# Informe Laboratorio N°3

Brayan Smit Mosquera Palacios

Rafael Sandoval Morales

Semestre X

Sistemas de comunicación

Universidad Tecnológica del Choco

“Diego Luis Córdoba”

Quibdó – Choco

02/04/2025.

# Introducción

En este informe llevaremos el paso a paso de agregar los servicios de DNS y Directorio Activo que permite la administración centralizada de usuarios, grupos y recursos en una red. Con el Directorio Activo, los administradores pueden gestionar permisos y acceso a recursos de manera eficiente, facilitando la organización y seguridad de la red.

El Sistema de Nombres de Dominio (DNS) es otro componente crítico en un entorno de red. Su función principal es traducir nombres de dominio legibles por humanos (como www.ejemplo.com) en direcciones IP, que son necesarias para la comunicación entre dispositivos en la red. En un servidor Windows Server 2012, DNS no solo actúa como un servicio para resolver nombres, sino que también se integra estrechamente con el Directorio Activo.

Cuando se instala Active Directory en un servidor, se recomienda configurar un servidor DNS para facilitar la localización de recursos dentro del dominio. Esto permite a los clientes encontrar controladores de dominio y otros servicios esenciales sin complicaciones. Además, el DNS ayuda a mantener la organización del tráfico en la red, asegurando que las peticiones sean dirigidas correctamente a los servidores correspondientes.

# Objetivos

**Objetivo general.**

Implementar y administrar el Directorio Activo y el servicio DNS en un servidor Windows Server 2012 para optimizar la gestión de recursos.

**Objetivos específicos.**

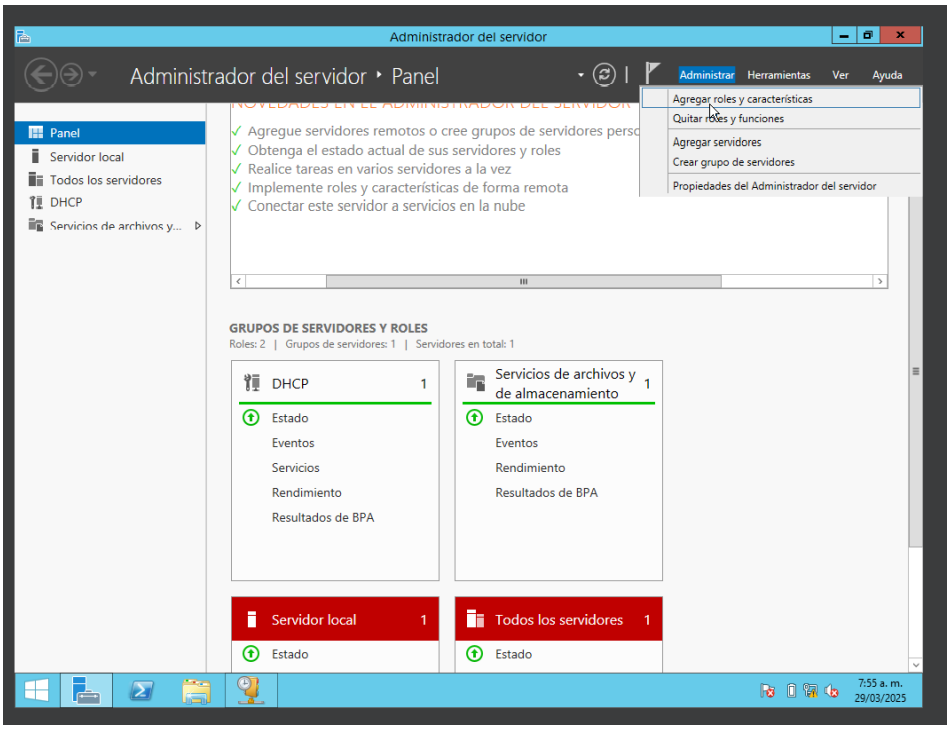
- Configurar el Directorio Activo
- Configurar el servicio DNS
- Gestionar cuentas de usuario

# Topología del sistema de comunicación

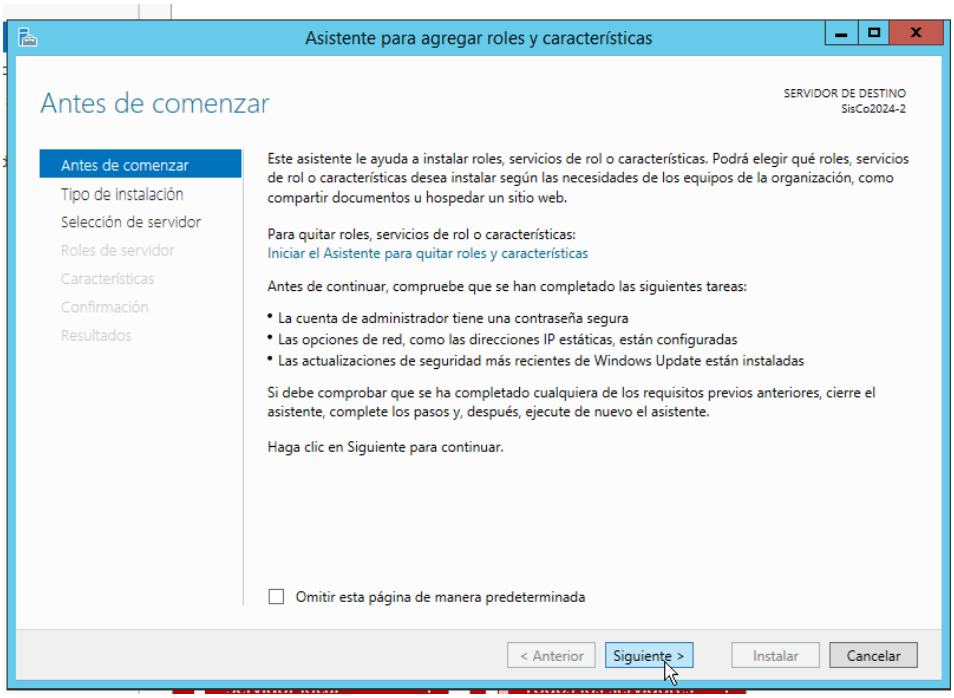

# Topología de la unidad organizacional

# Instalación del Dirección Activo y el DNS

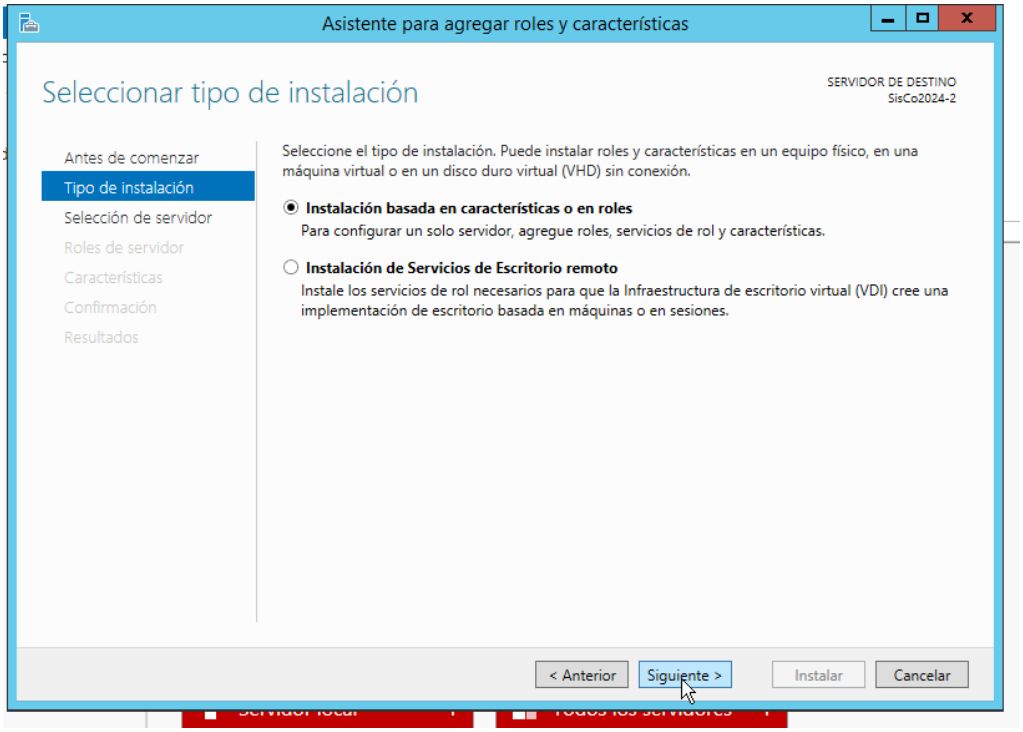
Ingresan al administrador de servicio clic administrar agregar rol y característica



