Colección Certificaciones

Preparación para la certificación **MCSA**

Windows Server 2016

Gestión de las identidades

EXAMEN N°70-742

77 trabajos prácticos
155 preguntas-respuestas

GRATIS:
UN EXAMEN EN BLANCO en línea
con respuestas comentadas y detalladas

Armelin ASIMANE
Vahé TOULOUMIAN

eni

Windows Server 2016

MCSA 70-741 - Infraestructura de red

El examen **70-741 "Windows Server 2016 – Infraestructura de red"** es el segundo de los tres exámenes obligatorios para obtener la certificación **MCSA Windows Server 2016**. Valida sus competencias y conocimientos acerca de las funcionalidades de red disponibles en Windows Server 2016.

Para ayudarle a preparar eficazmente el examen, **este libro cubre todos los objetivos oficiales**, tanto desde el punto de vista teórico como desde un punto de vista práctico. Ha sido elaborado por formadores profesionales reconocidos, también consultores, certificados técnicamente y pedagógicamente por Microsoft. De este modo, la experiencia pedagógica y técnica de los autores le confieren un enfoque claro y visual, alcanzando un nivel técnico muy elevado.

Capítulo tras capítulo, podrá **validar sus conocimientos teóricos** gracias a la gran cantidad de **preguntas y respuestas incluidas (86 en total)** , poniendo de relieve tanto los elementos fundamentales como las características específicas de los distintos conceptos abordados.

Cada capítulo se completa con **trabajos prácticos (23 en total)** que le permitirá medir su autonomía. Estos ejercicios concretos, más allá incluso de los objetivos fijados por el examen, le permitirán forjarse una experiencia relevante y adquirir verdaderas competencias técnicas sobre situaciones reales.

A este dominio del producto y de los conceptos se le añade la preparación específica para el examen 70-741: en esta página podrá acceder **gratuitamente a 1 examen en blanco en línea**, destinado a entrenarle en condiciones próximas a las de la prueba. En este sitio web, cada pregunta que se plantea se inscribe en el espíritu de la certificación y, para cada una, las respuestas están lo suficientemente desarrolladas como para identificar y completar sus últimas lagunas.

Los capítulos del libro:

Jérôme BEZET-TORRES - Nicolas BONNET

Nicolas BONNET es Consultor y Formador en sistemas operativos de Microsoft desde hace varios años y cuenta con más de 10 años de experiencia en la administración de sistemas informáticos. Posee las certificaciones MCT (Microsoft Certified Trainer), MCSA (Windows 7, 8, 10, 2008, 2012 y Office 365) y es un reconocido Microsoft MVP (Most Valuable Professional) Windows and Devices for IT. Es miembro de las comunidades cmd (http://cmd.community) y aos (http://aos.community).
Jérôme BEZET-TORRES es Consultor y Formador en tecnologías de Sistemas y Redes sobre diversos entornos. Posee las certificaciones MCSA en Windows Server 2012 y Microsoft Certified Trainer (MCT).

Introducción

El examen **70-741 "Windows Server 2016 - Infraestructura de red"** es el segundo de los tres exámenes obligatorios para obtener la**certificación MCSA Windows Server 2016**. Valida sus competencias y conocimientos acerca de las funcionalidades de implementación de red disponibles en Windows Server 2016.

Para ayudarle a preparar eficazmente el examen, **este libro cubre todos los objetivos oficiales** (enumerados en un listado en el anexo) tanto desde el punto de vista teórico como desde un punto de vista práctico.

Cada capítulo se organiza de la siguiente manera:

- Una definición de los **objetivos a alcanzar**: permite exponer, con precisión, las competencias que se abordan en cada capítulo una vez se haya validado.
- Una sección de **formación teórica**: permite definir los términos y conceptos abordados y esquematizar, mediante un hilo conductor, los distintos puntos a asimilar.
- Una sección de **validación de conocimientos adquiridos**: propuesta bajo la forma de preguntas y respuestas (**86 en total**). Estas preguntas, y sus respuestas comentadas, ponen de relieve tanto los elementos fundamentales como las características específicas de los distintos conceptos abordados.
- **Trabajos prácticos** (**23 en total**): permiten ilustrar, con precisión, ciertas partes del curso y le darán también los medios necesarios para medir su autonomía. Estos ejercicios concretos, más allá incluso de los objetivos fijados por el examen, le permitirán forjarse una experiencia relevante y adquirir verdaderas competencias técnicas sobre situaciones reales.

A este dominio del producto y de los conceptos se le suma la preparación específica a la certificación: en el sitio web www.edieni.com **podrá acceder gratuitamente a 1 examen en blanco en línea**, destinado a entrenarse en condiciones similares a las de la prueba. En este sitio web cada pregunta que se plantea se inscribe en el espíritu de la certificación y, para cada una, las respuestas están lo suficientemente desarrolladas como para identificar y completar sus últimas lagunas.

Organización de las certificaciones

Los anteriores cursos de certificación permitían acceder a la certificación MCITP (*Microsoft Certified IT Professional*). Estos últimos han pasado a llamarse MCSA (*Microsoft Certified Solutions Associate*) y MCSE (*Microsoft Certified Solutions Expert*).

Certificación MCSA

La certificación MCSA se compone de tres certificaciones. La primera es la certificación 70-740, relativa a la instalación y la configuración del almacenamiento, así como la virtualización con Hyper-V y el servidor Nano. La segunda es la certificación 70-741, correspondiente a la red y Windows Server 2016, y por último la certificación 70-742 permite adquirir las competencias vinculadas a Active Directory, los certificados y la protección de los datos. Hay que superar estas tres certificaciones para obtener el título de MCSA Windows Server 2016. Por último, aquellas personas que ya posean el título de MCSA Windows Server 2008 o MCSA Windows Server 2012, basta con que superen la certificación 70-443, que es la actualización de competencias a Windows Server 2016.

MCSE Cloud Platform and Infrastructure

La certificación MCSE (*Microsoft Certified Solutions Expert*) Cloud Platform and Infrastructure garantiza que puede dirigir un centro de datos altamente eficaz y moderno y que dispone de la experiencia necesaria en los siguientes dominios: tecnologías cloud, administración de las identidades, administración de los sistemas, virtualización, almacenamiento e implementación de la red.

Obtener una certificación **MCSE: Cloud Platform and Infrastructure** le permite optar a puestos de administrador cloud, de arquitecto cloud, de especialista en consultoría informática y de analista en seguridad de la información.

Esta certificación **MCSE** no caduca y no necesita ninguna renovación. Sin embargo, cada año tiene la opción de validar de nuevo la certificación y recibir un resultado suplementario en su expediente de resultados. Para ello, debe superar un examen único de entre una lista de opciones, para demostrar su implicación en la ampliación o la profundización de sus competencias en un sector específico de la tecnología.

Para obtener la certificación MCSE hay que ser previamente **MCSA Server 2016** o **MCSA Cloud Plaform** o **MCSA Linux on Azure** o **MCSA Server 2012** y a continuación superar uno de los siguientes exámenes:

- **Developing Microsoft Azure Solutions**: examen 70-532
- **Implementing Microsoft Azure Infrastructure Solutions**: examen 70-533
- **Architecting Microsoft Azure Solutions**: examen 70-534
- **Designing and Implementing Cloud Data Platform Solutions**: examen 70-473
- **Designing and Implementing Big Data Analytics Solutions**: examen 70-475
- **Securing Windows Server 2016**: examen 70-744
- **Designing and Implementing a Server Infrastructure**: examen 70-413
- **Implementing an Advanced Server Infrastructure**: examen 70-414
- **Monitoring and Operating a Private Cloud**: examen 70-246
- **Configuring and Deploying a Private Cloud**: examen 70-247

Cómo se organiza este libro

Este libro le prepara para el examen **70-741 - La red con Windows Server 2016**. Este libro se estructura en varios capítulos que le aportarán los conocimientos teóricos necesarios sobre cada área de conocimiento. A continuación, se proponen al lector los trabajos prácticos, que le permitirán poner en práctica los puntos abordados en la parte teórica.

Es preferible, por tanto, seguir los capítulos en orden. En efecto, éstos conducen de manera progresiva al lector por las competencias necesarias para superar el examen. Al finalizar cada capítulo, se proponen una serie de preguntas que le permitirán validar el nivel que debe alcanzarse. Si lo supera, el lector puede pasar al siguiente capítulo.

Se invita al lector a crear la maqueta, que sirve para la realización de los trabajos prácticos. Esta maqueta se compone de servidores que ejecutan Windows Server Windows Server 2016 Standard y equipos clientes con Windows 10 Enterprise.

La configuración de los roles se realiza conforme se avanza en los capítulos. El primer capítulo sobre el direccionamiento IP permite obtener los conocimientos necesarios para planificar e implementar el direccionamiento. Se estudian las direcciones IPv4 e IPv6, las herramientas dedicadas a la configuración y también aquellas utilizadas para resolver problemas. La configuración se realizará con Windows PowerShell y con Netsh. Por último, se presentan los mecanismos de transición y de comunicación entre redes IPv4 e IPv6.

A continuación, se estudian los servidores DNS y DHCP, mediante el análisis de las distintas zonas y registros, así como las nociones de transferencia de zona y de borrado de los datos. Los talleres prácticos permiten comprender el despliegue y la configuración de DNS con el servidor Nano. Se invita al lector, tras hablar de DHCP, a implementar IPAM, funcionalidad aparecida con Windows Server 2012 y que permite administrar los planes de direccionamiento IP de la empresa.

Los dos capítulos siguientes abordan los servicios de red. El lector podrá estudiar así las distintas soluciones de VPN (*DirectAccess* o VPN clásica) y su implementación en los talleres prácticos. Por último, se estudiará una parte correspondiente a la optimización de los servidores de archivos con la implementación de DFS (espacio de nombres, escenario DFS, replicación DFS-R) y de BranchCache para garantizar la seguridad de los datos y su acceso.

El último capítulo presenta funcionalidades de red avanzadas y su integración con el hipervisor Microsoft Hyper-V. Se aborda la virtualización de redes con el Network Controller, que constituye el elemento central de la administración de una infraestructura de red física o virtual. Se aborda también la virtualización de redes con el estudio del Software Defined Networking.

Competencias probadas tras el examen 70-741

Puede encontrar, al final del libro, la tabla resumen de competencias probadas.

1. El examen de certificación

El examen de certificación se compone de varias preguntas. Para cada una de ellas se proponen varias respuestas. Es necesario marcar una o varias de estas respuestas. Para superar el examen es preciso obtener una puntuación de 700.

El examen se realiza en un centro homologado Pearsonvue, no obstante la inscripción debe realizarse en el sitio web www.prometric.com. Se presentan varios sitios en la región, es necesario, una vez seleccionado el examen deseado (70-741), seleccionar el centro así como la fecha y la hora del encuentro.

El día D dispondrá de varias horas para responder a las preguntas. No dude en tomarse el tiempo necesario para leer bien la pregunta y todas las respuestas. Es posible marcar las preguntas para realizar una relectura antes de finalizar el examen. El resultado se obtiene al finalizar el examen.

2. Preparación del examen

Para preparar el examen de forma óptima es necesario, en primer lugar, disponer de tiempo para leer los distintos capítulos y, a continuación, trabajar en los trabajos prácticos.

Las preguntas disponibles al finalizar cada módulo le permiten validar sus conocimientos. No pase al siguiente capítulo sin haber comprendido bien el anterior, y vuelva a trabajarlo tantas veces como sea necesario. Con el libro se ofrece un examen en blanco que le permitirá poner a prueba sus conocimientos antes de realizar el examen.

Las máquinas virtuales utilizadas

Para poder realizar los trabajos prácticos y para evitar multiplicar el número de máquinas se utiliza un sistema de virtualización. El capítulo presenta, por ello, la instalación de una maqueta. Esta última utiliza el hipervisor de Microsoft (Hyper-V). También puede, si lo desea, utilizar su propio sistema de virtualización.

A continuación se instalan varias máquinas virtuales que ejecutan Windows Server 2016 o Windows 10.

Es posible descargar las versiones de evaluación de estos productos en los siguientes enlaces:

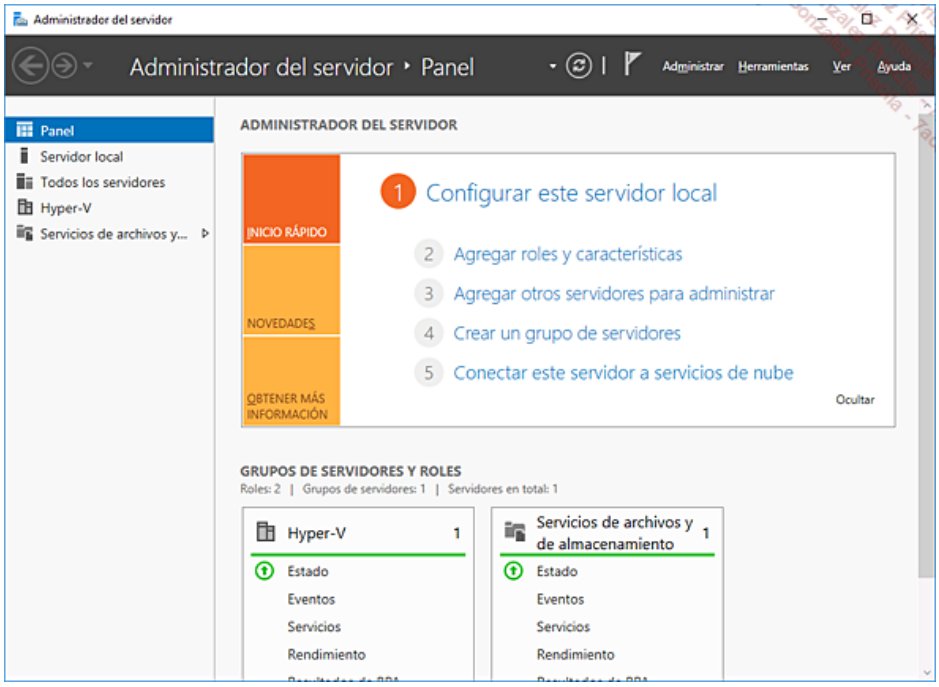
Windows 10: https://www.microsoft.com/es-es/evalcenter/evaluate-windows-10-enterprise

Windows Server 2016: https://www.microsoft.com/es-es/evalcenter/evaluate-windows-server-2016

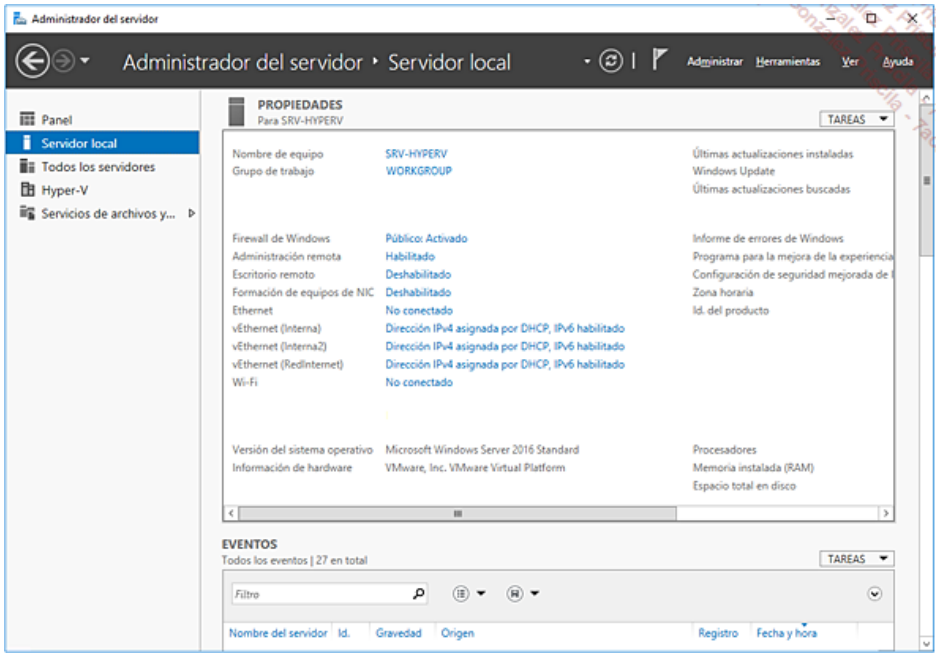
El administrador del servidor

La consola **Administrador del servidor** permite administrar el conjunto del servidor. Presente desde Windows Server 2008 se produjo, con Windows Server 2012, un cambio importante.

Permite agregar/eliminar roles, y también la administración de equipos remotos: es posible, con ayuda de **WinRM**, instalar roles y características. También es posible configurar un conjunto de servidores para administrarlos mediante esta consola.

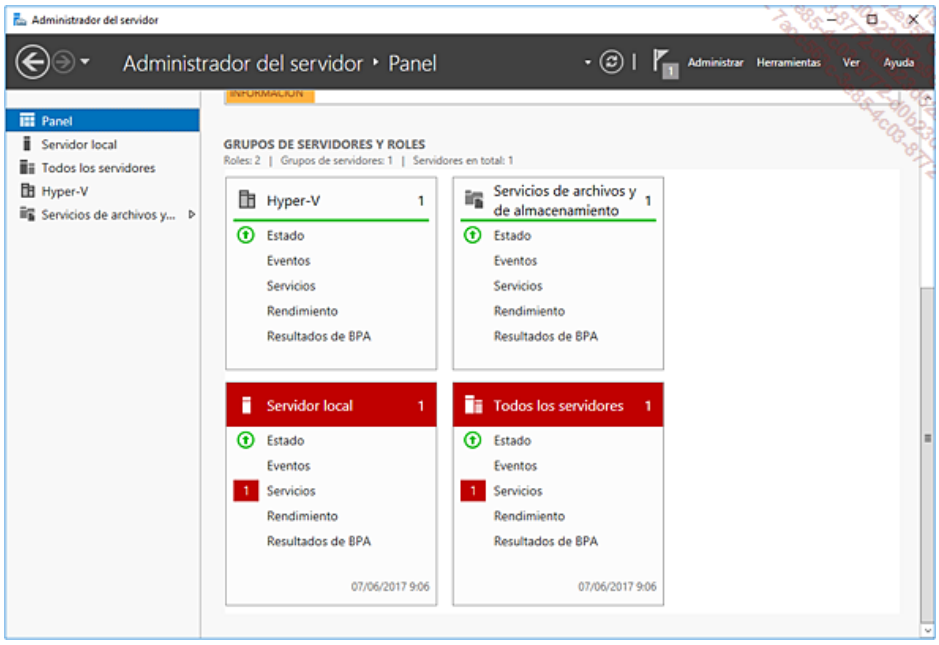


La gestión del servidor local se lleva a cabo, también, mediante esta consola. Es posible modificar cierta información muy rápidamente, como por ejemplo el nombre del equipo, el grupo de trabajo o el dominio al que pertenece. La configuración del escritorio remoto, o la gestión remota, también son configurables.



La propiedad **Configuración de seguridad mejorada de Internet Explorer** permite activar o desactivar la seguridad mejorada de Internet Explorer. Por defecto, esta opción está activa.

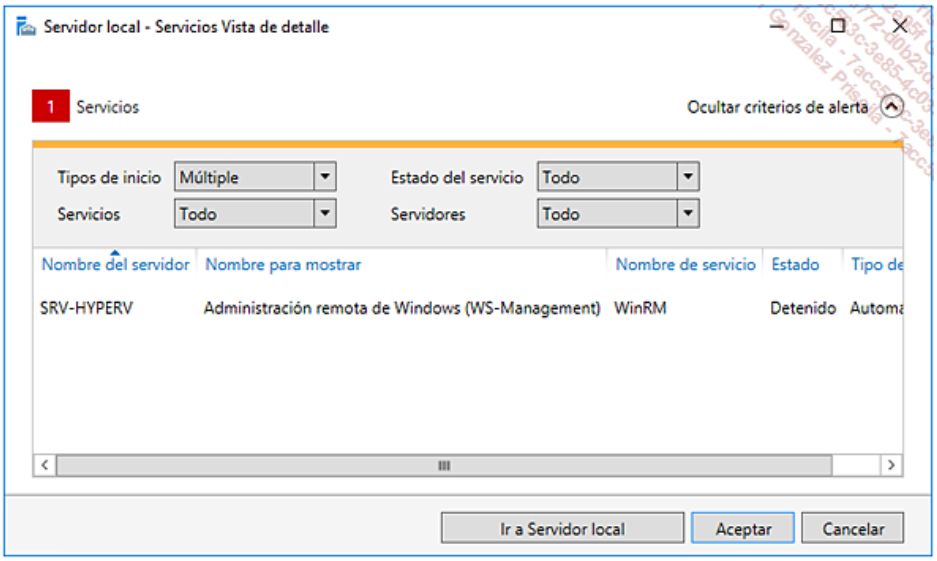
El **Panel** permite, también, asegurar rápidamente que no existe ningún problema en el servidor.



De este modo, es posible ver en la captura de pantalla anterior que los roles **Hyper-V** y **Servicios de archivos y de almacenamiento** funcionan correctamente.

Se auditan varios elementos: **Eventos**, **Servicios**, **Rendimiento** y **Resultados de BPA**. Servicios está precedido por una cifra, lo que indica al administrador que algún servicio tiene un error, está detenido…

Haciendo clic en **Servicios** se abre una ventana que muestra los detalles del servicio afectado.

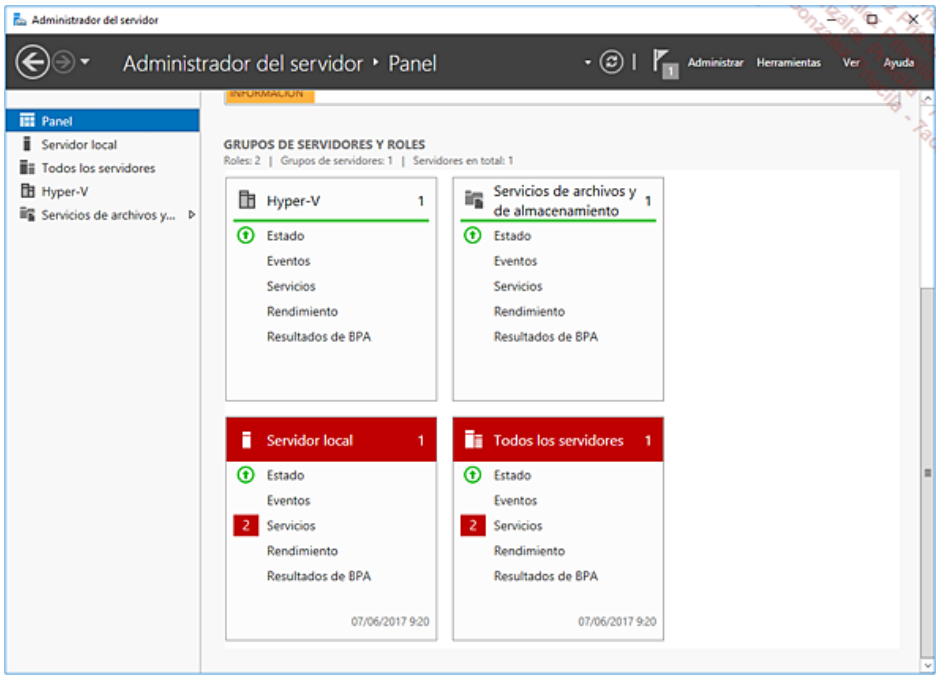


Detengamos el servicio de spooler ejecutando el comando `net stop spooler`.

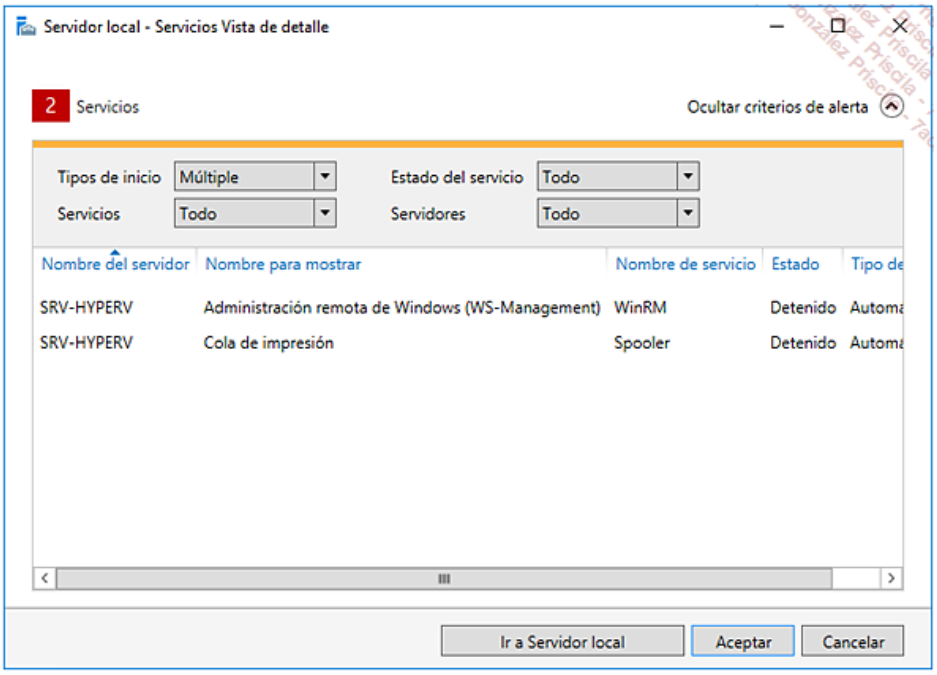
La detención del servicio spooler provocará la creación de un nuevo evento.

Volviendo a la consola **Administrador del servidor**, se ejecuta un nuevo análisis. También es posible actualizar la consola para ver el cambio.

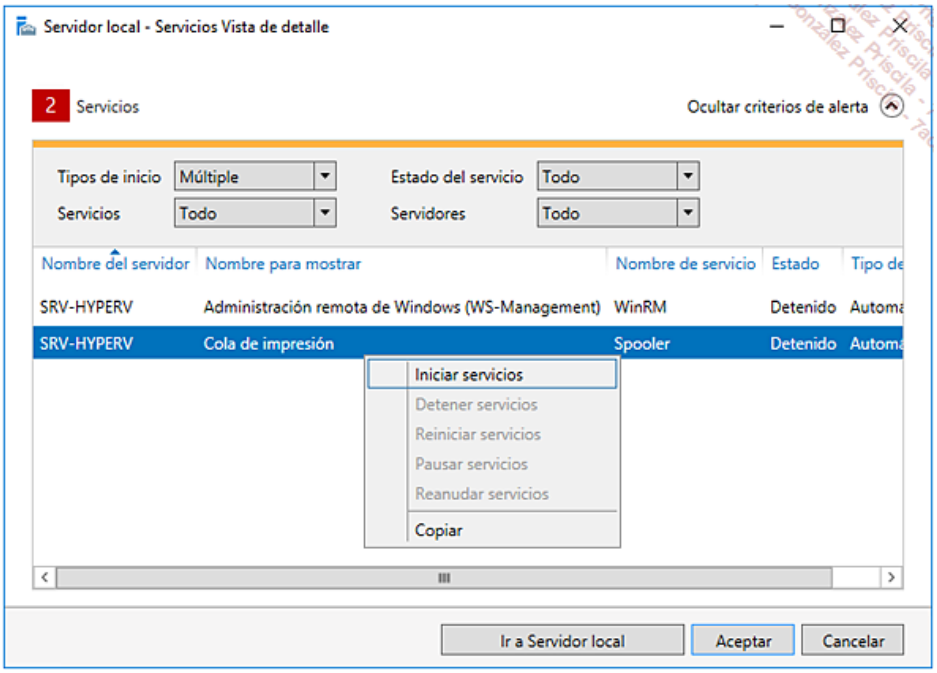
La consola le indica, ahora, que existen problemas sobre dos servicios.

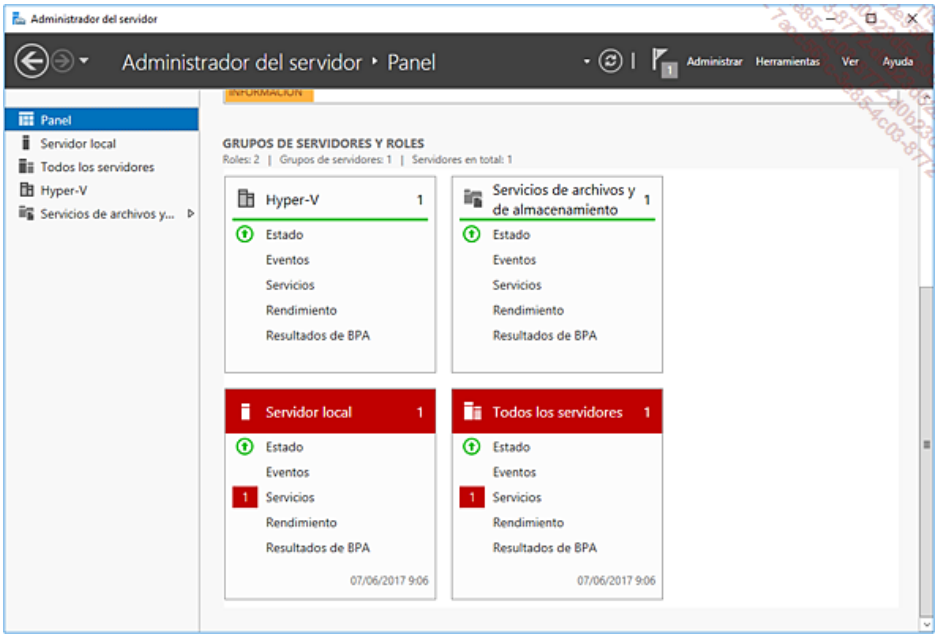


Se abre una nueva ventana indicando el o los servicios que presentan problemas, haciendo clic en el vínculo **Servicios**.



Es posible iniciar el o los servicios deseados haciendo clic con el botón derecho en la fila correspondiente al servicio que presenta el problema y, a continuación, seleccionando la opción **Iniciar servicios**. Actualizando la consola **Administrador del servidor** comprobará que el problema relativo al spooler ha desaparecido.



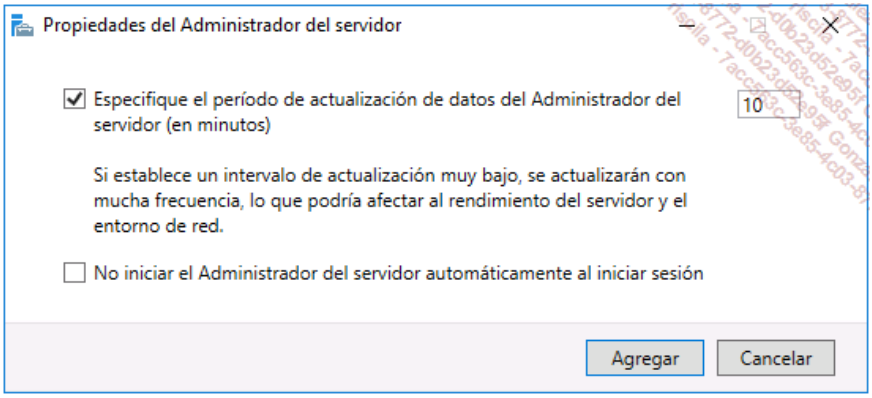


El problema del servicio desaparece. Es posible realizar la misma operación para los servicios remotos. Es, no obstante, obligatorio crear un grupo que incluya estos servidores (este punto se aborda más adelante en este capítulo).

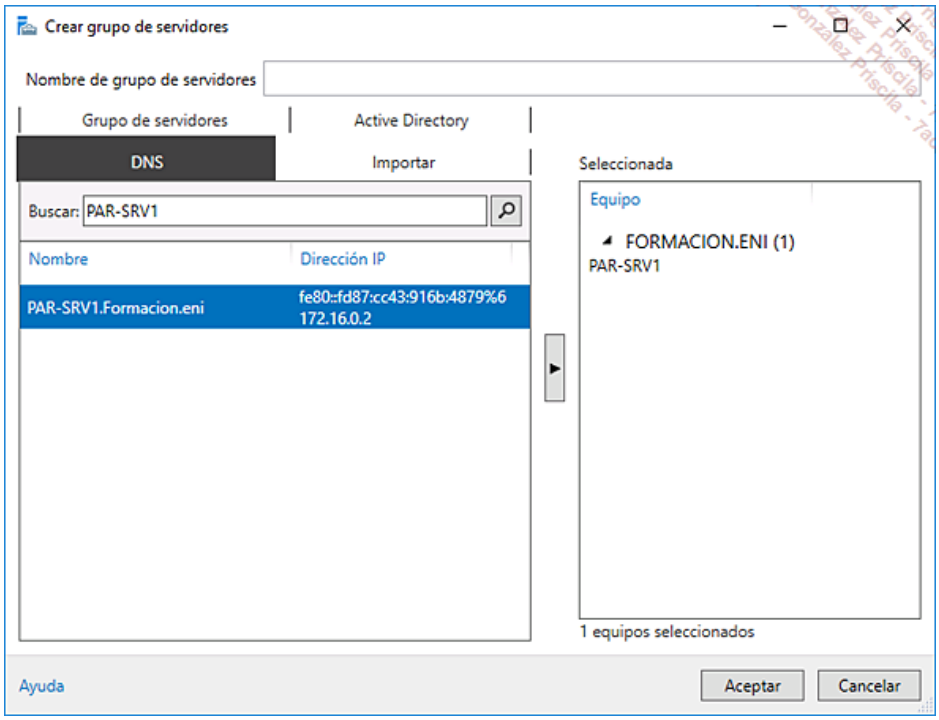
El menú **Herramientas** permite acceder a un conjunto de consolas (Administración de equipos, Servicios, Firewall de Windows con seguridad avanzada…) y de herramientas (Diagnóstico de memoria de Windows, Windows PowerShell…).

