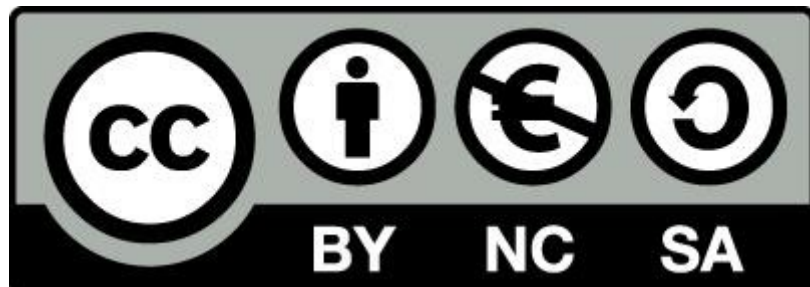


SISTEMAS OPERATIVOS EN RED

UT 7 – Directorio Activo en Windows Server

Mario García Alcázar

Esta obra esta sujeta a la Licencia Reconocimiento-NoComercial-SinObraDerivada 3.0 España de Creative Commons. Para ver una copia de esta licencia, visite <http://creativecommons.org/licenses/by-nc-nd/3.0/es/> o envíe una carta Creative Commons, PO Box 1866, Mountain View, CA 94042, USA.



Última revisión Julio de 2017.

Índice de contenido

Sumario

1. Introducción.....	4
2. Conceptos fundamentales.....	5
2. Conceptos básicos en una estructura de Directorio Activo.....	7
3. Instalar un dominio básico desde la interfaz gráfica.....	12
3.1 Instalar el rol Servicios de dominio de Active Directory.....	12
3.2 Promocionar el servidor como controlador de dominio.....	18
4. Creación de usuarios, grupos y equipos en el dominio.....	23
4.1 Operaciones sobre cuentas de usuario.....	26
4.1.1 Creación de usuarios.....	26
4.1.2 Eliminar un usuario.....	28
4.1.2 Modificar valores de las cuentas.....	29
4.1.3 Recuperar contraseñas.....	31
4.1.4 Establecer horas de inicio de sesión.....	31
4.1.5 Limitar los equipos desde los que un usuario puede iniciar sesión.....	32
4.1.6 Hacer que un usuario sea miembro de un grupo.....	33
4.2 Operaciones sobre cuentas de equipo.....	34
4.2.1 Modificar valores en las cuentas de los equipos.....	35
4.3 Operaciones sobre cuentas de grupos.....	36
4.3.1 Crear una cuenta de grupo.....	36
4.3.2 Añadir miembros a un grupo.....	36
4.3 Operaciones sobre unidades organizativas.....	37
4.3.1 Crear una nueva unidad organizativa.....	37
4.3.2 Eliminar una unidad organizativa.....	38
5. Conectar equipos clientes al dominio.....	40

1. Introducción.

En el tema interior tratamos la instalación básica de Windows Sever 2016, no obstante, este es solo un pequeño paso del conjunto de tareas necesarias para configurar el servidor.

De hecho una vez realizada la instalación, comienza la parte de configuración del servidor, en la cual definiremos la estructura y elementos de un servidor de dominio Windows.

En este tema trataremos dicha instalación, así como la creación de usuarios y grupos en el dominio.

2. Conceptos fundamentales.

En el sentido más amplio, un directorio no es más que una lista detallada de objetos. Por ejemplo, una guía de teléfonos es un tipo de directorio que guarda información sobre personas, empresas y otras entidades. De cada uno de los elementos representados, se almacena su nombre, dirección y número de teléfono.

En muchos sentidos, **Active Directory Domain Services** (AD DS) es muy parecido a una guía telefónica, aunque resulta más flexible. Se basa en el concepto de **dominio** que introdujo Windows NT con el fin de facilitar la administración. Sin embargo, ahora el objetivo es crear una estructura dinámica y fácilmente accesible, a través de la que se puede almacenar la información de toda la organización, tanto relativa a la estructura del propio directorio como de su administración, y acceder a ella de forma centralizada.

AD DS puede almacenar información sobre la organización, sitios, ordenadores, usuarios, objetos compartidos y cualquier otra cosa que pueda formar parte de la infraestructura de red. Además, toda esta información se guarda en una base de datos jerárquica con estructura de árbol.

Por otra parte, Active Directory permite la replicación de la información almacenada en los controladores de dominio o servidores. Es decir, se puede enviar la información contenida en la base de datos de un servidor 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.

Además de administrar políticas que serán válidas en toda la organización, Active Directory permite realizar operaciones como la instalación de programas, de forma simultánea y centralizada, en multitud de clientes o aplicar actualizaciones críticas en toda la organización.

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. Podemos verlos representados en la siguiente tabla:

Componentes de AD DS	
Componentes físicos	Componentes lógicos
Controladores de dominio	Dominios
Sitios	Bosques
	Árboles
Subredes	Unidades organizativas

2. Conceptos básicos en una estructura de Directorio Activo.

Una vez que disponemos de una idea global del concepto de directorio y de lo que son los dominios, es conveniente que hagamos un repaso de la terminología que vamos a emplear cuando hablemos de Active Directory Domain Services.

Los **principales conceptos** que debemos conocer son los siguientes:

- **Directorio.**

Es un repositorio único para la información relativa a los usuarios y recursos de una organización. Active Directory es un tipo de directorio y contiene información sobre las propiedades y la ubicación de los diferentes tipos de recursos dentro de la red.

- **Dominio.**

Es una colección de objetos dentro del directorio que forman un subconjunto administrativo. Pueden existir diferentes dominios dentro de un bosque, cada uno de ellos con su propia colección de objetos y unidades organizativas.

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. Más adelante, en este mismo apartado, definiremos los conceptos de bosque y unidad organizativa.

- **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.

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.

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

- **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 (facilitarán la apertura y el cierre de sesión, las búsquedas en el directorio, etc.).

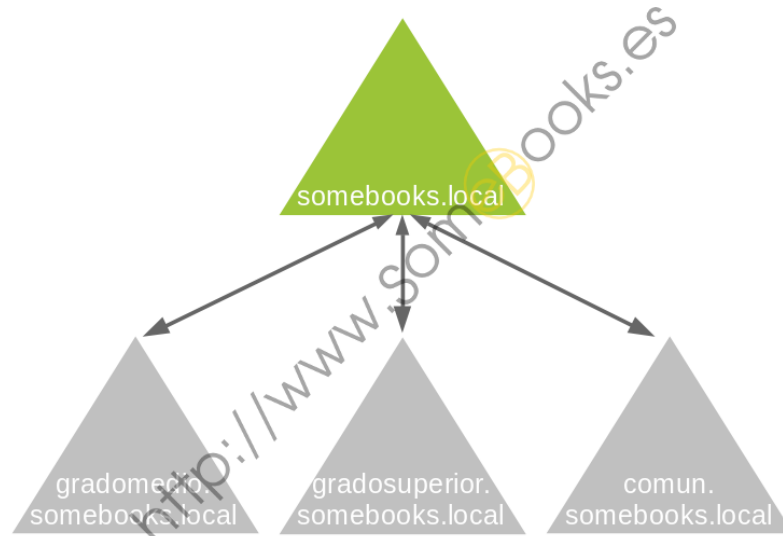
En un dominio dado, puede haber varios controladores de dominio asociados, de modo que cada uno de ellos represente un rol diferente dentro del directorio. Sin embargo, a todos los efectos, todos los controladores de dominio, dentro del mismo dominio, tendrán la misma importancia.

- **Árboles**

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

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.

En la imagen de ejemplo, podemos ver que los dominios `somebooks.es`, `informatica.somebooks.es` forman parte del mismo árbol, mientras que `quesliceoflinux.com` y `somebooks.es` no.



- **Bosque.**

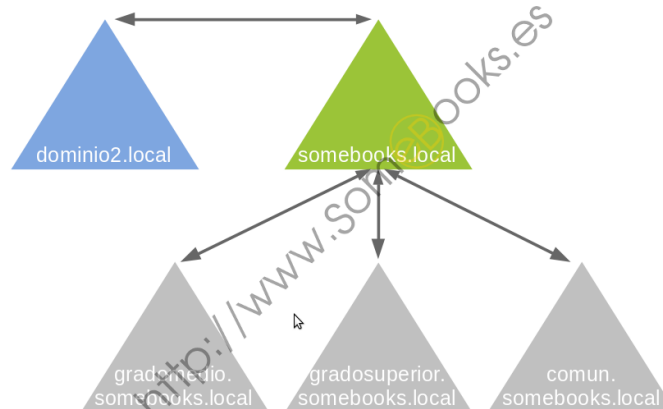
El Bosque es el mayor contenedor lógico dentro de Active Directory, abarcando a todos los dominios dentro de su ámbito. Los dominios están interconectados por Relaciones de confianza transitivas que se construyen automáticamente (consultar más adelante el concepto de Relación de confianza). De esta forma, 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, 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.

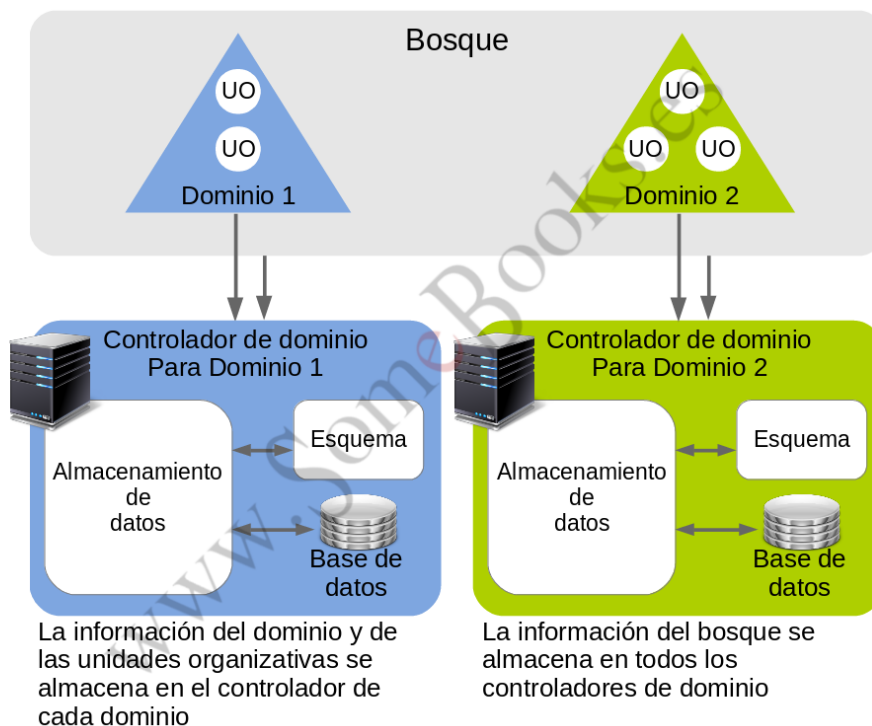


- **Unidad Organizativa**

Una Unidad Organizativa es un contenedor de objetos que permite organizarlos en subconjuntos, dentro del dominio.