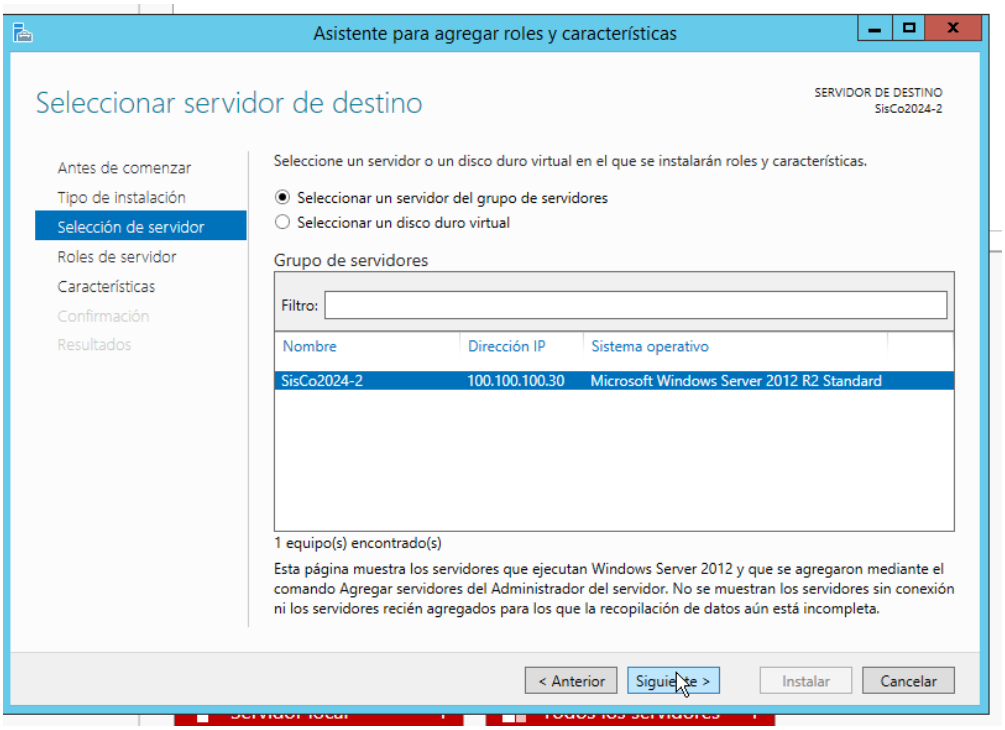

Le damos clic en siguiente para comenzar agregar los roles y característica



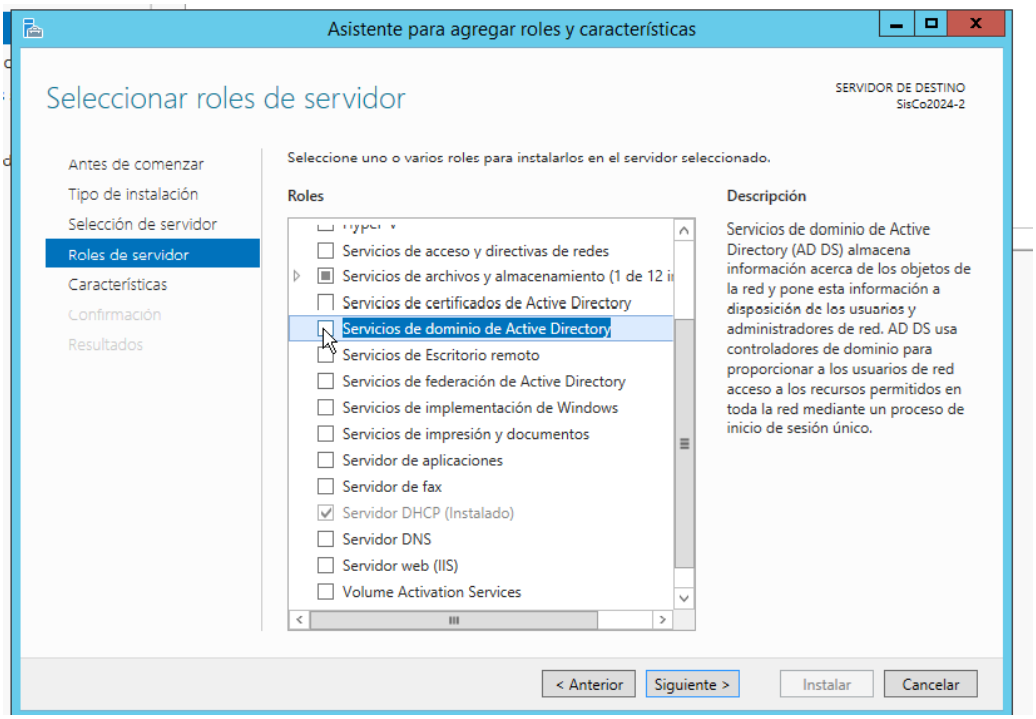
Le dan clic en el tipo de instalación y luego en siguiente

