



Active Directory

En esta guía haremos la instalación y configuración de un directorio activo o comúnmente "dominio".

Este servicio es útil cuando el tamaño de la red crece haciendo que la gestión y personalización de usuarios y equipos sea costosa en tiempo y recurso. Imaginemos una red en la que los equipos son compartidos, es decir, cualquiera puede sentarse en un equipo e identificarse con su propio usuario. Para empezar, esto requiere que cada usuario sea creado en todos y cada uno de los equipos de la red.

Es altamente probable que, al volver de vacaciones, el usuario no recuerde su contraseña y solicite a algún administrador su cambio. Esto, aparentemente sencillo y rápido, requiere de replicarlo en todos los equipos de la red. De la misma manera, el alta de un nuevo usuario, asignación de diferentes privilegios, permisos para acceder a recursos como impresoras o el bloqueo inmediato de un determinado usuario requiere de la actuación individual en cada equipo de la red.

La respuesta a este problema pasa por "Active Directory" en Windows o "LDAP" en Linux. Ambos sirven para guardar las credenciales de los usuarios de manera que las comprobaciones de autenticación ya no se hacen en local y sí en estos servidores llamados "controladores".

Gracias a LDAP o AD podemos crear el usuario solamente en "el dominio". De esta manera, todos los equipos del dominio validarán las credenciales en el controlador.

Podemos visualizar un directorio activo como una base de datos que almacena información sobre la autenticación de usuarios, sus permisos, la organización de recursos y las distintas políticas o configuraciones que se pueden aplicar a equipos o usuarios.

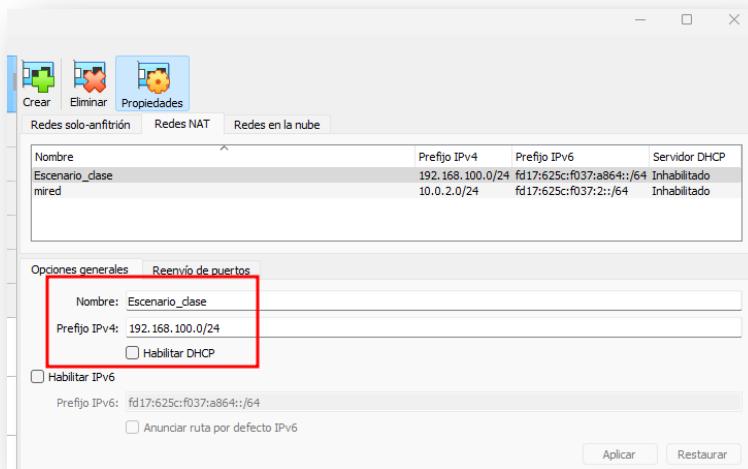
Los conceptos de debemos manejar son estos 5:

- Controlador de dominio. Es el servidor (o varios) donde corre el servicio AD
- Dominio: Es el FQDN que se usa en la organización.
- Unidades Organizativas (OU). Divisiones administrativas de usuarios y recursos para una mejor organización.
- Grupos. Metadato administrativo para agrupar usuarios que comparten permisos.
- Políticas de grupo (GPO). Reglas que configuran equipos y usuarios.

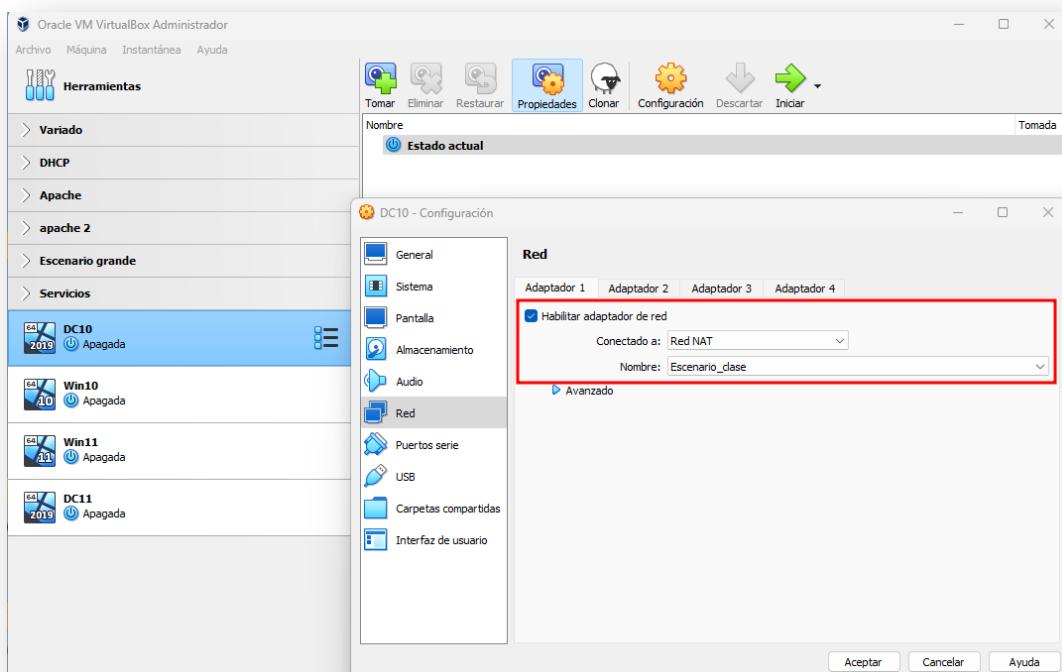


Configuración máquinas virtuales

Para el correcto funcionamiento de nuestro escenario debemos usar una red NAT configurada con una dirección de red de nuestra elección y con el servicio DHCP deshabilitado.



Yo configuraré mi red NAT en VirtualBox para usar la red 192.168.100.X como se ve en la captura anterior. Después debo asegurarme de que todas las máquinas virtuales que usaré en este escenario están correctamente configuradas para usar esta red.