De este modo, podremos establecer una estructura lógica que represente de forma adecuada nuestra organización y simplifique la administración.

Ejemplos de unidades organizativas podrían ser los departamentos de una empresa (informática, administración, dirección, etc)



- **Esquema**

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

- **Sitio**

Un Sitio es un grupo de ordenadores que se encuentran relacionados, de una forma lógica, con una localización geográfica particular. En realidad, pueden encontrarse físicamente en ese lugar o, como mínimo, estar conectados, mediante un enlace permanente, con el ancho de banda adecuado.

- **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.

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. Instalar un dominio básico desde la interfaz gráfica.

En realidad, la instalación de un dominio en Windows Server se divide en dos subtareas: primero tendremos que instalar el rol Servicios de dominio de Active Directory en el servidor y después convertiremos (promocionaremos) el servidor en un controlador de dominio.

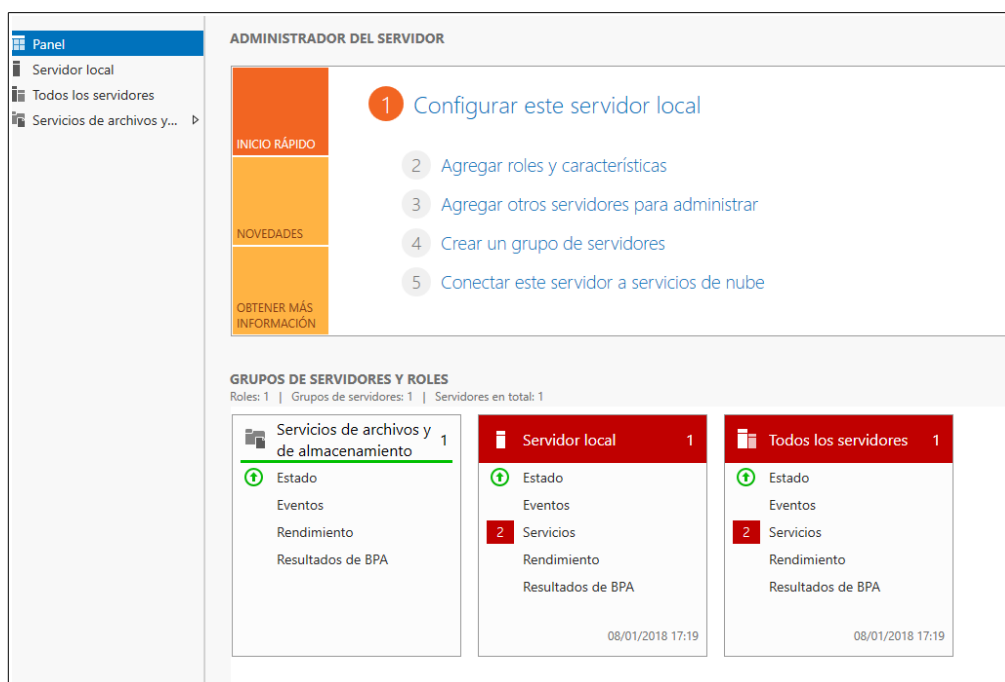
3.1 Instalar el rol Servicios de dominio de Active Directory

Cuando iniciamos sesión con la cuenta de Administrador en Windows Server 2016, lo normal es que se abra automáticamente la ventana del Administrador del servidor. En esta pantalla ejecutaremos los siguientes pasos:

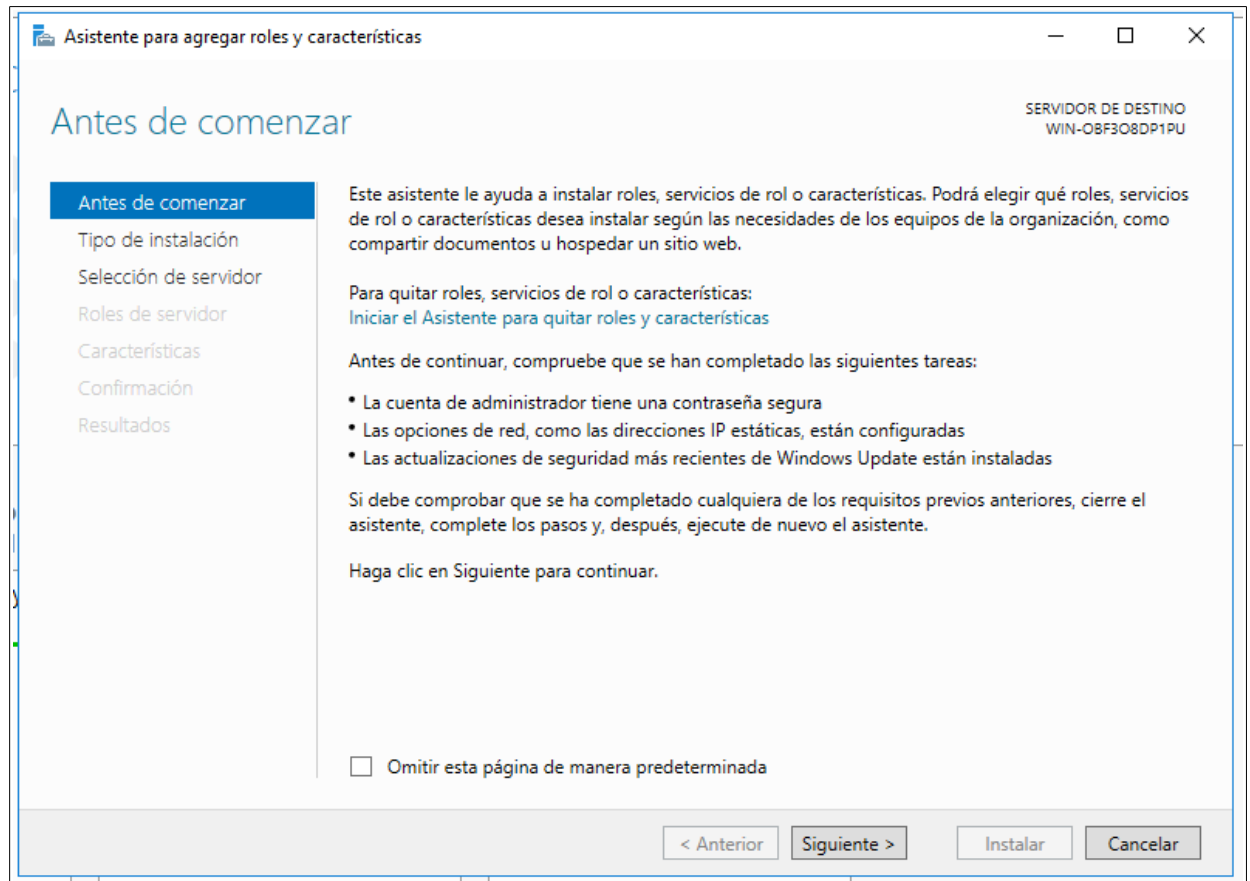
1. Pulsaremos el enlace **“Configurar este servidor local”**.

Aquí cambiaremos el nombre del servidor y desactivaremos el firewall de Windows.

2. Haremos clic sobre el enlace **“Agregar roles y características”** de la página principal de la ventana.



Sistemas Operativos en Red
UT 7 – Directorio activo en Windows Server

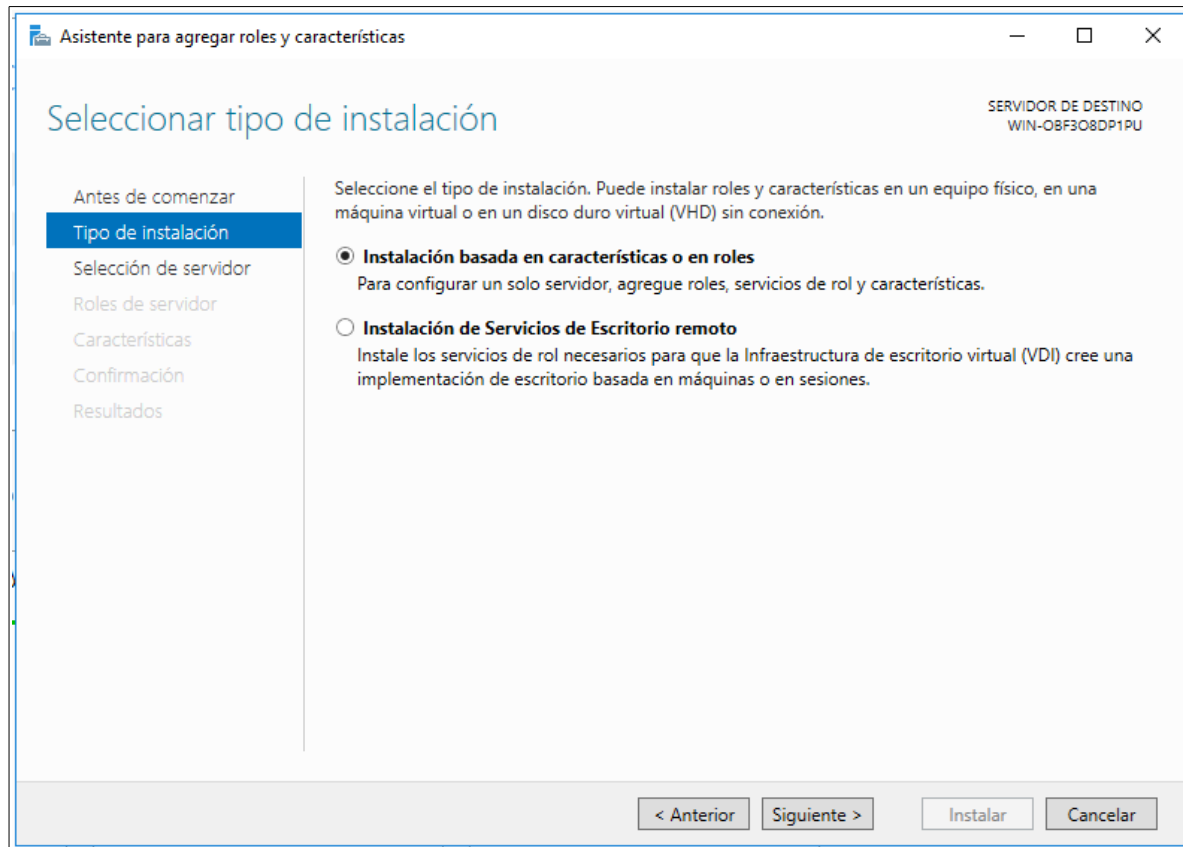


En ese momento se iniciará el Asistente para agregar roles y características. Este asistente no es específico de Active Directory, sino que nos puede guiar a través de la instalación de otras funciones tan diversas como DNS, Internet Information Server (IIS), fax, etc.

En esta pantalla pulsaremos **Aceptar**.