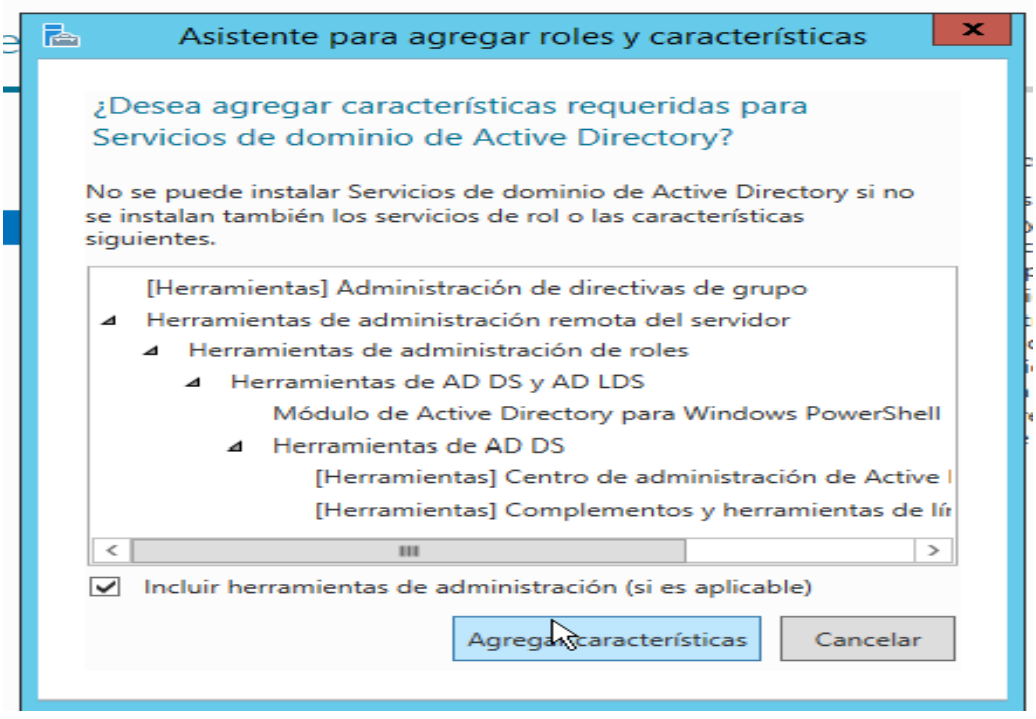



Selecciona el servidor donde van a agregar las funciones clic en siguiente

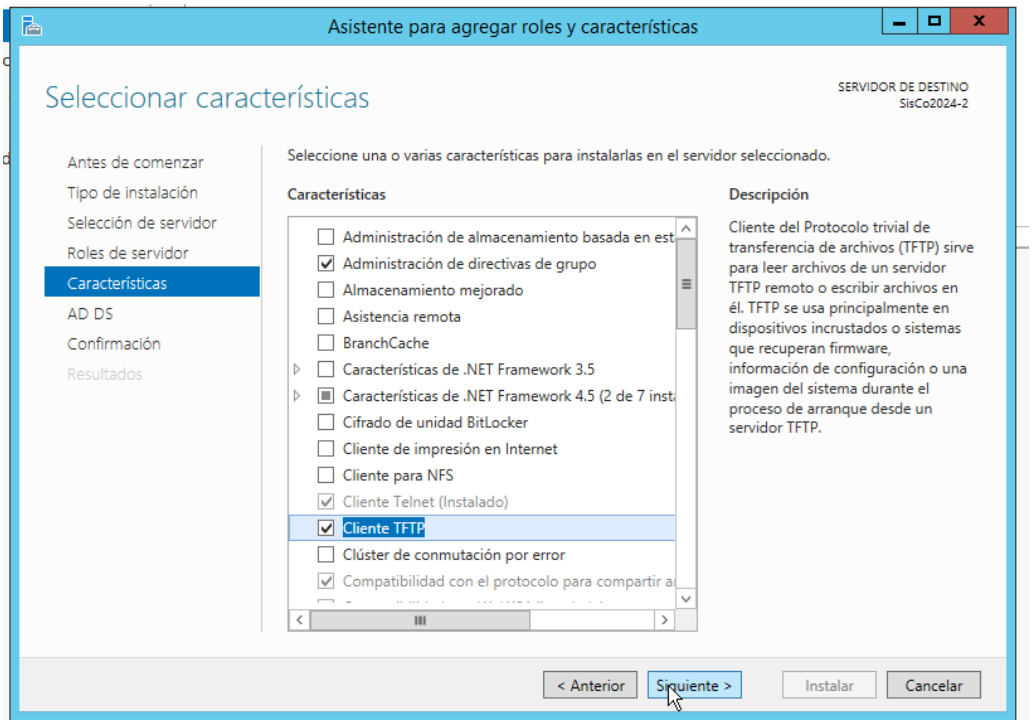


Eligen el rol del servicio y luego clic en siguiente

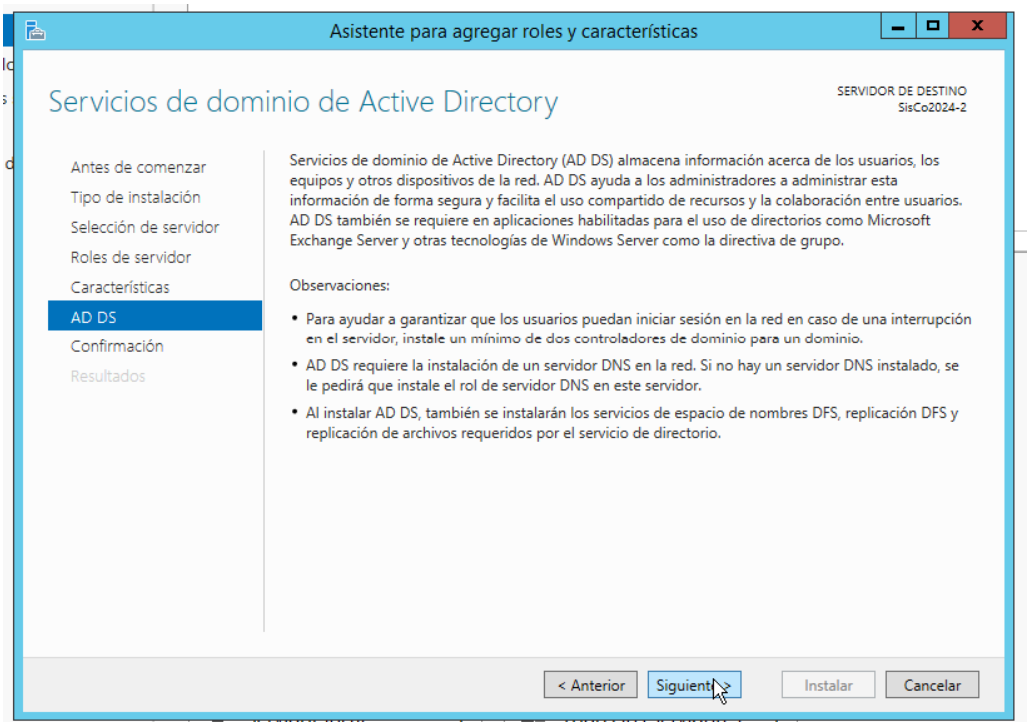


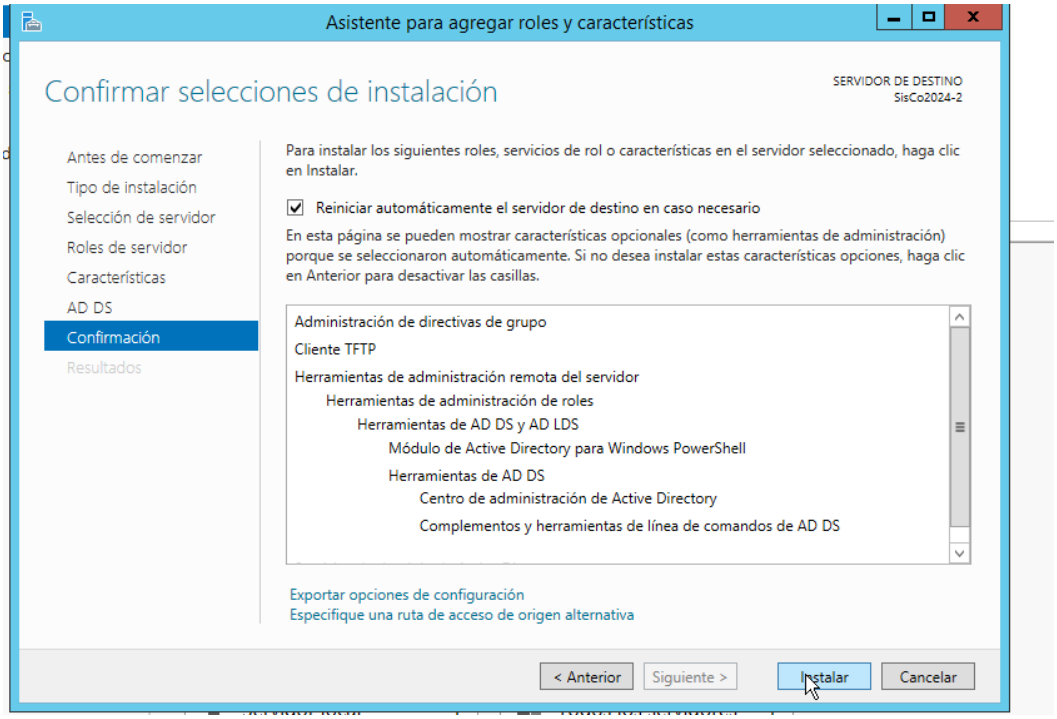
Le agregan las características y luego clic en siguiente

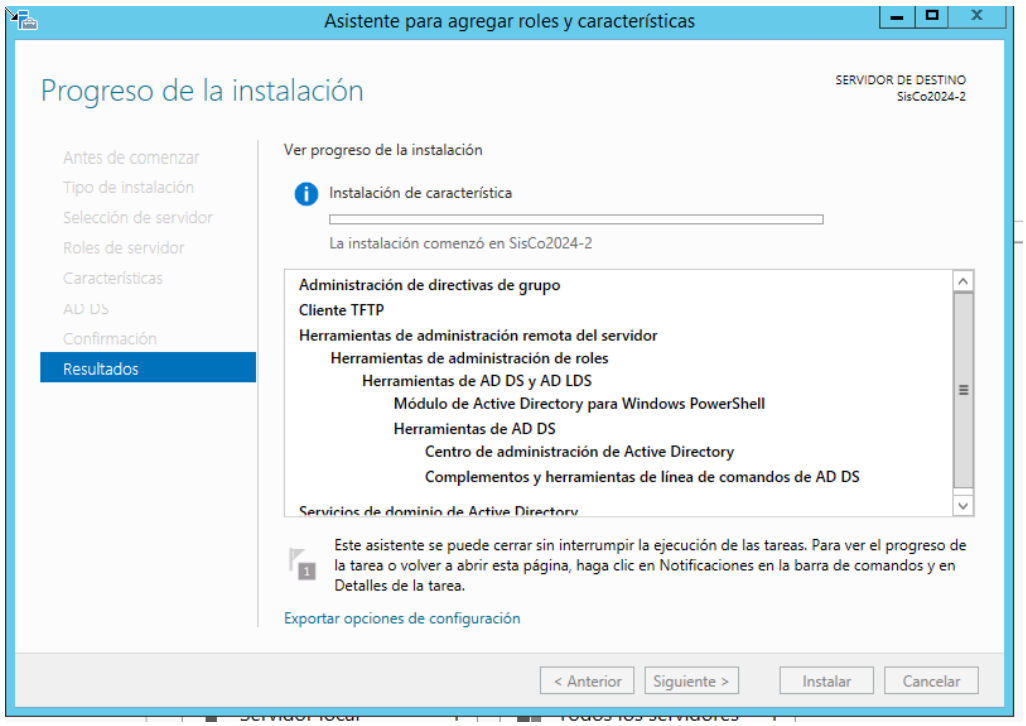



Luego le dan siguiente servicio  de dominio del directorio

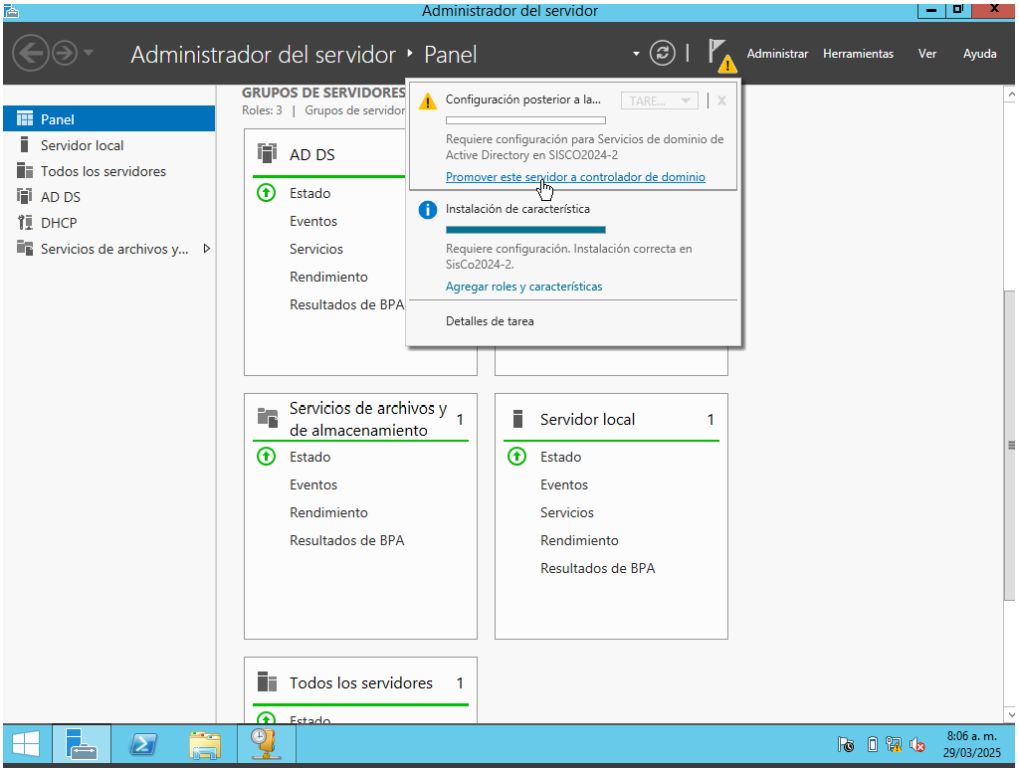


Le dan clic en reiniciar automático y luego en instalar y espere que instale los roles y características