Haciendo clic en **Administrar** aparece un menú contextual que permite acceder a un conjunto de opciones:

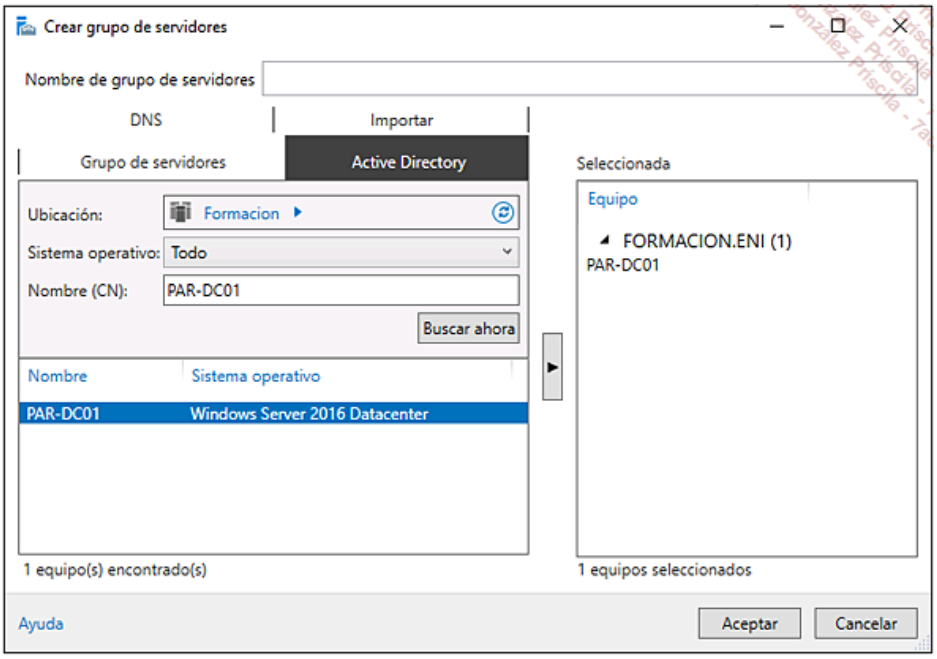
- **Propiedades del Administrador del servidor**: es posible especificar el período de actualización de los datos del Administrador del servidor. Por defecto, el valor está configurado a 10 minutos. El Administrador del servidor puede configurarse para que no se ejecute automáticamente tras iniciar sesión.



- **Crear grupo de servidores**: con el objetivo de poder administrar varios servidores desde esta máquina, conviene crear un grupo de servidores. Es posible agregar/quitar roles o, simplemente, supervisarlos. Es posible agregar servidores escribiendo su nombre o una dirección IP en la pestaña **DNS**.



Es posible realizar la búsqueda del puesto con ayuda de Active Directory, seleccionando la ubicación (raíz del dominio, unidad organizativa…) y, a continuación, seleccionando el nombre de la máquina.



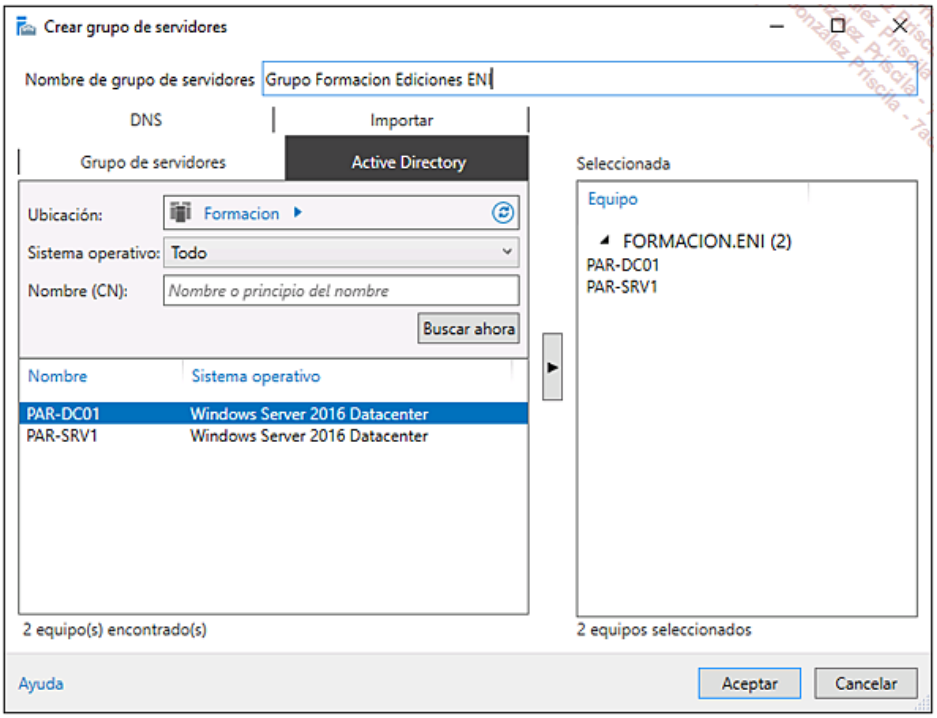
- **Agregar/Quitar roles y características**: las operaciones para agregar o quitar roles pueden realizarse sobre el servidor local o sobre una máquina remota. Se utiliza el protocolo WinRM para llevar a cabo esta acción.

Cuando se agrega un nuevo rol aparece un nodo en la columna izquierda. Haciendo clic sobre él, el panel central da acceso a las propiedades y eventos del rol.

1. Creación de un grupo de servidores

Como hemos podido ver, la creación de un grupo nos permite realizar la administración de manera remota.

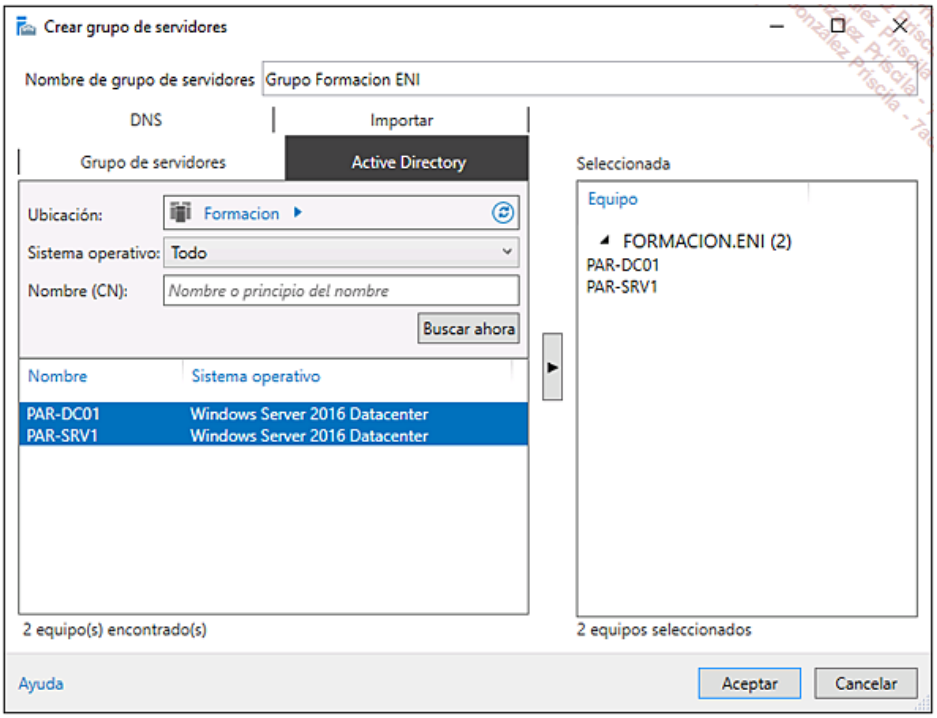
Esto se realiza desde la consola **Administrador del servidor**. El menú **Administrar** permite llevar a cabo esta operación (seleccione la opción**Crear grupo de servidores**). En la etapa de creación es necesario asignar un nombre al grupo mediante el campo **Nombre de grupo de servidores**.



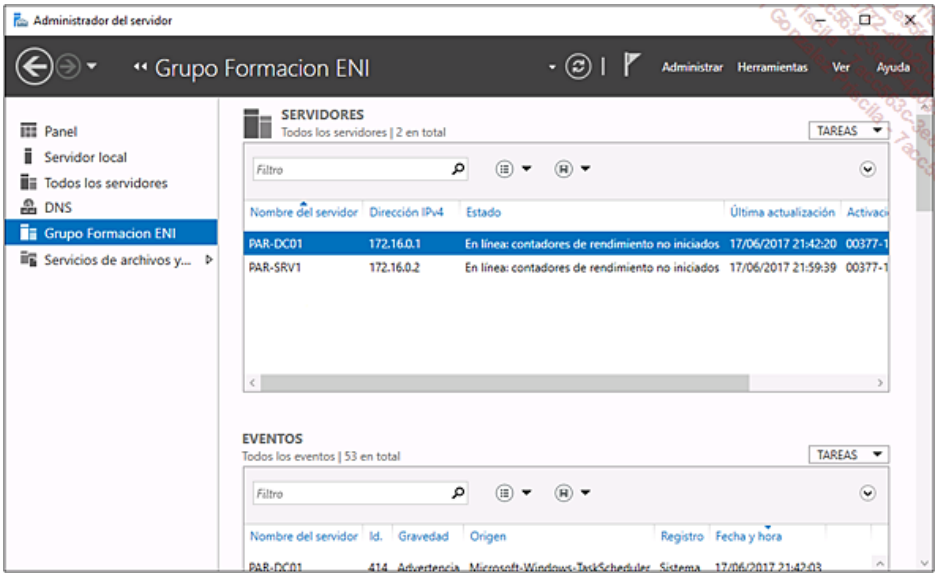
A continuación, basta con agregar los servidores con ayuda de las distintas pestañas. La pestaña **Active Directory** da acceso a una lista desplegable **Sistema operativo**. Permite filtrar sobre un tipo de sistema concreto (por ejemplo: Windows Server 2012 R2 o 2016 / Windows 8 y Windows 10).

Basta, entonces, con hacer clic en el botón **Buscar ahora**, seleccionar los servidores deseados (AD1, AD2…) y, a continuación, incluirlos en el

grupo mediante el botón ubicado entre los campos de selección y el campo **Seleccionada**.



El nuevo grupo está disponible en la consola Administrador del servidor.

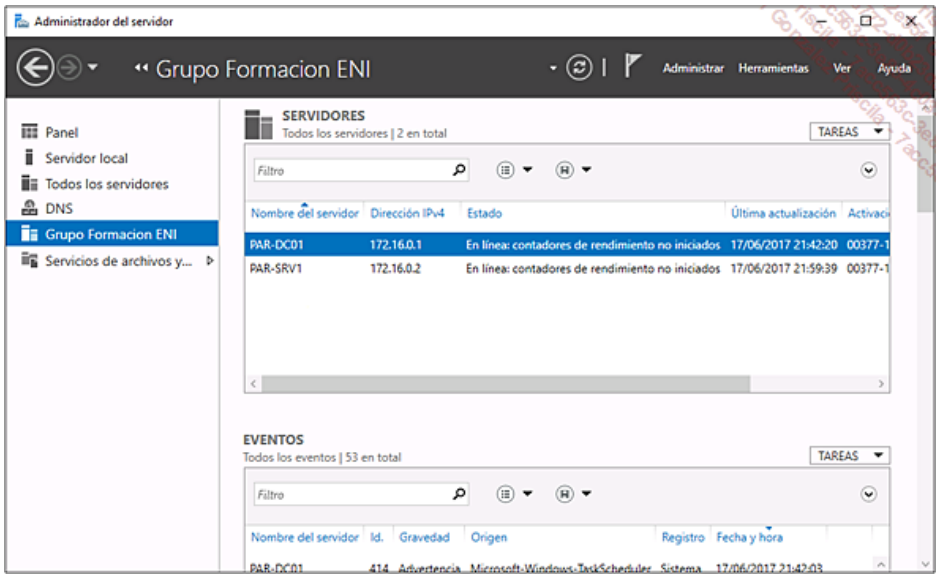


Este grupo permite recuperar el estado de salud de los puestos.

2. Instalación remota de un rol

Se ha creado el grupo en un servidor, vamos, a continuación, a utilizarlo para instalar el rol Servidor de fax en un servidor remoto. En la consola, es necesario hacer clic en el vínculo **Agregar roles y características**.

En la ventana de selección del servidor de destino es posible seleccionar el servidor sobre el que se quiere realizar la instalación.

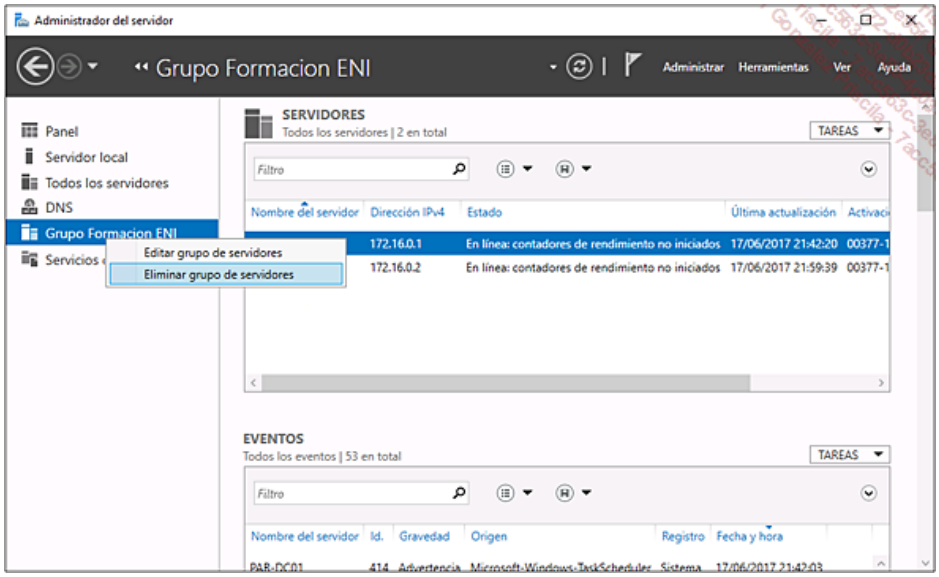


A continuación, seleccione el rol que desea instalar y continúe con la instalación.

3. Eliminar un grupo de servidores

La eliminación de un grupo de servidores se opera de manera tan sencilla como su creación. La operación se realiza desde la consola Administrador del servidor.

Haciendo clic con el botón derecho sobre el grupo afectado, aparece la opción **Eliminar grupo de servidores** disponible.



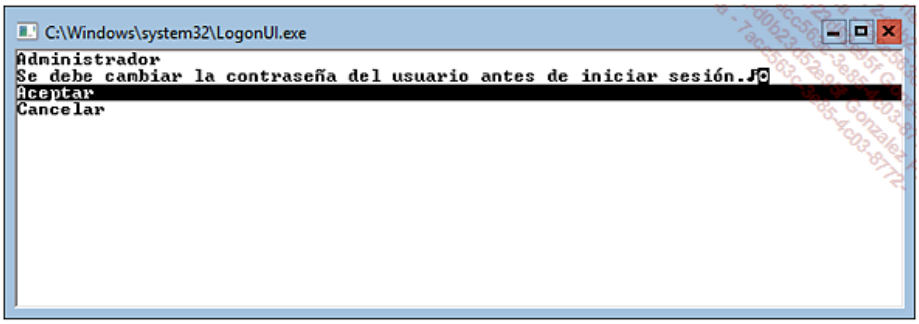
A pesar de eliminar el grupo, los puestos siguen estando presentes en la sección **Todos los servidores**.

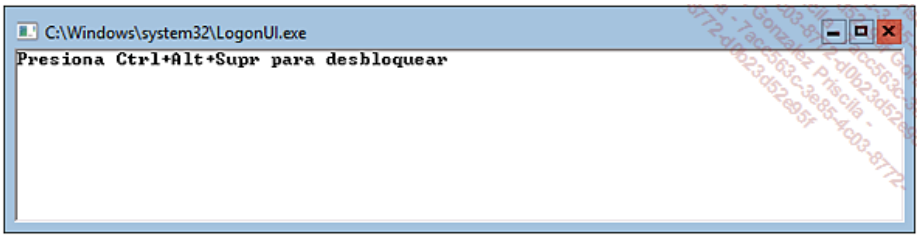
Es preciso eliminarlos manualmente haciendo clic con el botón derecho sobre la fila del servidor afectado.

Servidor en modo instalación mínima

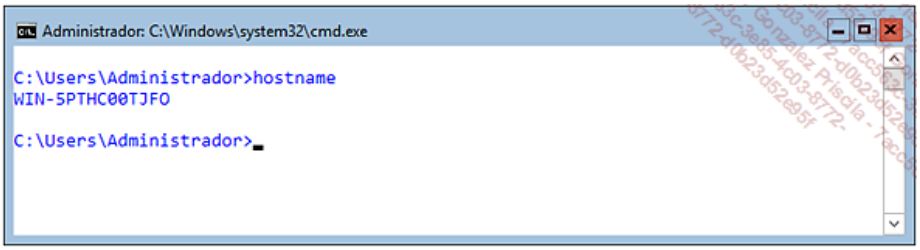
Cuando se instala un servidor en modo **Instalación mínima** o modo **Core**, el programa **explorer.exe** no se encuentra instalado. Sólo está presente la ventana de comandos.

En la versión Core de Windows Server 2016 ya no existe la posibilidad de agregar la interfaz gráfica, de modo que la ventana de login difiere si la comparamos con la ventana de inicio de sesión de Windows Server 2012 R2 Core.





La administración del servidor se realiza mediante comandos DOS. Escribiendo el comando `hostname` es posible obtener el nombre genérico asignado al servidor. Durante la instalación, dado que no se provee el nombre, se le asignará un nombre generado aleatoriamente.



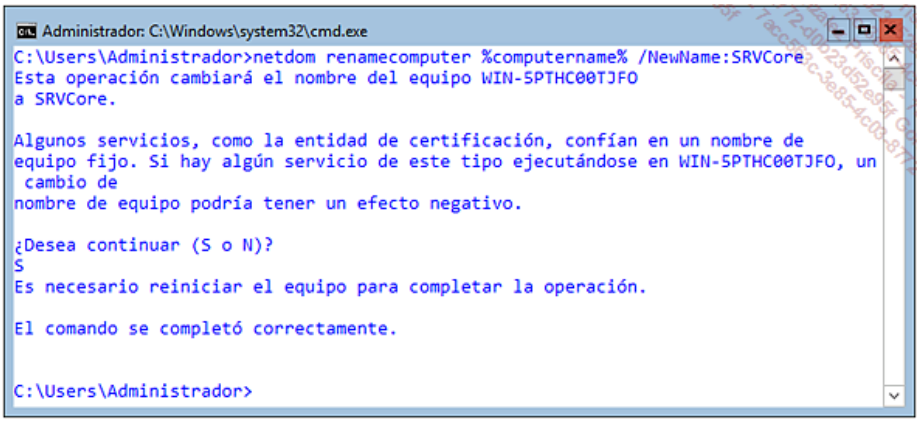
Para cambiar el nombre, es posible utilizar la herramienta **sconfig** (véase más adelante en este mismo capítulo) o el comando `netdom`.

La sintaxis del comando `netdom` es la siguiente:

```
netdom renamecomputer NombreActual /NewName:SRVCore
```

`NombreActual` puede remplazarse por `%computername%`.

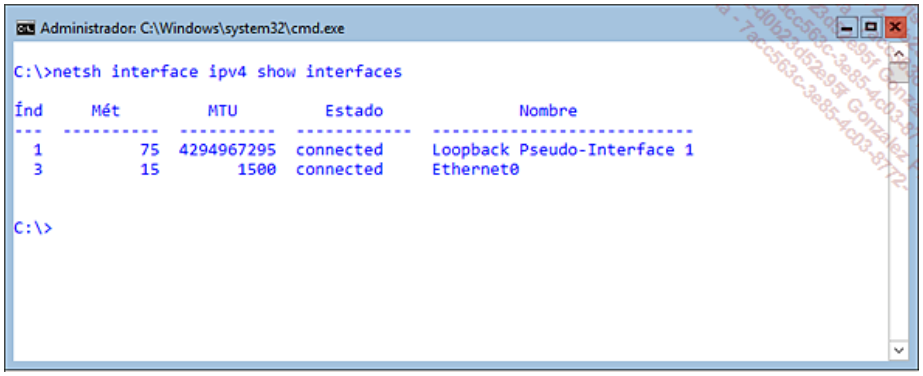
Es necesaria una validación, para ello basta con presionar la tecla **S** y, a continuación, la tecla [Enter].



Para hacer efectivo el nombre, el servidor debe reiniciarse. Para realizar esta operación puede ejecutar el comando `shutdown -r -t 0`.

La opción `-r` permite reiniciar el servidor, `-t 0` indica que se desea un reinicio inmediato.

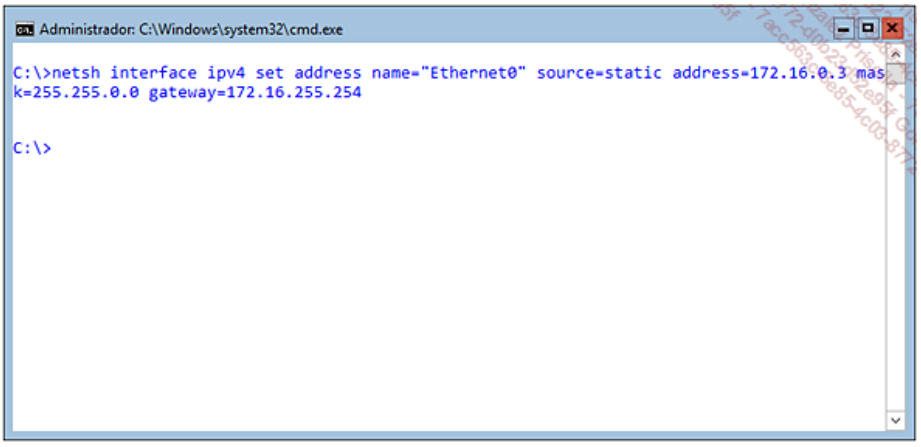
Antes de configurar la tarjeta de red es preciso recuperar su nombre. Para realizar esta operación puede utilizar el comando `netsh interface ipv4 show interfaces`.



El nombre de la tarjeta de red es Ethernet0, el comando que permite configurar la interfaz es:

```
netsh interface ipv4 set address name="NombreTarjeta" source=static
address=172.16.0.3 mask=255.255.0.0 gateway=172.16.255.254
```

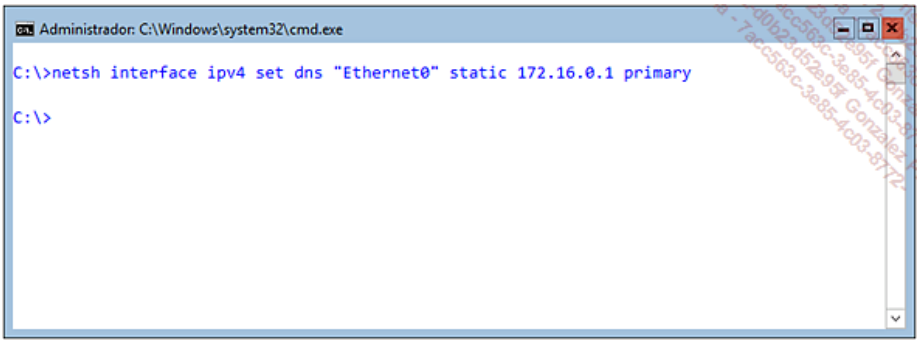
Remplace `NombreTarjeta` por el verdadero nombre de la tarjeta de red, `Ethernet0` en este caso.



Ha configurado la tarjeta, aunque la dirección del servidor DNS no se ha informado. El comando `netsh` permite agregar el servidor DNS:

```
netsh interface ip set dns "NombreTarjeta" static 172.16.0.1 primary
```

Remplace `NombreTarjeta` por el verdadero nombre de la tarjeta de red, `Ethernet0` en nuestro caso.

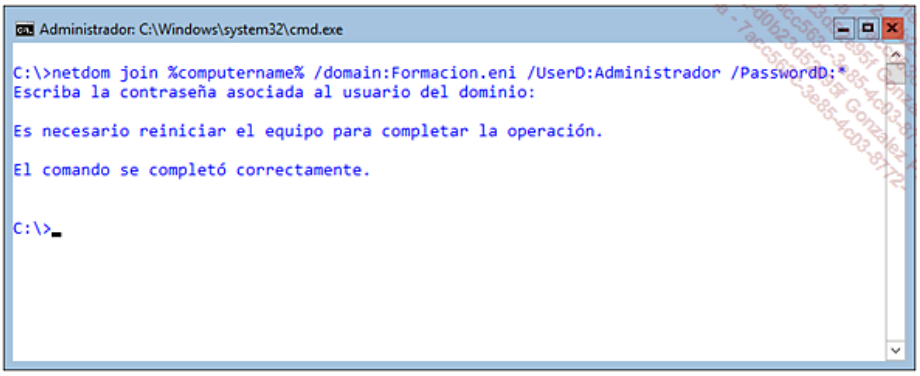


El comando `ipconfig /all` permite verificar la correcta configuración del puesto.

A continuación es posible unir el servidor al dominio Active Directory, para ello conviene utilizar el siguiente comando:

```
netdom join %computerName% /domain:Formacion.eni/UserD:Administrador
/passwordD:*
```

Debe informarse la contraseña, puesto que se ha pasado un asterisco en la opción `/passwordD`. Cuando la informe, no se mostrará ningún carácter.



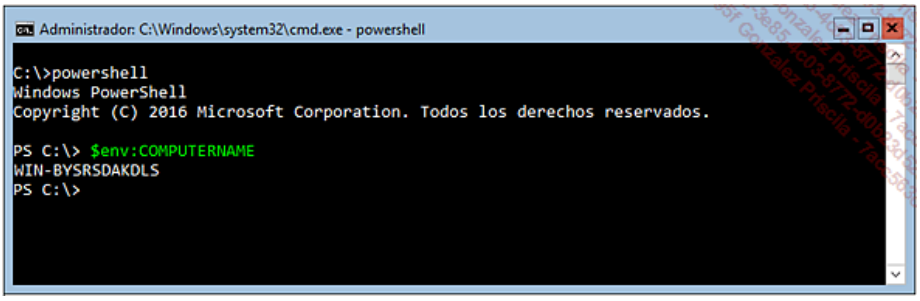
La última etapa consiste en reiniciar el servidor con el objetivo de aplicar la configuración y unirlo al dominio.

Continuando con la configuración de nuestro servidor, vamos a desactivar a continuación el firewall. Una vez más, el comando `netsh` nos permite realizar esta acción:

```
netsh firewall set opmode disable
```

La configuración del servidor Core también puede realizarse en su totalidad con PowerShell.

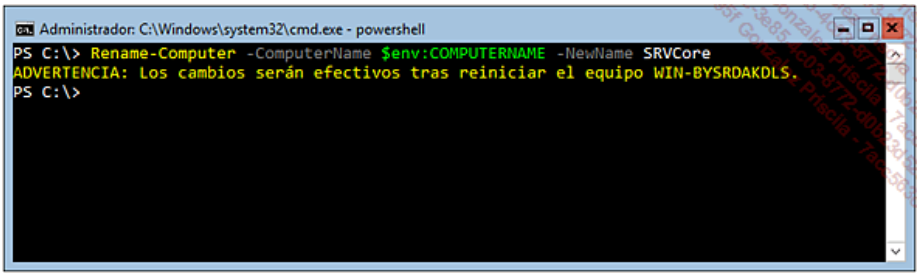
En primer lugar, hay que ejecutar desde una consola de comandos el comando `powershell.exe`. Para encontrar el nombre de la máquina, se utiliza una variable de entorno `$ENV:COMPUTERNAME`.



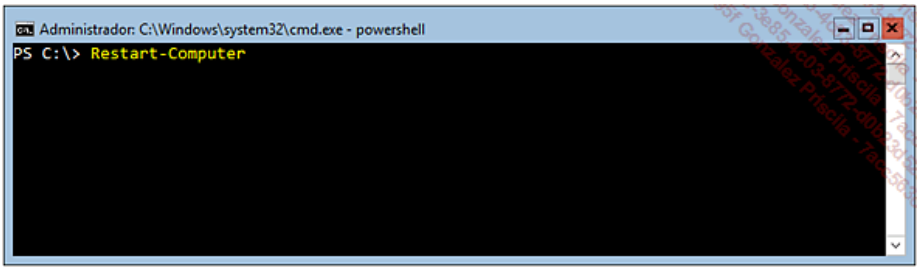
Para renombrar el servidor utilizaremos el comando:

```
Rename-Computer -ComputerName $env:COMPUTERNAME -NewName SRVCore
```

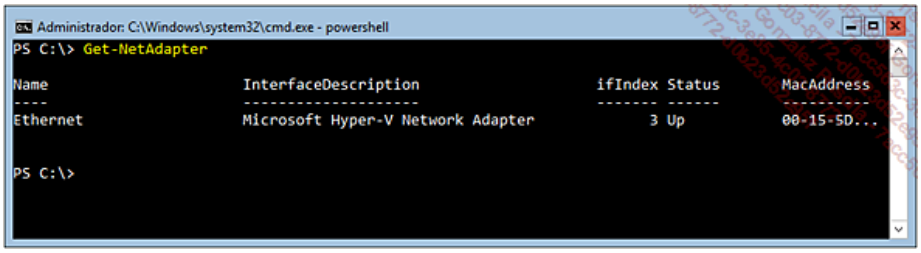
En lugar de la variable de entorno `$env:COMPUTERNAME`, puede utilizarse el nombre de la máquina.



Por último, para que el nombre sea efectivo, el servidor debe reiniciarse. Para realizar esta operación debe ejecutarse el comando `Restart-Computer`.

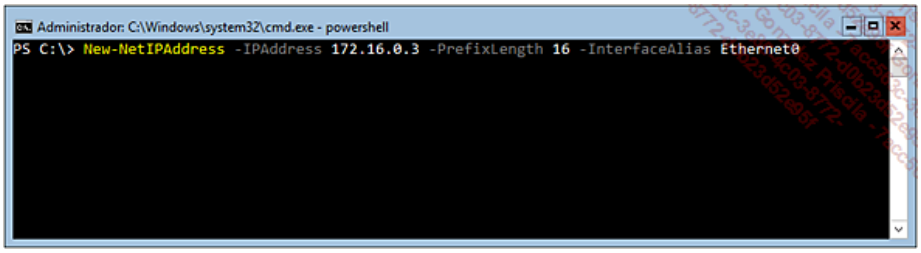


Antes de configurar la tarjeta de red, es preciso recuperar su nombre. Para realizar esta operación puede utilizarse el comando `get-NetAdapter`.



El nombre de la tarjeta de red es Ethernet0, el comando que permite realizar la configuración de la interfaz es:

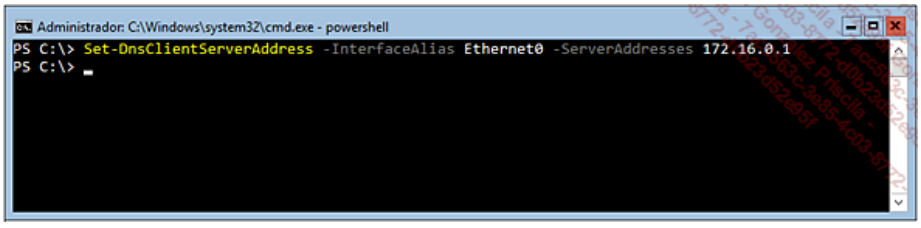
```
New-NetIPAddress -IPAddress 172.16.0.3 -PrefixLength 16 -InterfaceAlias
Ethernet0
```



Se ha configurado la tarjeta, pero la dirección del servidor DNS no se ha informado. Para ello, utilice el comando:

```
Set-DnsClientServerAddress -InterfaceAlias Ethernet0 -ServerAddresses
172.16.0.1
```

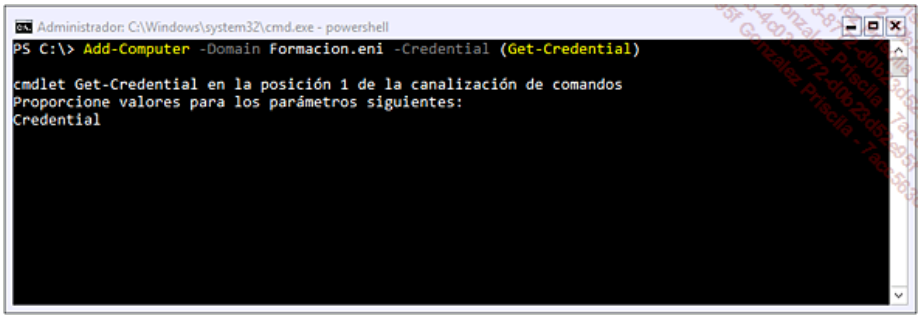
Si desea agregar varios servidores DNS, utilice la siguiente sintaxis ("172.16.0.1","172.16.0.33").