Seguidamente veremos una nueva pantalla donde seleccionaremos **“Instalación basada en características o roles”**.

Sistemas Operativos en Red
UT 7 – Directorio activo en Windows Server



3. En la siguiente pantalla, seleccionaremos “**seleccionar un servidor del grupo de servidores**”. Esta opción nos permite instalar el dominio en un servidor Windows Server presente en la red.

Asistente para agregar roles y características

Seleccionar servidor de destino

SERVIDOR DE DESTINO
WIN-OBF3O8DP1PU

Antes de comenzar
Tipo de instalación
Selección de servidor
Roles de servidor
Características
Confirmación
Resultados

Seleccione un servidor o un disco duro virtual en el que se instalarán roles y características.

☒ Seleccionar un servidor del grupo de servidores
☐ Seleccionar un disco duro virtual

Grupo de servidores

Filtro:

Nombre	Dirección IP	Sistema operativo
WIN-OBF3O8DP1PU	10.0.2.15	Microsoft Windows Server 2016 Standard

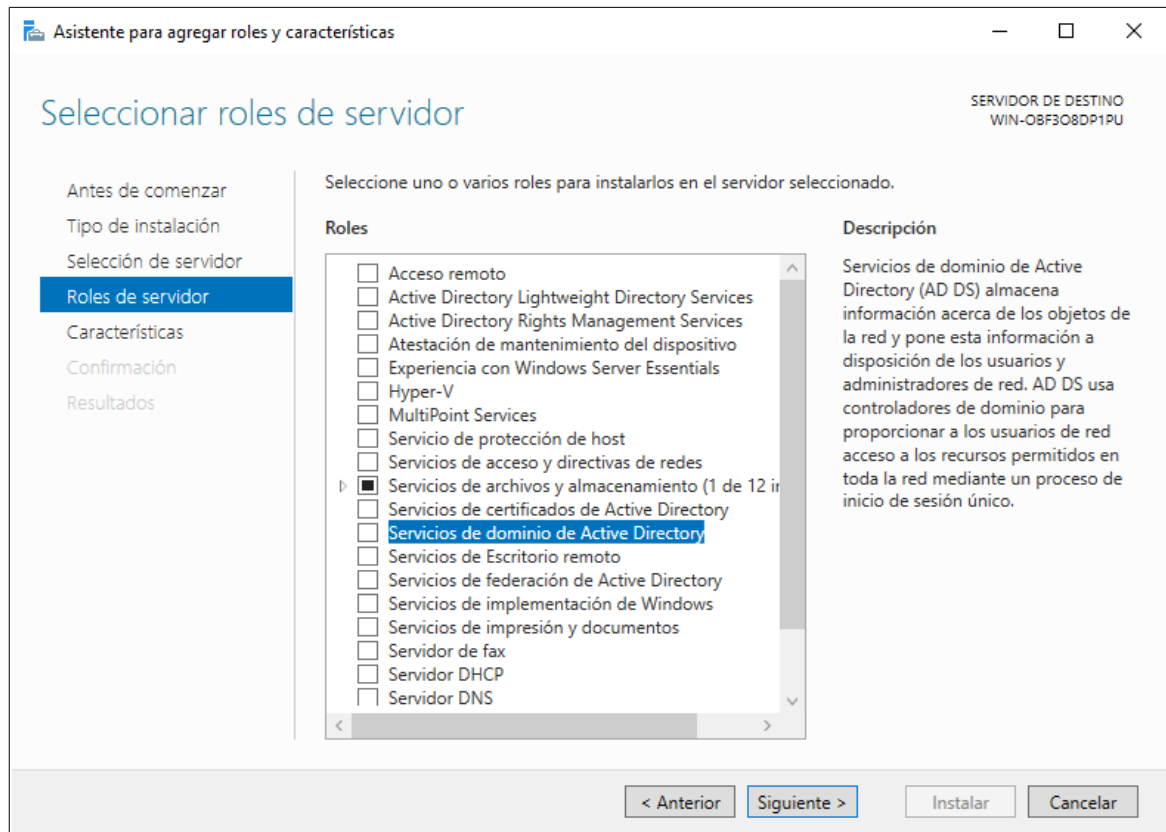
1 equipo(s) encontrado(s)

Esta página muestra los servidores que ejecutan Windows Server 2012 o una versión más reciente de Windows Server, y que se agregaron mediante el comando Agregar servidores del Administrador del servidor. No se muestran los servidores sin conexión ni los servidores recién agregados para los que la recopilación de datos aún está incompleta.

< Anterior Siguiente > Instalar Cancelar

Sistemas Operativos en Red
UT 7 – Directorio activo en Windows Server

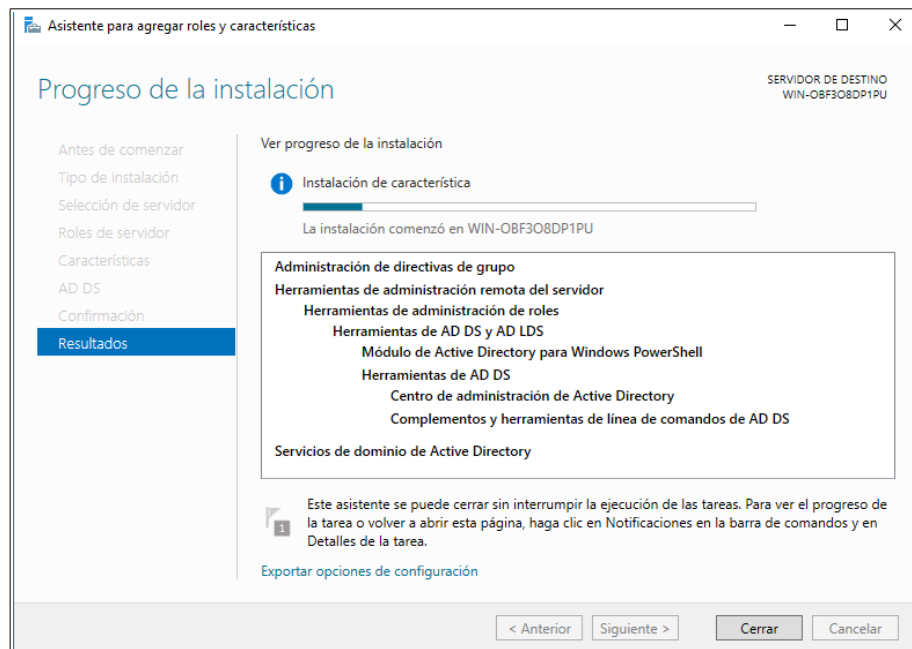
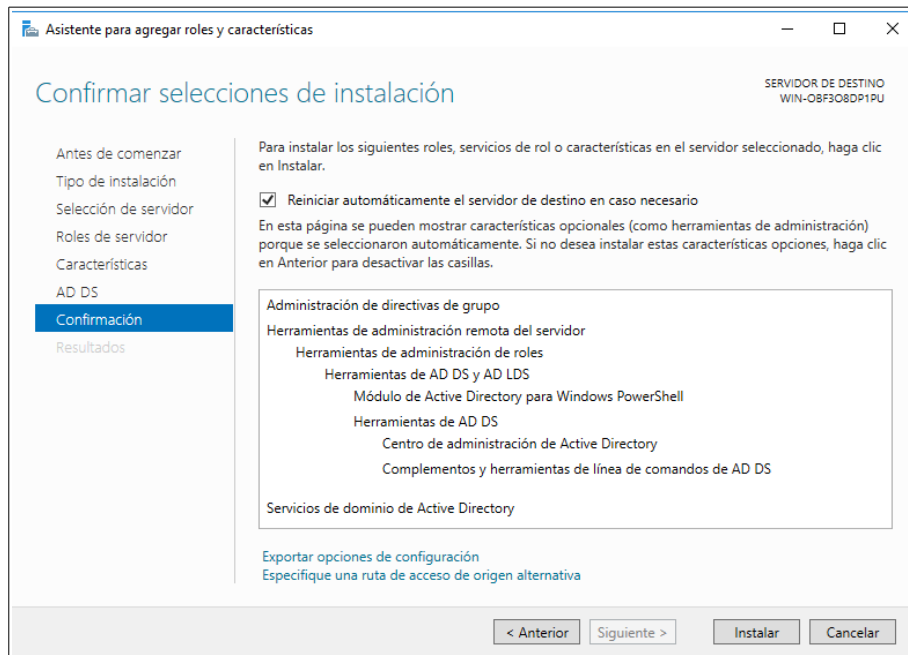
4. En este momento el sistema nos pide que indiquemos el servicio a instalar. Nosotros pulsaremos en **“Servicios de dominio de Active Directory”**.



Sistemas Operativos en Red

UT 7 – Directorio activo en Windows Server

5. Seguidamente pulsaremos el botón **“Siguiente”** hasta llegar a la pantalla de confirmación, donde seleccionaremos la opción de **“Reiniciar automáticamente si es necesario”**.

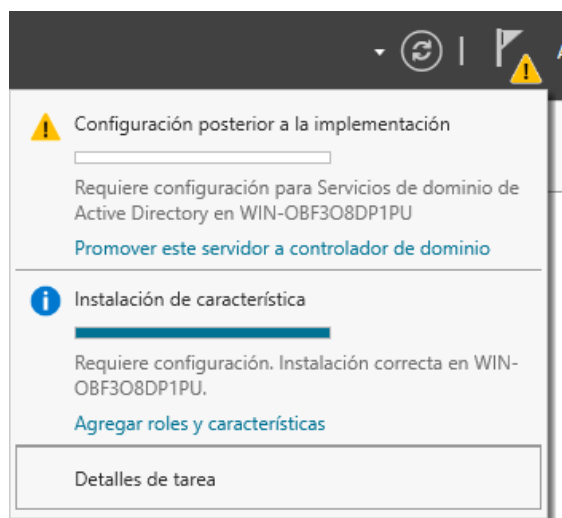


Es posible que durante este proceso el sistema nos indique que es necesario la instalación de un servidor DNS. Nosotros lo instalaremos en futuras configuraciones.

3.2 Promocionar el servidor como controlador de dominio

Como hemos dicho más arriba, después de realizar la instalación del rol Servicios de dominio de Active Directory, bastará con hacer clic sobre el enlace “**Promover este servidor a controlador de dominio**” de la última pantalla del asistente, para iniciar la promoción.

Sin embargo, si hubiésemos cerrado la ventana, también podremos hacer uso del icono que aparece en la parte superior del Administrador del servidor.



Una vez pulsado este enlace seguiremos los pasos siguientes:

1. Primero hemos de **indicar el tipo del dominio a instalar**. Las opciones son:

- Agregar un controlador de dominio a un dominio existente.

Con esta opción añadimos este equipo como controlador de un dominio ya existente en otro servidor de la red.