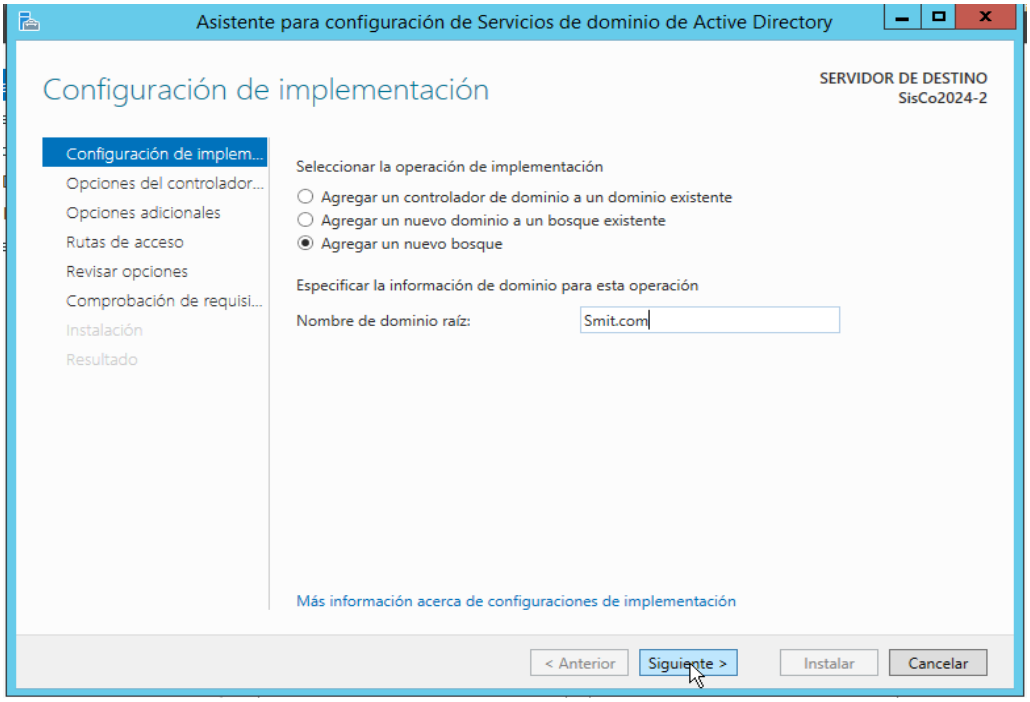


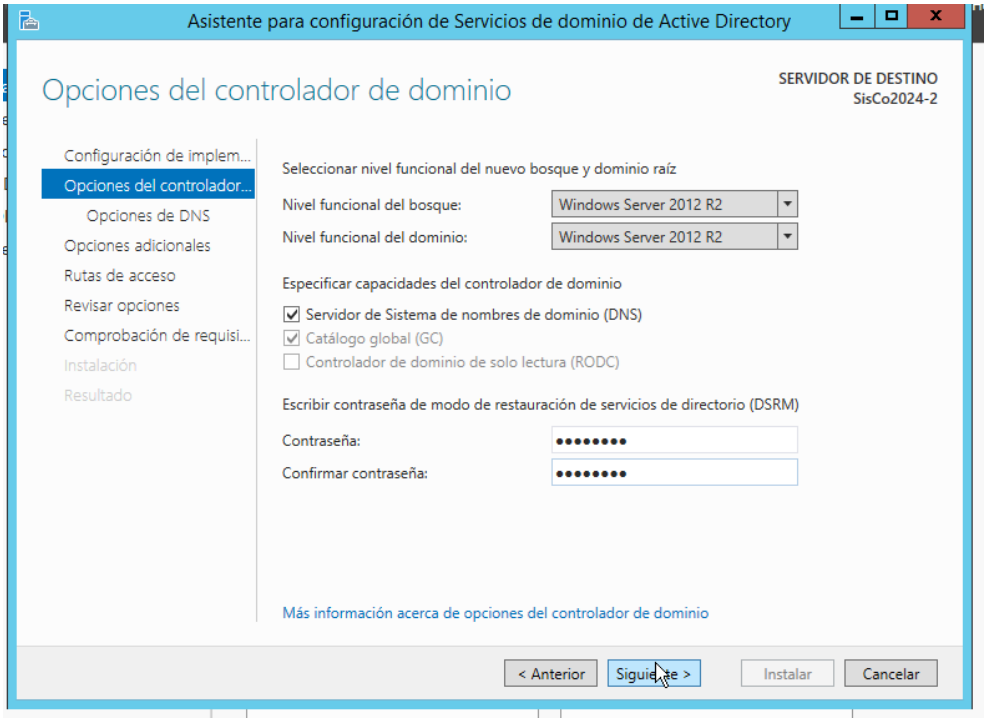
Luego que termine la instalación le damos clic en la icono notificación y clic promover este servidor de dominio



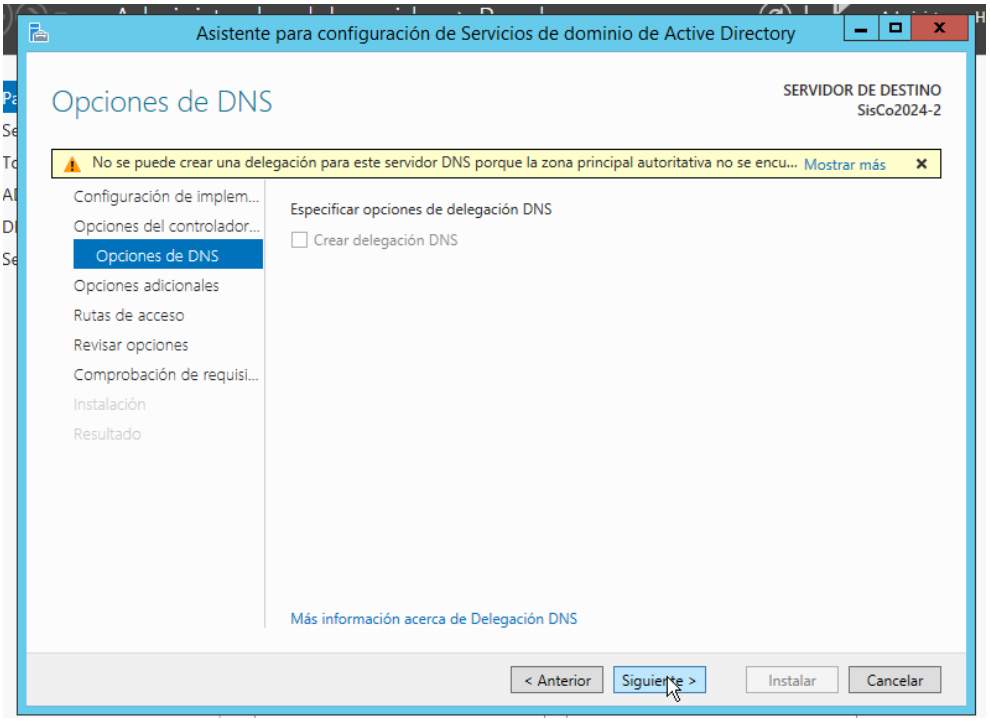

Le dan clic en agregar un nuevo bosque y le agrega el nombre de su dominio y le agrega el .COM, .NET, .EDU etc. Luego en siguiente



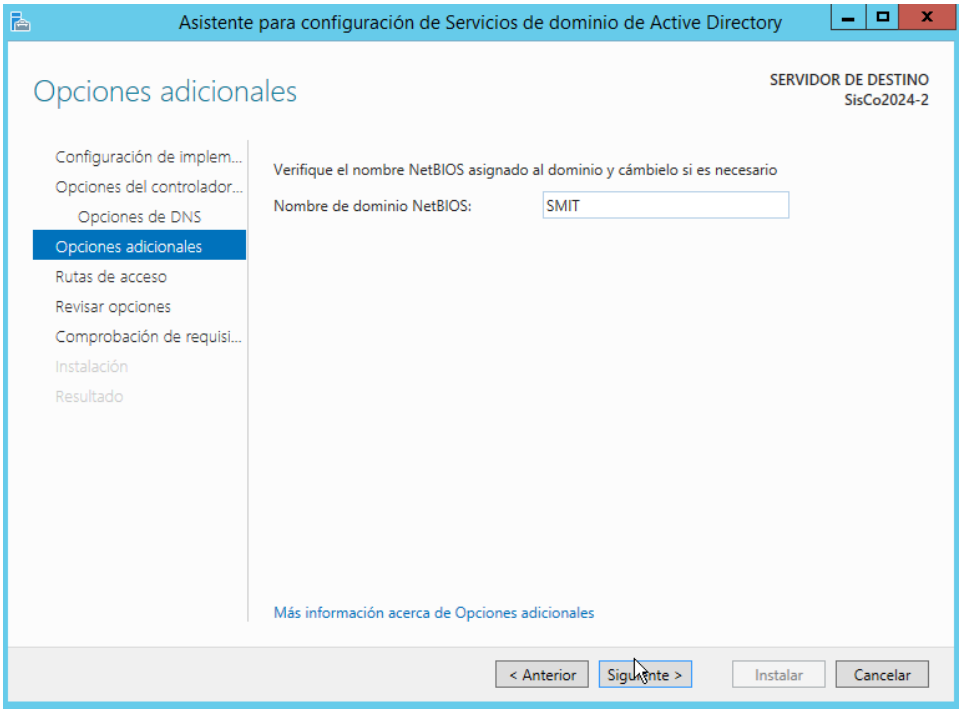
Aquí agregar la contraseña que ingresamos a nuestro pese (Brayan00) y luego clic en siguiente