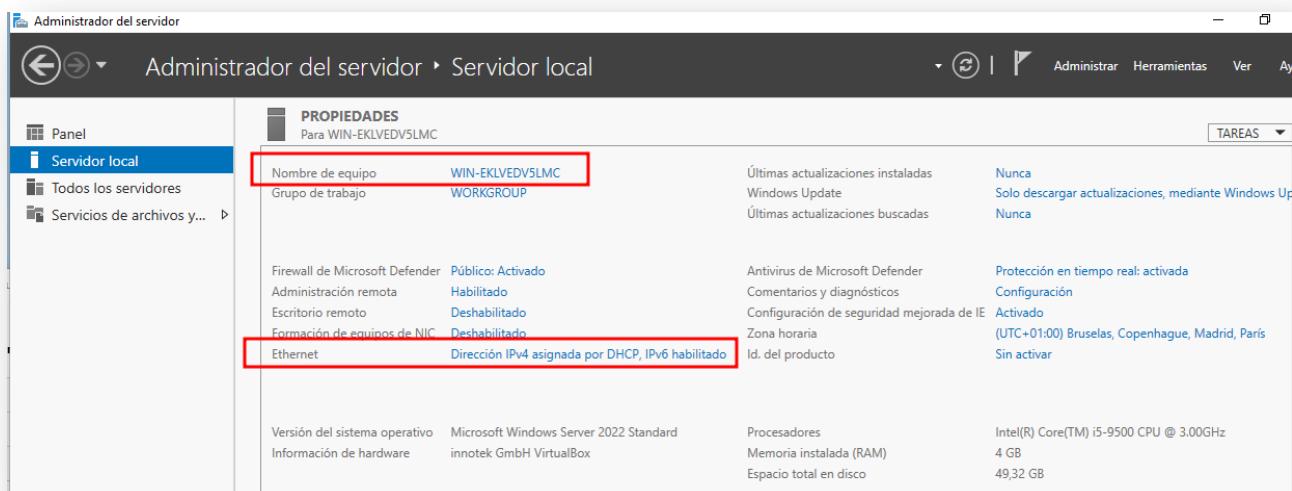




Configuración del DC01 (local)

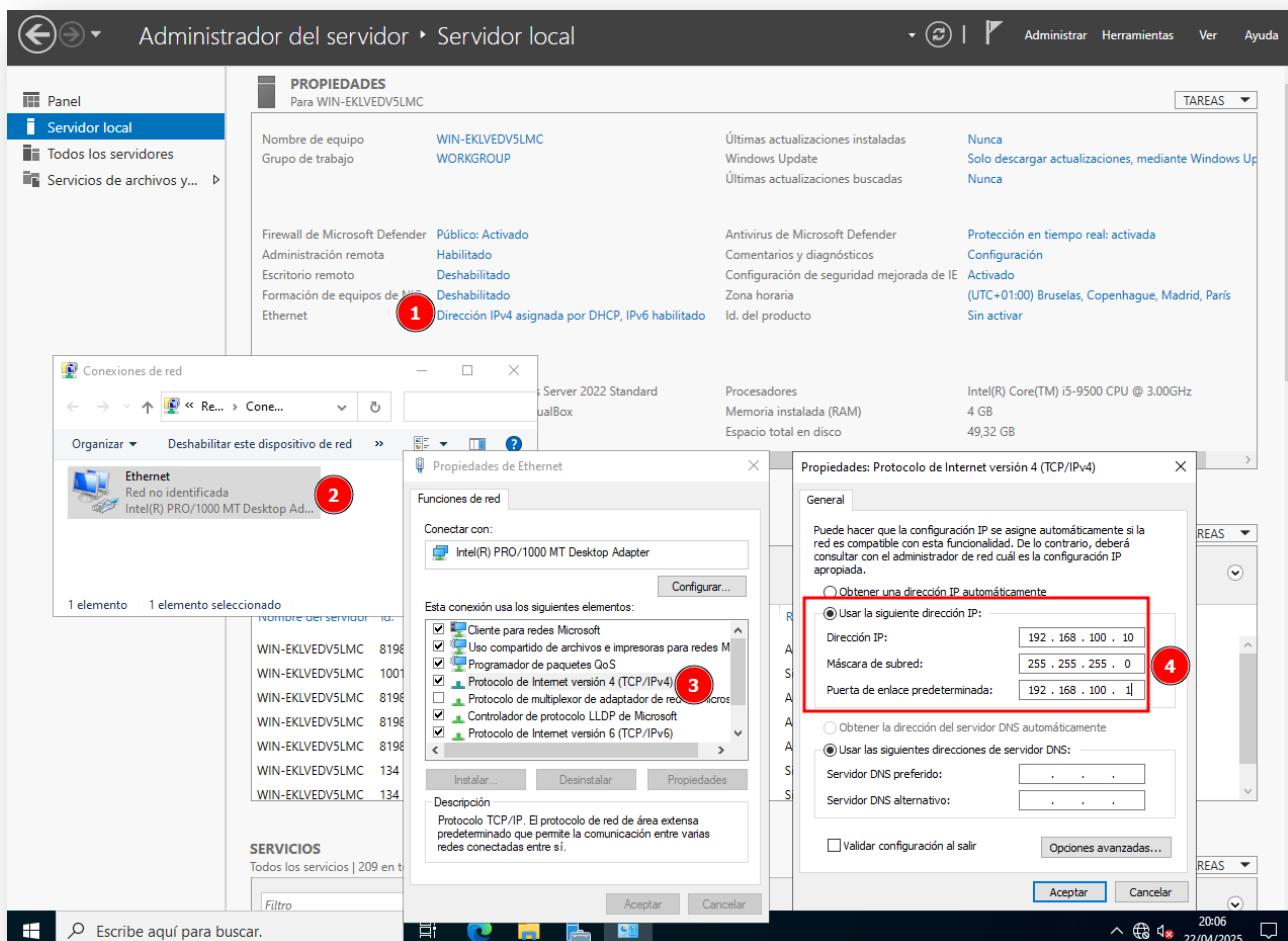
El primer paso consiste en configurar nuestro único equipo en la red, el servidor "DC01". En Active Directory usaremos principalmente el nombre del equipo y dejaremos las IPs para configuraciones mucho más específicas. Por esta razón será necesario tener una política clara en la asignación de nombres para así facilitar la gestión en general y los incidentes en particular. Con el uso y asignación de IPs ya sabemos que pasa algo parecido.

Para nuestro servidor "DC10" usaremos el nombre "dc10" y la IP será la terminada en 10, en mi caso la 192.168.100.10. Recordemos que la red NAT de VirtualBox nos proporciona una puerta de acceso a internet en la IP terminada en 1, en mi caso la 192.168.100.1. Por ahora no configuraremos ningún DNS.