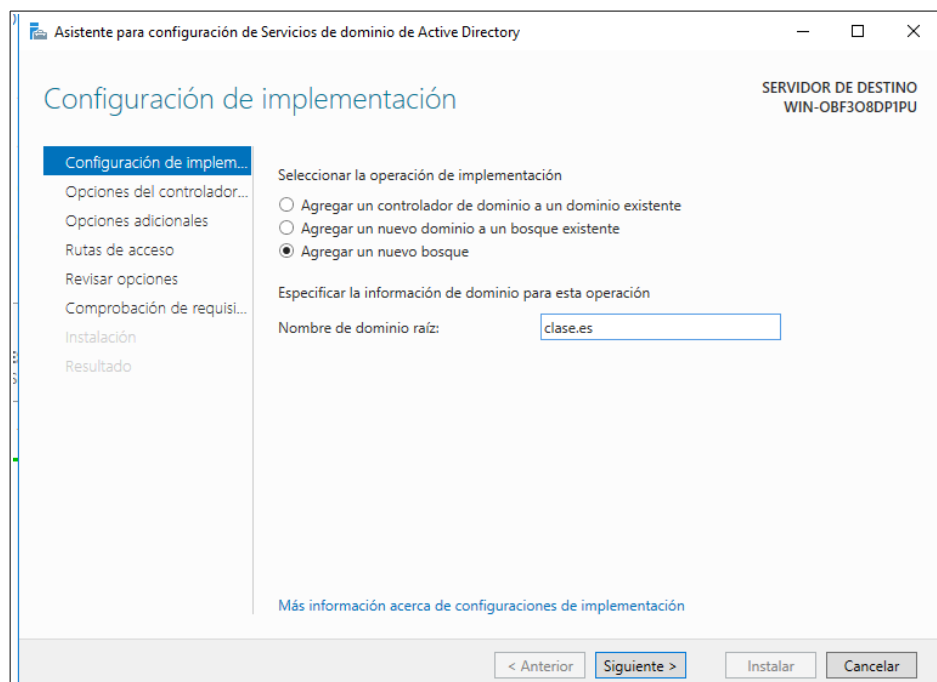
- Agregar un nuevo dominio a un bosque existente.

Con esta opción añadimos este equipo como controlador de un nuevo dominio en un bosque de dominios existente.

- Agregar un nuevo bosque.

Con esta opción creamos un bosque nuevo con un único dominio.

En nuestro ejemplo, como no existen bosques ni dominios previos, seleccionaremos esta opción, y como dominio pondremos **clase.es**



2. En la siguiente pantalla indicaremos una serie de **opciones de instalación del controlador**. Concretamente:

- Nivel funcional del bosque y dominio. Por defecto dejaremos Windows server 2016.
- Capacidades del controlador de dominio. Dejaremos la opciones por defecto
- Contraseña del administrador para la restauración de servicios.

Asistente para configuración de Servicios de dominio de Active Directory

Opciones del controlador de dominio

SERVIDOR DE DESTINO
WIN-0BF308DP1PU

Configuración de implem...
Opciones del controlador de dominio
Opciones de DNS
Opciones adicionales
Rutas de acceso
Revisar opciones
Comprobación de requisi...
Instalación
Resultado

Seleccionar nivel funcional del nuevo bosque y dominio raíz

Nivel funcional del bosque: Windows Server 2016

Nivel funcional del dominio: Windows Server 2016

Especificar capacidades del controlador de dominio

☒ Servidor de Sistema de nombres de dominio (DNS)

☒ Catálogo global (GC)

☐ Controlador de dominio de solo lectura (RODC)

Escribir contraseña de modo de restauración de servicios de directorio (DSRM)

Contraseña: *

Confirmar contraseña: *

Más información acerca de opciones del controlador de dominio

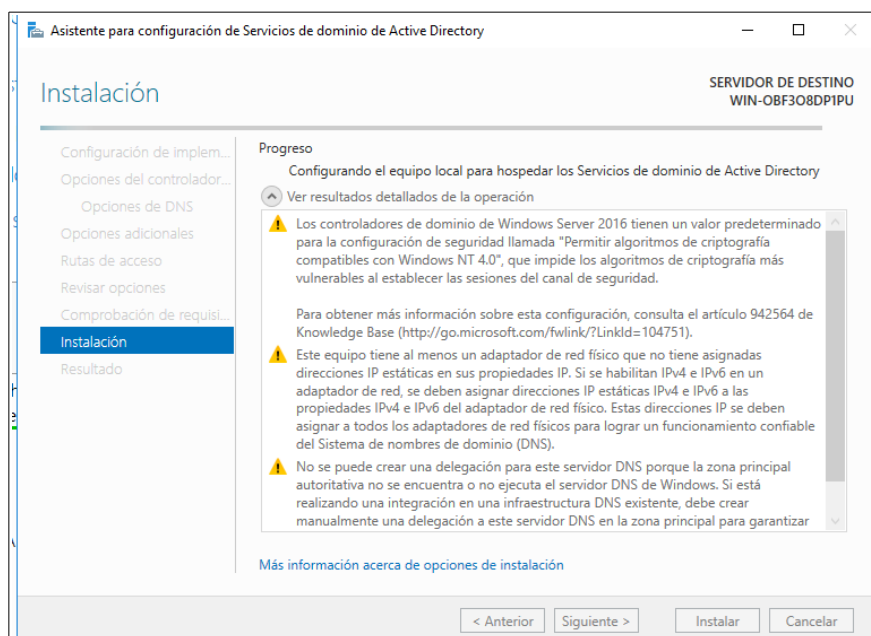
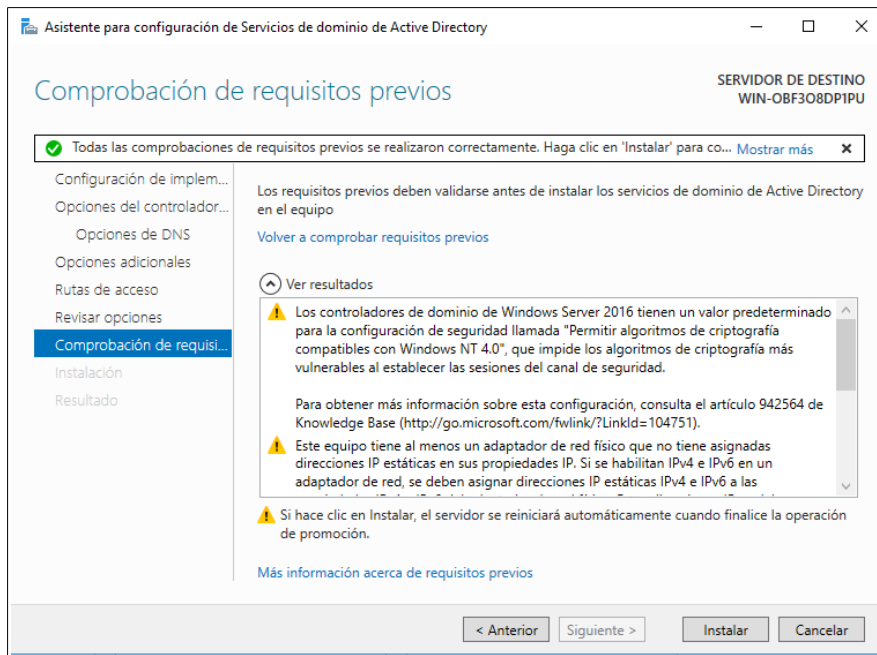
< Anterior Siguiente > Instalar Cancelar

3. A continuación el sistema nos solicita si queremos hacer una delegación de DNS. Esto enlazaría este servidor con otro servidor DNS ya instalado en la red. Como no existe en nuestro ejemplo, no podemos seleccionarlo.
4. En el siguiente paso, el asistente sugiere un nombreNetBIOS para el dominio raíz del bosque. Lógicamente, podemos aceptar el nombre que nos propone o indicar cualquier otro.
5. Indicamos la ubicación de la base de datos del dominio (dejaremos los valores por defecto)
6. El sistema nos muestra los posibles errores de configuración. Podremos resolverlos ahora o en el futuro.

Sistemas Operativos en Red

UT 7 – Directorio activo en Windows Server

Por ejemplo, un error muy común es instalar el dominio sin que el servidor tenga una IP fija.



7. El sistema se reiniciará al acabar la instalación. Este proceso es algo lento.

8. En el caso de quiera **eliminar el controlador de dominio**, para por ejemplo reiniciar el proceso, basta con abrir el Administrador del servidor, si aún no lo está, desplegar el menú Administrar y pulsar en la opción “**Asistente para quitar roles y características**”.

Una vez hecho esto, quitaremos la opción “**Servicios de dominio de Active Directory**”.

4. Creación de usuarios, grupos y equipos en el dominio.

Hasta ahora hemos instalado Windows Server y configurado Active Directory, no obstante, nada de esto no tiene sentido si no creamos nuevos elementos como **usuarios, grupos y equipos**. En este apartado clasificaremos los diferentes tipos de elementos que podemos tener en el sistema y su proceso de creación y gestión.

Para comenzar definiremos cada uno de los elementos antes mencionados.

- **Cuenta de usuario.**

Como ya comentábamos en el capítulo anterior, una de las primeras ideas que deben quedar claras cuando hablamos de cuentas de usuario es que no siempre representan a personas concretas, sino que también pueden ser utilizadas como mecanismos de acceso para determinados servicios o aplicaciones de la máquina local o, incluso, de un equipo remoto.

En definitiva, **una cuenta de usuario es un objeto que posibilita el acceso a los recursos del dominio de dos modos diferentes:**

- Permite autenticar la identidad de un usuario, porque sólo podrán iniciar una sesión aquellos usuarios que dispongan de una cuenta en el sistema asociada a una determinada contraseña.
- Permite autorizar, o denegar, el acceso a los recursos del dominio, porque, una vez que el usuario haya iniciado su cuenta para iniciar sesión en el dominio, sólo tendrá acceso a los recursos para los que haya recibido los permisos correspondientes.

- **Cuentas integradas**

Cuando se crea el dominio, se crean también dos nuevas cuentas: **Administrador** e **Invitado**.

Posteriormente, cuando es necesario, se crea también la cuenta **Asistente de ayuda**. Estas son las denominadas **cuentas integradas** y disponen de una serie de derechos y permisos predefinidos:

- Administrador. Tiene control total sobre el dominio y no se podrá eliminar ni retirar del grupo Administradores (aunque sí podemos cambiarle el nombre o deshabilitarla).
- Invitado. Está deshabilitada de forma predeterminada y, aunque no se recomienda, puede habilitarse, por ejemplo, para permitir el acceso a los

usuarios que aún no tienen cuenta en el sistema o que la tienen deshabilitada. De forma predeterminada no requiere contraseña, aunque esta característica, como cualquier otra, puede ser modificada por el administrador.

- Asistente de ayuda. Se utiliza para iniciar sesiones de Asistencia remota y tiene acceso limitado al equipo. Se crea automáticamente cuando se solicita una sesión de asistencia remota y se elimina cuando dejan de existir solicitudes de asistencia pendientes de satisfacer.

