SISTEMAS OPERATIVOS EN RED

UNIDAD 3 SERVICIO DE DIRECTORIO EN WINDOWS

UNIDAD 3 SERVICIO DE DIRECTORIO EN WINDOWS.

1. SERVICIO DE DIRECTORIO

Un **Directorio o Servicio de Directorio** es un conjunto de aplicaciones que sirve para, en una red informática, organizar y centralizar la información de los usuarios, equipos, grupos, dominios, recursos compartidos, políticas de seguridad, etc.

Al tener la información centralizada, se permite una mejor gestión de los recursos y un mayor control de acceso sobre los usuarios por parte del administrador.

En *Windows Server* contamos con el servicio de directorio **Active Directory**, que proporciona funcionalidades como las directivas de grupo, instalación remota de sistemas operativos y aplicaciones etc.

Cuando utilizamos **Active Directory**, tenemos a nuestra disposición herramientas de administración para creación de usuarios y grupos, establecer políticas de grupo, incluir unos grupos dentro de otros en diferentes niveles, un acceso sencillo al árbol de usuarios, ordenadores, impresoras y contactos, etc.

Active Directory permite simplificar y centralizar la administración de los usuarios y equipos y mejorar el acceso a los recursos de una red de ordenadores.

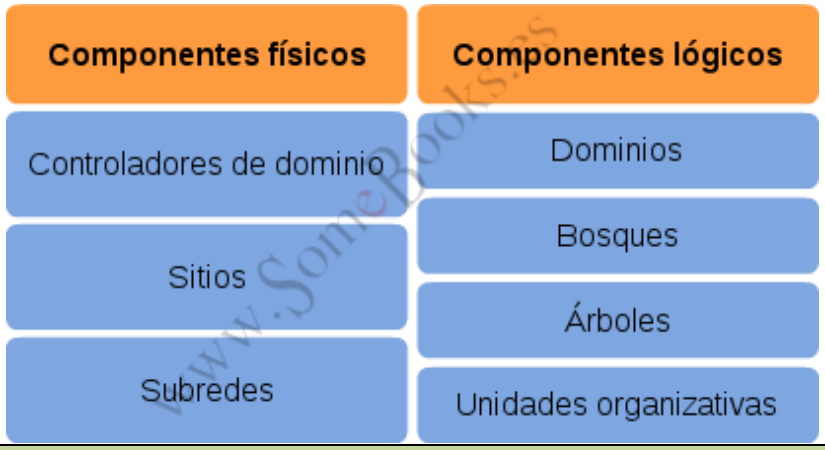
Para almacenar información sobre los usuarios, grupos y servicios relacionados utiliza una base de datos, pero la utilidad de AD es mayor, ya que, además de la información sobre los usuarios, mantiene información sobre los servidores, clientes, directivas de seguridad, etc.

Por otro lado, **Active Directory** resulta útil tanto en redes pequeñas como en instalaciones con millones de elementos relacionados.

Obviamente, podemos utilizar Windows Server 2016/2019 sin usar **Active Directory**, pero estaremos prescindiendo de un amplio conjunto de capacidades.

En cuanto a la estructura del servicio de directorio, lo primero que debemos saber es que existen dos tipos de componentes en **Active Directory**: *los componentes físicos* y *los componentes lógicos*.

Veámoslos representados en la siguiente tabla:



Active Directory está basado en una serie de estándares establecidos por la Unión Internacional de Telecomunicaciones (UIT) llamados X.500.

El protocolo LDAP se creó como una versión ligera de X.500

Una de las ventajas que ofrece **Active Directory** es que puede utilizar **LDAP** (Lightweight Directory Access Protocol, en español, Protocolo Ligero de Acceso a Directorios), un protocolo de acceso estándar que permitirá la consulta de información contenida en el directorio. Sin embargo, también puede utilizar ADSI (**Active Directory** Services Interface, en español, Interfaces de Servicio de **Active Directory**), un conjunto de herramientas ofrecidas por Microsoft, que tienen una interfaz orientada a objetos y que permiten el acceso a características de **Active Directory** Domain Services que no están soportadas por LDAP.

2. CONCEPTOS BÁSICOS EN UNA ESTRUCTURA DE DIRECTORIO ACTIVO

2.1. Dominio

Un **dominio** es un conjunto de equipos, usuarios y recursos de una misma red y bajo la misma base de datos de directorio.

Los dominios son las estructuras principales del AD. Todos los objetos forman parte de un dominio y la política de seguridad es uniforme en él.

Un controlador de dominio es un equipo con **Active Directory** instalado, que gestiona la base de datos de usuarios, grupos y recursos de red.

Para poner nombre a los dominios se utiliza el **protocolo DNS.** Por este motivo, **Active Directory** necesita al menos un servidor DNS instalado en la red

Cada dominio debe tener un nombre de dominio o DNS que lo identifica y que servirá para denominar a los equipos de la red que pertenezcan a ese dominio. Por ej. Si un **equipo1** pertenece al dominio **smrdominio.com** el nombre completo del equipo será **equipo1.smrdominio.com** y si en el mismo dominio existe una impresora **impr1** esta tendrá como nombre completo **impr1.smrdominio.com.**

Aunque en una red de Windows Server 20016/2019 deben estar configurados tanto **Active Directory** como DNS, los dominios de **Active Directory** y DNS tienen finalidades diferentes:

- Los dominios de **Active Directory** permiten administrar cuentas, recursos y los mecanismos de seguridad.
- Los dominios **DNS** establecen una jerarquía de dominios que se emplea, principalmente, para la resolución de nombres.

Los nombres de dominio válidos se restringen a las letras del código ASCII estándar Aa-Zz, los dígitos y el guión. El guión se admite, pero no debe tener más de un guión y no debe de empezar por él.

Actividad

De los siguientes nombres de dominios, di cuál serían correctos y cuáles no

A) servidor.es
B) mi-servidor.es
C) mi--servidor.es
D) mi.-.servidor.es
E) –servidor.es

2.2. Objeto

La palabra **Objeto** se utiliza como nombre genérico para referirnos a cualquiera de los componentes que forman parte del directorio, como una impresora o una carpeta compartida, pero también un usuario, un grupo, etc. Incluso podemos utilizar la palabra objeto para referirnos a una **Unidad organizativa**.

Cada objeto dispondrá de una serie de características específicas (según la clase a la que pertenezca) y un nombre que permitirá identificarlo de forma precisa.

Como veremos más adelante, las características específicas de cada tipo de objeto quedarán definidas en el **Esquema de la base de datos**.

Definición de usuario:

Desde un punto de vista informático, un usuario es un conjunto de permisos y de privilegios sobre determinados recursos.

En este sentido, un usuario no tiene que ser, necesariamente, una persona.

En general, los objetos se organizan en tres categorías:

Usuarios: identificados a través de un nombre (y, casi siempre, una contraseña), que pueden organizarse en grupos, para simplificar la administración.

Recursos: que son los diferentes elementos a los que pueden acceder, o no, los usuarios según sus privilegios. Por ejemplo, carpetas compartidas, impresoras, etc.

Servicios: que son las diferentes funciones a las que los usuarios pueden tener acceso. Por ejemplo, el correo electrónico.

Cuando instalamos **Active Directory** en un ordenador con Windows Server 2016/2019, convertimos a ese ordenador en un **Controlador de dominio**. .

Existen objetos que pueden contener a su vez otros objetos, como es el caso de los grupos de usuarios y de las unidades organizativas.

2.3. Controlador de dominio

Un **Controlador de dominio** (domain controller) contiene la base de datos de objetos del directorio para un determinado dominio, incluida la información relativa a la seguridad. Además, será responsable de la autenticación de objetos dentro de su ámbito de control.

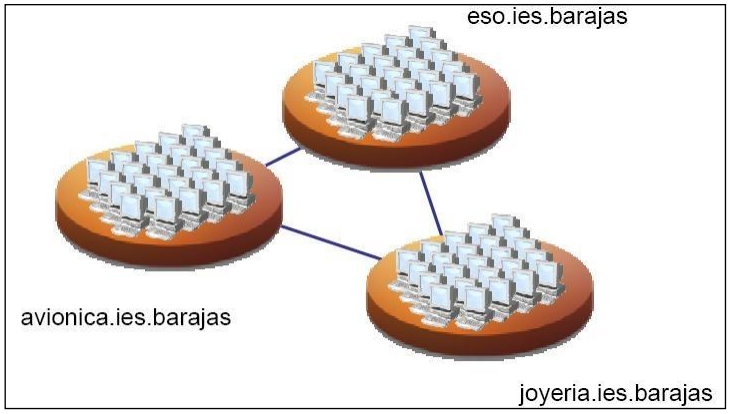
En un dominio dado, puede haber varios controladores de dominio asociados, de modo que cada uno de ellos represente un rol diferente dentro del directorio. Sin embargo, a todos los efectos, todos los controladores de dominio, dentro del mismo dominio, tendrán la misma importancia.

AD permite la replicación de controladores de dominio. Es decir, se puede enviar la información contenida en la base de datos a diferentes controladores de dominio a través de la red.

De esta forma, un usuario creado en un determinado controlador de dominio, podría iniciar sesión en cualquier cliente unido a otro controlador de dominio diferente sin ninguna complicación.

2.4. Árboles

Un **Árbol** es simplemente una colección de dominios que dependen de una raíz común y se encuentran organizados como una determinada jerarquía. Dicha jerarquía también quedará representada por un espacio de nombres DNS común.



Árbol de dominios del IES Barajas

De esta forma, sabremos que los dominios **gonzalonazareno.es** e **informatica.gonzalonazareno.es** forman parte del mismo árbol, mientras que **pino.com** y **empresa.pino.es** no.

El objetivo de crear este tipo de estructura es fragmentar los datos del Directorio Activo, replicando sólo las partes necesarias y ahorrando ancho de banda en la red.

Si un determinado usuario es creado dentro de un dominio, éste será reconocido automáticamente en todos los dominios que dependan jerárquicamente del dominio al que pertenece.