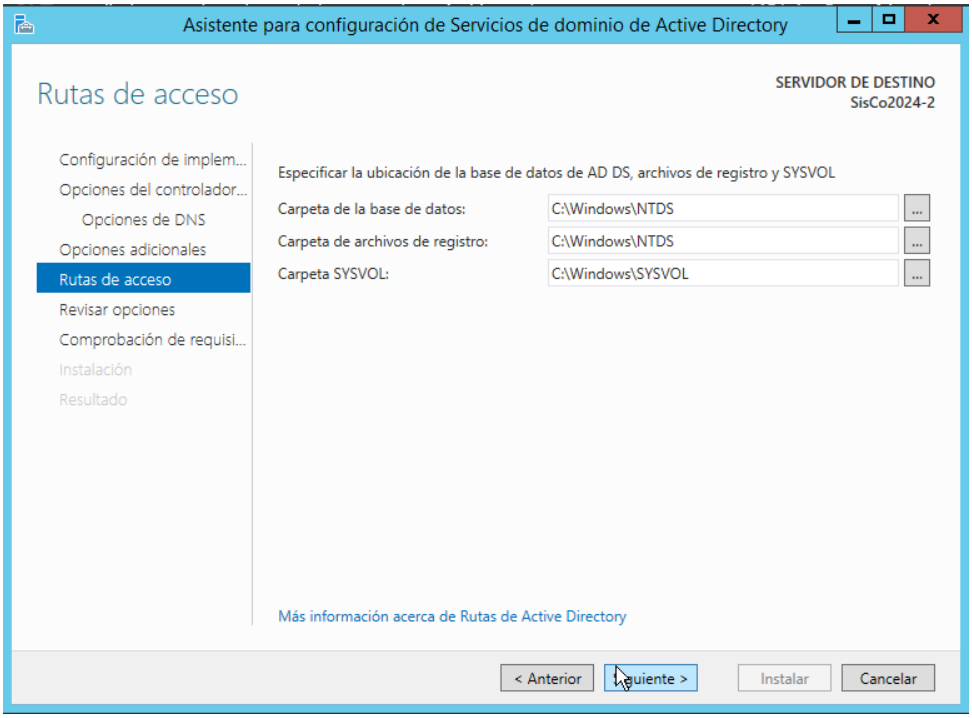

Por q el servidor no tiene DNS nos crea uno automática mente y clic en siguiente



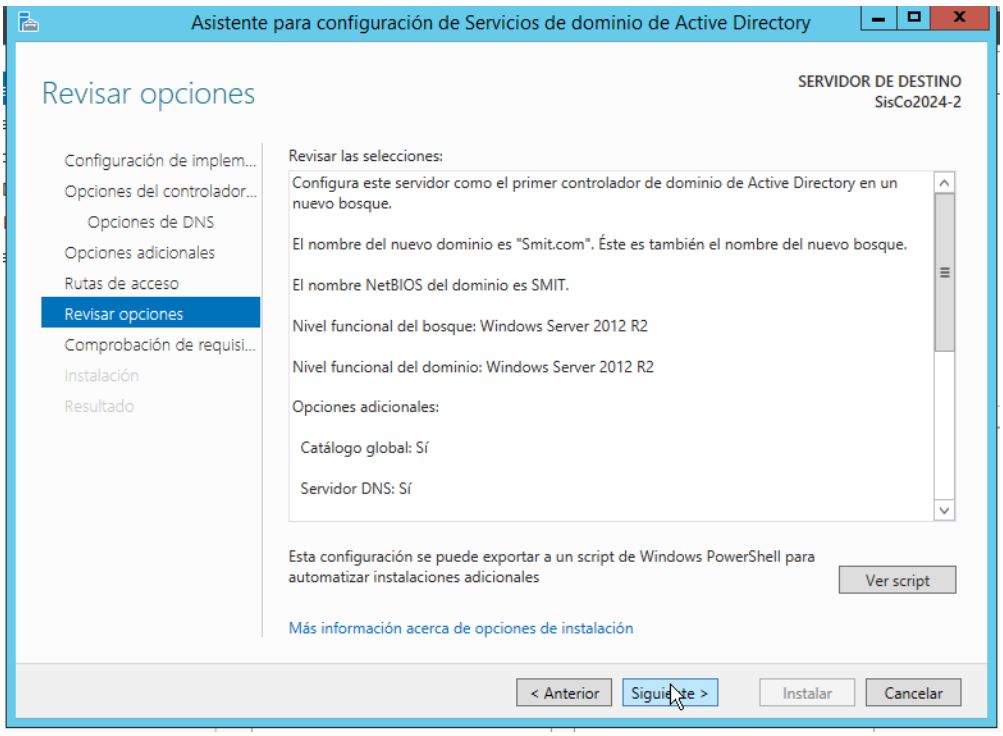
Le damos clic en siguiente en opciones adicionales por que el nombre del NetBios se agrega automática mente