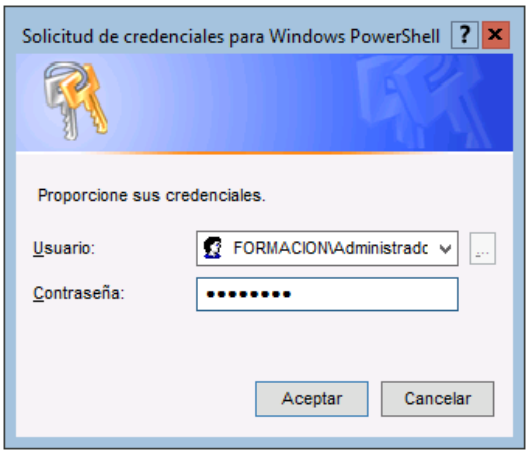


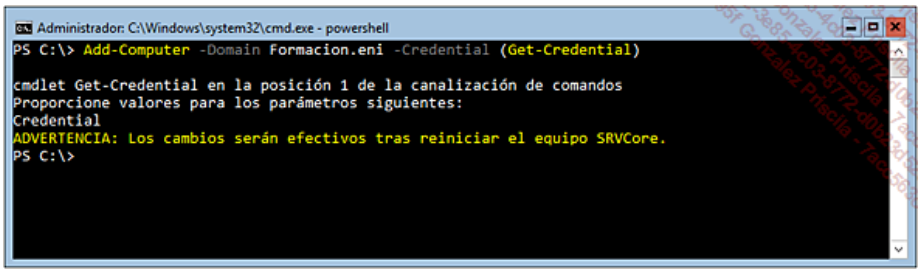
A continuación es posible unir el servidor al dominio; para ello conviene utilizar el comando:

```
Add-Computer -Domain Formacion.eni -Credential (Get-Credential)
```

El hecho de utilizar el comando `Get-Credential` abre una ventana de autenticación.







La última etapa es el reinicio para tener en cuenta la unión al dominio.

Continuaremos con la configuración de nuestro servidor deshabilitando el cortafuegos. Necesitaremos para ello dos comandos PowerShell.

```
Get-NetFirewallProfile | Set-NetFirewallProfile -Enabled False
```

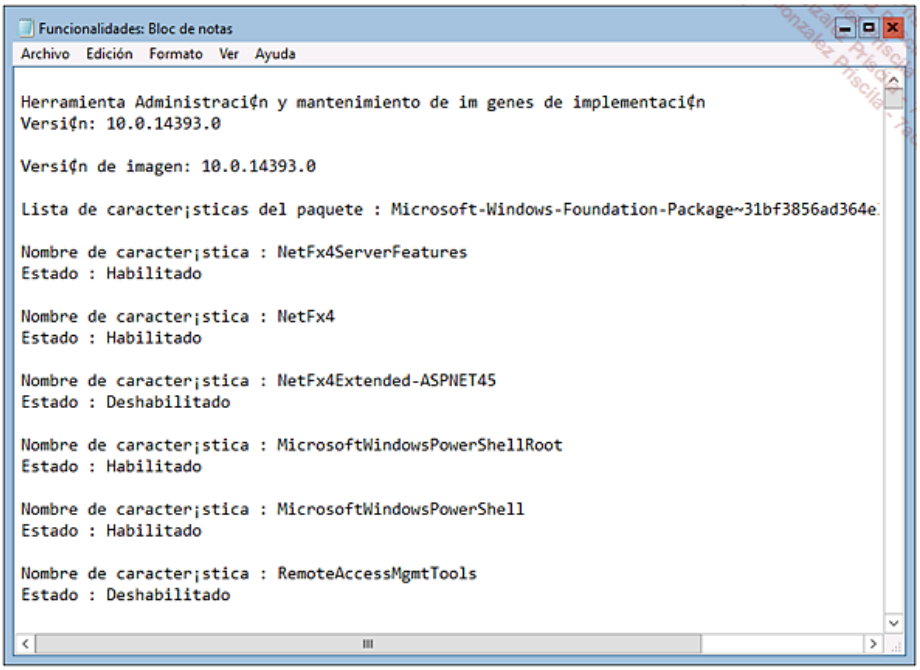
1. Instalación de roles con una instalación en modo Core

El servidor no posee una interfaz gráfica, por lo que la instalación debe realizarse por línea de comandos. Vamos a utilizar el comando `dism`para enumerar, habilitar o eliminar cualquier funcionalidad del sistema operativo.

Para enumerar la lista de roles y características es preciso utilizar el comando `dism`:

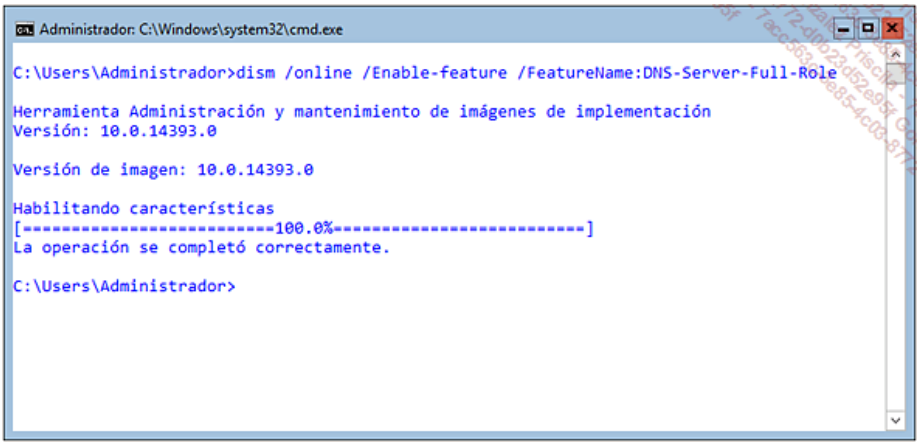
```
dism /online /get-features | Out-file - PsPath 'C:\Caracteristicas.txt'
```

Las características disponibles en el sistema operativo en ejecución (opción `/online`) se enumeran (`/get-features`). El resultado se escribe en el archivo Caracteristicas.txt.



El archivo muestra el nombre de cada funcionalidad y su estado. Para agregar el rol o la característica es preciso utilizar el comando `dism`. Antes de cualquier intento de instalación, debe recuperarse el nombre de la funcionalidad concreta. Por ejemplo, para DNS, el nombre es `DNS-Server-Full-Role`.

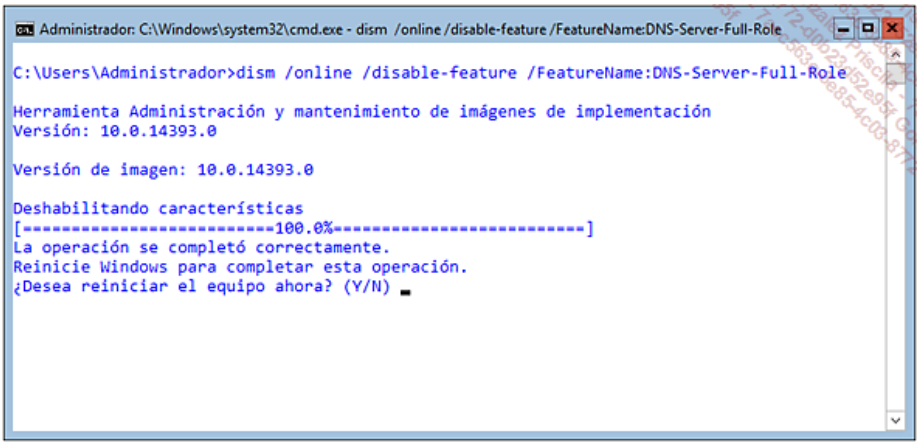
Ejecutando el comando `dism /online /Enable-Feature /FeatureName:DNS-Server-Full-Role` en una ventana de comandos DOS es posible realizar su instalación.



Ahora es posible administrar el rol desde un servidor que posea interfaz gráfica. En el caso de que el firewall esté habilitado, piense en que debe autorizar la administración remota.

Por último, `dism` puede, a su vez, eliminar una funcionalidad. Para realizar esta operación debe ejecutar el siguiente comando:

```
dism /online /disable-feature /FeatureName:DNS-Server-Full-Role
```



Se elimina el rol del servidor y se le invita a reiniciar el equipo para que tengan efecto las modificaciones.

2. Configuración con sconfig

Un servidor Core no posee interfaz gráfica, por lo que la configuración debe realizarse por línea de comandos. El comando `sconfig`, presente en las instalaciones mínimas, evita al administrador tener que introducir los distintos comandos utilizados para configurar el nombre del servidor o la configuración IP.

Es posible realizar más operaciones:

- Configuración del grupo de trabajo o de la unión a un dominio Active Directory.
- Cambio del nombre de equipo.
- Agregar una cuenta de administrador local.
- Descargar e instalar las actualizaciones de Windows Update.
- Configuración de la fecha y la zona horaria.
- Desconexión, parada y reinicio del servidor.

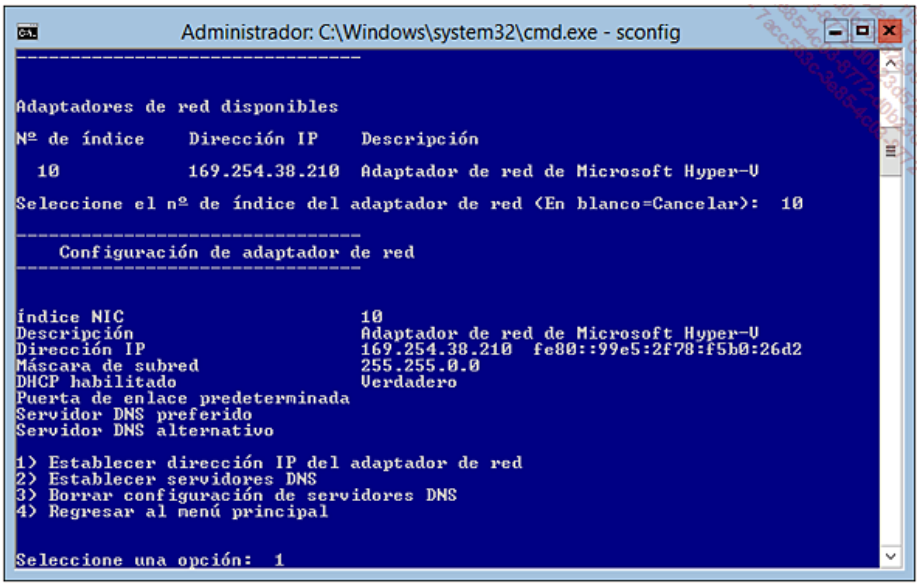
Para acceder a la interfaz basta con ejecutar el comando `sconfig` en una ventana de comandos DOS.

Para seleccionar la zona horaria debe seleccionar la opción número 9. Para ello, escriba 9 y, a continuación, presione la tecla [Enter]. Podrá modificar la zona horaria así como la fecha y la hora del servidor.

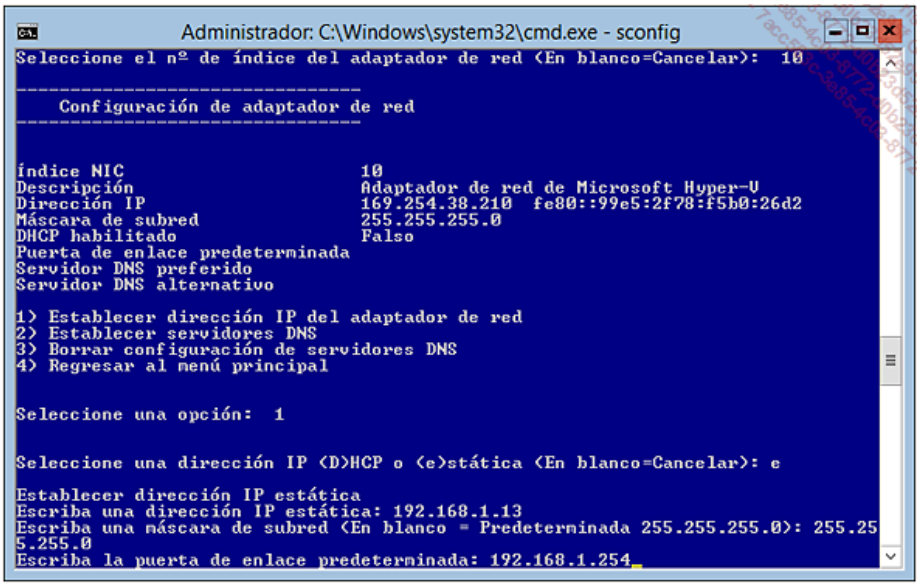
El menú le permite, también, acceder a la **Configuración de red** (opción 8).

En primer lugar, conviene seleccionar la tarjeta de red deseada mediante su índice.

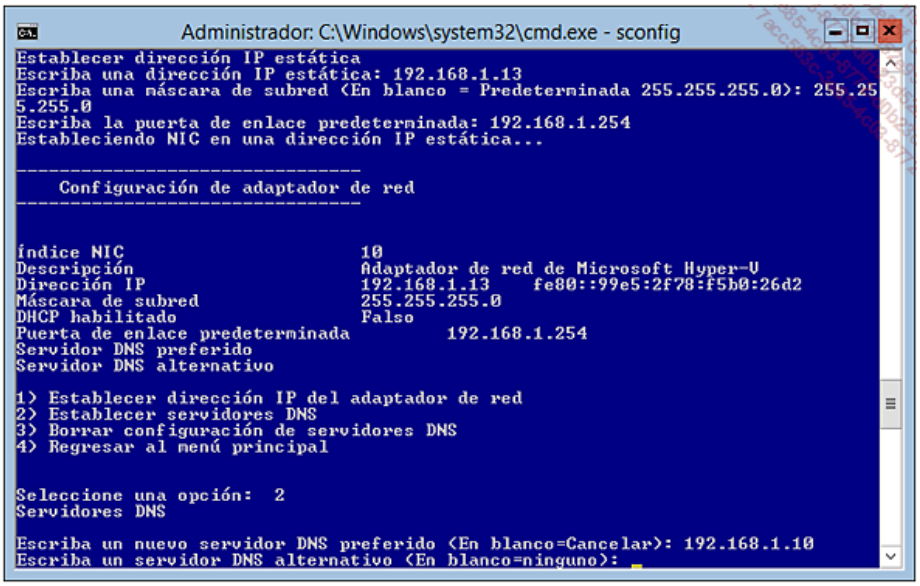
Una vez seleccionada la interfaz de red es preciso seleccionar el parámetro que desea modificar (dirección de la tarjeta de red, servidor DNS...).



Escriba **e** (para realizar una configuración estática) y, a continuación, valide su elección presionando la tecla [Enter]. Es necesario configurar, a continuación, la dirección IP, la máscara de subred y la puerta de enlace predeterminada.



No debe olvidar la configuración DNS, para ello se presenta la opción 2.



De este modo, la configuración de un servidor en modo instalación mínima resulta mucho más sencilla.

Servidor Nano

Windows Server 2016 ofrece una nueva opción de instalación: Nano Server. Nano Server es una versión del sistema operativo optimizada para las clouds privadas y los centros de datos. Se relaciona con Windows Server en modo Core, aunque está significativamente aligerado. Entre otros, solo soporta aplicaciones de 64 bits, herramientas y agentes.

De este modo, esta versión ocupa menos espacio en disco, se despliega mucho más rápido y requiere muchas menos actualizaciones y reinicios. La opción de instalación Nano está disponible para las ediciones Standard y Datacenter de Windows Server 2016.

Microsoft pone a nuestra disposición una herramienta que permite al administrador aprovisionar, crear y personalizar servidores Nano a través de una interfaz gráfica. La herramienta está disponible en la siguiente dirección: http://aka.ms/NanoServerImageBuilder

Hyper-V

El capítulo dedicado a la instalación de un entorno de pruebas presenta la instalación de una maqueta, en la que el sistema de virtualización propuesto es Hyper-V. Este sistema se presenta en este capítulo.

Se trata de un sistema de virtualización disponible en los sistemas operativos de servidor desde Windows Server 2008, y actualmente está disponible la versión 5. La ventaja de este hypervisor es el acceso inmediato al hardware de la máquina host (obteniendo así mejores tiempos de respuesta). Es posible instalar el rol Hyper-V con Windows Server 2016 en modo instalación completa (con la interfaz gráfica instalada) o en modo instalación mínima (sin interfaz gráfica).

1. Requisitos previos de hardware

Como ocurre con muchos roles en Windows Server 2016, Hyper-V tiene ciertos requisitos previos. El hardware de la máquina host está afectado por estos requisitos previos.

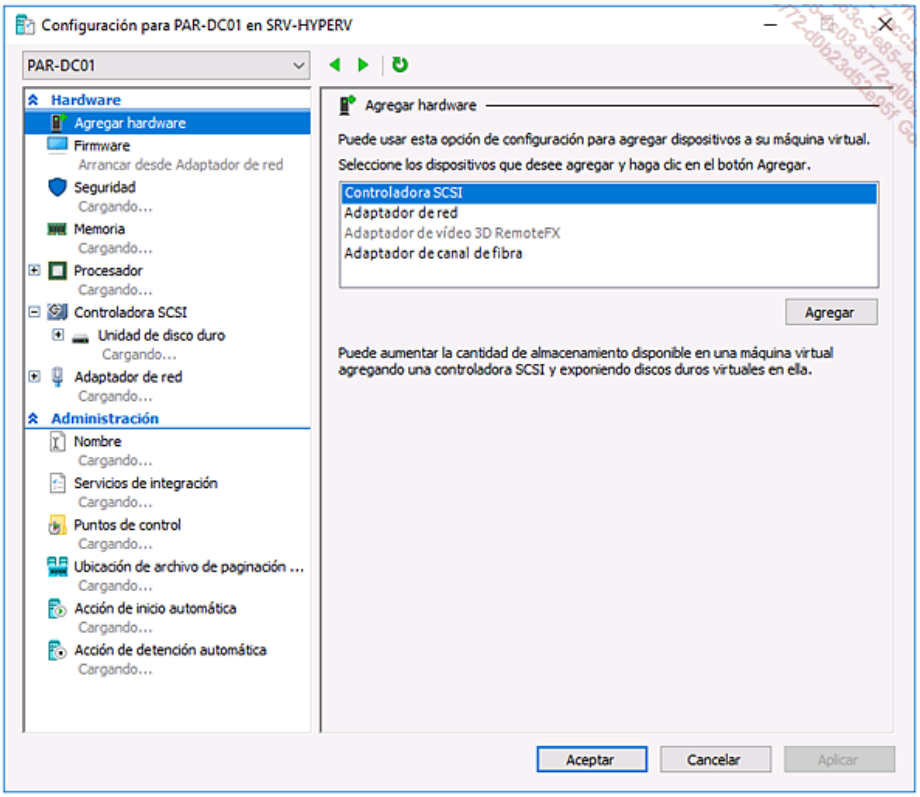
La máquina o servidor host debe poseer un procesador de 64 bits y soportar SLAT (*Second Level Address Translation*). La capacidad del procesador debe, también, responder a ciertas exigencias de las máquinas virtuales. Éstas pueden soportar un máximo de 128 procesadores virtuales. La cantidad de memoria en el servidor host debe ser superior a la memoria configurada en las máquinas virtuales. Durante la asignación de memoria a las máquinas virtuales es preciso reservar una parte para el funcionamiento de la máquina física. Si la máquina host posee 32 GB de memoria disponible, se recomienda reservar 1 o 2 GB para el funcionamiento del servidor físico (el tamaño de la reserva varía en función de los roles que estén instalados en la máquina física).

2. Las máquinas virtuales en Hyper-V

Por defecto, una máquina virtual utiliza los siguientes componentes:

- BIOS: se simula la BIOS de un ordenador físico, es posible configurar varias opciones:
  - El orden de arranque para la máquina virtual (red, disco duro, DVD…).
  - La activación o bloqueo automático del teclado numérico.
- Arranque seguro UEFI disponible con máquinas de segunda generación.
- Memoria RAM: a la máquina virtual se le asigna una cantidad de la memoria disponible. Como máximo, es posible asignar 5,5 TB de memoria. Desde Windows Server 2008 R2 SP1 es posible asignar memoria dinámicamente (se verá más adelante en este mismo capítulo).
- Procesador: como con la memoria, es posible asignar uno o varios procesadores (en función del número de procesadores y del número de núcleos de la máquina física). Es posible asignar, como máximo, 128 procesadores a una máquina virtual.
- Controlador IDE: es posible configurar dos controladores IDE en la VM (*Virtual Machine*), cada uno con dos discos como máximo.
- Controlador SCSI: agrega un controlador SCSI a la máquina virtual. De este modo, es posible agregar discos duros o lectores de DVD.
- Tarjeta de red: por defecto, la tarjeta de red de la máquina virtual no se hereda, lo que permite obtener una mejor tasa de transferencia, pero impide a la máquina realizar un arranque PXE (arranque del servidor en la red y carga de una imagen). Para poder iniciar en red es preciso agregar una tarjeta de red heredada.
- Tarjeta de vídeo 3D RemoteFX: este tipo de tarjetas permiten una representación gráfica de mejor calidad, aprovechando DirectX.

Seleccionando una máquina virtual y, a continuación, haciendo clic en **Configuración** en el menú **Acciones**, aparece la siguiente ventana.



Es posible configurar los siguientes componentes durante la creación de una máquina virtual (tarjeta de red, disco duro, lector DVD) o accediendo a la configuración de la máquina correspondiente.

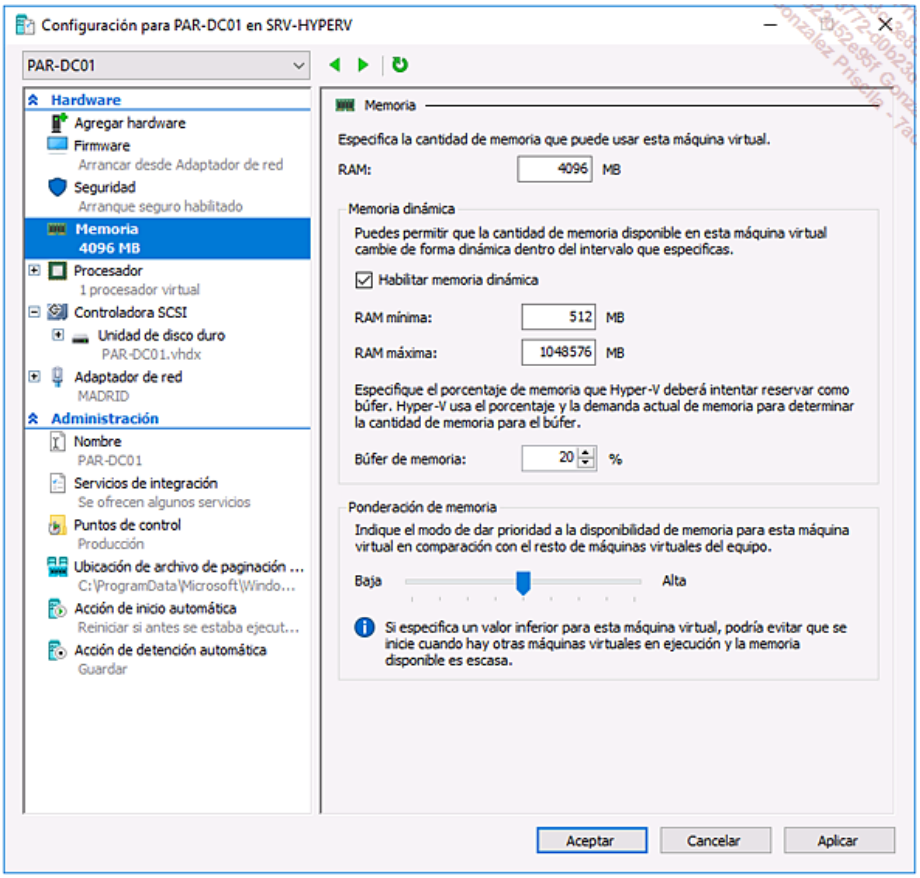
3. La memoria dinámica con Hyper-V

Tras la aparición de Windows Server 2008, el sistema de virtualización Hyper-V permitía asignar únicamente una cantidad de memoria estática. De este modo, el número de máquinas virtuales se veía reducido. Si se deseaba asignar 4 GB de RAM a un servidor, la cantidad de memoria reservada era idéntica, incluso si no existía ninguna actividad sobre la máquina virtual.

La memoria dinámica permite asignar una cantidad mínima de memoria. No obstante, si la máquina virtual necesita más memoria, está autorizada a solicitar una cantidad suplementaria (esta última no puede exceder la cantidad máxima acordada). Esta funcionalidad se ha incluido en los sistemas operativos de servidor desde Windows Server 2008 R2 SP1.

A diferencia de Windows Server 2008 R2, cualquier administrador puede modificar, en Windows Server 2012 R2, los valores mínimo y máximo de la memoria dinámica que una máquina puede consumir cuando ésta se encuentra encendida.

La memoria buffer es una funcionalidad que permite a la máquina virtual aprovechar una cantidad de RAM suplementaria si fuera necesario.



El peso de la memoria permite implementar prioridades acerca de la disponibilidad de la memoria.

4. El disco duro de las máquinas virtuales

Un disco duro virtual es un archivo que utiliza Hyper-V para representar los discos duros físicos. De este modo, es posible almacenar, en estos archivos, sistemas operativos o datos. Es posible crear un disco duro utilizando:

- La consola Administrador de Hyper-V.
- La consola Administrador de discos.
- El comando de DOS diskpart.
- El comando de PowerShell New-VHD.

Con la llegada de la nueva versión de Hyper-V, contenida en Windows Server 2012, es posible utilizar un nuevo formato, el VHDX.

Este nuevo formato ofrece varias ventajas respecto a su predecesor, el formato VHD (*Virtual Hard Disk*). De este modo, el tamaño de los archivos no está limitado a 2 TB, cada disco duro virtual puede tener un tamaño máximo de 64 TB. El VHDX es menos sensible a la corrupción de archivos tras un corte inesperado (debido a un fallo de corriente, por ejemplo) del servidor. Es posible convertir los archivos VHD existentes en VHDX (este punto se aborda más adelante en este mismo capítulo).

Windows Server 2012 R2 soporta el almacenamiento de los discos duros virtuales sobre particiones de archivo SMB 3. Tras la creación de una imagen virtual Hyper-V bajo Windows Server 2012 R2 es posible especificar un recurso compartido de red.

Los distintos tipos de discos

Durante la creación de un nuevo disco duro virtual, es posible crear distintos tipos de discos, incluyendo discos de tamaño fijo, dinámico o pass-through. Durante la creación de un disco virtual de tamaño fijo se reserva en disco el tamaño total correspondiente al archivo. De este modo, es posible limitar la fragmentación en el disco duro de la máquina host y mejorar el rendimiento. No obstante, este tipo de discos ofrecen el inconveniente de que consumen el espacio de disco incluso si el archivo VHD no contiene datos.

Durante la creación de un disco de tamaño dinámico se define un tamaño máximo para los archivos. El tamaño del archivo aumenta en función del contenido hasta alcanzar el tamaño máximo. Durante la creación de un archivo VHD de tipo dinámico, este último tiene un tamaño de 260 KB frente a los 4096 KB necesarios para un formato VHDX. Es posible crear un archivo VHD mediante el cmdlet de PowerShell `New-VHD` y el parámetro `-Dynamic`.

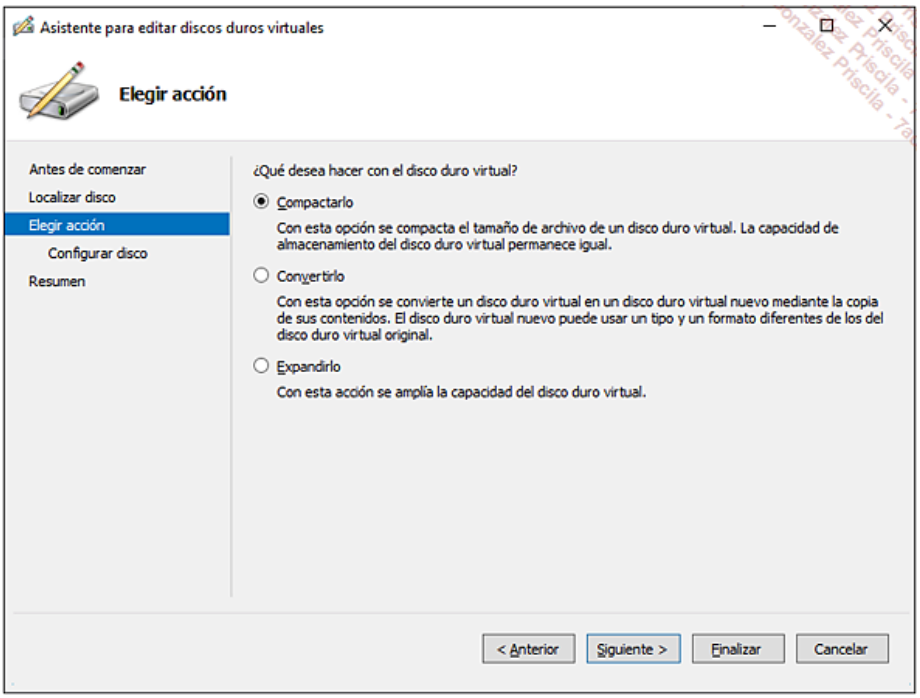
El disco virtual de tipo pass-through permite a una máquina virtual acceder directamente al disco físico. El disco se considera como un disco interno para el sistema operativo de la máquina virtual. Esto puede resultar muy útil para conectar la máquina virtual a una LUN (*Logical Unit Number*) iSCSI. No obstante, esta solución requiere un acceso exclusivo de la máquina virtual al disco físico correspondiente. Este último debe dejarse fuera de servicio mediante la consola Administrador de discos.

Administración de un disco virtual

Es posible realizar ciertas operaciones sobre los archivos VHD. Es posible, por ejemplo, comprimirlo para reducir el volumen utilizado o convertir el formato VHD en VHDX. Durante la conversión del disco virtual, el contenido se copia sobre un nuevo archivo (conversión de un archivo de tamaño fijo en uno de tamaño dinámico, por ejemplo). Una vez copiados los datos e implementado el nuevo disco, el anterior archivo se elimina.

Es posible realizar otras operaciones tales como la reducción de un archivo dinámico. Esta opción permite reducir el tamaño de un disco siempre que no utilice todo el espacio que se le ha asignado. Para los discos de tamaño fijo es necesario convertir antes el archivo VHD en un archivo de tipo dinámico.

Estas acciones pueden llevarse a cabo mediante el **Asistente para editar discos duros virtuales**, opción **Editar disco...** en el panel **Acciones**. La ventana nos da acceso a varias opciones.



También es posible utilizar los cmdlets de PowerShell `resize-partition` y `resize-vhd` para realizar la compresión de un disco duro virtual dinámico.

Los discos de diferenciación

Un disco de diferenciación permite reducir el tamaño necesario para el almacenamiento. En efecto, este tipo de discos consiste en crear un disco padre común a varias máquinas virtuales y un disco que contiene las modificaciones que se realizan respecto al disco padre, disco que es propio de cada máquina.

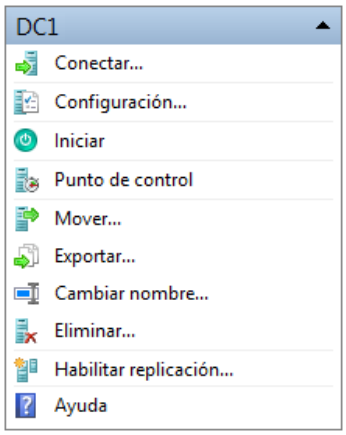
El tamaño necesario para almacenar las máquinas virtuales se ve, de este modo, reducido. Preste atención, la modificación de un disco padre provoca errores en los vínculos con los discos de diferenciación. Es, por tanto, necesario volver a conectar los discos de diferenciación utilizando la opción **Inspeccionar disco...** en el panel **Acciones**.

Es posible crear un disco de diferenciación utilizando el cmdlet de PowerShell `New-VHD`. El siguiente comando permite crear un disco de diferenciación llamado Diferencial.vhd, que utiliza un disco padre llamado Padre.vhd.

```
New-VHD c:\Diferencial.vhd -ParentPath c:\Padre.vhd
```

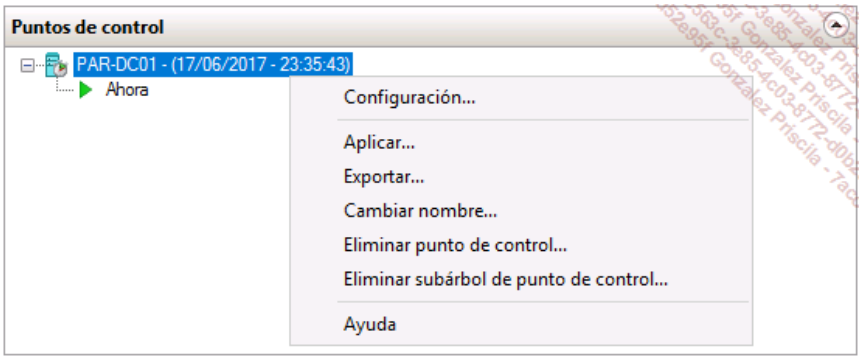
5. Los puntos de control en Hyper-V

Un punto de control (instantánea), antes llamado snapshot, se corresponde con una "foto" de la máquina virtual en el momento en que se realiza. Este último está contenido en un archivo con la extensión avhd o avhdx en función del tipo de archivo de disco duro seleccionado. Es posible realizar un snapshot seleccionando la máquina y haciendo clic en la opción **Punto de control** en el panel **Acciones**. La principal diferencia es que esta función está ahora soportada en producción.



Cada máquina puede poseer hasta 50 puntos de control. Si este último se crea mientras la máquina se encuentra iniciada, el punto de control incluirá el contenido de la memoria viva. Si se utiliza un punto de control para restablecer un estado anterior, es posible que la máquina virtual no pueda conectarse al dominio. En efecto, se produce un intercambio entre el controlador de dominio y la máquina virtual unida al dominio. Restaurando una máquina, este intercambio (contraseña) se restablece también. No obstante, la contraseña restablecida puede no seguir siendo válida, de modo que se rompería el canal seguro. Es posible reiniciarla realizando una nueva unión al dominio o utilizando el comando`netdom resetpwd`.