Actividad

De los siguientes dominios ¿Cuáles formarían un árbol de dominio si el dominio raíz es servidor.es? Diséñalo gráficamente

A) tres.servidor.es B) uno.servidor.es
C) dos.servidor2.es
D) dep1.uno.servidor.es
E) dos.es.servidor
F) dep2.uno.servidor.es

2.5. Bosque

El **Bosque** es el mayor contenedor lógico dentro de **Active Directory**, abarcando a todos los dominios dentro de su ámbito. Los dominios están interconectados por **Relaciones de confianza transitivas** que se construyen automáticamente. De esta forma, todos los dominios de un bosque confían automáticamente unos en otros y los diferentes árboles podrán compartir sus recursos.

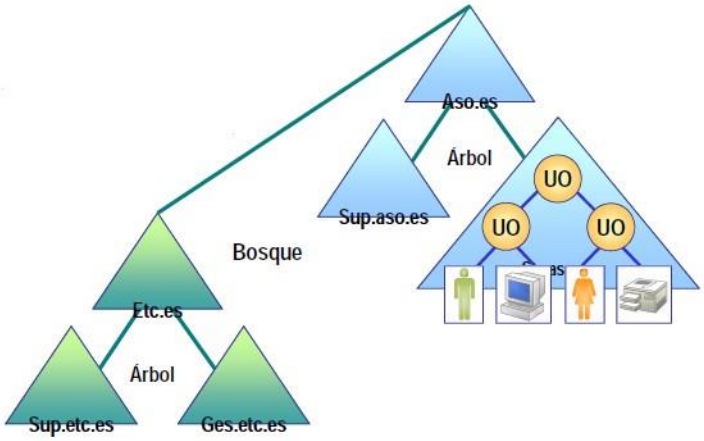
Como ya hemos dicho, los dominios pueden estar organizados jerárquicamente en un árbol que comparte un espacio de nombres DNS común. A su vez, diferentes árboles pueden estar integrados en un bosque. Al tratarse de árboles diferentes, no compartirán el mismo espacio de nombres.

De forma predeterminada, un bosque contiene al menos un dominio, que será el dominio raíz del bosque. En otras palabras: cuando instalamos el primer dominio en un ordenador de nuestra red que previamente dispone de Windows Server 2016/2019, además del propio dominio, estamos creando la raíz de un nuevo árbol y también la raíz de un nuevo bosque.

El dominio raíz del bosque contiene el **Esquema del bosque**, que se compartirá con el resto de dominios que formen parte de dicho bosque.

En la siguiente imagen se puede apreciar un bosque de dominio, que está formado por dos árboles:

1) El que tiene por dominio raíz a **Etc.es**.
2) El que tiene por dominio raíz a **Aso.es**.



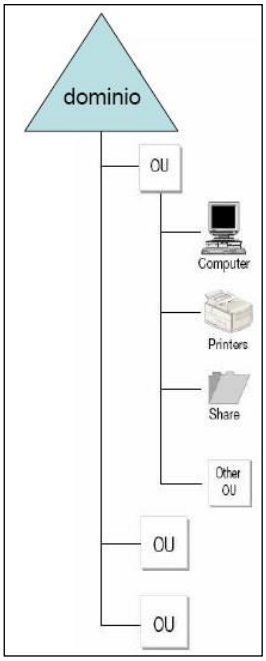
Bosque de dominio

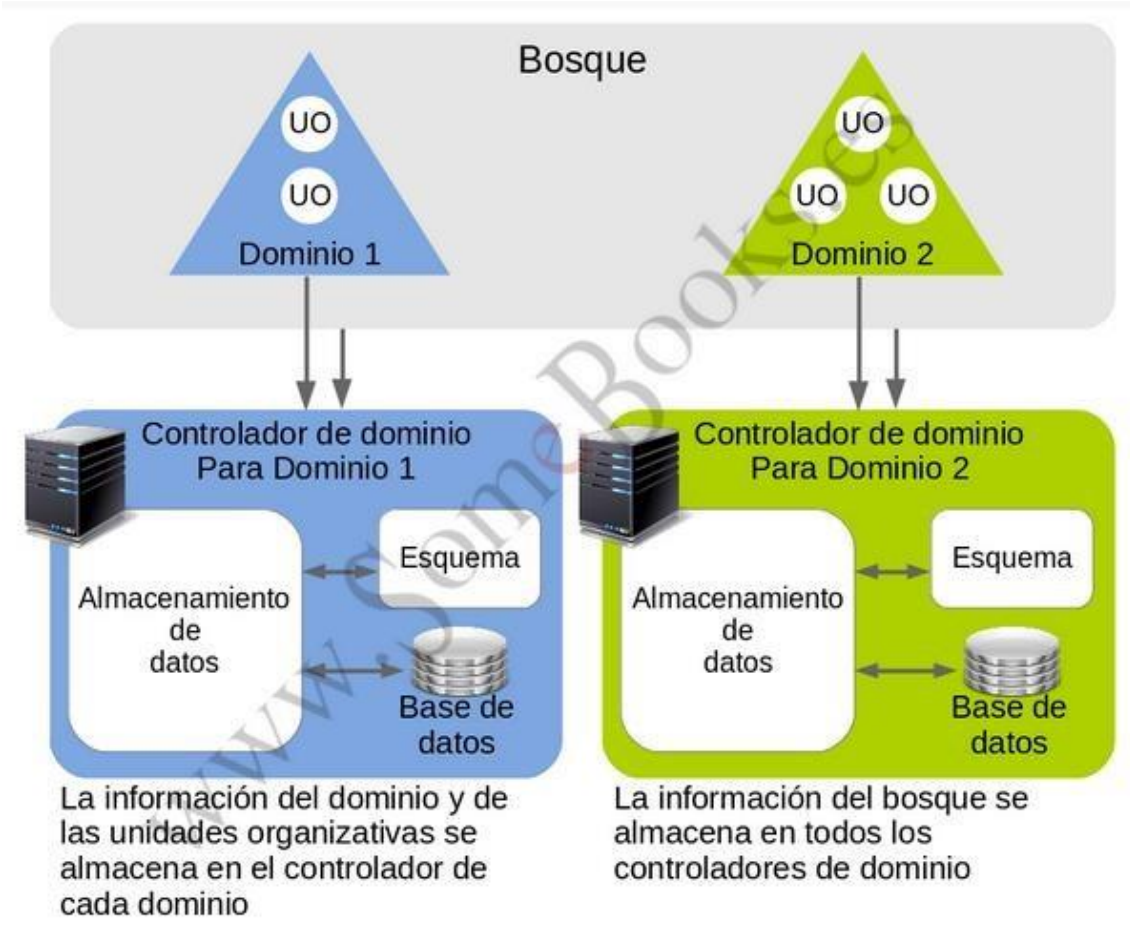
2.6. Unidad Organizativa

Una **Unidad Organizativa** (UO) es un contenedor de objetos como usuarios, grupos y equipos con unos requisitos comunes para su mantenimiento, administración y configuración y así evitar tener mezclado elementos de diferentes categorías.

Una vez creada una unidad organizativa, se puede modificar sin que afecte al funcionamiento de nuestro equipo.

La unidad organizativa se creará sobre un dominio, u otra UO, así que a la hora de crearla hay que indicar primero dónde la vamos a crear.



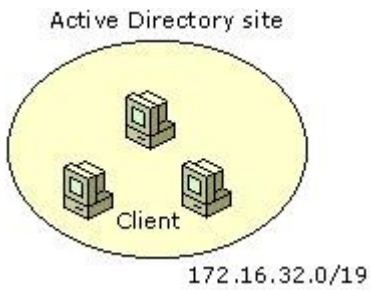


2.7. Sitio

En **Active Directory**, un **sitio** es un conjunto de equipos correctamente conectados mediante una red de alta velocidad, como por ejemplo una red de área local (LAN).

Todos los equipos pertenecientes al mismo sitio normalmente se encuentran en el mismo edificio o en la misma red corporativa. Un solo sitio consta de una o varias subredes de Protocolo Internet (IP). Las subredes son subdivisiones de una red IP, donde cada subred posee su propia y exclusiva dirección de red.

La siguiente ilustración muestra varios clientes dentro de una subred que define un sitio de **Active Directory**.



Los sitios y las subredes se representan en **Active Directory** por medio de objetos de sitio y subred que se pueden crear mediante Sitios y servicios de Active Directory. Cada objeto de sitio se asocia con uno o varios objetos de subred.

Un sitio es un componente físico del AD.

Es importante no confundir los términos *sitio* y *dominio*:

- **Dominio**: agrupación lógica de usuarios y equipos.
- **Sitio**: agrupación física de equipos.

2.8. Catálogo Global en AD

El **catálogo global** es un almacén central de información de todos los objetos del directorio de los dominios del bosque. Tiene una copia completa de todos los objetos (todos sus atributos) del directorio de su dominio y una copia parcial (almacena los atributos usados con más frecuencia en las operaciones de búsqueda) de todos los objetos de los directorios de los otros dominios del bosque.

Cuando se instala **Active Directory** (AD DS), se crea el catálogo global para un nuevo bosque automáticamente en el primer controlador de dominio del bosque. Se puede agregar la funcionalidad de catálogo global a otros controladores de dominio adicionales. También se puede quitar el catálogo global de un controlador de dominio.