- **Cuenta de equipo**

Como ocurría con las cuentas de usuario, una cuenta de equipo sirve para autenticar a los diferentes equipos que se conectan al dominio, permitiendo o denegando su acceso a los diferentes recursos del dominio.

Del mismo modo que con las cuentas de usuario, las cuentas de equipo deben ser únicas en el dominio.

Aunque una cuenta de equipo se puede crear de forma manual (como veremos más adelante), también se puede crear en el momento en el que el equipo se une al dominio.

- **Cuenta de grupo**

Un grupo es un conjunto de objetos del dominio que pueden administrarse como un todo. Puede estar formado por cuentas de usuario, cuentas de equipo, contactos y otros grupos.

Podemos utilizar los grupos para simplificar algunas tareas, como:

- Simplificar la administración: Podemos asignar permisos al grupo y éstos afectarán a todos sus miembros.
- Delegar la administración: Podemos utilizar la directiva de grupo para asignar derechos de usuario una sola vez y, más tarde, agregar los usuarios a los que queramos delegar esos derechos.
- Crear listas de distribución de correo electrónico: Sólo se utilizan con los grupos de distribución que comentaremos más abajo.

El Directorio Activo proporciona un conjunto de grupos predefinidos que pueden utilizarse tanto para facilitar el control de acceso a los recursos como para delegar determinados roles administrativos. Por ejemplo, el grupo Operadores de copia de seguridad permite a sus miembros realizar copias de seguridad de todos los controladores de dominio, en el dominio al que pertenecen.

Por otra parte hay que comentar el concepto de “**ámbito de los grupos**”.

El ámbito de un grupo establece su alcance, es decir, en qué partes de la red puede utilizarse, y el tipo de cuentas que pueden formar parte de él. En ese sentido, pueden pertenecer a una de las siguientes categorías:

- Ámbito local: Entre sus miembros pueden encontrarse uno o varios de los siguientes tipos de objetos:
 - Cuentas de usuario o equipo.
 - Otros grupos de ámbito local.
 - Grupos de ámbito global.
 - Grupos de ámbito universal.

Las cuentas o grupos contenidos tendrán necesidades de acceso similares dentro del propio dominio. Por ejemplo, los que necesiten acceder a una determinada impresora.

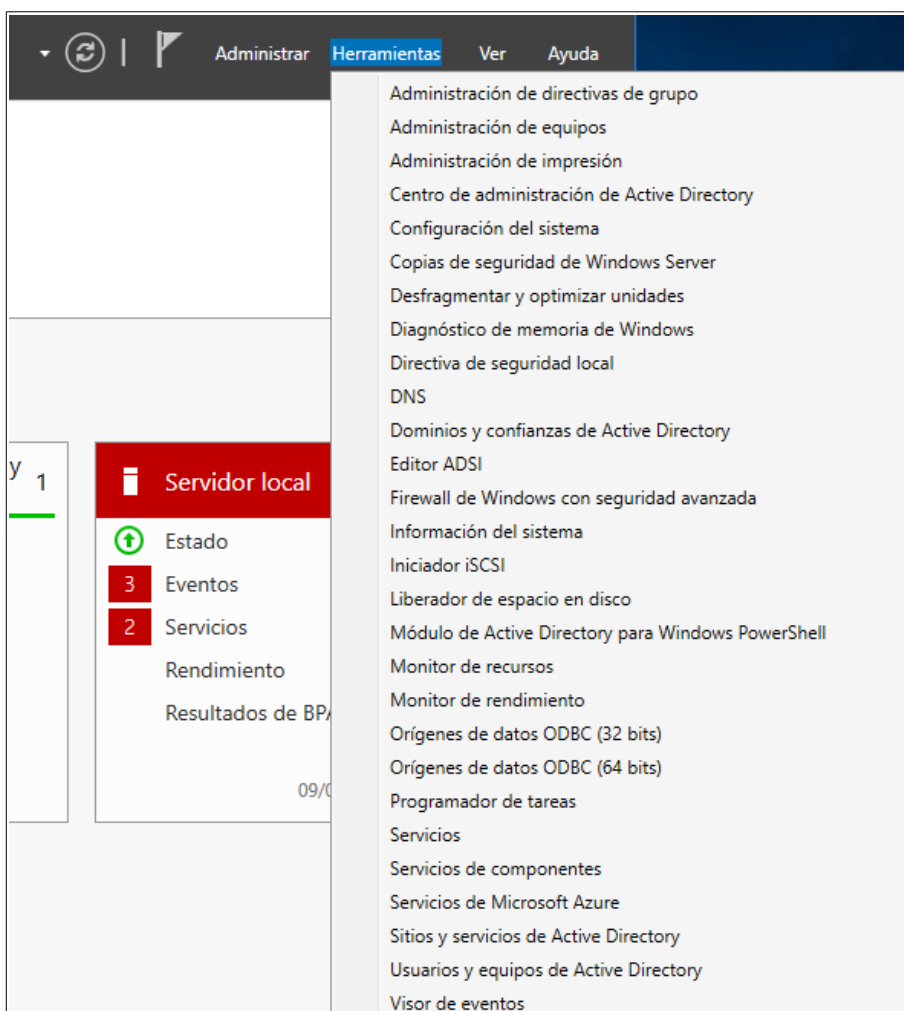
- Ámbito global: Sólo pueden incluir otros grupos y cuentas que pertenezcan al dominio en el que esté definido el propio grupo. Los miembros de este tipo de grupos pueden tener permisos sobre los recursos de cualquier dominio dentro del bosque. Sin embargo, estos grupos no se replican fuera de su propio dominio, de modo que, la asignación de derechos y permisos que alberguen, no serán válidas en otros dominios del bosque.
- Ámbito universal: Entre sus miembros pueden encontrarse cuentas o grupos de cualquier dominio del bosque, a los que se les pueden asignar permisos sobre los recursos de cualquier dominio del bosque.

4.1 Operaciones sobre cuentas de usuario.

En este apartado trataremos las principales operaciones sobre cuentas de usuario, creación, eliminación, introducción en grupos, etc.

4.1.1 Creación de usuarios.

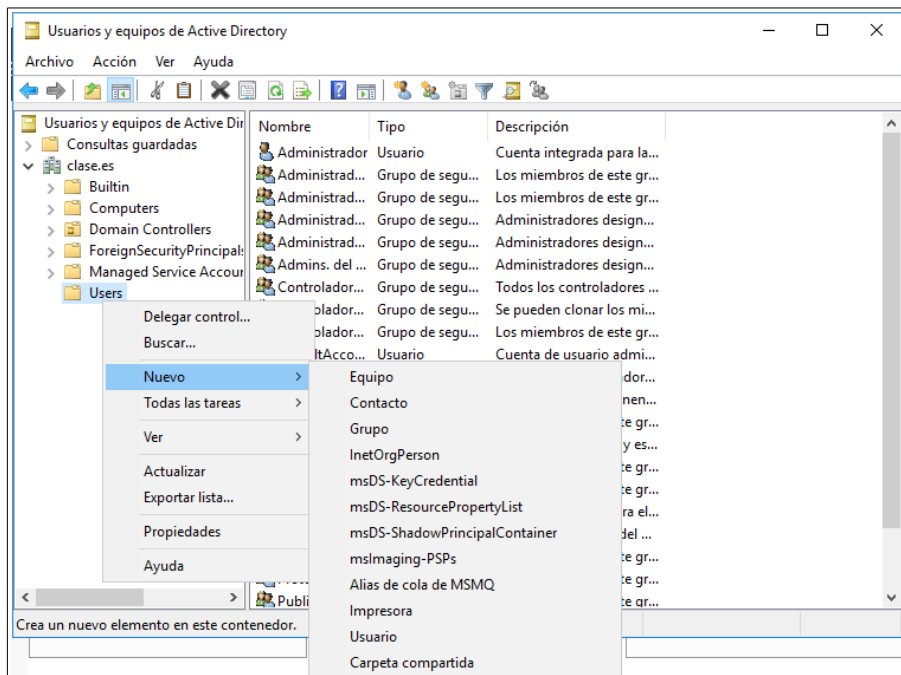
Para crear usuarios simplemente accederemos a **Administrador del servidor** → **Herramientas** → **Usuarios y equipos de Active Directory**.



Sistemas Operativos en Red

UT 7 – Directorio activo en Windows Server

En la siguiente pantalla, **desplegamos el icono con el nombre del dominio** (en nuestro ejemplo Clase.es) y pulsamos el botón derecho del ratón, seleccionando **nuevo** → **usuario**

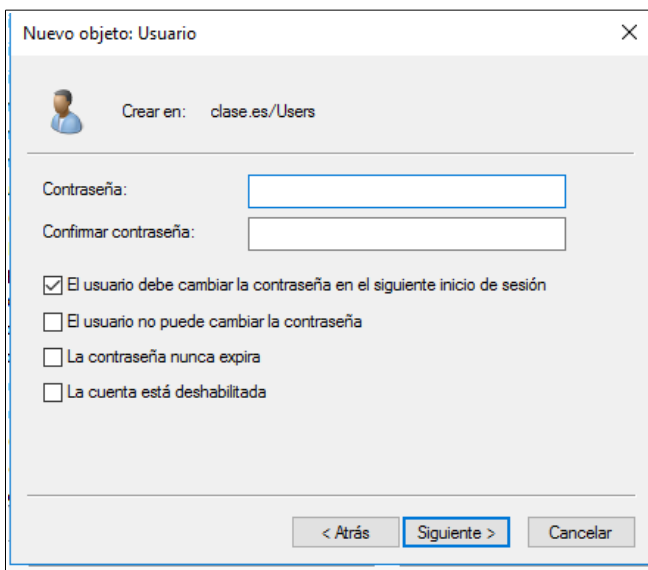


Ahora introduciremos la información de la cuenta de usuario.

The screenshot shows the 'Nuevo objeto: Usuario' (New Object: User) dialog box. The 'Crear en' (Create in) field is set to 'clase.es/Users'. The 'Nombre de pila' (First name) field is 'usu1', 'Apellidos' (Last name) is empty, and 'Nombre completo' (Full name) is 'usu1'. The 'Nombre de inicio de sesión de usuario' (User logon name) field is 'usu1' and the domain dropdown is '@clase.es'. The 'Nombre de inicio de sesión de usuario (anterior a Windows 2000)' (User logon name (pre-Windows 2000)) field is 'CLASE\'usu1'. The 'Siguiente' (Next) button is highlighted.

El sistema nos pedirá también la contraseña del usuario e información acerca de:

- Si el usuario está obligado a cambiarla al iniciar por primera vez la sesión.
- Si el usuario no puede cambiar su contraseña.
- Si la contraseña caduca
- Si la cuenta está deshabilitada.



Es importante tener en cuenta que **la contraseña debe cumplir los requerimientos de seguridad del sistema operativo**. Es decir, que de forma predeterminada deberá tener un mínimo de seis caracteres de larga y contener caracteres de, al menos, tres de los cuatro conjuntos siguientes:

- Mayúsculas del alfabeto inglés.
- Minúsculas del alfabeto inglés.
- Dígitos decimales (del 0 al 9).
- Caracteres no alfanuméricos.