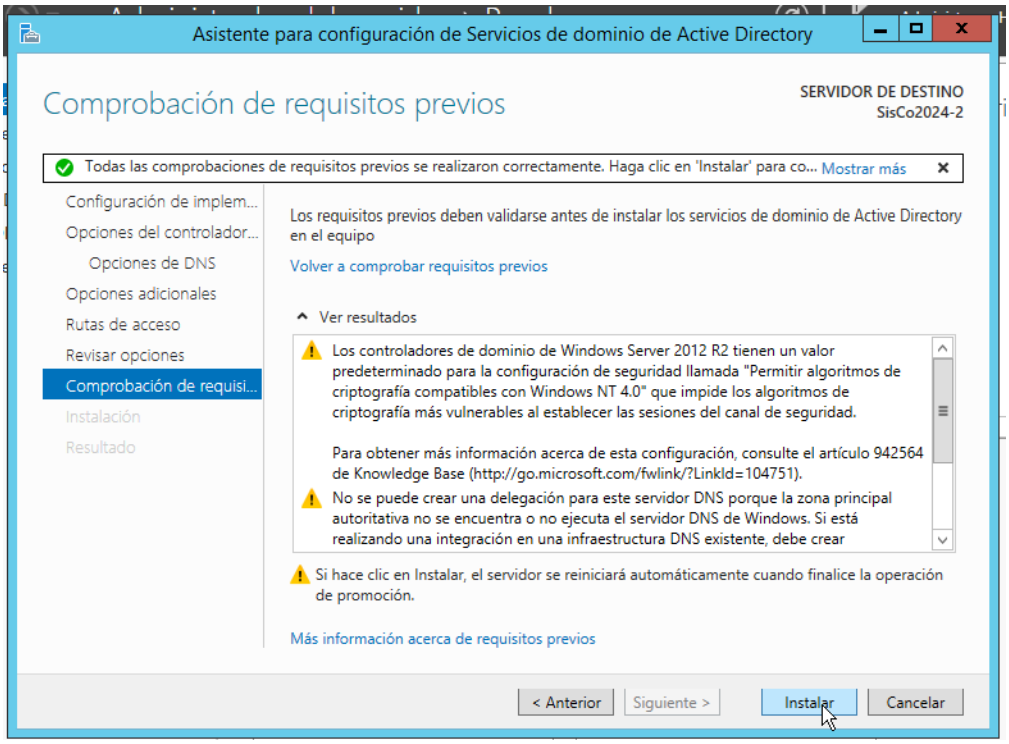

Le dan clic en siguiente rusta de acceso



Luego clic en siguiente en revisar las opciones de los procesos anteriores

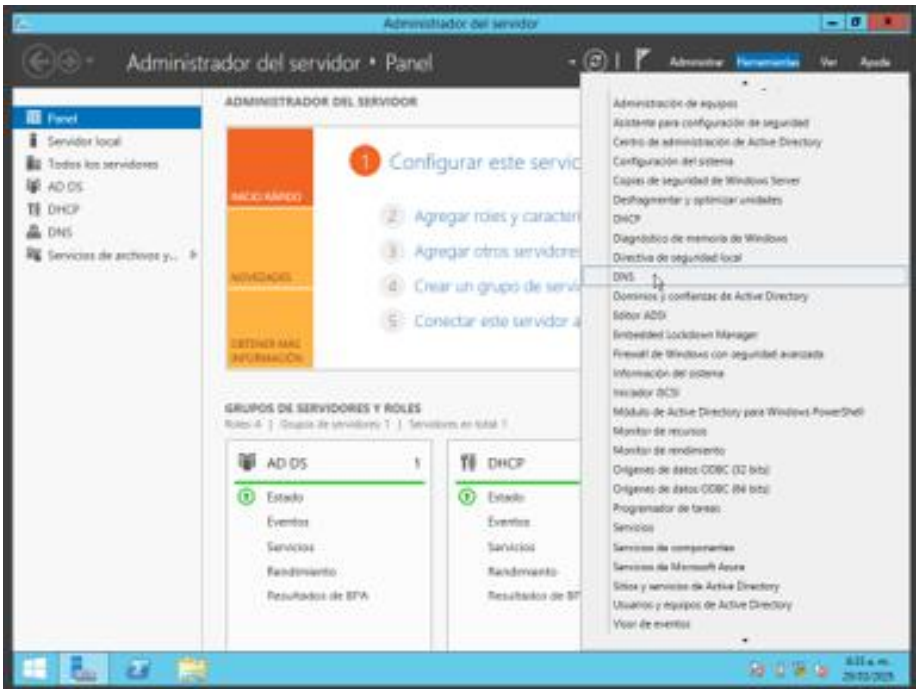



Clic en instalar los requisitos previos

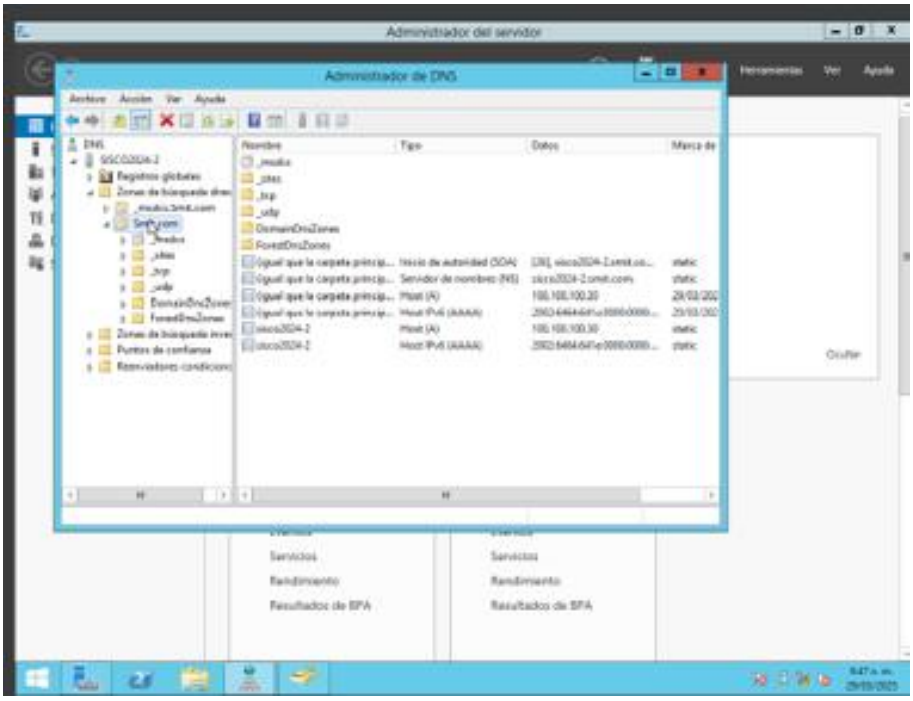


# Configuración de DNS

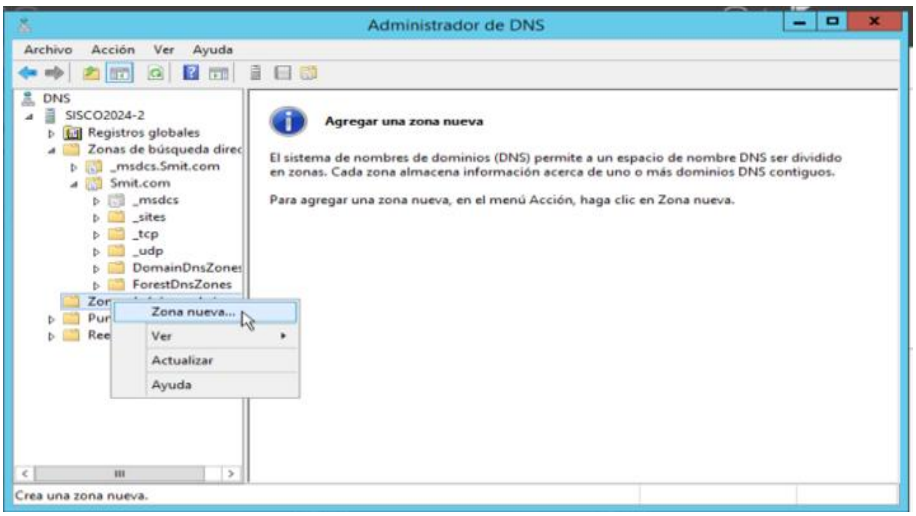
Aquí le enseñaremos a configurar el DNS le damos clic herramienta y luego en DNS



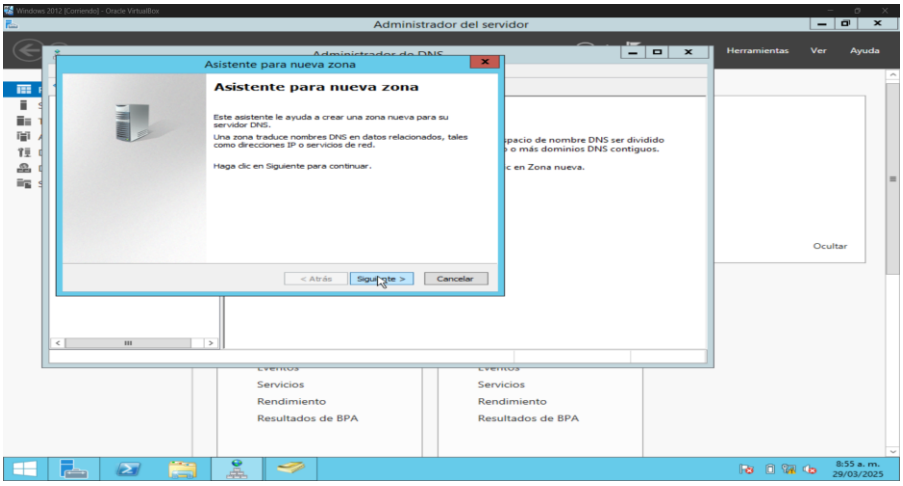

Clic en Smit.com para ver administrador del DNS



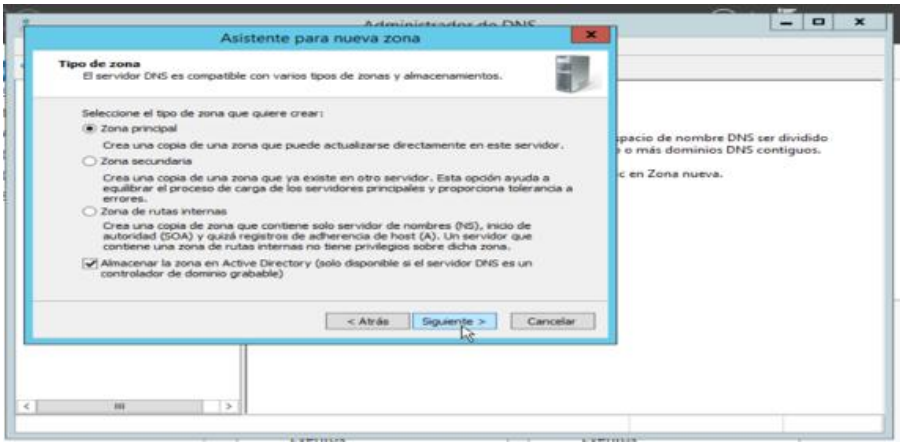
Le dan clic izquierdo en zona inversa luego clic zona nueva



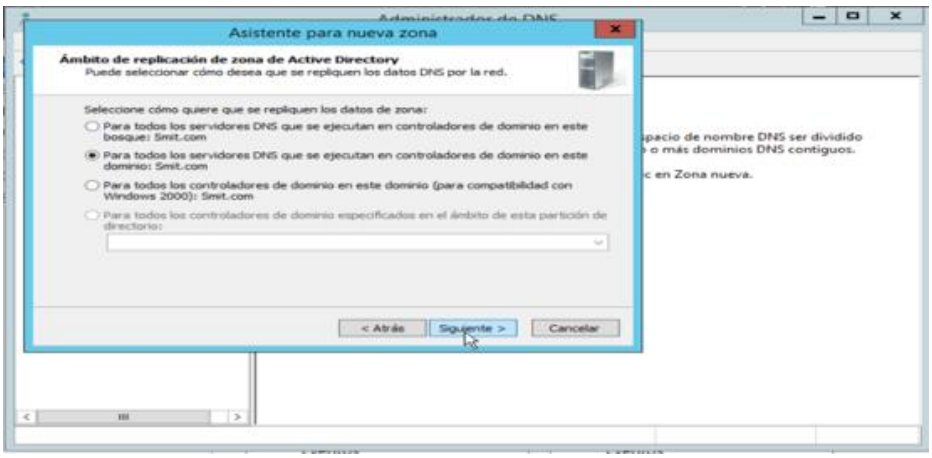

Clic en siguiente en asistente para zona nueva



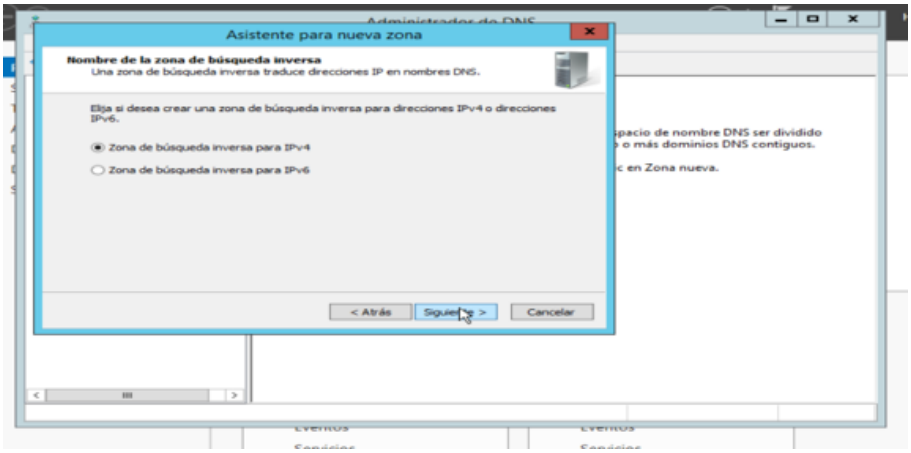

Le damos clic en zona principal y luego en siguiente para elegir el tipo de zona



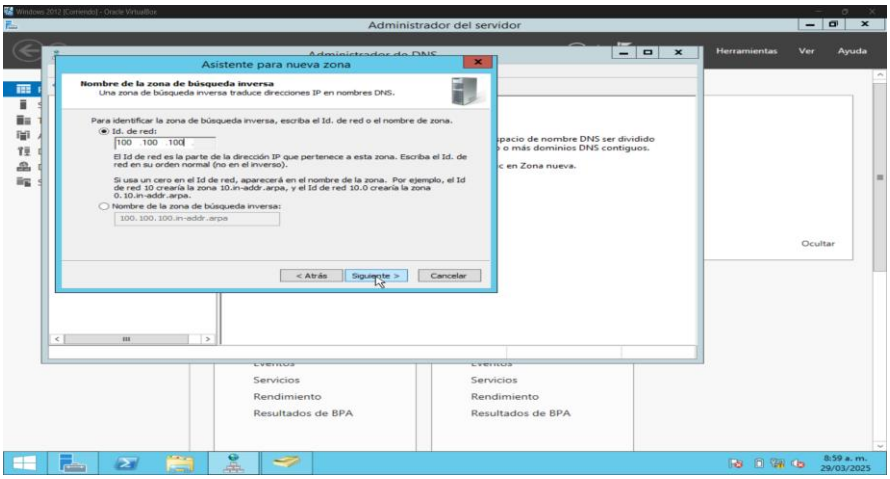
Clic en ámbito recomendado por el sistema y luego siguiente