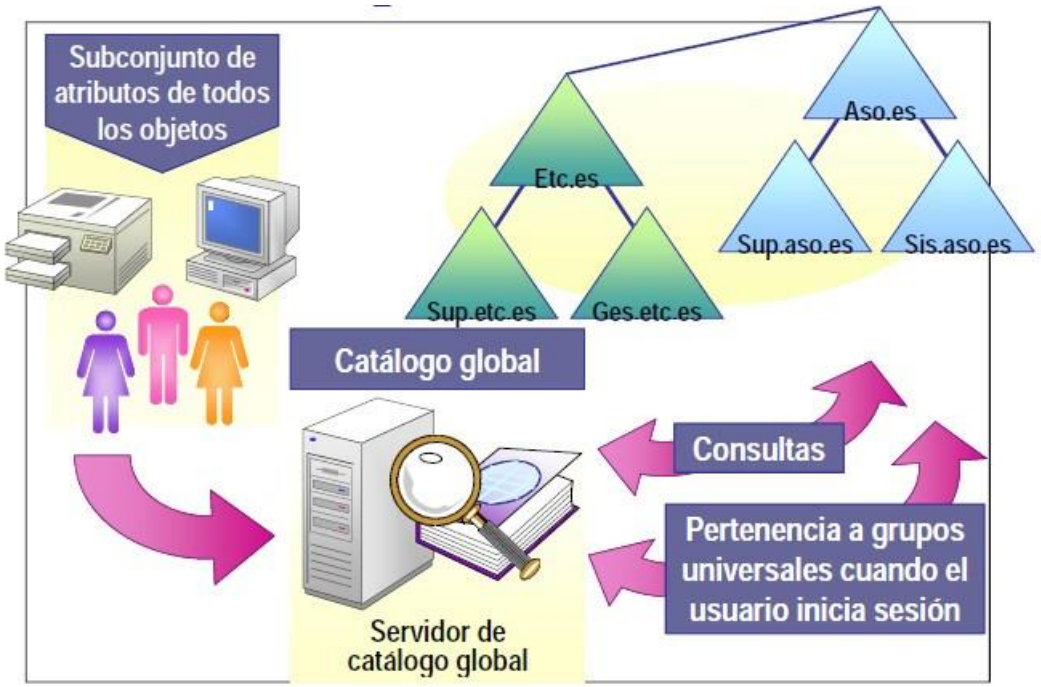
Como ya sabemos **Active Directory** funciona mediante una base de datos central en la que se almacenan todos los objetos del directorio, cuando se inicia sesión en un cliente de la red o se accede a un recurso del directorio se envía una consulta al controlador de dominio el cual responde indicando si el objeto existe y si se puede acceder a este o no.

Esto es así ya que todos los controladores de dominio son a la vez servidores de catálogo global para su dominio lo que implica que guardan la información de todos los objetos.

Pero todo esto va aún más lejos cuando trabajamos con redes más complejas compuestas por dos o más dominios que forman un árbol o un bosque, en este caso los servidores de catálogo global almacenan también parte de la información de los otros dominios en los que conviven.

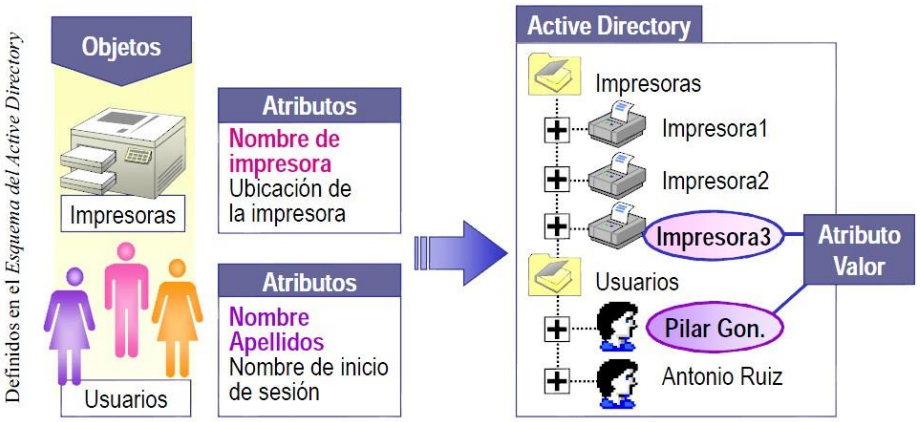
En este caso el servidor de catálogo global almacena una lista completa del resto de objetos, no así de todos sus atributos lo que podría llegar a ser un problema en redes muy grandes.

Gracias a esto podemos solicitar o acceder a un recurso de un dominio distinto del nuestro que se encuentre en el mismo bosque.



2.9. Esquema

En **Active Directory** Domain Services se utiliza la palabra **Esquema** para referirse a la estructura de la base de datos. En este sentido, utilizaremos la palabra atributo para referirnos a cada uno de los tipos de información almacenada.



2.10. Relaciones de confianza

En el contexto de **Active Directory**, las **Relaciones de confianza** son un método de comunicación seguro entre dominios, árboles y bosques. Las relaciones de confianza permiten a los usuarios de un dominio del Directorio Activo autenticarse en otro dominio del directorio. Además, permite a los dominios compartir usuarios y grupos y por tanto, asignar permisos a usuarios o grupos de otro dominio.

El dominio que confía es el encargado de autenticar el inicio de sesión del dominio en el que confía. Esto permite que los usuarios del último puedan acceder a los recursos del dominio que confía. Es decir, si el dominio A confía en el dominio B, el dominio A autenticará a los usuarios del B y los usuarios del B podrán acceder a los recursos del dominio A.

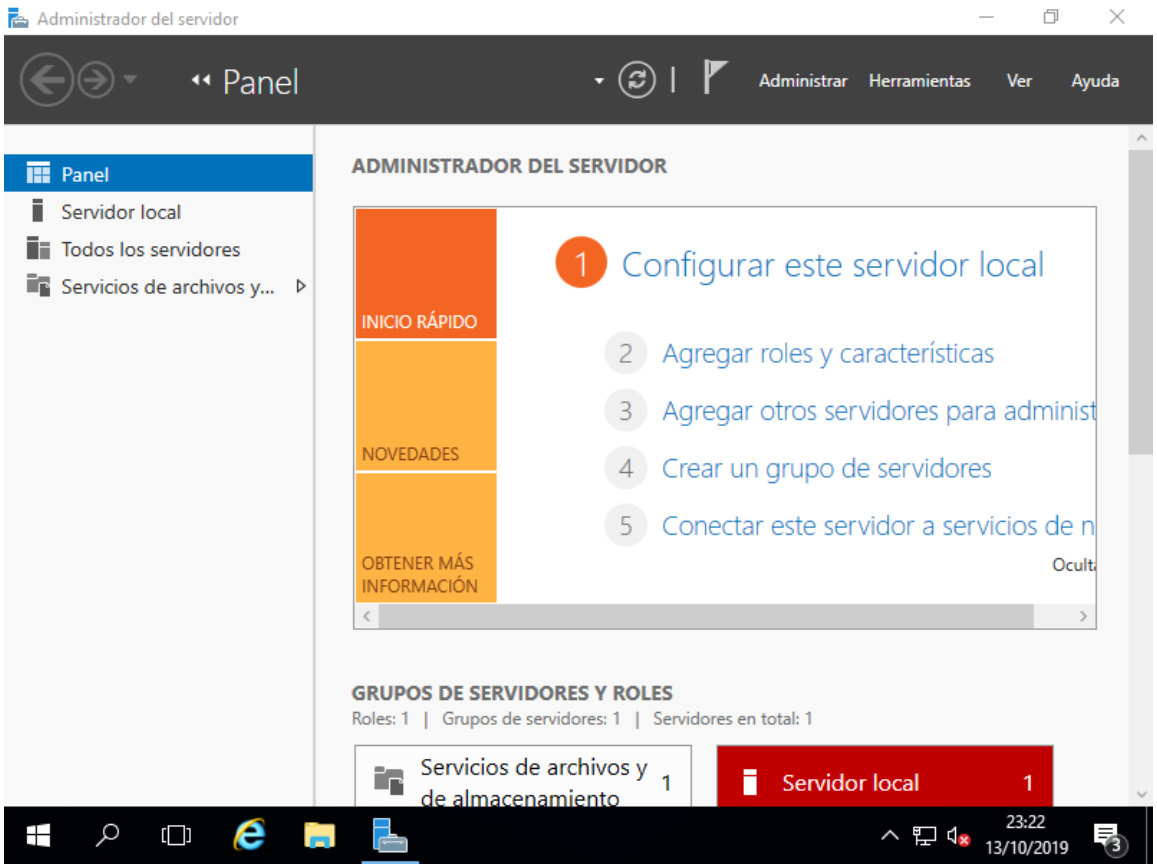
Existen dos tipos de relaciones de confianza: unidireccionales y bidireccionales. Además, las relaciones de confianza pueden ser transitivas (A confía en B y B confía en C, luego A confía en C).

3. INSTALACIÓN DEL DIRECTORIO ACTIVO

Según lo que hemos comentando en anteriormente, es evidente que para poder obtener el máximo rendimiento de nuestro servidor Windows Server 2016/2019 debemos convertirlo en un controlador de dominio primario.

Para llevar a cabo el proceso descrito en el párrafo anterior, autenticados en el equipo "SERVIDOR" con las credenciales del usuario "Administrador", ejecutaremos el **Administrador del servidor del equipo.**

"SERVIDOR" Windows Server 2016/2019, y una vez en ella nos situaremos sobre el apartado *Agregar roles y características*.

