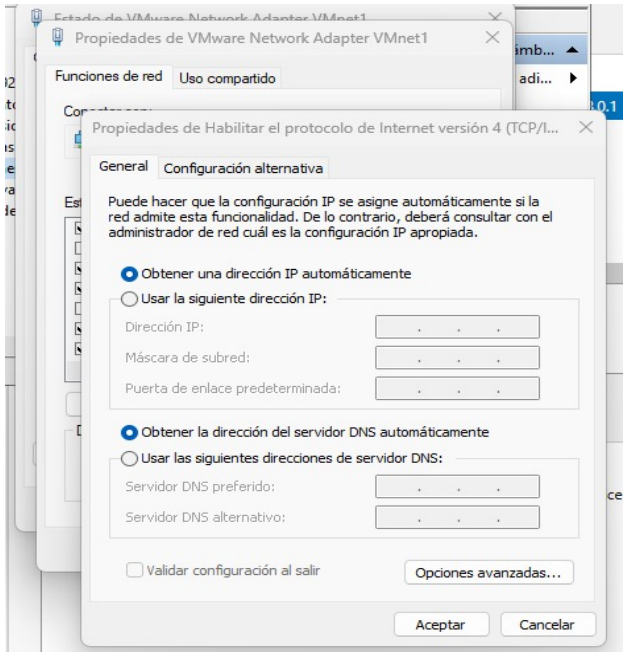


Ilustración 136. Configuración TCP/IP automática en el cliente

Fuente: Elaboración propia

Al verificar la configuracion del adaptador, se debe observar que se ha puesto en este, el sufijo DNS previamente configurado, ademas de que se ha puesto la direccion IPv4 y tambien la IP a la cual esta relacionado el dominio que se ha configurado.

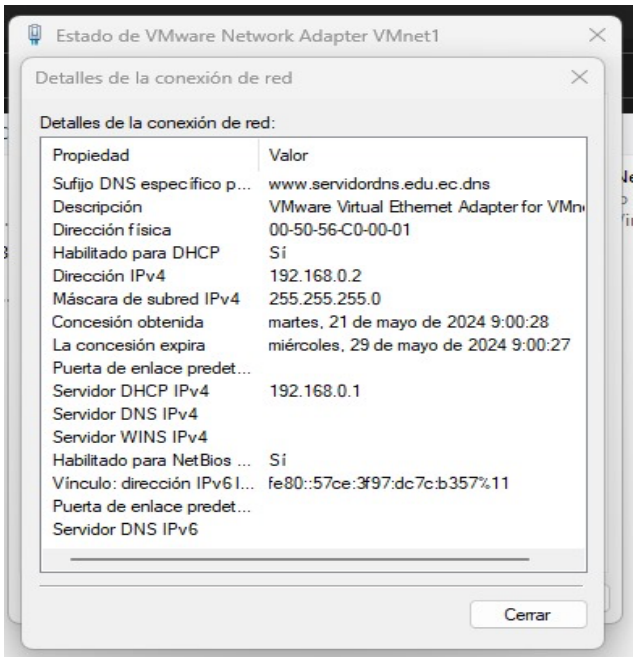


Ilustración 137. Estado del Adaptador de Red

Fuente: Elaboración propia

Otra manera que se puede encontrar para realizar esta verficacion, es mediane el uso del CMD de windows, una vez que abrimos esta pestaña, utilizamos el comando **ipconfig /all** y asi ver todos los datos de los adaptadores, pero en este caso se debe verificar el adaptador conectado con el servidor.

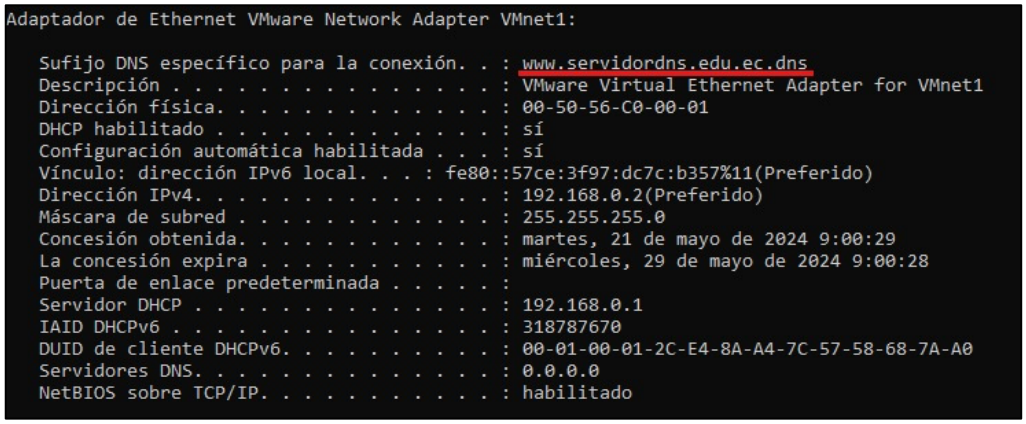


Ilustración 138. Verificación con IPConfig/all

Fuente: Elaboración propia

Otra manera de verificar, es mediante el uso del comando Nslookup, el cual en termi generales es utilizado para poder realizar consultas en el sistema de nombres de dominios, por lo que en este caso lo usamos con el servicio DNS y DHCP configurado, y verifocar si esta configuración es correcto.

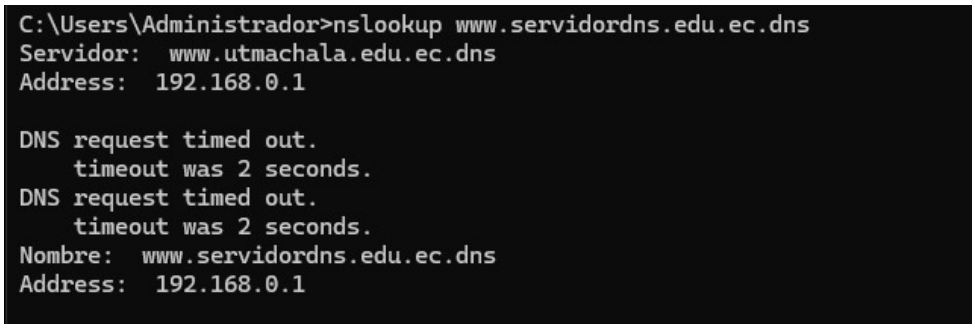


Ilustración 139. Utilización de Nslookup

Fuente: Elaboración propia

Servidores Web

Un servidor web es un equipo informático de alto rendimiento cuya función principal es ofrecer el servicio de enviar la información solicitada por sus clientes (como ordenadores, dispositivos móviles, impresoras o usuarios). Estos servidores forman parte de una infraestructura más amplia y se especializan en alojar, mediante servicios de web hosting, todos los elementos que conforman una página web (como imágenes, textos o videos). Luego, distribuyen estos contenidos a los usuarios a través de los navegadores utilizando el protocolo HTTP. (Hipertext Transfer Protocol) (Rock Content, 2024).

Funcionamiento de un servidor web

La comunicación entre un servidor y sus clientes se basa en el Protocolo de Transferencia de Hipertexto (HTTP) o en su variante codificada, el Protocolo de Transferencia de Hipertexto Seguro (HTTPS). Para comprender su funcionamiento, es esencial saber que el servidor web permanece constantemente a la espera de solicitudes de información. Es importante destacar que cada computadora, smartphone o tablet posee una dirección IP única e irrepetible que la distingue de otros dispositivos en la red. Esta identificación permite al servidor web enviar la información exacta que el usuario está esperando. Para que el servidor web pueda desempeñar su función, es necesario que reciba una solicitud por parte de un navegador. En términos prácticos, esto implica que se envía una petición desde una dirección IP hacia la dirección IP del servidor que aloja los archivos del sitio web en cuestión.

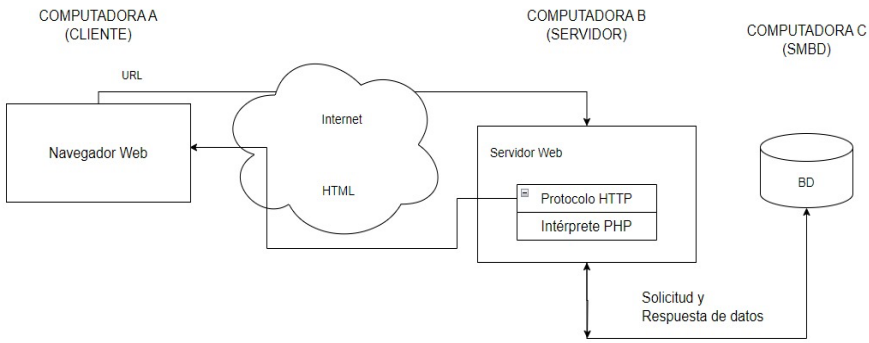


Ilustración 140. Funcionamiento de servidor web

Fuente: (Instituto Consorcio Clavijero, 2025.)

Sitios Web

Un sitio web es un conjunto de páginas web enlazadas entre sí, alojadas en un servidor y accesibles a través de internet y de un navegador, que comparten una misma dirección única o URL. Este conjunto de páginas se utiliza para mostrar información, compartir contenido, vender productos o servicios, y conectar con otros usuarios (Instituto Consorcio Clavijero, 2025).

Protocolo http

El Protocolo de Transferencia de Hipertexto (HTTP) es fundamental para la World Wide Web (web), ya que permite la comunicación entre un navegador y un servidor web. Se basa en un modelo de comunicación mediante solicitudes y respuestas entre un cliente y un servidor. Por defecto, HTTP emplea el puerto TCP 80 en el servidor y está especificado en los documentos RFC 1945, RFC 2616 y RFC 2774 (Ruiz & Ulloa, 2013).

Protocolo https

El protocolo de transferencia de hipertexto seguro (HTTPS) es la versión segura de HTTP, que emplea SSL/TLS para establecer un canal cifrado a través del cual se transmite la información.

El HTTPS está encriptado para aumentar la seguridad de las transferencias de datos. Esto garantiza que datos sensibles, como contraseñas, no se envíen en texto claro. Si un tercero intercepta la comunicación, solo podrá acceder a datos encriptados que no podrá interpretar. Este protocolo utiliza por defecto el puerto TCP 443 (Ruiz & Ulloa, 2013), (Cloudflare, 2025).

SSL	TLS
Es un protocolo de seguridad estándar que proporciona una capa de cifrado y autenticación para garantizar la seguridad de las comunicaciones en línea. Cifrado de datos: SSL/TLS utiliza algoritmos de cifrado para codificar los datos durante la transferencia, lo que impide que alguien pueda acceder a la información en tránsito.	Reemplazado posteriormente por TLS, pero el término "SSL" a menudo se usa de manera genérica para referirse a ambos protocolos. Función principal: SSL/TLS se utiliza para proteger la integridad y confidencialidad de los datos transmitidos a través de Internet entre un cliente (como un navegador web) y un servidor.

Ilustración 141. SSL

Fuente: Elaboración propia

Certificados https (SSL)

Según Kaspersky (2025), un certificado SSL es un certificado digital que autentica la identidad de un sitio web y habilita una conexión cifrada. La sigla SSL significa Secure Sockets Layer (Capa de sockets seguros), un protocolo de seguridad que crea un enlace cifrado entre un servidor web y un navegador web. El certificado SSL mantiene seguras las conexiones a Internet y evita que se lea o modifique la información transferida entre dos sistemas. Un ícono de candado junto a la URL en la barra de direcciones, significa que hay un certificado SSL que protege el sitio web

Los certificados SSL funcionan de la siguiente manera:

1. Un navegador o servidor intenta conectarse a un sitio web mediante certificados SSL.

2. El navegador o servidor solicita que el servidor web se identifique.

3. El servidor responde enviando una copia de su certificado SSL.

4. El navegador o servidor verifica la validez y confianza del certificado; si lo considera seguro, procede a notificarlo al servidor.

5. Posteriormente, el servidor responde con una confirmación firmada digitalmente, lo que da inicio a una sesión protegida mediante SSL

6. Finalmente, el intercambio de datos cifrados ocurre entre ambas partes: el navegador o servidor y el servidor web.

Internet Information Services (IIS)

Internet Informatión Services, es un servidor web creado por Microsoft, diseñado para facilitar el hospedaje y la gestión de sitios web en plataformas que utilizan Windows Server. Se ha consolidado como una de las soluciones más reconocidas y empleadas en el ámbito del desarrollo web. Proporciona una plataforma robusta y escalable para la entrega de contenido web, de modo que le permite a los desarrolladores y administradores de sistemas gestionar y ejecutar aplicaciones y sitios web de manera eficiente (Casero, 2024).

Arquitectura de Internet Information Services

Según Casero (2024), IIS posee una arquitectura modular y adaptable compuesta por diversos elementos que actúan de manera coordinada para ofrecer servicios web eficaces. Entre sus principales componentes se destacan los siguientes:

- Servidor Web
- Módulos de procesamiento
- Herramientas de configuración y administración

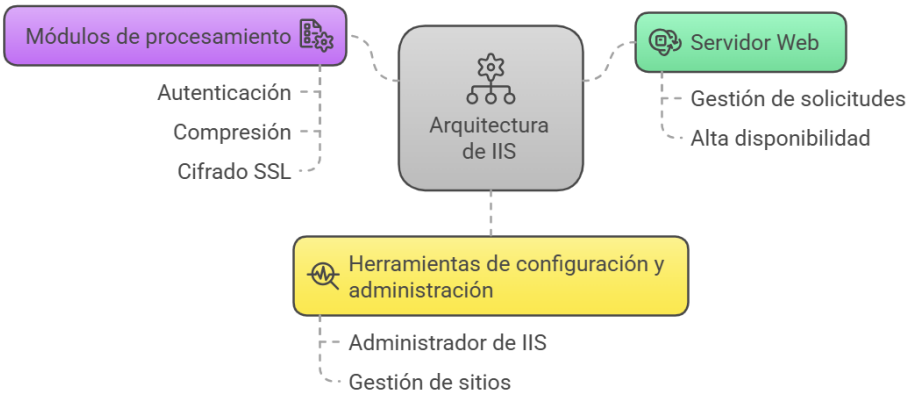


Ilustración 142. SSL

Fuente: Elaboración propia

Caso práctico

Diagrama de Red y Configuración Previa

Antes de proceder con la instalación del servidor IIS, es fundamental tener una comprensión clara de la configuración de la red y los equipos involucrados en el proceso. El siguiente gráfico ilustra la disposición de los elementos clave dentro de la red, destacando las direcciones IP asignadas a cada uno de los dispositivos, así como el flujo de comunicación entre los clientes y el servidor IIS a través de Internet.

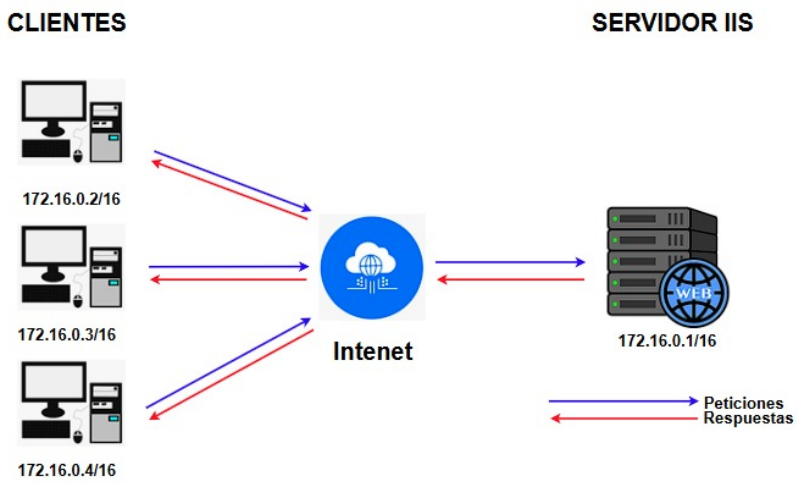


Ilustración 143. Administración del servidor

Fuente: Elaboración propia

Instalación del servicio de IIS

Navegamos al panel de control llamado "Administración del Servidor" para acceder a las herramientas y configuraciones administrativas del servidor.

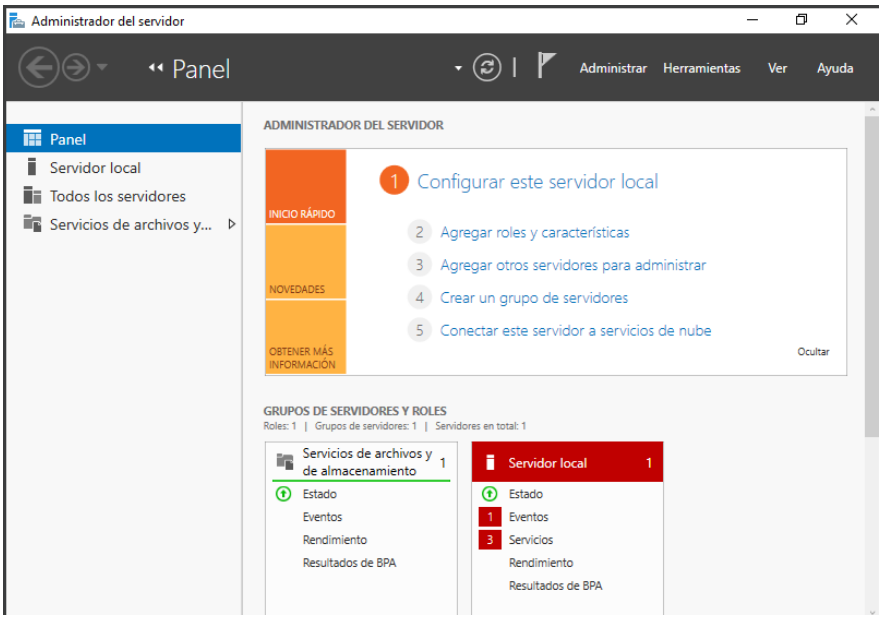


Ilustración 144. Administración del servidor

Fuente: Elaboración propia

Hacemos clic en la opción "Agregar roles y características" para iniciar el asistente que permite la instalación de nuevas funcionalidades y servicios en el servidor.

Ilustración 145. Roles y características

Fuente: Elaboración propia

Al aparecer esta pantalla, procedemos a hacer clic en el botón “Siguiente” para continuar con el proceso de configuración

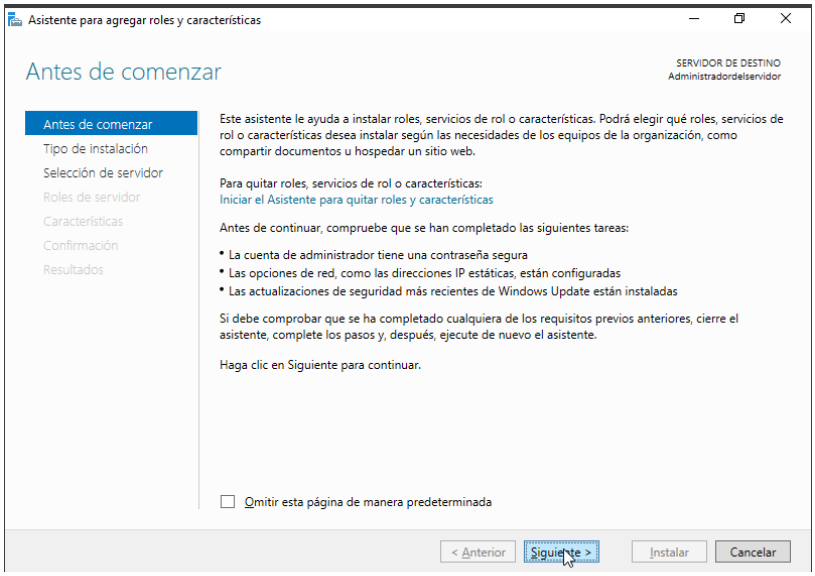


Ilustración 146. Sección antes de comenzar

Fuente: Elaboración propia

Seleccione la opción “Instalación basada en características o roles” y haga clic en “Siguiente” para continuar con el proceso.

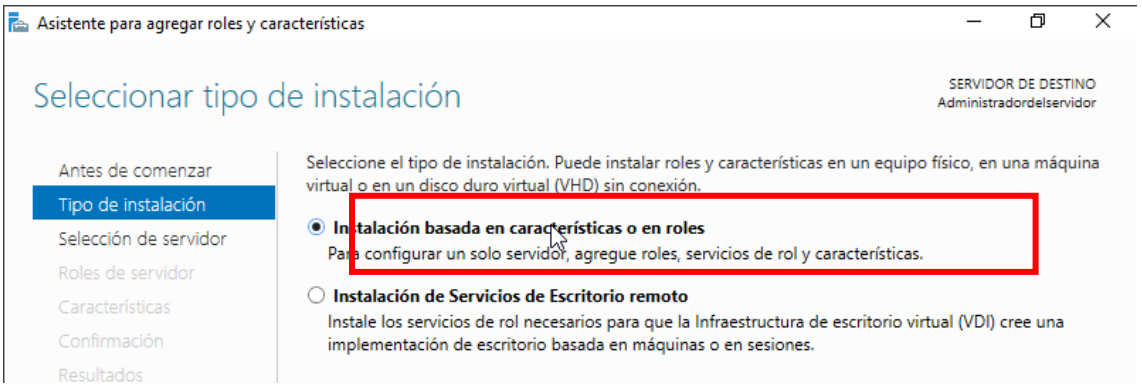


Ilustración 147. Roles y características

Fuente: Elaboración propia

Seleccionamos el servidor de destino, por lo generale es el nombre del equipo y damos siguiente.

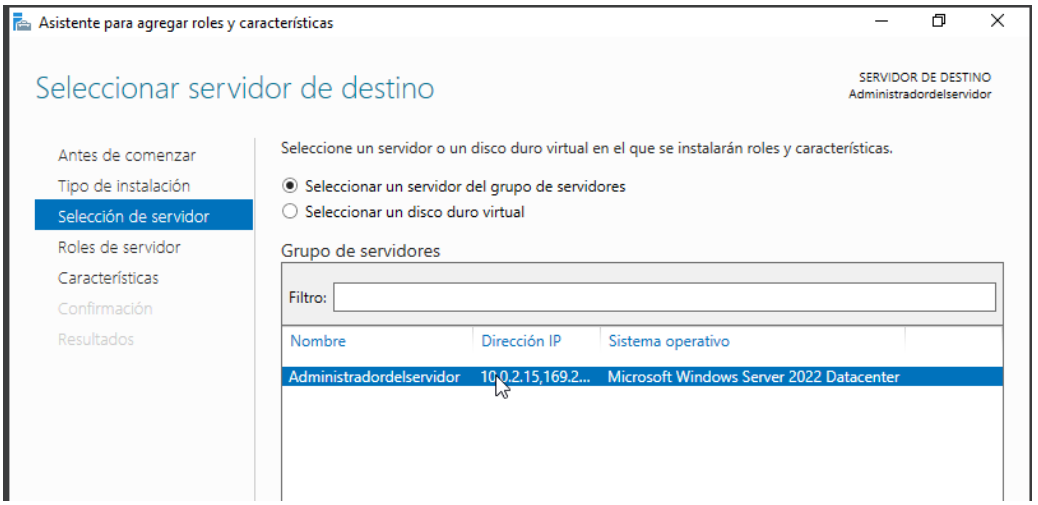


Ilustración 148. Selección de servidor

Fuente: Elaboración propia

En la sección de Roles de Servidor, se selecciona la opción "Servidor Web (IIS)" para habilitar las funciones relacionadas con el servidor web.

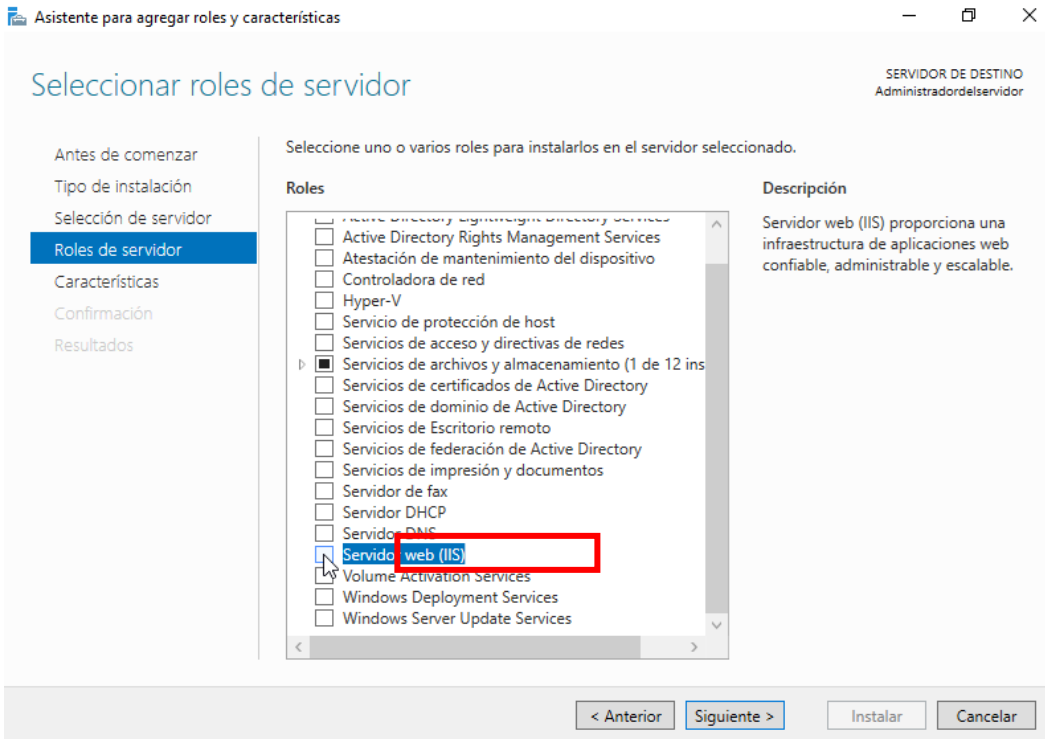


Ilustración 149. Servidor web

Fuente: Elaboración propia

Se muestra la siguiente ventana en la cual se debe hacer clic en "Agregar Característica" y luego en "Siguiente" para continuar con el proceso.

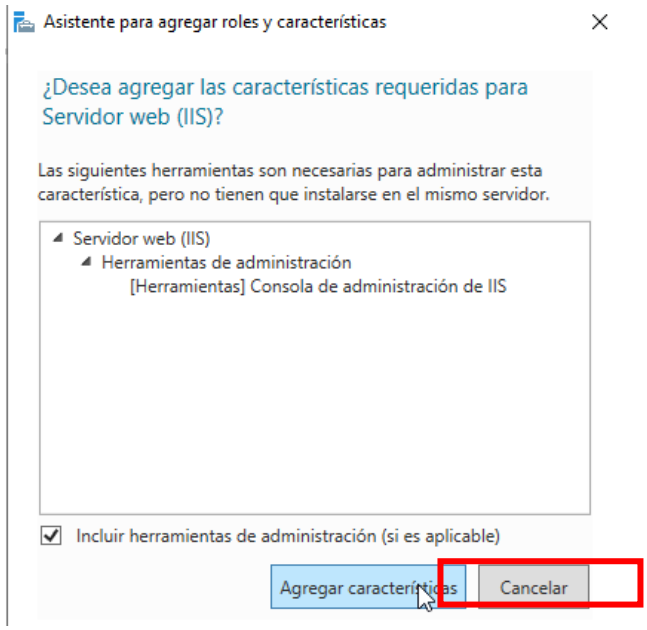


Ilustración 150. Agregar características

Fuente: Elaboración propia

Se mostrará un resumen del Rol de Instalación, en el cual se debe hacer clic en "Siguiente" para proceder.

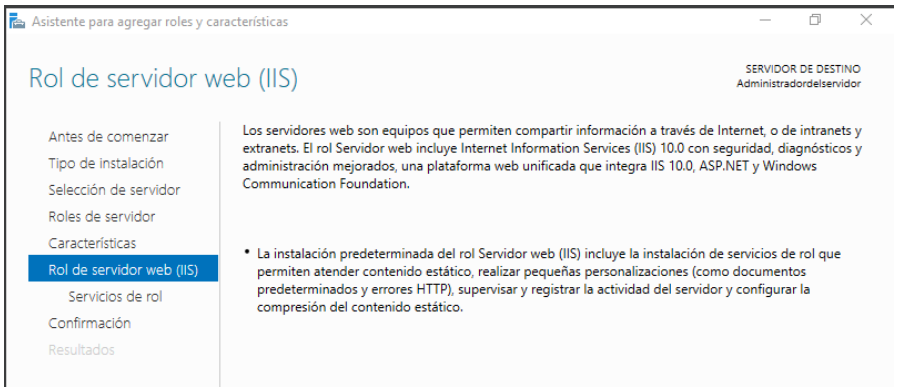


Ilustración 151. Rol del servidor

Fuente: Elaboración propia

En los “Servicios de Rol” no modificamos nada y damos a siguiente.

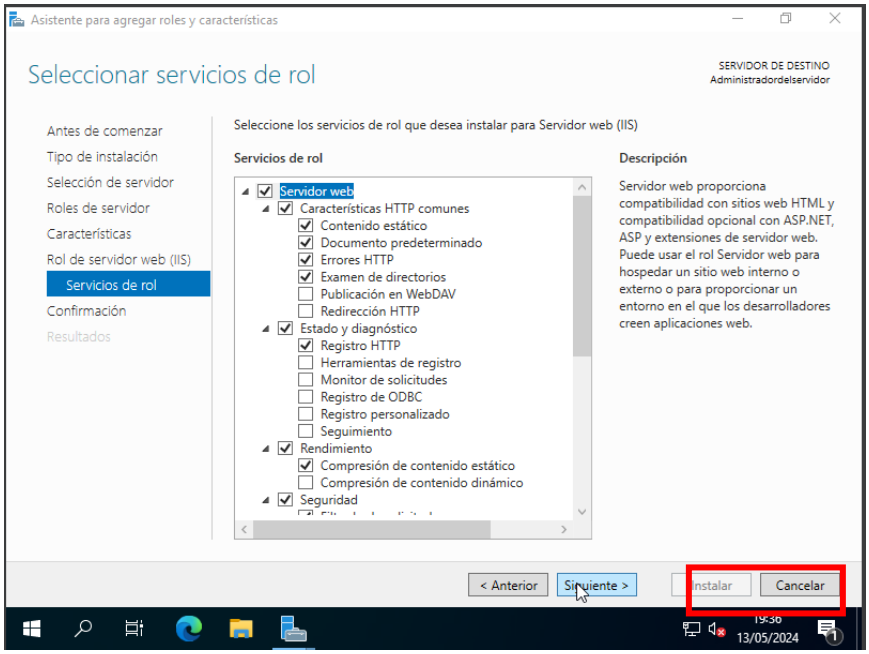


Ilustración 152. Selección de servicios de rol

Fuente: Elaboración propia

Se mostrará un resumen de instalación, en el cual simplemente se debe hacer clic en “Instalar” para iniciar el proceso.

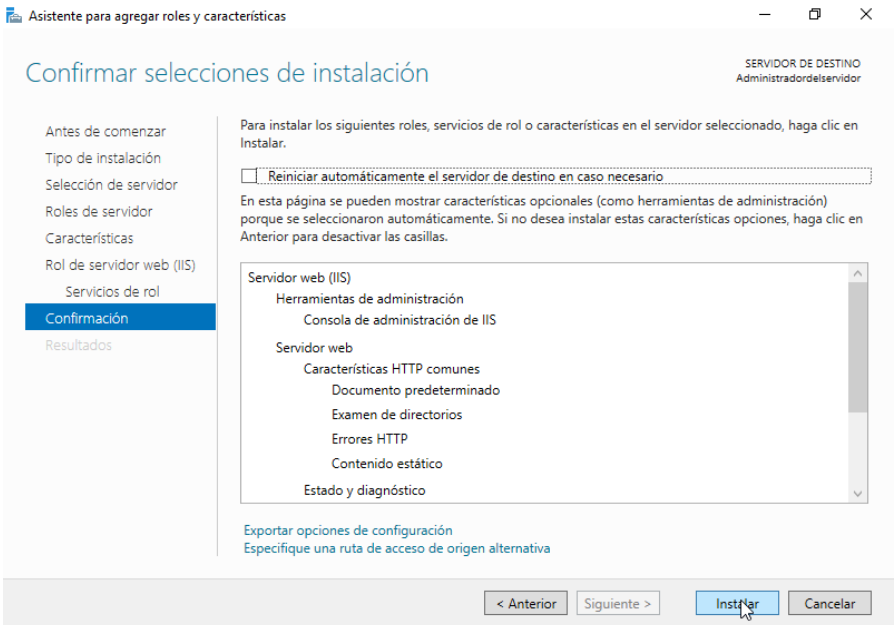


Ilustración 153. Confirmación de instalación

Fuente: Elaboración propia

Para comprobar la instalación, se debe ir a la sección de "Herramientas" y verificar que aparezca el paquete de instalación.

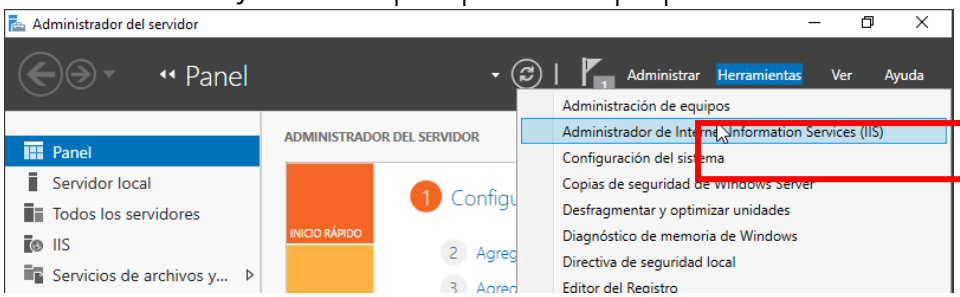


Ilustración 154. Herramientas instaladas

Fuente: Elaboración propia

Otra manera de comprobar la instalación es acceder al cliente, introducir la dirección IP en el navegador y verificar que se visualice la página por defecto.