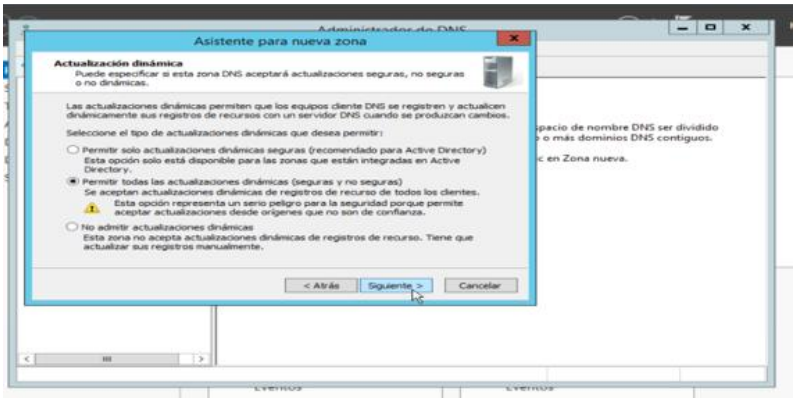

Le damos clic en zona de búsqueda inversa para IPv4



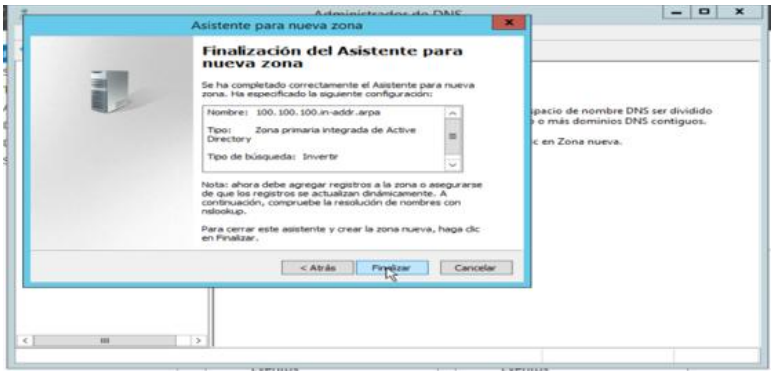

Agregamos la inversa de la IP del servidor (100.100.100)luego clic en siguiente



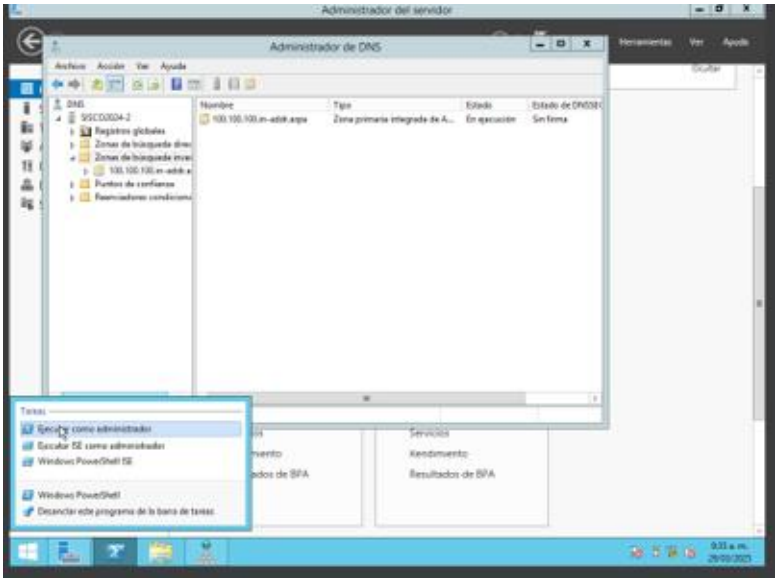
Luego clic en siguiente en actualización dinámica escoger la que mas requiera



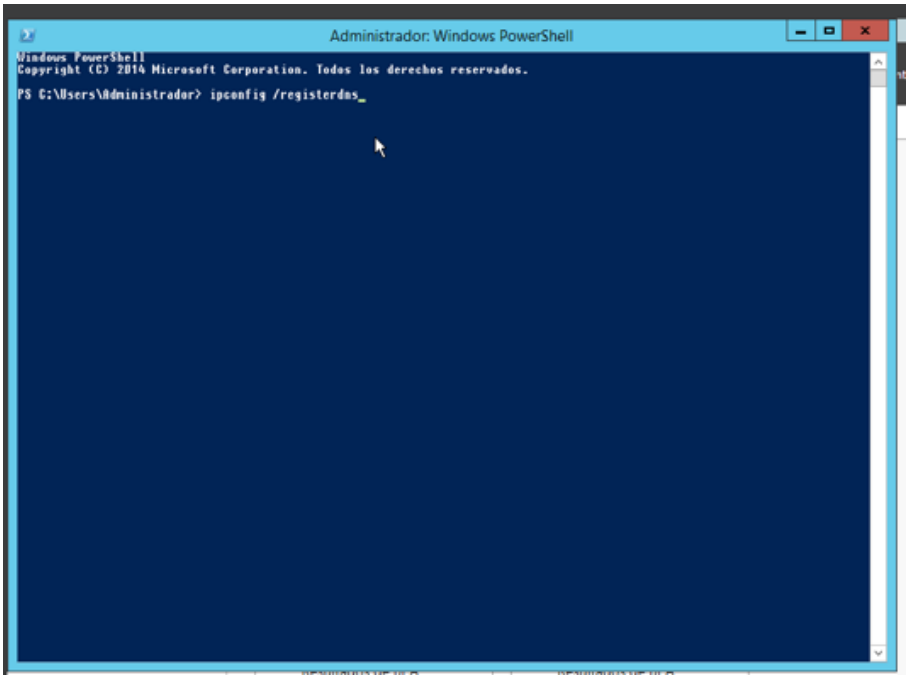

Luego clic en finalizar para terminar la configuración

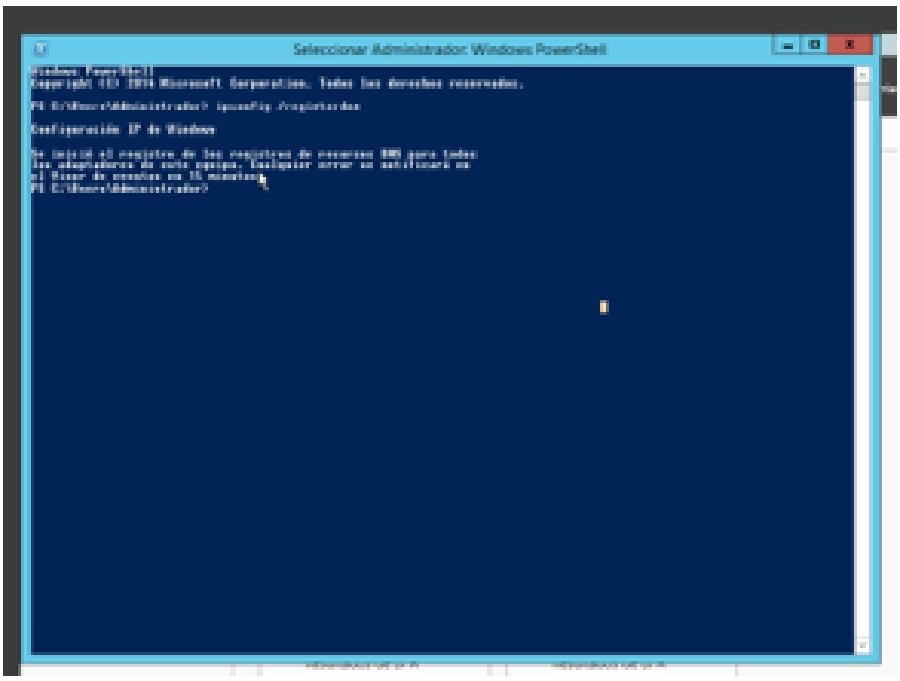



Asi le debe quedar la zona creada

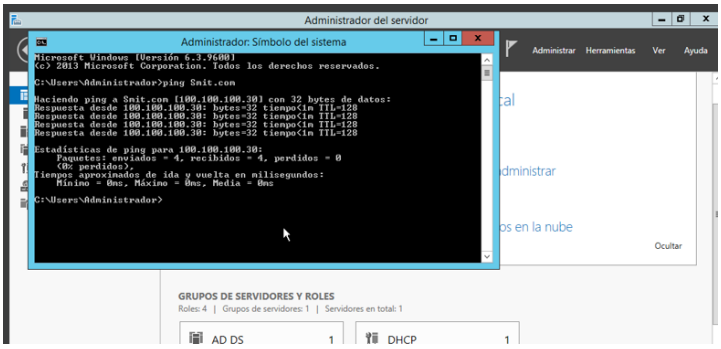


Le damos clic en administrador Windows PowerShell o en cmd  y agregamos el comando (ipconfig /registerdas) para activar todo las configuraciones

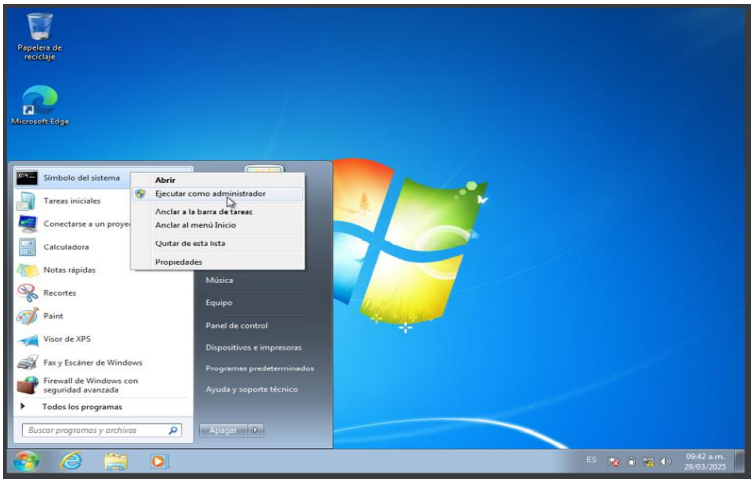


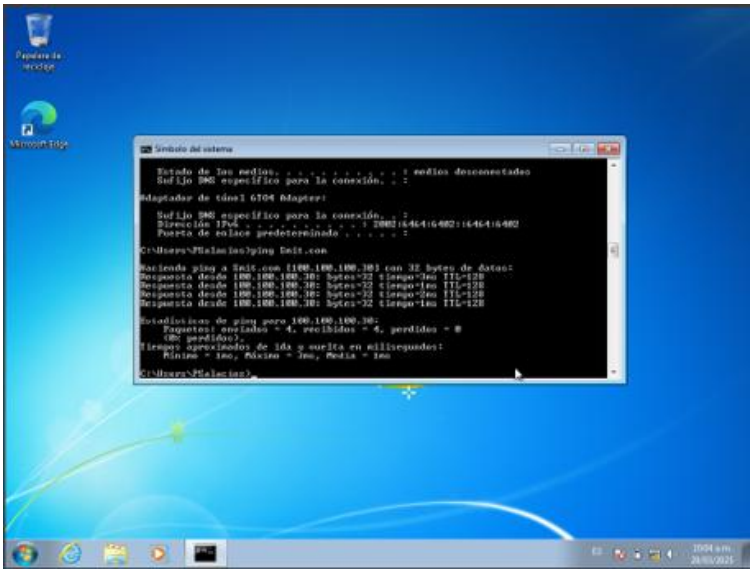
Entramos al cmd para agregar el comando (ping Smit.com) ver si agarro la configuración en nuestro DNS