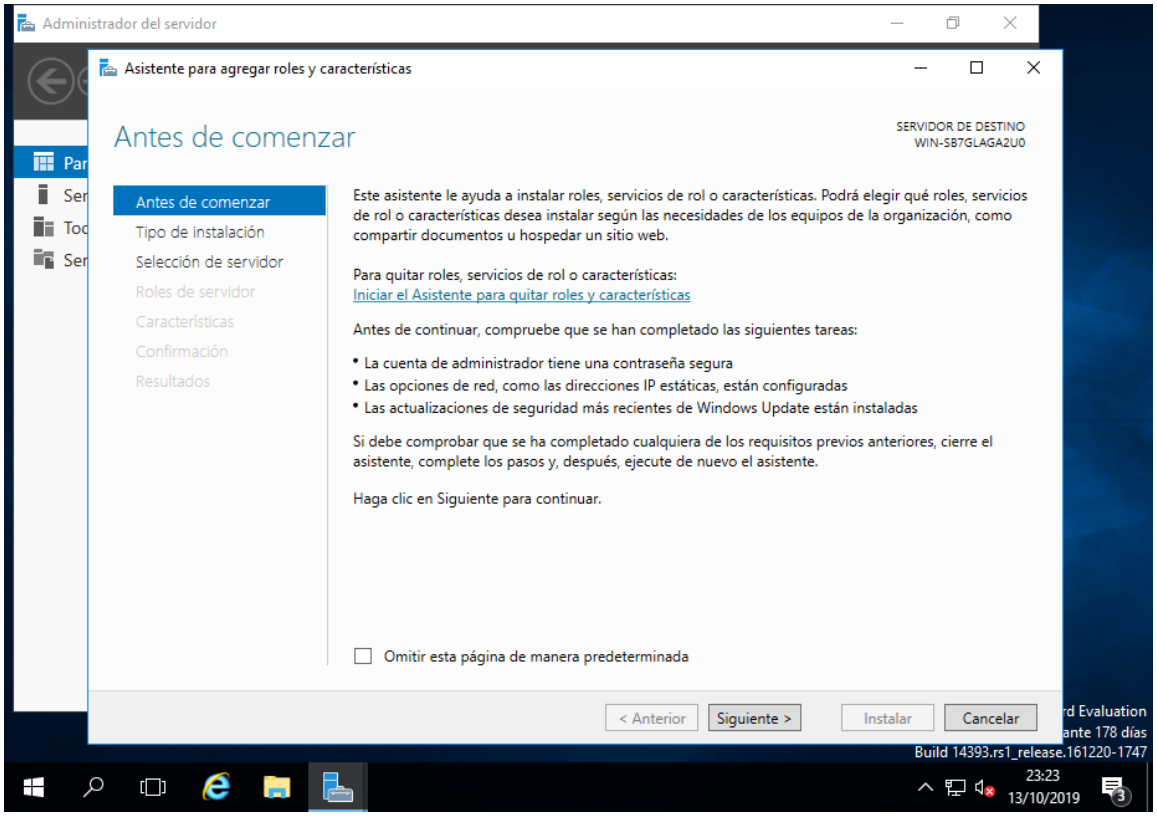


Como resultado de la acción anterior se nos presentará la primera ventana del asistente de agregación de funciones del servidor. Una vez configurados el nombre y la dirección IP del servidor procedemos a instalar los roles respectivos. Instalando el rol de directorio activo. Desde el Administrador el servidor seleccionamos la opción Agregar roles y características donde veremos el siguiente asistente, que nos indica que debemos comprobar que se han completado las siguientes tareas previas:

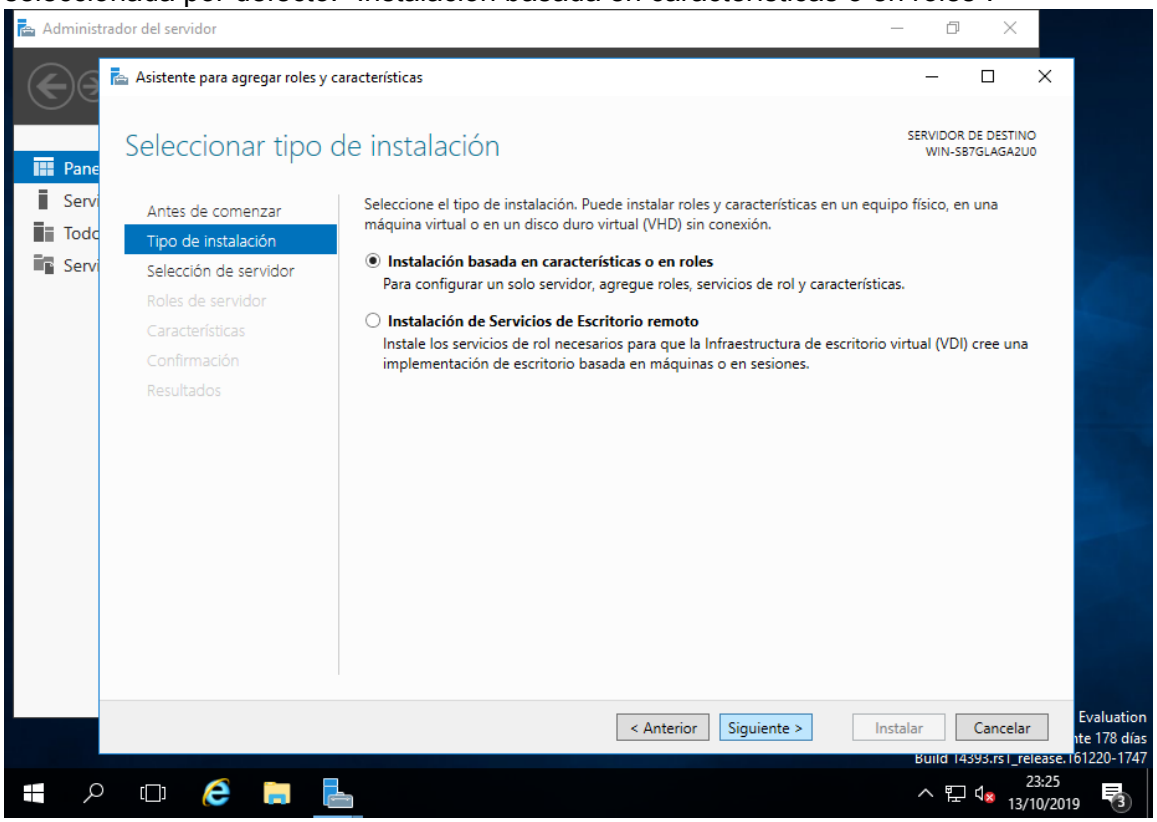
- La cuenta administrador tiene una contraseña segura.

- Las direcciones IP como las direcciones de red estáticas, están configuradas.
- Las actualizaciones de Windows Update están instaladas.

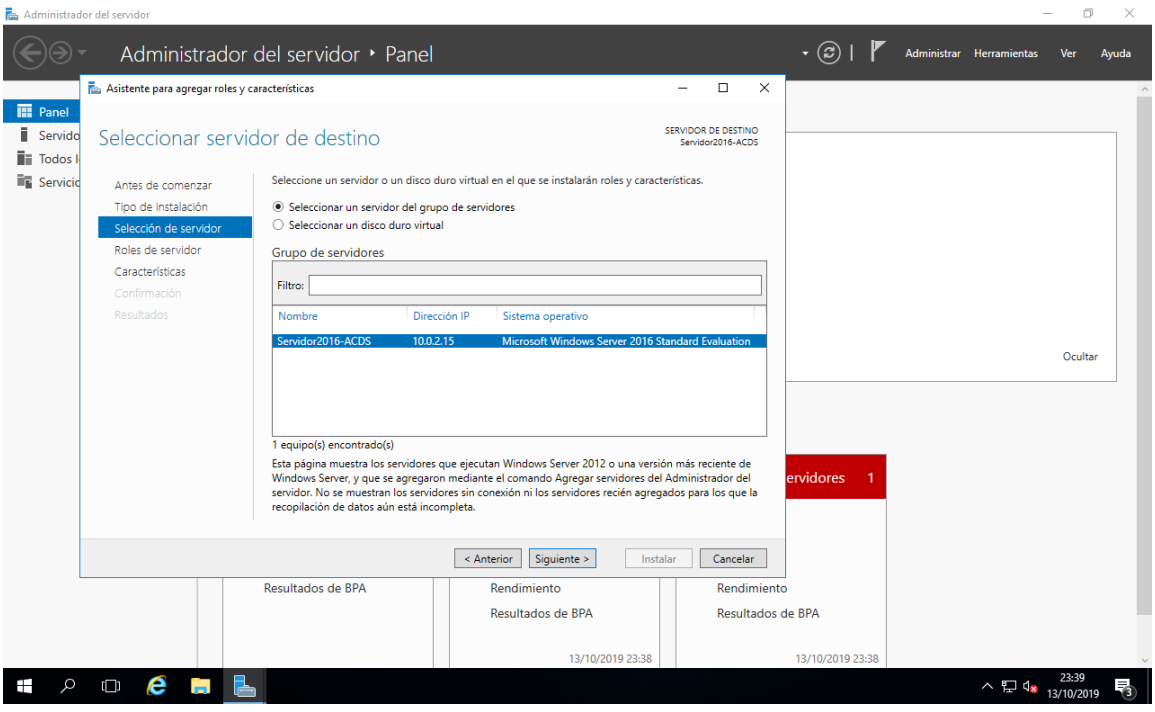
, y tras ello pulsaremos sobre el botón **Siguiente**.



Pulsamos Siguiente para elegir el tipo de instalación la cual será la que está seleccionada por defecto: “Instalación basada en características o en roles”.

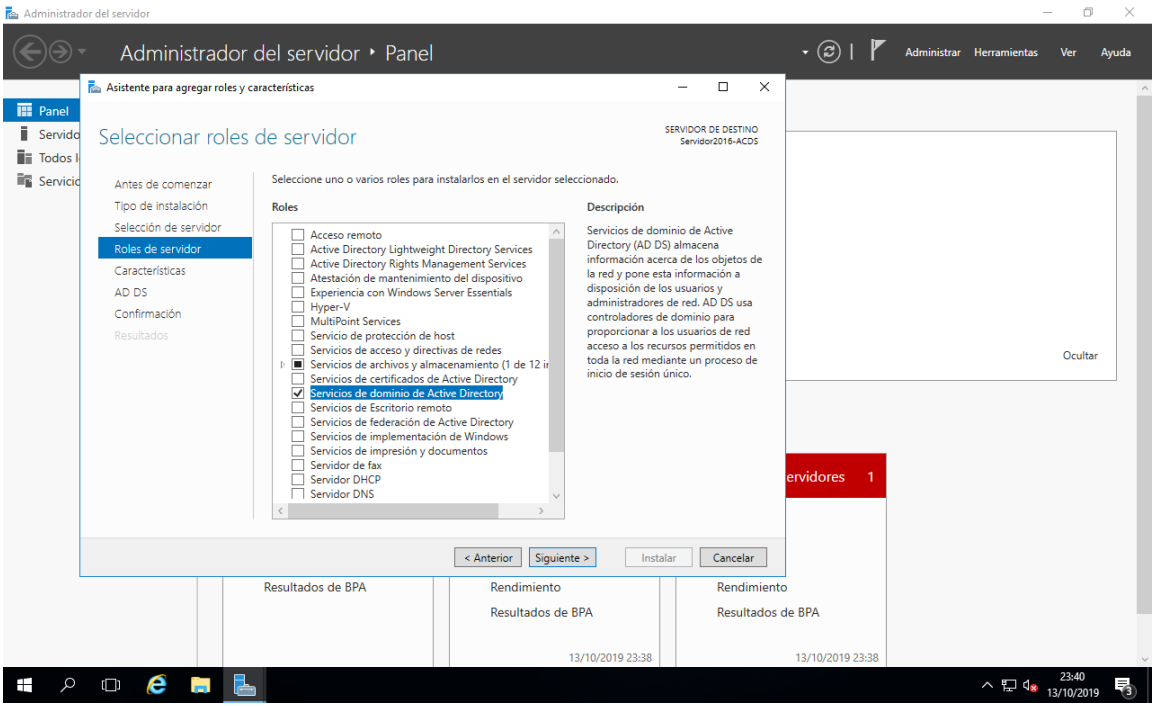


Pulsamos Siguiente y en la siguiente ventana seleccionamos el servidor donde instalaremos el rol.