Preste atención: el punto de control no remplaza, en ningún caso, a la copia de seguridad, pues los avhd o avhdx se almacenan en el mismo volumen que la máquina virtual. En caso de degradación en el disco, se perderían todos los archivos. Por el contrario, se puede utilizar un punto de control para exportar la máquina virtual en un instante T y así podríamos hablar de copia de seguridad si la exportación se almacena en un soporte diferente.



6. Gestión de redes virtuales

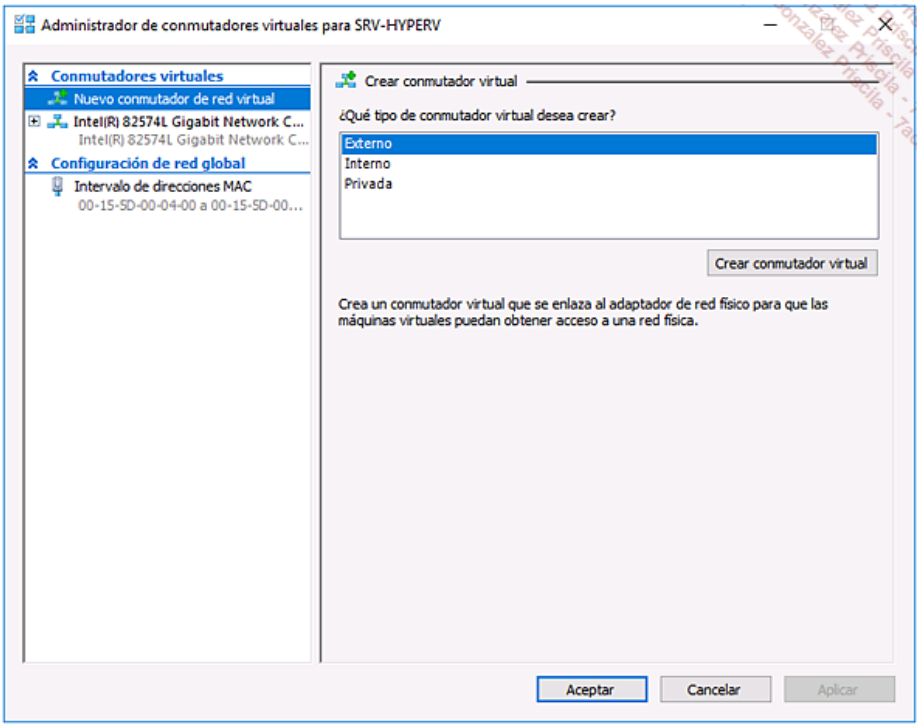
Es posible crear varios tipos de redes y aplicarlos a una máquina virtual, lo cual permite a las distintas estaciones comunicarse entre sí o con los equipos externos a la máquina host (router, servidor…).

Los conmutadores virtuales

Un conmutador virtual se corresponde con un conmutador físico, que podemos encontrar en cualquier red informática. También conocido como red virtual, con Windows Server 2008, hablamos ahora de conmutador virtuales desde Windows Server 2012. Es posible gestionarlos utilizando la opción Administrador de conmutadores virtuales en el panel **Acciones**.

Es posible crear tres tipos de conmutadores:

- **Externo**: con este tipo de conmutador virtual es posible utilizar la tarjeta de red de la máquina host en la máquina virtual. De este modo, este conmutador virtual tiene una conexión sobre la red física que le permite acceder a los equipos o servidores de la red física.
- **Interno**: permite crear una red entre la máquina física y las máquinas virtuales. Es imposible, para las máquinas de la red física, comunicarse con las VM.
- **Privada**: la comunicación puede realizarse únicamente entre las máquinas virtuales, la máquina host no puede conectarse con ninguna de las VM.



Una vez creado, conviene volver a vincular la tarjeta de red de la VM con el conmutador deseado.

Requisitos previos y objetivos

1. Requisitos previos

Poseer ciertas nociones sobre virtualización de servidores.

Tener nociones sobre el funcionamiento de un sistema operativo.

2. Objetivos

Configuración del servidor Hyper-V.

Instalación de la maqueta que permitirá realizar los trabajos prácticos.

El entorno de pruebas

El entorno de pruebas permite crear un entorno virtual o físico para llevar a cabo las pruebas. Éstas se realizan sin poner en riesgo máquinas o servidores en producción.

La virtualización permite disminuir el número de máquinas físicas necesarias. Todas las máquinas virtuales funcionan sobre el mismo servidor físico. Será, no obstante, necesario disponer de una cantidad de memoria y un espacio de disco suficientes.

1. Configuración necesaria

Se requiere una máquina potente para soportar todas las máquinas virtuales; la maqueta descrita más adelante está equipada con un procesador Core I7 con 16 GB de RAM (recomendado), aunque con 8 GB de RAM sigue siendo viable, bastará con arrancar únicamente las máquinas necesarias. Es útil guardar como mínimo 1 GB de memoria para la máquina host, quedando los 7 GB restantes para el conjunto de máquinas virtuales. El sistema operativo instalado es Windows Server 2016.

La solución de virtualización que se ha escogido es Hyper-V, integrada en las versiones servidor de Windows desde la versión 2008. Es posible, desde Windows 8 o Windows 10, utilizar Hyper-V en los sistemas operativos cliente.

2. Instalación de Windows Server 2016

Antes de instalar Windows Server 2016 en el puesto físico es necesario respetar los requisitos previos del sistema operativo.

- **Procesador**: 1,4 GHz como mínimo, y arquitectura de 64 bits.
- **Memoria RAM**: 512 MB como mínimo. No obstante, un servidor equipado con 1024 MB es, en mi opinión, el mínimo aceptable.
- **Espacio de disco**: una instalación básica, sin ningún rol, requiere un espacio de disco de 15 GB. Habrá que prever un espacio más o menos adecuado en función del rol del servidor.

Desde Windows 2008 se proporcionan dos tipos de instalación:

- Una instalación completa: con una interfaz gráfica que permite administrar el servidor de manera visual o por línea de comandos.
- Una instalación mínima: el sistema operativo se instala sin ninguna interfaz gráfica. Sólo se muestra en pantalla una línea de comandos: la instalación de roles y características, o la administración cotidiana del servidor, se realizan por línea de comandos. Es, no obstante, posible administrar los distintos roles de forma remota instalando archivos RSAT en un puesto remoto. Ciertos criterios, tales como las características técnicas del servidor o la voluntad de reducir la administración, facilitan la elección entre ambos tipos de instalación. Si el servidor posee características limitadas o si desea reducir el número de actualizaciones que tendrá que instalar se recomienda realizar una instalación mínima.

Existe un tercer tipo de instalación llamado Nano Server que ha aparecido con Windows Server 2016. Esta versión, como su nombre indica, resulta muy ligera y económica en términos de recursos, todavía más que un servidor Core. Para ello, Microsoft ha conservado únicamente lo esencial, reduciendo de forma drástica el tiempo de despliegue de una máquina virtual Nano Server (unos 3 minutos), lo que reduce a su vez la superficie de ataque. La administración de un Nano Server se realiza exclusivamente de manera remota con PowerShell mediante **PowerShell Remoting**, **PowerShell Direct**, o bien mediante herramientas de administración remota.

Una vez terminada la instalación del servidor es necesario reconfigurar el nombre del servidor y definir su configuración IP.

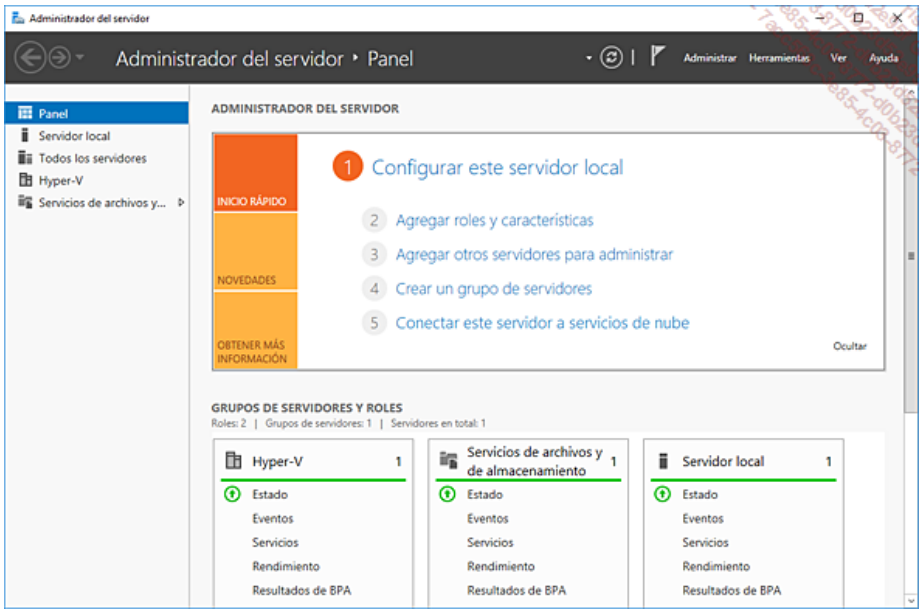
Creación de las máquinas virtuales

La siguiente etapa consiste en la instalación del rol Hyper-V y la creación, instalación y configuración posterior de las distintas máquinas virtuales.

El conjunto de scripts PowerShell utilizados en este capítulo están disponibles para su descarga desde la página Información.

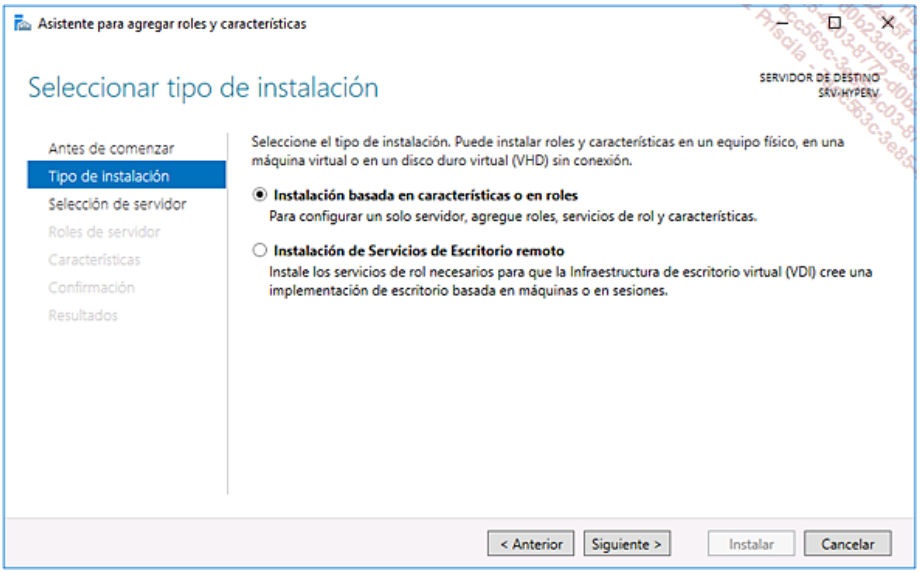
Haga clic en el **Administrador del servidor** .

En la consola, haga clic en **Agregar roles y características**.

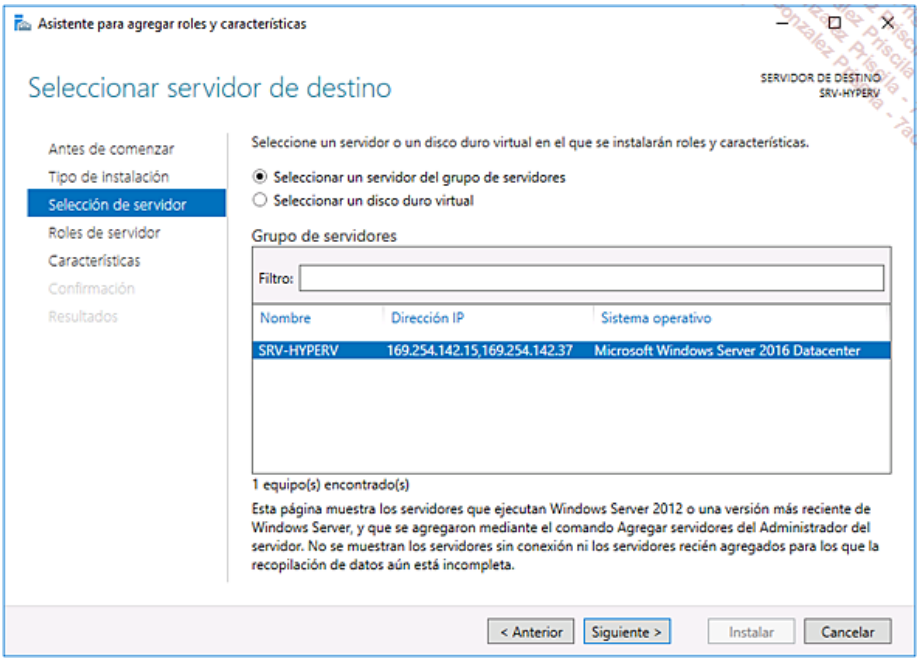


Se abre el asistente, haga clic en **Siguiente**.

Dado que Hyper-V es un rol, deje marcada la opción por defecto **Instalación basada en características o en roles** y, a continuación, haga clic en **Siguiente**.



Verifique que el servidor de destino es el suyo y haga clic en **Siguiente**.



Marque la opción **Hyper-V** y, a continuación, haga clic en **Agregar características**.

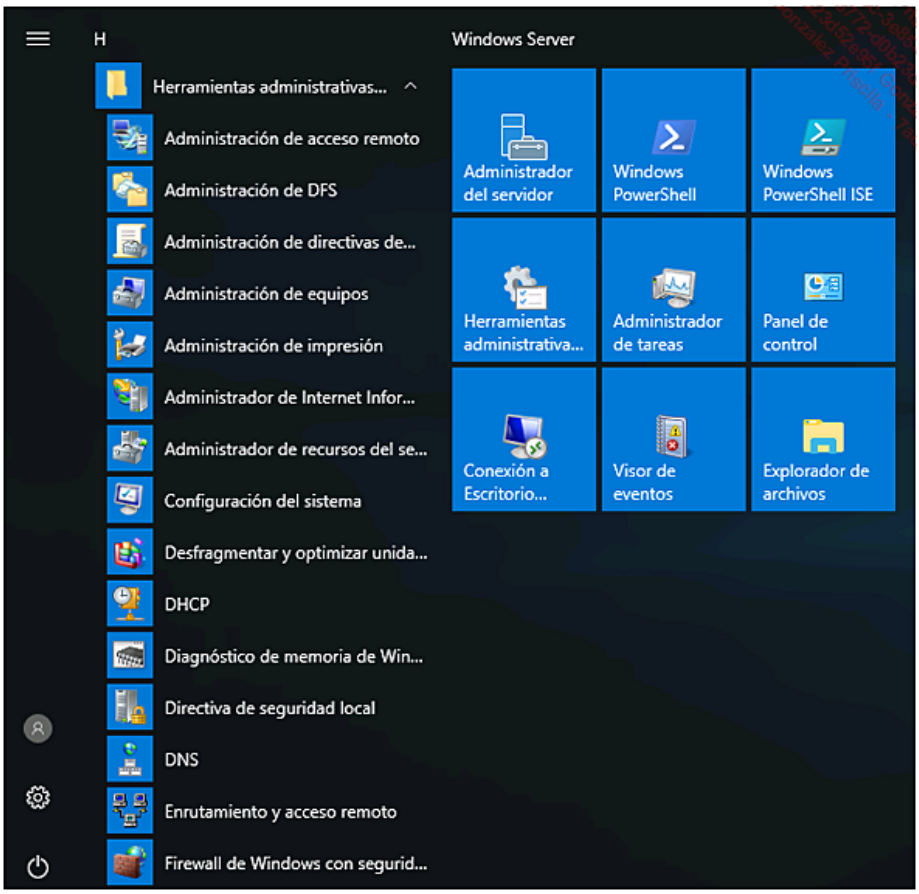
Haga clic en **Siguiente** en la ventana de instalación de características.

Es necesario crear un conmutador virtual: haga clic en la tarjeta de red para realizar un puente entre la red física y la máquina virtual.

Haga clic dos veces en **Siguiente** y, a continuación, en **Instalar**.

Reinicie el servidor una vez terminada la instalación.

Haga clic en el botón **Inicio** y, a continuación, acceda a las Herramientas administrativas y haga clic en el **Administrador de Hyper-V**.



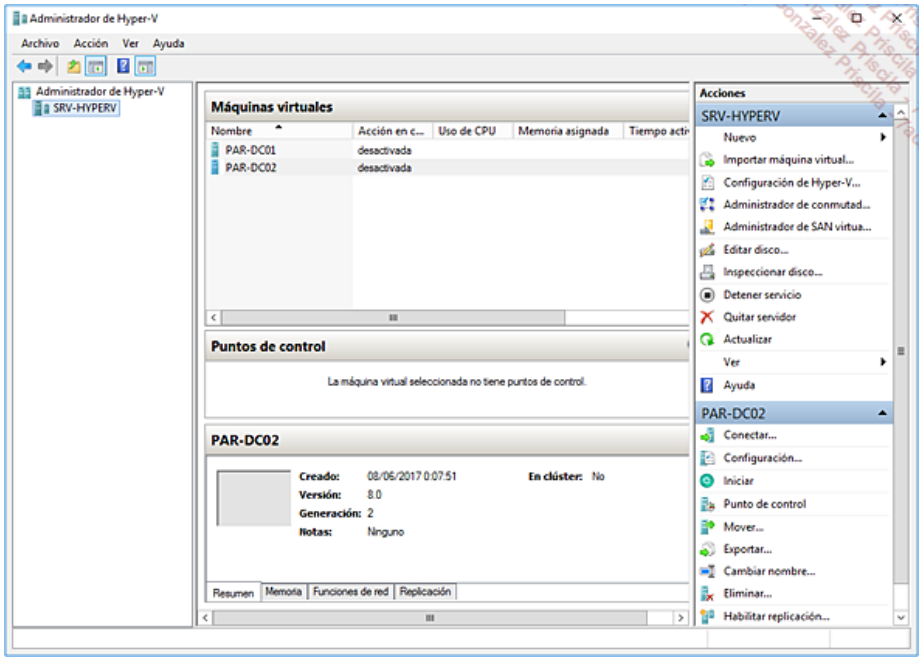
Ahora es preciso configurar la interfaz de red. Es posible utiliza la tarjeta física o crear una tarjeta interna. Para esto último, existen dos opciones:

- **Red interna**: se crea una red virtual entre la máquina host y las máquinas virtuales. Es imposible alcanzar una máquina en la red física

(servidor, impresora de red…).

- **Red privada**: las máquinas virtuales están aisladas de la máquina host, es imposible conectar con la máquina física y las máquinas de la red física.

Haga clic en **Administrador de conmutadores virtuales** en la consola Hyper-V (panel **Acciones**).

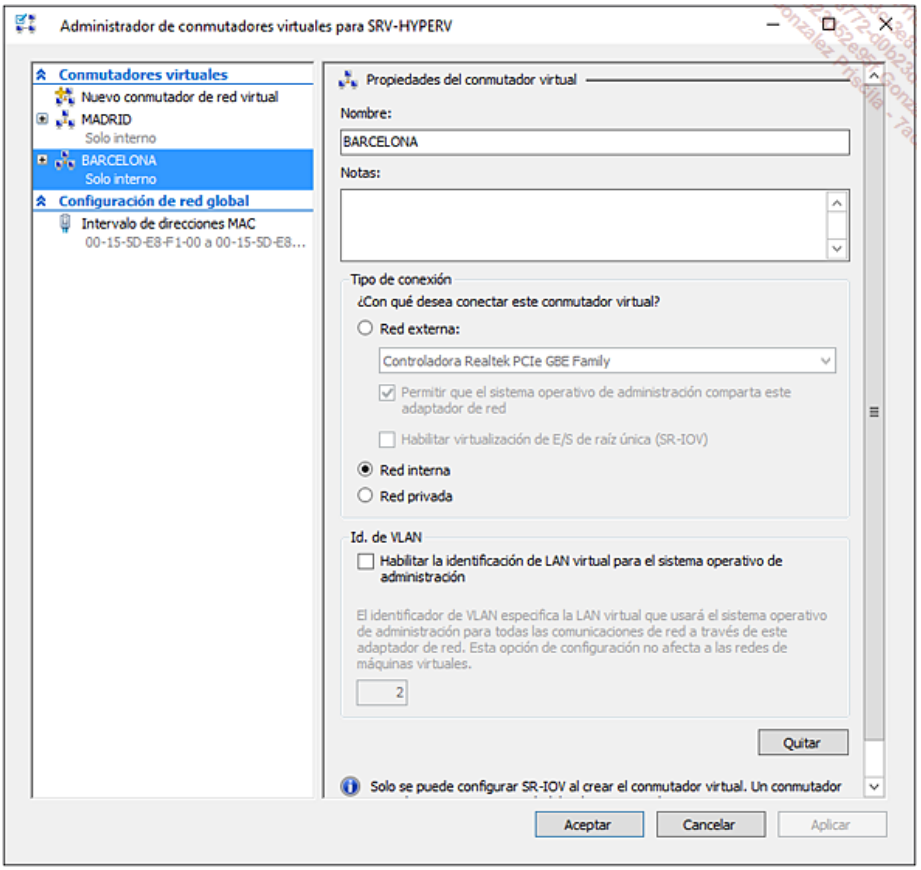


Haga clic en **Nuevo conmutador de red virtual** y, a continuación, seleccione el tipo **Interno**.

Acepte la selección haciendo clic en el botón **Crear conmutador virtual**.

Dé nombre a la tarjeta creada en la red virtual **MADRID**.

Repita la operación para crear el conmutador de red virtual **BARCELONA**.



Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

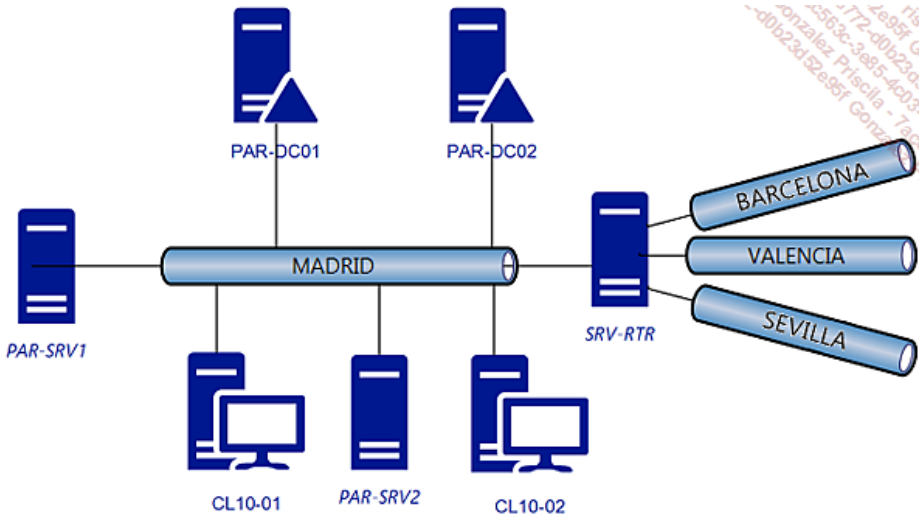
1. Esquema de la maqueta

Se van a crear siete máquinas virtuales, los sistemas operativos utilizados serán Windows Server 2016 y Windows 10 Enterprise.

Durante la instalación de las máquinas virtuales, éstas serán miembro del grupo de trabajo Workgroup. A continuación, crearemos el dominio de Active Directory Formacion.local. Se utilizarán dos redes, con dos rangos diferentes de direcciones IP, enlazadas mediante un servidor SRV-RT.

La maqueta contiene cinco servidores y dos puestos cliente:

- PAR-DC01, controlador de dominio del dominio Formacion.eni.
- PAR-DC02, controlador de dominio del dominio Formacion.eni.
- PAR-SRV1, servidor miembro del dominio Formacion.eni.
- PAR-SRV2, servidor miembro del dominio Formacion.eni.
- SRV-RTR, servidor miembro con el rol de enrutador.
- CL10-01, puesto de cliente Windows 10 Enterprise miembro del dominio Formacion.eni.
- CL10-02, puesto de cliente Windows 10 Enterprise miembro del dominio Formacion.eni.



Roles instalados y configuración de los servidores y puestos:

	Rol instalado	Configuración IP
PAR-DC01	Active Directory, DNS	Dirección IP: 172.16.0.1 Máscara de subred: 255.255.0.0 Puerta de enlace predeterminada: 172.16.255.254 Servidor DNS primario: 172.16.0.01
PAR-DC02	Active Directory y DNS	Dirección IP: 172.16.0.2 Máscara de subred: 255.255.0.0 Puerta de enlace predeterminada: 172.16.255.254 Servidor DNS primario: 172.16.0.1
PAR-SRV1	Ningún rol	Dirección IP: 172.16.0.3 Máscara de subred: 255.255.0.0 Puerta de enlace predeterminada: 172.16.255.254 Servidor DNS primario: 172.16.0.1
PAR-SRV2	Ningún rol	Dirección IP: 172.16.0.4 Máscara de subred: 255.255.0.0 Puerta de enlace predeterminada: 172.16.255.254 Servidor DNS primario: 172.16.0.1
CL10-01 y**CL10-02**	Ningún rol	Configuración atribuida por el servidor DHCP
SRV-RTR	Enrutador	**Tarjeta de red MADRID**: Dirección IP: 172.16.255.254 Máscara de subred: 255.255.0.0 Servidor DNS primario: 172.16.0.1 **Tarjeta de red BARCELONA**: Dirección IP: 172.17.255.254 Máscara de subred: 255.255.0.0

La instalación y la configuración de los roles se detallan más adelante en este libro.

Con Hyper-V tenemos la posibilidad de crear discos duros diferenciales, de modo que podemos crear un disco duro que contenga una versión de Windows Server 2016 Datacenter y un disco duro que contenga la versión de Windows 10 Enterprise. Ahorraremos espacio en disco para crear las máquinas virtuales, pues compartirán todas ellas un mismo disco duro padre. Esta configuración debería evaluarse si se dispone de un disco duro SSD de poca capacidad.

El procedimiento detallado a continuación debe reproducirse para los demás servidores, pudiendo escoger entre dos métodos: **Clásico** o**Diferencial**.

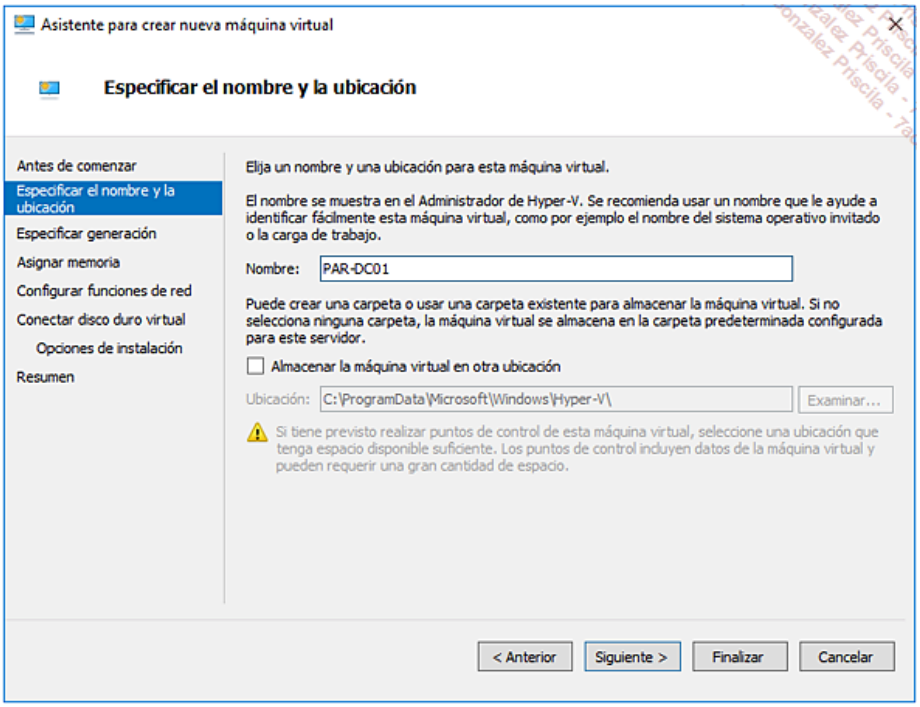
2. Método Clásico

a. Creación y configuración de la VM

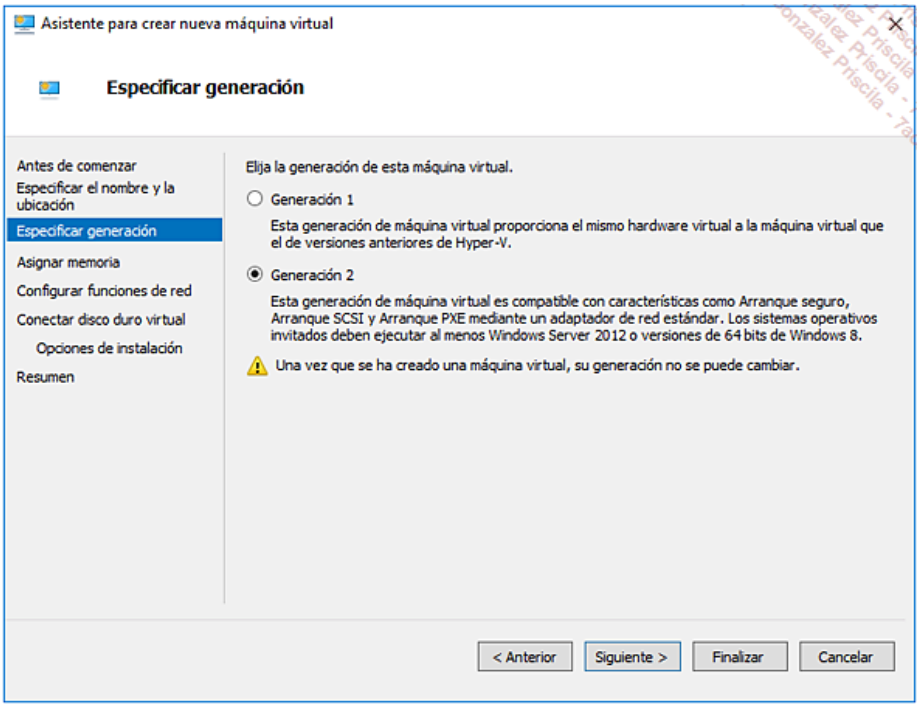
En la consola Hyper-V, haga clic en **Nuevo** dentro del panel **Acciones** y, a continuación, en **Máquina virtual**.

En la ventana **Antes de comenzar**, haga clic en **Siguiente**.

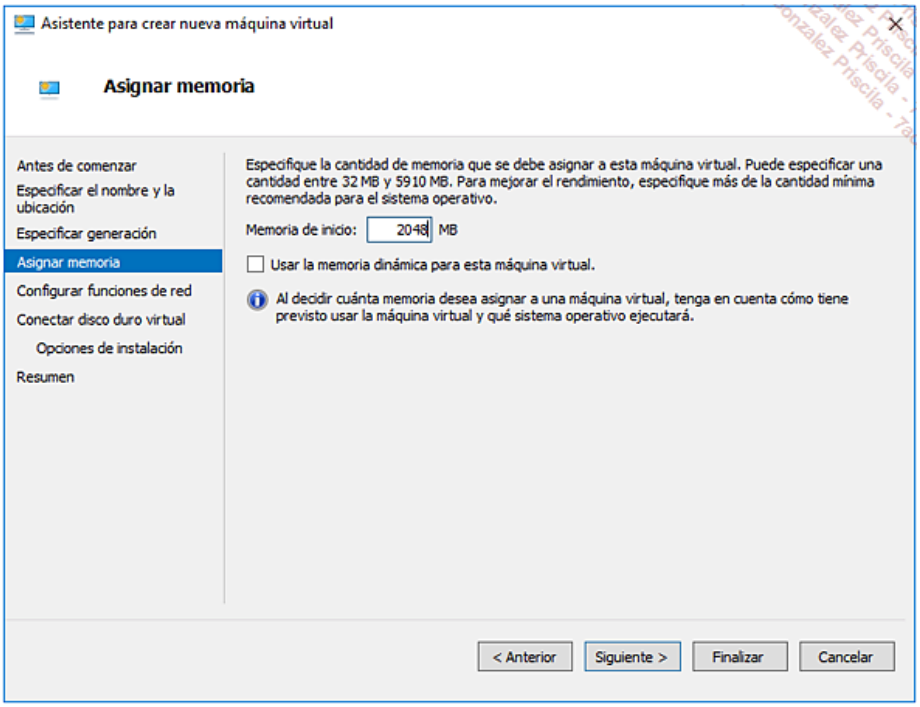
Escriba **PAR-DC01** en el campo **Nombre** y, a continuación, haga clic en **Siguiente**.