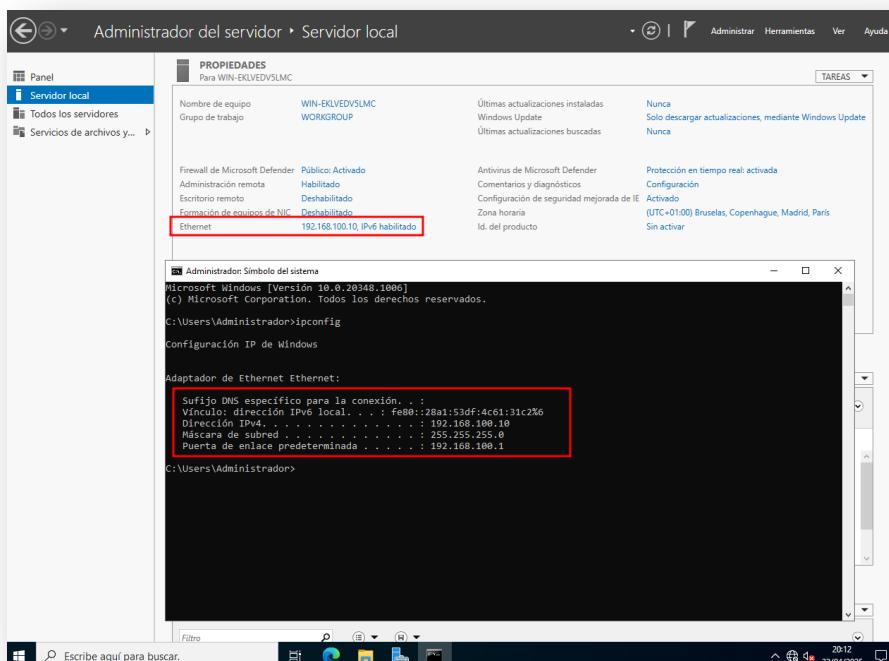
Al arrancar el servidor y autenticarnos correctamente aparecerá el "Administrador del servidor", un panel de mando desde donde podemos ver el estado general de los servidores y los servicios que se ejecutan en ellos. Al pinchar en "servidor local" podemos ver un resumen del estado y configuración donde comprobamos que el nombre del equipo aún está por defecto y que la configuración IP está aún en DHCP.

Hay muchas maneras de cambiar la IP y fijar una manualmente. En guías anteriores vimos como hacerlo a través de comandos, aquí aprovecharemos alguna de las opciones gráficas.



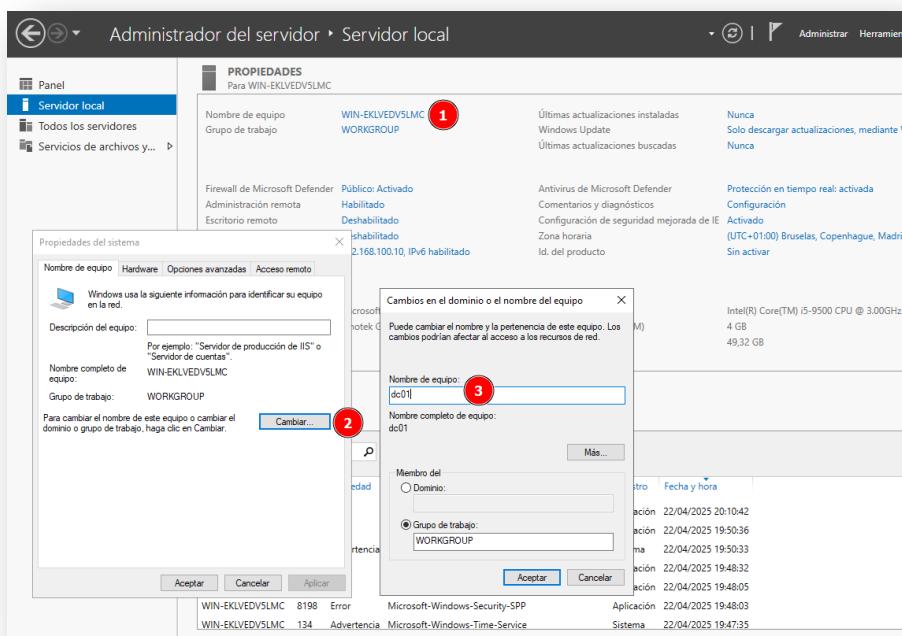
Desde la configuración Ethernet del panel del servidor local accedemos a las interfaces de red instaladas en el servidor. Desde las propiedades de esta interfaz editamos las propiedades del "Protocolo de Internet versión 4" y allí indicamos la dirección IP, máscara y puerta de enlace. Como por ahora no vamos a navegar podemos dejar el DNS vacío (será necesario después).

Este cambio no requiere reinicio del sistema y en unos segundos veremos que el panel de administración del servidor local ya muestra la IP que hemos asignado. Recordemos que siempre podremos ver esta información también mediante los comandos que ya conocemos.

The screenshot shows the Windows Server Local Administrator interface. In the center, there's a window titled "PROPIEDADES Para WIN-EKLVEDV5LMC". It displays basic system information like the computer name (WIN-EKLVEDV5LMC), workgroup (WORKGROUP), and various service status. Below this, a "Propiedades del sistema" (System Properties) window is open, specifically the "Hardware" tab. A command prompt window is also visible, showing the output of the "ipconfig" command, which includes details about the Ethernet adapter, such as its IP address (192.168.100.10), subnet mask (255.255.255.0), and default gateway (192.168.100.1).

El cambio de nombre del equipo es muy similar. Pulsando sobre el nombre que aparece en el panel del servidor local se nos desplegará las propiedades del sistema y allí haremos clic sobre el botón "Cambiar". Una vez cambiado el nombre del equipo, aceptamos y nos pedirá un reinicio para que los cambios entren en funcionamiento.



This screenshot shows the "PROPIEDADES" window for the same computer (WIN-EKLVEDV5LMC). A red circle labeled "1" highlights the computer name "WIN-EKLVEDV5LMC". A red circle labeled "2" points to the "Cambiar..." button in the "Nombre de equipo" section of the "Propiedades del sistema" dialog. A red circle labeled "3" points to the new computer name "dc01" entered into the "Nombre de equipo" field of the "Cambiando el nombre o el dominio del equipo" (Changing Computer Name or Domain) dialog. The dialog also shows the "Grupo de trabajo" (Workgroup) is set to "WORKGROUP".



El resultado final debería ser un panel de servidor local donde el nombre del equipo y su IP sean los planificados.

The screenshot shows the 'PROPIEDADES' (Properties) window for a local server named 'dc01'. The 'Servidor local' (Local Server) tab is selected. Key configuration details shown include:

- Nombre de equipo (Computer Name): dc01
- Grupo de trabajo (Workgroup): WORKGROUP
- Firewall de Microsoft Defender: Público: Activado (Public: Enabled)
- Administración remota: Habilitado (Remote Administration: Enabled)
- Escritorio remoto: Deshabilitado (Remote Desktop: Disabled)
- Formación de equipos de NIC: Deshabilitado (NIC Team Formation: Disabled)
- Ethernet: 192.168.100.10, IPv6 habilitado (Ethernet: 192.168.100.10, IPv6 enabled)

Instalación del role Active Directory

Ahora que ya tenemos el equipo correctamente configurado en la red vamos a instalar y configurar el servicio "Active Directory" para crear y gestionar nuestro propio dominio. A través de "Agregar roles y características" añadimos a nuestro único servidor el role de "Servicios de dominio de Active Directory". Se añadirán automáticamente las características necesarias, no es necesario agregar ninguna característica extra.