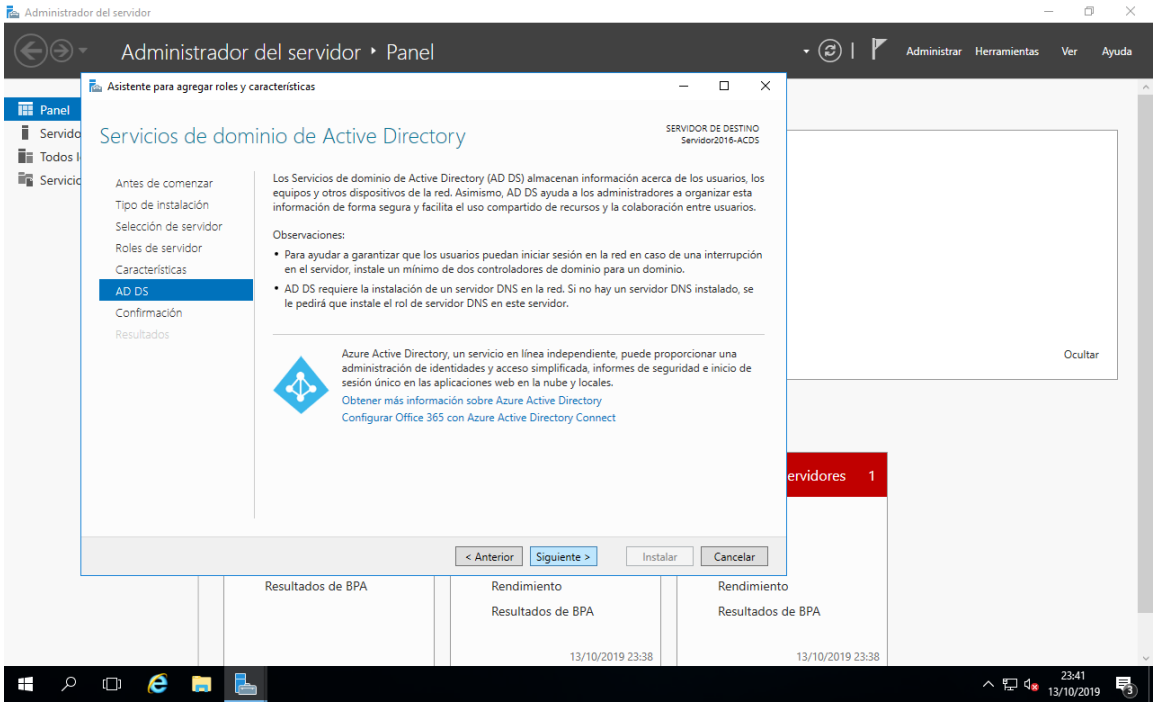


Pulsamos de nuevo Siguiente y en la siguiente ventana seleccionamos la casilla “Servicios de dominio de Active Directory”. (Lo normal es también seleccionar servidor DNS y DHCP. Pero eso ya irá en gusto y necesidades de cada empresa).

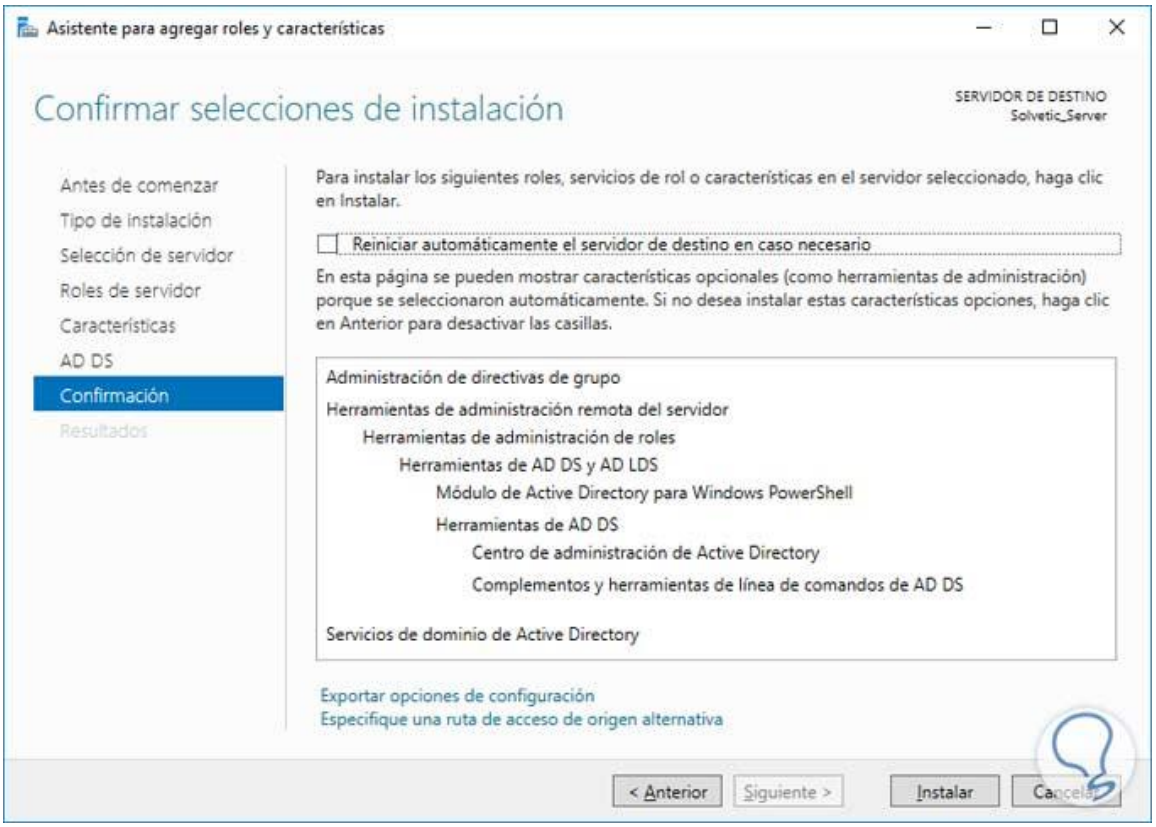
Activando pues, en nuestro caso, la casilla **Servicios de dominio de Active Directory** para configurar como controlador de dominio este equipo *Windows Server 2016/2019*, tras lo cual pulsaremos sobre el botón **Siguiente**.



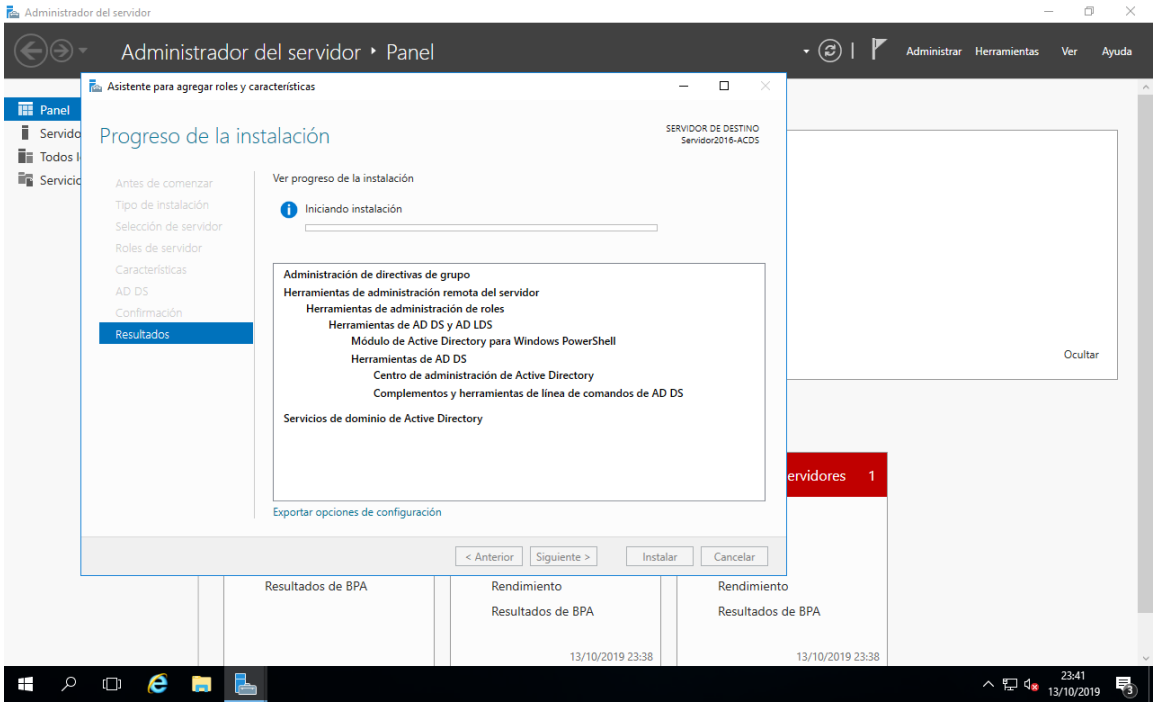
En la siguiente ventana se nos informa de las características de la función que estamos a punto de instalar, así como de los requisitos y configuraciones que precisamos para instalar el servicio correspondiente; en dicha ventana pulsaremos directamente sobre el botón **Siguiente**.