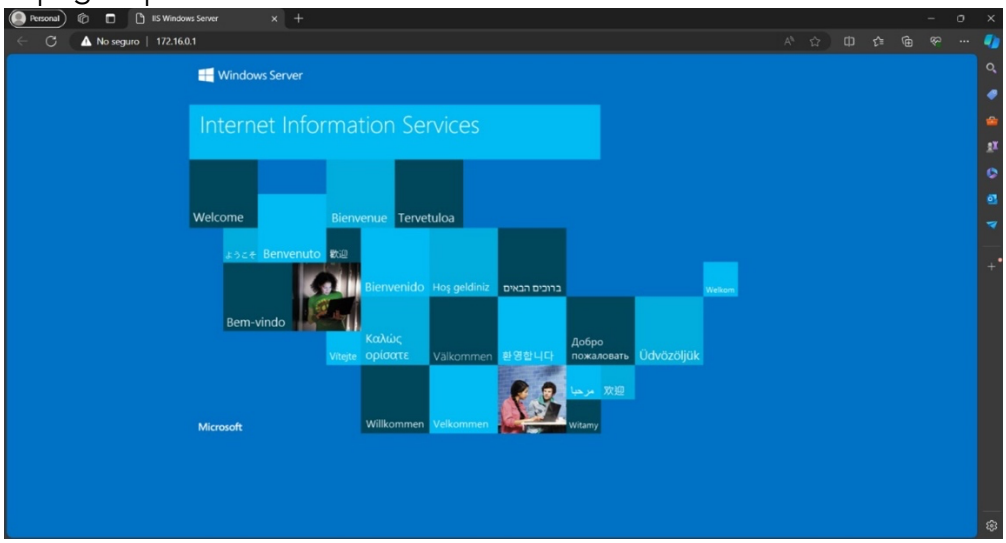


Ilustración 155. IP en el navegador

Fuente: Elaboración propia

Implementación del Sitio Web utilizando HTTP en IIS.

Ir a la siguiente ruta **C:\inetpub\wwwroot.**

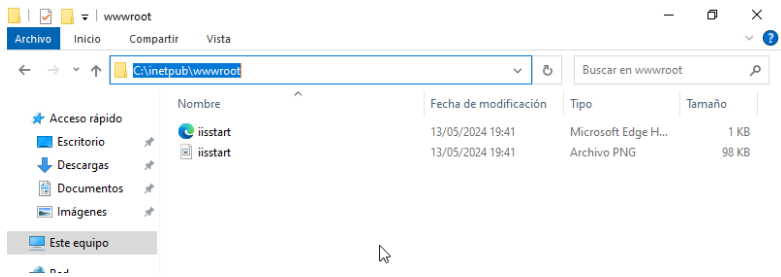


Ilustración 156. Ruta Root

Fuente: Elaboración propia

Creamos una carpeta, en este caso le colocamos de nombre “utmach”

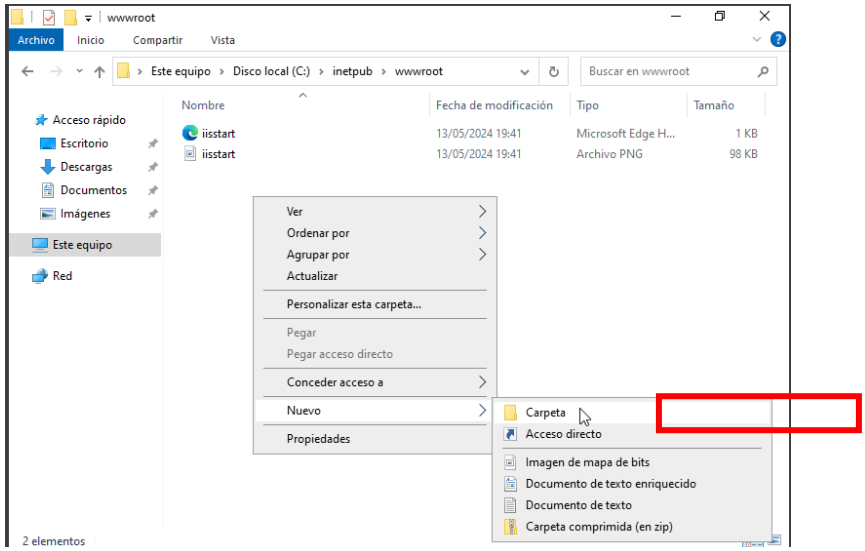


Ilustración 157. Crear carpeta para página

Fuente: Elaboración propia

Agregar un archivo con código HTML para el sitio web.

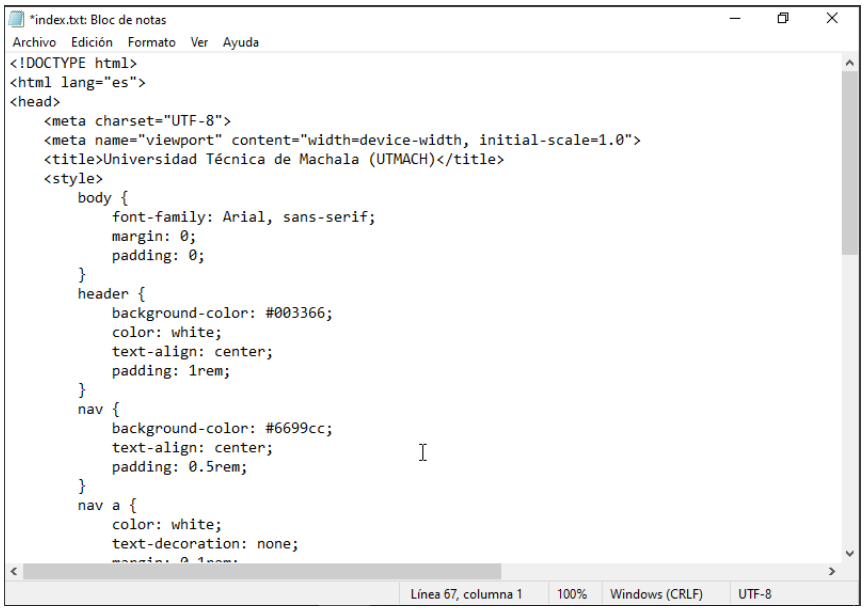


Ilustración 158. HTML de la página

Fuente: Elaboración propia

Agregar el sitio web al Servicio de IIS.

Diríjase a "Herramientas" y haga clic en "Administrador de Internet Information Services (IIS)".

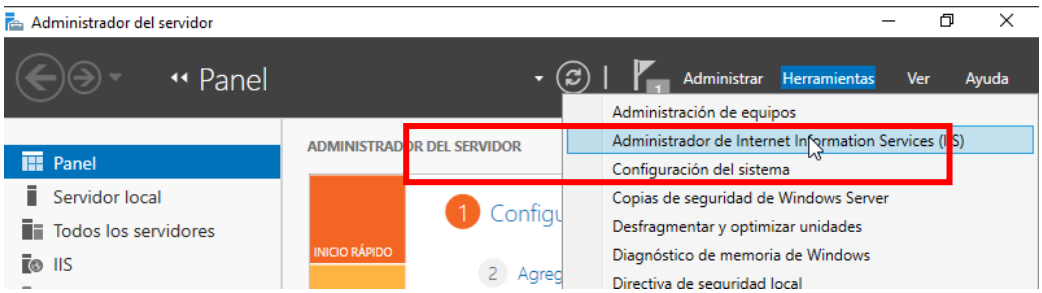


Ilustración 159. Selección de Administrador de IIS

Fuente: Elaboración propia

Aparece la siguiente pantalla en la cual debemos agregar el sitio web.

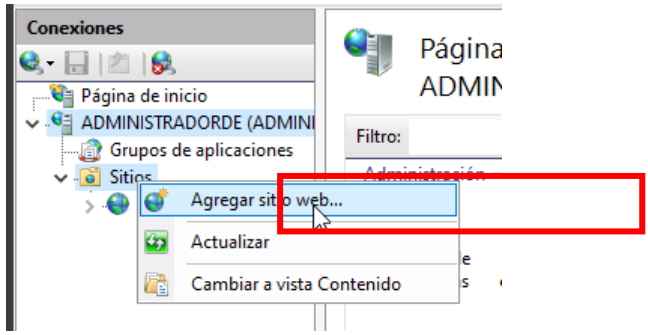


Ilustración 160. Agregar sitio web

Fuente: Elaboración propia

Se agregan las configuraciones correspondientes, como: el nombre del sitio, la ruta en la que se encuentra nuestro sitio web, la dirección IP del servidor web y el número del puerto http (en este caso 80).

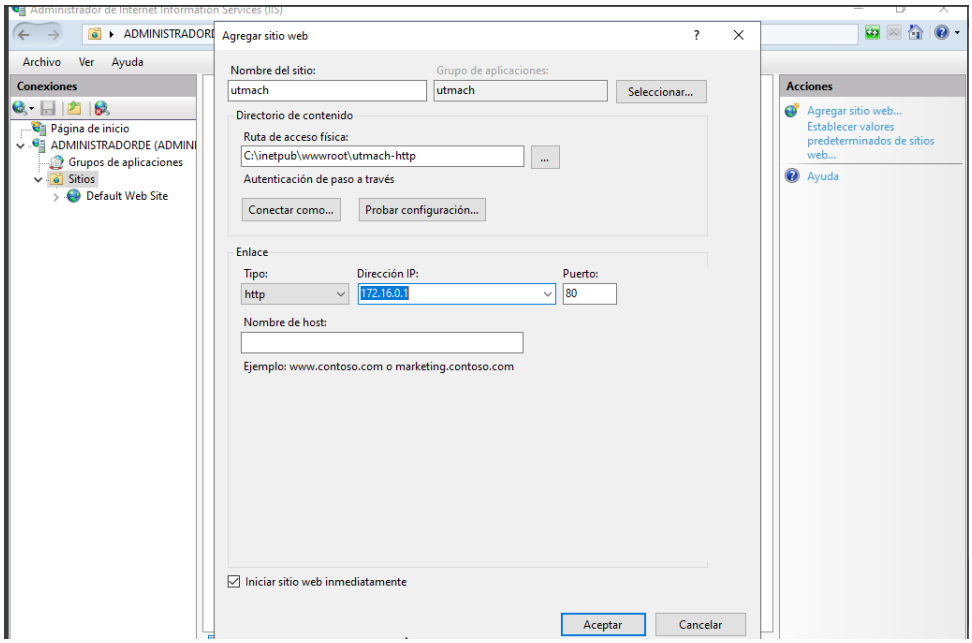


Ilustración 161. Configuración IP

Fuente: Elaboración propia

Visualizamos el sitio web agregado

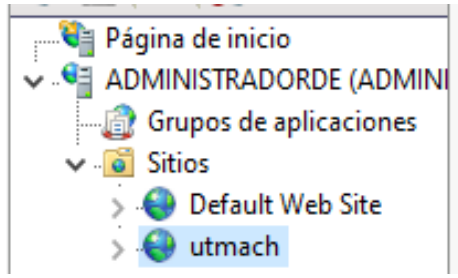


Ilustración 162. Visualización de sitio web

Fuente: Elaboración propia

Verificamos dentro de administrador si los documentos predeterminados del sitio existen.

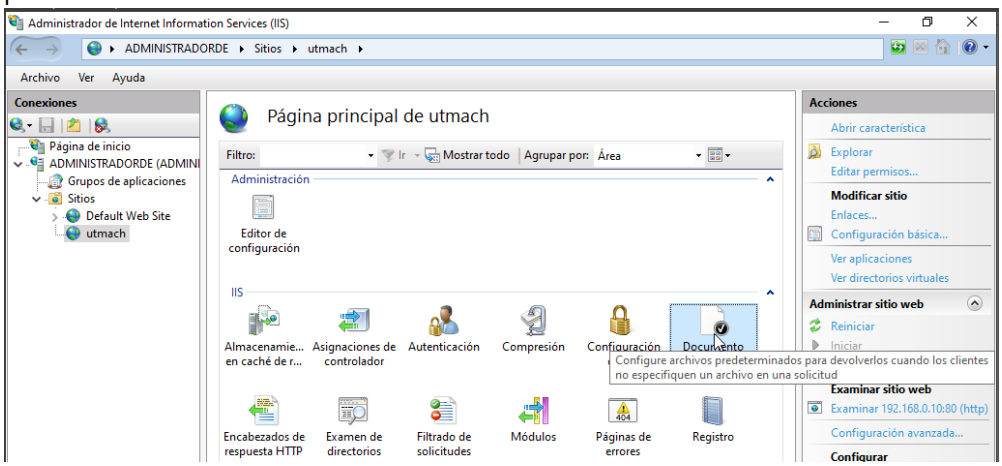


Ilustración 163. Administrador de IIS

Fuente: Elaboración propia

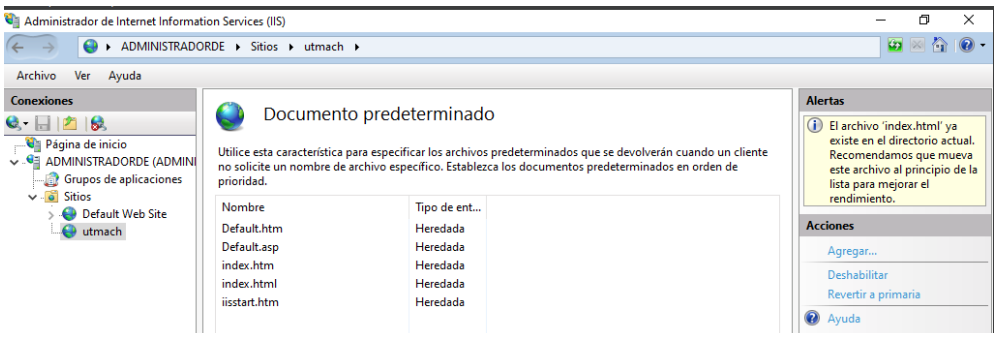


Ilustración 164. Documentos predeterminados

Fuente: Elaboración propia

Prueba del sitio web desde la máquina cliente

Desde la máquina cliente, utilizando un navegador de internet ingresamos la dirección IP del servidor web para comprobar el sitio web.

Ilustración 165. Comprobación de sitio web

Fuente: Elaboración propia

Implementación del Sitio Web utilizando HTTPS en IIS.

Para la implementación del Sitio Web utilizando HTTPS, en primer lugar creamos un certificado para el protocolo https.

Creación de un certificado para el protocolo HTTPS.

En el administrador del Servicio IIS damos clic donde dice "Certificado de Servidor".

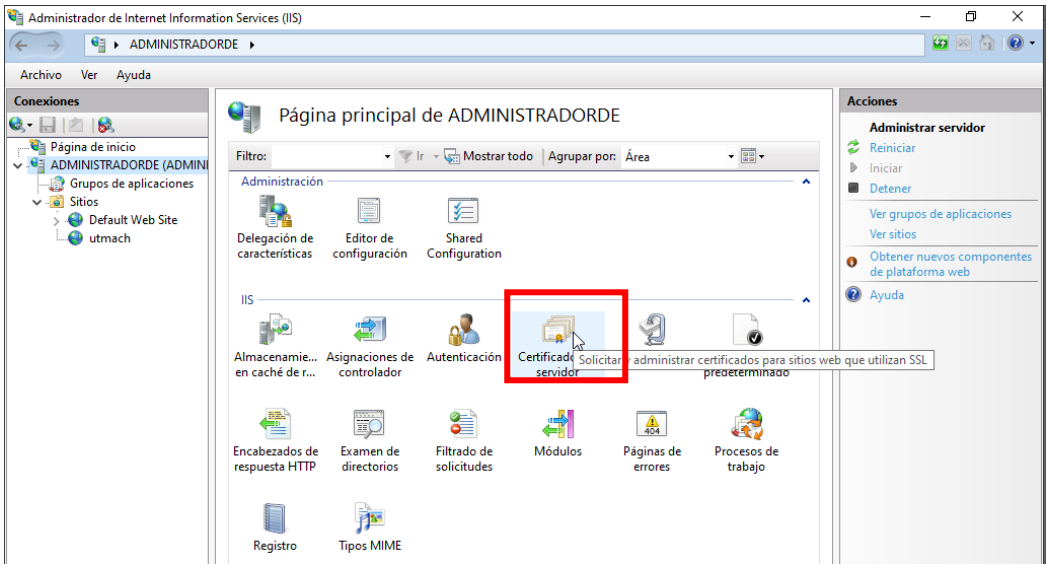


Ilustración 166: Certificado del servidor

Fuente: Elaboración propia

En la derecha se encuentra la opción de “crear certificado auto firmado” y le damos clic.

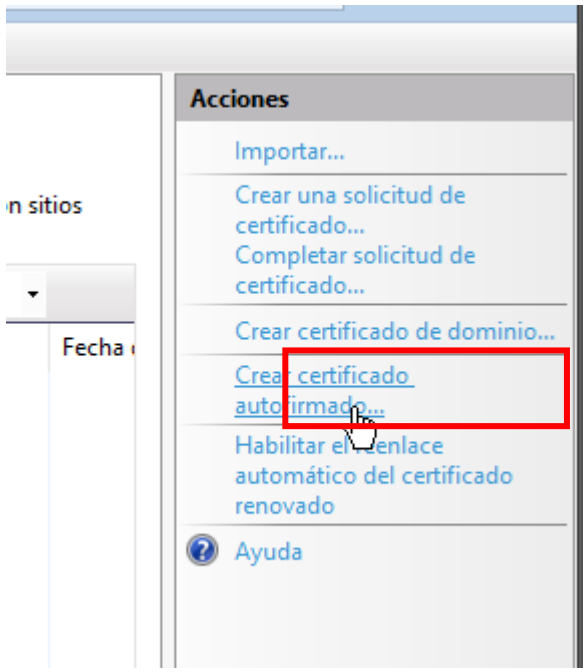


Ilustración 167: Certificado auto firmado

Fuente: Elaboración propia

Le asignamos un nombre al auto certificado que tenemos y le damos aceptar.

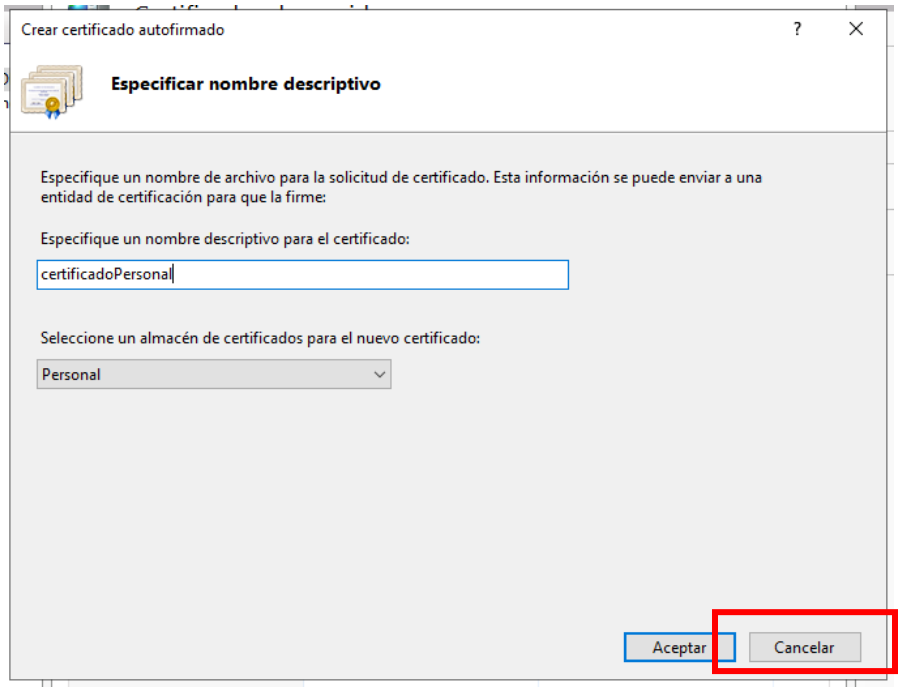


Ilustración 168: Nombre del certificado

Fuente: Elaboración propia

Nos mostrará el certificado que tenemos.

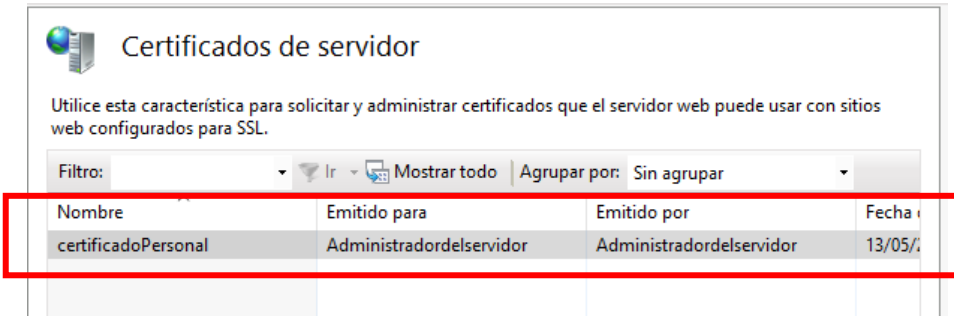


Ilustración 169: Certificados generados

Agregación del sitio web al Servicio de IIS.

Diríjase a "Herramientas" y haga clic en "Administrador de Internet Information Services (IIS)".

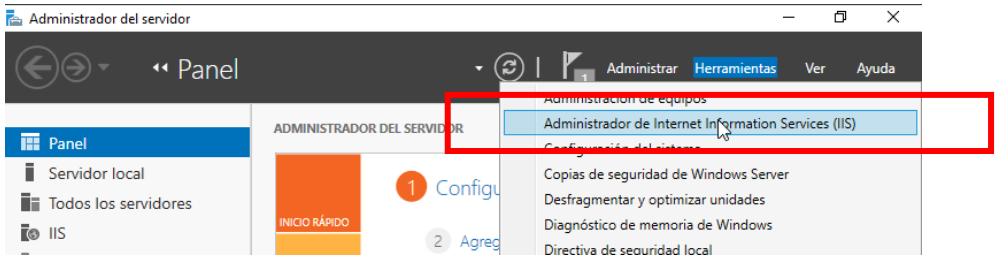


Ilustración 170: Servicio IIS

Fuente: Elaboración propia

Aparece la siguiente pantalla en la cual debemos agregar el sitio web.

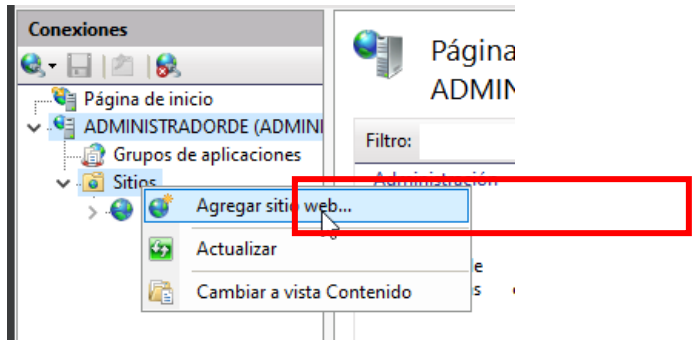


Ilustración 171: Agregar sitio web

Fuente: Elaboración propia

Agregamos configuración correspondiente como nombre del sitio, ruta, IP del sitio y el certificado que tenemos.

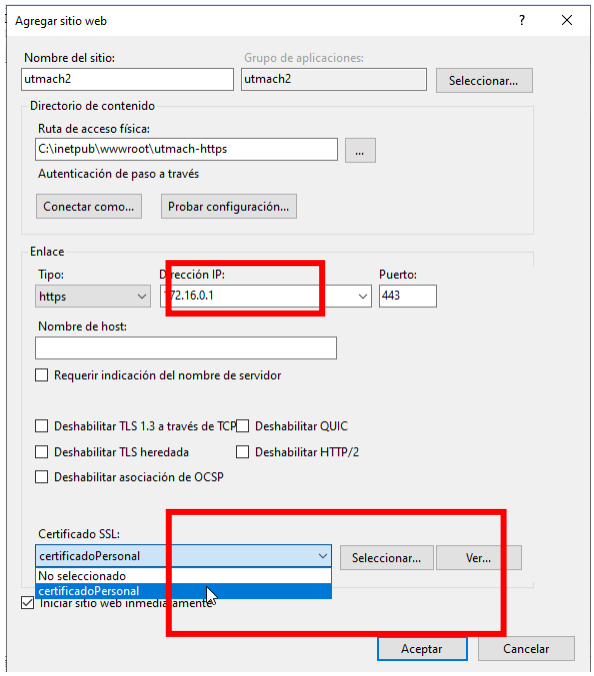


Ilustración 172. *Configuración del nombre del sitio, ruta e IP del sitio y certificado*

Fuente: Elaboración propia

Visualizamos el sitio web agregado

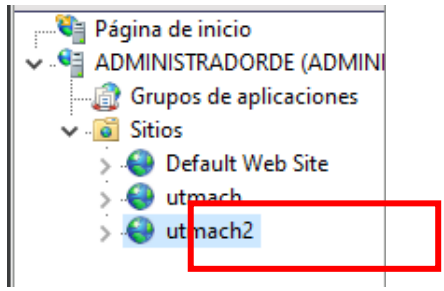


Ilustración 173. Visualizamos el sitio agregado

Fuente: Elaboración propia

Verificamos dentro de administrador si los documentos predeterminados del sitio existen.

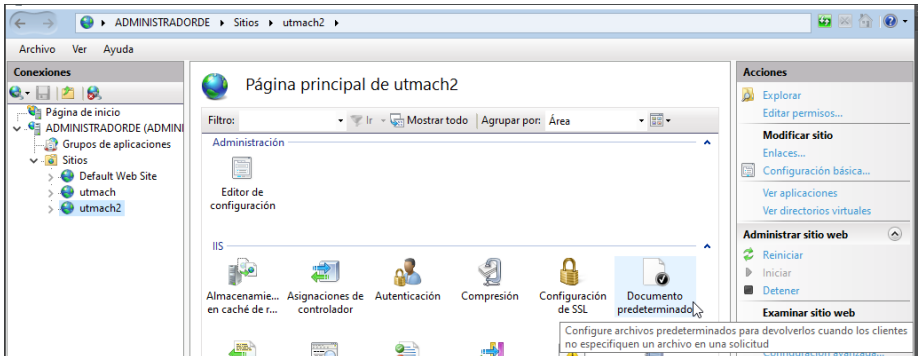


Ilustración 174. Verificamos si los documentos existen

Fuente: Elaboración propia

Visualización del sitio web desde el cliente

Agregamos la IP en un navegador para comprobar el sitio web.

Ilustración 175. Visualizamos el sitio web tipo HTTPS

Fuente: Elaboración propia

Implementación de un DNS para el sitio web

Crear zonas directas

Desde el Administrador de Servidor DNS, se debe proceder a la creación de una nueva zona directa en las zonas de búsqueda directa.

Vamos a herramientas para acceder al servicio de DNS.

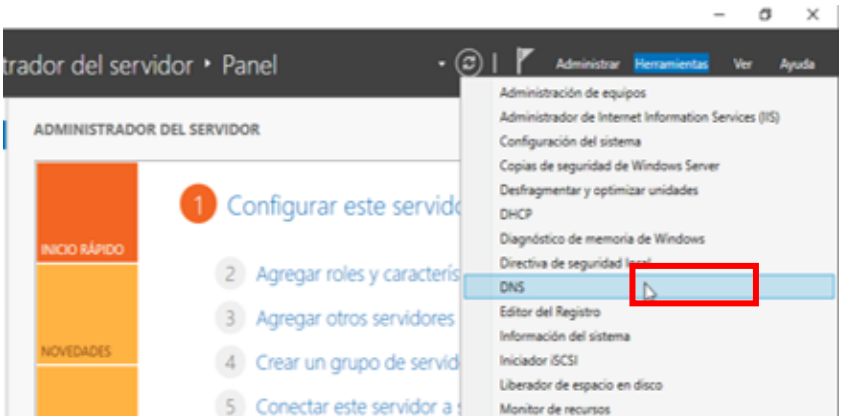


Ilustración 176. Herramienta DNS

Fuente: Elaboración propia

Se hace clic derecho y se selecciona "Nueva Zona", lo que abrirá una nueva ventana.

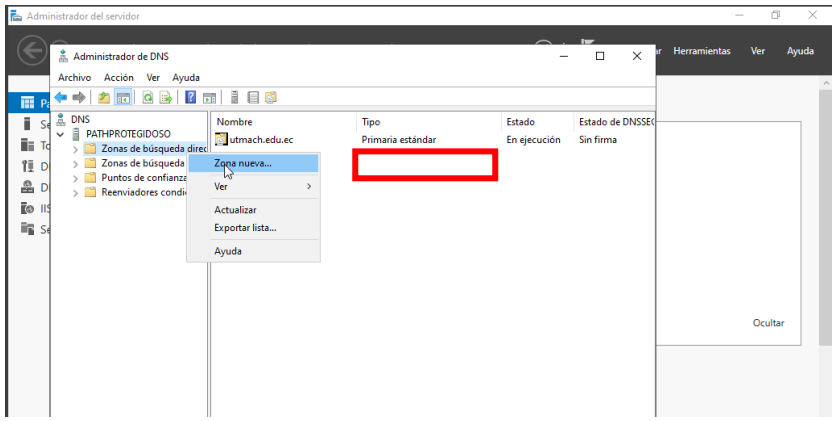


Ilustración 177. Zona nueva

Fuente: Elaboración propia

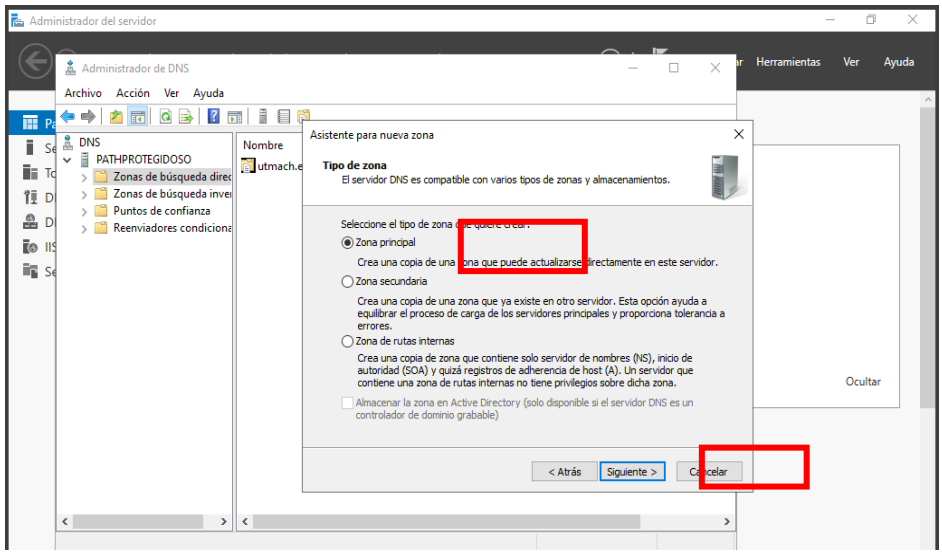


Ilustración 178. Selección de zona principal

Fuente: Elaboración propia

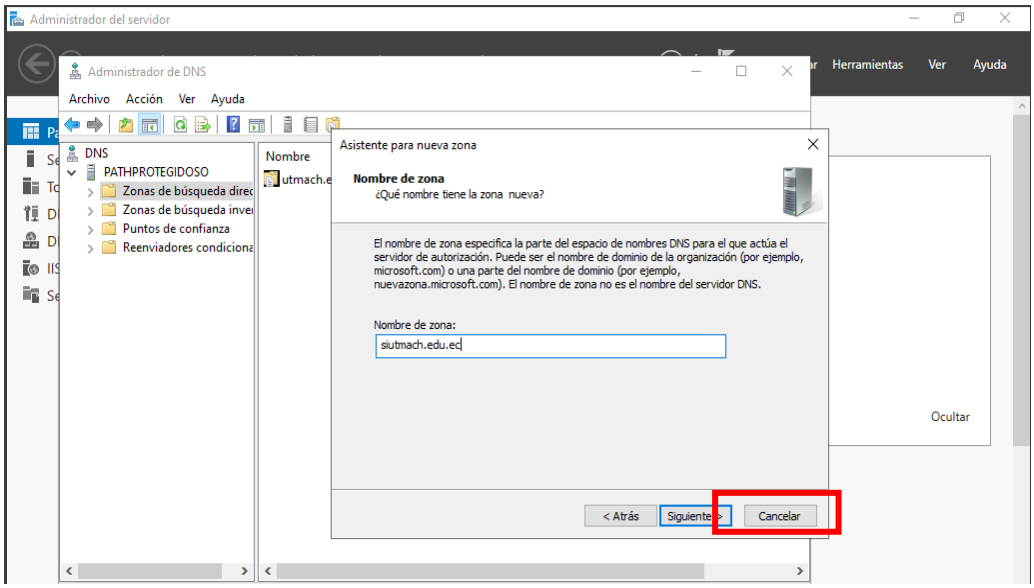


Ilustración 179. Nombre de la zona nueva

Fuente: Elaboración propia

Se hace clic en "Finalizar" para agregar la nueva zona.

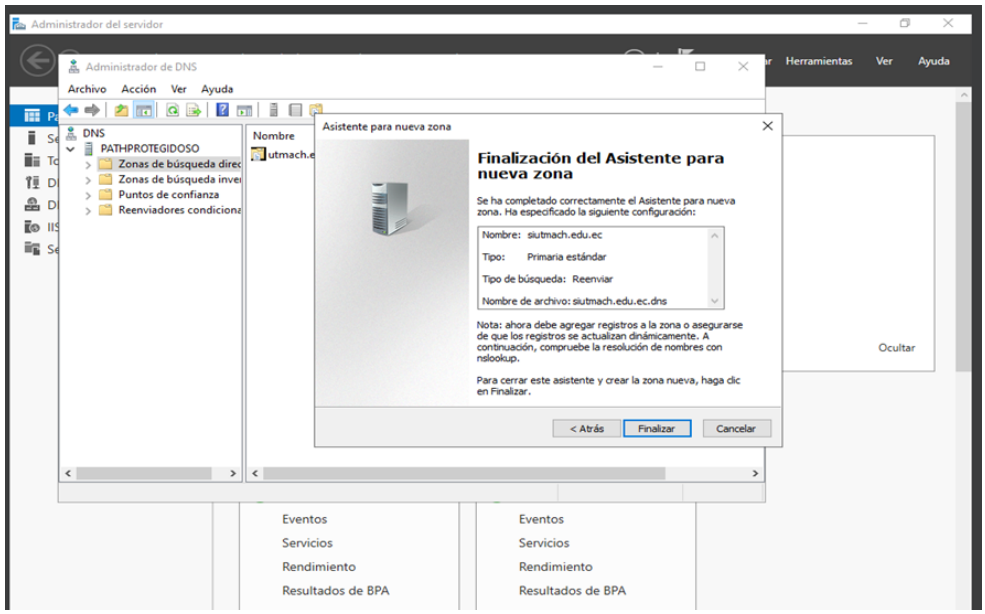


Ilustración 180. Finalización de creación de zona nueva

Fuente: Elaboración propia

Desde el Administrador de Servidor DNS, se procede a crear un nuevo Host en las zonas de búsqueda directa, ingresando la dirección IP del servidor.