The screenshot shows the 'Asistente para agregar roles y características' (Role and Feature Wizard) window. The 'Roles de servidor' (Server Roles) step is selected. In the 'Roles' list, the 'Servicios de dominio de Active Directory' checkbox is checked, indicating it is the selected role to be installed. The 'Descripción' (Description) pane provides information about the selected role.



En una de las ventanas finales del asistente de instalación del AD nos recuerda que es buena idea tener un mínimo de 2 controladores de dominio y que necesitará hacer uso de un servidor DNS. Como nosotros no tenemos instalado ningún servicio DNS es este escenario, el asistente lo instalará.

Servicios de dominio de Active Directory

SERVIDOR DE DESTINO
dc01

Observaciones:

- Para ayudar a garantizar que los usuarios puedan iniciar sesión en la red en caso de una interrupción en el servidor, instale un mínimo de dos controladores de dominio para un dominio.
- AD DS requiere la instalación de un servidor DNS en la red. Si no hay un servidor DNS instalado, se le pedirá que instale el rol de servidor DNS en este servidor.

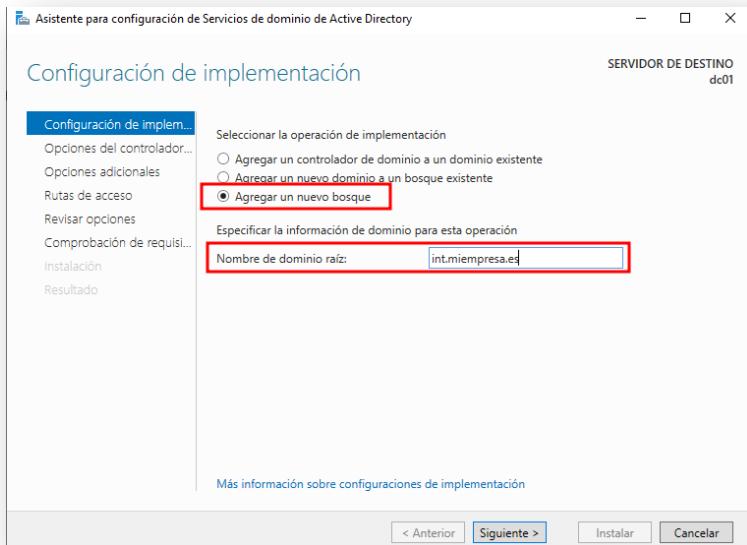
Azure Active Directory, un servicio en línea independiente, puede proporcionar una administración de identidades y acceso simplificada, informes de seguridad e inicio de sesión único en las aplicaciones web en la nube y locales.

[Obtener más información sobre Azure Active Directory](#)
[Configurar Office 365 con Azure Active Directory Connect](#)

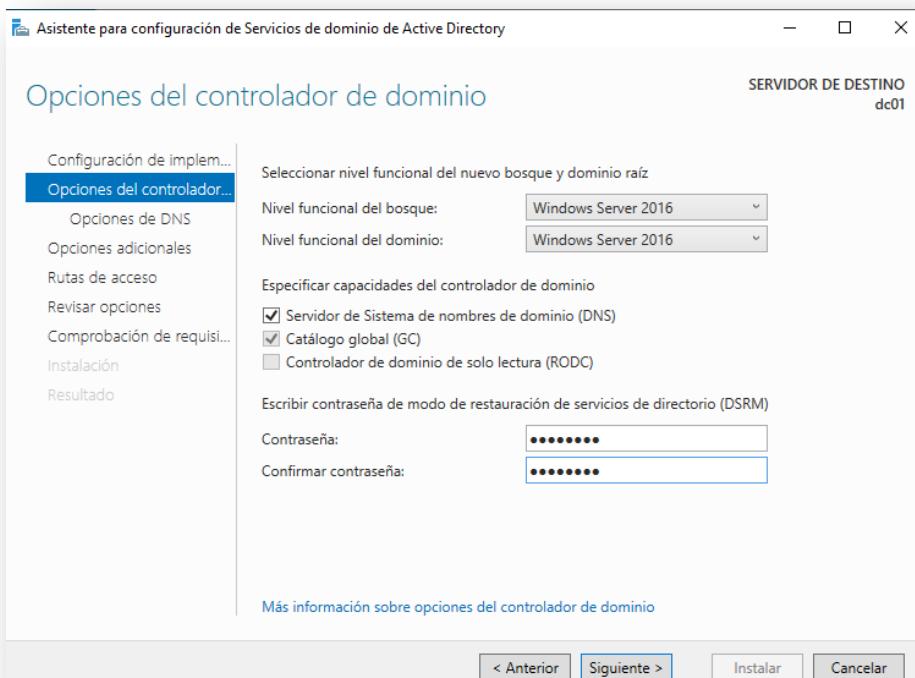
Al acabar la instalación aparecerán mensajes recordando que es necesario configurar el AD para que funcione. Para realizar la configuración y puesta en marcha pulsaremos en "Promover este servidor a controlador de dominio".

La primera pregunta que hace el asistente es cómo se va a incorporar este nuevo controlador de dominio a la infraestructura existente. Es posible que queramos añadir este controlador a un dominio ya existente o tal vez queramos añadir un nuevo dominio a un bosque, pero en este caso empezamos de cero así que seleccionaremos "Aregar a un nuevo bosque". En esta misma ventana tendremos que seleccionar el nombre de nuestro dominio. En este caso usaré un subdominio "int" del dominio "miempresa.es".

Digamos que la parte de la intranet de mi empresa tiene esa URL.

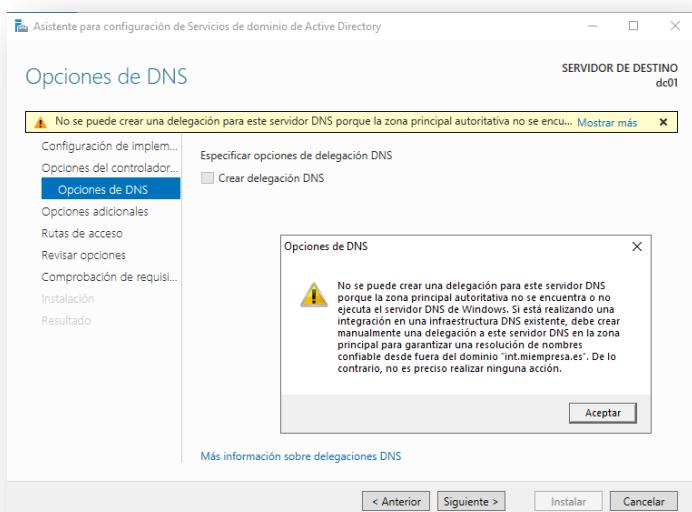


En la siguiente ventana del asistente tendremos que indicar la versión más antigua de servidor AD que estemos usando a nivel de bosque y dominio. Esto limitará las funcionalidades de las nuevas versiones para mantener compatibilidad con los servidores que ya estén funcionando. En nuestro caso no debemos preocuparnos por compatibilidad porque este es nuestro único servidor por ahora. Algo importante en esta ventana es escribir (y custodiar) una contraseña para restauración de servicios en caso de problemas.