4.1.2 Eliminar un usuario.

Basta con acceder a **Administrador del servidor** → **Herramientas** → **Usuarios y equipos de Active Directory** , pulsar el botón derecho del ratón sobre el usuario a

eliminar y seleccionar “**Eliminar**”.

4.1.2 Modificar valores de las cuentas

Una vez que hemos creado una cuenta, podemos volver a la herramienta **Usuarios y equipos de Active Directory** en cualquier momento para ajustar sus propiedades.

Como antes, usaremos el menú Herramientas del Administrador del Servidor. En su interior, haremos clic sobre Usuarios y equipos de Active Directory (recuerda que también puedes utilizar la consola Herramientas comunes que creamos en el capítulo anterior).

Una vez abierta la ventana, hacemos clic con el botón derecho del ratón sobre el usuario que queremos modificar.

The screenshot shows the 'Propiedades: usu1' window with the 'General' tab selected. The window contains the following fields and buttons:

- Nombre de pila:** usu1 (highlighted with a blue border)
- Iniciales:** (empty field)
- Apellidos:** (empty field)
- Nombre para mostrar:** usu1
- Descripción:** (empty field)
- Oficina:** (empty field)
- Número de teléfono:** (empty field) and **Otros...** button
- Correo electrónico:** (empty field)
- Página web:** (empty field) and **Otros...** button
- Buttons at the bottom:** Aceptar, Cancelar, Aplicar, Ayuda

De forma predeterminada, estaremos situados sobre la solapa General, que contiene los datos que introdujimos en el primer paso de creación de la cuenta y otros complementarios, como una Descripción, un Número de teléfono, etc.

A pesar de que la ventana Propiedades dispone de hasta 13 solapas diferentes, no es objetivo de este texto explicarlas todas en detalle.

Algunas de las pestañas más importantes son:

- **Cuenta.** En ella podremos cambiar los nombres de inicio de sesión del usuario (al fin y al cabo, el único valor imprescindible para que la cuenta mantenga su identidad es suSID).

También podremos cambiar las opciones de cuenta, aunque ahora dispondremos de algunas opciones más, que no teníamos cuando la creamos:

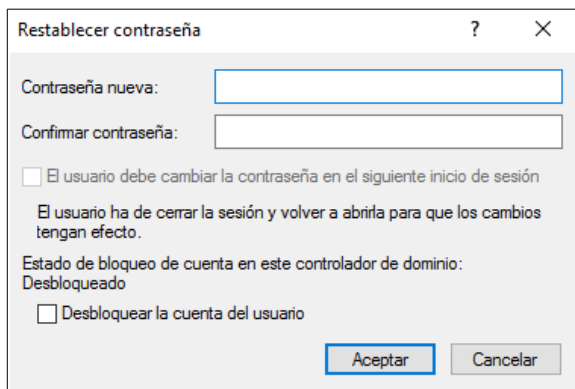
- Almacenar contraseña utilizando cifrado reversible: Sólo se utiliza cuando la cuenta de usuario utilizará un cliente Apple para iniciar sesión en elDominio.
 - La tarjeta inteligente es necesaria para un inicio de sesión interactivo: Sólo se utiliza en entornos donde los clientes disponen de un lector de tarjetas y los usuarios disponen de una tarjeta con un Número de Identificación Personal (PIN) asociado. En estos casos, la contraseña se establece automáticamente con un valor aleatorio y complejo.
 - La cuenta es importante y no se puede delegar: Esta opción permite el control sobre una cuenta de usuario (como una cuenta de invitado o una cuenta temporal). Se puede utilizar cuando la cuenta no puede utilizarse por otra cuenta para delegar sobre ella.
 - Usar tipos de cifrado DES de kerberos para esta cuenta: Habilita la compatibilidad con el estándar de cifrado de datos (DES).
 - Esta cuenta admite cifrado AES de Kerberos de 128 y 256 bits: Estas opciones sólo estarán disponibles si el nivel de funcionalidad del dominio esWindows Server 2008 (incluido R2) oWindows Server 2003.
 - No pedir la autenticación Kerberos previa: Ofrece compatibilidad con implementaciones alternativas al protocolo Kerberos. Habilitar esta opción puede suponer una pérdida de seguridad en el sistema.
 - Otra de las opciones que tenemos a nuestra disposición es la de establecer una caducidad para la cuenta. Lo normal es que el valor asignado sea Nunca. Sin embargo, si necesitamos crear una cuenta para un usuario que utilizará los recursos durante un tiempo limitado (por ejemplo, un trabajador temporal), podemos establecer una fecha para que la cuenta quede deshabilitada de forma automática.
- **Perfil**, que trataremos en el siguiente tema para con figurar perfiles fijos y móviles.
 - **Sesiones**, que nos permite modificar el tiempo de cierre de sesión por inactividad del usuario.

4.1.3 Recuperar contraseñas.

En ocasiones, un usuario olvida su contraseña (por un simple descuido, porque la política de seguridad de la empresa obliga a cambiar las contraseñas con frecuencia, porque el usuario lleva tiempo sin entrar en el sistema, etc.). Por cuestiones de seguridad, Windows Server no permite que nadie, ni siquiera el administrador, pueda ver la contraseña de un usuario. Sin embargo, una operación que sí podemos hacer como administradores es asignar una contraseña nueva, comunicarla por un medio seguro al usuario, y obligar a que éste la cambie en su primer inicio de sesión. De esta forma, la contraseña resultante volverá a ser conocida sólo por el usuario implicado.

Como en los apartados anteriores, usaremos el menú Herramientas del Administrador del Servidor. En su interior, haremos clic sobre **Usuarios y equipos de Active Directory** (o bien, utilizaremos la consola Herramientas comunes que creamos en el capítulo anterior).

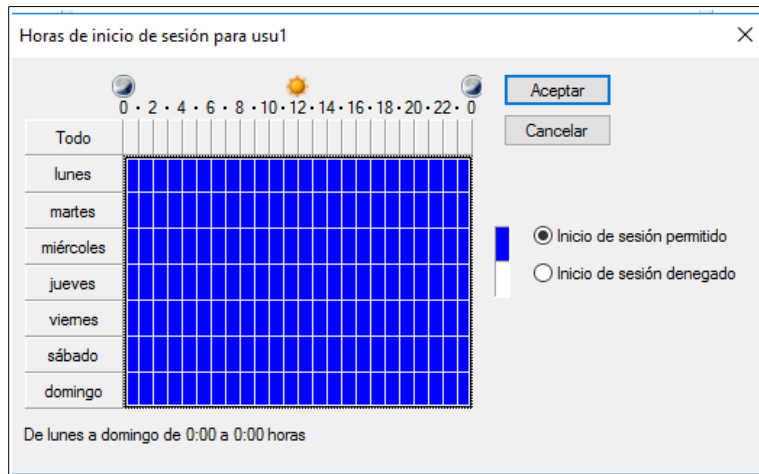
Una vez abierta la ventana, **hacemos clic con el botón derecho del ratón sobre el usuario que queremos modificar**.



4.1.4 Establecer horas de inicio de sesión

Una de las precauciones más básicas que podemos considerar respecto de la seguridad de una red es la de impedir que los usuarios inicien sesión en el sistema fuera del horario que hayamos establecido para ello (por ejemplo, fuera de su jornada laboral).

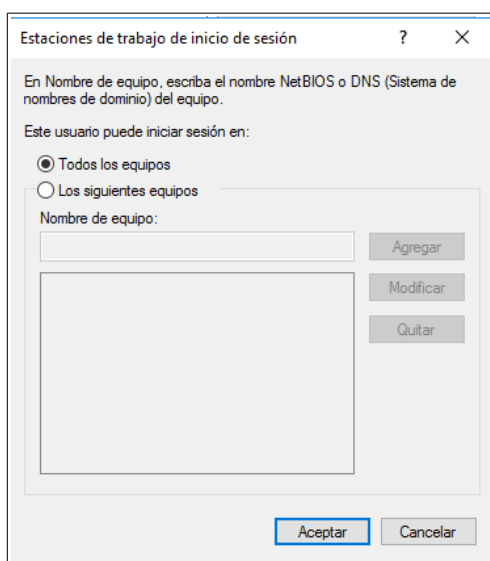
Para conseguirlo, comenzaremos por abrir la **ventana Usuarios y equipos de Active Directory** (tal y como hemos visto en apartados anteriores) y buscar la cuenta de usuario que queremos configurar. Después hacemos clic con el botón derecho del ratón sobre ella y accederemos a la **pestaña cuenta y en ella al botón horas de inicio de sesión**.



4.1.5 Limitar los equipos desde los que un usuario puede iniciar sesión

En el apartado anterior hemos aprendido cómo limitar las horas en las que un usuario puede iniciar sesión en el equipo. Esto ofrece un grado de seguridad considerable a nuestra red, porque nos aseguramos de que un usuario no puede utilizar el sistema en momentos no autorizados. Sin embargo, aún podemos complementar la medida anterior si fijamos también los lugares desde los que el usuario puede iniciar sesión, impidiendo que pueda acceder al sistema desde un punto de la red diferente al que utiliza habitualmente para realizar su trabajo.

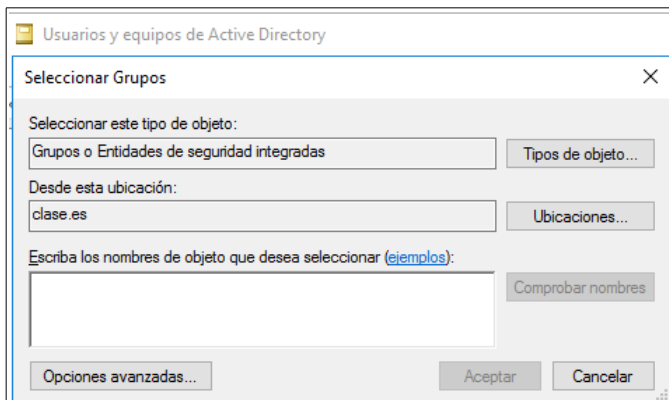
Para conseguirlo, accederemos a la **pestaña cuentas** de la **ventana Usuarios y equipos de Active Directory** y pulsaremos el botón **iniciar sesión en...**



4.1.6 Hacer que un usuario sea miembro de un grupo

Una de las cosas que haremos con casi todos nuestros usuarios es hacerlos miembros de uno o varios grupos. Esta operación la podemos hacer desde la propia cuenta de usuario o desde el grupo al que queremos asignarle miembros. De momento veremos esta primera opción y, más adelante, veremos cómo hacer lo mismo desde un grupo.