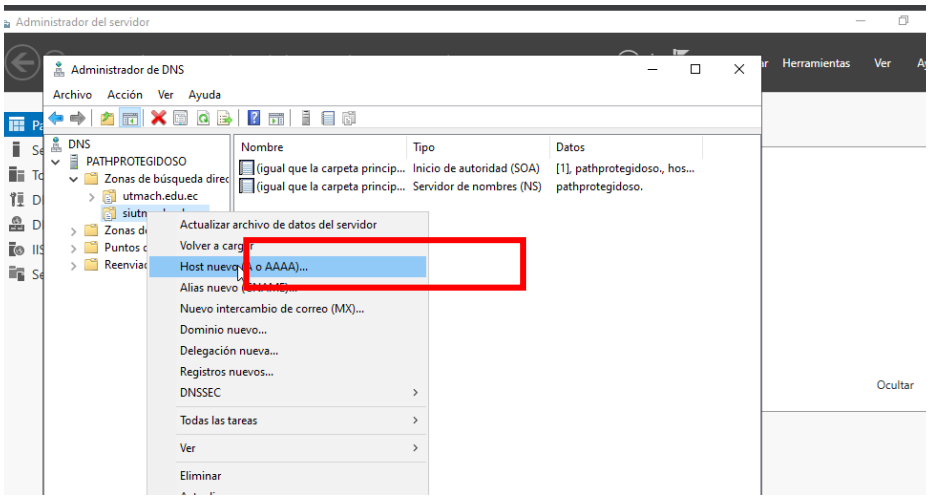


Ilustración 181. Creación de nuevo host

Fuente: Elaboración propia

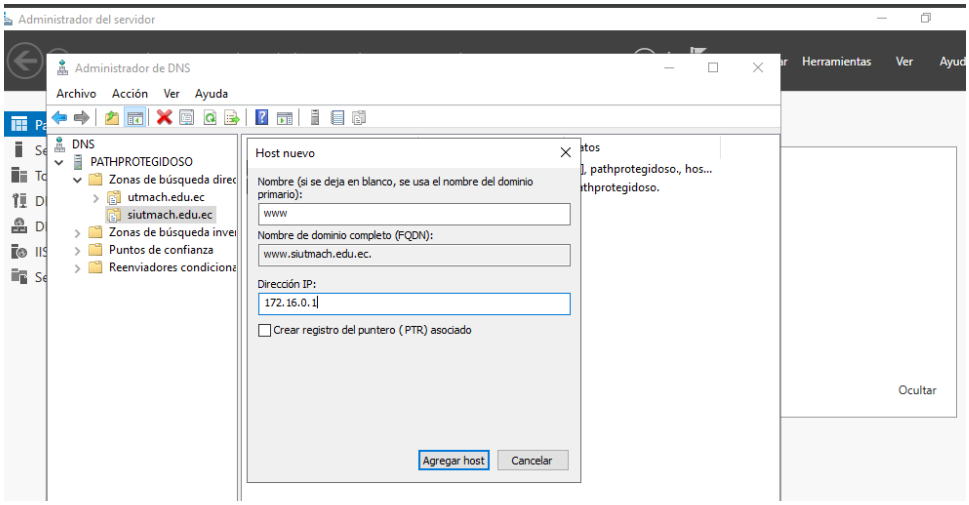


Ilustración 182. Nombre de nuevo dominio

Fuente: Elaboración propia

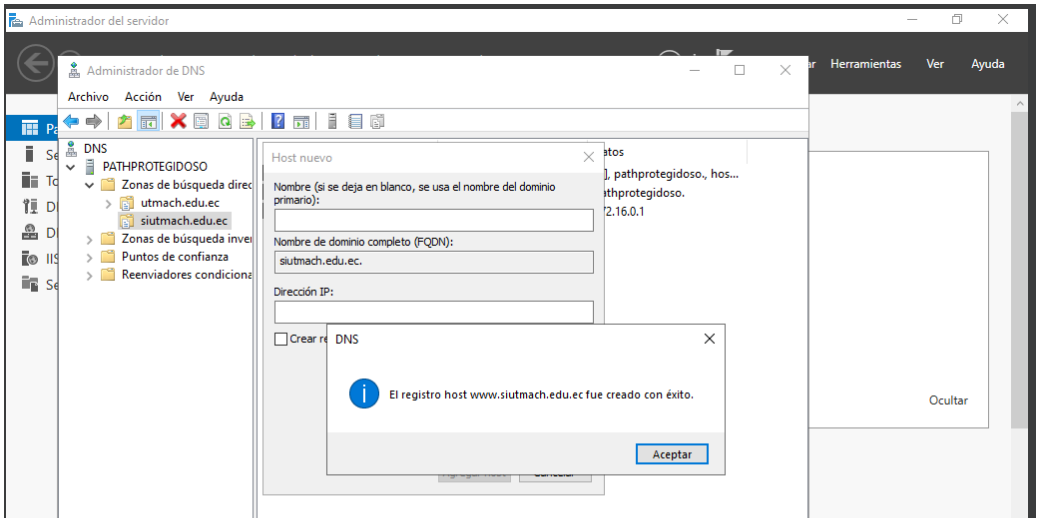


Ilustración 183. Registro de dominio exitoso

Fuente: Elaboración propia

Al ya contar con una zona inversa asociada a la misma IP, no se requiere crear otra. En su lugar, se procede a crear un nuevo puntero (PTR).

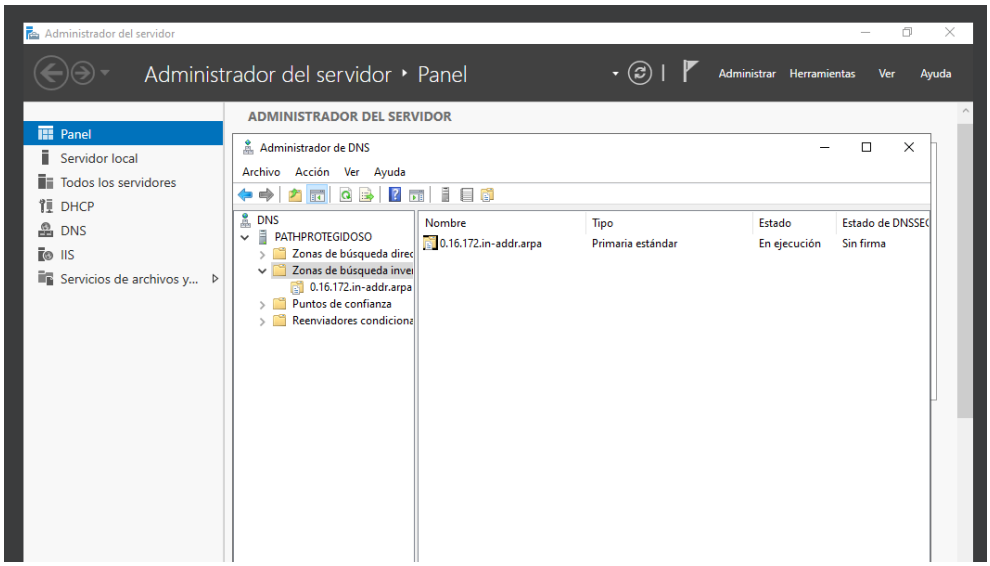


Ilustración 184. Creación de nuevo puntero

Fuente: Elaboración propia

Desde el Administrador de Servidor DNS crear un nuevo puntero (PTR)

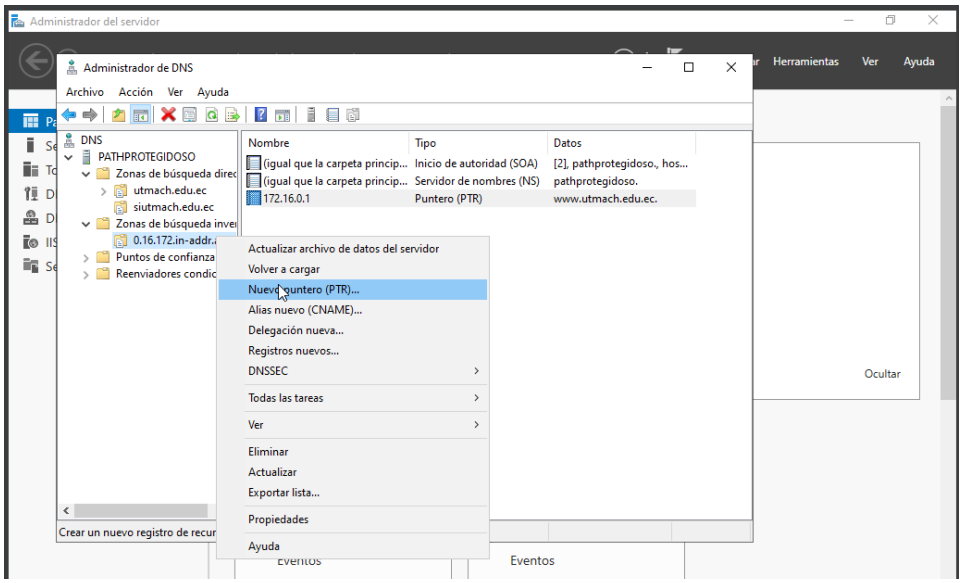


Ilustración 185. Puntero

Fuente: Elaboración propia

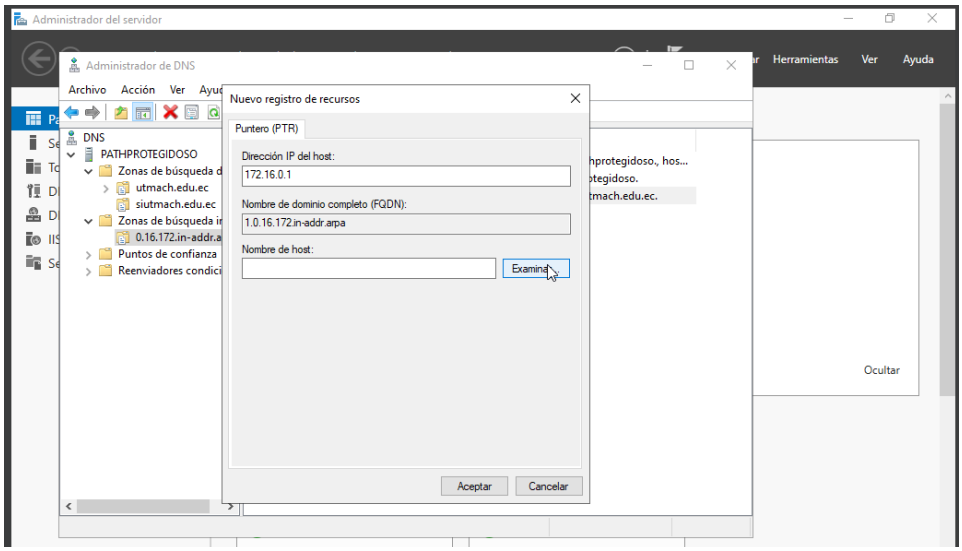


Ilustración 186: Configuración IP del puntero

Fuente: Elaboración propia

Aquí se puede observar que el puntero ha sido creado exitosamente.

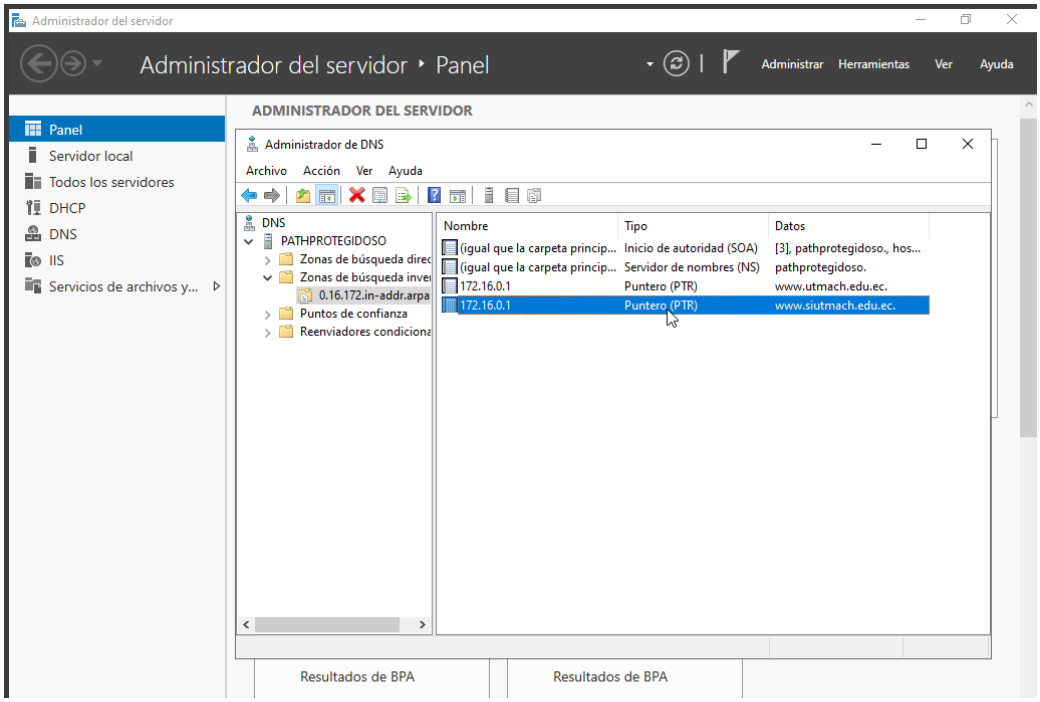


Ilustración 187. Puntero creado

Fuente: Elaboración propia

Agregación del nombre del host DNS en el sitio web

En el panel izquierdo se selecciona el sitio web al que se le agregará el nombre del DNS y se hace clic en "Modificar enlace".

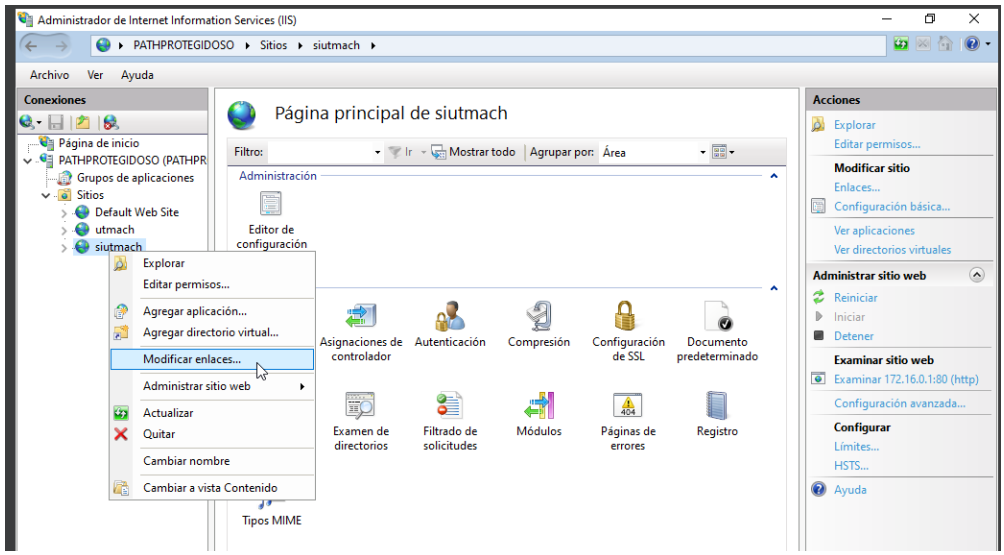


Ilustración 188. Modificación de enlace

Fuente: Elaboración propia

En la siguiente ventana, se hace clic en el botón Modificar.

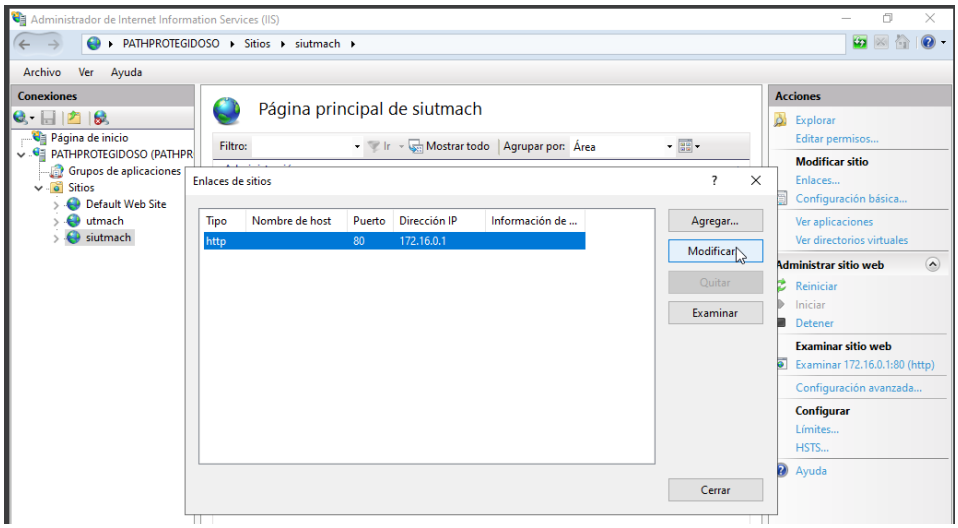


Ilustración 189. Enlaces a sitios

Fuente: Elaboración propia

En la siguiente ventana colocamos el nombre del host, en este caso: www.siutmach.edu.ec

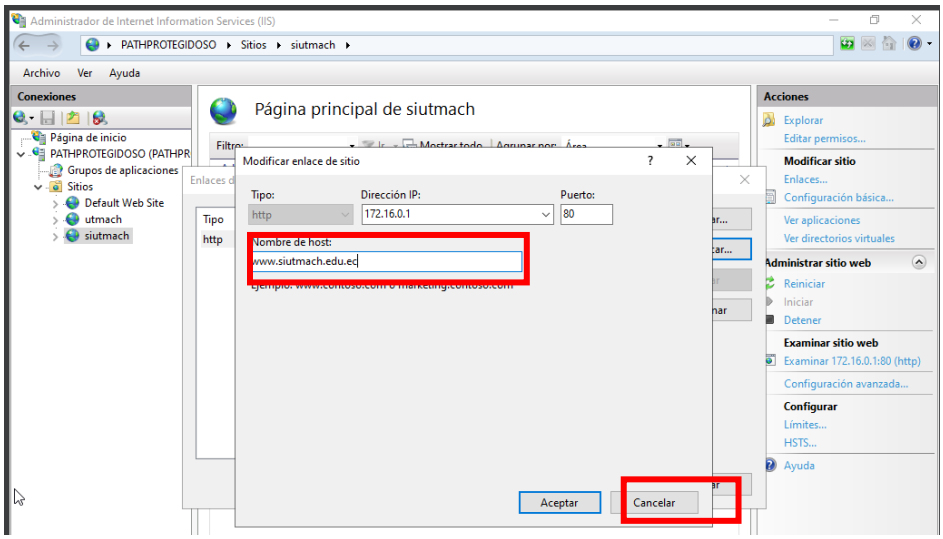


Ilustración 190. Modificación de enlace a sitios

Fuente: Elaboración propia

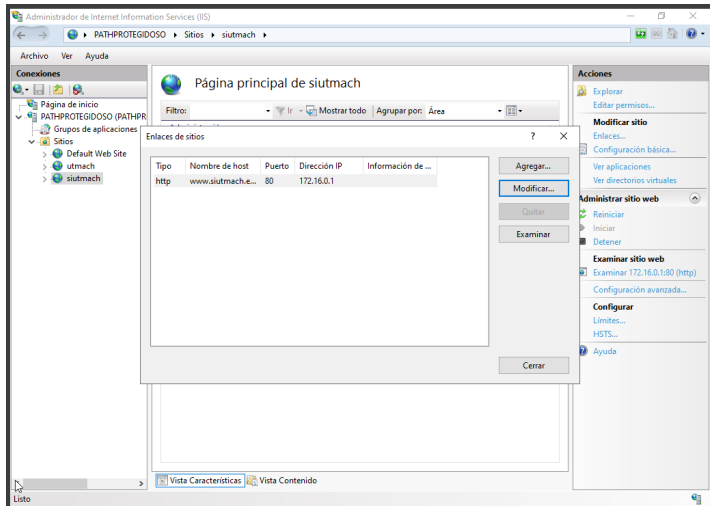


Ilustración 191. Sitio modificado

Fuente: Elaboración propia

Ahora, reiniciamos el sitio web modificado.

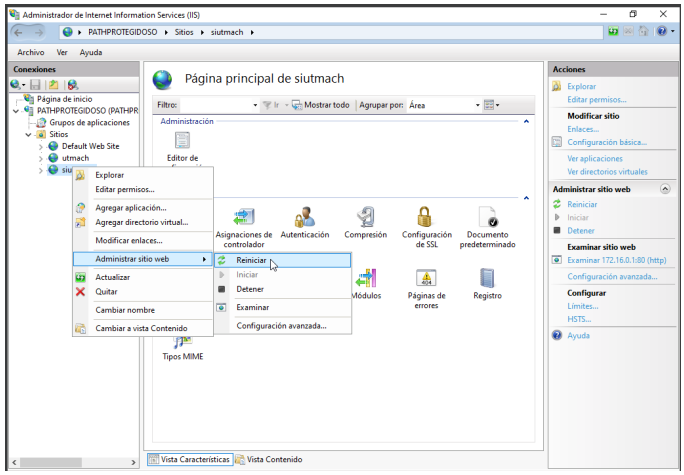


Ilustración 192. Reinicio de sitios

Fuente: Elaboración propia

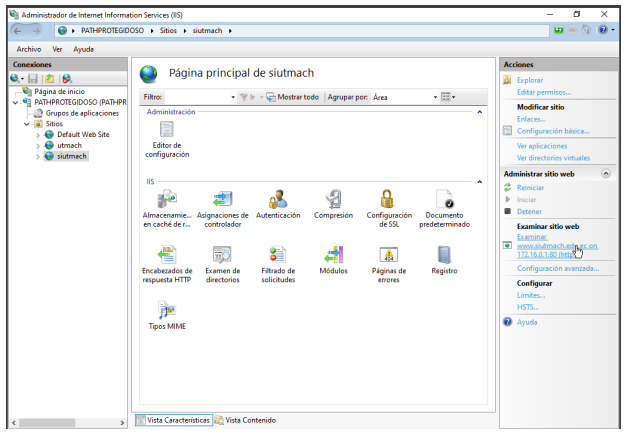


Ilustración 193. Sitios web

Fuente: Elaboración propia

Visualización desde el cliente utilizando el nombre del host configurado en el servidor

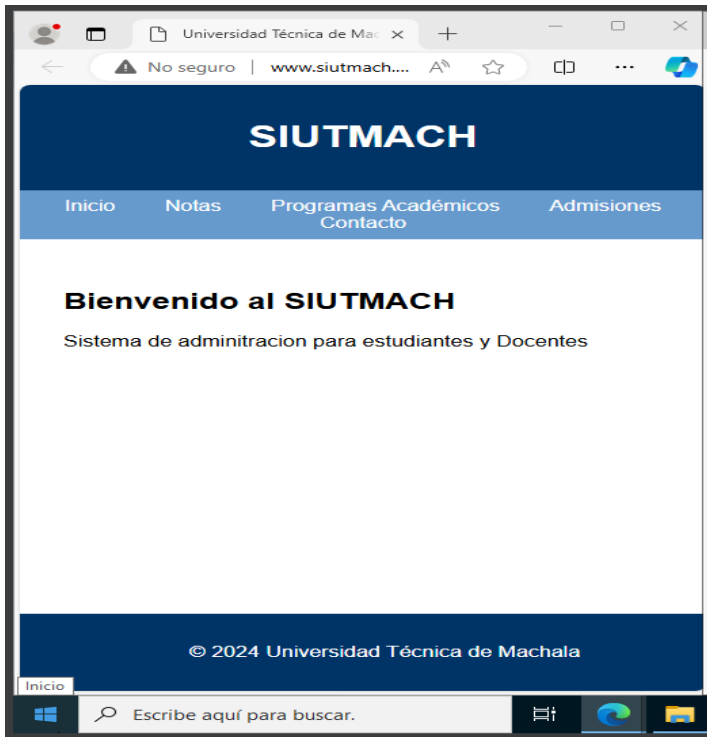


Ilustración 194. Realización de pruebas

Fuente: Elaboración propia

Resumen del Capítulo II

El capítulo II, aborda tres servicios de la infraestructura de redes modernas: DHCP, DNS e IIS (web), analizando su instalación, configuración y funcionamiento dentro de un entorno Windows Server. Se comienza con el servicio de DHCP (Protocolo para la configuración dinámica del host) que automatiza la asignación de direcciones IP y parámetros de red, para la gestión y reduciendo errores. Se realiza la configuración del servicio mediante un ámbito, con el manejo de exclusiones, reservas y filtros para controlar el acceso. Además, se incluyen comandos de diagnóstico como ipconfig /all, release y renew. Luego se trabaja con el DNS (Sistema de Nombres de Dominio), esencial para la resolución de nombres en redes locales y globales. Se explican sus puertos, tipos de servidores (maestros, esclavos y de caché), estructura jerárquica de nombres de dominio, registros de recursos (A, MX, CNAME, PTR, entre otros) y la creación de zonas directas e inversas. Se incluyen pruebas de conectividad y comandos como nslookup y ping, que permiten verificar la correcta configuración del servicio. Finalmente, se presenta IIS (Internet Information Services), que es el software de servidor web de Microsoft, se describe su arquitectura modular, el funcionamiento de los protocolos HTTP y HTTPS, y la importancia de los certificados SSL para garantizar comunicaciones seguras. Se guía al lector en la implementación de sitios web tanto en HTTP como en HTTPS, incluyendo la creación de certificados, configuración de enlaces DNS y pruebas desde el cliente.

Este capítulo ofrece una combinación de teoría y práctica que permite al lector comprender y aplicar los servicios de red esenciales para entornos empresariales, fortaleciendo la seguridad, disponibilidad y eficiencia de las comunicaciones digitales.

Preguntas De Revisión

Evaluación de Conocimientos Adquiridos

1. Entendimiento de Conceptos Básicos:
   - Defina con claridad qué es Windows Server Core y explique en qué se diferencia de la versión con experiencia de escritorio. Si no puede hacerlo con seguridad, investigue más y elabore un cuadro comparativo.
   - Describa qué es Internet Information Services (IIS), cómo funciona su modelo de gestión de solicitudes y cuáles son sus principales ventajas. Considere elaborar un esquema que detalle este modelo.
2. Habilidades Prácticas:
   - Evalúe su capacidad para instalar y configurar Windows Server Core utilizando herramientas como PowerShell o SConfig. Si encuentra dificultades, detalle qué aspectos necesita revisar o aprender con mayor profundidad.
   - Evalúe también su capacidad para instalar y configurar IIS en un entorno con Windows Server. Prepare una lista de pasos para agregar roles, asignar puertos y gestionar sitios web.
3. Aplicación de Políticas de Seguridad:
   - Explique cómo aplica medidas de seguridad en Server Core y en IIS. Incluya la configuración de autenticación, el uso de cifrado SSL/TLS y la protección del sistema minimizando la superficie de ataque.
   - Discuta cómo asegura el cumplimiento de buenas prácticas en ambos entornos. Cree una lista de verificación que incluya puntos como puertos seguros, certificados, filtrado de solicitudes y módulos esenciales activados.
4. Resolución de Problemas:
   - Diagnostique y resuelva un problema común en Server Core, como una falla en la conexión de red o error en el ingreso al

dominio. Documente el proceso paso a paso.

- Realice también una tarea de mantenimiento en IIS, como restaurar la configuración de un sitio o corregir un error de carga. Describa el procedimiento y evalúe su efectividad.

Autoevaluación Personal

1. Reflexión sobre el Aprendizaje:
   - ¿Qué aspectos de la administración de IIS encuentra más desafiantes? Explique por qué y proponga estrategias para superar esas dificultades.
   - Determine qué herramientas, lecturas o prácticas adicionales necesita para mejorar su dominio de la administración de servidores en entornos web.
2. Plan de Mejora Continua:
   - Establezca sus próximos pasos para profundizar en el uso profesional de Windows IIS. Esto puede incluir prácticas con roles específicos, lectura de documentación técnica o desarrollo de laboratorios.
   - Investigue certificaciones relacionadas como Microsoft Certified: Windows Server Hybrid Administrator Associate o cursos sobre IIS y administración de servidores. Elabore una lista de opciones y fije metas claras para alcanzarlas.

Referencias Bibliográficas

Microsoft. (2025). *Información general sobre DHCP (Protocolo de configuración dinámica de host)*. Microsoft Learn. https://learn.microsoft.com/es-es/windows-server/networking/technologies/dhcp/dhcp-top

OmniSecu. (2025). *DHCP (Dynamic Host Configuration Protocol) messages*. https://www.omnisecu.com/tcpip/dhcp-dynamic-host-configuration-protocol-messages.php

De Luz, S. (2024, octubre 9). *¿Qué es el protocolo DHCP y cómo funciona?* RedesZone. https://www.redeszone.net/tutoriales/internet/que-es-protocolo-dhcp/

EITCA Academy. (2023, 5 de agosto). *¿Qué son las exclusiones en un ámbito DHCP y cómo las configura?* https://es.eitca.org/la-seguridad-cibern%C3%A9tica/eitc-es-la-administraci%C3%B3n-del-servidor-de-Windows-de-wsa/configuraci%C3%B3n-de-zonas-dhcp-y-dns-en-el-servidor-de-Windows/alcances-y-exclusiones-de-dhcp/examen-revisi%C3%B3n-dhcp-alcances-y-exclusiones/%C2%BFQu%C3%A9-son-las-exclusiones-en-un-%C3%A1mbito-dhcp-y-c%C3%B3mo-se-configuran%3F/

Riveros García, M. (2023, julio 25). *¿Qué es el protocolo DHCP y para qué sirve?* ManageEngine Blog. https://blogs.manageengine.com/latam/2023/07/25/que-es-el-protocolo-dhcp-para-que-sirve.html

García de Zúñiga, F. (2024, mayo 3). *¿Qué es y para qué sirve un servidor DHCP?* Arsys. https://www.arsys.es/blog/que-es-y-para-que-sirve-un-servidor-dhcp

Rodríguez Raposo, A. (2001). *Los nombres de dominio de internet: Presente y futuro de la situación en España*. Revista Economía Industrial, (338), 71–84. https://www.mintur.gob.es/Publicaciones/Publicacionesperiodicas/EconomiaIndustrial/RevistaEconomiaIndustrial/338/07rodriguez338.pdf

Barbieri, A. (2023). *Traduciendo nombres a direcciones (DNS)*. Libros de Cátedra. https://sedici.unlp.edu.ar/bitstream/handle/10915/167115/Documento_completo.pdf?sequence=1&isAllowed=y

IBM Corporation. (2010). *IBM i 7.1: Protocolo de configuración dinámica de hosts (DHCP)*. https://www.ibm.com/docs/en/ssw_ibm_i_71/rzakk/rzakk.pdf

Cloudflare. (2025). *¿Qué es un DNS? | Registros DNS*. https://www.cloudflare.com/es-es/learning/dns/dns-records/

InterGrupo. (2013). *Windows Server 2012: Zonas DNS*. https://elhacker.info/manuales/Servidores/Windows%20Server%202012%20Zonas%20DNS.pdf

WPADE. (2024, 26 de enero). *¿Qué es el puerto DNS? Puerto 53 UDP/TCP funcionando*. https://www.wpade.com/es/dns-port.html

IONOS. (2019, 18 de julio). *nslookup: la herramienta para acceder a las entradas DNS*. https://www.ionos.es/digitalguide/servidores/herramientas/nslookup/

Kessler, G. C., & Shepard, S. D. (1997). *A primer on Internet and TCP/IP tools and utilities* (RFC 2151). RFC Editor. https://www.rfc-editor.org/rfc/rfc2151.html

Rock Content. (2024, 5 de marzo). *¿Qué es un servidor?*. https://rockcontent.com/es/blog/que-es-un-servidor/

Instituto Consorcio Clavijero. (2025). *Tema 1.1: Introducción a la programación web*. En *Desarrollo de aplicaciones en web*. https://cursos.clavijero.edu.mx/cursos/145_daw/modulo1/contenidos/tema1.1.html

Ruiz, M., & Ulloa, C. (2013, mayo 23). *Análisis de comunicaciones y protocolos TCP/IP utilizando herramientas de software para la captura de paquetes*. ResearchGate. https://www.researchgate.net/profile/Cristian-Ulloa/publication/240614123_Analisis_de_protocolos_TCP_con_sniffer_Wireshark/links/02e7e51c66b6a37861000000/Analisis-de-protocolos-TCP-con-sniffer-Wireshark.pdf

Cloudflare. (2025). *¿Qué es HTTPS?*. https://www.cloudflare.com/es-es/learning/ssl/what-is-https/

Kaspersky. (2025). *¿Qué es un certificado SSL y por qué es importante?* Recuperado de https://latam.kaspersky.com/resource-center/definitions/what-is-a-ssl-certificate

Casero, A. (2024, 8 de abril). *¿Cómo funciona el servidor web IIS?*. KeepCoding Bootcamps. https://keepcoding.io/blog/como-funciona-iis-internet-information-services/

CAPÍTULO 3

ADMINISTRACIÓN DEL SERVICIO DE PROXY

Introducción a los Servidores Proxy

Objetivos

Implementar un servidor proxy con funciones de almacenamiento en caché para la mejora de la velocidad de acceso y la carga del ancho de banda.

Configurar políticas de filtrado de contenido para el bloqueo de sitios web inseguros o no permitidos.

Incorporar autenticación y autorización para el acceso exclusivo a usuarios autorizados.

Los servidores proxy son tecnologías clave en la administración moderna de redes, ya que actúan como intermediarios entre los dispositivos clientes y los servidores finales. Su función principal es recibir solicitudes de los usuarios, procesarlas y reenviarlas a los destinos correspondientes, devolviendo luego las respuestas. Esta intermediación no solo permite una mayor eficiencia en el manejo del tráfico, sino que también proporciona importantes beneficios en términos de seguridad, anonimato, control de acceso y gestión del rendimiento.