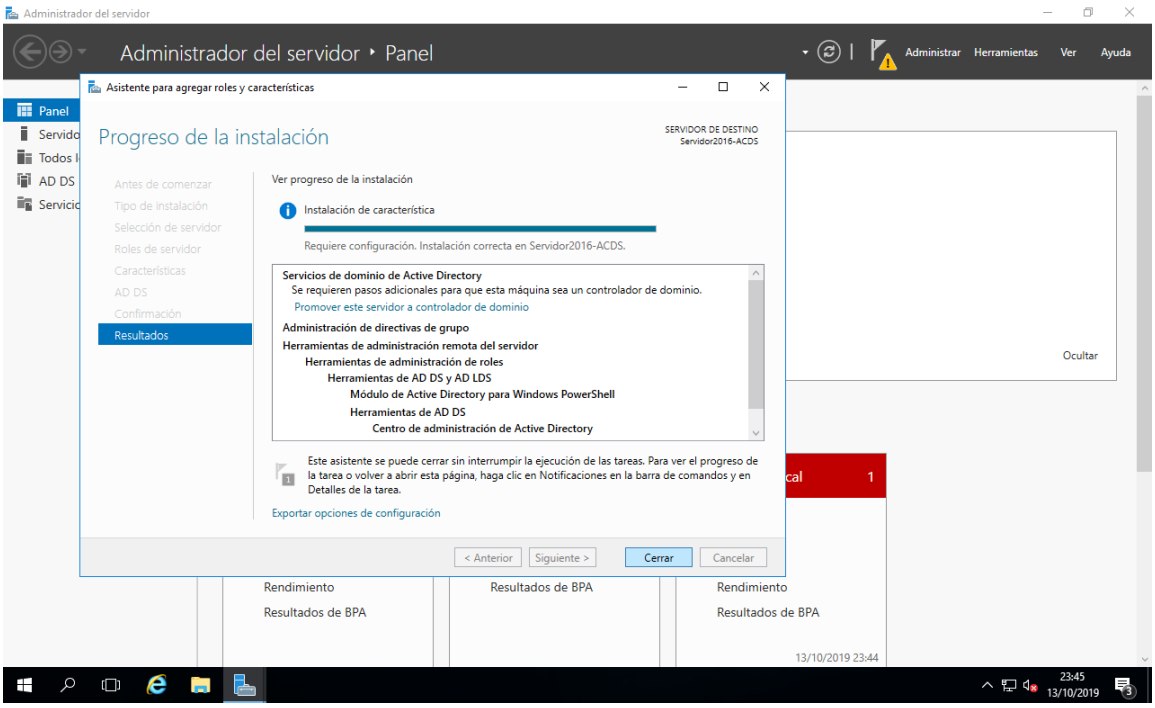
El asistente de instalación del servicio solicitado, nos informa de que está preparado para instalarlo con las configuraciones especificadas, así pues pulsaremos en dicha ventana sobre el botón **Instalar** para dar comienzo de modo efectivo al proceso de instalación.



El proceso de instalación dará comienzo pues según lo previsto.



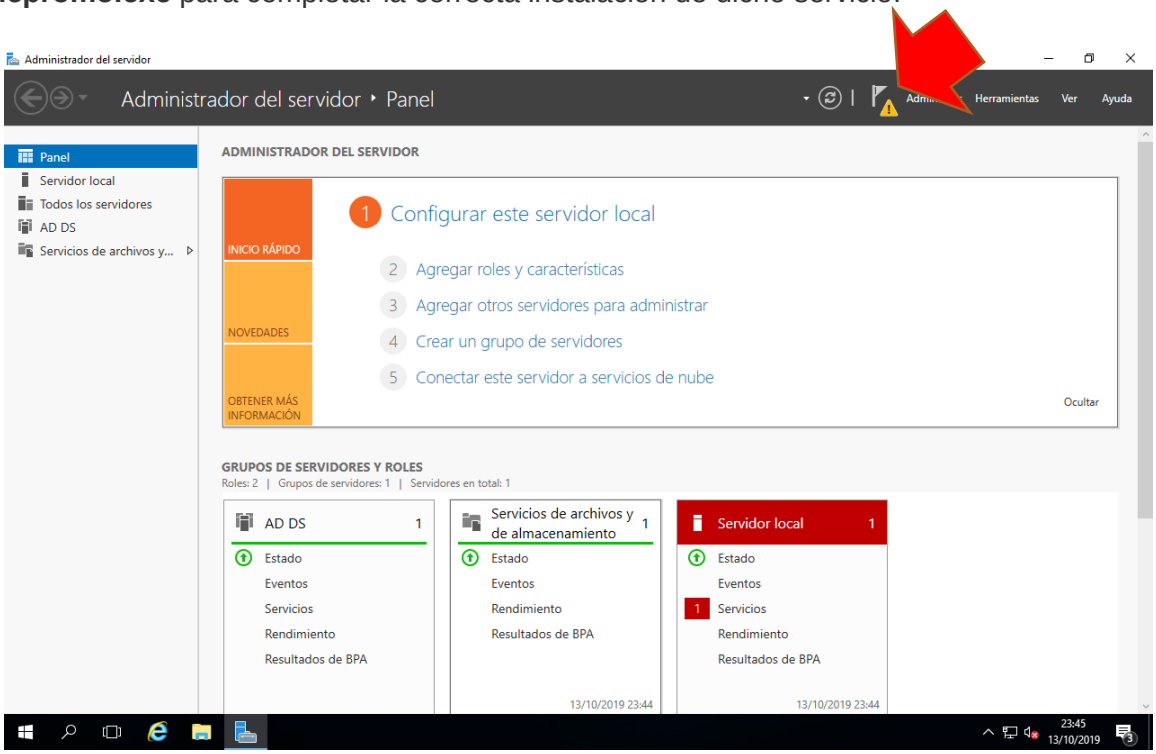
Una vez concluido el proceso de instalación del servicio de dominio de ***Active Directory***, se nos informa de que dicho proceso se ha efectuado correctamente, y se nos comunica de que para completar la instalación y configurar el servicio instalado deberemos ejecutar el comando **dcpromo.exe** para promocionar el equipo "SERVIDOR" *Windows Server 2016/2019* a controlador de dominio; cerraremos el asistente de instalación pulsando sobre el botón **Cerrar** en la ventana de la imagen inferior.



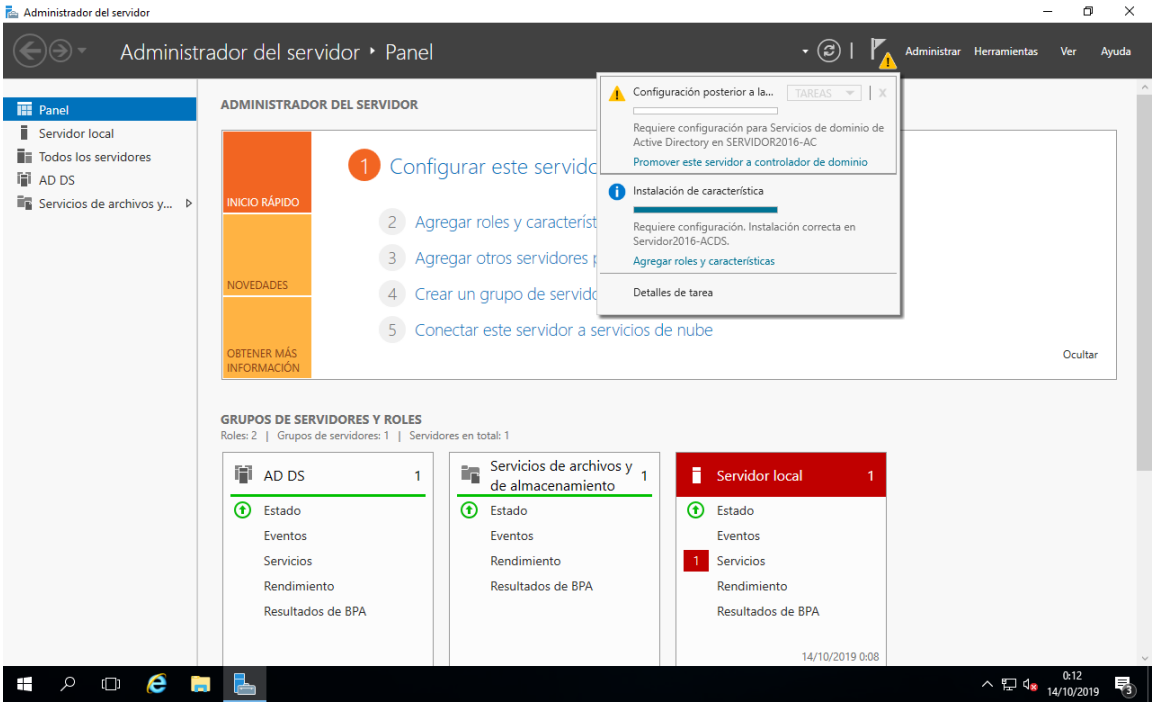
Llegados a este punto podremos dar por concluido este apartado, quedando aun pendiente la ejecución del comando **dcpromo** que llevaremos a cabo a continuación.