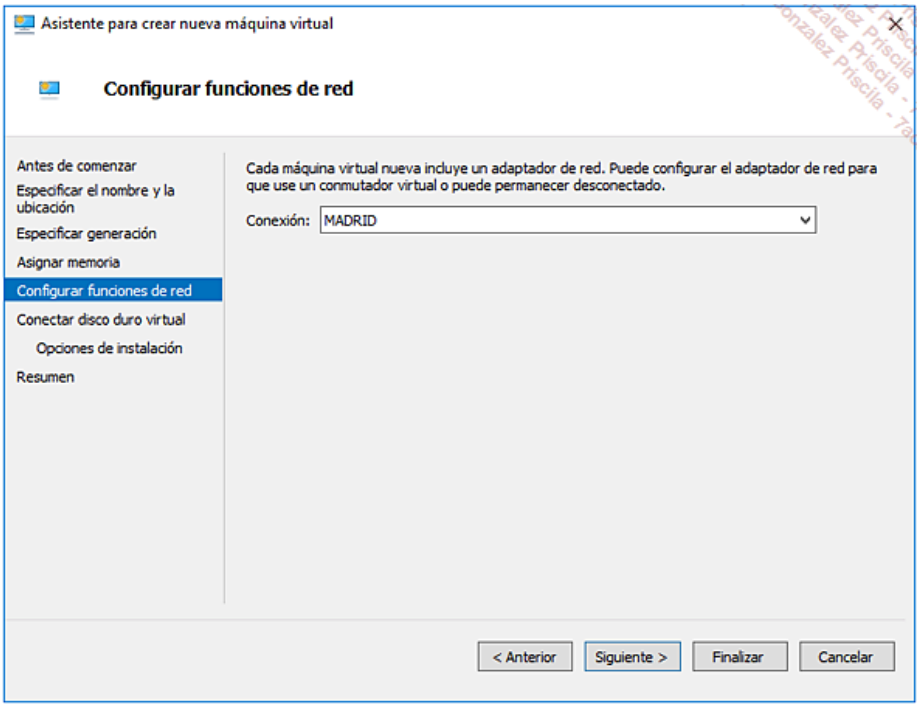
Seleccione la opción **Generación 2** y, a continuación, haga clic en el botón **Siguiente**.



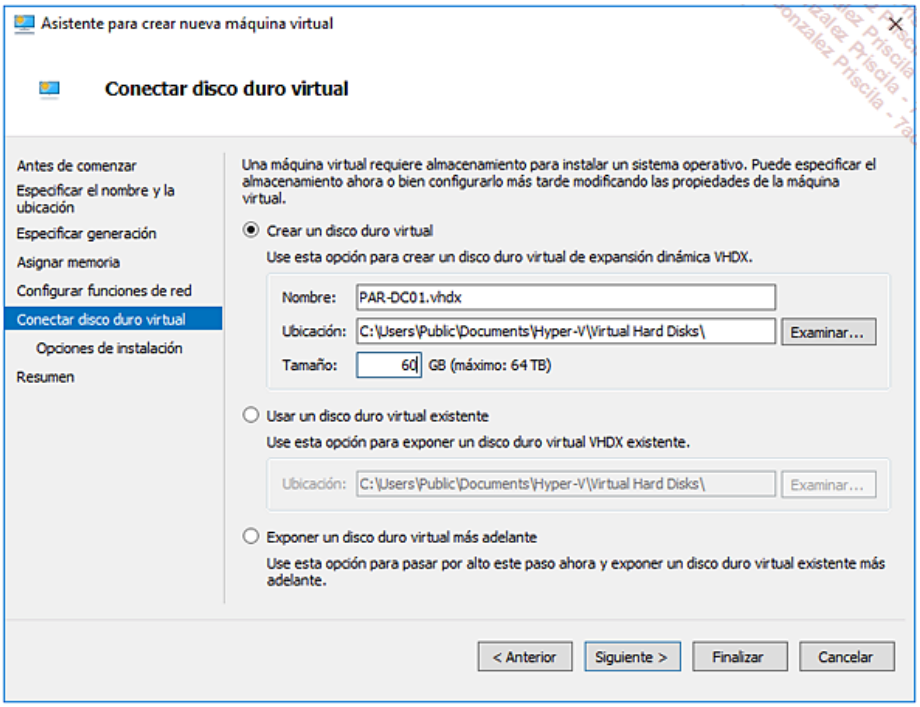
Escriba **2048** en el campo **Memoria de inicio**. Haga clic en **Siguiente**.



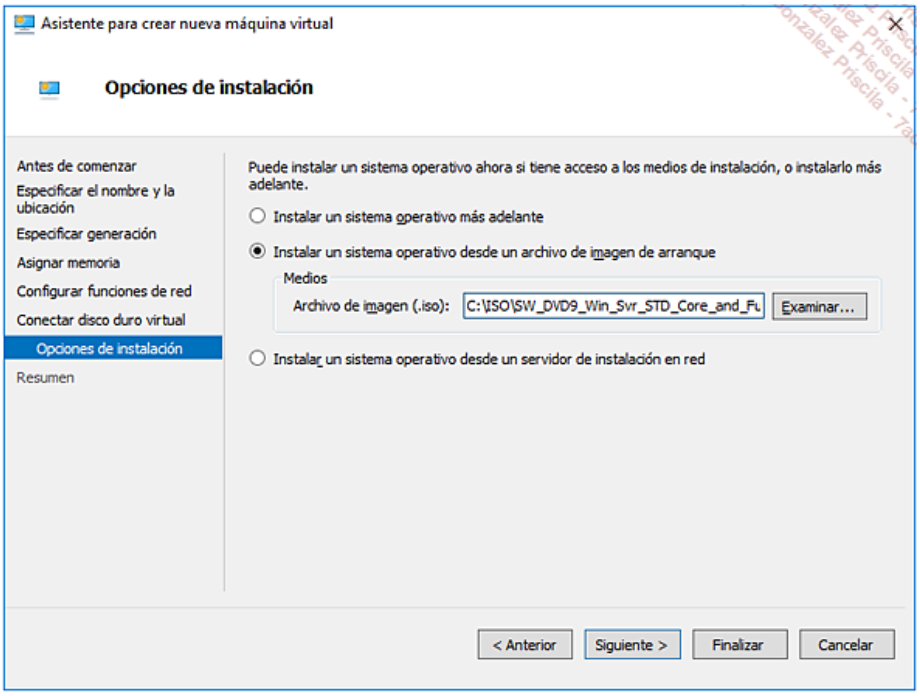
En la ventana **Configurar funciones de red**, seleccione la tarjeta de red deseada (**MADRID**) y haga clic en **Siguiente**.



Escriba **60** en el campo **Tamaño** del disco y valide con el botón **Siguiente**.



Conecte, a la máquina virtual, la ISO o el DVD de Windows Server 2016 y haga clic en **Siguiente**.



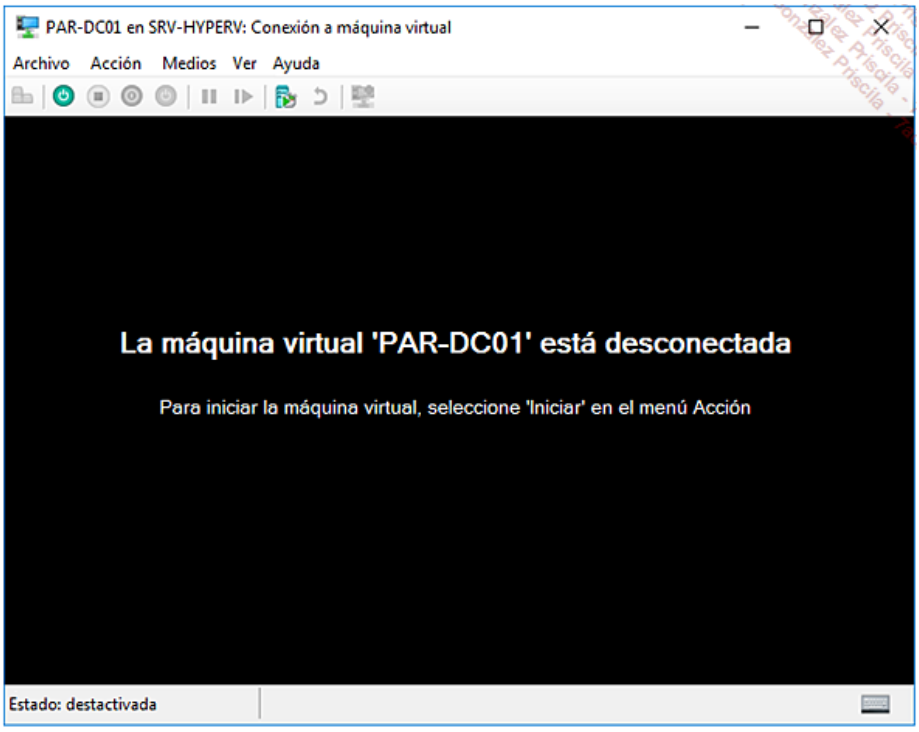
En la ventana de resumen, haga clic en **Finalizar**.

Aparece la nueva máquina en la ventana central de la consola.

El disco duro de la máquina se ha creado, pero está virgen. Es preciso particionarlo e instalar un sistema operativo.

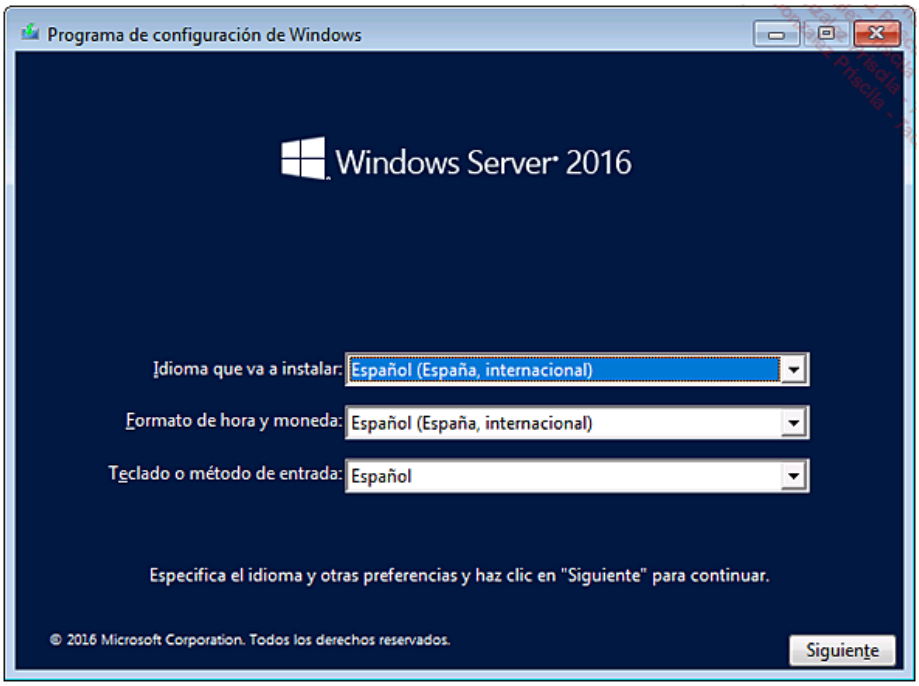
b. Instalación del sistema operativo

En la consola Hyper-V, haga doble clic en la máquina que acaba de crear y, a continuación, haga clic en el botón que permite iniciar la VM (icono verde).



La máquina arranca y se inicia la instalación de Windows Server 2016.

Haga clic en **Siguiente** en la ventana que permite escoger el idioma (el idioma **Español** está seleccionado por defecto).

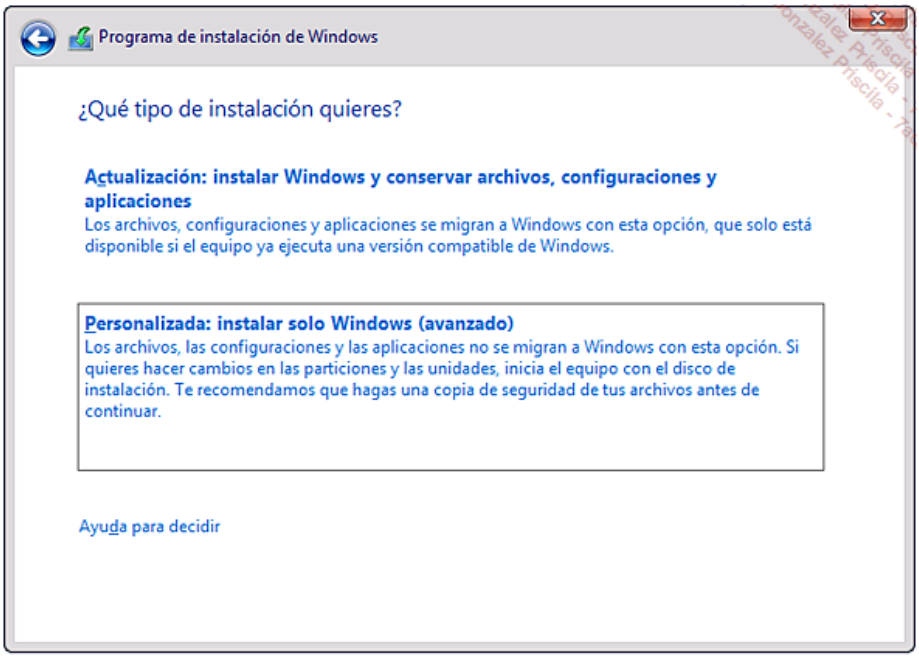


Haga clic en **Instalar ahora** para iniciar la instalación.

Haga clic en la versión **Datacenter (Experiencia de escritorio)** (instalación con interfaz de usuario).

Acepte el contrato de licencia y, a continuación, haga clic en **Siguiente**.

Seleccione el tipo de instalación **Personalizada: instalar solo Windows (avanzado)**.

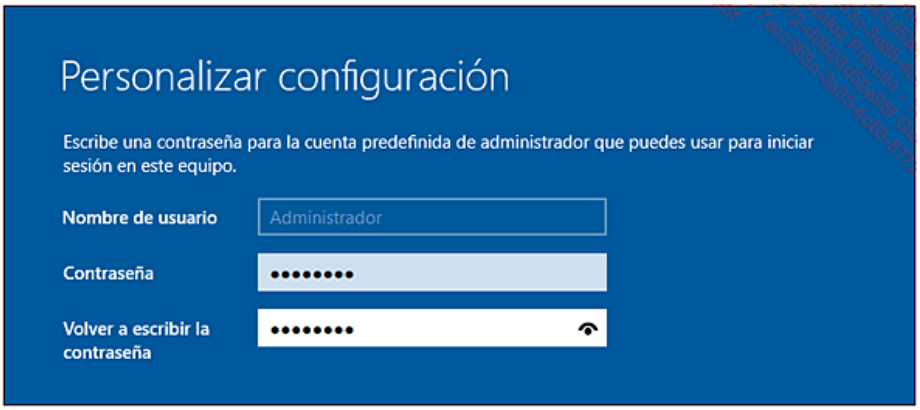


Con ayuda de la opción **Opciones de unidad (avanz.)**, cree dos particiones de 30 GB.

Haga clic en la primera partición de 30 GB y, a continuación, en **Siguiente**.

Se completa la instalación…

Escriba la contraseña **Pa$$w0rd** y, a continuación, confírmela.



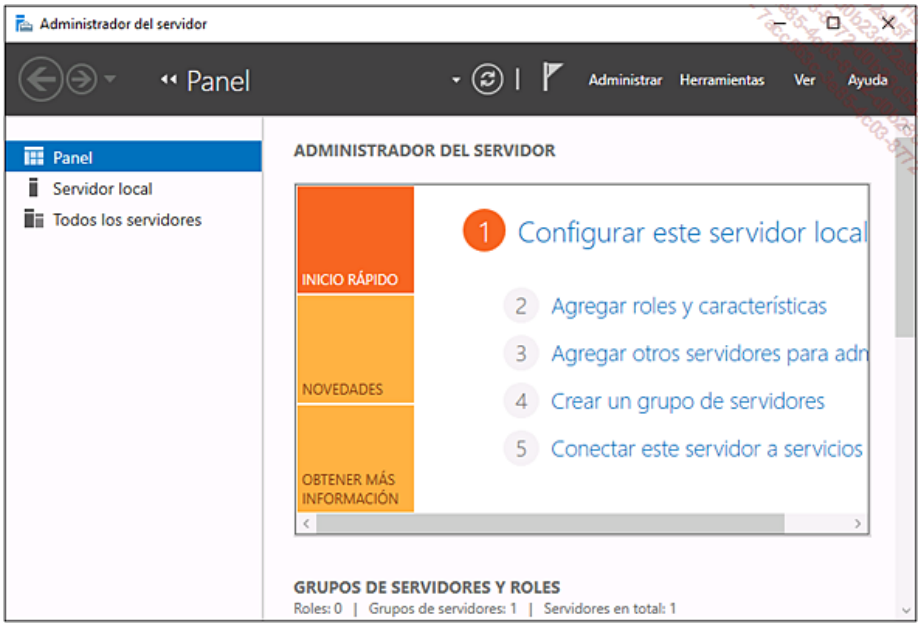
Termina la instalación. La siguiente etapa consiste en la modificación del nombre del equipo y la configuración IP de la máquina. Los roles se instalarán a lo largo de los siguientes capítulos.

c. Configuración post-instalación

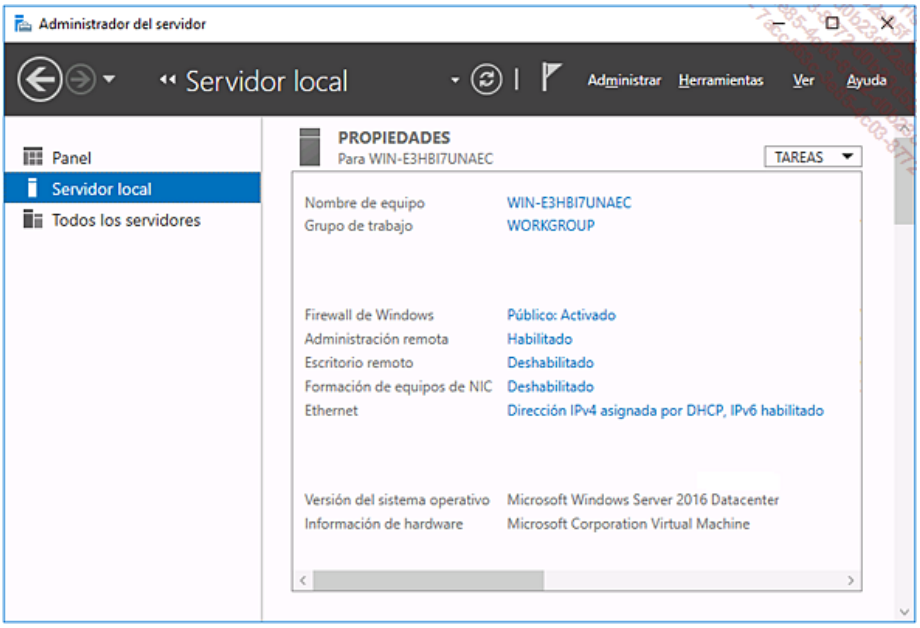
Realice un [Ctrl][Alt][Fin] en la máquina virtual recién instalada, o haga clic en el primer icono de la barra de herramientas para escribir un nombre de usuario y una contraseña.

Abra una sesión como administrador, introduciendo la contraseña configurada en la sección anterior.

En el **Administrador del servidor**, haga clic en **Configurar este servidor local**.



Haga clic en **Nombre de equipo** para abrir las propiedades del sistema.



Haga clic en **Cambiar** y, a continuación, escriba **PAR-DC01** en el campo **Nombre de equipo**.

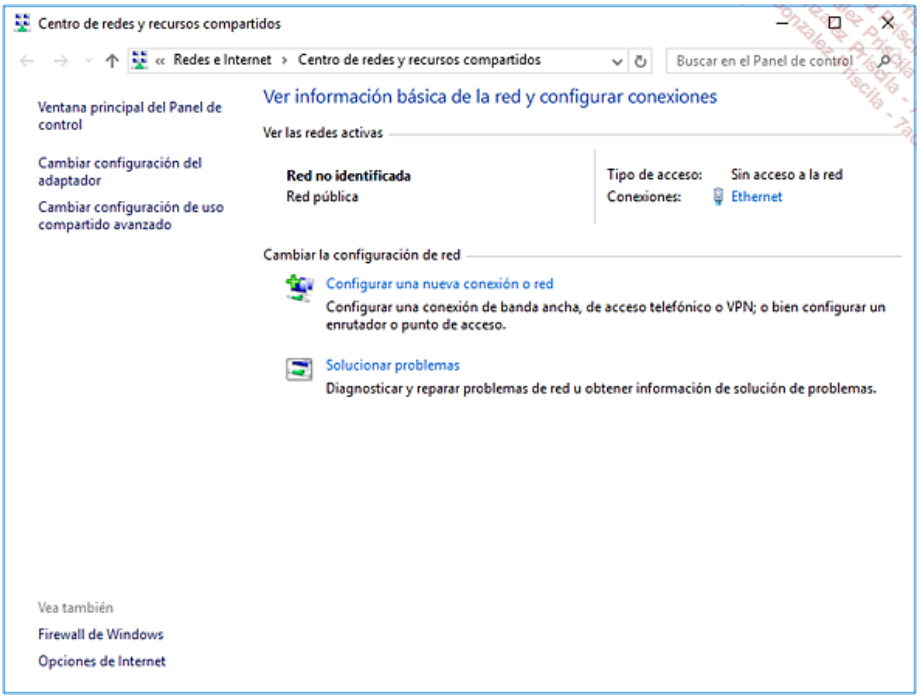
Haga clic dos veces en **Aceptar** y, a continuación, en **Cerrar**.

Reinicie la máquina virtual para que se hagan efectivos los cambios.

A continuación es preciso configurar la dirección IP de la tarjeta de red.

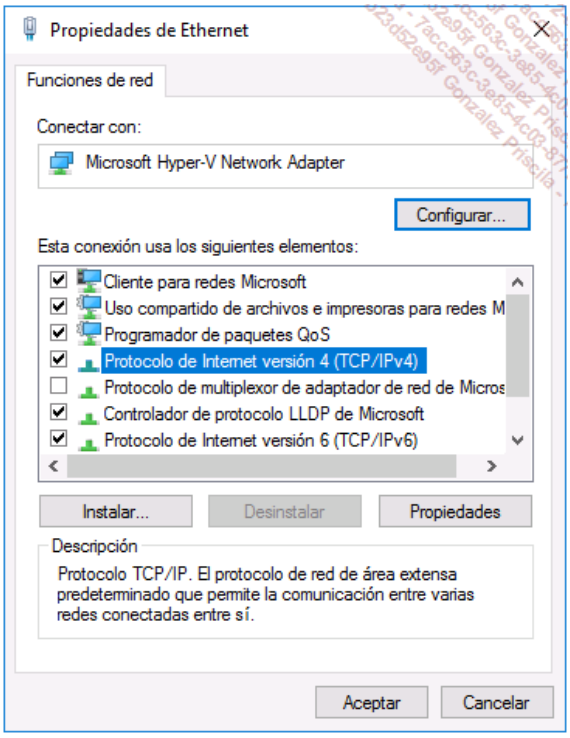
Haga clic con el botón derecho en **Centro de redes y recursos compartidos** y, a continuación, haga clic en **Abrir**.

Haga clic en **Cambiar configuración del adaptador**.

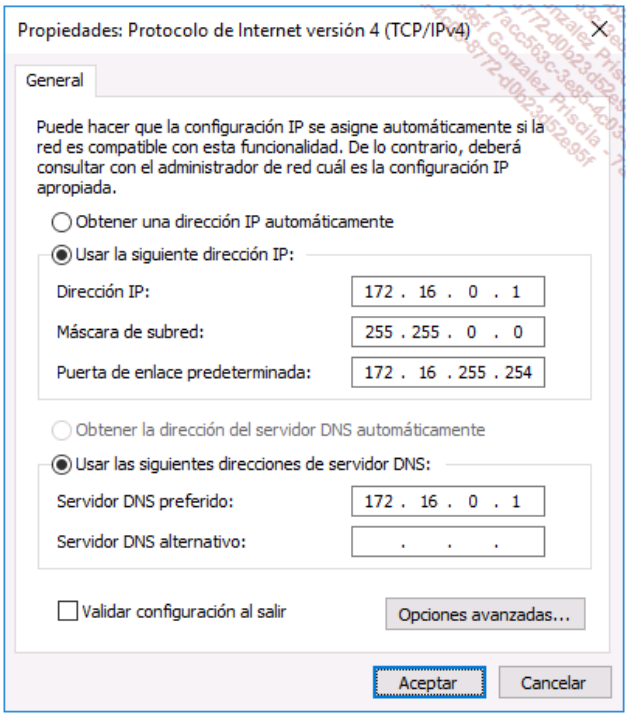


Haga doble clic en la tarjeta de red y, a continuación, en **Propiedades**.

En la ventana de **Propiedades**, haga doble clic en **Protocolo de Internet versión 4 (TCP/IPv4)**.



Configure la interfaz de red como se muestra a continuación.



Estas manipulaciones hay que reproducirlas, con otros parámetros, en las siguientes máquinas virtuales.

Las modificaciones que hay que llevar a cabo son el nombre del equipo y su configuración IP.

3. Máquina virtual PAR-DC02

Este servidor es el segundo controlador de dominio de la maqueta, llamado **PAR-DC02**. La cantidad de memoria asignada es de 2048 MB y el disco virtual de 60 GB.

- **Dirección IP**: 172.16.0.2
- **Máscara de subred**: 255.255.0.0
- **Puerta de enlace predeterminada**: 172.16.255.254

- **Servidor DNS preferido**: 172.16.0.1
- **Contraseña del administrador local**: Pa$$w0rd

Los roles se instalarán en los siguientes capítulos.

4. Máquina virtual PAR-SRV1

Servidor miembro del dominio. Se instalarán distintos roles más adelante.

La cantidad de memoria asignada es de 2048 MB y el disco virtual de 60 GB.

- **Nombre de equipo**: PAR-SRV1
- **Dirección IP**: 172.16.0.3
- **Máscara de subred**: 255.255.0.0
- **Puerta de enlace predeterminada**: 172.16.255.254
- **Servidor DNS preferido**: 172.16.0.1
- **Contraseña del administrador local**: Pa$$w0rd

5. Máquina virtual PAR-SRV2

Servidor miembro del dominio. Se instalarán distintos roles más adelante.

La cantidad de memoria asignada es de 2048 MB y el disco virtual de 60 GB.

- **Nombre de equipo**: PAR-SRV2
- **Dirección IP**: 172.16.0.4
- **Máscara de subred**: 255.255.0.0
- **Puerta de enlace predeterminada**: 172.16.255.254
- **Servidor DNS preferido**: 172.16.0.1
- **Contraseña del administrador local**: Pa$$w0rd

6. Máquina virtual CL10-01

Puesto cliente con Windows 10, esta máquina es miembro del dominio. La configuración IP se realizará mediante un contrato DHCP.

La cantidad de memoria asignada es de 2048 MB y el disco virtual de 30 GB está particionado con una única partición.

- **Nombre de equipo**: CL10-01
- **Contraseña del administrador local**: Pa$$w0rd

7. Máquina virtual CL10-02

Puesto cliente con Windows 10, esta máquina es miembro del dominio. La configuración IP se realizará mediante un contrato DHCP.

La cantidad de memoria asignada es de 2048 MB y el disco virtual de 30 GB está particionado con una única partición.

- **Nombre de equipo**: CL10-02
- **Contraseña del administrador local**: Pa$$w0rd

8. Máquina virtual SRV-RTR

Servidor miembro del dominio. Se instalarán distintos roles más adelante.

La cantidad de memoria asignada es de 2048 MB y el disco virtual de 60 GB, repartido en dos particiones. Este servidor virtual contiene dos interfaces, cada una conectada a un conmutador virtual distinto.

- **Nombre de equipo**: SRV-RTR

Tarjeta de red 1:

- **Dirección IP**: 172.16.255.254
- **Máscara de subred**: 255.255.0.0
- **Servidor DNS preferido**: 172.16.0.1

Tarjeta de red 2:

- **Dirección IP**: 172.17.255.254
- **Máscara de subred**: 255.255.0.0
- **Contraseña del administrador local**: Pa$$w0rd

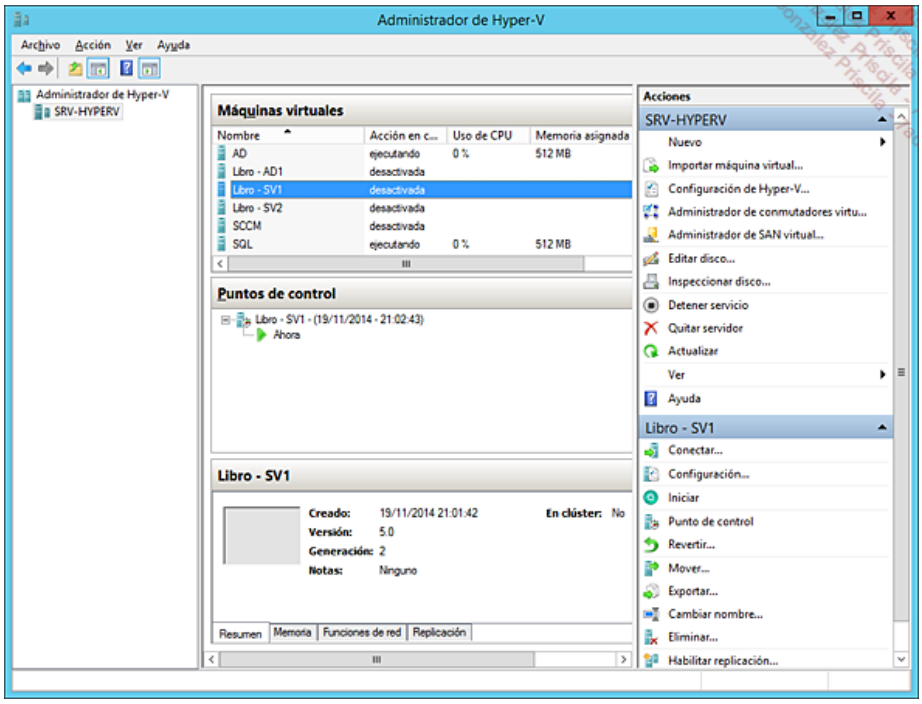
9. Las instantáneas

Las instantáneas permiten salvaguardar el estado de la máquina virtual. Es, así, posible restablecer la captura instantánea y volver con facilidad a un estado anterior.

Abra la consola **Administrador de Hyper-V**.

Haga clic con el botón derecho sobre la VM elegida y, a continuación, seleccione **Instantánea**.

En la consola aparece la captura instantánea.



Una vez realizada la misma operación sobre el conjunto de máquinas virtuales, es posible restaurar el estado de una o varias VM de la maqueta.

10. Método Diferencial

El conjunto de comandos y de scripts PowerShell utilizados en esta sección están disponibles para su descarga desde la página Información.

a. Configuración de PowerShell

En primer lugar, hay que preparar el entorno autorizando la ejecución de scripts PowerShell.

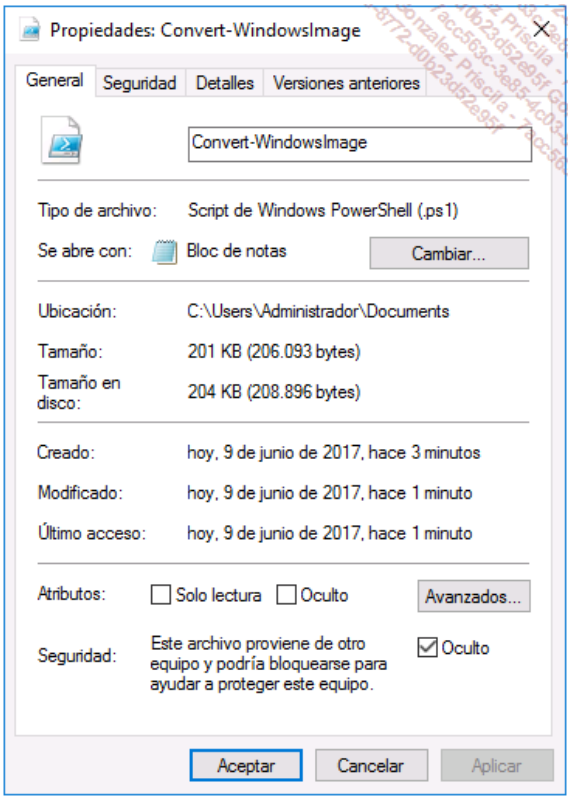
En una consola de comandos **PowerShell** abierta como **Administrador**:

```
Set-ExecutionPolicy RemoteSigned -Force
```

Recuperar el script PowerShell **convert-WindowsImage.ps1** del centro de scripts en la siguiente dirección: https://goo.gl/isVDjz

Aceptar el contrato de licencia y **abrir** la ubicación donde se haya descargado el archivo.

Hacer clic con el botón derecho en el archivo convert-windowsImage.ps1, seleccionar **Propiedades**, marcar la opción **Oculto** de la fila**Seguridad** y, a continuación, hacer clic en **Aceptar**.