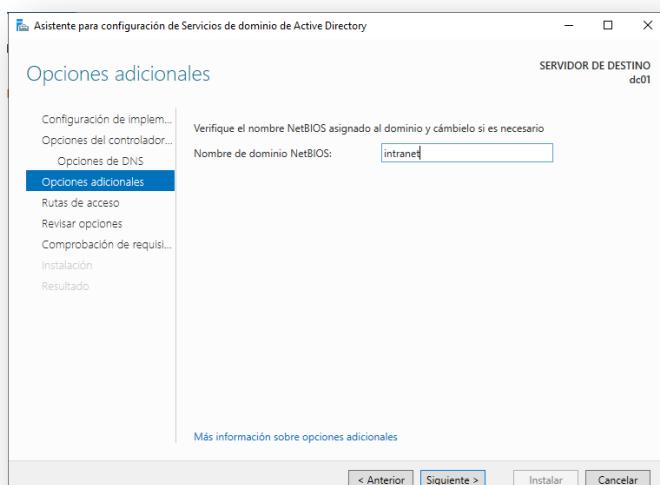




La siguiente ventana gestiona el necesario servidor DNS que necesitamos. Como ya hemos dicho, en AD se usa preferentemente nombres en lugar de IPs por ello es necesario tener acceso a los registros de un DNS para poder crear las nuevas asociaciones entre nombres de equipos y sus IPs. En esta ventana se nos informa que el asistente no ha sido capaz de encontrar ningún servidor DNS autoritativo Windows para nuestra zona "int.miempresa.es". De haberlo encontrado nos daría la opción de crear una delegación DNS para que el AD pudiera escribir en él. En nuestro escenario no tenemos ningún DNS por lo que saltamos este paso y se descargará y configurará automáticamente un servidor DNS en este equipo.

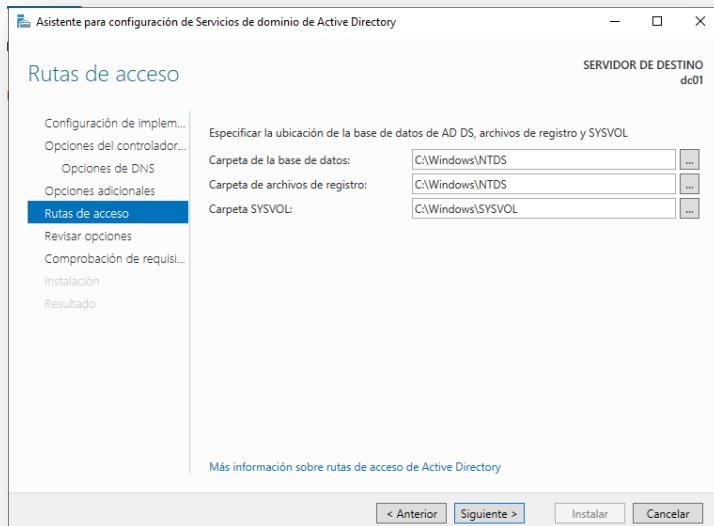


En la siguiente ventana podemos crear un "Alias" para el nombre del dominio. De esta manera podemos convertir un nombre de dominio "técnico" en algo más amigable. En nuestro caso lo cambiaremos por "intranet".





La siguiente ventana no la modificaremos, pero hace referencia a las carpetas locales de "dc01" donde se guardarán los metadatos del dominio. En un escenario más serio podríamos cambiar estas rutas apuntando a algún tipo de RAID u otro sistema de ficheros con tolerancia a fallos y alta disponibilidad.



La siguiente ventana del asistente es un resumen de lo que se va a hacer. Tal vez lo más interesante es comprobar que se instalará un servidor DNS y que la contraseña del administrador del dominio será la misma que la del administrador del equipo local. También tenemos la opción de descargar es script en PowerShell para poder realizar esta configuración por la línea de comandos.



Asistente para configuración de Servicios de dominio de Active Directory

Revisar opciones

SERVIDOR DE DESTINO
dc01

- Configuración de imple...
- Opciones del controlador...
- Opciones de DNS
- Opciones adicionales
- Rutas de acceso
- Revisar opciones**
- Comprobación de requisisi...
- Instalación
- Resultado

Revisar las selecciones:

Configura este servidor como el primer controlador de dominio de Active Directory en un nuevo bosque.

El nombre del nuevo dominio es "int.miempresa.es". Éste es también el nombre del nuevo bosque.

El nombre NetBIOS del dominio es intranet.

Nivel funcional del bosque: Windows Server 2016

Nivel funcional del dominio: Windows Server 2016

Opciones adicionales:

Catálogo global: Sí

Servidor DNS: Sí

Crear delegación DNS: No

Carpeta de la base de datos: C:\Windows\NTDS

Carpeta del archivo de registro: C:\Windows\NTDS

Carpeta SYSVOL: C:\Windows\SYSVOL

El servicio Servidor DNS se configurará en este equipo.

Este equipo se configurará para usar este servidor DNS como servidor DNS preferido.

La contraseña del nuevo administrador de dominio será la misma que la del administrador local de este equipo.

Esta configuración se puede exportar a un script de Windows PowerShell para automatizar instalaciones adicionales

[Ver script](#)

Más información sobre opciones de instalación

[< Anterior](#) [Siguiente >](#) [Instalar](#) [Cancelar](#)

La última ventana del asistente es una comprobación de que el equipo cumple con los requisitos para ser controlador de dominio. Veremos algunos mensajes de aviso en referencia a valores predeterminados y la advertencia de que no se ha encontrado una delegación del DNS (así que asume que él será el autoritativo para ese dominio). Lo verdaderamente importante es que en la parte superior pone que sí cumple con los requisitos así podemos proceder a la instalación sin problema.