3.1. Configuración

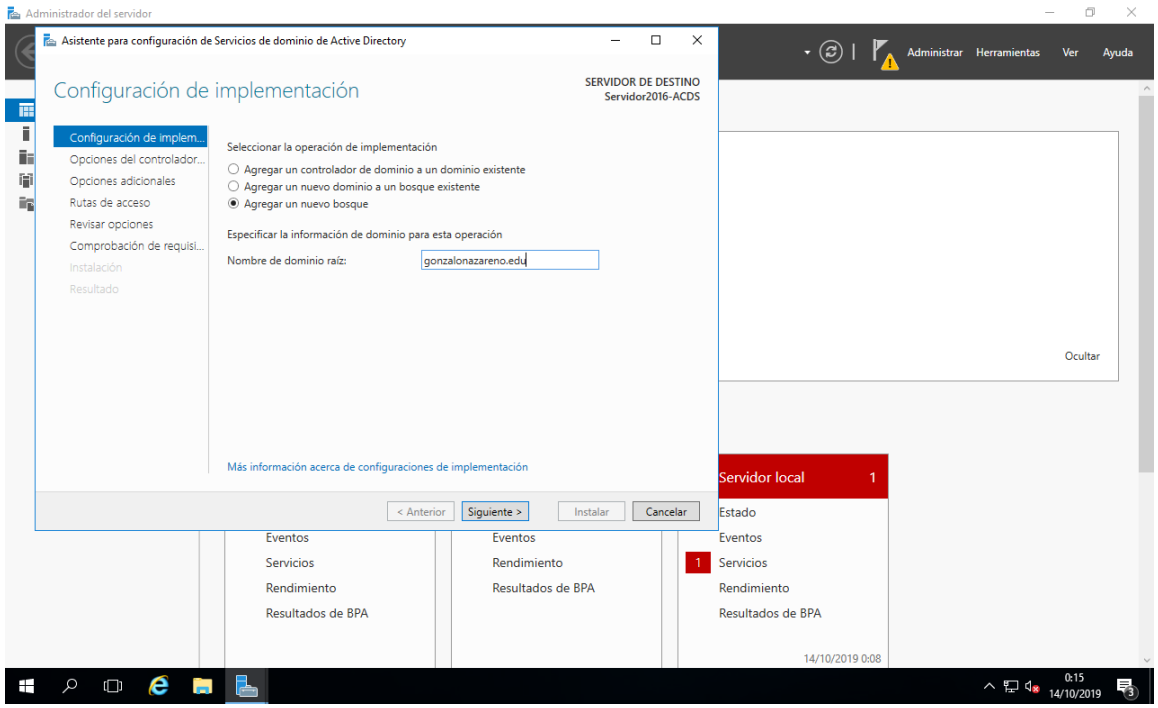
De vuelta a la ventana de "Administrador del servidor", podremos comprobar que han sido instalados los *Servicios de dominio de Directorio Activo*, pero que dicha instalación aun no se ha completado en su totalidad, pues debemos ejecutar el comando **dcpromo.exe** para completar la correcta instalación de dicho servicio.



El siguiente paso consiste en promover el equipo para que cumpla las funciones de controlador de dominio, recordemos que el comando dcpromo ya está obsoleto por parte de Microsoft.
Cuando hemos instalado el rol anterior podemos ver una advertencia en la parte superior del administrador del servidor:



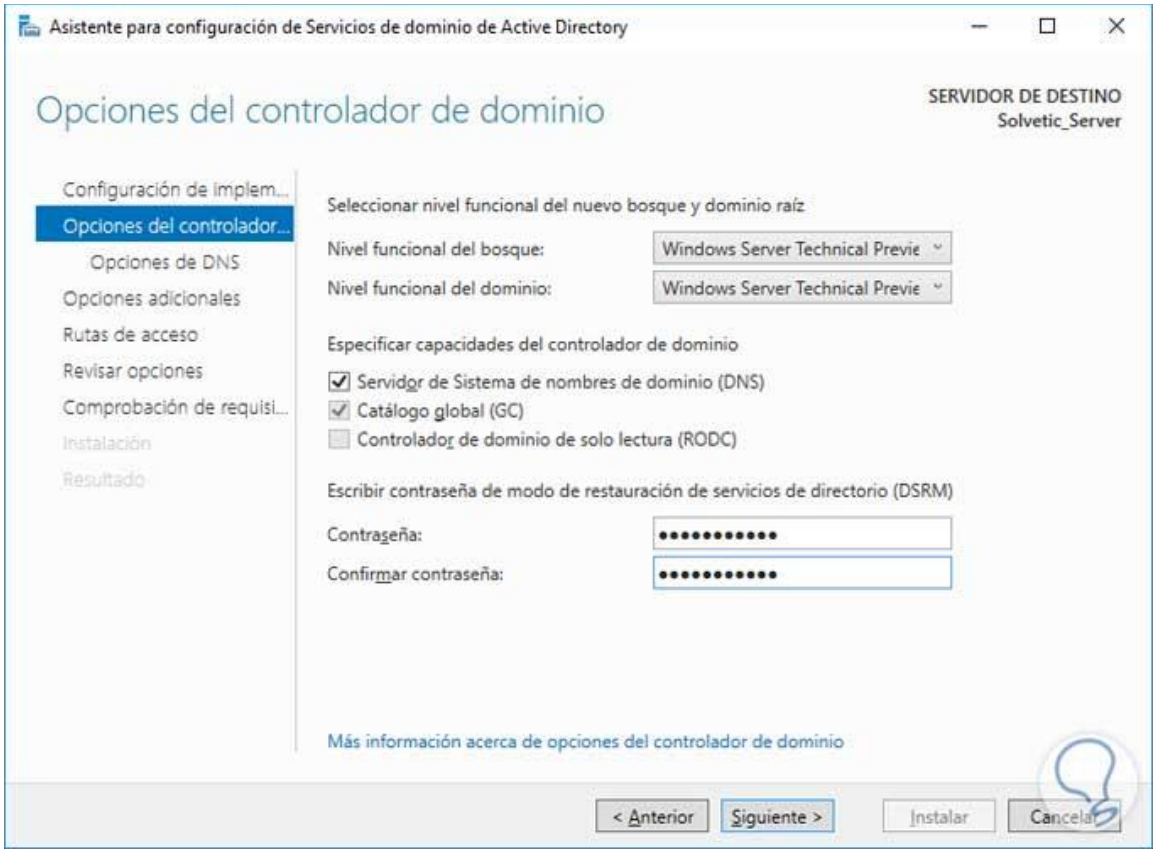
Al desplegarla debemos seleccionar la opción ***Promover este servidor a controlador de domino*** y se desplegará el siguiente asistente donde lo primero que debemos definir es un nuevo bosque con el nombre de nuestro dominio, en este caso es gonzalonazareno.edu



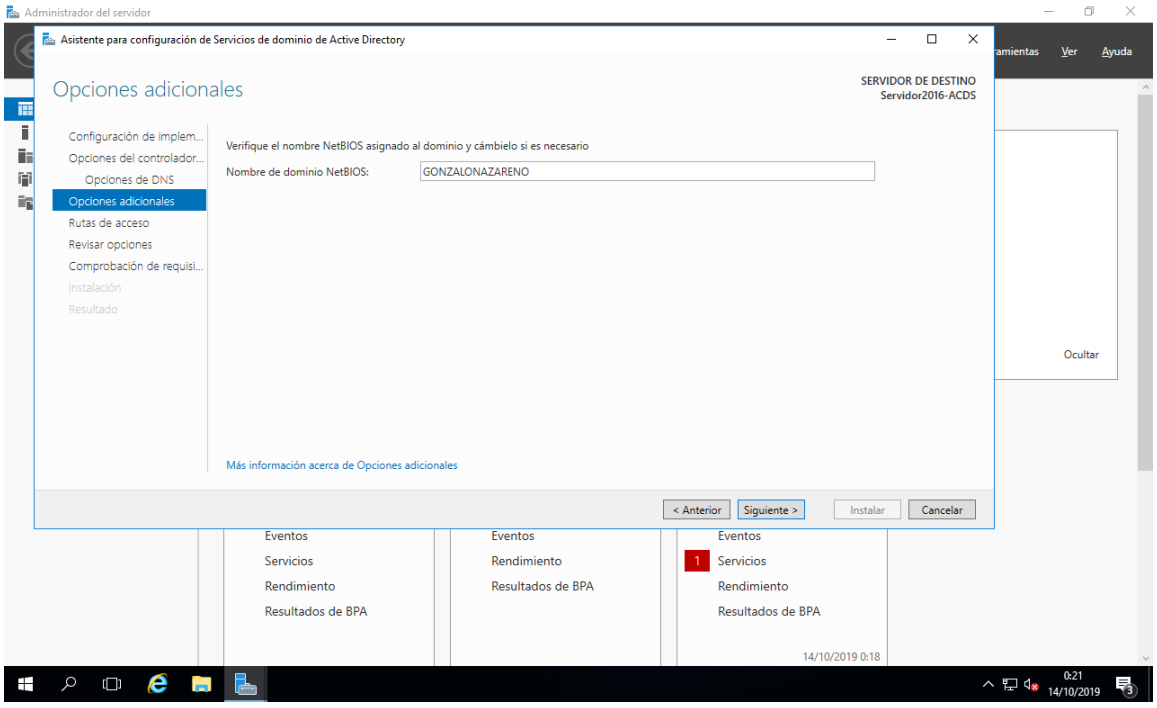
Pulsamos Siguiente y en la próxima ventana debemos definir los siguientes parámetros:

- Nivel funcional del bosque.
- Nivel funcional del dominio.

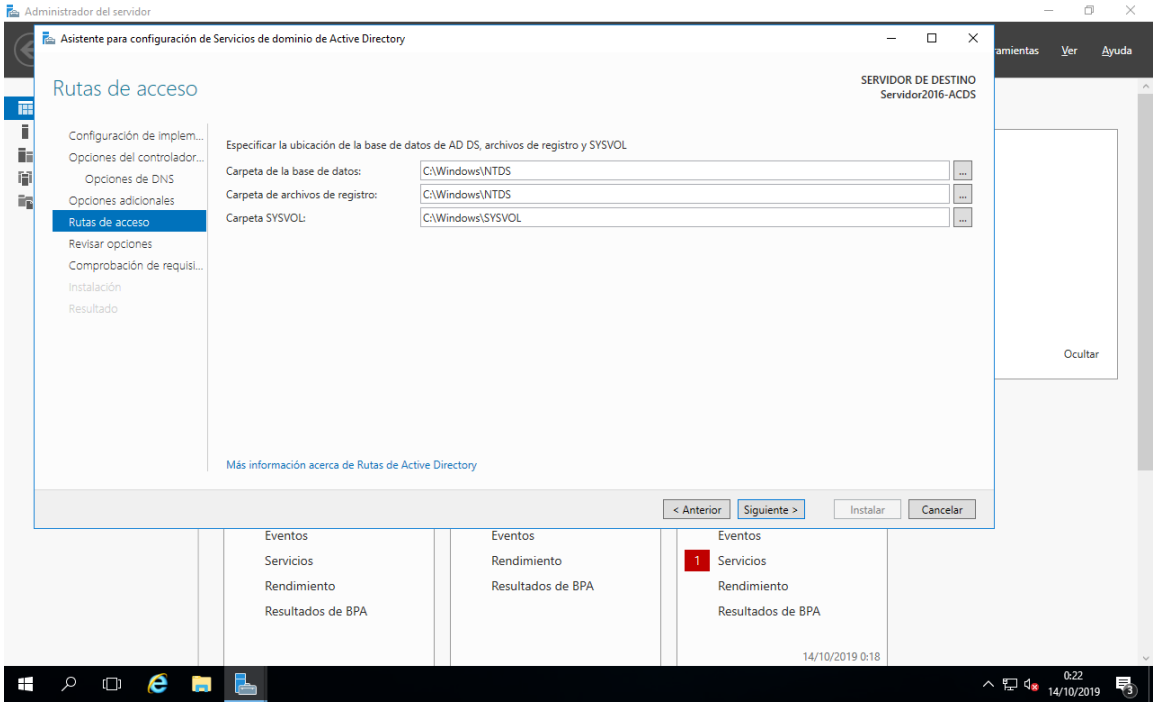
- Definir las funciones del dominio (Ser DNS, RODC, etc).
- Contraseña DSRM (Esta aplica cuando debemos iniciar el directorio activo en modo de restauración).