Como de costumbre, debemos comenzar abriendo la herramienta Usuarios y equipos de Active Directory (tal y como hemos visto en apartados anteriores). Una vez ahí, hacemos clic con el botón derecho del ratón sobre el nombre de la cuenta del cliente y seleccionamos **“Agregar a un grupo”**

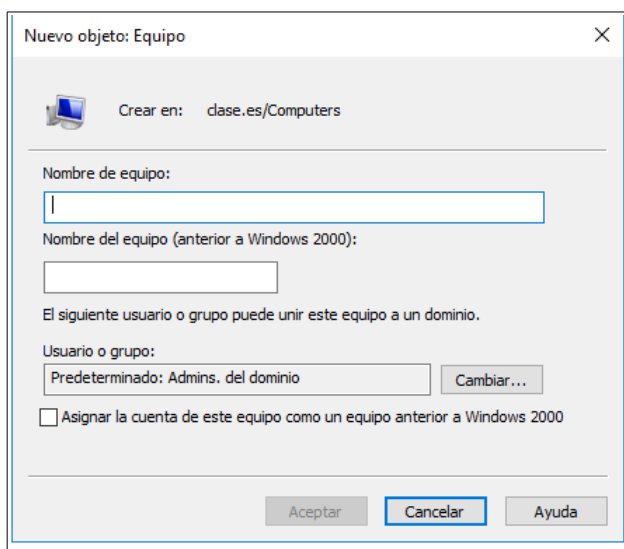


4.2 Operaciones sobre cuentas de equipo.

Para crear una cuenta de equipo, debemos volver a la herramienta Usuarios y equipos de Active Directory, bien desde el menú Herramientas del Administrador del Servidor, bien desde la consola Herramientas comunes que creamos en el capítulo anterior.

Como hicimos con las cuentas de usuario, cuando se abra la ventana Usuarios y equipos de Active Directory, buscaremos en el panel de la izquierda el contenedor que nos interese. En este caso, utilizaremos el contenedor **Computers**.

Después haremos clic con el botón derecho del ratón sobre el contenedor.



En ella, rellenaremos el nombre que queremos que tenga la cuenta de equipo que estamos creando (Nombre de equipo).

Además, de forma automática, se irá completando el campo Nombre del equipo (anterior a Windows 2000) con los primeros 15 caracteres que escribamos en el campo de arriba. Además, las minúsculas se convertirán en mayúsculas.

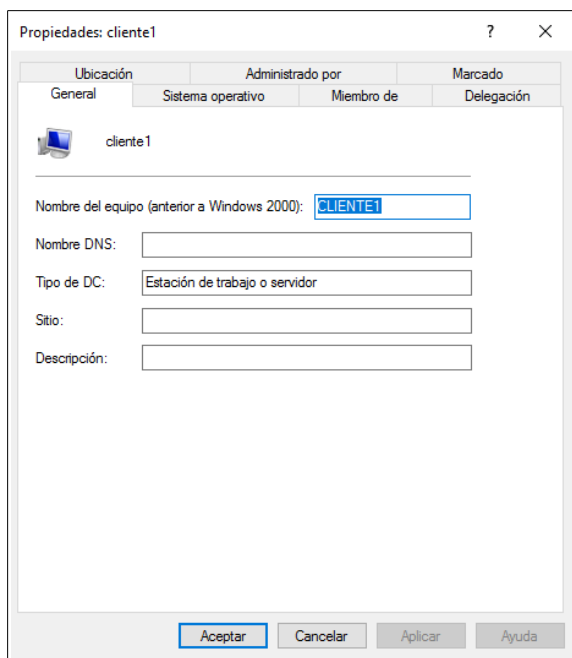
También podremos elegir el usuario o grupo que podrá unir a este equipo al dominio, aunque, de forma predeterminada sólo lo podrán hacer los administradores. Si el cliente que utilizará esta cuenta de equipo ejecuta Windows 95, Windows 98 o Windows NT, deberemos marcar la opción Asignar la cuenta de este equipo como un equipo anterior a Windows 2000.

4.2.1 Modificar valores en las cuentas de los equipos

Igual que ocurría con las cuentas de usuario, podemos volver a la herramienta Usuarios y equipos de Active Directory en cualquier momento para ajustar las propiedades de las cuentas de equipos.

Como antes, usaremos el menú Herramientas del Administrador del Servidor y, después, Usuarios y equipos de Active Directory (o la consola Herramientas comunes que creamos en el capítulo anterior).

Una vez abierta la ventana, hacemos clic con el botón derecho del ratón sobre el equipo que queremos modificar.



Aunque las cuentas de equipo y las cuentas de usuario representan objetos diferentes dentro del dominio, existen aspectos que se administran de una forma prácticamente idéntica. Por este motivo, en lugar de volver a incluir paso a paso el modo de realizar estas operaciones, haremos referencia a sus equivalentes en las cuentas de usuario. En concreto, me estoy refiriendo a las siguientes:

- Deshabilitar una cuenta de equipo
- Hacer que un equipo sea miembro de un grupo
- Eliminar una cuenta de equipo

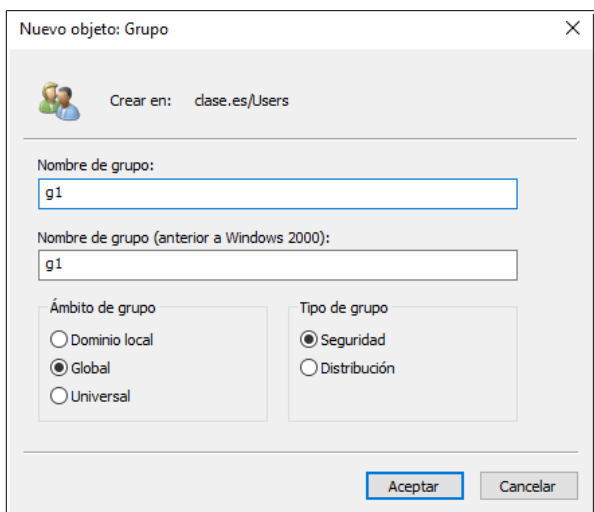
4.3 Operaciones sobre cuentas de grupos.

En este apartado trataremos las principales operaciones de gestión de grupos.

4.3.1 Crear una cuenta de grupo.

Si lo que queremos es crear un nuevo grupo, deberemos volver a la herramienta Usuarios y equipos de Active Directory, usando alguno de los métodos que ya conocemos.

Como en ocasiones anteriores, cuando se abra la ventana Usuarios y equipos de Active Directory, buscaremos en el panel de la izquierda el contenedor en el que queramos guardar el nuevo grupo. En este caso, volveremos a usar el contenedor Users, que ya utilizamos para las cuentas de usuario. Después haremos clic con el botón derecho del ratón sobre el contenedor.

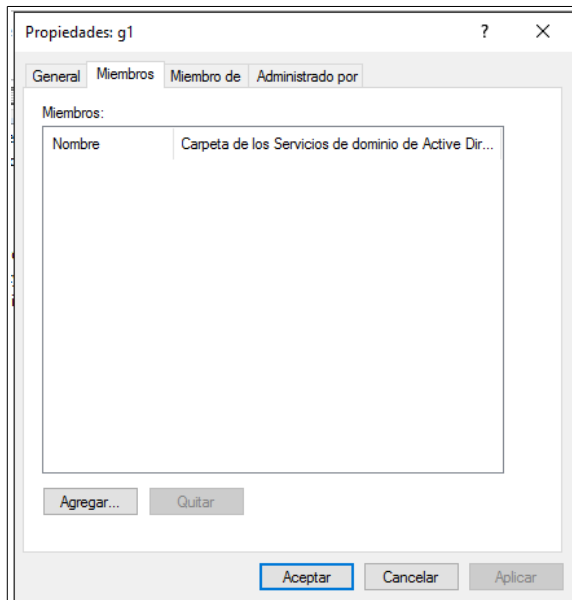


4.3.2 Añadir miembros a un grupo.

Ya vimos cómo convertir a un usuario en miembro de un grupo desde la propia cuenta de usuario. Sin embargo, si necesitamos añadir varios usuarios, será mucho más cómodo hacerlo desde el propio grupo.

Como acabamos de ver en el apartado anterior, para añadir un nuevo miembro a un grupo, deberemos abrir la ventana **Propiedades** de dicho grupo y elegir la solapa

Miembros.



4.3 Operaciones sobre unidades organizativas.

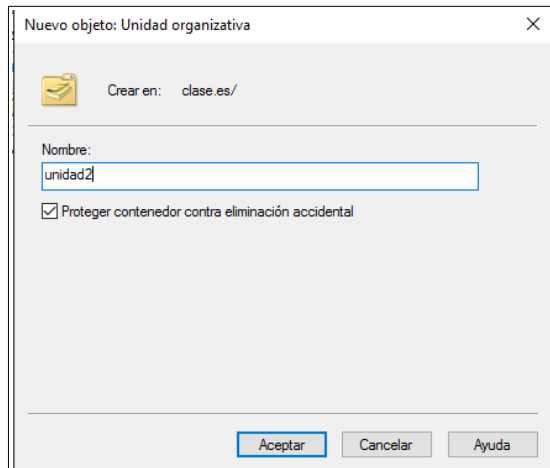
Como recordarás, las **Unidades Organizativas** (en inglés, Organizational Units o, simplemente, OUs) son contenedores del Directorio Activo que pueden incluir usuarios, equipos, grupos y otras unidades organizativas.

A una Unidad Organizativa le podemos otorgar valores de configuración de directiva de grupo o podemos delegar sobre ella una parte de la autoridad administrativa. De esta forma, un usuario puede tener autoridad para administrar una determinada unidad organizativa y no tenerla para el resto. En definitiva, esto significa que podemos definir contenedores que representen la organización lógica de nuestra red.

4.3.1 Crear una nueva unidad organizativa

Lo primero es aprender a crear una Unidad Organizativa, aunque, a estas alturas del capítulo, no creo que esta operación suponga una dificultad.

Como de costumbre, comenzamos por abrir la herramienta Usuarios y equipos de Active Directory. A continuación, ponemos el puntero del ratón sobre el nombre del dominio y hacemos clic con el botón derecho.



Podemos mover usuarios, grupos o equipos a una unidad organizativa, arrastrándolos encima de esta, en ventana Usuarios y equipos de Active Directory.

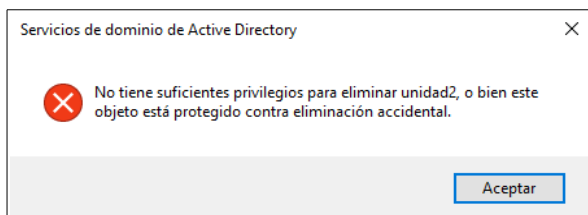
4.3.2 Eliminar una unidad organizativa

Puede que alguna vez necesitemos eliminar alguna de las Unidades Organizativas que hayamos definido.

En realidad, el proceso es parecido a la eliminación de cualquier otro objeto, pero con algunas particularidades que veremos a continuación.