Entre sus funciones más destacadas se encuentra el almacenamiento en caché, que permite acelerar la carga de contenido previamente solicitado; el filtrado de contenido, que bloquea accesos a sitios maliciosos o inapropiados; y el anonimato, que oculta la dirección IP del usuario para proteger su identidad. Asimismo, los servidores proxy permiten a las organizaciones imponer restricciones geográficas, controlar el uso de ancho de

banda, e incluso analizar el tráfico en tiempo real para detectar patrones sospechosos o ineficiencias.

Este capítulo aborda tanto los fundamentos teóricos como las aplicaciones prácticas del servicio de proxy, presentando los distintos tipos existentes, sus usos, ventajas y procedimientos de instalación y configuración. Además, se destacan las estrategias de seguridad asociadas y las buenas prácticas para su administración en entornos empresariales y académicos.

Preguntas de Enfoque

Preguntas de Inicio

1. ¿Qué es un servidor proxy y cuál es su papel dentro de una arquitectura de red segura y eficiente?
2. ¿Cuáles son los principales tipos de servidores proxy y qué características diferencian su uso?
3. ¿Cómo puede un servidor proxy contribuir a la seguridad, el control de acceso y el rendimiento en una red empresarial?

Competencias o Problemas a Resolver

Al finalizar este capítulo, los lectores serán capaces de:

- Comprender y explicar los conceptos fundamentales de los servidores proxy y su funcionamiento como intermediarios en la red.
- Identificar y aplicar los distintos tipos de proxies según el contexto o necesidad de la organización.
- Instalar, configurar y administrar un servicio de proxy, incluyendo la definición de políticas de acceso, almacenamiento en caché y monitoreo del tráfico.

- Diseñar soluciones de proxy seguras, escalables y adaptables a diferentes entornos tecnológicos.

Problemas a Resolver

1. ¿Cómo se puede implementar un servidor proxy que combine eficiencia, anonimato y control de contenido en una organización?
2. ¿Qué estrategias permiten optimizar el rendimiento de un proxy en redes con alto volumen de tráfico?
3. ¿Cómo se puede usar un proxy para mejorar la seguridad y visibilidad del tráfico en una infraestructura empresarial?

Servidores Proxy

Definición de Proxy

Un servidor proxy es un intermediario entre un cliente (como un usuario o aplicación) y un servidor de destino. Recibe las solicitudes del cliente, las puede reenviar, modificar o responder directamente. Además de facilitar la comunicación, ofrece una capa de seguridad al ocultar la dirección IP real del usuario, protegiéndolo de posibles ataques. Al actuar como puerta de enlace entre el usuario e Internet, el proxy ayuda a gestionar el tráfico y a mantener el anonimato en línea (Fortinet, 2023; Microsoft, 2023).

Funcionamiento del servidor proxy

Según Gómez Montoya, Sepúlveda Rodríguez y Candela Uribe (2012), así como Hoces-Moral López (2019), un servidor proxy opera de la siguiente forma: cuando un cliente solicita una página web, el proxy recibe esa solicitud y verifica si ya tiene almacenada la información en su memoria caché. Si la posee, revisa si está actualizada; en caso afirmativo, se la entrega al cliente. Si la información no está actualizada, el proxy la renueva antes de enviarla. Si no la tiene en caché, la obtiene del servidor de origen, la guarda y luego la proporciona al cliente. Por lo general, el proxy escucha en el puerto 3128, aunque este puerto puede cambiarse siempre que esté disponible.

Ilustración 195. Realización de pruebas

Fuente: Elaboración propia

Tipos de Proxy

Proxy de reenvío: Un proxy de reenvío actúa como intermediario entre un cliente y una red externa. Este tipo de servidor analiza las solicitudes que salen de la red interna y decide cómo gestionarlas antes de enviarlas al destino externo. Generalmente, los proxies que se utilizan con más frecuencia son de este tipo. Ejemplos comunes incluyen las VPN y los filtros de contenido en la web (Senteno, Polanía & Pulido, 2019).

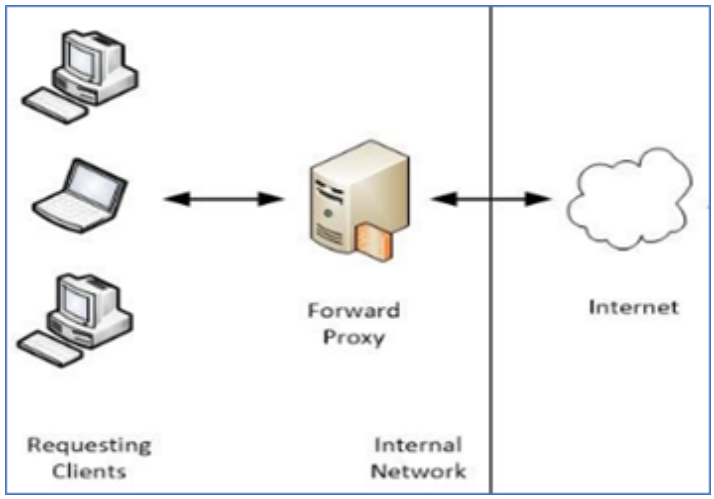


Ilustración 196. Proxy de reenvío

Fuente: (Microsoft, 2024)

Proxy inverso: Según (Microsoft, 2023), un servidor proxy inverso se encuentra entre una red y muchos otros recursos internos, se encarga de recibir las solicitudes externas y distribuirlas entre distintos servidores internos. Entre sus funciones principales están:

- Distribuir el tráfico para optimizar el rendimiento mediante balanceo de carga.
- Entregar contenido en caché para disminuir la presión sobre los servidores internos.
- Gestionar el cierre de conexiones TLS/SSL.
- Proteger la infraestructura interna ocultando sus detalles a los usuarios externos.

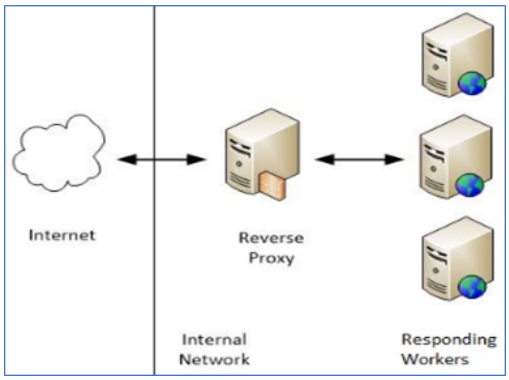


Ilustración 197. Proxy inverso

Fuente: (Microsoft, 2023)

Proxy transparente: es un servidor intermediario que intercepta el tráfico entre el usuario e Internet sin alterar el contenido de las solicitudes o respuestas. Este tipo de proxy suele emplearse en entornos como bibliotecas o centros educativos para aplicar filtros de contenido. Dado que no requiere configuración por parte del usuario, se presenta como una solución de fácil mantenimiento en comparación con otros tipos de servidores proxy (Hassel, 2025; Microsoft, 2025).

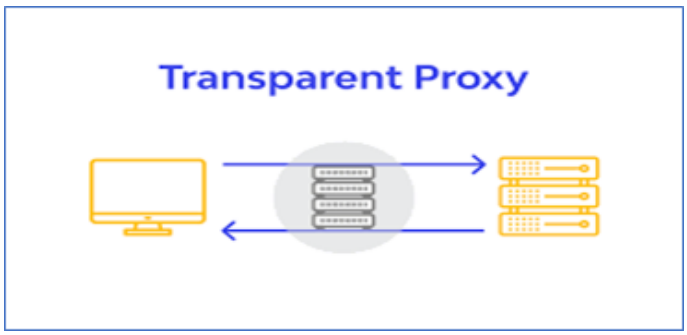


Ilustración 198. Proxy transparente

Fuente: (Wallarm, 2025.)

Beneficios del servidor proxy

- Almacenamiento en caché: Los proxies pueden almacenar respuestas a solicitudes frecuentes, lo que mejora el tiempo de respuesta del cliente y reduce la carga del servidor original.
- Filtrado de contenido: Al aplicar normas o políticas de seguridad, se puede bloquear el acceso a ciertos sitios web o categorías de contenido. (Maskat et al., 2025)
- Control de acceso: Para regular quién tiene acceso a los recursos a través del proxy, implementan métodos de autorización y autenticación.
- Optimización de la red: Al servir y almacenar contenido en caché y al reducir el tráfico innecesario, mejoran la eficiencia general de la red.

Desafíos y Consideraciones

- Latencia Adicional: La intermediación puede causar latencia adicional en la comunicación cuando se utiliza un proxy.

- Seguridad: Al exponer datos delicados o permitir acceso no autorizado, un proxy mal configurado puede ser un punto de vulnerabilidad.

- Mantenimiento y Administración: Para garantizar que las políticas de filtrado y almacenamiento en caché sean efectivas y actualizadas, es necesaria una gestión constante (Rashid, 2022).

- Compatibilidad: Algunos protocolos y aplicaciones pueden no funcionar correctamente a través de proxies, especialmente si son altamente específicos o personalizados.

Software Squid

Es un software de código abierto que opera como servidor proxy y permite almacenar páginas en caché, distribuido bajo la Licencia Pública General (GPL). Sus usos son diversos: puede optimizar el rendimiento de un servidor web mediante el almacenamiento de solicitudes repetidas como consultas DNS para usuarios que comparten una red, funcionar como caché web y reforzar la seguridad al filtrar el tráfico. (IONOS, 2020).

Caso práctico

Configuración e instalación de un Servidor Proxy con Squid en Windows Server

Configurar una dirección IP estática al Servidor

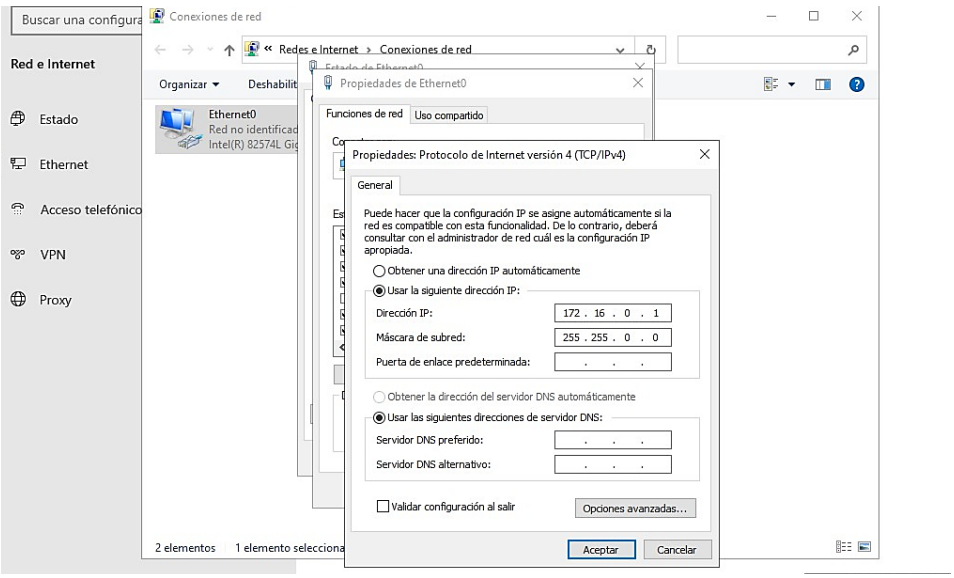


Ilustración 199. Asignación de una IP en el servidor.

Fuente: Elaboración propia

Configurar una dirección IP estática en el cliente

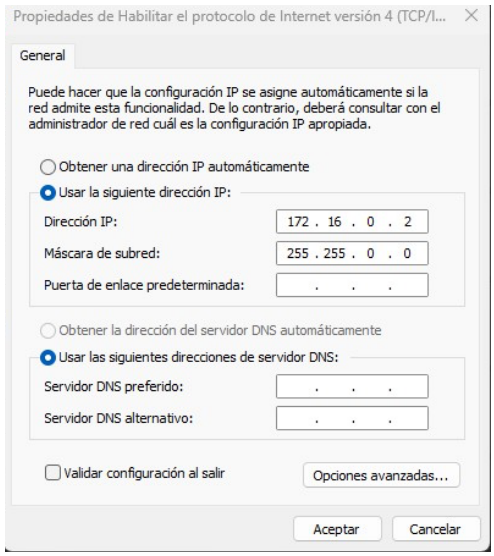


Ilustración 200. Asignación de una IP en el cliente.

Fuente: Elaboración propia

Verificar la conexión del servidor al cliente y del cliente al servidor.

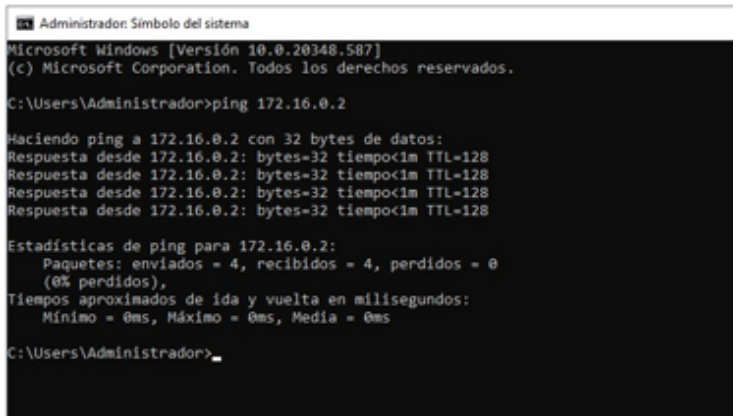


Ilustración 201. Ping del servidor al cliente.

Fuente: Elaboración propia

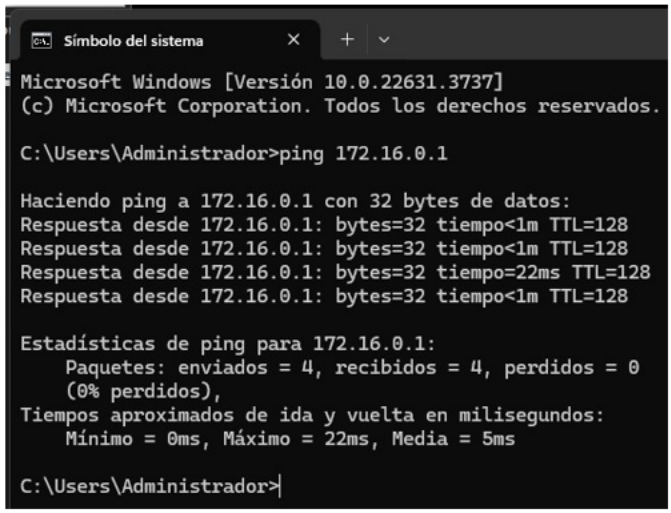


Ilustración 202. Ping del cliente al servidor.

Fuente: Elaboración propia

Instalación de Squid en Windows Server 2022.

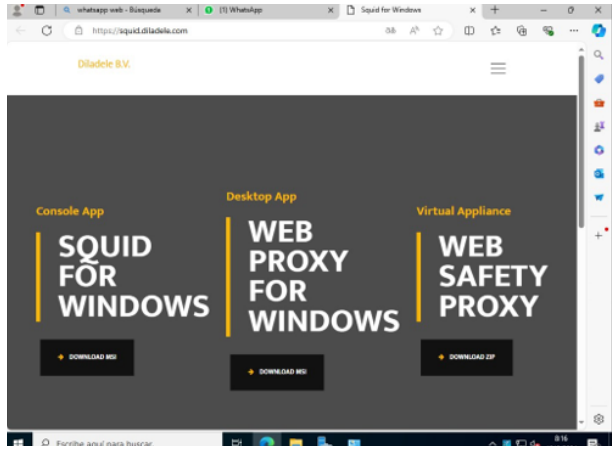


Ilustración 203. Página donde se descargó el squid.

Fuente: Elaboración propia

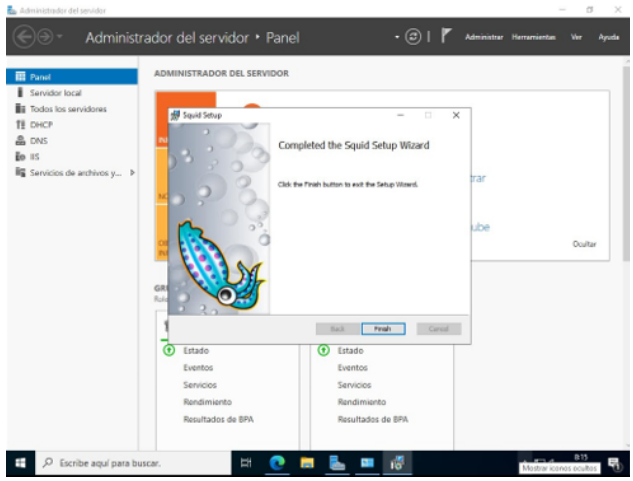


Ilustración 204. Instalación de proxi.

Fuente: Elaboración propia

Verificar si se ha instalado el servicio y que este en ejecución

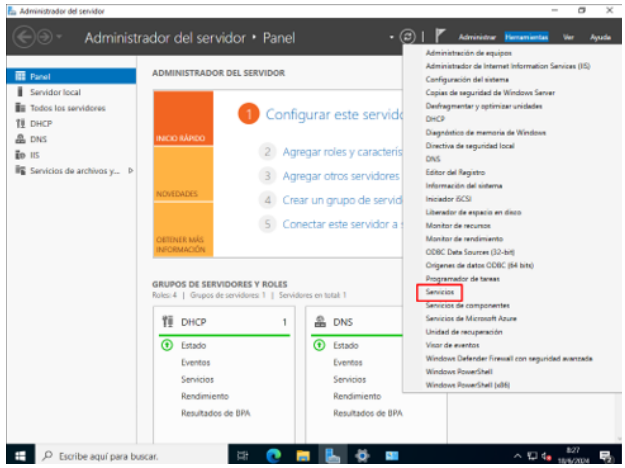


Ilustración 205. Ingresando a la tabla de servicios.

Fuente: Elaboración propia

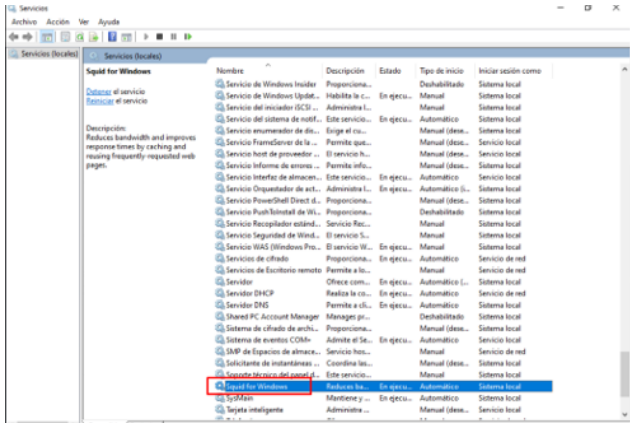


Ilustración 206. Verificación de que el squid este instalado en los servicios.

Fuente: Elaboración propia

Restricción de sitios web

Establecer reglas de control para prohibir el ingreso a algunos sitios web

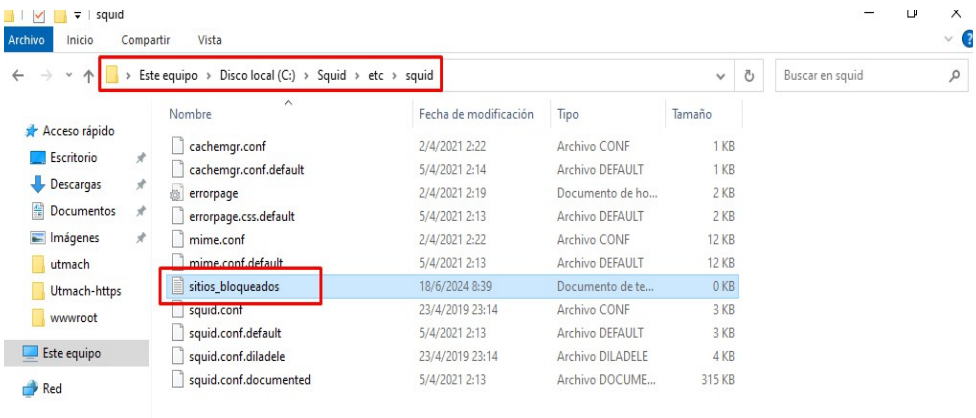


Ilustración 207. Archivo donde se aplicarán los sitios web restringidos.

Fuente: Elaboración propia

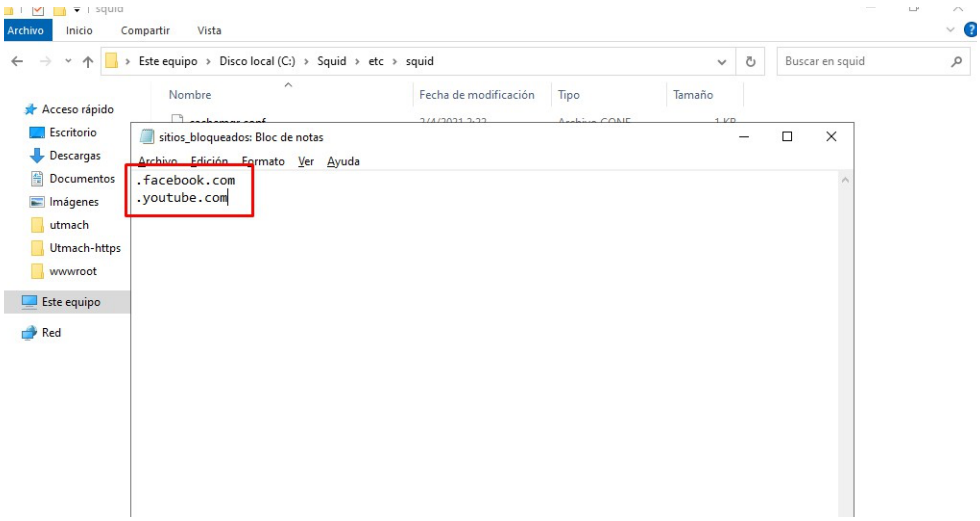


Ilustración 208. Sitios web que se restringirán.

Fuente: Elaboración propia

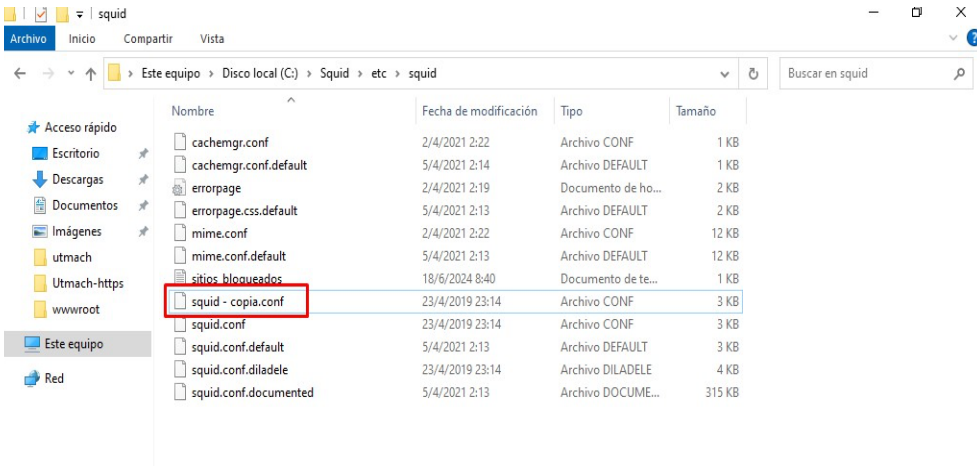


Ilustración 209. Squid.conf archivo donde se configura el proxy.

Fuente: Elaboración propia

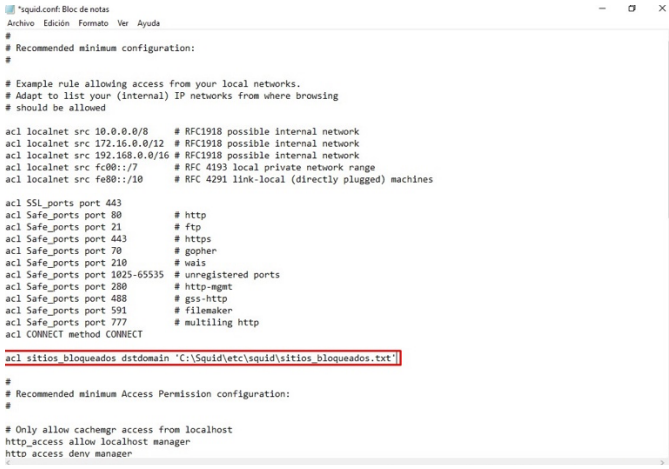


Ilustración 210. Se detalla la ruta donde se encuentra el doc. de los sitios bloqueados.

Fuente: Elaboración propia

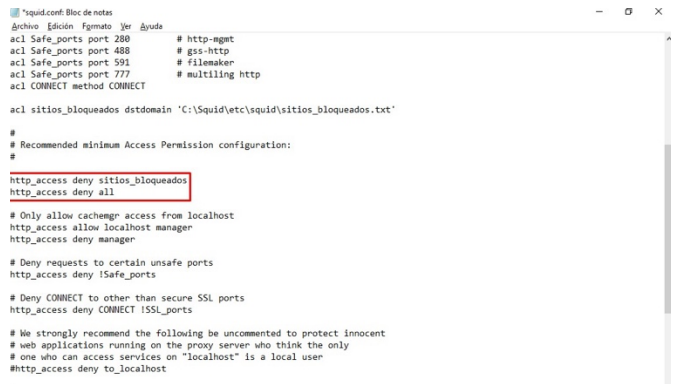


Ilustración 211. Se habilita la restricción de los sitios web.

Fuente: Elaboración propia

A continuación, se configura la dirección IP del servidor proxy con su correspondiente número de puerto en el navegador de internet de la máquina cliente.

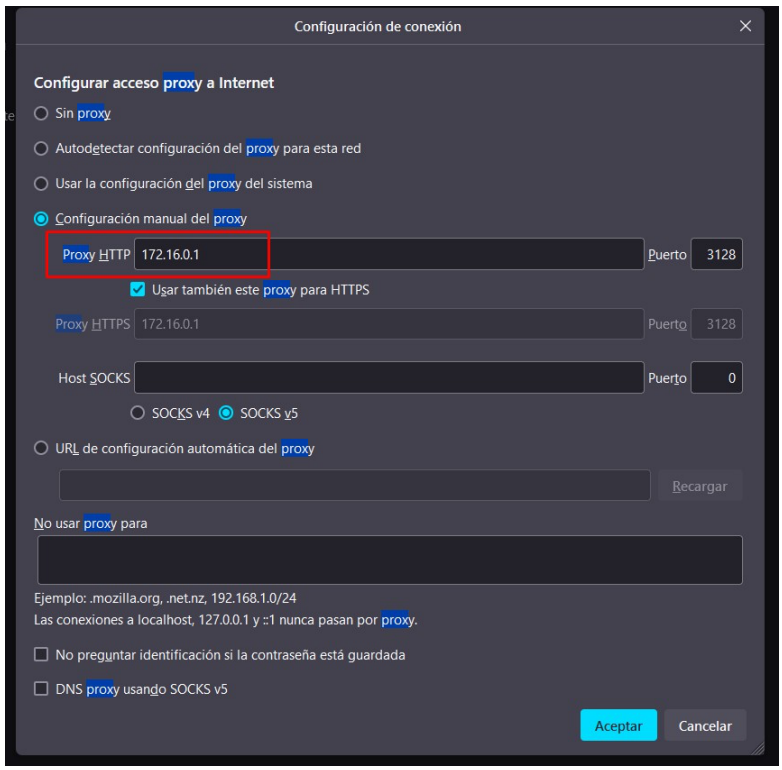


Ilustración 212. Se configura la IP del proxi en el navegador.

Fuente: Elaboración propia

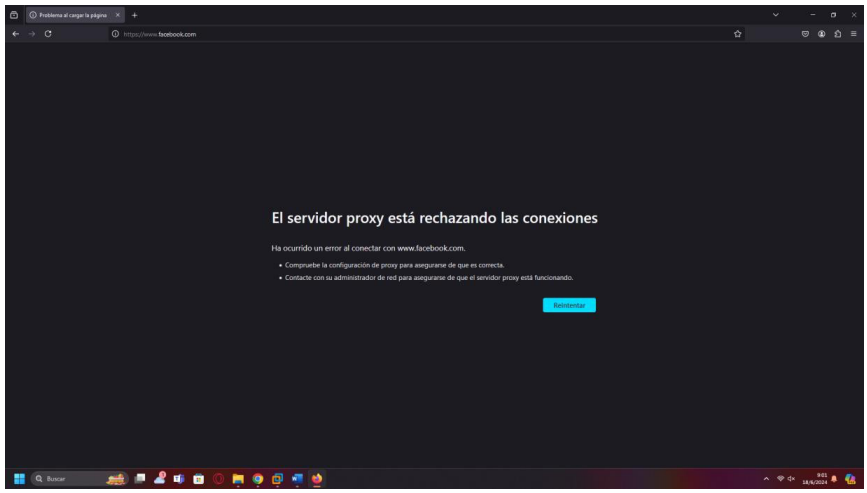


Ilustración 213. El proxi bloquea las páginas restringidas.

Fuente: Elaboración propia

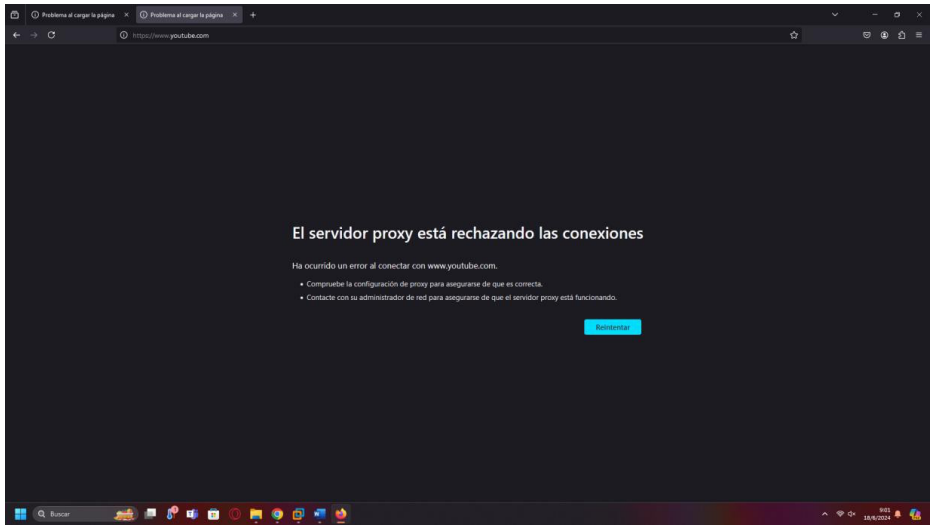


Ilustración 214. El proxi bloquea las páginas restringidas 2.

Fuente: Elaboración propia

Restricción de patrones

Establecer reglas de control para prohibir el ingreso a algunos sitios web mediante búsqueda de patrones.

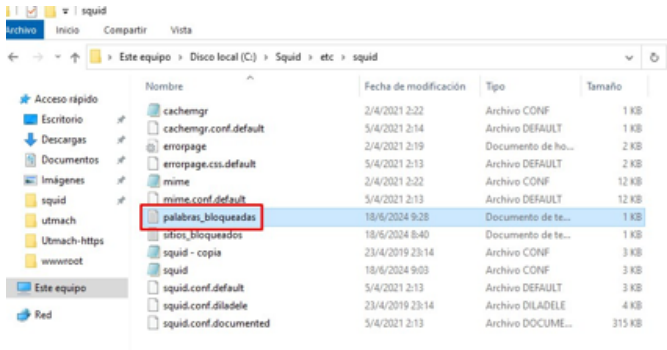


Ilustración 215. Archivo donde se configurarán las palabras bloqueadas.

Fuente: Elaboración propia

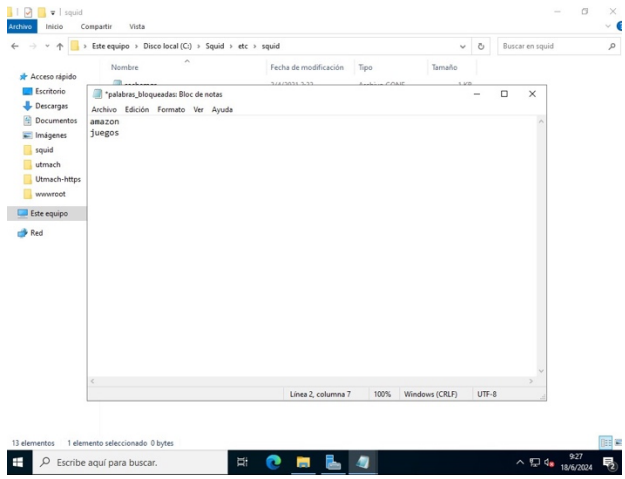


Ilustración 216. Palabras que el proxy bloqueara.

Fuente: Elaboración propia

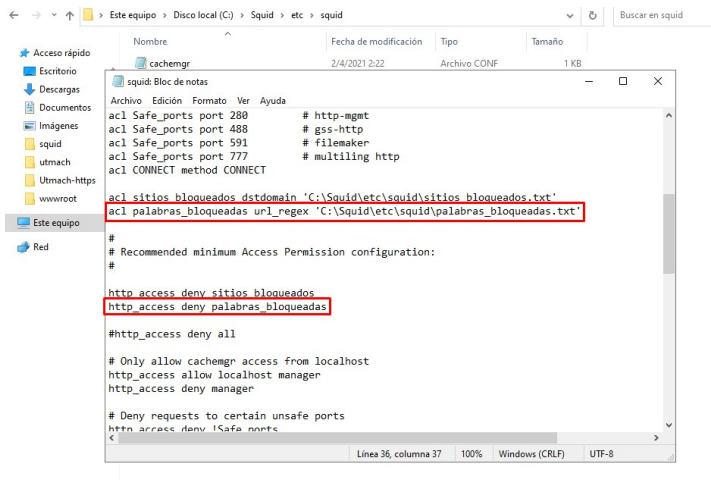


Ilustración 217 Configuración de las palabras bloqueadas en el squid.conf.