Asistente para configuración de Servicios de dominio de Active Directory

Comprobación de requisitos previos

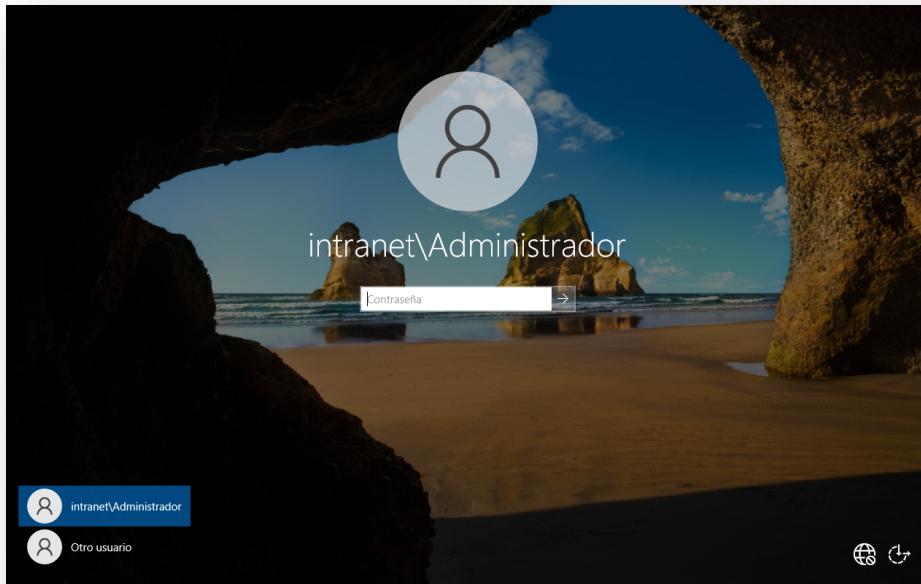
SERVIDOR DE DESTINO
dc01

✓ Todas las comprobaciones de requisitos previos se realizaron correctamente. Haga clic en 'Instalar' para co... [Mostrar más](#) ×

Configuración de implementación Opciones del controlador... Opciones de DNS Opciones adicionales Rutas de acceso Revisar opciones Comprobación de requisitos previos Instalación Resultado	<p>Los requisitos previos deben validarse antes de instalar los servicios de dominio de Active Directory en el equipo</p> <p>Volver a comprobar requisitos previos</p> <p>Ver resultados</p> <p>! Los controladores de dominio de Windows Server 2022 tienen un valor predeterminado para la configuración de seguridad denominada "Permitir algoritmos de criptografía compatibles con Windows NT 4.0" que evita el uso de algoritmos de criptografía débiles al establecer sesiones de canal de seguridad.</p> <p>Para obtener más información acerca de esta opción de configuración, consulte el artículo 942564 de Knowledge Base (http://go.microsoft.com/fwlink/?LinkId=104751).</p> <p>! No se puede crear una delegación para este servidor DNS porque la zona principal autoritativa no se encuentra o no ejecuta el servidor DNS de Windows. Si está realizando una integración en una infraestructura DNS existente, debe crear manualmente una delegación a este servidor DNS en la zona principal para garantizar una resolución de nombres confiable desde fuera del dominio "int.miempresa.es". De lo contrario, no es preciso realizar ninguna acción.</p> <p>i Comprobación de requisitos previos completada</p> <p>✓ Todas las comprobaciones de requisitos previos se realizaron correctamente. Haga clic en 'Instalar' para comenzar la instalación.</p> <p>! Si hace clic en Instalar, el servidor se reiniciará automáticamente cuando finalice la operación de promoción.</p> <p>Más información sobre requisitos previos</p>
---	--

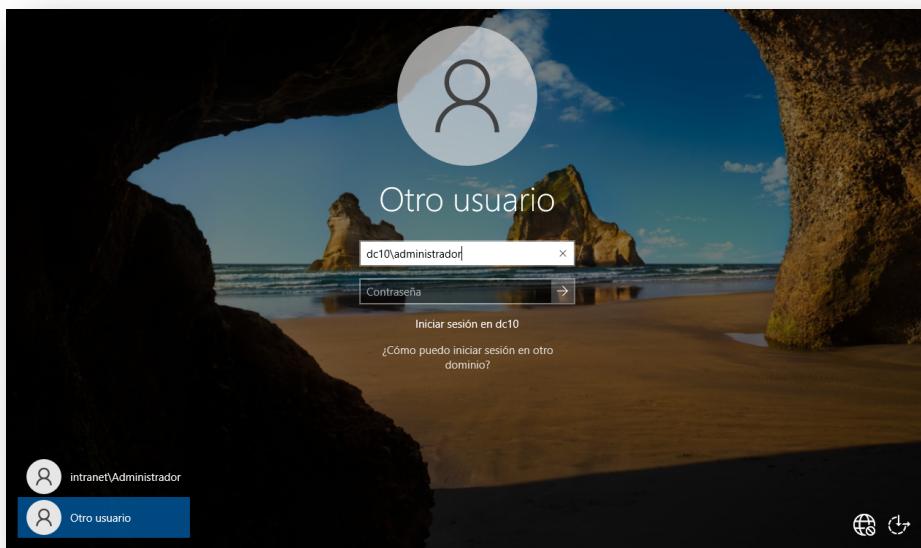
[< Anterior](#) [Siguiente >](#) [Instalar](#) [Cancelar](#)

El equipo se reiniciará automáticamente después de la instalación y arrancará como controlador de dominio. El primer cambio que notaremos es que ahora podemos foguearnos en el dominio o como usuario local.



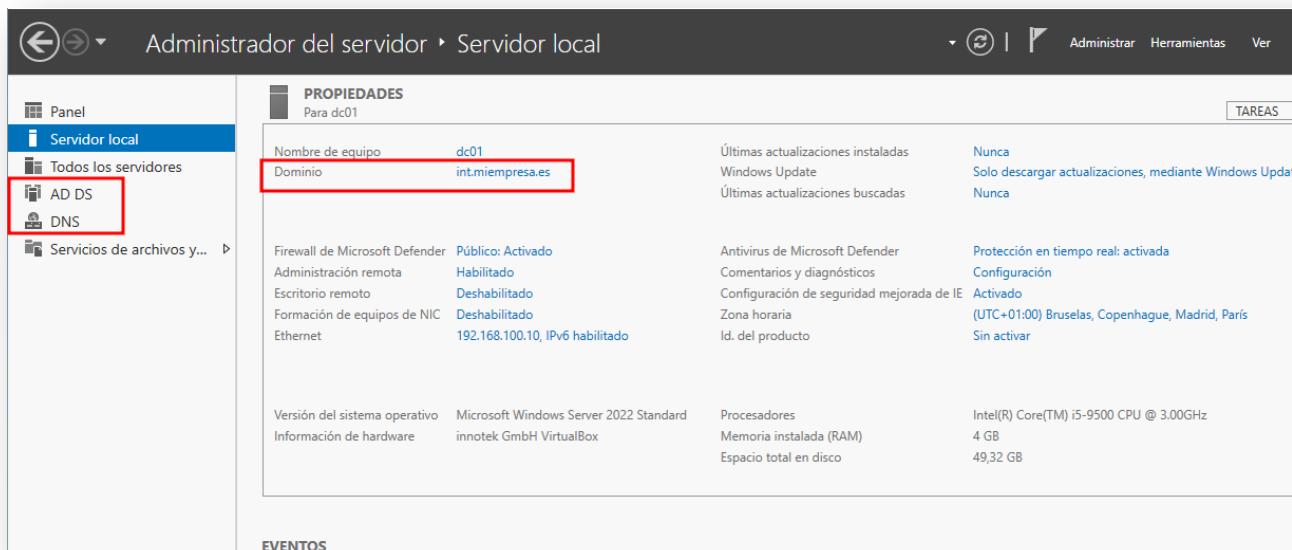
Recordemos que ahora tenemos dos usuarios "Administradores". Uno es local y pertenece solamente al equipo "dc10". El otro es del dominio y pertenece a cualquier equipo dentro de "int.miempresa.es". Para poder distinguirlos ahora los veremos precedidos del ámbito al que pertenezcan.