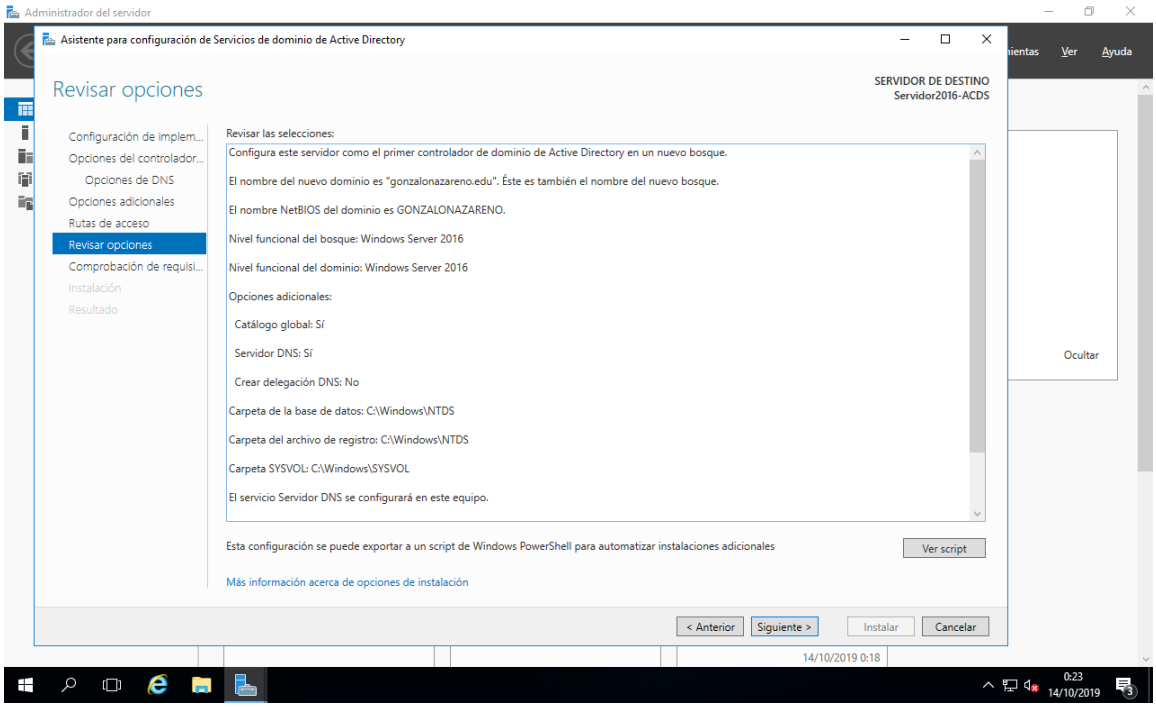
Pulsamos Siguiente y en la ventana desplegada sobre la delegación del DNS podemos omitirla pulsando de nuevo Siguiente y a continuación veremos el nombre de NetBIOS del equipo.



De nuevo pulsamos Siguiente y veremos las rutas donde se almacenarán los archivos de registro, de sistema, etc, estos valores no es recomendable modificarlos.

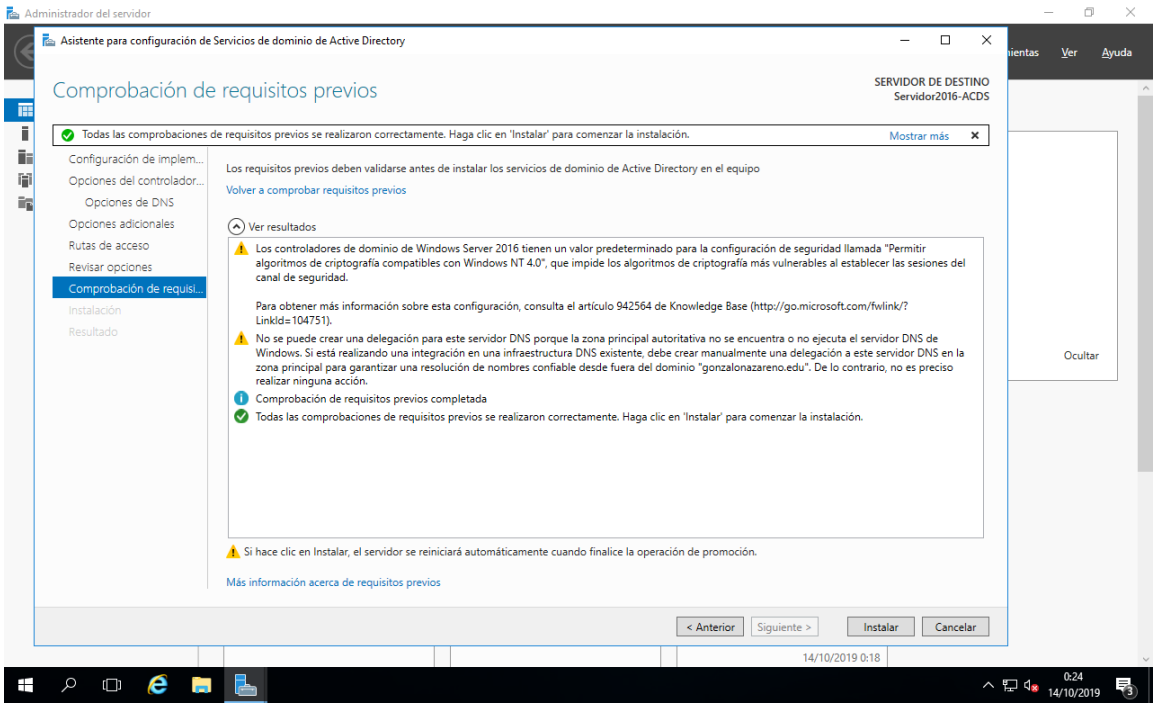


Pulsamos Siguiente y veremos un resumen con las características y funcionalidades a instalar.



Al pulsar Siguiente el sistema comprobará que todos los parámetros estén correctos para iniciar el proceso de promoción a controlador de dominio.

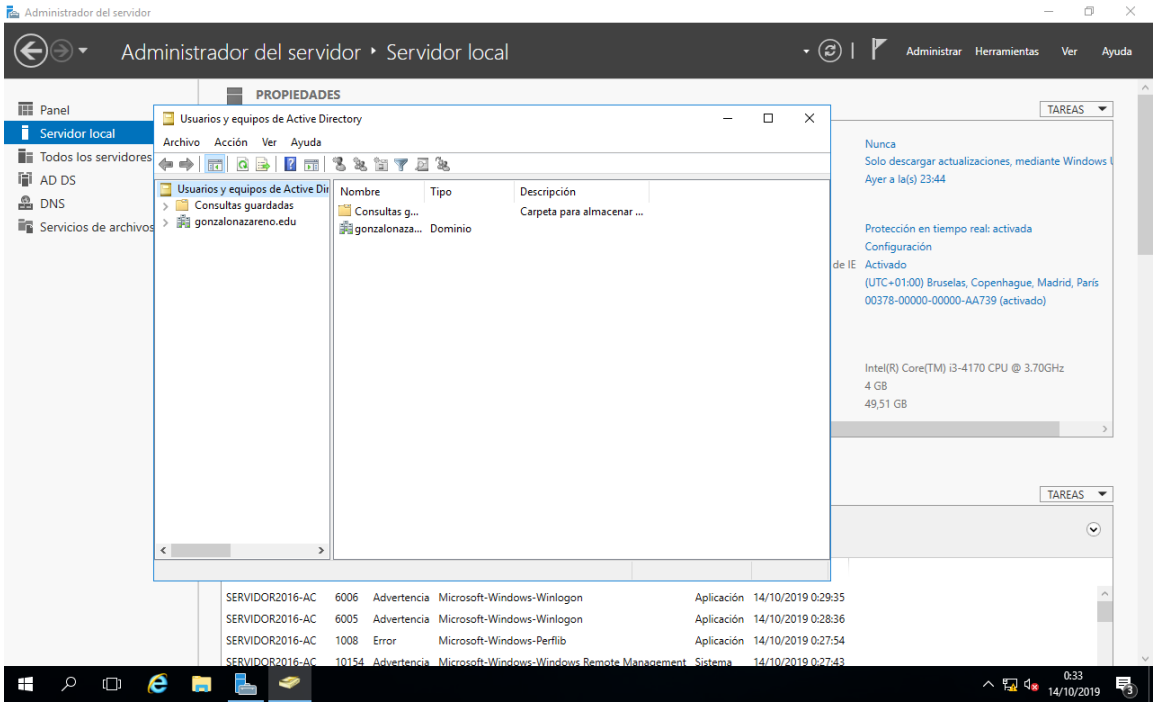
Si todos los requisitos están correctos veremos lo siguiente:



Pulsamos Instalar para iniciar el proceso de promoción a controlador de dominio en Windows Server 2016. Una vez promovido el equipo debemos reiniciar el sistema para que todos los cambios surtan efecto.

4. OBJETOS QUE ADMINISTRA UN DOMINIO.

- Usuarios globales
- Grupos
- Equipos
- Unidades Organizativas



Este punto lo desarrollaremos en el siguiente tema.