Fuente: Elaboración propia

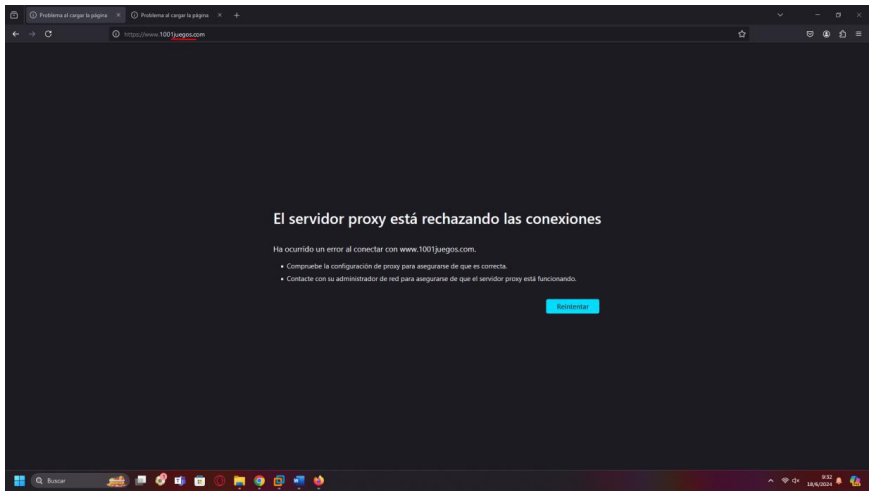


Ilustración 218. El proxi bloquea las palabras configuradas.

Fuente: Elaboración propia

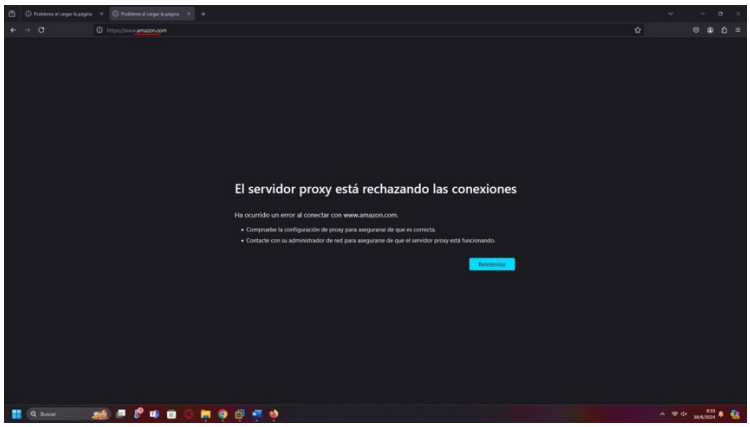


Ilustración 219. El proxi bloquea las palabras configuradas 2.

Fuente: Elaboración propia

Autentificación

Establecer reglas de control para que un usuario se pueda autenticar al momento de ingresar a un sitio controlado por el servidor proxy.

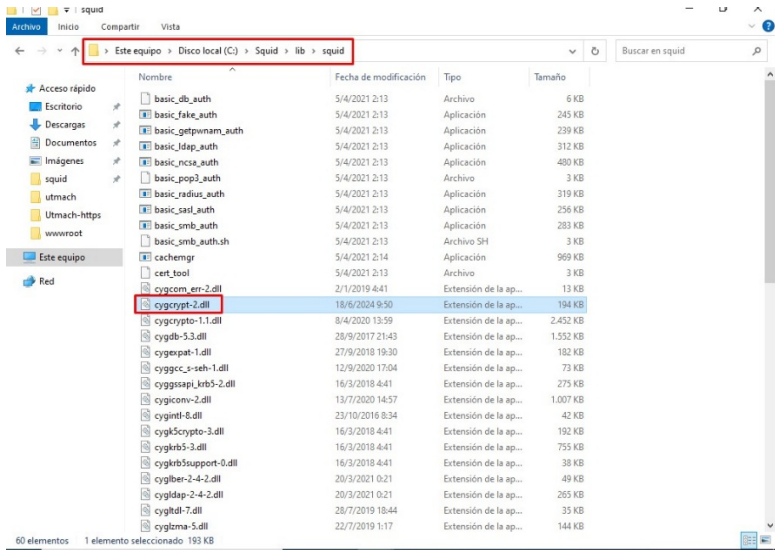


Ilustración 220. Archivo donde se guardan los usuarios.

Fuente: Elaboración propia

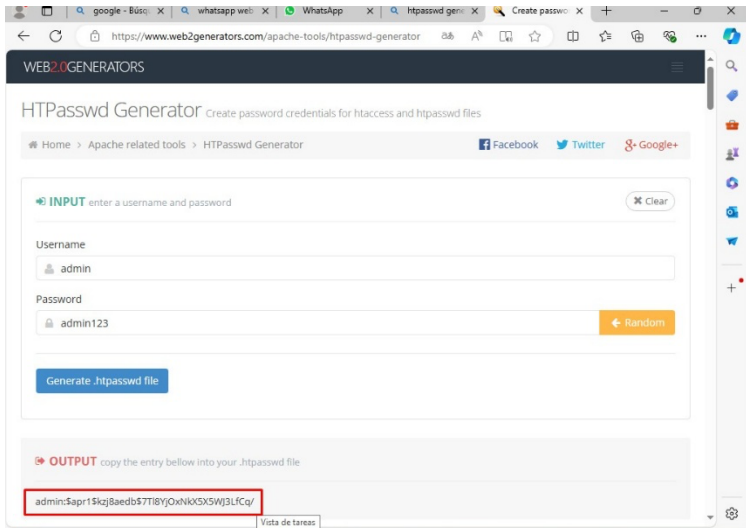


Ilustración 221. Se crea un usuario administrador.

Fuente: Elaboración propia

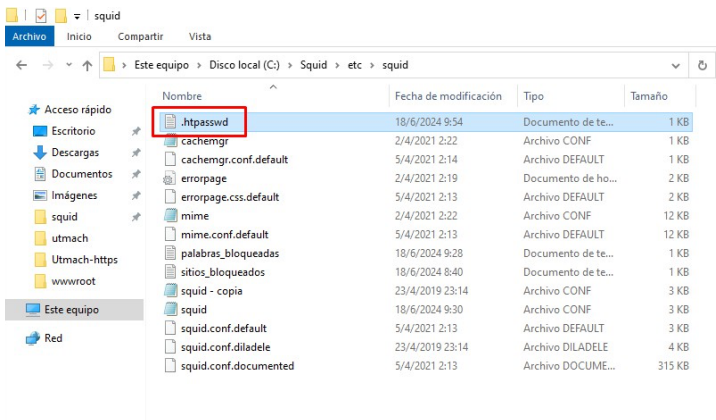


Ilustración 222. Archivo donde se guarda la contraseña del administrador.

Fuente: Elaboración propia

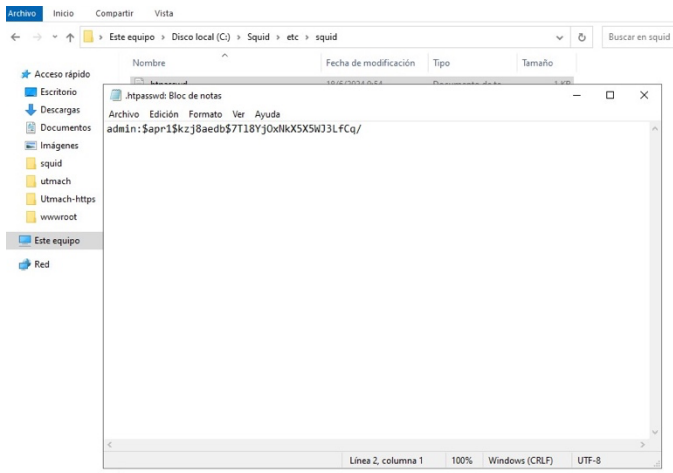


Ilustración 223. La contraseña aparece encriptada.

Fuente: Elaboración propia

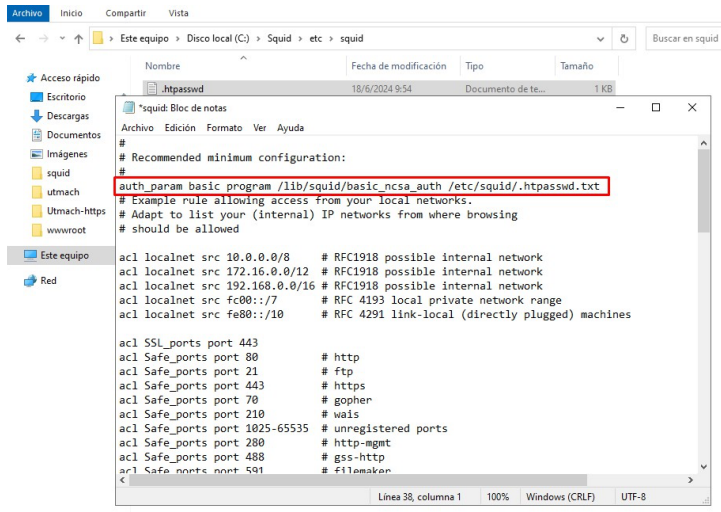


Ilustración 224. Ruta donde la contraseña se encuentra.

Fuente: Elaboración propia

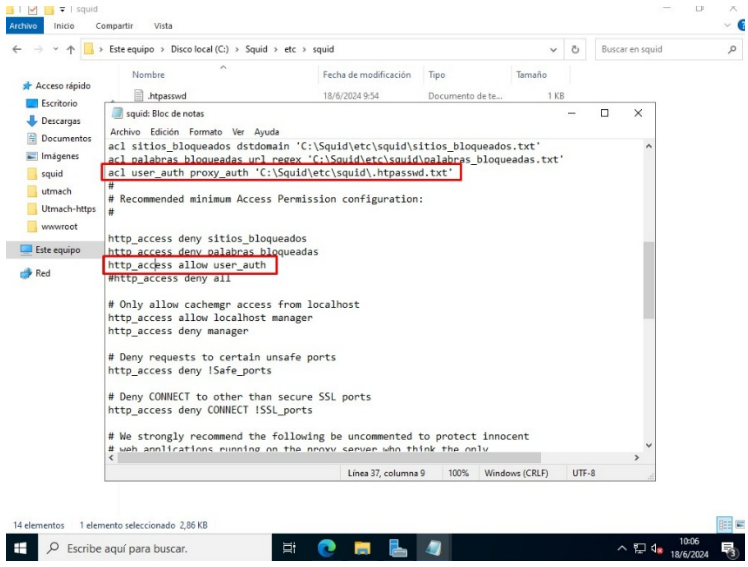


Ilustración 225. Habilita a los usuarios.

Fuente: Elaboración propia

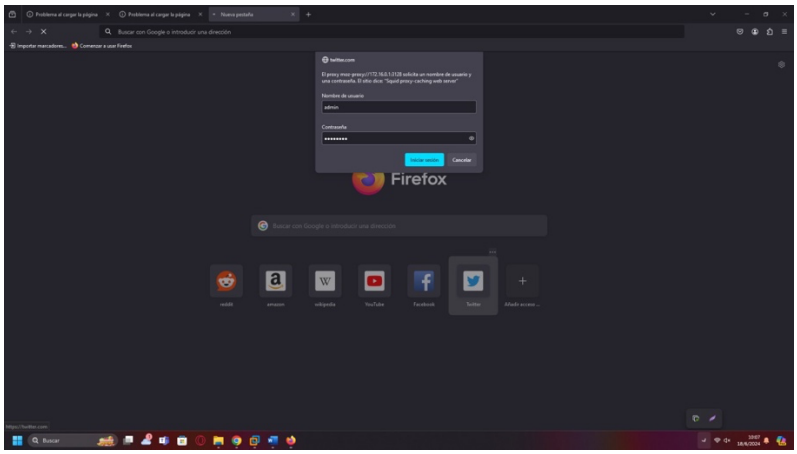


Ilustración 226. El usuario inicia sesión.

Fuente: Elaboración propia

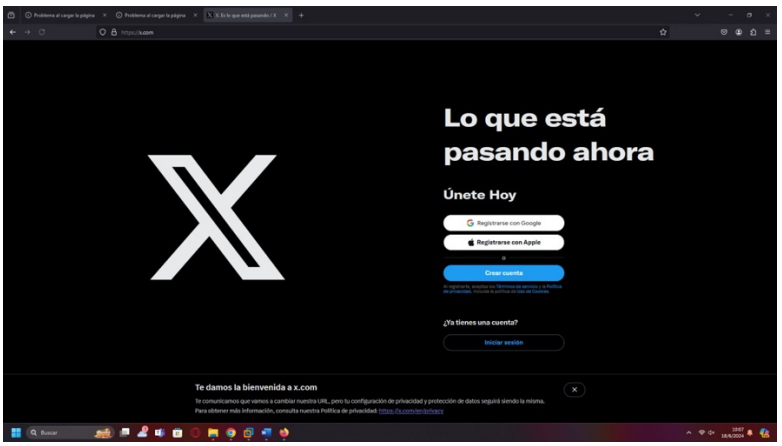


Ilustración 227. Administrador para entrar a las páginas restringidas.

Fuente: Elaboración propia

Restricción de horario

Establecer reglas de control para que un usuario se pueda o no acceder a sitios web a cierta hora del día.

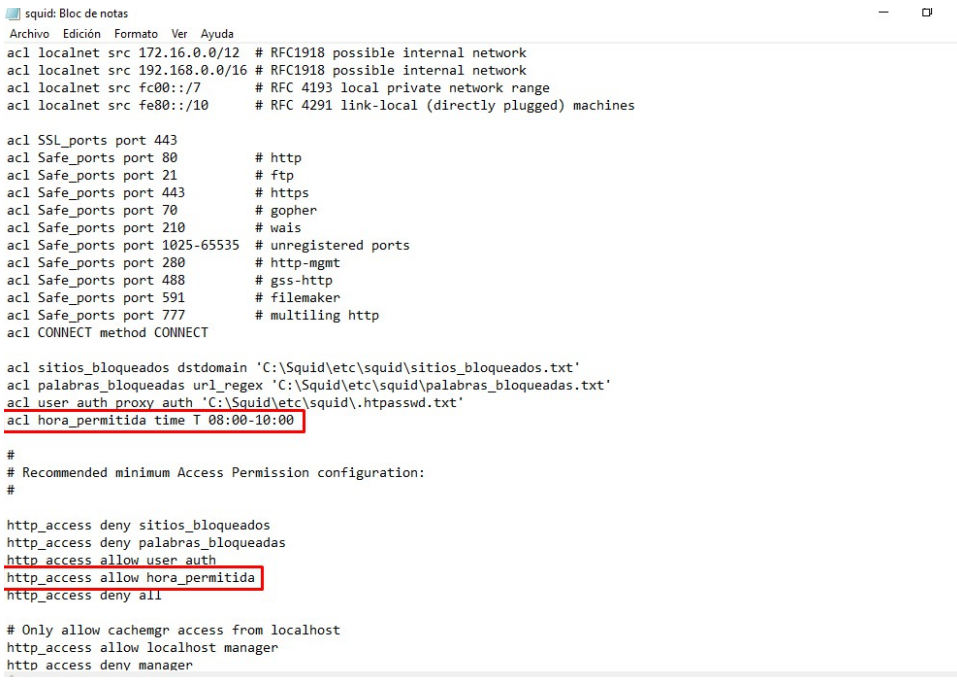


Ilustración 228. Configuración del squid.conf donde se restringe el acceso a ciertas paginas durante un horario.

Fuente: Elaboración propia

Horario permitido de los martes de 08 a 10 Am

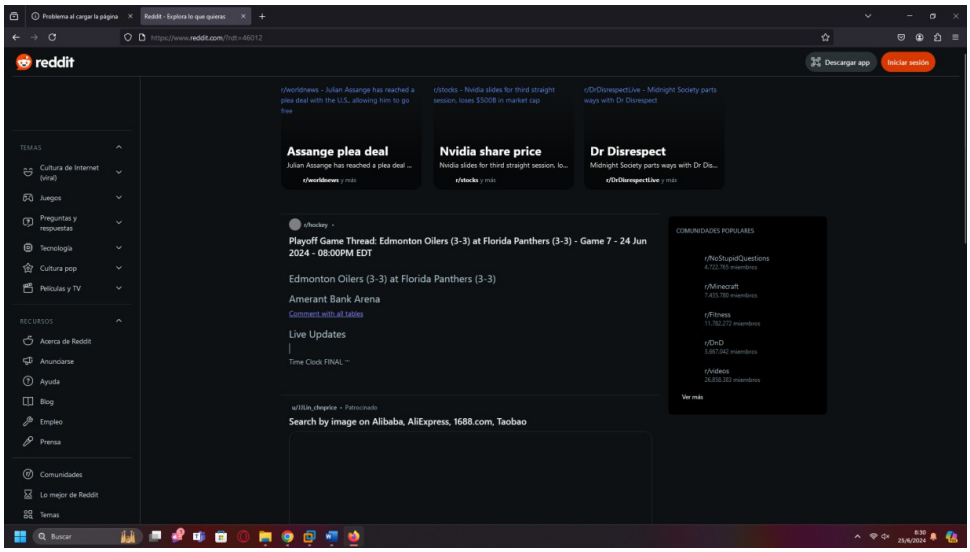


Ilustración 229. El proxy permite el acceso a la página ya que está dentro del horario establecido.

Fuente: Elaboración propia

Horario permitido de los martes de 10 a 11 Am

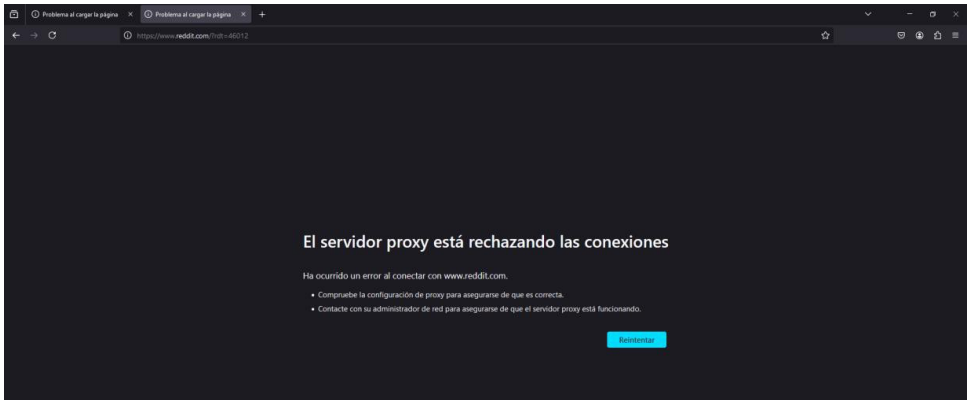


Ilustración 230. El proxy bloquea el acceso a la página ya que esta fuera del horario establecido.

Fuente: Elaboración propia

Restricción por IP

Configurar el servicio proxy para restringir el acceso total, a todos los equipos, me al siguiente rango de direcciones 172.16.50.20, 172.16.50.21, 172.16.50.22 y 172.16.50.23.

Ilustración 231. Se establece el rango de IP que tendrán acceso.

Fuente: Elaboración propia

Verificar en el cliente si el servicio proxy, está ejecutando la regla anteriormente mencionada.

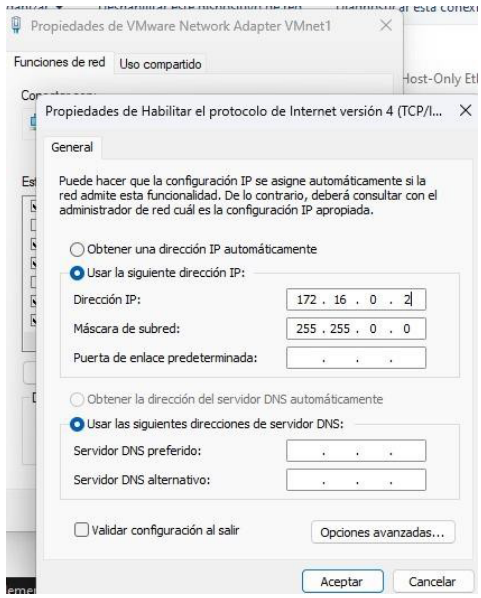


Ilustración 232. Se cambia la IP del cliente.

Fuente: Elaboración propia

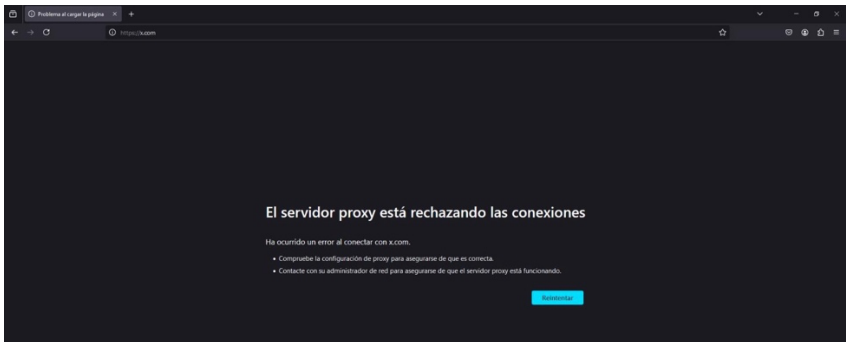


Ilustración 233. El proxy bloquea a la IP no autorizada.

Fuente: Elaboración propia

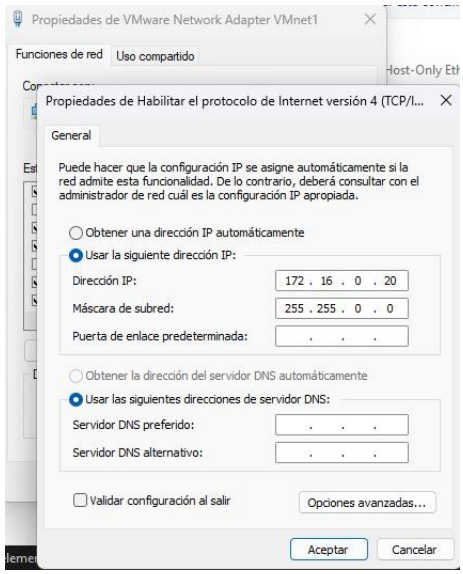


Ilustración 234. Se cambia a una IP que este autorizada.

Fuente: Elaboración propia

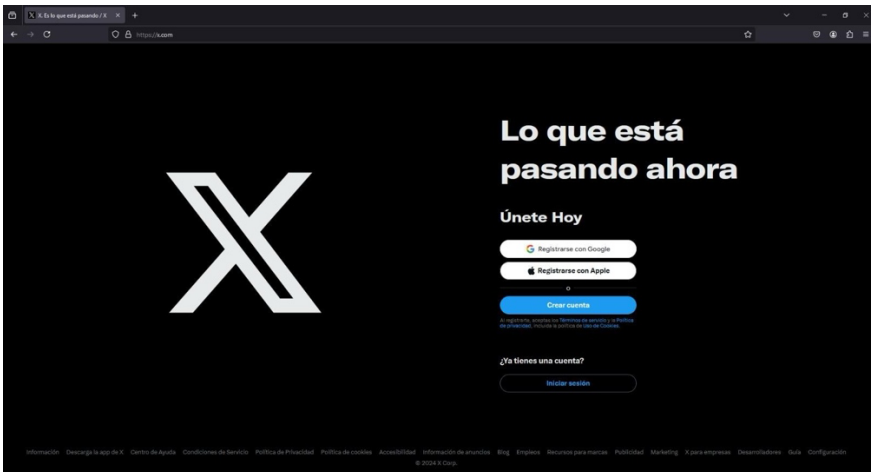


Ilustración 235. Se permite el ingreso a las páginas.

Fuente: Elaboración propia

Restricción por ancho de banda

Configurar el servicio proxy para restringir el ancho de banda total a los equipos con IP 172.16.50.24, 172.16.50.25, 172.16.50.22, 172.16.50.27 y al resto le asigne todo el ancho de banda.

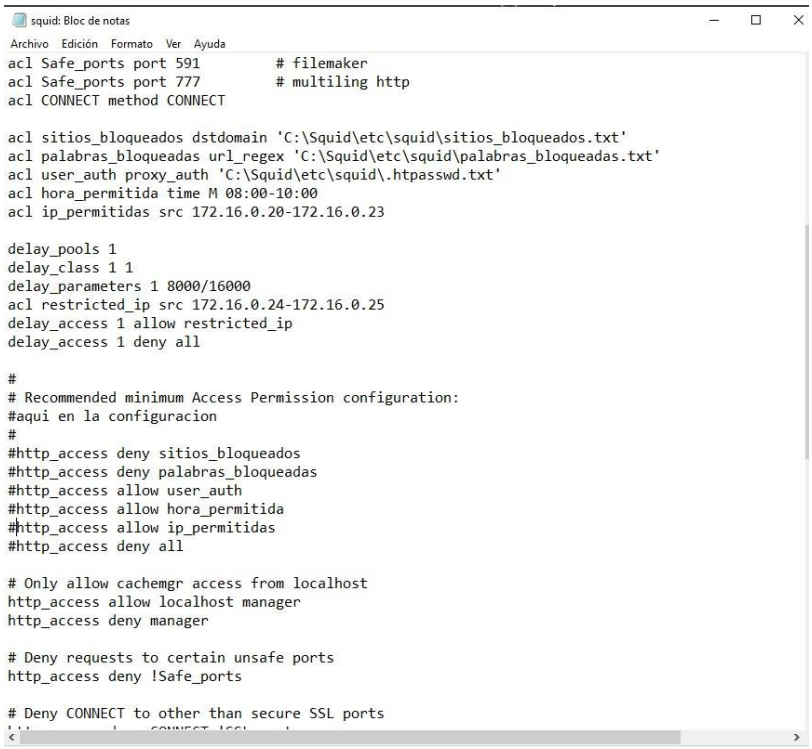


Ilustración 236. Se limita el ancho de banda que reciben los equipos.

Fuente: Elaboración propia

Verificar en el cliente si el servicio proxy, está ejecutando la regla anteriormente mencionada.

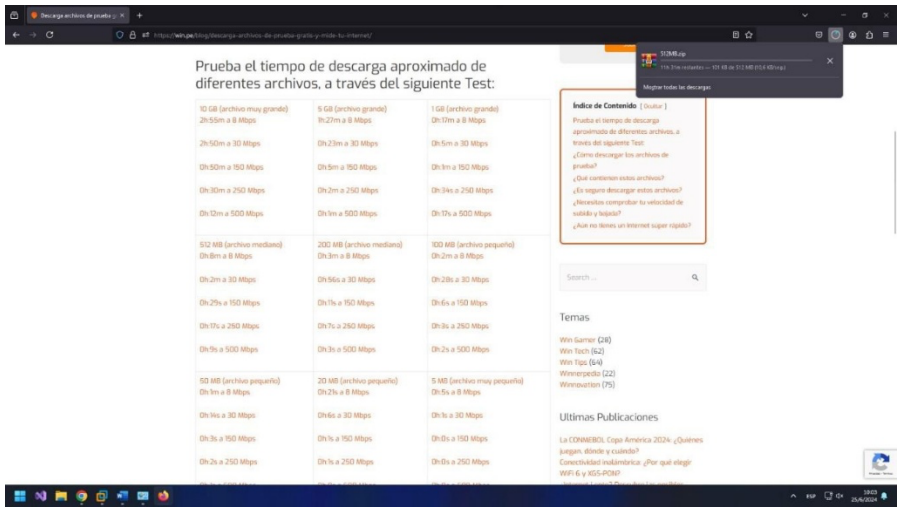


Ilustración 237. El proxy limita el ancho de banda.

Fuente: Elaboración propia

Registros de Logs

Configurar el servicio proxy para registrar las actividades del administrador de almacenamiento.

```
# Leave coredumps in the first cache dir
coredump_dir /var/cache/squid
cache_store_log C:\Squid\var\log\squid\store.log
```

Ilustración 238. Ruta donde se encuentran los logs.

Fuente: Elaboración propia

Verificar desde el cliente se han registrado actividades en los registros log.

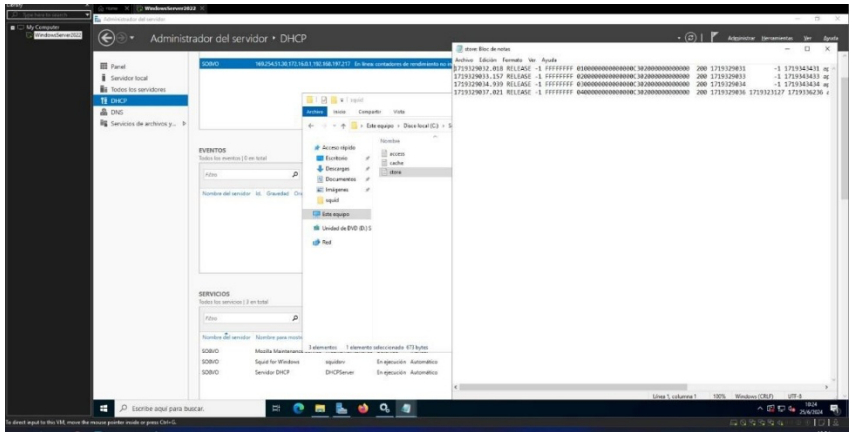


Ilustración 239. Se verifican los logs.

Fuente: Elaboración propia

Mostrar de forma gráfica algunos registros de la red usando ntopng.

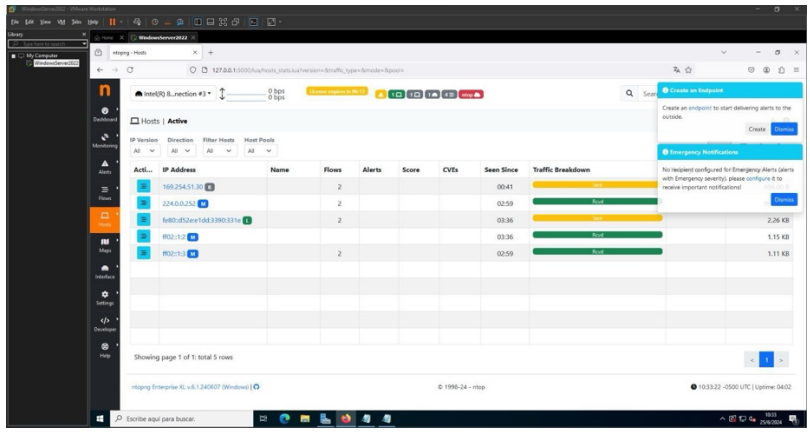


Ilustración 240. Gráfica donde se representan los logs.

Fuente: Elaboración propia

Resumen del Capítulo III

En este capítulo, se introduce el concepto de servidor proxy como intermediario entre el cliente y el servidor de destino, destacando su papel en la mejora de la seguridad, el rendimiento y el control del tráfico en redes. También se explican los principales tipos de proxy: de reenvío, inverso y transparente, cada uno con aplicaciones específicas en entornos corporativos, educativos y públicos. Se detallan los beneficios del uso de proxies, como son: el almacenamiento en caché, el filtrado de contenido, el control de acceso y la optimización de la red, así como los desafíos asociados, como la latencia, la seguridad, la compatibilidad y la necesidad de mantenimiento constante. El capítulo se enfoca en la implementación práctica de un software de código abierto para servidores proxis como es el Squid, entre las diversas configuraciones que se presentan tenemos: restricciones de sitios web, bloqueo de palabras por patrones, autenticación de usuarios, control de acceso por horarios y registro de actividades o logs. Se guía al lector en la instalación, configuración y verificación del servicio, incluyendo pruebas de conectividad entre cliente y servidor.

Preguntas de Revisión

Evaluación de Conocimientos Adquiridos

1. Entendimiento de Conceptos Básicos:

- Defina con claridad qué es un servidor proxy y explique su función dentro de una red empresarial. Si no puede hacerlo con seguridad, investigue más sobre el tema y redacte un breve resumen que incluya sus principales usos.
- Describa los diferentes tipos de servidores proxy y los beneficios que ofrecen. Considere elaborar un esquema comparativo que muestre sus funciones y aplicaciones prácticas.

2. Habilidades Prácticas:

- Evalúe su capacidad para instalar y configurar un servidor proxy utilizando herramientas como Squid, Nginx o Apache Traffic Server. Si encuentra dificultades, detalle qué aspectos necesita revisar o aprender con mayor profundidad.
- Reflexione sobre su habilidad para establecer políticas de filtrado, reglas de acceso y caché. Prepare una lista de pasos para configurar un proxy funcional que incluya monitoreo básico y control de acceso.

3. Aplicación de Políticas de Seguridad

- Explique cómo aplica y administra medidas de seguridad en un servidor proxy, tales como el anonimato, el filtrado de contenido y la restricción de sitios web. Si este proceso le resulta complejo, identifique qué recursos podrían ayudarle a mejorar.

- Discuta cómo implementa y verifica políticas de control de acceso y registro del tráfico en la red. Cree una lista de verificación para garantizar la privacidad y seguridad en la navegación de los usuarios.

4. Resolución de Problemas:

- Diagnostique y resuelva un problema común relacionado con la conexión o el filtrado en un servidor proxy. Documente el procedimiento utilizado y reflexione sobre los pasos tomados y los resultados obtenidos.
- Realice una tarea de mantenimiento, como la limpieza de la caché o la actualización de reglas de acceso. Describa el procedimiento y evalúe la mejora obtenida en el rendimiento o la seguridad del proxy.

Autoevaluación Personal

1. Reflexión sobre el Aprendizaje:

- Identifique los aspectos más desafiantes de la configuración y administración de un servidor proxy. Explique por qué representan una dificultad y proponga una estrategia para abordarlos.
- Determine qué recursos adicionales (documentación técnica, laboratorios prácticos, tutoriales) necesita para profundizar su conocimiento en la implementación y gestión de servidores proxy.

2. Plan de Mejora Continua:

- Establezca los próximos pasos en su plan de aprendizaje para dominar el uso de servidores proxy. Esto puede incluir prácticas adicionales, simulaciones en entornos reales o el desarrollo de un proyecto específico.
- Investigue qué certificaciones o cursos están disponibles relacionados con redes y seguridad informática (por ejemplo, Cisco CCNA, CompTIA Network+ o Fortinet NSE). Haga una lista de opciones y fije objetivos concretos para alcanzarlas.