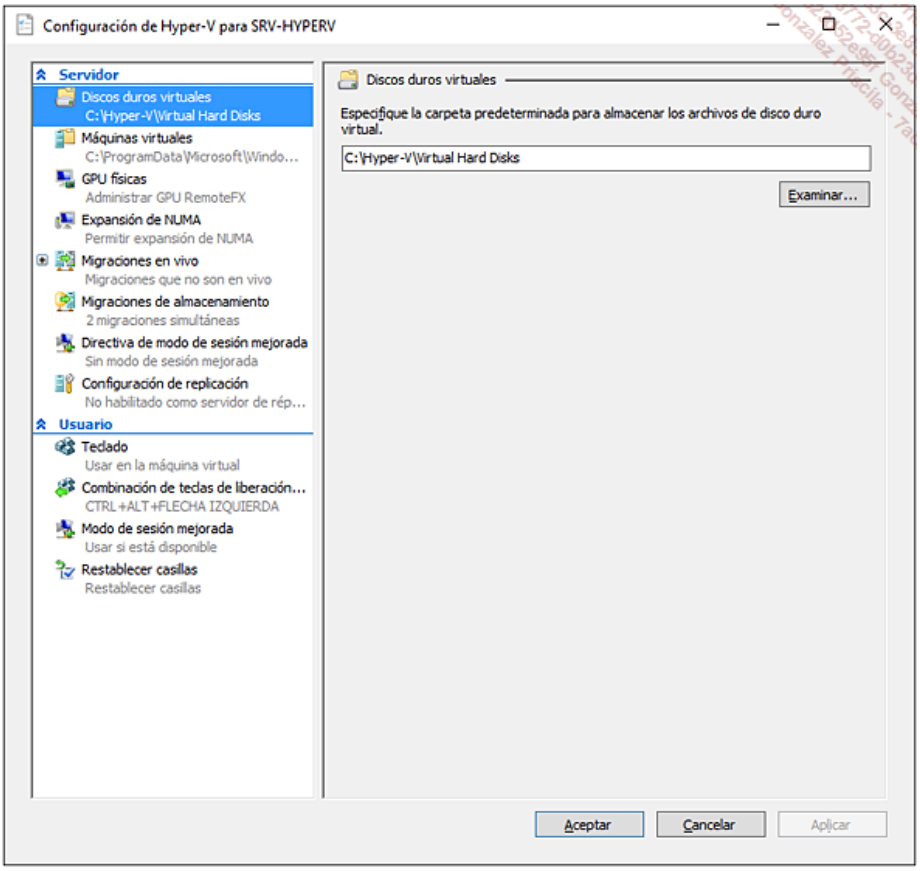


b. Configuración de Hyper-V

En una consola PowerShell, ejecute los siguientes comandos para crear el árbol de carpetas:

```
New-Item -Name Base -Path 'C:\Hyper-V\Virtual Hard Disks' -ItemType Directory
New-Item -Name ISO -Path C:\ -ItemType Directory
```

En la sección **Acciones** del administrador Hyper-V, haga clic en **Parámetros de Hyper-V**, y a continuación en **Discos duros virtuales**. Haga clic en **Examinar** y seleccione la ruta C:\Hyper-V\Virtual Hard Disks.



c. Creación de los discos padres

Vamos a presentar cómo utilizar el script PowerShell convert-WindowsImage.ps1. Copie las imágenes ISO de Windows Server 2016 y de Windows 10 Entreprise en la carpeta ISO.

Las versiones de evaluación pueden descargarse siguiendo los enlaces:

Windows 10: https://www.microsoft.com/es-es/evalcenter/evaluate-windows-10-enterprise

Windows Server 2016: https://www.microsoft.com/es-es/evalcenter/evaluate-windows-server-2016

Ejecute **Windows PowerShell ISE** y abra el archivo convert-WindowsImage.ps1.

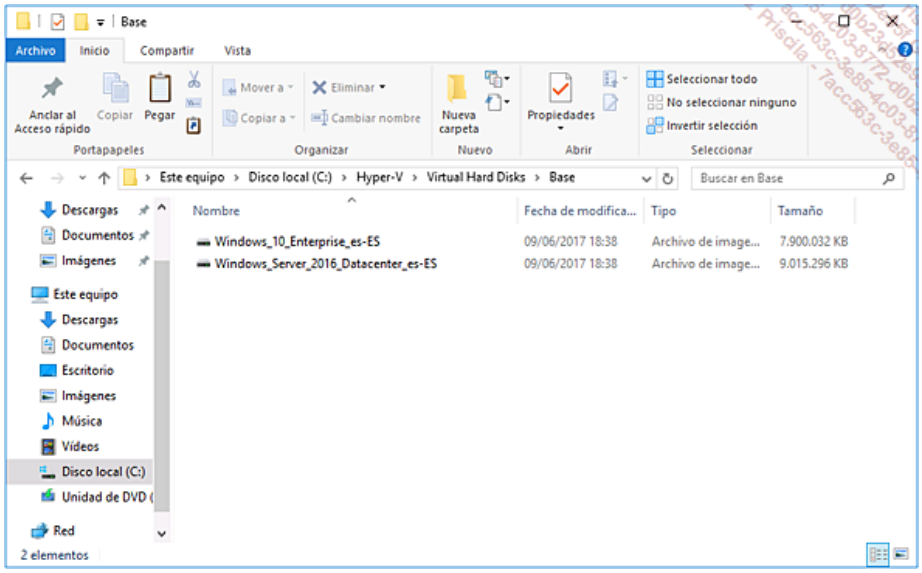
Ejecute el siguiente comando para la creación del disco padre de Windows Server 2016:

```
Convert-WindowsImage -SourcePath
C:\ISO\SW_DVD9_Win_Svr_STD_Core_and_DataCtr_Core_2016_64Bit_Spanish_-
2_MLF_X21-22829.ISO -Edicion ServerDataCenter -VHDType Dynamic -VHDFormat
VHDX -VHDPartitionStyle GPT -SizeBytes 60GB -VHDPath 'C:\Hyper-V\Virtual
Hard Disks\Base\Windows_Server_2016_Datacenter_es-ES.vhdx'
```

Ejecute el siguiente comando para la creación del disco padre de Windows 10 Enterprise:

```
Convert-WindowsImage -SourcePath
C:\ISO\es_windows_10_enterprise_version_1607_updated_jul_2016_x64_dvd_
9058241.iso -Edicion Entreprise -VHDType Dynamic -VHDFormat VHDX -
VHDPartitionStyle GPT -SizeBytes 60GB -VHDPath 'C:\Hyper-V\Virtual Hard
Disks\Base\Windows_10_Entreprise_es-ES.vhdx'
```

Una vez ejecutados ambos comandos, obtiene los discos duros padres presentes en la carpeta C:\Hyper-V\Virtual Hard Disks\Base.



11. Creación y configuración de la VM PAR-DC01

La máquina PAR-DC01 será el primer controlador de dominio del bosque Formacion.eni, poseerá los roles AD-DS y DNS.

Abra **Windows PowerShell ISE** y ejecute los siguientes comandos PowerShell para la creación del disco diferencial de la máquina:

```
$VMName = "PAR-DC01"
$VMMemory = 2048MB
$Location = "C:\Hyper-V\Virtual Hard Disks"
New-vhd New-VHD -ParentPath 'C:\Hyper-V\Virtual Hard
Disks\Base\Windows_Server_2016_Datacenter_es-ES.vhdx' -Path "$Location\
$VMName.vhdx" -SizeBytes 60GB -Differencing
```

Tras crear el disco duro diferencial, a continuación hay que crear la máquina virtual y asignarle el disco creado previamente.

Ejecute los siguientes comandos PowerShell para la creación de la máquina virtual:

```
New-VM -Name $VMName -Generation 2 -MemoryStartupBytes $VMMemory
-SwitchName MADRID -NoVHD -Verbose
Add-VMHardDiskDrive -VMName $VMName -Path "$Location\$VMname.vhdx" -Verbose
```

Ejecute los siguientes comandos PowerShell para modificar el orden de arranque de la máquina:

```
$BootOrder = Get-VMFirmware $VMName
$genNet = $BootOrder.BootOrder[0]
$genHD = $BootOrder.BootOrder[1]
$genNet
$genHD

Set-VMFirmware -VMName $VMName -BootOrder $genHD,$genNet
```

Ejecute el siguiente comando PowerShell para renombrar la máquina virtual y asignarle una dirección IPv4:

```
Invoke-Command -VMName $VMName -ScriptBlock {Rename-computer -ComputerName
$Env:COMPUTERNAME -NewName $VMName
New-netIPAddress -IPAddress 172.16.0.1 -PrefixLength 16 -InterfaceAlias
Ethernet0 -DefaultGateway 172.16.255.254
Set-DnsClientServerAddress -InterfaceAlias Ethernet0 -ServerAddresses 172.16.0.1
Restart-computer -Force} -Credential (Get-Credential -UserName Administrador
-Message 'Config VM')
```

12. Máquina virtual PAR-DC02

La máquina **PAR-DC02** será un controlador de dominio suplementario del bosque Formacion.eni, poseerá también los roles AD-DS y DNS.

Abra **Windows PowerShell ISE** y ejecute los siguientes comandos para la creación de un disco diferencial de la máquina:

```
$VMName = "PAR-DC02"
$VMMemory = 2048MB
$Location = "C:\Hyper-V\Virtual Hard Disks"
New-vhd New-VHD -ParentPath 'C:\Hyper-V\Virtual Hard
Disks\Base\Windows_Server_2016_Datacenter_es-ES.vhdx' -Path "$Location\
$VMName.vhdx" -SizeBytes 60GB -Differencing
```

Tras haber creado el disco duro diferencial, a continuación hay que crear la máquina virtual y asignarle el disco creado previamente.

Ejecute los siguientes comandos para la creación de la máquina virtual:

```
New-VM -Name $VMName -Generation 2 -MemoryStartupBytes $VMMemory -SwitchName
MADRID  -NoVHD -Verbose
Add-VMHardDiskDrive -VMName $VMName -Path "$Location\$VMname.vhdx" -Verbose
```

Ejecute los siguientes comandos para cambiar el orden de arranque de la máquina:

```
$BootOrder = Get-VMFirmware $VMName
$genNet = $BootOrder.BootOrder[0]
$genHD = $BootOrder.BootOrder[1]
$genNet
$genHD

Set-VMFirmware -VMName $VMName -BootOrder $genHD,$genNet
```

Ejecute el siguiente comando PowerShell para renombrar la máquina virtual y asignarle una dirección IPv4:

```
Invoke-Command -VMName $VMName -ScriptBlock {Rename-computer -ComputerName
$Env:COMPUTERNAME -NewName PAR-DC02
New-netIPAddress -IPAddress 172.16.0.2 -PrefixLength 16 -InterfaceAlias
Ethernet0 -DefaultGateway 172.16.255.254
Set-DnsClientServerAddress -InterfaceAlias Ethernet0 -ServerAddresses 172.16.0.1
Restart-computer -Force} -Credential (Get-Credential -UserName Administrador
-Message 'Config VM')
```

13. Máquina virtual PAR-SRV1

La máquina **PAR-SRV1** es un servidor miembro del dominio Formacion.eni.

Abra **Windows PowerShell ISE** y ejecute los siguientes comandos para la creación del disco diferencial de la máquina:

```
$VMName = "PAR-SRV1"
$VMMemory = 2048MB
$Location = "C:\Hyper-V\Virtual Hard Disks"
New-vhd New-VHD -ParentPath 'C:\Hyper-V\Virtual Hard
Disks\Base\Windows_Server_2016_Datacenter_es-ES.vhdx' -Path "$Location\
$VMName.vhdx" -SizeBytes 60GB -Differencing
```

Tras haber creado el disco duro diferencial, a continuación hay que crear la máquina virtual y asignarle el disco creado previamente.

Ejecute los siguientes comandos para la creación de la máquina virtual:

```
New-VM -Name $VMName -Generation 2 -MemoryStartupBytes $VMMemory -SwitchName
MADRID -NoVHD -Verbose
Add-VMHardDiskDrive -VMName $VMName -Path "$Location\$VMname.vhdx" -Verbose
```

Ejecute los siguientes comandos para cambiar el orden de arranque de la máquina virtual:

```
$BootOrder = Get-VMFirmware $VMName
$genNet = $BootOrder.BootOrder[0]
$genHD = $BootOrder.BootOrder[1]
$genNet
$genHD

Set-VMFirmware -VMName $VMName -BootOrder $genHD,$genNet
```

Ejecute el siguiente comando PowerShell para renombrar la máquina virtual y asignarle una dirección IPv4:

```
Invoke-Command -VMName $VMName -ScriptBlock {Rename-computer -ComputerName
$Env:COMPUTERNAME -NewName PAR-SRV1
New-netIPAddress -IPAddress 172.16.0.3 -PrefixLength 16 -InterfaceAlias
Ethernet0 -DefaultGateway 172.16.255.254
Set-DnsClientServerAddress -InterfaceAlias Ethernet0 -ServerAddresses 172.16.0.1
Restart-computer -Force} -Credential (Get-Credential -UserName Administrador
-Message 'Config VM')
```

14. Máquina virtual PAR-SRV2

La máquina **PAR-SRV2** es un servidor miembro del dominio Formacion.eni.

Abra **Windows PowerShell ISE** y ejecute los siguientes comandos para la creación del disco diferencial de la máquina:

```
$VMName = "PAR-SRV2"
$VMMemory = 2048MB
$Location = "C:\Hyper-V\Virtual Hard Disks"
New-vhd New-VHD -ParentPath 'C:\Hyper-V\Virtual Hard
Disks\Base\Windows_Server_2016_Datacenter_es-ES.vhdx' -Path "$Location\
$VMName.vhdx" -SizeBytes 60GB -Differencing
```

Tras haber creado el disco duro diferencial, a continuación hay que crear la máquina virtual y asignarle el disco creado previamente.

Ejecute los siguientes comandos para la creación de la máquina virtual:

```
New-VM -Name $VMName -Generation 2 -MemoryStartupBytes $VMMemory
-SwitchName MADRID  -NoVHD -Verbose
Add-VMHardDiskDrive -VMName $VMName -Path "$Location\$VMname.vhdx" -Verbose
```

Ejecute los siguientes comandos para cambiar el orden de arranque de la máquina virtual:

```
$BootOrder = Get-VMFirmware $VMName
$genNet = $BootOrder.BootOrder[0]
$genHD = $BootOrder.BootOrder[1]
$genNet
$genHD

Set-VMFirmware -VMName $VMName -BootOrder $genHD,$genNet
```

Ejecute el siguiente comando PowerShell para renombrar la máquina virtual y asignarle una dirección IPv4:

```
Invoke-Command -VMName $VMName -ScriptBlock {Rename-computer -ComputerName
$Env:COMPUTERNAME -NewName PAR-SRV2
New-netIPAddress -IPAddress 172.16.0.4 -PrefixLength 16 -InterfaceAlias
Ethernet0 -DefaultGateway 172.16.255.254
Set-DnsClientServerAddress -InterfaceAlias Ethernet0 -ServerAddresses 172.16.0.1
Restart-computer -Force} -Credential (Get-Credential -UserName Administrador
-Message 'Config VM')
```

15. Máquina virtual SRV-RTR

La máquina **SRV-RTR** es un servidor autónomo que realiza las tareas de un router o enrutador.

Abra **Windows PowerShell ISE** y ejecute los siguientes comandos para la creación del disco diferencial de la máquina:

```
$VMName = "SRV-RTR"
$VMMemory = 2048MB
$Location = "C:\Hyper-V\Virtual Hard Disks"
New-vhd New-VHD -ParentPath 'C:\Hyper-V\Virtual Hard
Disks\Base\Windows_Server_2016_Datacenter_es-ES.vhdx' -Path "$Location\
$VMName.vhdx" -SizeBytes 60GB -Differencing
```

Tras haber creado el disco duro diferencial, a continuación hay que crear la máquina virtual y asignarle el disco creado previamente.

Ejecute los siguientes comandos para la creación de la máquina virtual:

Ejecute el siguiente comando para agregar una tarjeta de red a la máquina en la red **BARCELONA**:

```
New-VM -Name $VMName -Generation 2 -MemoryStartupBytes $VMMemory -SwitchName
MADRID  -NoVHD -Verbose
Add-VMHardDiskDrive -VMName $VMName -Path "$Location\$VMname.vhdx" -Verbose
```

```
Add-VMNetworkAdapter -VMName $VMName -SwitchName BARCELONA
```

Ejecute los siguientes comandos para cambiar el orden de arranque de la máquina virtual **SRV-RTR**.

```
$BootOrder = Get-VMFirmware $VMName
$genNet = $BootOrder.BootOrder[0]
$genHD = $BootOrder.BootOrder[1]
$genNet
$genHD

Set-VMFirmware -VMName $VMName -BootOrder $genHD,$genNet
```

Ejecute el siguiente comando PowerShell para renombrar la máquina virtual y asignarle una dirección IPv4:

```
Invoke-Command -VMName $VMName -ScriptBlock {Rename-computer -ComputerName
$Env:COMPUTERNAME -NewName SRV-RTR
New-netIPAddress -IPAddress 172.16.255.254 -PrefixLength 16 -InterfaceAlias
Ethernet0
New-netIPAddress -IPAddress 172.17.255.254 -PrefixLength 16 -InterfaceAlias
Ethernet1
Restart-computer -Force} -Credential (Get-Credential -UserName Administrador
-Message 'Config VM')
```

16. Máquinas virtuales CL10-01 y 02

Las máquinas clientes Windows 10 están unidas al dominio Formacion.eni.

Abra **Windows PowerShell ISE** y ejecute los siguientes comandos para la creación del disco diferencial de la máquina:

```
$VMName = "CL10-01"
$VMMemory = 2048MB
$Location = "C:\Hyper-V\Virtual Hard Disks"
New-vhd New-VHD -ParentPath 'C:\Hyper-v\Virtual Hard
Disks\Base\Windows_10_Entreprise_es-ES.vhdx' -Path "$Location\$VMName.vhdx"
-SizeBytes 60GB -Differencing
```

Tras haber creado el disco duro diferencial, a continuación hay que crear la máquina virtual y asignarle el disco creado previamente.

Ejecute los siguientes comandos para la creación de la máquina virtual:

```
New-VM -Name $VMName -Generation 2 -MemoryStartupBytes $VMMemory -SwitchName
MADRID -NoVHD -Verbose
Add-VMHardDiskDrive -VMName $VMName -Path "$Location\$VMname.vhdx" -Verbose
```

Ejecute los siguientes comandos para cambiar el orden de arranque de la máquina virtual:

```
$BootOrder = Get-VMFirmware $VMName
$genNet = $BootOrder.BootOrder[0]
$genHD = $BootOrder.BootOrder[1]
$genNet
$genHD

Set-VMFirmware -VMName $VMName -BootOrder $genHD,$genNet
```

Para la máquina virtual **CL10-02**.

Ejecute los siguientes comandos para la creación del disco diferencial de la máquina:

```
$VMName = "CL10-02"
$VMMemory = 2048MB
$Location = "C:\Hyper-V\Virtual Hard Disks"
```

```
New-vhd New-VHD -ParentPath 'C:\Hyper-v\Virtual Hard
Disks\Base\Windows_10_Entreprise_es-ES.vhdx' -Path "$Location\$VMName.vhdx"
-SizeBytes 60GB -Differencing
```

Tras haber creado el disco duro diferencial, a continuación hay que crear la máquina virtual y asignarle el disco creado previamente.

Ejecute los siguientes comandos para la creación de la máquina virtual:

```
New-VM -Name $VMName -Generation 2 -MemoryStartupBytes $VMMemory -SwitchName
MADRID -NoVHD -Verbose
Add-VMHardDiskDrive -VMName $VMName -Path "$Location\$VMname.vhdx" -Verbose
```

Ejecute los siguientes comandos para cambiar el orden de arranque de la máquina virtual:

```
$BootOrder = Get-VMFirmware $VMName
$genNet = $BootOrder.BootOrder[0]
$genHD = $BootOrder.BootOrder[1]
$genNet
$genHD

Set-VMFirmware -VMName $VMName -BootOrder $genHD,$genNet
```

17. Configuración de la memoria dinámica

El conjunto de máquinas virtuales se configurarán para utilizar la asignación dinámica de la memoria RAM. Cada una de ellas dispondrá de un mínimo de 512 MB, de 1 GB en el arranque y podrá utilizar hasta 2 GB, salvo para los servidores miembros y los controladores de dominio cuyo máximo alcanzará los 3 GB. Los clientes y el router tendrán una prioridad del 50 %, los controladores de dominio tendrán una prioridad del 80 % y los servidores miembros tendrán una prioridad del 60 %.

```
Get-VM | % {
$VMname = $_.Name
switch ($VMname)
{
{$VMname -like "CL*"} {Write-Host "Config Dynamic Memory for $VMname"
-ForegroundColor Cyan;Set-VMMemory $VMname -DynamicMemoryEnabled $true
-MinimumBytes 512MB -StartupBytes 1024MB -MaximumBytes 2GB -Priority 50
-Buffer 25}
{$VMname -like "*DC*"} {Write-Host "Config Dynamic Memory for $VMname"
-ForegroundColor Yellow;Set-VMMemory $VMname -DynamicMemoryEnabled $true
-MinimumBytes 512MB -StartupBytes 1024MB -MaximumBytes 3GB -Priority 80
-Buffer 25}
{$VMname -like "PAR-SRV*"} {Write-Host "Config Dynamic Memory for $VMname"
-ForegroundColor Green;Set-VMMemory $VMname -DynamicMemoryEnabled $true
-MinimumBytes 512MB -StartupBytes 1024MB -MaximumBytes 3GB -Priority 60
-Buffer 25}
{$VMname -like "SRV-*"} {Write-Host "Config Dynamic Memory for $VMname"
-ForegroundColor Red;Set-VMMemory $VMname -DynamicMemoryEnabled $true
-MinimumBytes 512MB -StartupBytes 1024MB -MaximumBytes 2GB -Priority 50
-Buffer 25}
Default {}}}
```

18. Creación de un punto de control

A continuación vamos a crear un punto de control para el conjunto de máquinas virtuales que acabamos de crear, de modo que en cualquier momento sea posible volver a un estado previo y realizar de nuevo los ejercicios para entrenarnos.

En su servidor Hyper-V, abra una consola de comandos PowerShell o PowerShell ISE y ejecute los siguientes comandos:

```
$VMname = ("PAR-DC01","PAR-DC02","PAR-SRV1","PAR-SRV2","SRV-RTR",
"CL10-01","CL10-02")
foreach ($item in $VMname)
{
CHECKPOINT-VM -Name $item -Snapshotname "Initial_LAB"
}
```

19. Configuración posinstalación

Las etapas de configuración complementarias (instalación de Active Directory, unión de las máquinas al dominio Formacion.eni) pueden realizarse mediante un script PowerShell disponible para su descarga desde la página Información.

Requisitos previos y objetivos

1. Requisitos previos

Poseer conocimientos acerca del direccionamiento IP.

Poseer nociones acerca de los protocolos y la pila TCP/IP.

2. Objetivos

Ser capaz de planificar y construir un plan de direccionamiento IP.

Ser capaz de configurar un equipo con una dirección IPv4.

Ser capaz de resolver problemas y administrar la conectividad de red.

Ser capaz de configurar un equipo con una dirección IPv6.

Ser capaz de implementar la transición a IPv6.

Planificar el direccionamiento IPv4

Es importante para un administrador de red comprender el funcionamiento del direccionamiento IPv4. Comprendiendo el direccionamiento, las máscaras de subred y las puertas de enlace predeterminadas será capaz de gestionar, resolver problemas y hacer evolucionar su red.

1. Las direcciones IPv4

El direccionamiento es una de las funciones principales de los protocoles de la capa de red. Permite implementar la transmisión de datos entre hosts situados en una misma red o en dos redes diferentes. La versión 4 (IPv4) y la versión 6 (IPv6) del protocolo IP proporcionan un direccionamiento jerárquico para los paquetes que transportan los datos.

La elaboración, la implementación y la administración de un modelo de direccionamiento IP garantizan un funcionamiento óptimo de las redes.

Este capítulo describe con detalle la estructura de las direcciones IP y su aplicación en la creación y la prueba de redes y de subredes IP.

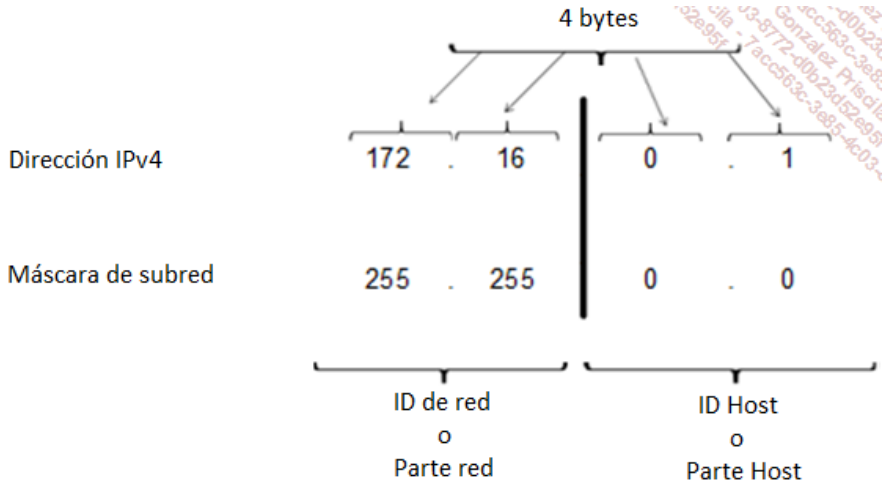
a. Principio de funcionamiento

Una dirección IPv4 posee una longitud de 32 bits, es decir, 4 bytes de 8 bits (1 byte = 8 bits). Cada byte está separado por puntos y escrito de forma decimal (de 0 a 255). Se habla de un formato **decimal punteado**.

Una dirección IP es un identificador **único** que permite reconocer un puesto en la red (de la misma manera que un número de la Seguridad Social es también un identificador único, que identifica a un hombre o una mujer). Esta dirección puede configurarse de forma manual o automática, y asignarse a cualquier interfaz de red que realice la petición.

Una dirección IP por sí sola no puede interpretarse y leerse correctamente, de modo que nos vemos obligados a asociarle una máscara de subred que va a determinar la parte **red** de la dirección (ID de la red) y la parte **host** (ID único).

Tomemos como ejemplo un puesto que posea la dirección IP 172.16.0.1 y una máscara de subred 255.255.0.0.



b. El modo binario

Para comprender el funcionamiento de los dispositivos de red, hay que estudiar las direcciones, aunque un ordenador solo las podrá interpretar de manera binaria. La notación binaria es una representación de información que utiliza únicamente 1 y 0. Los ordenadores se comunican mediante datos binarios.

Los datos binarios pueden utilizarse para representar numerosos tipos de datos. Por ejemplo, cuando escribe en un teclado, las letras aparecen por pantalla en un formato que puede leer y comprender. Sin embargo, el ordenador convierte cada letra en una serie de cifras binarias para el almacenamiento y el transporte. Para realizar esta conversión, el ordenador utiliza el código ASCII (*American Standard Code for Information Interchange*).

Por lo general, no es necesario conocer la conversión binaria de las letras; sin embargo, resulta muy importante comprender el uso del formato binario para las direcciones IP. Cada dispositivo de una red debe poder ser identificado mediante una dirección binaria única. En las redes IPv4, esta dirección se representa mediante una cadena de 32 bits (compuesta de 1 y de 0). A nivel de la capa de red, los paquetes incluyen esta información de identificación única para los sistemas de origen y de destino. Por consiguiente, en una red IPv4, cada paquete incluye una dirección de origen de 32 bits y una dirección de destino de 32 bits en el encabezado de capa 3.

Para la mayoría de los usuarios, es difícil interpretar una cadena de 32 bits y es todavía más difícil memorizarla. Por este motivo, representamos las direcciones IPv4 en formato decimal punteado y no en formato binario. Por ello, tratamos cada byte como un número decimal comprendido en un rango de 0 a 255. Para comprender este proceso, es necesario poseer ciertos conocimientos en materia de conversión de números binarios a números decimales.

c. Numeración ponderada

Para dominar la conversión entre los números binarios y decimales, conviene comprender el sistema de numeración llamado numeración

ponderada. En numeración ponderada, un dígito puede representar distintos valores según la posición que ocupa. En el sistema decimal, la base es **10**. En el sistema binario, utilizaremos la **base 2**. En particular, el valor que una cifra representa es la cifra multiplicada por la base elevada a la potencia correspondiente a su posición. Algunos ejemplos nos permitirán comprender mejor el funcionamiento de este sistema.

Para el número decimal 172, el valor que la cifra 1 representa es 1*10^2 (1 vez 10 elevado a 2). El 1 se encuentra en la posición llamada "centena". La numeración ponderada hace referencia a esta posición como la posición base^2, pues la base es 10 y la potencia es 2. La cifra 7 representa 7*10^1 (7 veces 10 elevado a 1).

En la numeración ponderada en base 10, 172 representa:

*172 = (1 * 10^2) + (7 * 10^1) + (2 * 10^0)*

o

*172 = (1 * 100) + (7 * 10) + (2 * 1)*

d. Sistema binario

En el sistema binario, la base es 2. Por consiguiente, cada posición representa una suma de la potencia de 2. En los números binarios de 8 bits, el sistema en base 2 solo comprende dos cifras: 0 y 1.

Base	2	2	2	2	2	2	2	2
Exponente	7	6	5	4	3	2	1	0
Valores de los bits	128	64	32	16	8	4	2	1
Dirección binaria	1	0	1	0	1	1	0	0
Valores binarios de los bits	128		32		8	4		

Si se suman los valores binarios de los bits (128 + 32 + 8 + 4), obtenemos 172. Acabamos de convertir el número 172 a binario: 10101100.

2. Conversión binario/decimal

a. Binario/decimal

Si se descompone un byte, se da cuenta que este último posee 8 bits, cada uno de estos bits posee un rango. El peso débil, situado más a la derecha, posee el rango 0 (como vemos a continuación). El peso fuerte, el situado más a la izquierda, posee el rango 8. Para obtener el valor decimal de cada rango, es necesario elevar 2 a la potencia del rango del bit.

De este modo, el bit que tiene rango 0 posee el valor decimal 1, pues $2^0 = 1$, el que tiene rango 1 posee el valor 2, pues $2^1 = 2$...

7	6	5	4	3	2	1	0
128	64	32	16	8	4	2	1

Para realizar la conversión binario/decimal, es preciso sumar los valores decimales correspondientes a los bits configurados a 1.

Si un byte posee el valor binario 0100 1001, tiene como valor decimal 73.

Los bits configurados a 1 se corresponden con los de rango 0, 3 y 6, que equivale a 1 + 8 + 64, es decir, 73.

b. Conversión decimal/binario

Esta conversión es más complicada; para explicarla utilizaremos un ejemplo: el valor 102 debe convertirse a binario. Para realizar la conversión, vamos a utilizar la resta.

Para realizar la conversión, conviene empezar por el bit de peso más fuerte, que en este caso se corresponde con el rango 7.

El valor decimal del rango 7 es igual a 128; este valor es mayor que 102. No podemos efectuar la resta. El valor binario del rango 7 es, por lo tanto, igual a 0.

El valor decimal del rango 6 es igual a 64; este valor es menor que 102. El valor binario del rango 6 es, por lo tanto, igual a 1. Queda por convertir el número 38 (102-64).

El valor decimal del rango 5 es igual a 32; este valor es menor que 38. El valor binario del rango 5 es, por lo tanto, igual a 1. Queda por convertir el número 6 (38-32).

El valor decimal del rango 4 es igual a 16; este valor es mayor que 6. El valor binario del rango 4 es, por lo tanto, igual a 0.

El valor decimal del rango 3 es igual a 8; este valor es mayor que 6. El valor binario del rango 3 es, por lo tanto, igual a 0.

El valor decimal del rango 2 es igual a 4; este valor es inferior a 6. El valor binario del rango 2 es, por lo tanto, igual a 1. Queda por convertir el número 2 (6-4).

El valor decimal del rango 1 es igual a 2; este valor es igual a 2. El valor binario del rango 1 es, por lo tanto, igual a 1.

De modo que hemos convertido el número 102, el valor binario del rango 0 vale 0.

El valor decimal 102 se ha convertido en el número binario 0110 0110.

3. Clases de direcciones IPv4

La RFC 1700 agrupa los rangos de monodifusión según diversos tamaños, llamados direcciones de clase A, B y C. Establece a su vez direcciones de clase D (multidifusión) y de clase E (experimentales).

Las clases de direcciones de monodifusión A, B y C definen redes de tamaño específico y bloques de direcciones específicas para estas redes. Una empresa o una organización obtendrán un rango completo de bloques de direcciones de clase A, B o C. El uso del espacio de direccionamiento se denominará direccionamiento por clase.

a. Clase A

Un bloque de direcciones de **clase A** se crea para gestionar redes de gran tamaño, que contengan más de **16 millones de direcciones** de host. Las direcciones IPv4 de clase A utilizan un prefijo /8 invariable, el primer byte indica la dirección de la red. Los tres bytes siguientes se corresponden con las direcciones de los hosts. Todas las direcciones de clase A requieren que el bit de mayor peso valga cero. Esto implica que no haya más de 128 redes de clase A disponibles, de 0.0.0.0/8 a 127.0.0.0/8. Incluso aunque las direcciones de clase A reservan la mitad del espacio al direccionamiento, solo pueden asignarse a 120 empresas u organizaciones, debido a su límite de **128 redes**.

Las direcciones cuyo primer byte es igual a 127 no pueden utilizarse, puesto que se corresponden con una dirección de bucle invertido.

b. Clase B

El espacio de direccionamiento de **clase B** existe para responder a las necesidades de aquellas redes de tamaño medio o de gran tamaño, que contienen hasta **65.000 hosts**. Las direcciones IP de clase B utilizan los dos primeros bytes para indicar la dirección de red. Los dos bytes siguientes se corresponden con las direcciones de los hosts. Como con la clase A, el espacio de direccionamiento para las clases de direcciones restantes debería estar reservado. En las direcciones de clase B, los dos bytes de mayor peso del primer byte valen 10. Esto limita el bloque de direcciones de clase B de 128.0.0.0/16 a 191.255.0.0/16. La clase B asigna las direcciones de una manera más eficaz que la clase A, pues reparte de manera equitativa el 25 % del espacio de direccionamiento IPv4 total de unas **16.000 redes**.

c. Bloques de direcciones C

El espacio de direccionamiento de la **clase C** era el más habitual en las antiguas clases de direcciones, destinado a redes de pequeño tamaño, que contuvieran un máximo de 254 hosts. Los bloques de direcciones de clase C utilizan el prefijo /24; de este modo, una red de clase C no puede utilizar más que el último byte para las direcciones de los hosts, los tres primeros bytes se corresponden con la dirección de la red. Los bloques de direcciones de clase C reservan el espacio de direccionamiento mediante un valor fijo de 110 para los tres bits de mayor peso del primer byte. Esto limita el bloque de direcciones de clase C de 192.0.0.0/24 a 223.255.255.0/24. Si bien ocupa solo el 12,5 % del espacio de direccionamiento IPv4, puede asignar direcciones a 2 millones de redes.

d. Direcciones especiales

Como en toda red, existen direcciones que tanto los equipos como los hosts de la red no pueden utilizar. Estas direcciones son dos y siempre poseen las mismas características, que son: la dirección de red, que representa la primera dirección IP de la red y la dirección de difusión o broadcast, que es la última dirección IP de una red.