Los equipos que pertenecen a un AD arrancarán preferentemente contra el dominio. Si queremos forzar a que se comprueben las credenciales contra el equipo local tendremos que hacer explícito en ámbito y el usuario como se ve en la siguiente captura.



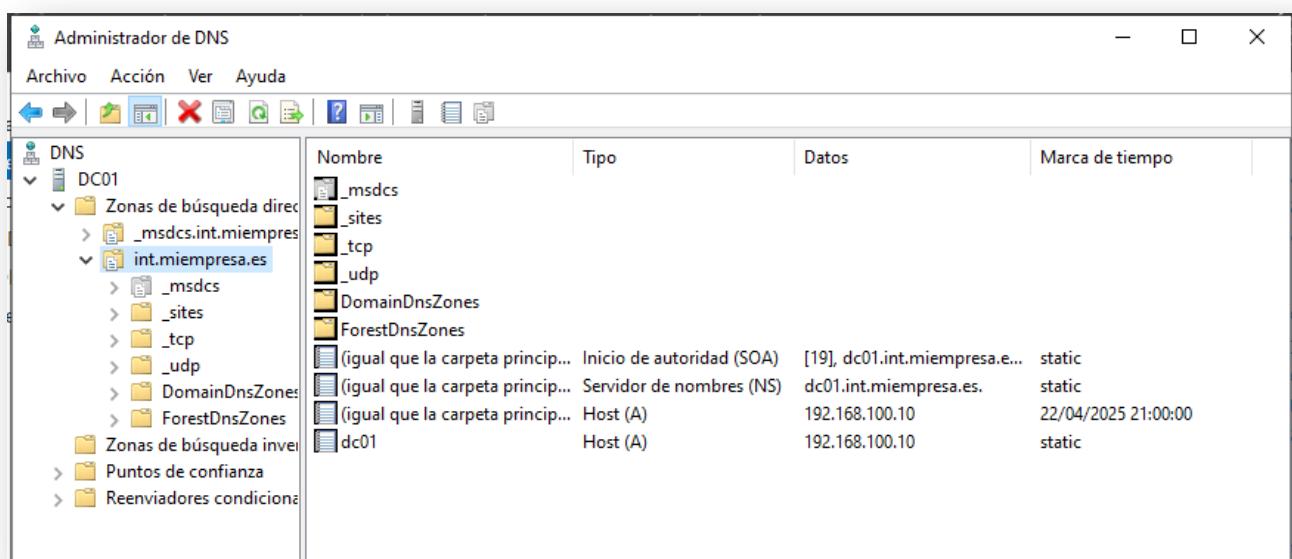


Una vez autenticados como administradores del dominio en "dc01" podremos comprobar en el panel que ya no pertenecemos a ningún grupo de trabajo y sí pertenecemos al dominio "int.miempresa.es". Además también podemos ver como se ha creado un panel para el DNS y otro para en AD



PROPIEDADES		TAREAS	
Nombre de equipo	dc01	Últimas actualizaciones instaladas	Nunca
Dominio	int.miempresa.es	Windows Update	Solo descargar actualizaciones, mediante Windows Updat
		Últimas actualizaciones buscadas	Nunca
Firewall de Microsoft Defender	Público: Activado	Antivirus de Microsoft Defender	Protección en tiempo real: activada
Administración remota	Habilitado	Comentarios y diagnósticos	Configuración
Escritorio remoto	Deshabilitado	Configuración de seguridad mejorada de IE	Activado
Formación de equipos de NIC	Deshabilitado	Zona horaria	(UTC+01:00) Bruselas, Copenhague, Madrid, París
Ethernet	192.168.100.10, IPv6 habilitado	Id. del producto	Sin activar
Versión del sistema operativo	Microsoft Windows Server 2022 Standard	Procesadores	Intel(R) Core(TM) i5-9500 CPU @ 3.00GHz
Información de hardware	innotek GmbH VirtualBox	Memoria instalada (RAM)	4 GB
		Espacio total en disco	49,32 GB

A través del menú "Herramientas" podemos acceder al administrador de DNS donde encontraremos que el asistente ha configurado correctamente los registros SOA, NS y A de nuestra zona "int.miempresa.es" y del equipo "dc01"