Referencias bibliográficas

Microsoft. (2023). *¿Qué es un proxy?*. Microsoft Learn. https://learn.microsoft.com/es-es/microsoft-cloud/dev/dev-proxy/concepts/what-is-proxy

Fortinet. (2023). *¿Qué es un servidor proxy? Definición, usos y más*. https://www.fortinet.com/lat/resources/cyberglossary/proxy-server

Hoces-Moral López, I. (2019). *Sistema proxy-web con filtrado y control de acceso* [Trabajo final de grado, Universitat Oberta de Catalunya]. Universitat Oberta de Catalunya. https://openaccess.uoc.edu/bitstream/10609/94506/6/ihocesmoralTFG0619memoria.pdf

Gómez Montoya, C., Sepúlveda Rodríguez, L., & Candela Uribe, C. (2012). *Servidor proxy caché: comprensión y asimilación tecnológica*. INGE CUC, 8(2), 45–56. https://repositorio.cuc.edu.co/bitstreams/98345a3e-e36c-4fcc-b17e-06ebabdf461c/download

Senteno, J., Polanía, C., & Pulido, C. (2019). *Propuesta de interceptor proxy como modelo de acceso seguro a un entorno web, para el Consorcio Infraestructura Educativa 2016* [Trabajo de grado, Universidad Cooperativa de Colombia]. https://repository.ucc.edu.co/server/api/core/bitstreams/c2bdd4a6-2492-4e2b-9ede-e312a47a19f6/content

Microsoft. (2024, marzo 14). *Crear un proxy de reenvío mediante el enrutamiento de solicitud de aplicaciones*. Microsoft Learn. https://learn.microsoft.com/es-es/iis/extensions/configuring-

application-request-routing-arr/creating-a-forward-proxy-using-application-request-routing

Hassel, K. (2025, marzo 27). *¿Qué es un proxy transparente? Una guía completa*. ExpressVPN. https://www.expressvpn.com/blog/transparent-proxy/

Microsoft. (2025, marzo 12). *Proxy transparente para Azure Stack Hub*. Microsoft Learn. https://learn.microsoft.com/es-es/azure-stack/operator/azure-stack-transparent-proxy?view=azs-2102

Wallarm. (2025). *¿Qué es un proxy transparente?*. https://www.wallarm.com/what/what-is-a-transparent-proxy

Maskat, K., Mohd Isa, M., Khairuddin, M., & Kamarudin, N. (2025). Enhancing the server-side internet proxy detection technique in [Título completo del artículo]. *JOIV: International Journal on Informatics Visualization*, 9(2). https://doi.org/10.62527/joiv.9.2.3410

Rashid, A. (2022). Proxy servers and their applications in modern network security. *International Journal of Information Security*, *21*(2), 159–175.

IONOS. (2020, 25 de septiembre). *Squid: el servidor proxy-caché de código abierto*. IONOS. https://www.ionos.es/digitalguide/servidores/configuracion/squid-el-servidor-proxy-cache-de-codigo-abierto/

CAPÍTULO 4

ADMINISTRACIÓN DEL SERVICIO DE ACTIVE DIRECTORY

Introducción a Active Directory

Objetivos

Configurar el servidor de Active Directory para la gestión de recursos de red en la máquina cliente.

Objetivos

Configurar el servidor de Active Directory para establecer un dominio de red funcional que permita la gestión centralizada de recursos, como usuarios, equipos, impresoras y aplicaciones.

Implementar políticas de seguridad y permisos en el servidor de Active Directory para garantizar un acceso controlado y seguro a los recursos de red por parte de los usuarios y equipos autorizados.

Un directorio representa una estructura organizativa jerárquica destinada a almacenar y gestionar datos relativos a los objetos presentes en una red. Un servicio de directorio, tal como Active Directory Domain Services (AD DS), proporciona los medios necesarios para almacenar estos datos de manera efectiva y ponerlos a disposición de los usuarios y administradores de la red. Por ejemplo, AD DS conserva información relativa a las cuentas de usuario, incluyendo nombres, contraseñas y números de teléfono, y permite a otros usuarios autorizados en la misma red acceder a dicha información.

Active Directory constituye un repositorio central de información acerca de los objetos presentes en una red, facilitando su búsqueda y utilización por parte de los usuarios y administradores. Para ello,

hace uso de un almacén de datos estructurado como base para la organización lógica y jerárquica de la información del directorio.

Este almacén de datos, comúnmente denominado directorio, alberga información acerca de los objetos presentes en Active Directory. Estos objetos típicamente comprenden recursos compartidos tales como servidores, volúmenes, impresoras, así como cuentas de usuario y equipo de red.

La seguridad en Active Directory se incorpora mediante la autenticación en el inicio de sesión y el control de acceso a los objetos presentes en el directorio. Gracias a un único inicio de sesión en la red, los administradores pueden gestionar los datos del directorio y la estructura organizativa en toda la red, mientras que los usuarios autorizados pueden acceder a los recursos disponibles en cualquier punto de la misma. La administración basada en políticas simplifica la gestión incluso en entornos de red de gran complejidad.

Preguntas de enfoque

Preguntas de Inicio

1. ¿Qué es Active Directory y por qué es fundamental para la gestión de redes en una organización?
2. ¿Cuáles son los principales componentes de Active Directory y qué funciones desempeñan?
3. ¿Cómo puede Active Directory mejorar la seguridad y la eficiencia en la administración de usuarios y recursos?

Competencias o Problemas a Resolver

Al finalizar este capítulo, los lectores serán capaces de:

- Comprender y explicar la estructura y los conceptos básicos de Active Directory.
- Configurar y administrar usuarios, grupos y unidades organizativas dentro de Active Directory.
- Implementar políticas de grupo para gestionar configuraciones y mejorar la seguridad de la red.

Problemas a Resolver

1. ¿Cómo se puede diseñar una estructura de Active Directory que soporte de manera eficiente el crecimiento de una organización?
2. ¿Qué estrategias pueden utilizarse para optimizar la replicación y la redundancia de datos en un entorno con múltiples dominios?
3. ¿Cómo se pueden aplicar políticas de seguridad mediante Active Directory para proteger datos sensibles?

Active Directory

Concepto de Active Directory

Active Directory Domain Services (AD DS) es una solución de Microsoft que actúa como un servicio de directorio centralizado, diseñado para almacenar, organizar y facilitar el acceso seguro a la información de los objetos en una red, como cuentas de usuario, contraseñas, equipos, impresoras y servidores. Esta información se gestiona a través de una estructura lógica y jerárquica basada en un directorio, lo que permite una administración eficiente tanto para usuarios como para administradores. Uno de sus principales pilares es la seguridad: AD DS emplea autenticación de inicio de sesión y control de acceso a los objetos del sistema, garantizando que solo los usuarios autorizados puedan acceder a los recursos. Además, los administradores pueden aplicar configuraciones y políticas de forma centralizada en todo el dominio, lo cual facilita el manejo de entornos complejos.

Active Directory Domain Services (AD DS) también incorpora varios elementos clave:

- El esquema, que es un conjunto de normas que establece qué tipos de objetos y atributos pueden existir en el directorio, así como las restricciones aplicables y el formato que deben tener los nombres de estos objetos.
- El catálogo global, el cual almacena información sobre todos los objetos dentro del directorio, permitiendo a usuarios y administradores localizar datos sin importar en qué dominio se encuentren almacenados.
- Un sistema de consulta e indexación, que permite que los objetos del directorio y sus propiedades se publiquen y sean

fácilmente localizables por usuarios o aplicaciones dentro de la red.

- Un servicio de replicación, encargado de distribuir la información del directorio entre los distintos controladores de dominio de una red. Cada uno de estos controladores conserva una copia completa de los datos del dominio, y cualquier modificación se propaga automáticamente a todos ellos (Microsoft, 2025).

Funcionamiento de Active Directory

El Active Directory (AD) funciona de forma similar a una base de datos, en la que se almacena todo tipo de datos de usuarios para poder identificarlos dentro de la red. Cada usuario está debidamente identificado con sus propios atributos como: el nombre, apellidos, correo, etc. Este usuario estará dentro de uno o varios grupos administrados por el AD, con sus propios privilegios y permisos previamente delimitados. Así, cuando el usuario inicia

sesión en su equipo con sus propias credenciales, será el AD quien confirme que es correcto verificando las

mismas y dándole acceso a los recursos, archivos y demás a los que tiene permiso (Ymant, 2025).

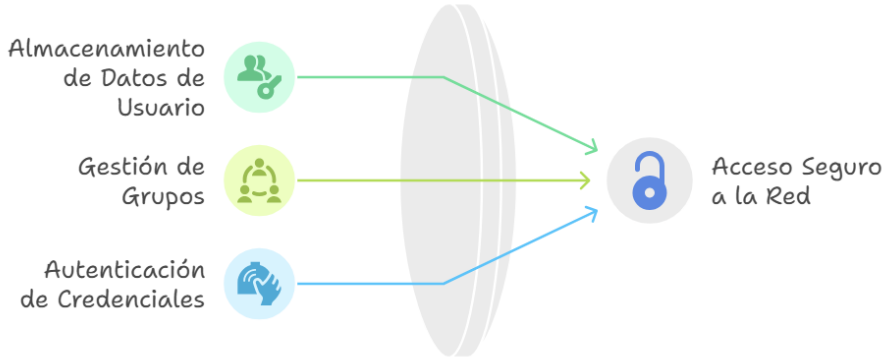


Ilustración 241. Autenticación con Active Directory.

Fuente: Elaboración propia

Estructura de Active Directory

Según Tecnozero (2025) y Castillo (2018), existen distintos elementos que se deben de conocer en Active Directory como:

Objeto

Un objeto es el nombre genérico que utilizamos para referirnos cualquier componente dentro de un directorio. Los objetos se dividen en tres tipos distintos:

- Recursos: elementos a los que cada usuario podrá acceder según sus permisos, como por ejemplo impresoras, equipos, entre otros.
- Servicios: son las funcionalidades a las que cada usuario puede acceder, por ejemplo, el correo electrónico, Web, FTP, etc.
- Usuarios: credencias de acceso a estaciones de trabajo y toda la información necesaria de los mismos (incluyen cuentas para conectarse, grupos de trabajo), etc.

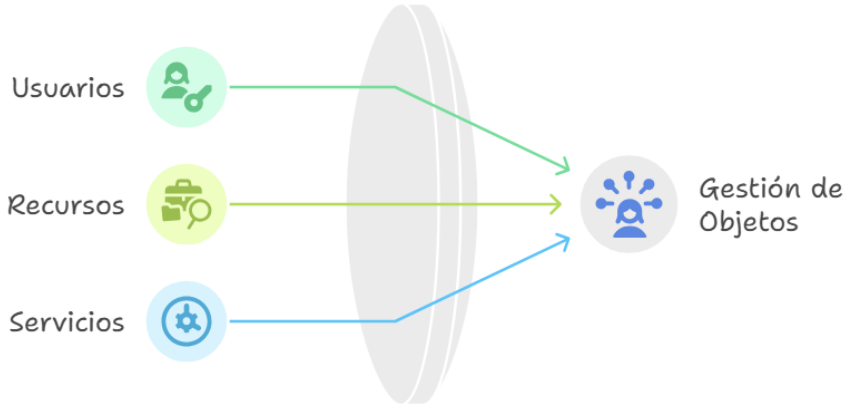


Ilustración 242. Objetos.

Fuente: Elaboración propia

Dominio

Los dominios en Active Directory permiten organizar objetos relacionados de forma que representen la estructura de red de una organización. Son elementos clave dentro de la estructura lógica del sistema, ya que agrupan objetos administrativos que comparten una misma base de datos, políticas de seguridad y vínculos de confianza con otros dominios. Active Directory también es un controlador de dominio, ya que podemos crear distintos dominios y gestionar lo permisos e interacción en cada uno de ellos. A esta relación entre dominios se le denomina relación de confianza o trust (Castillo, 2018).

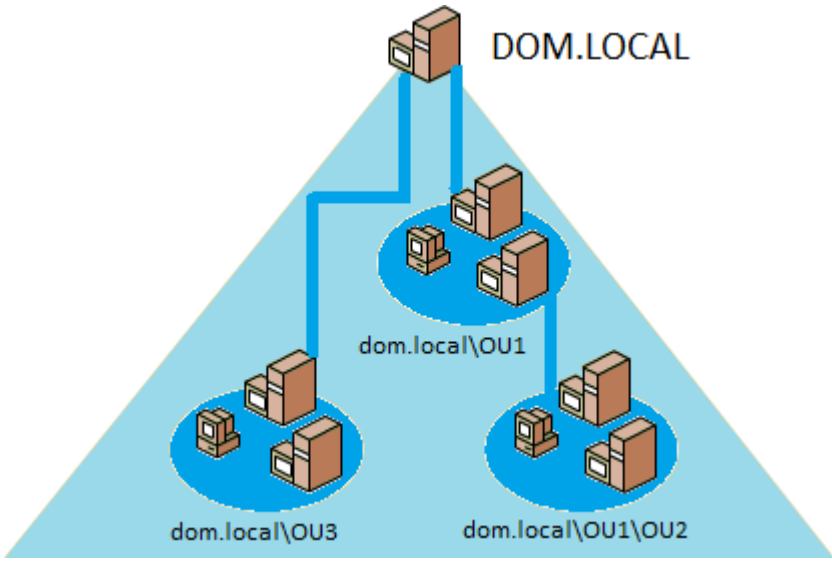


Ilustración 243. Dominio

Fuente: Tomado de (Pantallazos.es, 2015)

Controlador de dominio

Un controlador de dominio es el servidor que almacena la base de datos con los objetos del directorio pertenecientes a un dominio específico, incluyendo datos relacionados con la seguridad. Su función principal es autenticar a los objetos bajo su administración, permitiendo acciones como el inicio o cierre de sesión y la consulta de información en el directorio. En un mismo dominio pueden existir múltiples controladores de dominio, cada uno con funciones específicas, aunque todos poseen igual jerarquía operativa. Al

instalar Active Directory en un equipo con Windows Server, este pasa a desempeñar el rol de controlador de dominio (Ruiz, 2021).

Ilustración 244. Controlador de Dominio

Fuente: Tomado de (Mantenimiento IV, 2025)

Unidades organizativas

Una Unidad Organizativa (OU) actúa como un contenedor que agrupa objetos dentro de un dominio, permitiendo organizarlos en subconjuntos jerárquicos. Esta organización facilita la creación de una estructura lógica que refleje la forma en que está distribuida una empresa, haciendo más sencilla su administración. Además, las OU ofrecen la ventaja de permitir delegar total o parcialmente el control sobre los objetos que contienen a otros usuarios o grupos, lo cual es especialmente útil en entornos de red extensos. Como objeto contenedor más habitual, las OU sirven para estructurar otros elementos con fines administrativos, como dividir una organización en departamentos, facilitando así su gestión y localización. También es posible asignar a diferentes personas la administración de cada unidad organizativa. Su representación esquemática es mediante una carpeta y sigue un árbol jerárquico,

al igual que las carpetas del sistema de archivos de Windows. (Ruiz, 2021).

Ilustración 245. Controlador de Dominio

Fuente: Tomado de (Seguridad Informática y Sistemas Operativos en Red, 2015)

Árbol

Un árbol en Active Directory es un conjunto de dominios relacionados que comparten una raíz común y están organizados jerárquicamente. Esta estructura también se refleja mediante un espacio de nombres DNS compartido. La finalidad de este diseño es dividir la información del Directorio Activo para que solo se repliquen los datos esenciales, optimizando así el uso del ancho de banda en la red. Cuando se crea un usuario en un dominio específico, dicho usuario es automáticamente reconocido por

todos los dominios subordinados dentro de esa jerarquía (Ruiz, 2021).

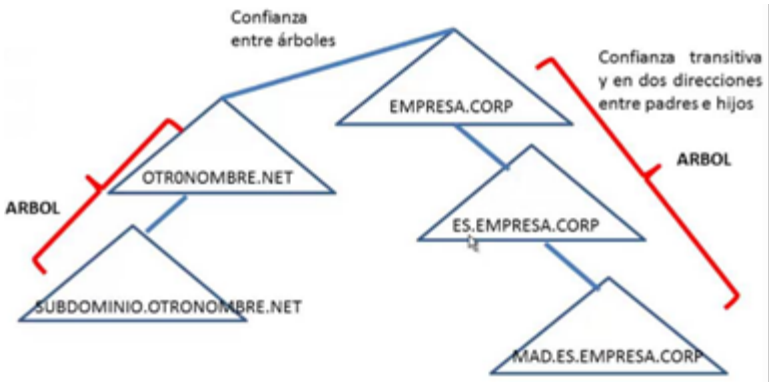


Ilustración 246. Controlador de Dominio

Fuente: Elaboración propia

Bosque

Un bosque en Active Directory agrupa todos los dominios que lo componen, cada uno con relaciones de confianza configuradas automáticamente pero también ajustables según las necesidades del administrador. Dentro de un bosque pueden existir múltiples árboles de dominio con nombres distintos. Al instalar el primer dominio en un servidor con Windows Server, no solo se establece la raíz de un árbol, sino también la raíz del bosque. El bosque representa el nivel más alto de organización lógica en Active Directory, englobando todos los dominios que lo integran. Así, el primer dominio instalado se convierte en el dominio raíz tanto del árbol como del bosque (Ruiz, 2021; Castillo, 2018).

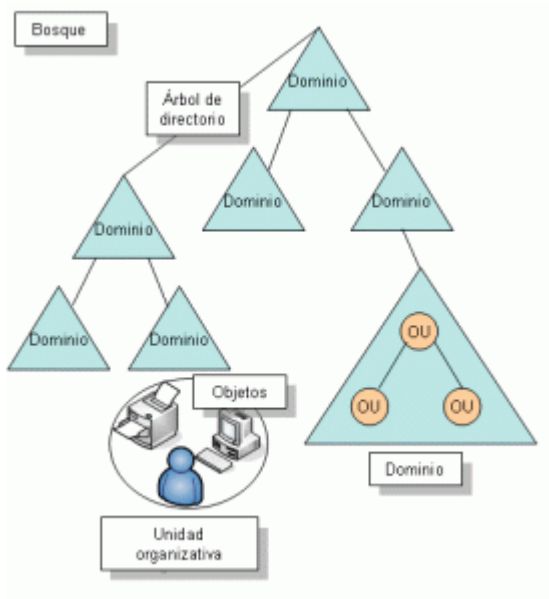


Ilustración 247. Controlador de Dominio

Fuente: Tomado de (alumnosaso201415, 2015)

. Caso Práctico 1: Instalación, Configuración y Administración de Active Directory en Windows Server

Descripción de la práctica: Esta práctica consiste en la instalación y configuración del servicio de Active Directory en un entorno de Windows Server, utilizando un ambiente cliente-servidor. El principal enfoque es familiarizar a los estudiantes con los pasos necesarios para instalar y configurar Active Directory Domain Services (AD DS), configurar un dominio, y administrar unidades organizativas y usuarios dentro de este entorno. Los estudiantes llevarán a cabo la configuración inicial del servidor y del cliente, asegurándose de que el sistema cliente pueda unirse correctamente al dominio y verificando la funcionalidad del AD mediante diversas pruebas de conectividad y configuración.

Realizar una configuración TCP/IP estática entre el cliente y el servidor.

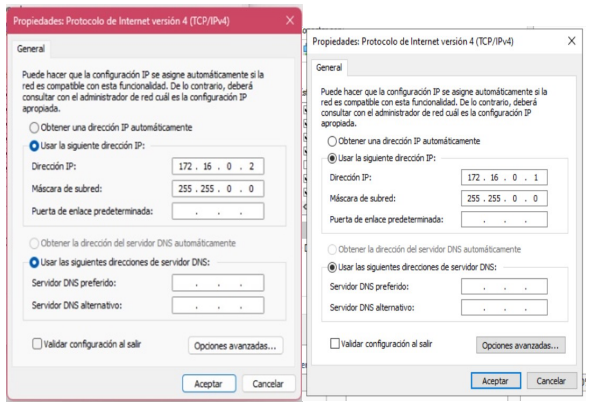


Ilustración 248. Asignación de IP estática al adaptador de red servidor y cliente

Fuente: Elaboración propia

Realizar pruebas de conectividad entre el cliente y el servidor mediante el comando ping

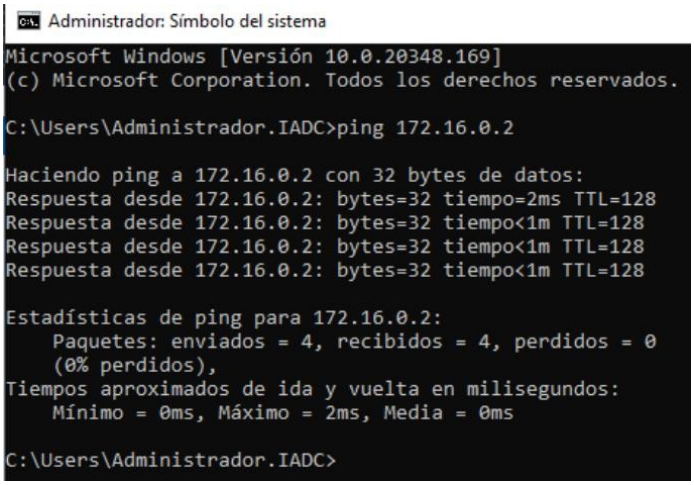


Ilustración 249. Prueba de conectividad.

Fuente: Elaboración propia

Servidor

Configuración de Active Directory en Windows Server 2022

Instalar el servicio de Active Directory Domain Services (AD DS), para ello acceder al Administrador del Servidor.

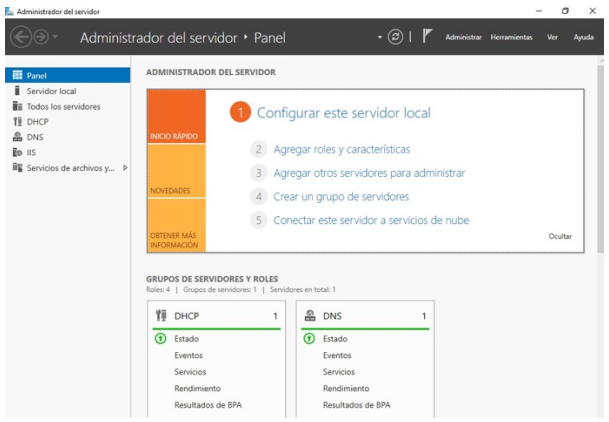


Ilustración 250. Administrador de Active Directory.

Fuente: Elaboración propia

Seleccionar "Agregar roles y características" y elegir "Instalación basada en característica

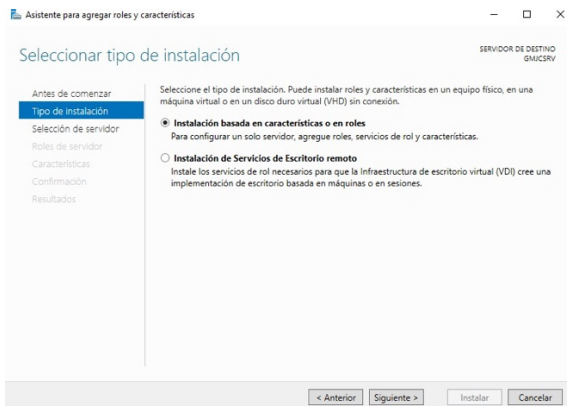


Ilustración 251. Selección del tipo de instalación.

Fuente: Elaboración propia

Seleccionar el servidor y marcar "Servicios de dominio de Active

Directory".

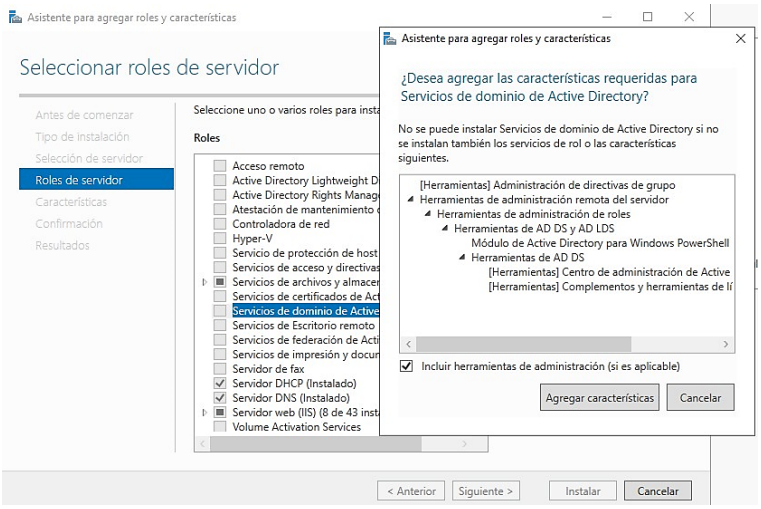


Ilustración 252. Selección de servicios de AD.

Fuente: Elaboración propia

Ahora, continuamos con la instalación.

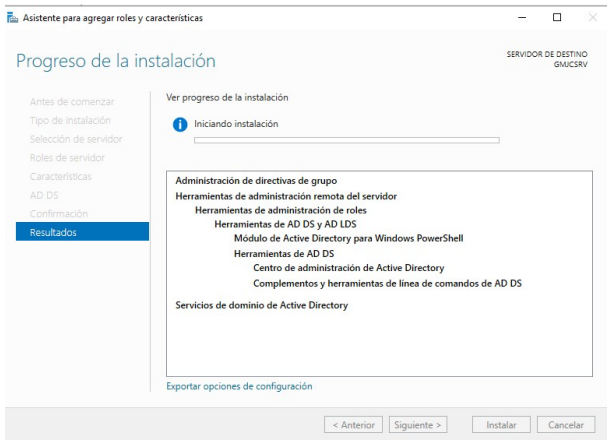


Ilustración 253. Proceso de instalación AD

Fuente: Elaboración propia

Configurar el dominio de Active Directory, para ello promover el servidor a controlador de dominio.

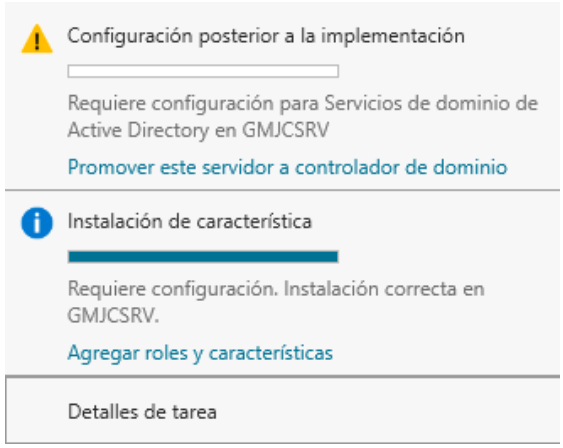


Ilustración 254. Promover el servidor a controlador de dominio

Fuente: Elaboración propia

Seleccionar "Agregar un nuevo bosque" e ingresar el nombre del dominio raíz.

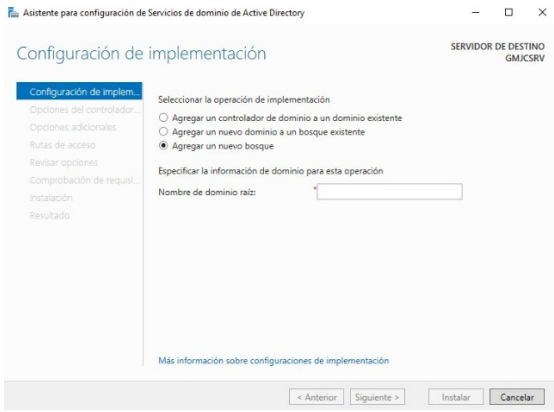


Ilustración 255. Agregar nuevo bosque

Fuente: Elaboración propia

Escribimos un nombre para el directorio raíz, en este caso de ejemplo: utmach.edu.ec

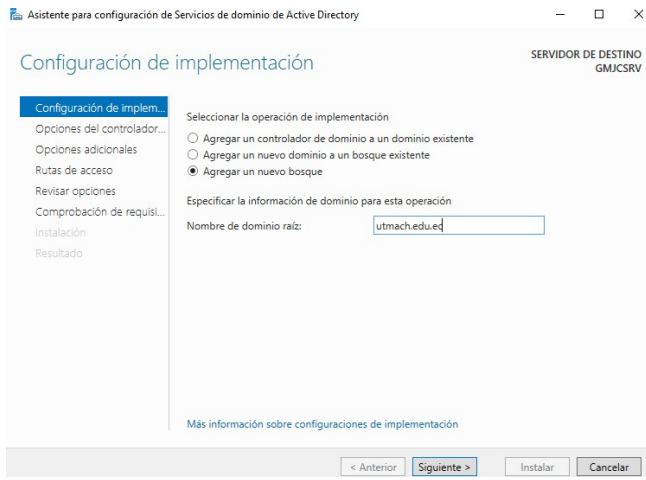


Ilustración 256. Ingresar el nombre de dominio raíz

Fuente: *Elaboración propia*

Configurar las opciones de dominio y forest.

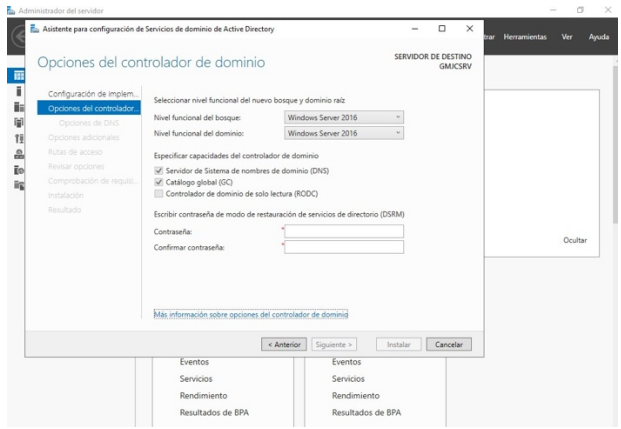


Ilustración 257. Opciones de controlador de dominio

Fuente: Elaboración propia

Especificar una contraseña para el modo de restauración de servicios de directorio (DSRM).

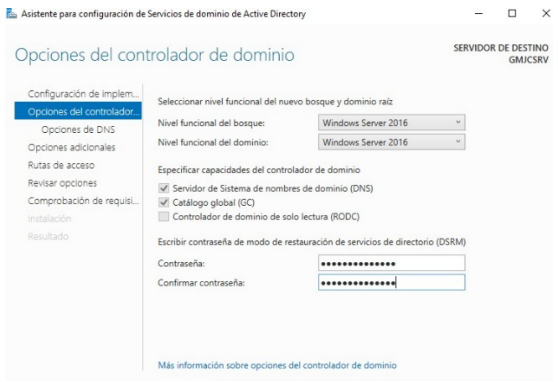


Ilustración 258. Opciones de controlador de dominio - llenado de datos

Fuente: Elaboración propia

Completar la instalación y reiniciar el servidor.

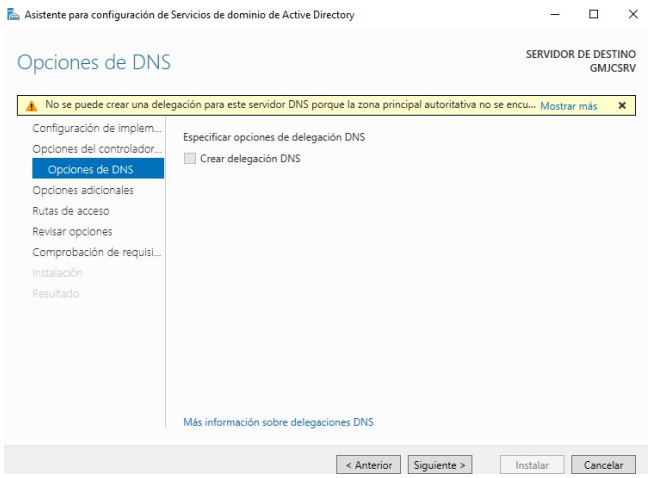


Ilustración 259. Creación de delegación de DNS

Fuente: Elaboración propia

Configuración del nombre de dominio NetBIOS

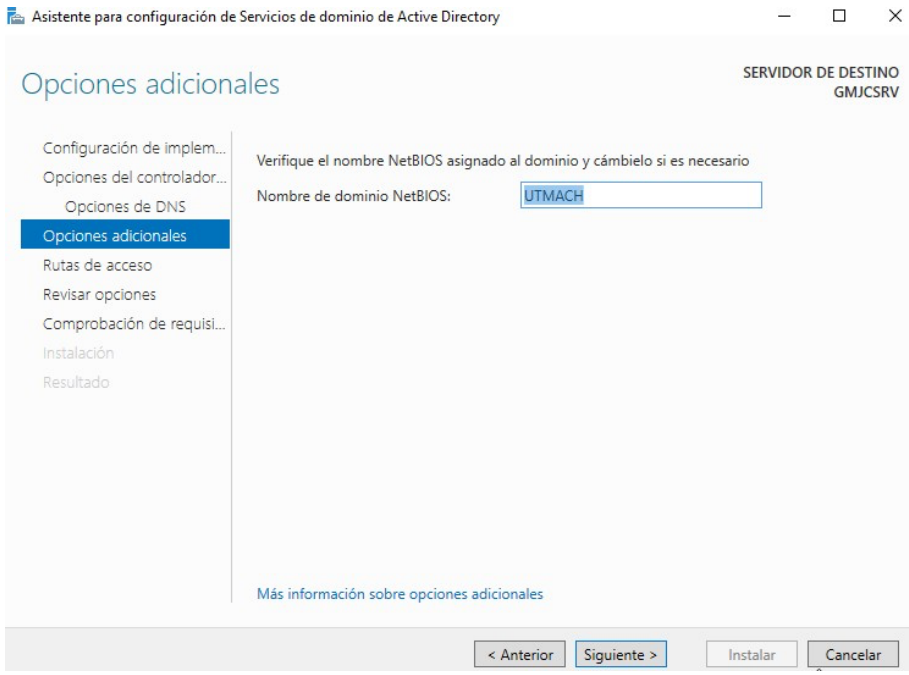


Ilustración 260. Configuración del nombre de dominio NetBIOS

Fuente: Elaboración propia

Especificación de las rutas de acceso a la base de datos, archivos y SYSVOL de Active Directory, en este caso le dejamos la ubicación por defecto.