Como de costumbre, comenzamos por abrir la herramienta Usuarios y equipos de Active Directory. A continuación, ponemos el puntero del ratón sobre el nombre de la Unidad Organizativa que queremos eliminar y hacemos clic con el botón derecho del ratón.

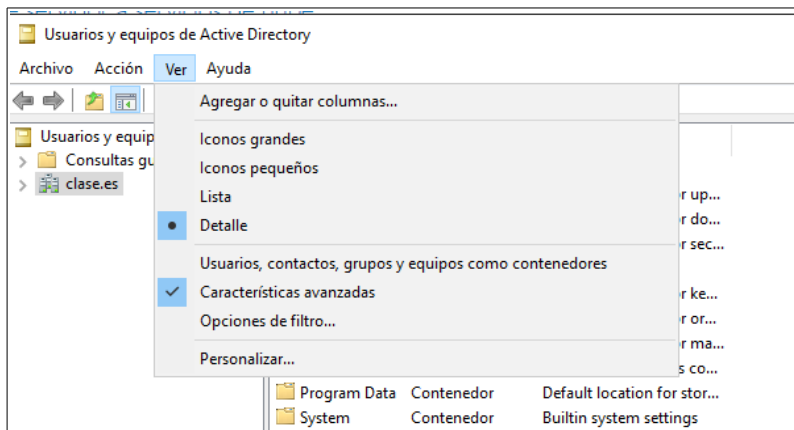
Si todo va bien, la Unidad organizativa desaparecerá del árbol del panel izquierdo. Sin embargo, también puede que tengamos un ligero contratiempo si, al crearla, elegimos la opción Proteger contenedor contra eliminación accidental. En ese caso, aparecerá un aviso como el de la ventana siguiente.



Sistemas Operativos en Red

UT 7 – Directorio activo en Windows Server

En estos casos, deberemos habilitar las características avanzadas de Usuarios y equipos de Active Directory, lo que nos permitirá tener un mayor control sobre todos los objetos que administramos con esta herramienta.



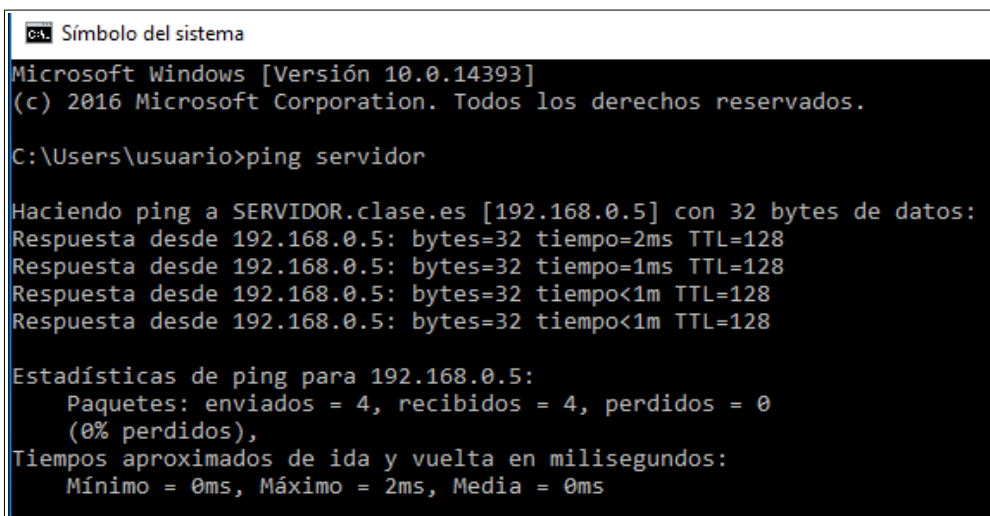
Después de esto, hacemos clic con el botón derecho del ratón sobre el nombre de la Unidad Organizativa. Se abrirá una ventana titulada Propiedades:, seguido del nombre de la Unidad Organizativa. En ella, haremos clic sobre la solapa Objeto y **quitaremos la selección de la opción Proteger objeto contra eliminación accidental.**

5. Conectar equipos clientes al dominio.

Para concluir este tema conectaremos un cliente Windows 10 al dominio que acabamos de configurar.

Los pasos a realizar son los siguientes:

1. **Configurar la dirección IP del servidor y del cliente para que estén en la misma subred.**
 - El servidor además deberá tener IP fija. Para verificar la conectividad utilizaremos el comando ping.
 - Además al configurar la IP del cliente, indicaremos que como dirección DNS la del servidor (ya que es ahí donde hemos instalado dicho servicio)



```
C:\> Símbolo del sistema
Microsoft Windows [Versión 10.0.14393]
(c) 2016 Microsoft Corporation. Todos los derechos reservados.

C:\Users\usuario>ping servidor

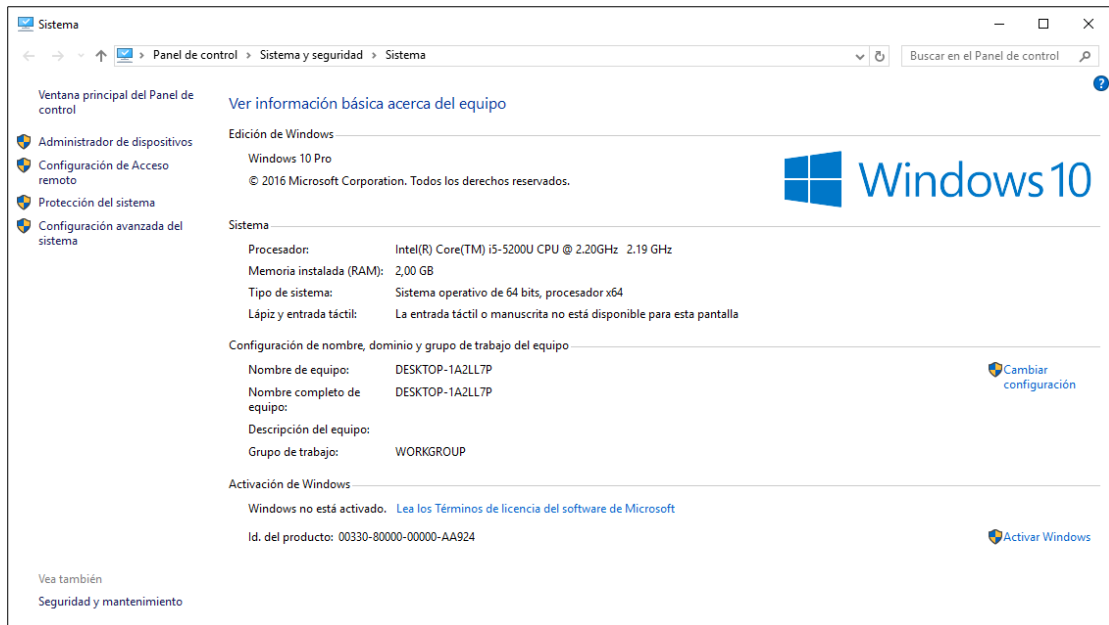
Haciendo ping a SERVIDOR.clase.es [192.168.0.5] con 32 bytes de datos:
Respuesta desde 192.168.0.5: bytes=32 tiempo=2ms TTL=128
Respuesta desde 192.168.0.5: bytes=32 tiempo=1ms TTL=128
Respuesta desde 192.168.0.5: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.0.5: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 192.168.0.5:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
              (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 2ms, Media = 0ms
```

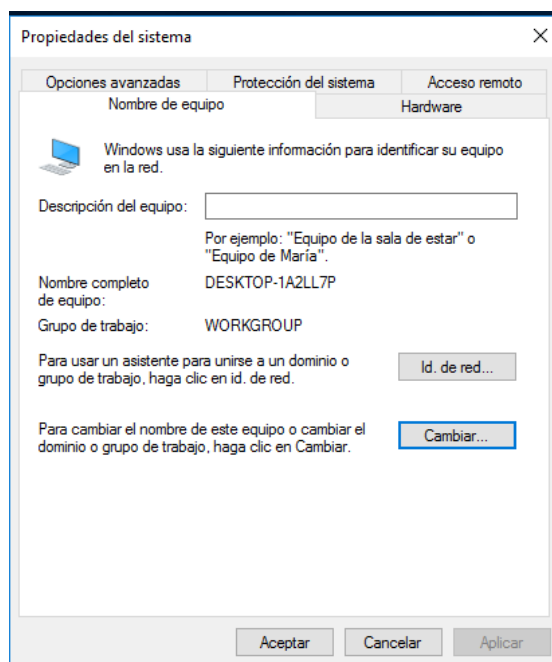

Sistemas Operativos en Red

UT 7 – Directorio activo en Windows Server

2. En el equipo cliente accedemos a **sistema** (en panel de control) y pulsamos el link “**Cambiar la configuración**”.

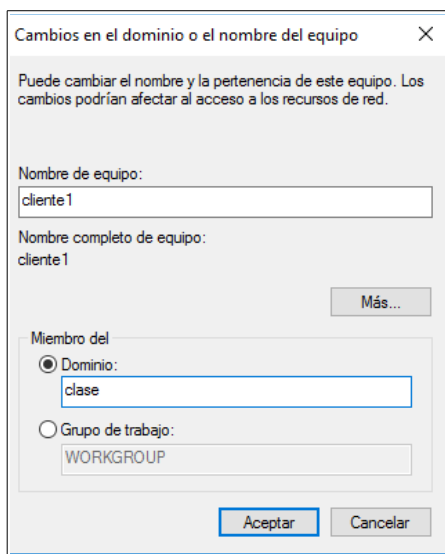


En esta pantalla pulsaremos el botón “**Cambiar**”.

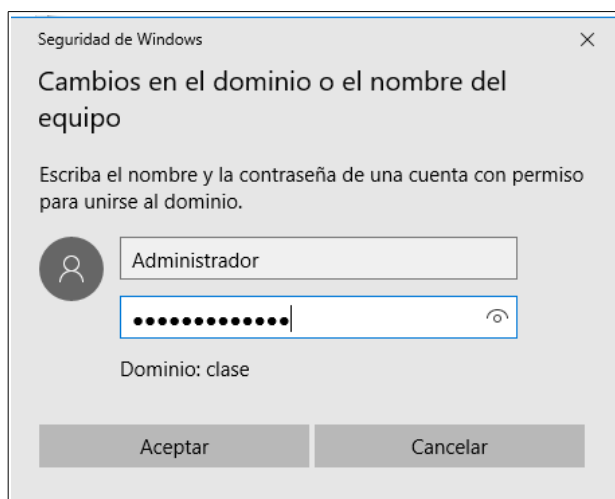


3. En esta pantalla cambiaremos dos cosas:

- El nombre del equipo. Esto no es necesario pero si conveniente, ya que el nombre por defecto suele ser bastante complicado).
- El Dominio. Debemos poner el nombre **NETBIOS** del dominio, en nuestro caso “clase”.



4. El sistema nos solicitará el nombre y contraseña de un usuario administrador del dominio.



5. Si todo ha ido bien, el cliente ya estará conectado al dominio.