Dirección de la red

Para identificar una dirección de red, hay que convertir la dirección en binario y, si todos los bits de la parte host valen 0, entonces es una dirección de red.

Ejemplo: tomemos la dirección 172.16.0.0 con una máscara de subred igual a 255.255.255.0.

Podemos observar que la máscara de subred identifica la parte de la red correspondiente a los tres primeros bytes y la parte host correspondiente al cuarto byte. En este caso, no tenemos por qué convertir a binario la parte host para saber que esta dirección es una dirección de red.

Dirección de difusión

Para identificar una dirección de red, hay que convertir la dirección en binario y, si todos los bits de la parte host valen 1, entonces es una dirección de difusión.

Ejemplo: tomemos la dirección 192.168.255.255 con una máscara de subred igual a 255.255.255.0.

Podemos observar que la máscara de subred identifica la parte de la red correspondiente a los tres primeros bytes y la parte host correspondiente al cuarto byte.

Convirtamos el 4.º byte a binario:

255 = 11111111

Se trata por tanto de una dirección de difusión, pues todos los bits de la parte host valen 1.

e. Resumen

La siguiente tabla resume las diferentes clases de direcciones IPv4:

Clase	Primer byte en decimal	Bits del primer byte	Parte red (R) y host (H) de la dirección	Máscara de subred por defecto	Número de redes y de hosts posible por red
A	1 - 127	**0**0000000-**0**1111111	R.H.H.H	255.0.0.0	128 redes (2^7) 16.777.214 hosts por red ((2^24)-2)
B	128 - 191	**10**000000-**10**111111	R.R.H.H	255.255.0.0	16.384 redes (2^14) 65.534 hosts por red ((2^16)-2)
C	192 - 223	**110**00000-**110**11111	R.R.R.H	255.255.255.0	2.097.152 redes (2^21) 254 hosts por red ((2^8)-2)
D	224 - 239	**1110**0000-**1110**1111	Dirección multidifusión		
E	240 - 255	**1111**0000-**1111**1111	Experimental		

En la tercera columna de la tabla, los bits en negrita no cambian nunca.

4. Direccionamiento privado/público IPv4

La fuerte demanda de direcciones IP debida a la democratización de la microinformática ha obligado a la creación de una nueva norma. La RFC 1918 (o direccionamiento privado) se ha creado para paliar el riesgo de escasez de direcciones IPv4. Esta escasez es, actualmente, efectiva y se ha normalizado un nuevo protocolo IP (IPv6).

Las direcciones privada y pública poseen, cada una, una utilidad diferente en un sistema de información.

La dirección IP pública se utiliza en la red Internet, es única en el mundo y está distribuida por organismos especializados. Estas direcciones se denominan enrutables en Internet y se compran o alquilan a proveedores de acceso a Internet. Todo router o módem-router (Livebox…) utilizado por una empresa o un particular para acceder a Internet posee una dirección IP pública y es potencialmente alcanzable desde el exterior.

Los puestos informáticos situados en una red de área local utilizan, por su parte, una dirección IP privada. Esta última no es enrutable desde Internet (ningún equipo en una red pública posee una dirección así), de modo que lo es únicamente dentro de una red de área local. Dos empresas diferentes cuyas redes no están unidas pueden poseer de esta manera el mismo direccionamiento.

Tras la creación de esta norma, los pools de direcciones IP públicas se han reservado para el direccionamiento de los puestos en una red de área local. De este modo, cada clase posee su lote de direcciones reservadas:

Clase A: 10.0.0.0 a 10.255.255.255

Clase B: 172.16.0.0 a 172.31.255.255

Clase C: 192.168.0.0 a 192.168.255.255

5. CIDR

La notación CIDR (*Classless Inter-Domain Routing*) permite escribir de una manera sintética la máscara de subred. Por convención se indica el número de bits a 1 en la máscara de subred.

Una máscara de subred válida es siempre una serie de bits a 1 seguida de una serie de bits a 0.

De esta manera, si recuperamos las máscaras de subred por defecto y por clase, obtenemos las siguientes máscaras de subred:

Clase A: 255.0.0.0 - **/8**

Clase B: 255.255.0.0 - **/16**

Clase C: 255.255.255.0 - **/24**

Subredes

Una subred consiste en dividir una red informática en varias subredes. La máscara de subred se utiliza para identificar la red sobre la que está conectada la máquina. Como una dirección IP, está compuesta de cuatro bytes donde los bits de la IP de la red están configurados todos a 1 (valor decimal 255) o configurados a 0 para el ID del host (valor decimal 0).

En las redes de gran tamaño, es posible utilizar los bits del IP de host para crear subredes. Se utilizan el primer byte y los bits de mayor peso (los primeros empezando por la izquierda), esto reduce el número de hosts direccionables. Tenemos máscaras de subred de longitud variable VLSM (*Variable Length Subnet Mask*).

El objetivo es encontrar la máscara de subred que mejor se adapte al número de máquinas situadas en la red para optimizar de una manera más eficaz el espacio de direccionamiento.

1. Ventaja de las subredes

La ventaja de las subredes es poder realizar una división lógica de la red física para impedir a ciertas máquinas físicas que se comuniquen entre sí; el objetivo es crear redes diferentes.

Es posible utilizar varias subredes entre sitios remotos. Cada sitio puede, de este modo, tener su propio direccionamiento manteniendo el mismo IP de red. La división lógica permite reducir el tráfico de red y las tramas de tipo broadcast, y necesita un router para vincularlas.

También es posible prohibir el acceso de una red a otra (por ejemplo, la red de producción no puede acceder a la red de gestión). De este modo, la seguridad está asegurada; esta operación requiere sin embargo un cortafuegos para trabajar con seguridad.

2. ¿Cómo calcular una subred?

Para calcular un número de subred tenemos dos posibilidades: o bien dividimos una red existente en n redes del mismo tamaño, o bien dividimos una red existente en n redes de distinto tamaño. El método es el mismo en ambos casos.

a. Método que hay que utilizar

Para ello hay que identificar el número de bits de la parte host que vamos a utilizar. Se utiliza la siguiente fórmula: **2^n ≥ número de subredes**.

Hay que referirse a la siguiente tabla que nos permite encontrar el número de bits que hay que utilizar.

7	6	5	4	3	2	1	0
128	64	32	16	8	4	2	1

Abreviaciones utilizadas:

- Dirección de red: @R
- Dirección IPv4 binaria: @IP
- Dirección de difusión o broadcast: @B
- Nueva máscara en binario: Nmb

Tomemos como ejemplo el siguiente caso: queremos dividir la red 172.16.0.0 /16 en tres redes.

- **1.ª etapa**: cálculo del número de bits que hay que utilizar, con tres posibilidades de la fórmula $2^n \geq 3$, cuyo resultado es n = 2, pues 2^2 es igual o mayor que 3. Vamos a utilizar, por tanto, 2 bits de la parte host para identificar nuestras subredes.
- **2.ª etapa**: cálculo de la nueva máscara en binario. La máscara se indica en notación CIDR /16.
  - Máscara en binario: 11111111 . 11111111 . 00000000 . 00000000
  - Nueva máscara en binario: 11111111 . 11111111. 11000000 . 00000000, es decir, una máscara en /18
- **3.ª etapa**: cálculo de la primera red con la máscara en /18. Se utilizan definiciones de dos direcciones especiales que caracterizan una red (dirección de red y dirección de difusión).
  - @IP: 10101100.00010000.00000000.00000000
  - Nmb: 11111111.11111111.11000000.00000000
  - @R1: 10101100.00010000.00000000.00000000, es decir, **172.16.0.0 /18**
  - @B1: 10101100.00010000.00111111.11111111, es decir, **172.16.63.255 /18**

Nuestra primera red empieza en **172.16.0.0** y termina en **172.16.63.255** con una máscara en **/18**.

Debemos reutilizar el método para encontrar las dos redes siguientes con una máscara **/18**.

- Para encontrar la dirección de red siguiente, utilizamos la dirección de broadcast de la red n.° 1 a la que se agrega 1 en binario.
  - @B1: 10101100.00010000.00111111.11111111 se agrega 1

- Nmb: 11111111.11111111.11000000.00000000
- @R2: 10101100.00010000.01000000.00000000, es decir, **172.16.64.0 /18**
- @B2: 10101100.00010000.01111111.11111111, es decir, **172.16.127.255 /18**

Nuestra segunda red empieza en **172.16.64.0** y termina en **172.16.127.255** con una máscara **/18**.

- Para encontrar la dirección de red siguiente, utilizamos la dirección de broadcast de la red n.° 2 a la que se agrega 1 en binario.
  - @B2: 10101100.00010000.01111111.11111111 se agrega 1
  - Nmb: 11111111.11111111.11000000.00000000
  - @R3: 10101100.00010000.10000000.00000000, es decir, **172.16.128.0 /18**
  - @B3: 10101100.00010000.10111111.11111111, es decir, **172.16.191.255 /18**

Nuestra tercera red empieza en **172.16.128.0** y termina en **172.16.191.255** con una máscara **/18**.

Recuerde que las direcciones de red y las direcciones de broadcast no pueden asignarse a un host o a un dispositivo de interconexión.

b. Subredes de máscaras variables VLSM

Tenemos la posibilidad de crear redes o subredes con tamaños (ID hosts) idénticos, y a continuación introduciremos la noción de máscara de longitud variable. Tomemos como ejemplo la compañía ABC, que desea crear varias redes de distinto tamaño. Para abordar este ejemplo vamos a utilizar el siguiente método, optimizando las máscaras de subred.

La compañía ABC desea dividir su red de la siguiente manera:

- 1 red que puede contener 60 direcciones
- 1 red que puede contener 250 direcciones
- 1 red que puede contener 30 direcciones
- 1 red que puede contener 2 direcciones

La red que hay que dividir es la red 10.0.0.0 / 8.

Abreviaturas utilizadas:

- Dirección de red: @R
- Dirección IPv4 en binario: @IP
- Dirección de difusión o broadcast: @B
- Nueva máscara en binario: Nmb
- **1.ª etapa**: esta vez, tenemos que calcular el número de bits de la parte host para cada red.

Empezamos siempre por las redes que contienen el mayor número de hosts.

Se calcula que n es el número de bits de la parte host con la siguiente fórmula:

(2^n) - 2 □ que el número de direcciones deseado, es decir, (2^n) - 2 □ 250, o sea n = 8.

Necesitamos una máscara de subred con 8 bits para la parte host.

- **2.ª etapa**: cálculo de la nueva máscara en binario. Restamos el número de bits encontrados del número total de bits de una máscara IPv4, es decir, 32 - 8 = 24 bits.
  - Máscara en binario: 11111111 . 00000000. 00000000 . 00000000
  - Nueva máscara en binario: 11111111 . 11111111. 11111111 . 0000000, es decir, una máscara /24
- **3.ª etapa**: cálculo de la primera red con la máscara /24. Se utilizan las definiciones de las dos direcciones especiales que caracterizan una red (dirección de red y dirección de difusión).
  - @IP: 00001010.00000000.00000000.00000000
  - Nmb: 11111111.11111111.11111111.00000000
  - @R1: 00001010.00000000.00000000.00000000, es decir, **10.0.0.0 /24**
  - @B1: 00001010.00000000.00000000.11111111, es decir, **10.0.0.255 /24**

Nuestra primera red empieza, por tanto, en **10.0.0.0**, y termina en **10.0.0.255** con una máscara **/24**.

Debemos recalcular nuestra máscara de subred para una red de 60 puestos.

Se calcula que n es el número de bits de la parte host con la siguiente fórmula:

(2^n) - 2 □ 60, n = 6

Necesitamos una máscara de subred con 6 bits para la parte host.

- **4.ª etapa**: cálculo de la nueva máscara en binario, es decir, 32 - 6 = 26 bits.
  - Nueva máscara en binario: 11111111 . 11111111. 11111111 . 1100000, es decir, una máscara /26
- Para encontrar la dirección de red siguiente, utilizamos la dirección de broadcast de la red n.º 1 a la que se agrega 1 en binario.
  - @B1: 00001010.00000000.00000000.11111111 se agrega 1
  - Nmb: 11111111.11111111.11111111.1100000
  - @R2: 00001010.00000000.00000001.00000000, es decir, **10.0.1.0 /26**
  - @B2: 00001010.00000000.00000001.00111111, es decir, **10.0.1.63 /26**

Nuestra segunda red empieza, por tanto, en **10.0.1.0**, y termina en **10.0.1.63** con una máscara **/26**.

Debemos recalcular nuestra máscara de subred para una red de 30 puestos.

Se calcula que n es el número de bits de la parte host con la siguiente fórmula:

(2^n) - 2 □ 30, n = 5

Necesitamos una máscara de subred con 5 bits para la parte host.

- **5.ª etapa**: cálculo de la nueva máscara en binario, es decir, 32 - 5 = 27 bits.
  - Nueva máscara en binario: 11111111 . 11111111. 11111111 . 1110000, es decir, una máscara /27
- Para encontrar la dirección de red siguiente utilizamos la dirección de broadcast de la red n.º 2 a la que se agrega 1 en binario.
  - @B3: 00001010.00000000.00000001.00111111 se agrega 1
  - Nmb: 11111111.11111111.11111111 .11100000
  - @R4: 00001010.00000000.00000001.01000000, es decir, **10.0.1.64 /27**
  - @B4: 00001010.00000000.00000001.01011111, es decir, **10.0.1.95 /27**

Nuestra tercera red empieza, por tanto, en **10.0.1.64**, y termina en **10.0.1.95** con una máscara **/27**.

Debemos recalcular nuestra máscara de subred para una red de 2 puestos.

Se calcula que n es el número de bits de la parte host con la siguiente fórmula:

(2^n) - 2 □ 2, n = 2

Necesitamos una máscara de subred con 2 bits para la parte host.

- **6.ª etapa**: cálculo de la nueva máscara en binario, es decir, 32 - 2 = 30 bits.
  - Nueva máscara en binario: 11111111 . 11111111. 11111111 . 1111100, es decir, una máscara /30
- Para encontrar la dirección de red siguiente, utilizamos la dirección de broadcast de la red n.º 3 a la que se agrega 1 en binario.
  - @B3: 00001010.00000000.00000001.01011111 se agrega 1
  - Nmb: 11111111.11111111.11111111 .11111100
  - @R4: 00001010.00000000.00000001.01100000, es decir, **10.0.1.96 /30**
  - @B4: 00001010.00000000.00000001.01100011, es decir, **10.0.1.99 /30**

Nuestra cuarta red empieza, por tanto, en **10.0.1.96**, y termina en **10.0.1.99** con una máscara **/30**.

Configurar y mantener IPv4

Una configuración IP incorrecta puede tener un impacto más o menos importante. En un servidor, varios servicios pueden sufrir funcionamientos parcialmente incorrectos o incluso dejar de funcionar. Es muy importante asegurar la configuración que se ha realizado o asignado automáticamente a un puesto.

Existen comandos DOS y PowerShell que pueden utilizarse para la administración y el mantenimiento cotidiano de una red, asegurar un correcto funcionamiento de los servicios o simplemente tratar de diagnosticar un problema de la red.

1. Configuración y control en DOS

a. Comando netsh

Es posible realizar la configuración IPv4 de un puesto con el comando `netsh`; he aquí un ejemplo:

```
Netsh interface ipv4 set address name="Ethernet" source=static
addr=10.10.0.10 mask=255.255.255.0 gateway=10.10.0.1
```

Este comando permite asignar la dirección IPv4 10.10.0.10 con una máscara /24 a la tarjeta de red llamada Ethernet, configurando la puerta de enlace 10.10.0.1.

Para configurar la dirección del servidor DNS primario, introducimos el comando:

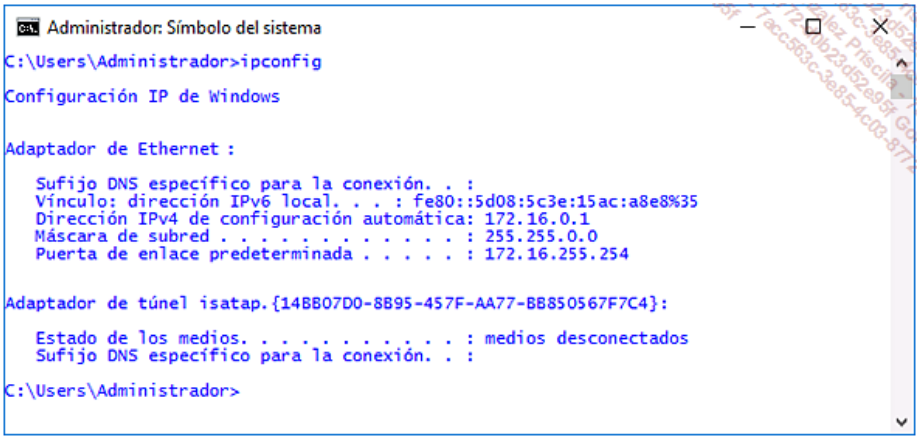
```
Netsh interface ipv4 set dns name="Ethernet" source=static addr=10.12.0.1
```

Y a continuación para la dirección del servidor DNS secundario:

```
Netsh interface ipv4 add dns name="Ethernet" 10.12.0.2 index=2
```

b. Comando ipconfig

El comando `ipconfig` permite mostrar la configuración IP de la interfaz o las interfaces de red.



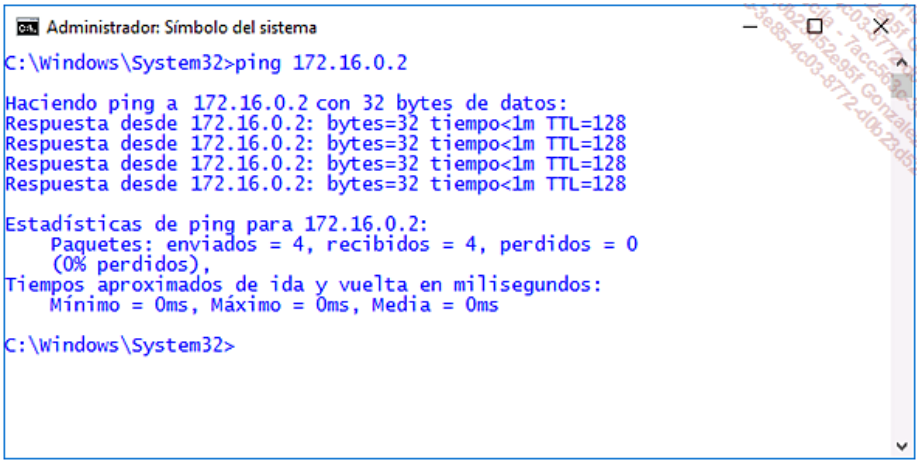
Asociándole opciones es posible realizar operaciones u obtener información:

- `ipconfig /all`: muestra la configuración completa de las interfaces de red presentes en el puesto.
- `ipconfig /release`: libera la configuración IP distribuida por el servidor DHCP.
- `ipconfig /renew`: solicita una nueva configuración al servidor DHCP.
- `ipconfig /displaydns`: muestra las entradas de la caché DNS.
- `ipconfig /flushdns`: permite vaciar la caché DNS.
- `ipconfig /registerdns`: obliga al puesto a registrarse en su servidor DNS.

c. Comando ping

Este comando permite comprobar la correcta comunicación entre dos puestos. Los problemas de conectividad en un puesto o un servidor se ponen de manifiesto rápidamente. El comando está compuesto de opciones facultativas y a continuación el nombre o la dirección IP de la

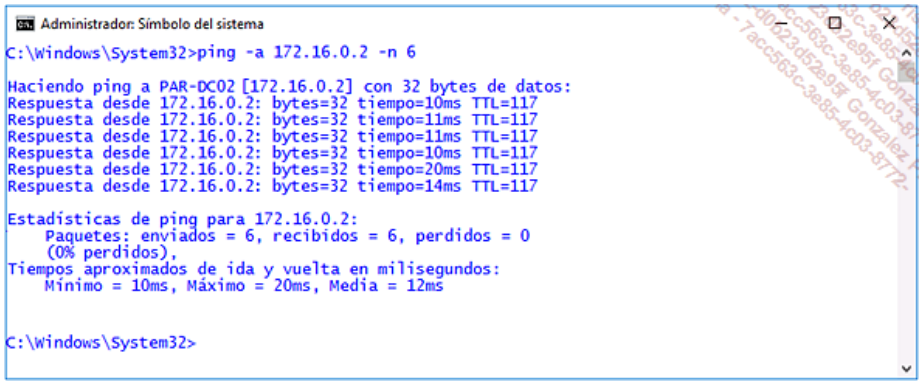
máquina que hay que comprobar.



Si no se indica ninguna opción, solo se envían cuatro tramas de tipo echo; si el puesto está encendido y conectado a la red devuelve una respuesta. En caso contrario, se obtiene una respuesta negativa.

Existen varias opciones que pueden aplicarse al comando:

- `-n número`: esta opción permite enviar x peticiones antes de detenerse, siendo x el número indicado a continuación de la n.
- `-t`: a diferencia de `-n`, el envío de tramas se realiza hasta que se solicite la parada.
- `-a`: permite la resolución de la dirección IP en nombre.



- `-4`: fuerza el uso de IPv4.
- `-6`: fuerza el uso de IPv6.

Ping es un comando que se basa en el protocolo ICMP, de modo que es posible comprobar un host remoto. Preste atención, sin embargo, a que este tipo de peticiones puede verse bloqueado por un cortafuegos.

d. Comando tracert

El comando `tracert` es un comando DOS que identifica todos los routers que se utilizan para alcanzar un destino. La trama es de tipo ICMP, es inútil utilizar este comando si el destino se encuentra en la misma red de área local. En efecto, el comando devuelve el nombre o la dirección IP de los routers que ha franqueado la trama echo.

Este comando resulta muy útil cuando se trata de resolver algún problema o encontrar qué router está mal configurado o no funciona correctamente.

Existen otros comandos, como `nslookup`, que pueden utilizarse para realizar pruebas de resolución de nombres.

2. Configuración y control en PowerShell

He aquí, a continuación, los comandos PowerShell que nos van a permitir configurar, supervisar y resolver problemas relacionados con la configuración IPv4 de nuestros servidores.

a. Comando Test-Connection

El cmdlet `Test-Connection` es el comando PowerShell que permite comprobar la conectividad entre dos dispositivos u ordenadores utilizando peticiones ICMP.

Este comando es más avanzado que el comando `ping` y ofrece las siguientes posibilidades:

- Enviar peticiones ICMP a varios hosts:

```
Test-Connection -ComputerName "PAR-DC01", "PAR-DC02", "SRV-RTR"
```

- Enviar peticiones ICMP de varios hosts a un host especificando la cuenta de usuario que hay que utilizar:

```
Test-Connection -Source "PAR-DC01", "PAR-DC02", "Localhost"
-ComputerName "SRV-RTR" -Credential formacion\Administrador
```

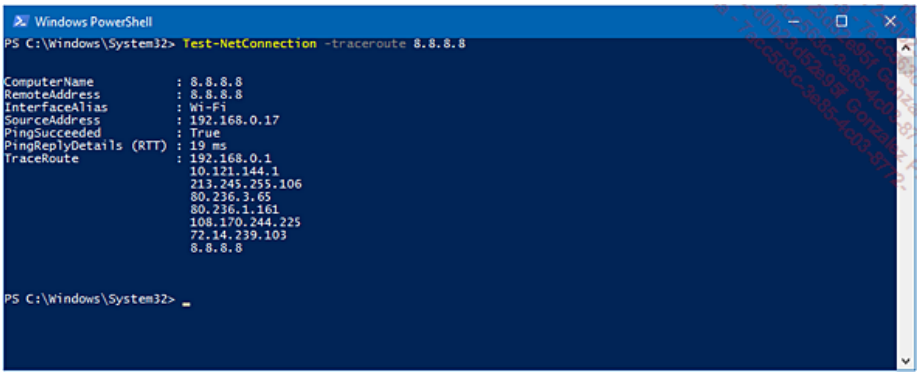
- De este modo es posible personalizar el comando con el número de peticiones enviadas, el tiempo de vida, el retardo:

```
Test-Connection -ComputerName "PAR-DC02" -Count 3 -Delay 2 -TTL
255 -BufferSize 256 -ThrottleLimit 32
```

b. Comando Test-Netconnection

El cmdlet `Test-NetConnection` muestra la información de diagnóstico de una conexión. La salida incluye los resultados de una búsqueda DNS, una lista de interfaces IP, una opción para comprobar una conexión TCP, reglas IPsec y una confirmación del establecimiento de la conexión. Este comando se utiliza para resolver problemas. Con este cmdlet, es posible obtener el mismo resultado que con el comando`tracert`:

```
Test-Netconnection -traceroute 8.8.8.8
```



c. Comando New-NetIPAddress

El cmdlet `New-NetIPAddress` nos permite configurar la dirección IPv4 e IPv6 de una interfaz de red. Lo más sencillo es utilizar el nombre de la tarjeta de red correspondiente a la interfaz que se desea configurar; para ello se utiliza el cmdlet `Get-NetAdapter`, que enumera el conjunto de interfaces de red.

```
New-NetIPAddress -IPAddress 172.16.0.1 -PrefixLength 16
-InterfaceAlias Ethernet0
```

Para configurar una dirección IPv6 con PowerShell es preciso utilizar el parámetro `-AddressFamily` con el valor IPV6.

Esto produce el siguiente comando para IPv6:

```
New-NetIPAddress -IPAddress FD00:AAAA:BBBB:CCCC::15 -PrefixLength
64 -InterfaceAlias Ethernet0 -AddressFamily IPv6
```

Con este comando se asigna la dirección IPV6 **FD00:AAAA:BBBB:CCCC::15** con un prefijo de **64** a la interfaz llamada Ethernet0.

d. Comando Set-DnsClientServerAddress

El cmdlet `Set-DnsClientServerAddress` nos permite configurar la dirección del servidor DNS de una interfaz de red.

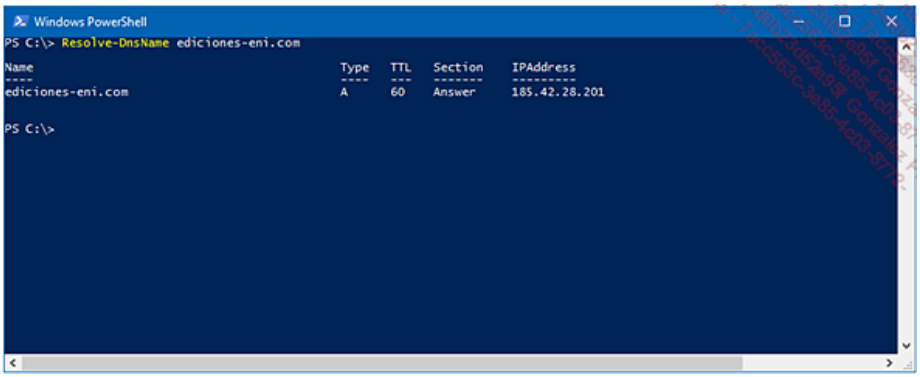
```
Set-DnsClientServerAddress -InterfaceAlias Ethernet0
-ServerAddresses 172.16.0.1
```

3. Comandos de PowerShell útiles

La siguiente tabla expone algunos comandos PowerShell que permite obtener información de configuración:

Comandos PowerShell	Acciones
`Get-NetRoute`	Muestra la tabla de enrutamiento IPv4 e IPv6.
`Get-DNSClient`	Muestra la información del servidor DNS configurado en la máquina.
`Get-DNSClientCache`	Muestra la caché DNS de la máquina.
`Get-DNSClientServerAddress`	Muestra el conjunto de direcciones de servidores DNS registrados para cada interfaz.
`Resolve-DNS`	Realiza la resolución de nombres.

Aquí, el comando `Resolve-DnsName` realiza la resolución del nombre de dominio ediciones-eni.com:


Windows PowerShell
PS C:\> Resolve-DnsName ediciones-eni.com
Name Type TTL Section IPAddress
ediciones-eni.com A 60 Answer 185.42.28.201
PS C:\>

Implementación del protocolo IPv6

Desde hace muchos años, prosigue la implementación del protocolo IPv6. Los sistemas operativos de cliente o de servidor poseen actualmente la posibilidad de ser direccionados mediante IPv6.

1. El protocolo IPv6

IPv6 se ha diseñado para ser el sucesor del protocolo IPv4. IPv6 posee una cantidad de espacio de direccionamiento mayor (128 bits) para un total de 340 sextillones de direcciones disponibles (lo que se corresponde al número 340 seguido de 36 ceros).

Sin embargo, IPv6 aporta direcciones más largas. Cuando la IETF empezó a desarrollar un sucesor para IPv4, el organismo utilizó esta oportunidad para corregir los límites de IPv4 y mejorar este protocolo. Por ejemplo, el ICMPv6 (*Internet Control Message Protocol version 6*) incluye la configuración automática y la resolución de direcciones, funciones que no están presentes en el protocolo ICMP para IPv4 (ICMPv4).

La falta de espacio de direccionamiento IPv4 ha sido el factor más importante a la hora de pasar a IPv6. Como África, Asia y otras partes del mundo están cada vez más conectadas a Internet, no hay suficientes direcciones IPv4 para tener en cuenta este crecimiento. El lunes 31 de enero de 2011 la IANA asignó los dos últimos bloques de direcciones IPv4 /8 a los organismos de registro de Internet locales (RIR).

a. Un formato hexadecimal

A diferencia de las direcciones IPv4, que se expresan en formato decimal punteado, las direcciones IPv6 se representan mediante valores hexadecimales. El formato hexadecimal se utiliza para representar los valores binarios de las tramas y de los paquetes, así como las direcciones MAC Ethernet.

El sistema de numeración en **base 16** utiliza las cifras 0 a 9 y las letras A a F.

Hexadecimal	Decimal	Binario
0	0	0000
1	1	0001
2	2	0010
3	3	0011
4	4	0100
5	5	0101
6	6	0110
7	7	0111
8	8	1000
9	9	1001
A	10	1010
B	11	1011
C	12	1100
D	13	1101
E	14	1110
F	15	1111

Esta tabla muestra las equivalencias en binario y decimal, así como los valores hexadecimales. Existen **16 combinaciones** únicas de cuatro bits, de **0000** a **1111**. El sistema hexadecimal de 16 dígitos es el sistema de numeración ideal, pues cuatro bits pueden representarse mediante un valor hexadecimal único.

b. Comprender el formato binario

Sabiendo que **8 bits** (un byte) es una agrupación binaria corriente, el rango binario de **00000000** a **11111111** se corresponde, en formato hexadecimal, al rango de **00** a **FF**. Los ceros de la izquierda se muestran para completar la representación de 8 bits. Por ejemplo, el valor binario **0000 1010** se corresponde con **0A** en formato hexadecimal.

Hexadecimal	Decimal	Binario
00	0	0000 0000
01	1	0000 0001
02	2	0000 0010
03	3	0000 0011
04	4	0000 0100
05	5	0000 0101
06	6	0000 0110
07	7	0000 0111
08	8	0000 1000
0A	10	0000 1010
0F	15	0000 1111
10	16	0001 0000
20	32	0010 0000
40	64	0100 0000
80	128	1000 0000
C0	192	1100 0000
CA	202	1100 1010
F0	240	1111 0000
FF	255	1111 1111

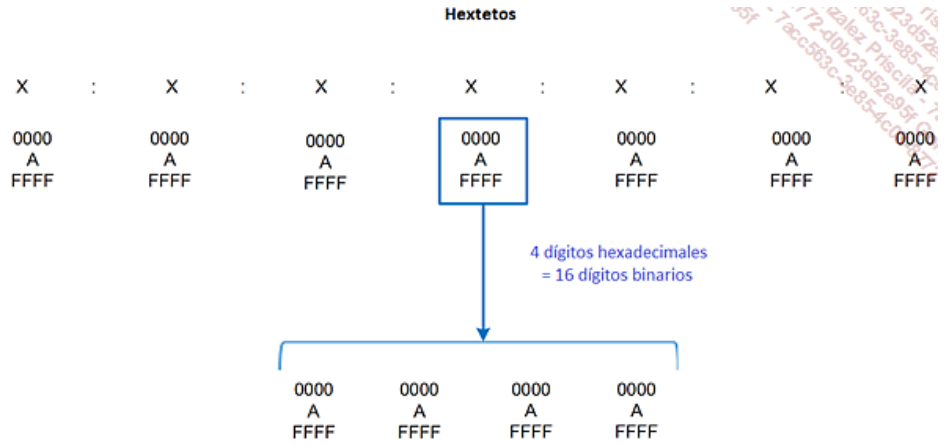
c. Conversiones hexadecimales

Las conversiones numéricas entre valores decimales y hexadecimales son muy sencillas, si bien la división o la multiplicación por 16 no siempre es cómoda.

Con un poco de práctica, es posible reconocer las configuraciones binarias que se corresponden con los valores decimales y hexadecimales. La tabla anterior ilustra estas configuraciones para determinados valores de 8 bits.

d. Representación de una dirección IPv6

Las direcciones IPv6 tienen una longitud de 128 bits y se escriben como una cadena de valores hexadecimales. Todos los grupos de 4 bits están representados por un único dígito hexadecimal, para un total de 32 valores hexadecimales. Las direcciones IPv6 no son sensibles a las mayúsculas y minúsculas, y pueden escribirse tanto en minúsculas como en mayúsculas.