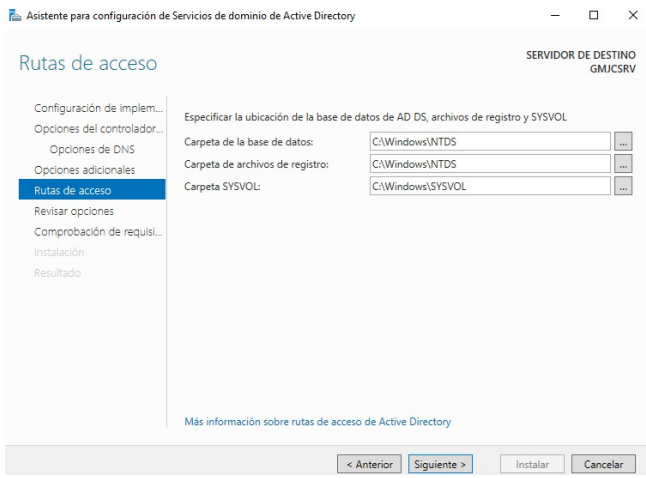


Ilustración 261. Especificación de las rutas de acceso

Fuente: Elaboración propia

En la siguiente ventana, hacemos clic en siguiente

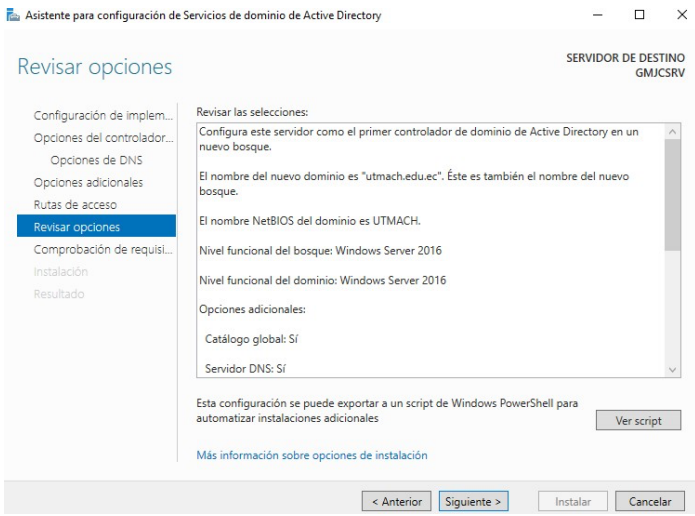


Ilustración 262. Revisión de las selecciones

Fuente: Elaboración propia

Luego, clic en el botón Instalar

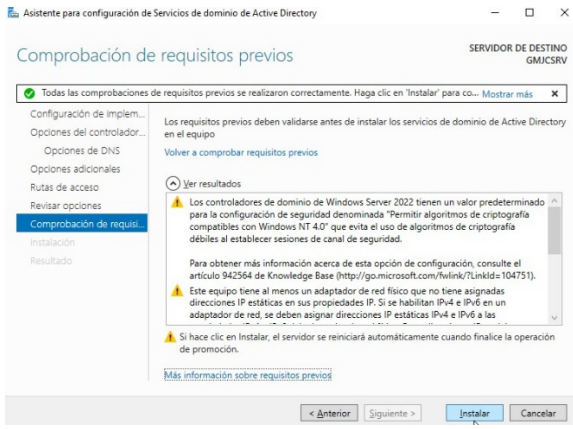


Ilustración 263. Comprobación de todos los requisitos

Fuente: Elaboración propia

Ahora, se reinicia la sesión para culminar con la configuración del dominio

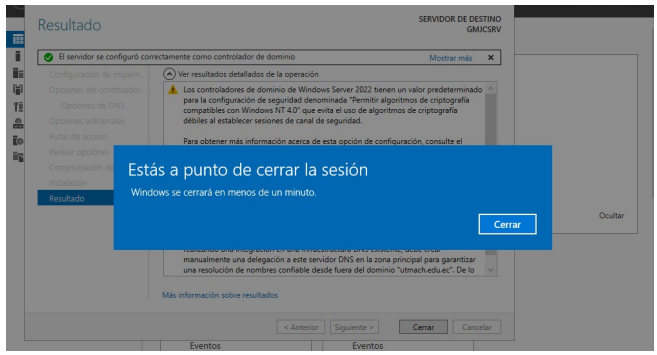


Ilustración 264. Reinicio de sesión para culminar con la configuración del dominio

Fuente: Elaboración propia

Crear unidades organizativas y usuarios de active directory

La opción de Herramientas del Administrador de Servidor, hacemos clic en “Usuarios y Equipos de Active Directory"

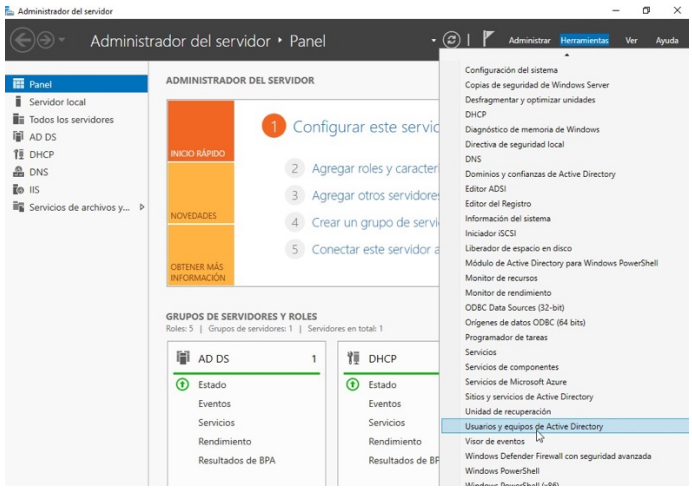


Ilustración 265. Herramientas del panel de AD

Fuente: Elaboración propia

En la siguiente ventana, crear una nueva Unidad Organizativa (OU), en este caso hemos creado una unidad organizativa llamada: practicaSO.

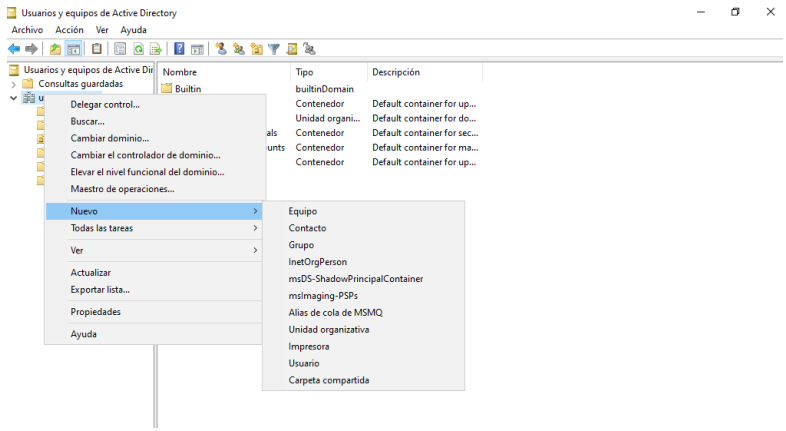


Ilustración 266. Creación de una Unidad Organizativa

Fuente: Elaboración propia

Después, añadir nuevos usuarios en la Unidad organizativa (OU) recién creada, para ello clic derecho en la OU, luego en Nuevo y luego en Usuario.

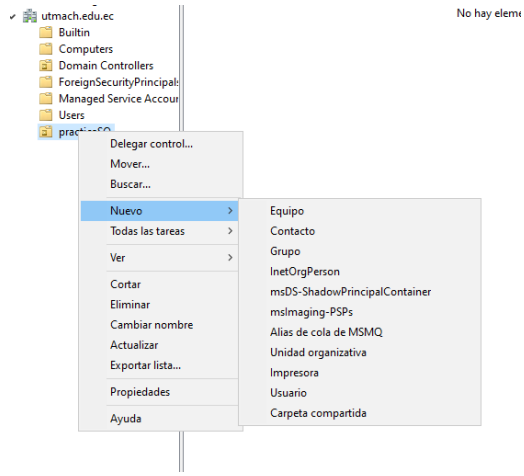


Ilustración 267. Adición de usuarios a la OU

Fuente: Elaboración propia

Nos aparece una ventana para ingresar datos básicos de un usuario como: nombres, apellidos, nombre completo, nombre de usuario. Aquí también se indica con que dominio se conectará este usuario, en caso detener varios dominios.

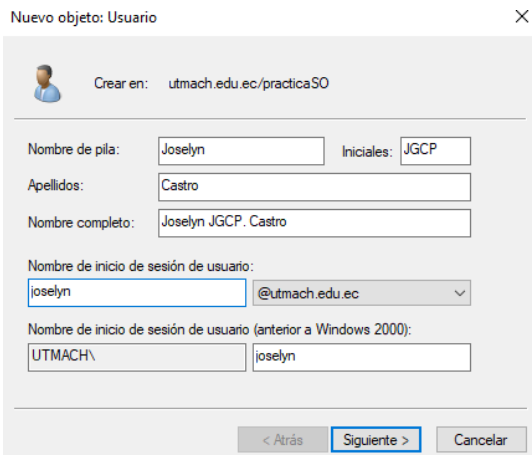


Ilustración 268. Creación de nuevo usuario en la OU

Fuente: Elaboración propia

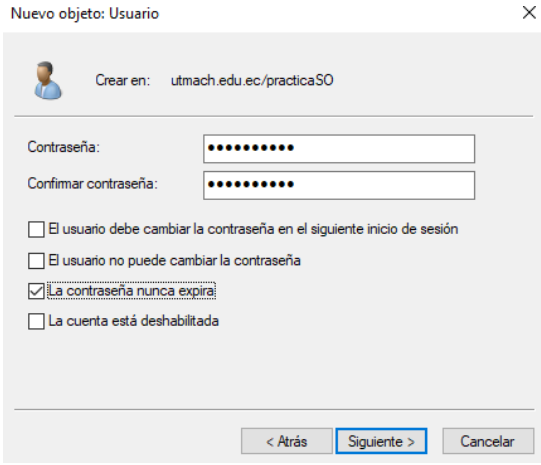


Ilustración 269. Opciones de usuario

Fuente: Elaboración propia

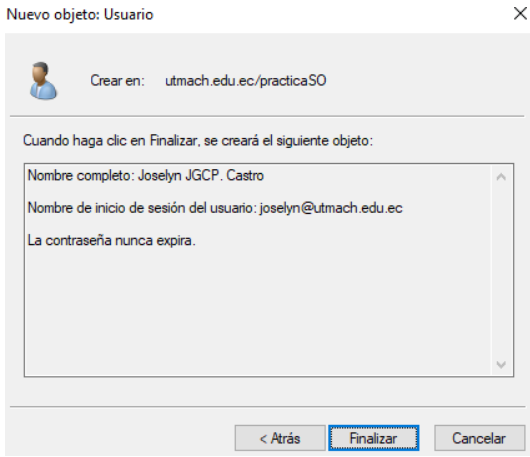


Ilustración 270. Finalización de la creación del usuario

Fuente: Elaboración propia

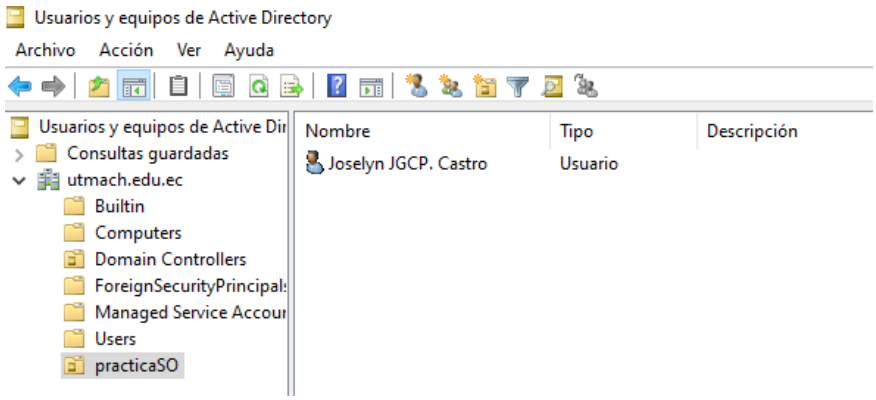


Ilustración 271. Usuario de Active Directory

Fuente: Elaboración propia

Cliente

Unirse al dominio de Active Directory:

Configurar el adaptador de red: Asignar una IP estática de clase C y configurar el DNS para que apunte alservidor AD DS.

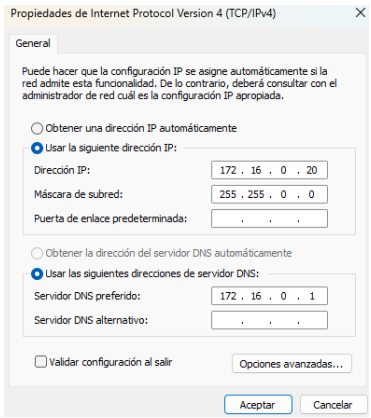


Ilustración 272. Asignación de IP clase C

Fuente: Elaboración propia

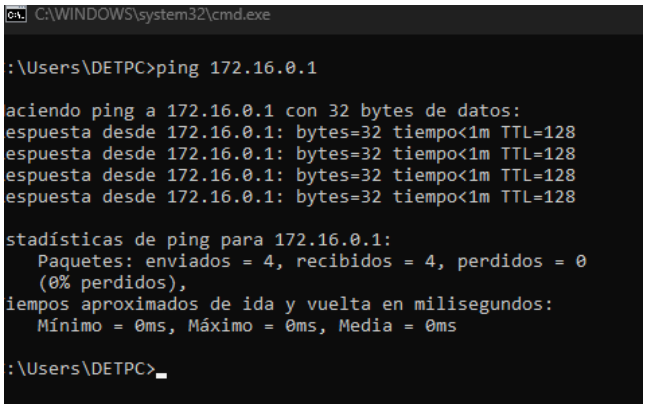


Ilustración 273. Conexión exitosa

Fuente: Elaboración propia

Unir el equipo al dominio:

- Abrir "Sistema" y hacer clic en "Cambiar configuración".
- Ingresar el nombre del dominio.
- Proporcionar las credenciales de administrador del dominio.

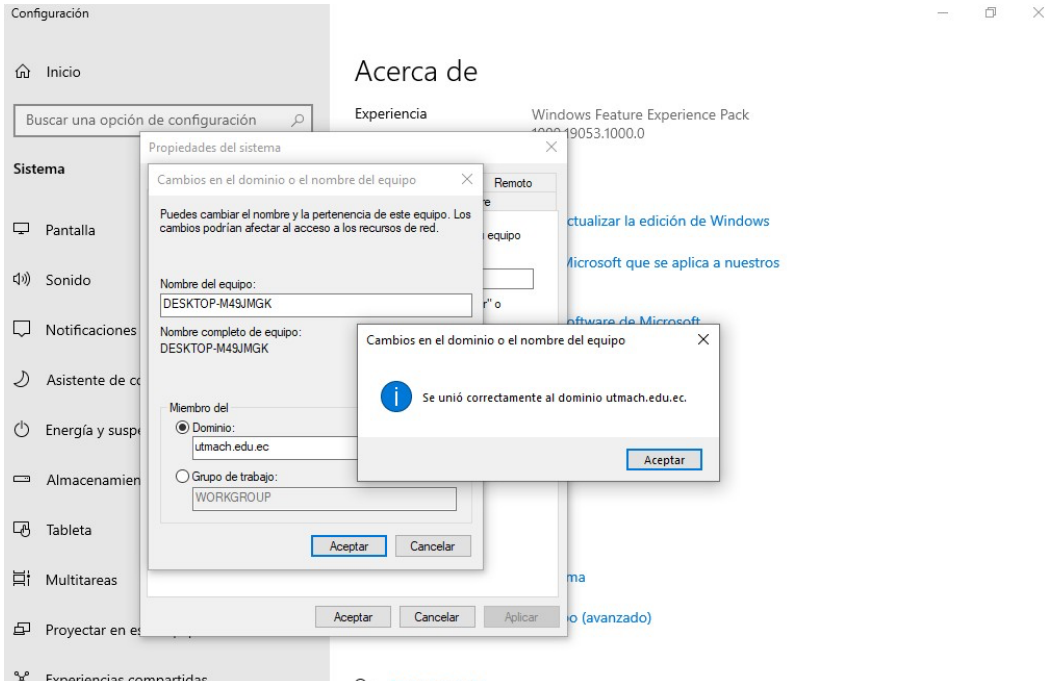


Ilustración 274. Conexión del equipo con el dominio

Fuente: Elaboración propia

Reiniciar el equipo.

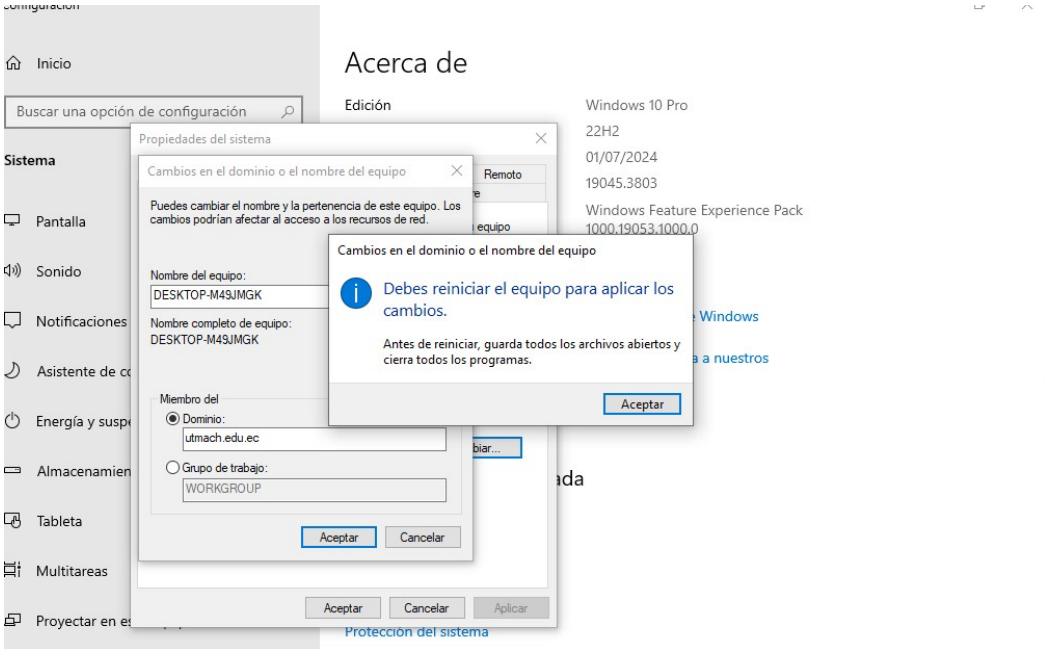


Ilustración 275. Reinicio del equipo para aplicar los cambios

Fuente: Elaboración propia

Pruebas

Verificar la conectividad y configuración de AD:

Comprobar la configuración de TCP/IP en el cliente.

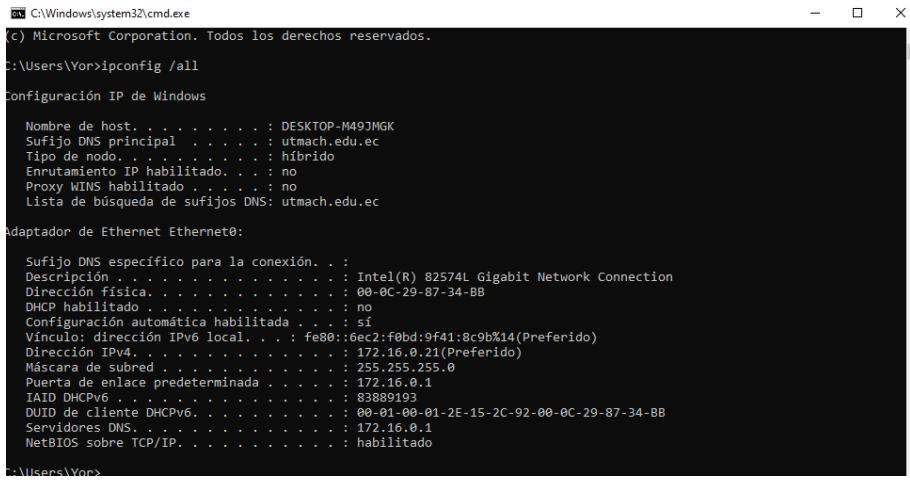


Ilustración 276. Configuración de TCP/IP

Fuente: Elaboración propia

Verificar la unión al dominio y la funcionalidad del AD, ejecutar nslookup para comprobar la resolución de nombres DNS.

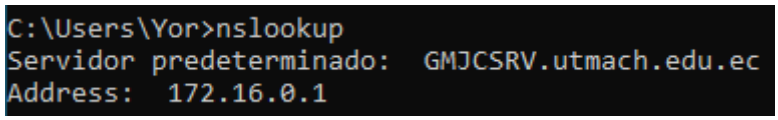


Ilustración 277. Comprobación de nombres DNS

Fuente: Elaboración propia

Utilizar ping para verificar la conectividad con el servidor AD DS.

```
C:\Users\Yor>ping 172.16.0.1

Haciendo ping a 172.16.0.1 con 32 bytes de datos:
Respuesta desde 172.16.0.1: bytes=32 tiempo=1ms TTL=128
Respuesta desde 172.16.0.1: bytes=32 tiempo<1m TTL=128
Respuesta desde 172.16.0.1: bytes=32 tiempo<1m TTL=128
Respuesta desde 172.16.0.1: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 172.16.0.1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 1ms, Media = 0ms
```

Ilustración 278. Verificación de conectividad

Fuente: Elaboración propia

Iniciar sesión en el cliente utilizando una cuenta de usuario del dominio creada previamente.

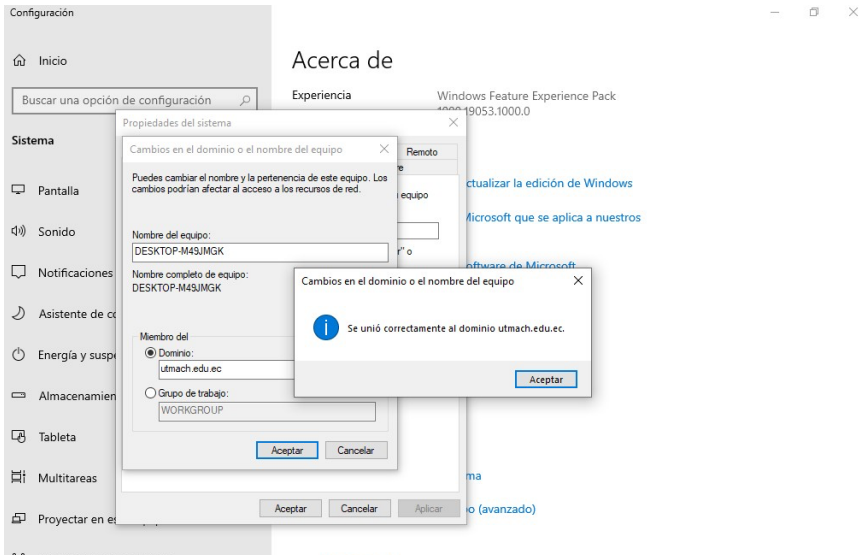


Ilustración 279. Unión del usuario con el dominio

Fuente: Elaboración propia

Caso Práctico 2: Gestión Avanzada de Permisos en Active Directory

Descripción de la práctica: Esta práctica se centra en la implementación y gestión avanzada de los servicios de Active Directory en un entorno de red utilizando Windows Server. Los estudiantes tendrán la oportunidad de profundizar en la configuración de permisos y restricciones, asegurando la correcta administración de recursos y la seguridad de la información. Durante la sesión, se configurarán políticas de grupo (GPO) para controlar el acceso y comportamiento de las cuentas de usuario y máquinas dentro de una unidad organizativa específica. Los participantes aplicarán configuraciones de seguridad para restringir cambios en el sistema y validarán la implementación mediante pruebas de conectividad y comprobaciones de políticas aplicadas.

Asignar una dirección IP estática de clase C en el adaptador de red del servidor y del cliente.

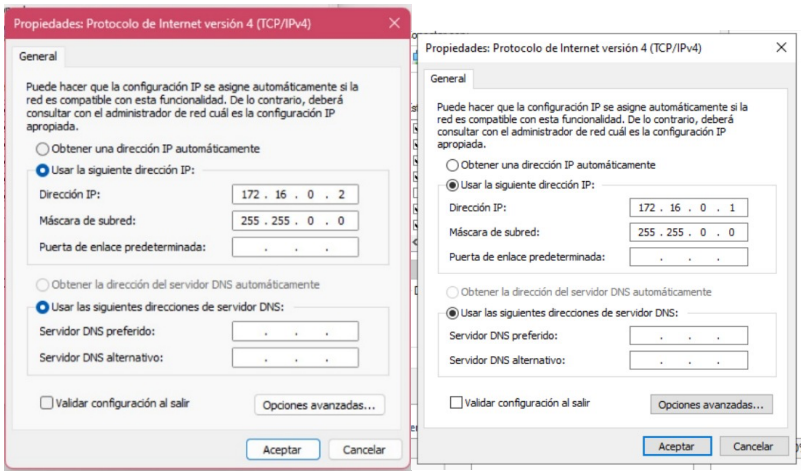


Ilustración 280. Asignación de IP

Fuente: Elaboración propia

Realizar pruebas de conectividad entre el cliente y el servidor mediante ping

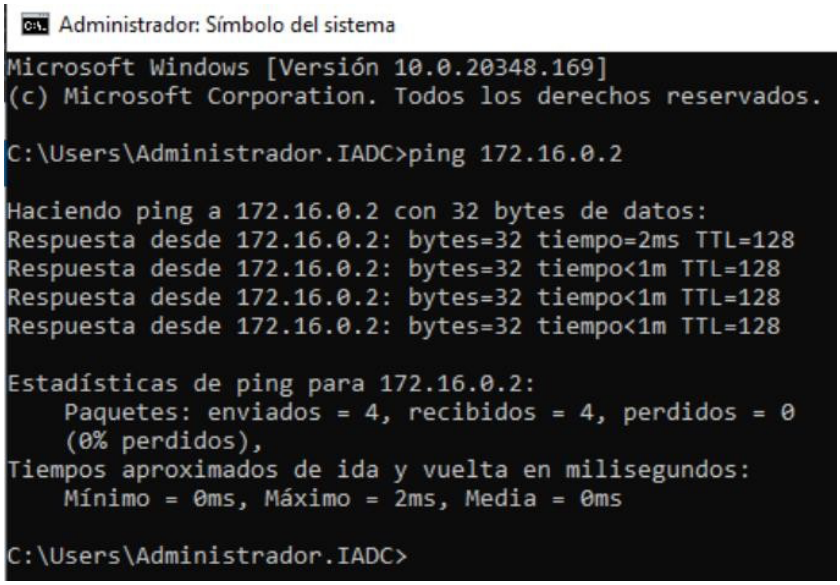


Ilustración 281. Pruebas de conectividad

Fuente: Elaboración propia

Servidor

Configurar permisos y restricciones en Active Directory.

Crear un nuevo usuario con el nombre de “UsuarioPractica”:

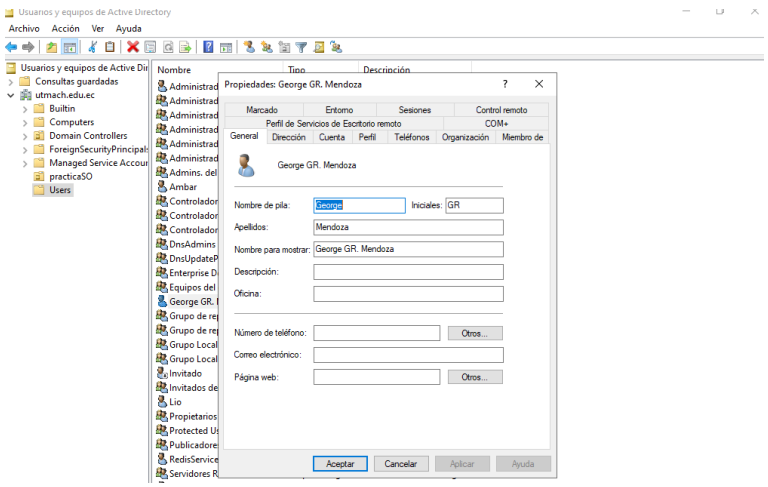


Ilustración 282. Creación de usuario

Fuente: Elaboración propia

Abrir "Usuarios y Equipos de Active Directory" y creamos un nuevo usuario llamado “UsuarioPractica” en el contenedor "Usuarios".

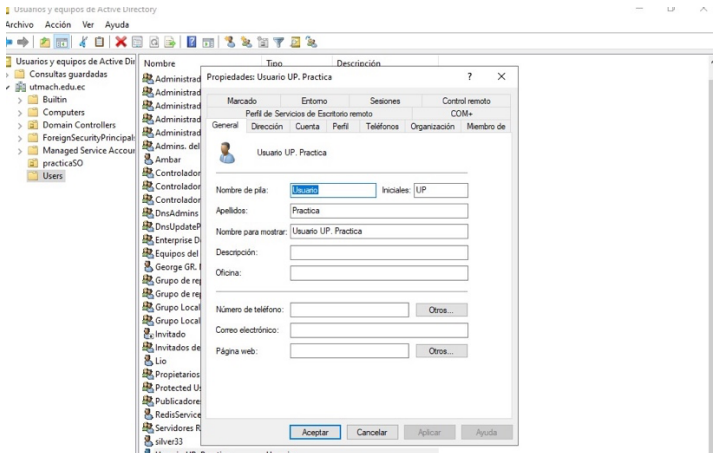


Ilustración 283. Creación de usuario para la práctica

Fuente: Elaboración propia

Crear una unidad organizativa con el nombre de “Practica 2”

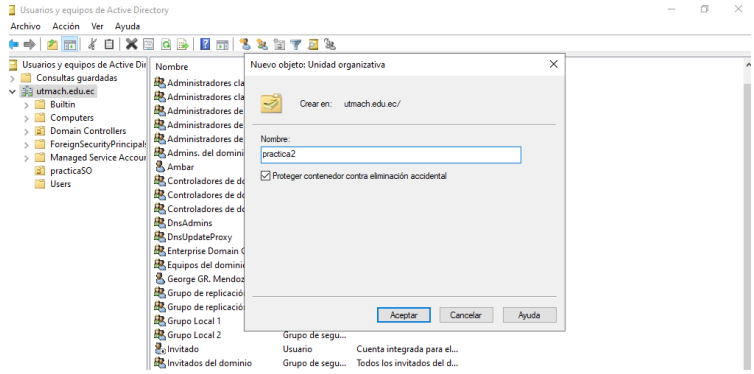


Ilustración 284. Creación de una nueva UO

Fuente: Elaboración propia

Mover el usuario “UsuarioPractica” a la nueva unidad organizativa “Practica 2”

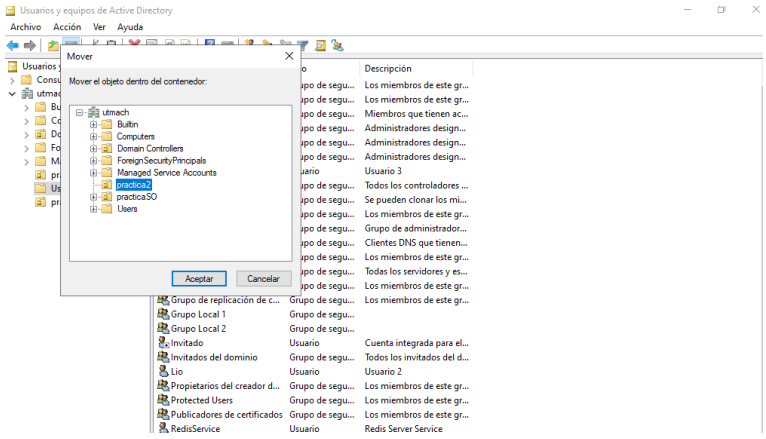


Ilustración 285. Mover el usuario creado a la nueva UO

Fuente: Elaboración propia

Crear una GPO con el nombre de “Bloqueo Automático Terminal” y vincularla a la unidad organizativa “Practica 2”, para ello abrir "Administración de directivas de grupo".

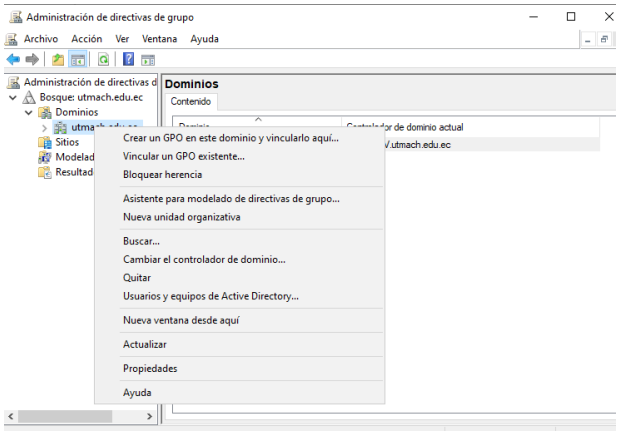


Ilustración 286. Administración de directivas

Fuente: Elaboración propia

Crear una nueva GPO llamada "Bloqueo Automático Terminal".

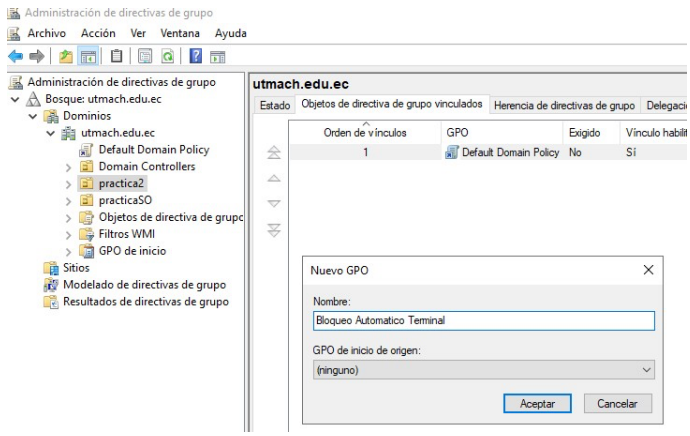


Ilustración 287. Creación de GPO

Fuente: Elaboración propia

Vincular la GPO a la OU "Practica 2", luego editar la GPO para habilitar:

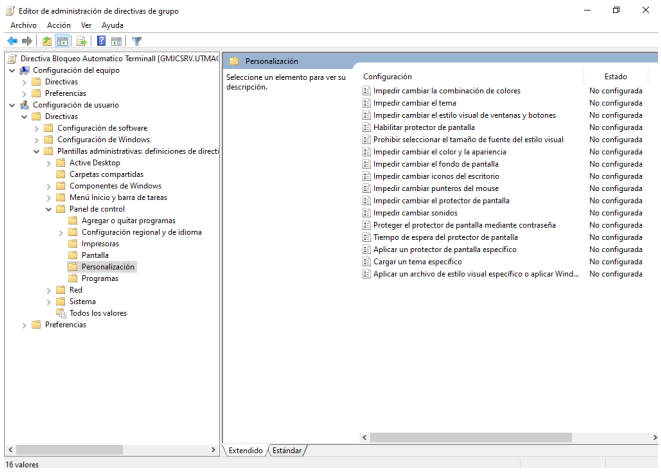


Ilustración 288. Configuración de la GPO

Fuente: Elaboración propia

Habilitar la opción de “Impedir cambiar el tema”, para que el usuario no pueda cambiar temas desde la máquina cliente.