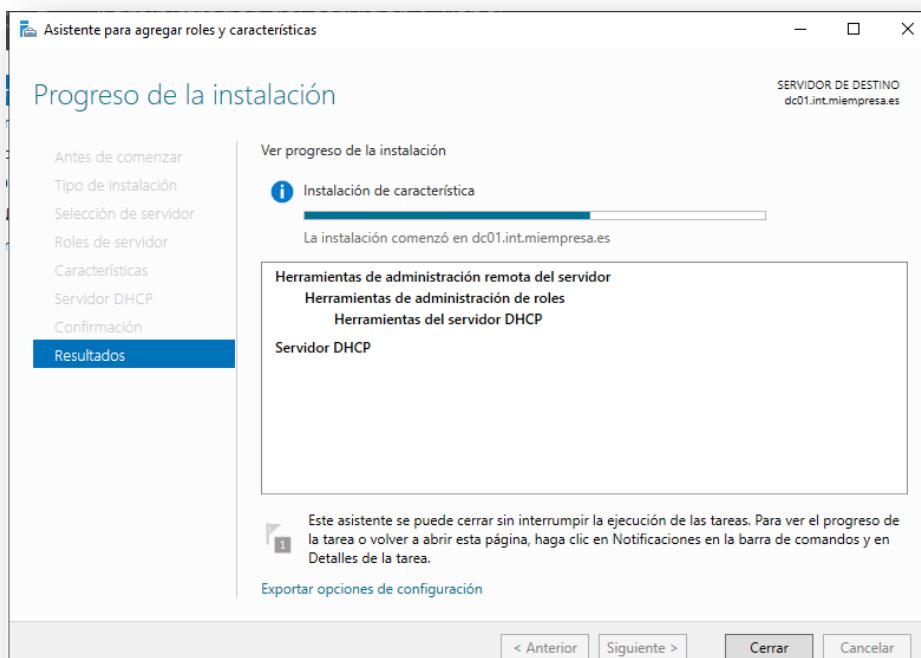


Nombre	Tipo	Datos	Marca de tiempo
_msdcs	Inicio de autoridad (SOA)	[19], dc01.int.miempresa.e...	static
_sites	Servidor de nombres (NS)	dc01.int.miempresa.es.	static
_tcp			
_udp			
DomainDnsZones			
ForestDnsZones			
(igual que la carpeta princip...)	Host (A)	192.168.100.10	22/04/2025 21:00:00
(igual que la carpeta princip...)	Host (A)	192.168.100.10	22/04/2025 21:00:00
dc01	Host (A)	192.168.100.10	static

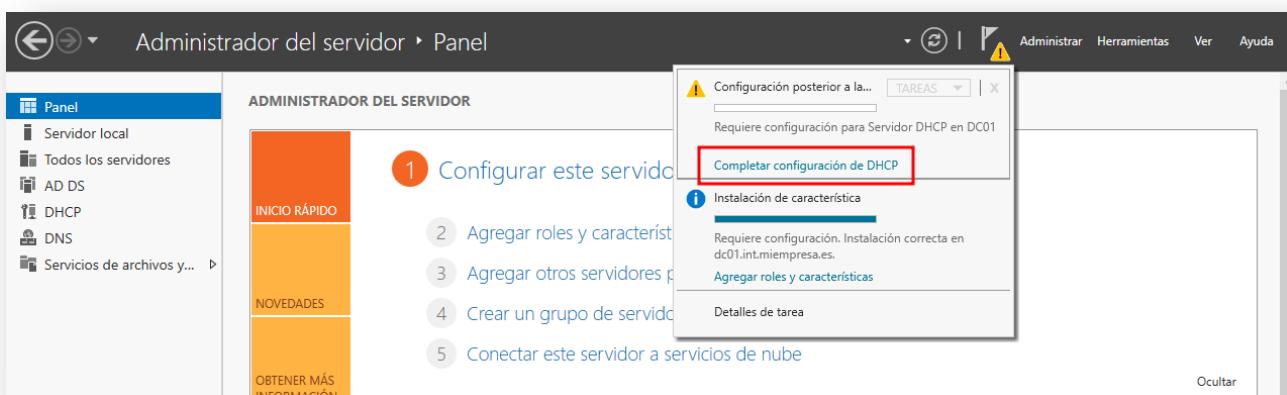


Instalación servicio DHCP (opcional)

Para simplificar la configuración de los nuevos equipos que se añadan al dominio vamos a instalar el servicio DHCP en "dc10" de manera que configure automáticamente los parámetros de red de los nuevos equipos. Para ello, desde "Aregar roles y características" seleccionamos el "role" de DHCP y dejamos que asigne las características que necesite para finalmente pinchar en "Instalar"



Para completar la puesta en marcha del servicio DHCP es necesario configurarlo. Podremos hacerlo desde varios puntos, yo seleccionaré el "Completar configuración DHCP" que aparece en las notificaciones.





El haber instalado el servidor DHCP después de promocionar el equipo "dc10" a controlador de dominio nos permite configurar el servicio DHCP teniendo en cuenta las credenciales del administrador del dominio.

Para crear un nuevo ámbito DHCP debemos entrar en el menú "Herramientas" y seleccionar "DHCP". Allí encontraremos que el servidor está totalmente identificado con su nombre de dominio. Desplegaremos la opción de IPv4 para crear en ella un "nuevo ámbito" y entonces aparecerá un asistente. En la primera ventana podemos poner un nombre significativo al DHCP, yo usaré "dhcp_dominio"

Asistente para ámbito nuevo

Nombre de ámbito
 Debe escribir un nombre identificativo para el ámbito. También puede proporcionar una descripción.

Escriba un nombre y una descripción para este ámbito. Esta información le ayuda a identificar rápidamente cómo se usa el ámbito y su red.

Nombre: 

Descripción:

< Atrás  Siguiente > Cancelar

En la siguiente ventana indicamos el rango de IP que serviremos. Yo usaré desde la 100 a la 200.

Asistente para ámbito nuevo

Intervalo de direcciones IP
 Para definir el intervalo de direcciones del ámbito debe identificar un conjunto de direcciones IP consecutivas.

Opciones de configuración del servidor DHCP
 Escriba el intervalo de direcciones que distribuye el ámbito.

Dirección IP inicial:
 Dirección IP final:

Opciones de configuración que se propagan al cliente DHCP

Longitud: 
 Máscara de subred:

< Atrás  Siguiente > Cancelar

Pasaremos algunas ventanas hasta llegar al "enrutador" o "puerta de enlace" donde añadiremos la IP acabada en 1, en mi caso la 192.168.100.1



Asistente para ámbito nuevo

Enrutador (puerta de enlace predeterminada)

Puede especificar los enrutadores, o puertas de enlace predeterminadas, que se distribuirán en el ámbito.

Para agregar una dirección IP para un enrutador usado por clientes, escriba la dirección.

Dirección IP:

<input type="text"/>	<input type="button" value="Agregar"/>
192.168.100.1	<input type="button" value="Quitar"/>
<input type="button" value="Arriba"/>	
<input type="button" value="Abajo"/>	

< Atrás Cancelar

La siguiente ventana del asistente tiene la información del DNS que ha detectado automáticamente y no es necesario hacer nada.

Asistente para ámbito nuevo

Nombre de dominio y servidores DNS

El Sistema de nombres de dominio (DNS) asigna y traduce los nombres de dominio que utilizan los clientes de la red.

Puede especificar el dominio primario que desea que los equipos clientes de su red usen para la resolución de nombres DNS.

Dominio primario:

Para configurar clientes de ámbito para usar servidores DNS en su red, escriba las direcciones IP para esos servidores.

Nombre de servidor:	Dirección IP:	<input type="button" value="Agregar"/>
<input type="text"/>	<input type="text" value="192.168.100.10"/>	<input type="button" value="Quitar"/>
<input type="button" value="Resolver"/>		<input type="button" value="Arriba"/>
		<input type="button" value="Abajo"/>

< Atrás Cancelar

Por último, activaremos el ámbito y lo probaremos con un equipo cliente.