Ingresamos a nuestra Windows 7 y clic ejecutar como administrador en el cmd

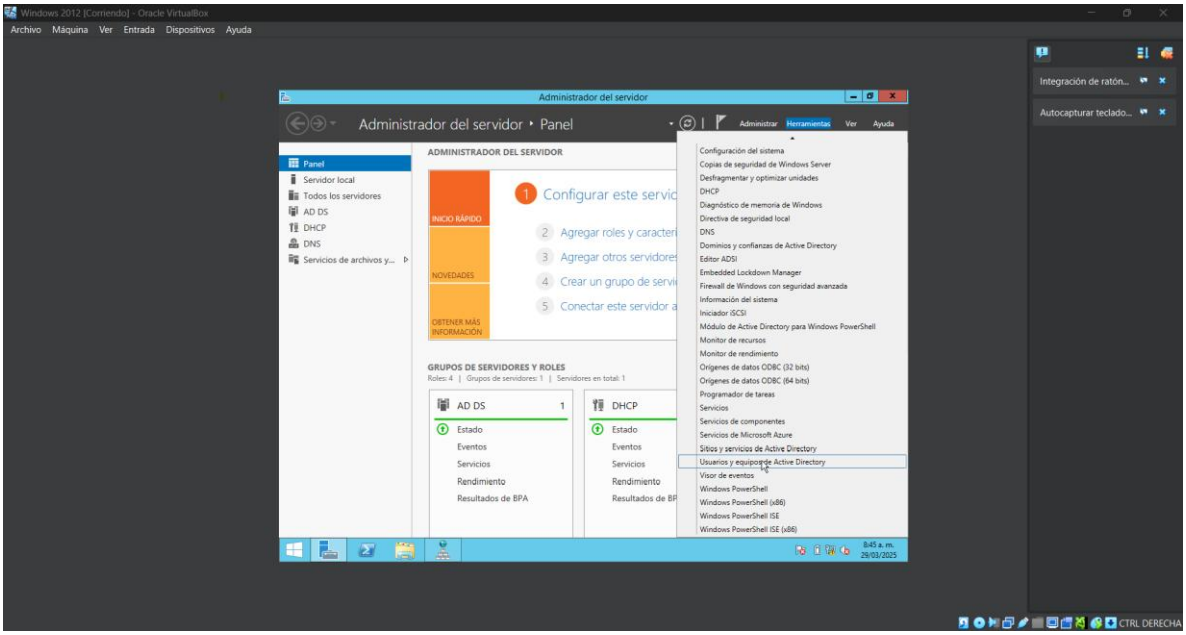



Entramos al cmd para agregar el comando (ping Smit.com) ver si agarro la configuración en nuestro DNS



# Configuración del directorio activo

Por la premura del tiempo no se pudo agregar la configuración del directorio activo pero para el informe n°4  estará la configuración y sus funciones dando pin de extremo a extremo




# Investigaciones

**Como crear un certificado digital en un directorio activo**

Servicios de certificados de Active Directory (AD CS) es un rol de Windows Server para emitir y administrar certificados de infraestructura de clave pública (PKI) que se usan en protocolos de autenticación y comunicación seguros.

Emisión y administración de certificados

Los certificados digitales se pueden usar para cifrar y firmar digitalmente documentos electrónicos y mensajes, así como para la autenticación de cuentas de equipo, usuario o dispositivo en una red. Por ejemplo, los certificados digitales se usan para proporcionar:

Confidencialidad mediante cifrado.

Integridad mediante firmas digitales.

Autenticación mediante la asociación de claves de certificado con cuentas de equipos, usuarios o dispositivos en un equipo red.

Características principales

AD CS proporciona las siguientes características importantes:

Entidades de certificación: las entidades de certificación raíz y subordinadas se usan para emitir certificados para los usuarios, equipos y servicios, y para administrar la validez de los certificados.

Inscripción web: la inscripción web permite a los usuarios conectarse con una entidad de certificación mediante un explorador web para solicitar certificados y recuperar listas de revocación de certificados (CRL).

Respondedor en línea: el servicio Respondedor en línea descodifica solicitudes de estado de revocación para certificados específicos, evalúa el estado de estos certificados y devuelve una respuesta firmada que contiene la información solicitada sobre el estado de los certificados.

Servicio de inscripción de dispositivos de red: el Servicio de inscripción de dispositivos de red permite obtener certificados a los enrutadores y otros dispositivos de red que no disponen de cuentas de dominio.

Atestación de clave de TPM: permite a la entidad de certificación (CA) comprobar que la clave privada está protegida por un TPM basado en hardware y que el TPM es de confianza para la entidad de certificación. La atestación de clave de TPM impide que el certificado se exporte a un dispositivo no autorizado y puede enlazar la identidad del usuario con el dispositivo.

Servicio web de directiva de inscripción de certificados: el Servicio web de directiva de inscripción de certificados permite que los usuarios y equipos obtengan información sobre directivas de inscripción de certificados.

Servicio web de inscripción de certificados: el Servicio web de inscripción de certificados permite que los usuarios y equipos obtengan información sobre directivas de inscripción de certificados. Junto con el Servicio web de directiva de

inscripción de certificados, permite la inscripción de certificados basada en directivas si el equipo cliente no es miembro de un dominio o si un miembro del dominio no está conectado a este.

Ventajas

Puede usar AD CS para aumentar la seguridad mediante el enlace de la identidad de una persona, un equipo o un servicio con la clave privada correspondiente. AD CS proporciona un método rentable, eficaz y seguro para administrar la distribución y el uso de certificados. Además del enlace de identidades y claves privadas, AD CS también incluye características que permiten administrar la inscripción y la revocación de certificados.

Puede usar la información de identidad del punto de conexión existente en Active Directory para registrar certificados, lo que significa que puede tener información insertada automáticamente en los certificados. AD CS también se puede usar para configurar directivas de grupo de Active Directory para designar a qué usuarios y máquinas se les permite qué tipos de certificados. La configuración de directiva de grupo habilita el control de acceso basado en roles o en atributos.

Algunas de las aplicaciones compatibles con AD CS son las extensiones seguras multipropósito al correo de Internet (S/MIME), las redes inalámbricas seguras, las redes privadas virtuales (VPN), el protocolo de seguridad de Internet (IPsec), el Sistema de cifrado de archivos (EFS), el inicio de sesión con tarjeta inteligente, los protocolos Capa de sockets seguros y Seguridad de la capa de transporte (TLS/SSL) y las firmas digitales.

**Cuál es el objetivo (cname y mx) de un dns**

Un registro CNAME "de nombre canónico" apunta desde un dominio alias a un dominio "canónico". Un registro CNAME se utiliza en lugar de un registro A, cuando un dominio o subdominio es un alias de otro dominio. Todos los registros CNAME deben apuntar a un dominio, nunca a una dirección IP. Imagina una búsqueda del tesoro en la que cada pista apunta a otra pista y la pista final apunta al tesoro. Un dominio con un registro CNAME es como una pista que puede apuntar a otra pista (otro dominio con un registro CNAME) o al tesoro (un dominio con un registro A).

Por ejemplo, supongamos que blog.example.com tiene un registro CNAME con el valor "example.com" (sin el "blog"). Esto quiere decir que cuando un servidor DNS accede a los registros DNS para blog.example.com, en realidad desencadena otra búsqueda DNS a example.com, devolviendo la dirección IP de example.com a través de su registro A. En este caso, diríamos que example.com es el nombre canónico (o nombre verdadero) de blog.example.com.

Con frecuencia, cuando los sitios tienen subdominios como blog.example.com o shop.example.com, esos subdominios tendrán registros CNAME que apuntan a un dominio raíz (example.com). De este modo, si la dirección IP del host cambia, solo hay que actualizar el registro A del DNS del dominio raíz y todos los registros CNAME seguirán junto con los cambios que se realicen en la raíz.

Un malentendido habitual es pensar que un registro CNAME debe resolver siempre al mismo sitio web que el dominio al que apunta, pero no es el caso. El registro CNAME solo apunta al cliente a la misma dirección IP que el dominio raíz. Una vez que el cliente llega a esa dirección IP, el servidor web seguirá manejando la URL en este sentido. Así, por ejemplo, blog.example.com puede tener un CNAME que apunte a example.com, dirigiendo al cliente a la dirección IP de example.com. Pero cuando el cliente se conecte realmente a esa dirección IP, el servidor web mirará la URL, verá que es blog.example.com y entregará la página del blog en lugar de la página de inicio.

Ejemplo de un registro CNAME:

| **blog.example.com** | **tipo de registro:** | **valor:** | **TTL** |
|---|---|---|---|
| @ | CNAME | es un alias de example.com | 32600 |

En este ejemplo, puedes ver que blog.example.com apunta a example.com y, si suponemos que se basa en nuestro registro A de ejemplo, sabemos que acabará por decidirse por la dirección IP 192.0.2.1.

## Conclusión

En resumen, tanto el Directorio Activo como el DNS son componentes esenciales para la administración eficiente de redes basadas en Windows Server 2012. Juntos, permiten una gestión centralizada y eficaz que mejora la seguridad y el rendimiento general del entorno informático.