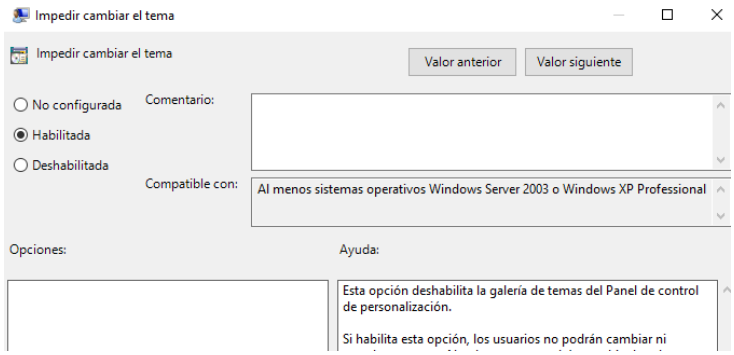


Ilustración 289. Habilitar la opción “Impedir cambiar el tema”

Fuente: Elaboración propia

Ahora, vamos a Habilitar la opción de "Impedir cambiar el fondo de pantalla" para que el usuario no pueda cambiar el fondo de pantalla desde la máquina cliente.

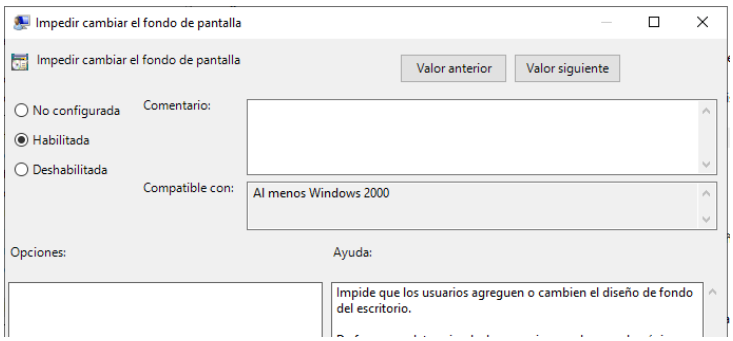


Ilustración 290. Habilitar la opción "Impedir cambiar el fondo de pantalla"

Fuente: Elaboración propia

Ejecutar el comando "gpupdate /force" y realizar pruebas:

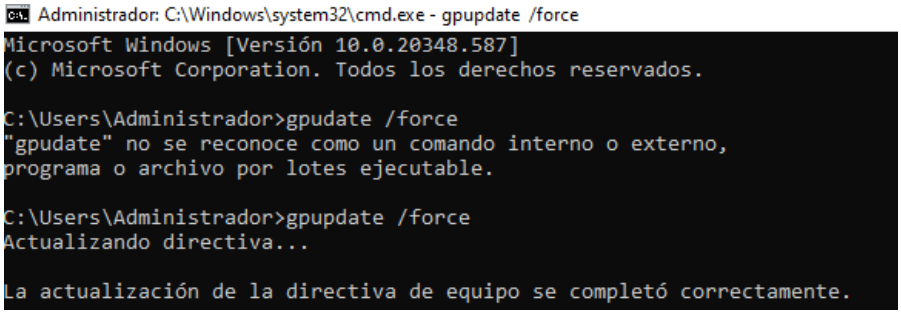


Ilustración 291. Pruebas en la consola

Fuente: Elaboración propia

En el cliente, abrir "Ejecutar" y escribir gpupdate /force.

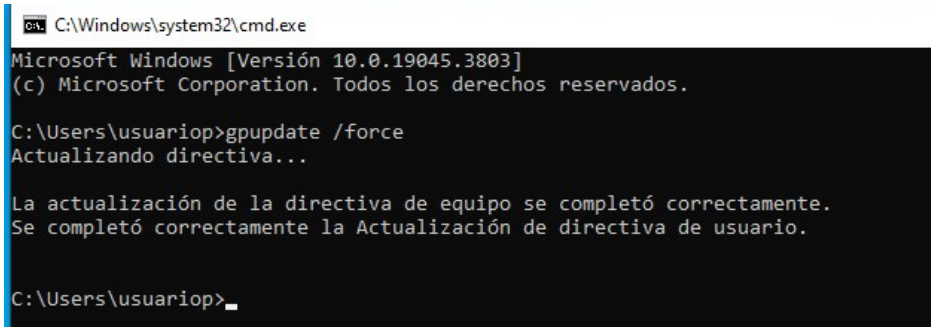


Ilustración 292. Actualización de directivas en el cliente

Fuente: Elaboración propia

Verificar desde el cliente que las políticas se aplican correctamente.

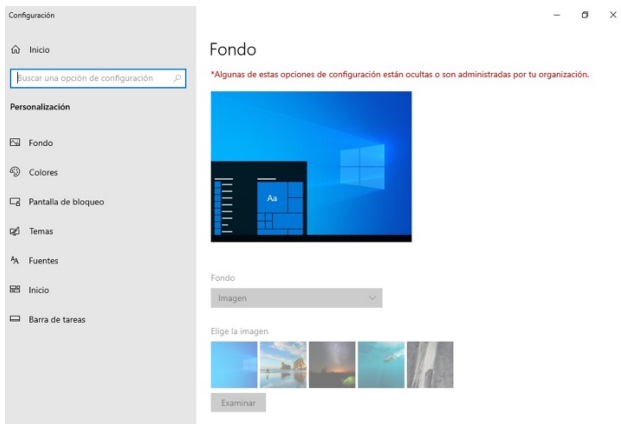


Ilustración 293. Pruebas de la restricción “Impedir cambiar el fondo de pantalla”

Fuente: Elaboración propia

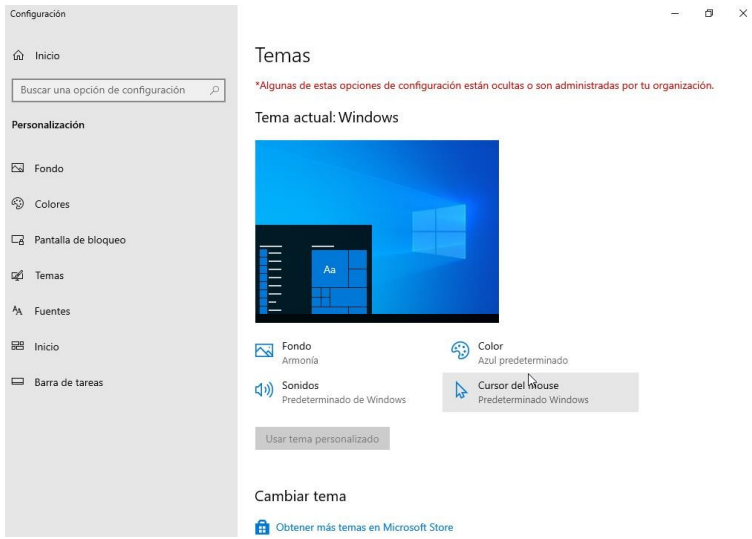


Ilustración 294. Pruebas de la restricción "Impedir cambiar el tema"

Fuente: Elaboración propia

Crear una GPO con el nombre de "No ejecución de aplicaciones especificadas"y vincularla a la unidad organizativa "Practica 2":

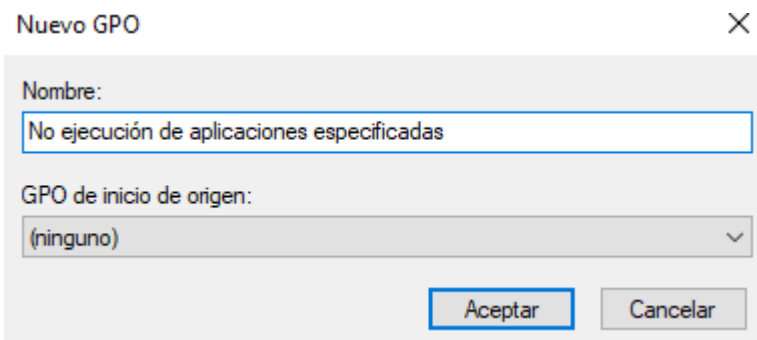


Ilustración 295. Creación de una nueva GPO

Fuente: Elaboración propia

Editar la GPO para habilitar:

"No ejecutar aplicaciones de Windows especificados" y agregar el nombre de la aplicación.

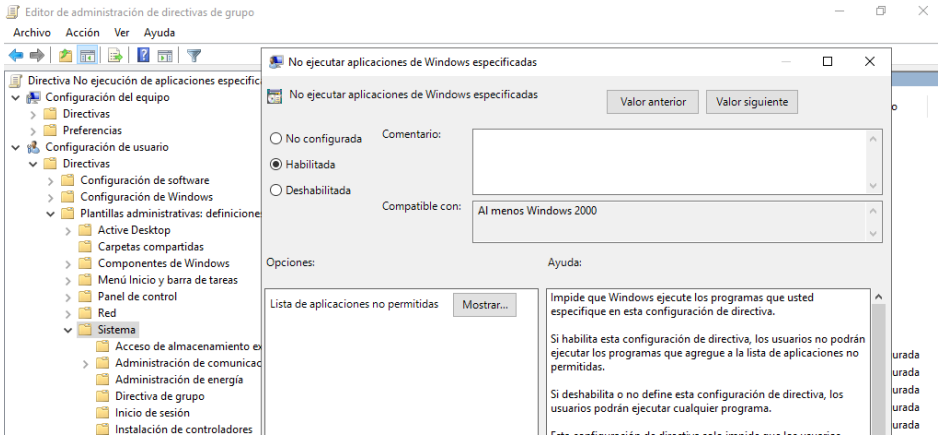


Ilustración 296. Edición de la GPO creada

Fuente: Elaboración propia

Ejecutar el comando "gpupdate /force" y realizar pruebas:

En el cliente, abrir "Ejecutar" y escribir gpupdate /force.

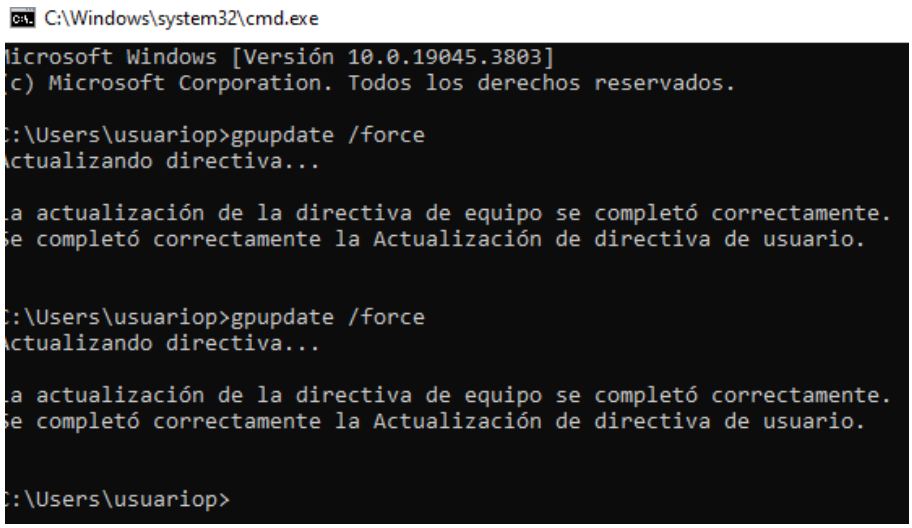


Ilustración 297. Actualización de directivas

Fuente: Elaboración propia

Intentar ejecutar la aplicación especificada para verificar que está bloqueada.

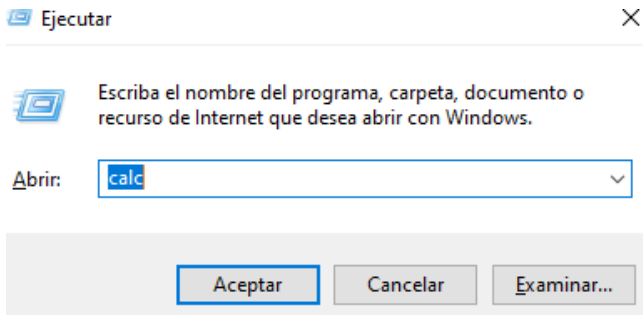


Ilustración 298. Ejecución de la aplicación calculadora

Fuente: Elaboración propia

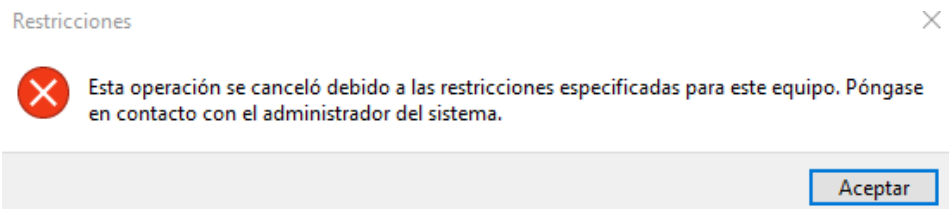


Ilustración 299. Comprobación de la restricción

Fuente: Elaboración propia

Crear una GPO con el nombre de "Impedir acceso a las unidades desde MiPC" y vincularla a la unidad organizativa "Practica 2": Editar la GPO para habilitar: "Impedir acceso a las unidades desde Mi PC" y seleccionar launidad a restringir.

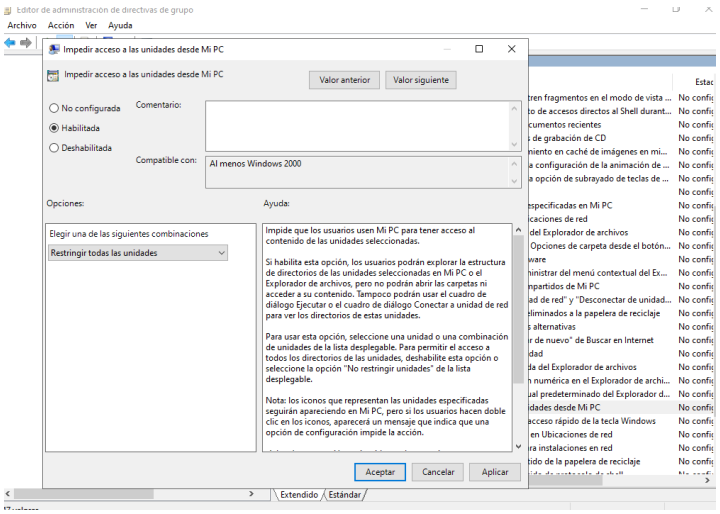


Ilustración 300. Restricción "Impedir acceso a las unidades desde Mi PC"

Fuente: Elaboración propia

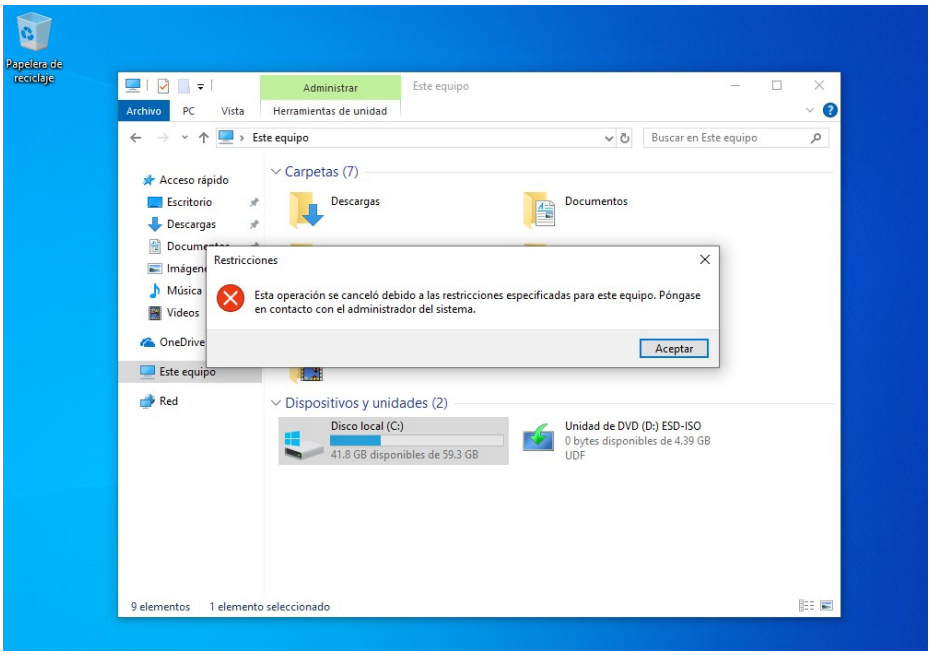


Ilustración 301. Comprobación de la restricción

Fuente: Elaboración propia

Crear una GPO con el nombre de “Bloquear para que no se cambien las IP” yvincularla a la unidad organizativa “Practica 2”:

Crear una nueva GPO llamada "Bloquear para que no se cambien las IP".

Vincular la GPO a la OU "Practica 2".

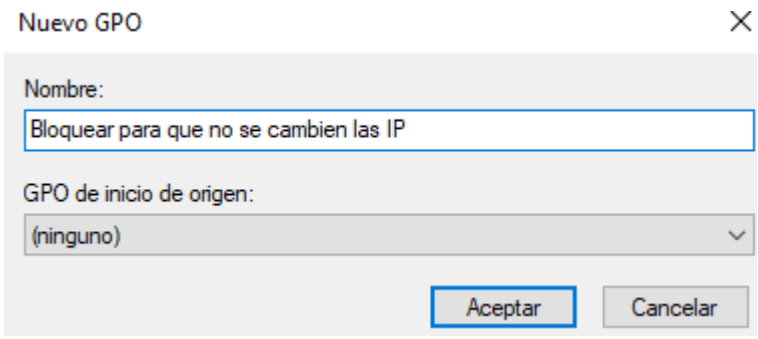


Ilustración 302. Nueva GPO llamada "Bloquear para que no se cambien las IP"

Fuente: Elaboración propia

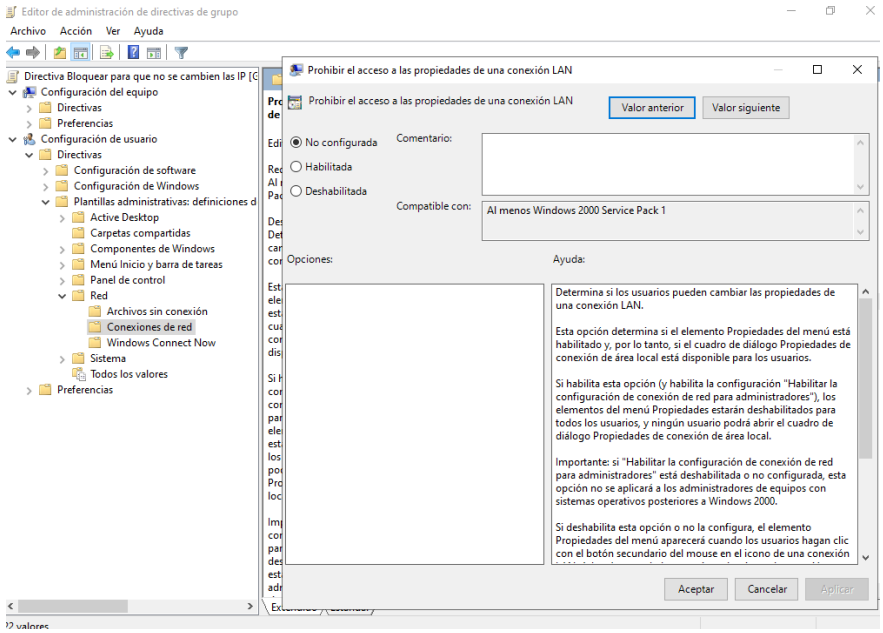


Ilustración 303. Prohibición al acceso de las propiedades de una conexión LAN

Fuente: Elaboración propia

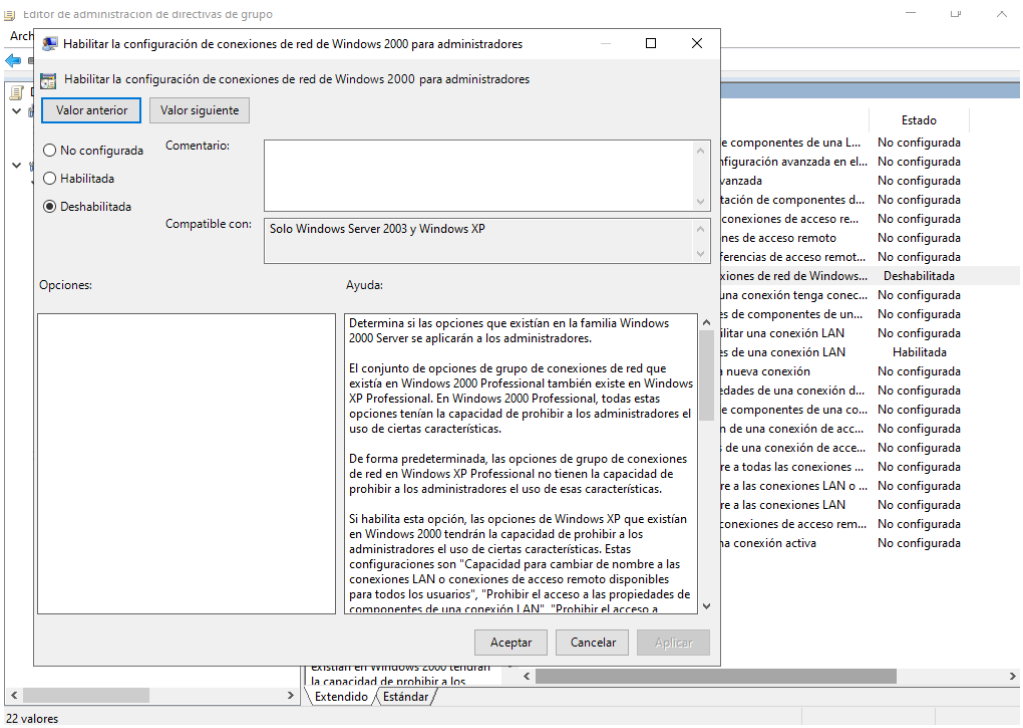


Ilustración 304. Deshabilitar la configuración de conexiones de red

Fuente: Elaboración propia

Ejecutar el comando “gpupdate /forcé

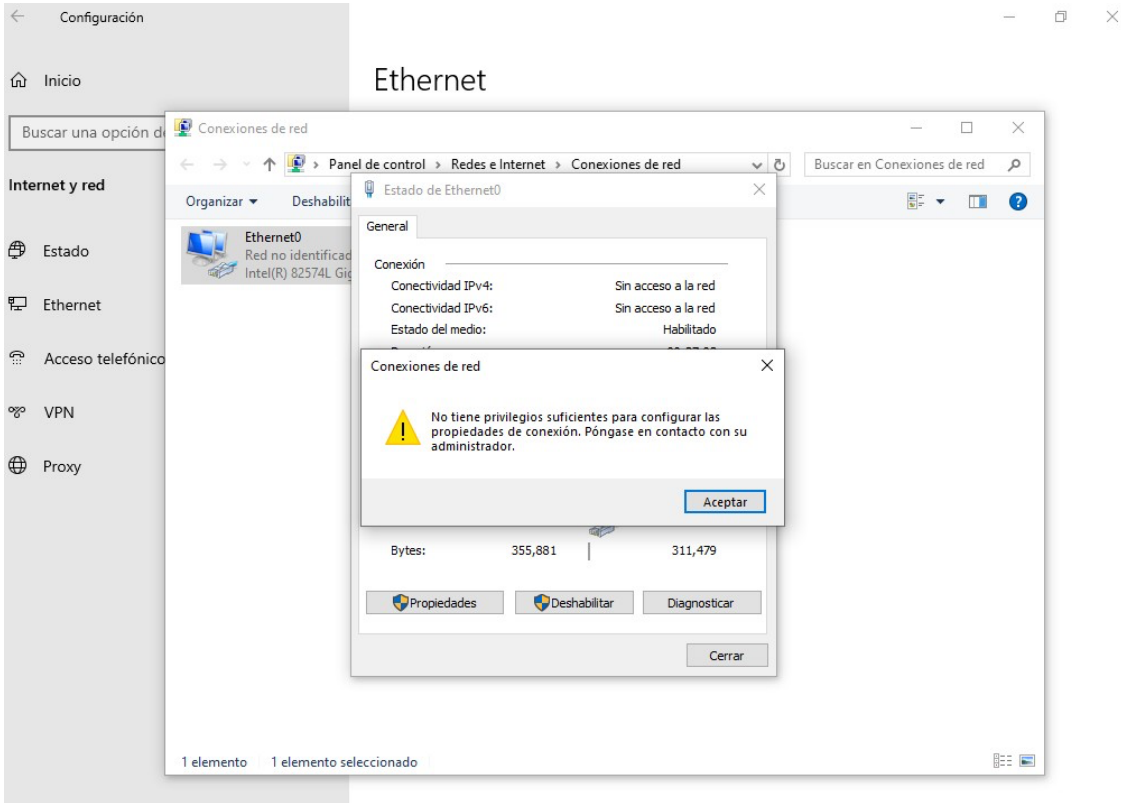


Ilustración 305. Verificar si se deshabilitó la configuración de red en el cliente

Fuente: Elaboración propia

Resumen del Capítulo IV

Este capítulo, aborda el servicio Active Directory Domain Services (AD DS), una herramienta esencial de Microsoft para la administración centralizada de redes. AD DS permite gestionar usuarios, equipos, recursos y políticas de seguridad dentro de una estructura jerárquica y lógica, facilitando el control y la organización de entornos corporativos o educativos. Se explican los componentes más importantes del servicio, como el esquema, el catálogo global, el sistema de indexación, y el servicio de replicación, que garantizan la disponibilidad y consistencia de los datos en toda la red. También se detallan los elementos estructurales de Active Directory: objetos, dominios, controladores de dominio, unidades organizativas (OU), árboles y bosques, cada uno con funciones específicas para la segmentación y administración eficiente de los recursos. En este capítulo, se incluye dos casos prácticos como son: 1) La instalación y configuración de Active Directory; en dónde se guía paso a paso en la instalación del servicio AD DS, la creación de un dominio, la configuración de unidades organizativas y usuarios, y la unión de equipos cliente al dominio; además se realizan pruebas de conectividad y verificación de autenticación para asegurar el correcto funcionamiento del entorno y 2) Gestión avanzada de permisos con GPO (Group Policy Objects): aquí se acrea y vincula políticas de grupo para controlar el comportamiento de usuarios y equipos. Entre las configuraciones aplicadas se encuentran restricciones para cambiar temas o fondos de pantalla, bloqueo de aplicaciones específicas, acceso limitado a unidades del sistema, y prohibición de cambios en la configuración de red. Estas políticas se validan mediante comandos y pruebas desde el cliente.

Este capítulo proporciona una base para comprender e implementar Active Directory en redes Windows Server,

combinando teoría, administración de seguridad y prácticas reales que fortalecen el aprendizaje.

Preguntas de Revisión

Evaluación de Conocimientos Adquiridos

1. Entendimiento de Conceptos Básicos:

- Defina de manera clara qué es Active Directory y explique su propósito en una red empresarial. Si no puede hacerlo con seguridad, investigue más sobre el tema y elabore un breve resumen.

- Describa la estructura jerárquica de Active Directory y los roles de sus componentes principales. Considere elaborar un esquema que detalle estos componentes para reforzar su comprensión.

2. Habilidades Prácticas:

- Evalúe su capacidad para instalar y configurar un controlador de dominio en un entorno virtualizado. Si encuentra dificultades, detalle qué aspectos necesita revisar o aprender más profundamente.

- Reflexione sobre su habilidad para crear y administrar Unidades Organizativas, usuarios y grupos en Active Directory. Prepare una lista de pasos o un tutorial sobre cómo realiza estas tareas.

3. Aplicación de Políticas de Seguridad:

- Explique cómo aplica y administra políticas de grupo (GPO) para controlar la configuración y seguridad de los equipos y usuarios en la red. Si este proceso le resulta complejo, identifique qué recursos podrían ayudarle a mejorar.

- Discuta cómo implementa y verifica las políticas de seguridad recomendadas para proteger los recursos de la organización. Elabore una lista de verificación para las políticas que aplica regularmente.

4. Resolución de Problemas:

- Diagnostique y resuelva un problema común relacionado con la autenticación o la replicación en Active Directory. Documente el proceso y reflexione sobre los desafíos encontrados.

- Realice una tarea de mantenimiento o recuperación, como la restauración de datos o la reconfiguración de controladores de dominio. Describa el procedimiento y evalúe su efectividad en la tarea.

Autoevaluación Personal

1. Reflexión sobre el Aprendizaje:

- Identifique los aspectos de la configuración y administración de Active Directory que encuentra más desafiantes y explique por qué. Considere cómo podría abordar estas dificultades de manera efectiva.

- Determine qué recursos adicionales o prácticas podría necesitar para mejorar su comprensión y habilidades en el uso de Active Directory. Elabore un plan de acción para adquirir estos recursos o prácticas.

2. Plan de Mejora Continua:

- Establezca los próximos pasos en su plan de aprendizaje para dominar Active Directory. Esto puede incluir seguir un curso

específico, leer documentación actualizada o realizar prácticas adicionales.

- Investigue qué certificaciones o cursos están disponibles para validar sus conocimientos y avanzar en su carrera profesional. Haga una lista de opciones y establezca objetivos para alcanzarlas.

Referencias bibliográficas

Microsoft. (2025, 24 de marzo). *Introducción a Active Directory Domain Services*. Microsoft Learn. https://learn.microsoft.com/es-es/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview

Ymant. (2025). *¿Qué es y cómo funciona Active Directory?* Ymant. Recuperado el 2 de junio de 2025, de https://www.ymant.com/blog/que-es-y-como-funciona-active-directory/#:~:text=C%C3%B3mo%20funciona%20Active%20Directory,%2C%20apellidos%2C%20correo%2C%20etc.

Castillo, J. A. (2018, diciembre 15). *Active Directory: Qué es y para qué sirve*. Profesional Review. Recuperado el 2 de junio de 2025, de https://www.profesionalreview.com/2018/12/15/active-directory/#Conceptos_importantes_en_Active_Directory

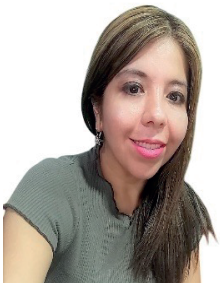
Tecnozero. (2025). *Directorio Activo de Microsoft: ¿Qué es y qué ventajas tiene para la empresa?* Recuperado el 2 de junio de 2025, de https://www.tecnozero.com/blog/directorio-activo-de-microsoft-que-es-que-ventajas-tiene-para-la-empresa/

Ruiz, P. (2021, 17 de octubre). *Capítulo 6: Dominios en Windows Server*. SomeBooks.es. Recuperado el 2 de junio de 2025, de https://somebooks.es/capitulo-3-dominios-en-windows-server-2012-r2/2/SomeBooks.es+3SomeBooks.es+3SomeBooks.es+3

Mantenimiento IV. (2025) *Active Directory (AD DS)*. Recuperado el 2 de junio de 2025, de https://cdsmante4.wordpress.com/active-directory/

Seguridad Informática y Sistemas Operativos en Red. (2015, 8 de octubre). *Configuración directorio activo Server 2012*. Recuperado el 2 de junio de 2025, de https://seguridadinformaticasistemasoperativosenred.wordpress.com/configuracion-directorio-activo-server-2012/

alumnosaso201415. (2015, 25 de febrero). *Estructura lógica de Active Directory*. Administración de Sistemas Operativos. Recuperado el 2 de junio de 2025, de https://administracionsistemasoperativos201415.wordpress.com/2015/02/25/estructura-logica-de-active-directory/Administración de Sistemas Operativos+2



Nancy Magaly Loja Mora
nmloja@utmachala.edu.ec
https://orcid.org/0000-0002-5583-4278
Profesional de nacionalidad ecuatoriana, su formación académica incluye un título de pregrado como Ingeniera en Sistemas Informáticos y Computación otorgado por la Universidad Técnica Particular de Loja en 2005. Posteriormente, continuó su formación académica con dos maestrías: la primera en Docencia y Gerencia en Educación Superior por la Universidad de Guayaquil en 2012, y la segunda en Gestión Estratégica de Tecnologías de la Información por la Universidad de Cuenca en 2020. Actualmente es egresada de la Maestría en Ciberseguridad de la Universidad Internacional de Valencia.
Se desempeña como profesora titular en la carrera de Tecnologías de la Información de la Facultad de Ingeniería Civil de la Universidad Técnica de Machala. Ha ocupado cargos como coordinadora académica y ha representado a los docentes ante el consejo directivo y el consejo universitario de su facultad. Es directora y miembro de grupos de investigación en el área de Gobierno de Tecnologías. Además, colabora activamente en proyectos de titulación con estudiantes de pregrado, enfocados en diversas áreas de las tecnologías como: Gobierno, Seguridad de la Información, entre otras.

Fausto Juvenal Loja Mora
https://orcid.org/0009-0007-8231-6867
faustol@gmail.com
Profesional ecuatoriano con sólida trayectoria en tecnología y gestión empresarial. Ingeniero en Sistemas Informáticos y Computación por la Universidad Técnica Particular de Loja (2003), cuenta además con un Diplomado en Fundamentos de la Educación a Distancia e Investigación (2006) por la misma institución. Obtuvo una Maestría en Administración de Empresas por la Universidad Espíritu Santo (2015) y una Maestría en Sistemas de Información con mención en Data Science (2023).
Actualmente se desempeña como Gerente de Transformación en Seguros Equinoccial y como docente universitario en diversas instituciones académicas del país. Posee más de 20 años de experiencia impulsando la transformación digital y la monetización de datos como palancas para el logro de la estrategia organizacional.

Ivanna Pauleth Álvarez Valarezo
ivanna.alvarez@utmachala.edu.ec
https://orcid.org/0000-0003-2434-9170
Ivanna Pauleth Álvarez Valarezo es estudiante de la carrera de Ingeniería en Tecnologías de la Información en la Universidad Técnica de Machala. Ha participado en el desarrollo de proyectos académicos y de vinculación con enfoque social y tecnológico, integrando conocimientos en sistemas operativos, redes y administración de servicios informáticos.
Su formación combina fundamentos teóricos con experiencia práctica en la implementación de soluciones orientadas a mejorar la infraestructura tecnológica en diversos contextos. Su enfoque académico se complementa con intereses en áreas emergentes como la ciberseguridad, la informática forense y la transformación digital en instituciones públicas.

ISBN: 978-9942-33-953-9

Compás
capacitación e investigación