El formato preferido para escribir una dirección IPv6 es x:x:x:x:x:x:x:x, cada "x" comprende **cuatro** valores **hexadecimales**. Para hacer referencia a los 8 bits de una dirección IPv4, utilizamos el término "byte". Para las direcciones IPv6, "**hexteto**" es el término no oficial que se utiliza para referirse a un segmento de 16 bits o cuatro valores hexadecimales. Cada "x" es un único hexteto, 16 bits o cuatro dígitos hexadecimales.

El formato preferido significa que la dirección IPv6 se escriba utilizando 32 dígitos hexadecimales. Esto no significa necesariamente que sea la solución ideal para representar una dirección IPv6. Veremos más adelante en este capítulo cómo podemos escribir direcciones IPv6, así como direcciones IPv6 especiales.

Ejemplo de direcciones IPv6 en formato preferido:

2001 : 0DB8 : 0000 : 1111 : 0000 : 0000 : 0000 : 0200

FE80 : 0000 : 0000 : 0000 : 0123 : 4567 : 89AB : CDEF

FF02 : 0000 : 0000 : 0000 : 0000 : 0001 : FF00 : 0200

0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0001

0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000

e. Regla n.° 1: omisión de los ceros al principio del segmento

La primera regla que permite abreviar la notación de las direcciones IPv6 es la omisión de los ceros al principio del segmento de 16 bits (o de cada hexteto). Por ejemplo:

- **01AB** equivale a 1AB
- **09F0** equivale a 9F0
- **0A00** equivale a A00
- **00AB** equivale a AB

Esta regla se aplica únicamente a los ceros al principio del segmento y NO a los ceros siguientes. La omisión de estos últimos produciría una dirección ambigua. Por ejemplo, el hexteto "ABC" podría ser "0ABC" o bien "ABC0".

Ejemplo de direcciones IPv6 en formato preferido:

- 2001 : 0DB8 : 0000 : 1111 : 0000 : 0000 : 0000 : 0200
- FE80 : 0000 : 0000 : 0000 : 0123 : 4567 : 89AB : CDEF
- FF02 : 0000 : 0000 : 0000 : 0000 : 0001 : FF00 : 0200
- 0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0001
- 0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000

Si aplicamos la regla n.° 1 obtenemos las direcciones IPv6 siguientes:

- 2001 : DB8 : 0 : 1111 : 0 : 0 : 0 : 200
- FE80 : 0 : 0 : 0 : 123 : 4567 : 89AB : CDEF
- FF02 : 0 : 0 : 0 : 0 : 1 : FF00 : 200
- 0 : 0 : 0 : 0 : 0 : 0 : 0 : 1
- 0 : 0 : 0 : 0 : 0 : 0 : 0 : 0

f. Regla n.° 2: omisión de las secuencias compuestas únicamente de ceros

La segunda regla que permite abreviar la notación de las direcciones IPv6 es que los **dos puntos dobles (::)** pueden reemplazar cualquier cadena única y **contigua** de uno o varios segmentos de 16 bits (hextetos) compuestos únicamente por ceros.

Los **dos puntos dobles (::)** pueden utilizarse **una única vez por dirección**; en caso contrario sería posible obtener varias direcciones diferentes. Cuando se utiliza la omisión de los ceros al principio del segmento, la notación de las direcciones IPv6 puede verse considerablemente reducida. Se trata del "formato comprimido".

Dirección no válida: 2001:0DB8::ABCD::1234, pues se han realizado dos compresiones.

Ejemplo de direcciones IPv6 en formato preferido:

- 2001 : 0DB8 : 0000 : 1111 : 0000 : 0000 : 0000 : 0200
- FE80 : 0000 : 0000 : 0000 : 0123 : 4567 : 89AB : CDEF
- FF02 : 0000 : 0000 : 0000 : 0000 : 0001 : FF00 : 0200
- 0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0001
- 0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000

Si aplicamos la regla n.° 1 obtenemos las direcciones IPv6 siguientes:

- 2001 : DB8 : 0 : 1111 : 0 : 0 : 0 : 200
- FE80 : 0 : 0 : 0 : 123 : 4567 : 89AB : CDEF
- FF02 : 0 : 0 : 0 : 0 : 1 : FF00 : 200
- 0 : 0 : 0 : 0 : 0 : 0 : 0 : 1
- 0 : 0 : 0 : 0 : 0 : 0 : 0 : 0

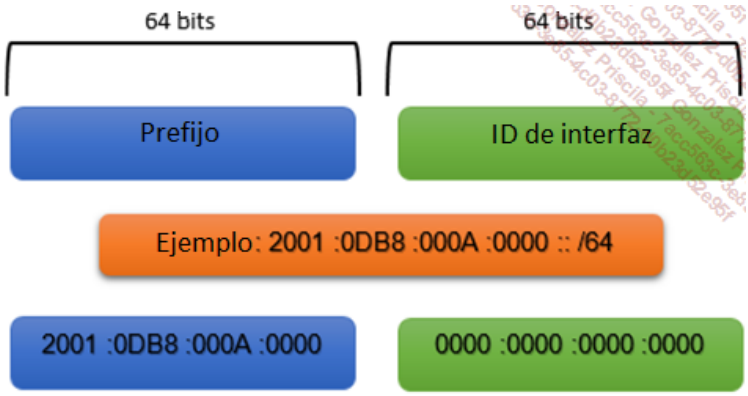
Si aplicamos la regla n.° 2 obtenemos las direcciones IPv6 siguientes:

- 2001 : DB8 : 0 : 1111 :: 200
- FE80 :: 123 : 4567 : 89AB : CDEF
- FF02 :: 1 : FF00 : 200
- :: 1
- ::

2. Longitud de prefijo IPv6

Recuerde que el prefijo (o la parte de red) de una dirección **IPv4** puede identificarse mediante una máscara de subred o una longitud de prefijo en formato decimal punteado (notación CIDR). Por ejemplo, la dirección IP 192.168.1.10 y la máscara de subred en formato decimal punteado 255.255.255.0 equivalen a 192.168.1.10/24.

IPv6 utiliza la longitud de prefijo para representar el prefijo de la dirección, de modo que no se usa el formato decimal punteado de la máscara de subred. La longitud de prefijo se utiliza para indicar la parte de red de una dirección IPv6 mediante con el formato de la dirección **IPv6 / longitud de prefijo**.



La longitud de prefijo puede ir de 0 a 128 bits. La longitud de prefijo IPv6 estándar para las redes de área local y la mayor parte de otros tipos de redes es /64. Esto significa que el prefijo o la parte de red de la dirección tiene una longitud de 64 bits, lo que deja 64 bits para el ID de la interfaz (parte host) de la dirección.

3. Tipos de direcciones IPv6

Existen tres tipos de direcciones IPv6:

- **Monodifusión**: una dirección de monodifusión IPv6 identifica una interfaz en un dispositivo IPv6 de forma única. Una dirección de origen IPv6 debe ser una dirección de monodifusión.
- **Multidifusión**: una dirección de multidifusión IPv6 se utiliza para enviar un paquete IPv6 único hacia varios destinos.
- **Anycast**: una dirección anycast IPv6 es una dirección de monodifusión IPv6 que puede asignarse a varios dispositivos. Un paquete enviado a una dirección anycast se encamina hacia el dispositivo más próximo que posea esta dirección.

A diferencia de IPv4, en IPv6 no existe ninguna dirección de difusión. Sin embargo, existe una dirección de multidifusión a todos los nodos IPv6 que ofrece globalmente los mismos resultados.

a. Direcciones locales únicas IPv6

Las direcciones locales únicas se corresponden con las direcciones privadas en IPv4 (RFC 1918). Este tipo de direcciones puede enrutarse únicamente en el interior de una compañía. Para evitar problemas de duplicación, que es posible encontrar en IPv4 cuando se interconectan varias redes, la dirección está compuesta de un prefijo de 40 bits.

Una dirección local única IPv6 está formada de la siguiente manera:

- Los siete primeros bits poseen un valor fijo igual a 1111110, el prefijo de la dirección es igual a FC00::/7.
- El identificador de la organización de 40 bits permite evitar los problemas de interconexión, pues se genera aleatoriamente.
- El identificador de subred permite la creación de subredes.
- Los 64 últimos bits se utilizan para representar el identificador de interfaz.

b. Direcciones globales unicast IPv6

Este tipo se corresponde con las direcciones IPv4 públicas, que permiten identificar un equipo en la red de Internet.

Caracterizadas por el prefijo **2000::/3**, pueden reservarse desde 1999. Algunos bloques están reservados para la implementación del túnel 6to4 (por ejemplo, el bloque **2002::/16**).

Esta dirección está compuesta de varios bloques:

- Los tres primeros bits (001) así como el prefijo de enrutamiento global (45 bits) permiten formar un primer bloque de 48 bits. Este último lo asigna el proveedor de acceso a Internet.
- El identificador de subred, codificado en 16 bits, permite la creación de subredes en una organización.
- El identificador de interfaz utiliza los 64 bits restantes, permite identificar un equipo específico en una subred. Este bloque se genera aleatoriamente o se asigna a través de un servidor DHCPv6.

c. Direcciones de enlace local IPv6

Una dirección de enlace local se asigna a una interfaz de red para permitirle comunicarse en la red local. Este tipo de dirección se genera automáticamente y no es enrutable. Su homóloga en IPv4 se corresponde con la dirección APIPA (169.254.x.x).

El prefijo utilizado para este tipo de dirección es **FE80::/64**. Los 64 bits restantes permiten identificar la interfaz.

Esta dirección está formada de la siguiente manera:

- Los 10 primeros bits (1111 1110 10), así como la serie de ceros, forman el prefijo de 64 bits (FE80::).
- El identificador de interfaz utiliza los 64 bits restantes, permite identificar un equipo específico en una subred. Este bloque se genera aleatoriamente o se asigna a través de un servidor DHCPv6.

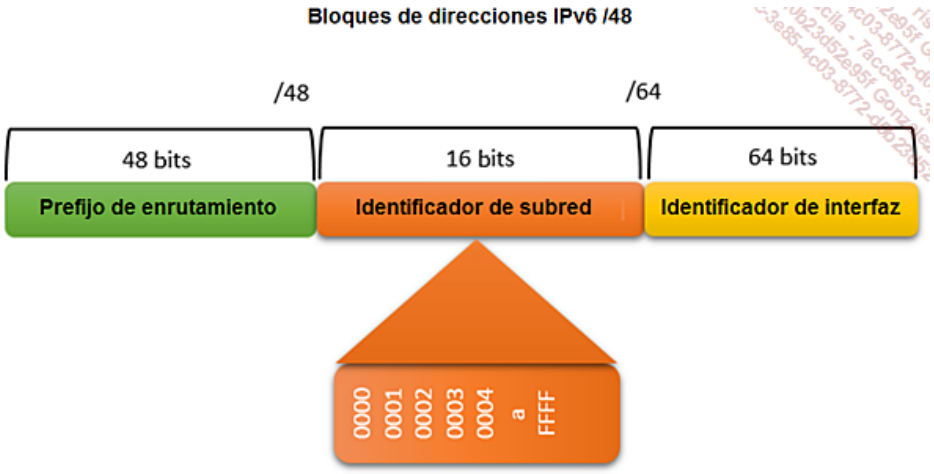
d. Equivalencia IPv4/IPv6

	IPv4	IPv6
Dirección no especificada	0.0.0.0	::
Dirección de bucle invertido	127.0.0.1	::1
Dirección APIPA	169.254.0.0/16	FE80::/64
Dirección de broadcast	255.255.255.255	Uso de tramas multicast
Dirección de multicast	224.0.0.0/4	FF00::/8

e. Subredes e IPv6

La división en subredes IPv6 exige un enfoque diferente al de las subredes IPv4. En efecto, IPv6 requiere tantas direcciones que el motivo de segmentación es diferente del de IPv4. Un espacio de direccionamiento IPv6 no está segmentado en subredes para conservar las direcciones, sino para tener en cuenta la distribución jerárquica y lógica de la red.

Recuerde que un bloque de direcciones IPv6 con el prefijo /48 contiene 16 bits para el IP de subred. La segmentación de la dirección mediante el ID de subred de 16 bits permite generar hasta 65 536 subredes, y no requiere tomar bits del ID de interfaz. Cada subred IPv6 /64 contiene unos dieciocho quintillones de direcciones, lo que supera sobradamente las necesidades de cualquier segmento de red IP.



Las subredes creadas a partir del ID de subred son fáciles de representar, puesto que no se requiere ninguna conversión a binario. Para determinar la siguiente subred disponible, basta con contar en hexadecimal.

Tomemos como ejemplo la siguiente dirección IPv6: 2001:0FA4:3FA::/48

Para crear subredes a partir de esta dirección IPv6 con el prefijo /48, vamos a incrementar los dieciséis bits disponibles para las subredes.

He aquí las 10 primeras subredes:

*2001:0FA4:3FA:**0001**::/64*

*2001:0FA4:3FA:**0002**::/64*

*2001:0FA4:3FA:**0003**::/64*

*2001:0FA4:3FA:**0004**::/64*

*2001:0FA4:3FA:**0005**::/64*

*2001:0FA4:3FA:**0006**::/64*

*2001:0FA4:3FA:**0007**::/64*

*2001:0FA4:3FA:**0008**::/64*

*2001:0FA4:3FA:**0009**::/64*

*2001:0FA4:3FA:**000A**::/64*

Los mecanismos de transición IPv4 - IPv6

La transición de IPv4 a IPv6 requiere la coexistencia entre los dos protocolos, pues son demasiados los servicios y las aplicaciones que están basados en IPv4 como para que este protocolo desaparezca repentinamente. Sin embargo, existen varias tecnologías que facilitan esta transición permitiendo la comunicación entre los hosts IPv4 únicamente e IPv6 únicamente. Existen también tecnologías que permiten la comunicación IPv6 sobre redes IPv4.

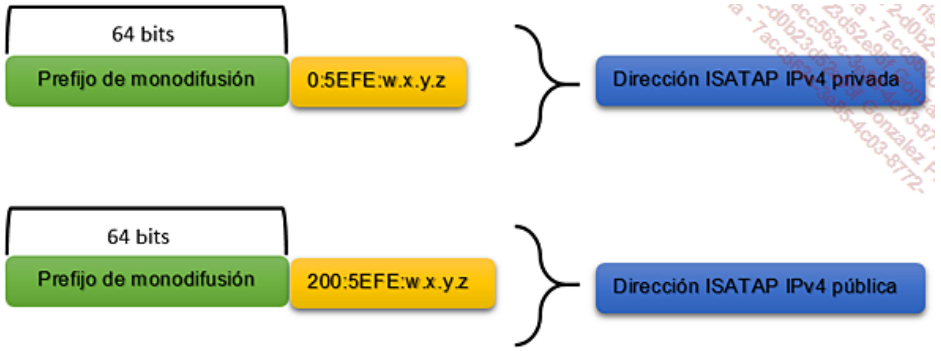
Este capítulo provee información acerca de ISATAP (*Intra-Site Automatic Tunnel Addressing Protocol*), 6to4 y Teredo, que ayudan a establecer la conectividad entre las tecnologías IPv4 e IPv6. Hablaremos también de PortProxy, que vuelve a las aplicaciones compatibles con IPv6.

1. Tecnología ISATAP

ISATAP es una tecnología de asignación de direcciones que puede utilizar para asegurar la conectividad IPv6 monodifusión entre hosts IPv6/IPv4 sobre una intranet IPv4. Los paquetes IPv6 se encapsulan en paquetes IPv4 para ser transmitidos sobre la red. De este modo es posible realizar directamente la comunicación entre dos hosts ISATAP sobre una red IPv4, y se puede utilizar un router ISATAP si una red alberga únicamente hosts IPv6.

Los hosts ISATAP no requieren ninguna configuración manual y puede crear direcciones ISATAP utilizando mecanismos de configuración automática de direcciones estándar. Si bien el componente ISATAP está activo por defecto, asigna direcciones ISATAP únicamente si puede resolver el nombre ISATAP en su red.

Las direcciones ISATAP se construyen según el siguiente modelo:



Dirección ISATAP privada: FD00::5EFE:192.168.25.1

Dirección ISATAP pública: 2001:DB8::200:5EFE:137.109.137.5

a. Un router ISATAP

Cuando no existe ningún host IPv6 (sin la parte IPv4 configurada a nivel de la tarjeta de red), el router ISATAP debe publicar el prefijo IPv6 que se utilizará por los clientes ISATAP. Cada equipo dispone de una interfaz ISATAP que se configura automáticamente para usar este prefijo. Cuando las aplicaciones utilizan la interfaz ISATAP, el paquete IPv6 se encapsula en un paquete IPv4 para transmitirse a la dirección IPv4 del host de destino.

Si únicamente existen hosts IPv6, entonces el router ISATAP descompacta a su vez los paquetes IPv6. Los hosts ISATAP envían los paquetes a la dirección IPv4 del router ISATAP, este descompacta los paquetes IPv6 y los envía únicamente sobre la red IPv6.

Tunneling ISATAP

Para configurar un router ISATAP existen varios mecanismos. El más sencillo consiste en configurar un registro de host ISATAP en el DNS para permitir la resolución del nombre del router ISATAP en una dirección IPv4.

Por defecto, los servidores DNS desde Windows Server 2008 disponen de una lista roja de peticiones globales que impide la resolución ISATAP, incluso aunque el registro del host esté configurado correctamente. Debe eliminar ISATAP de la lista roja de las peticiones globales en el DNS si utiliza un registro de host ISATAP para configurar los clientes ISATAP.

Para configurar ISATAP, es posible utilizar los siguientes comandos:

- Utilice el applet de comando Windows PowerShell `Set-NetIsatapConfiguration -Router x.x.x.x`.
- Utilice `Netsh Interface IPv6 ISATAP Set Router x.x.x.x`.
- Configure el parámetro de la directiva de grupo ISATAP Nombre de router.

2. Tecnología 6to4

6to4 es una tecnología que puede utilizar para asegurar la conectividad IPv6 monodifusión sobre la red Internet IPv4. Puede utilizar 6to4 para proveer la conectividad IPv6 entre dos sitios IPv6, o entre un host IPv6 y un sitio IPv6. Sin embargo, 6to4 no está bien adaptado a escenarios

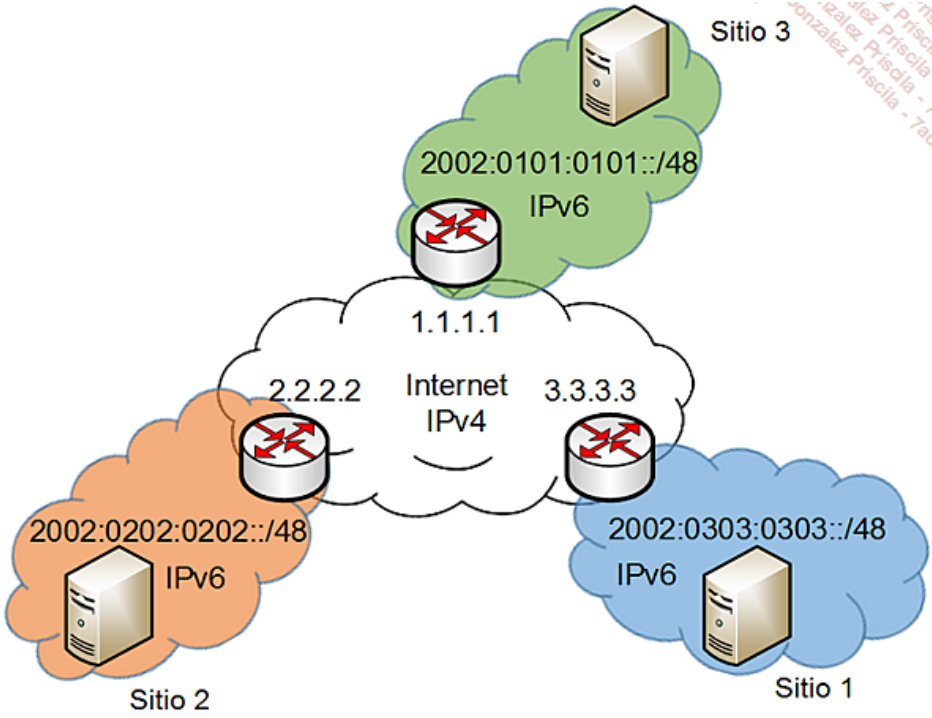
que requieran el proceso de traducción NAT.

Un router 6to4 garantiza a un sitio la conectividad IPv6 sobe la red Internet IPv4. Para ello, el router 6to4 posee una dirección IPv4 pública configurada en la interfaz externa, y una dirección IPv6 6to4 configurada en la interfaz interna. Para configurar los ordenadores cliente, la interfaz interna del router 6to4 publica la red 6to4. Cualquier ordenador cliente que empiece a utilizar la interfaz de red 6to4 es un host 6to4 capaz de enviar paquetes 6to4 al router 6to4 para que se envíen a otros sitios a través de la red Internet IPv4.

La dirección de red IPv6 que se utiliza para 6to4 está basada en la dirección IPv4 de la interfaz externa de un router IPv6.

El formato de dirección IPv6 es: 2002:WWXX:YYZZ:ID_subred:ID_Interfaz, donde WWXX:YYZZ es la representación hexadecimal de w.x.y.z separada por los dos puntos dobles (::).

Cuando un único host de la red Internet IPv4 participa de 6to4, se configura como host/router. Un host/router 6to4 no realiza el enrutamiento para los demás hosts, sino que genera su propia red IPv6 utilizada por 6to4.



3. Tecnología Teredo

Teredo es una tecnología similar a 6to4, permite transmitir a través de un túnel paquetes IPv6 sobre la red Internet IPv4. Sin embargo, Teredo funciona correctamente aunque se utilice la traducción de direcciones de red (NAT) para la conectividad de Internet. Teredo es necesario, pues muchos organismos utilizan direcciones IP privadas, que requieren la traducción de direcciones de red para acceder a Internet. Si un dispositivo NAT puede configurarse como router 6to4, entonces Teredo no es necesario.

La comunicación IPv6 entre dos clientes Teredo sobre la red Internet IPv4 requiere un servidor Teredo alojado en la red Internet IPv4. El servidor Teredo facilita la comunicación entre los dos clientes Teredo sirviendo de punto central para la inicialización de la comunicación. En general, los hosts situados tras un dispositivo NAT están autorizados a iniciar las comunicaciones salientes, pero no están autorizados a aceptar las comunicaciones entrantes. Para resolver este problema, ambos clientes Teredo inician la comunicación con el servidor Teredo. Una vez que se ha establecido la comunicación con el servidor Teredo, y que el dispositivo NAT ha autorizado las comunicaciones salientes, todas las comunicaciones posteriores se realizan directamente entre los dos clientes Teredo.

Estructura de la dirección Teredo

Una dirección Teredo es una dirección IPv6 de 128 bits, aunque utiliza una estructura diferente para las direcciones.

Para las direcciones IPv6 de monodifusión típicas, la estructura es la siguiente:

- 2001::/32 (32 bits). Se utiliza el prefijo específico a Teredo para todas las direcciones Teredo.
- Dirección IPv4 del servidor Teredo (32 bits) que identifica al servidor Teredo.
- **Opciones (16 bits)**. Existen varias opciones que describen la configuración de la comunicación, como por ejemplo si el cliente está situado tras un dispositivo NAT.
- **Puerto externo oculto (16 bits)**. Se trata del puerto externo utilizado para la comunicación con el dispositivo NAT para esta comunicación. Está oculto para impedir que el dispositivo NAT lo traduzca.
- **Dirección IP externa oculta (32 bits)**. Se trata de la dirección IP externa del dispositivo NAT, oculta para impedir que el dispositivo NAT la traduzca.

4. PortProxy

Los desarrolladores de aplicaciones utilizan API de red específicas para acceder a recursos de la red. Las API modernas pueden utilizar IPv4 o IPv6, dejando que el sistema operativo seleccione la versión del protocolo IP. Sin embargo, algunas aplicaciones más antiguas utilizan API que solo pueden trabajar con IPv4. El servicio PortProxy permite a las aplicaciones incompatibles con el protocolo IPv6 comunicarse con hosts IPv6. La activación del servicio permitirá a los paquetes IPv6 entrantes de la aplicación ser traducidos a IPv4, y a continuación ser pasados a la aplicación.

También puede utilizar PortProxy en un sistema que haga de intermediario entre dos hosts IPv4 únicamente y hosts IPv6 únicamente. Para ello, debe configurar el DNS para resolver el nombre de host remoto con la dirección del equipo PortProxy. Por ejemplo, un host IPv4 solo obtendría la resolución del nombre de host IPv6 únicamente con la dirección IPv4 del ordenador de PortProxy. De esta manera se enviarán los paquetes salientes al ordenador PortProxy, que los transmitirá al ordenador IPv6 únicamente.

Límites de PortProxy

- El PortProxy no es capaz de utilizar conexiones UDP, solo funcionan las conexiones TCP.
- No es posible modificar la información de las direcciones que se incorporan en la parte de "datos" de un paquete IP. Por ejemplo, con la aplicación FTP, los datos y la información de direccionamiento están incluidas en la parte "datos" del paquete. De modo que PortProxy no funcionará con la aplicación FTP.

Puede configurar PortProxy en Windows Server 2012 mediante `netsh interface PortProxy`. Sin embargo, por lo general es preferible utilizar una tecnología de tunneling en lugar de PortProxy.

Talleres

Los talleres son teóricos, de modo que no es necesario realizar ninguna manipulación.

1. Conversión binaria/decimal

Objetivo: realizar la conversión binaria/decimal en ambos sentidos

- **224**
- **172**
- **0001 1011**
- **172.125.10.33**
- **148**
- **1010 1011**

Solución

- **224**

El valor decimal del rango 7 es igual a 128; este valor es inferior a 224. El valor binario del rango 7 es, por tanto, igual a 1. Queda por convertir el número 96 (224-128).

El valor decimal del rango 6 es igual a 64; este valor es menor que 96. El valor binario del rango 6 es, por tanto, igual a 1. Queda por convertir el número 32 (96-64).

El valor decimal del rango 5 es igual a 32; el valor binario del rango 5 es, por tanto, igual a 1.

El valor binario de los demás rangos es igual a 0.

La conversión de 224 a binario es 1110 0000.

- **172**

El valor decimal del rango 7 es igual a 128; este valor es menor que 172. El valor binario del rango 7 es, por tanto, igual a 1. Queda por convertir el número 44 (172-128).

El valor decimal del rango 6 es igual a 64; este valor es mayor que 44. De modo que utilizamos el valor 0 para el rango 6.

El valor decimal del rango 5 es igual a 32; este valor es menor que 44. El valor binario del rango 5 es, por tanto, igual a 1. Queda por convertir el número 12 (44-32).

El valor decimal del rango 4 es igual a 16; este valor es mayor que 12. De modo que utilizamos el valor 0 para el rango 4.

El valor decimal del rango 3 es igual a 8; este valor es menor que 12. El valor binario del rango 3 es, por tanto, igual a 1. Queda por convertir el número 4 (12-8).

El valor decimal del rango 2 es igual a 4; este valor es igual a 4. El valor binario del rango 2 es, por tanto, igual a 1. No quedan valores por convertir, de modo que el valor binario de los demás rangos es igual a 0.

La conversión de 172 a binario es 1010 1100.

- **0001 1011**

Para encontrar el valor decimal, es necesario agregar el valor de los bits configurados a 1, es decir:

$2^4 + 2^3 + 2^1 + 2^0 = 16 + 8 + 2 + 1$

Si se convierte el valor binario 0001 1011, se obtiene el valor decimal 27.

- **172.125.10.33**

Se realiza la conversión de cada byte a binario:

172 :1010 1100

125 :0111 1101

10 :0000 1010

33 :0010 0001

La dirección IP 172.125.10.33 convertida a binario es:

1010 1100. 0111 1101. 0000 1010. 0010 0001

- **148**

El valor decimal del rango 7 es igual a 128; este valor es menor que 148. El valor binario del rango 7 es, por tanto, igual a 1. Queda por

convertir el número 19 (148-128).

El valor decimal del rango 6 es igual a 64; este valor es mayor que 19. De modo que utilizamos el valor 0 para el rango 6.

El valor decimal del rango 5 es igual a 32; este valor es mayor que 19. El valor binario del rango 5 es, por tanto, igual a 0.

El valor decimal del rango 4 es igual a 16; este valor es menor que 19. El valor binario del rango 4 es, por tanto, igual a 1. Queda por convertir el número 3 (19-16).

El valor decimal del rango 3 es igual a 8; este valor es mayor que 3. El valor binario del rango 3 es, por tanto, igual a 0.

El valor decimal del rango 2 es igual a 4; este valor es mayor que 4. El valor binario del rango 2 es, por tanto, igual a 0.

El valor decimal del rango 1 es igual a 2; este valor es menor que 3. El valor binario del rango 2 es, por tanto, igual a 1. Queda por convertir el número 1 (3-2).

El valor decimal del rango 0 es igual a 1; este valor es igual a 1. El valor binario del rango 1 es, por tanto, igual a 1.

La conversión de 148 a binario es 10010100.

- **1010 1011**

Para encontrar el valor decimal conviene agregar el valor de los bits configurados a 1, es decir: $2^7 + 2^5 + 2^3 + 2^1 + 2^0 = 128 + 32 + 16 + 8 + 2 + 1$

2. Direccionamiento IPv6

Objetivo: simplificar y/o "expandir" las siguientes direcciones IPv6

- **fe80:0000:0000:0000:0000:4cff:fe4f:4f50**
- **2001:0688:1f80:2000:0203:ffff:0018:ef1e**
- **2001:0688:1f80:0000:0203:ffff:4c18:00e0**
- **3cd0:0000:0000:0000:0040:0000:0000:0cf0**
- **0000:0000:0000:0000:0000:0000:0000:0000**
- **0000:0000:0000:0000:0000:0000:0000:0001**
- **fec0:0:0:ffff::1**
- **fe80::1**
- **fe80::4cd2:ffa1::1**

Solución

- **fe80:0000:0000:0000:0000:4cff:fe4f:4f50**

Recordamos la regla n.º 2 (omisión de las secuencias compuestas únicamente por ceros) y vemos que, tras la secuencia fe80, tenemos 4 secuencias de ceros consecutivos. La dirección puede simplificarse en **fe80::4cff:fe4f:4f50**.

- **2001:0688:1f80:2000:0203:ffff:0018:ef1e**

Con esta dirección se utiliza la regla n.º 1, que se corresponde con la omisión de los ceros situados al principio del segmento. La dirección se simplificará en **2001:688:1f80:2000:203:ffff:18:ef1e**.

- **2001:0688:1f80:0000:0203:ffff:4c18:00e0**

Aquí también utilizaremos la regla n.º 1, así como la regla n.º 2. He aquí el resultado tras la simplificación: **2001:688:1f80::203:ffff:4c18:e0**.

- **3cd0:0000:0000:0000:0040:0000:0000:0cf0**

Con esta dirección utilizaremos la regla n.º 2; podemos observar que es posible simplificar en dos secciones de la dirección. De modo que puede simplificarse en: **3cd0::40:0000:0000:cf0** o bien **3cd0:0000:0000:0000:0000:40::cf0**.

- **0000:0000:0000:0000:0000:0000:0000:0000**

Se trata de la dirección indeterminada, se escribe de la siguiente manera: **::**.

- **0000:0000:0000:0000:0000:0000:0000:0001**

Se trata de la dirección de bucle invertido, se escribe de la siguiente manera: **::1**.

- **fec0:0:0:ffff::1**

Observamos la presencia de **::** tras la secuencia ffff, indicando que ya se ha aplicado una contracción. La dirección expandida se escribe de la siguiente manera: **fec0:0000:0000:ffff:0000:0000:0000:0001**.

- **fe80::1**

De nuevo, se ha utilizado la regla n.º 2; la dirección expandida es **fe80:0000:0000:0000:0000:0000:0000:0001**.

- **fe80::4cd2:ffa1::1**

Esta dirección es incorrecta (está mal formada), pues se ha contraído dos veces, de modo que resulta imposible determinar el número de ceros que faltan.

3. Cálculo de subredes

Objetivo: calcular subredes con VLSM

La empresa Formacion.eni desea dividir su red optimizando el número de direcciones por subred. Esta empresa quiere, de este modo, segmentar la red 172.19.0.0 /16 en 4 redes de distintos tamaños: 2 redes de 450 puestos, 1 red de 60 puestos y 1 red de 20 puestos.

Solución

Abreviaturas utilizadas:

- Dirección de red: @R
- Dirección IPv4 en binario: @IP
- Dirección de difusión o broadcast: @B
- Nueva máscara en binario: Nmb
- **1.ª etapa**: tenemos que calcular el número de bits de la parte host para cada red.

Calculamos que n es el número de bits de la parte host con la siguiente fórmula:

(2^n) - 2 □ número de direcciones deseado, es decir, (2^n) - 2 □ 450, o sea n = 9

De modo que nos hace falta una máscara de subred con 9 bits para la parte host.

- **2.ª etapa**: cálculo de la nueva máscara en binario. Restamos al número total de bits contenidos en una máscara de subred el número de bits necesario encontrado antes, es decir, 32 - 9 = 23 bits.
  - Máscara en binario: 11111111 . 11111111. 00000000 . 00000000
  - Nueva máscara en binario: 11111111 . 11111111. 11111110 . 00000000, es decir, una máscara /23
- **3.ª etapa**: cálculo de la primera red con la máscara /23 utilizando las definiciones de las dos direcciones especiales que caracterizan una red (dirección de red y dirección de difusión).
  - @IP: 10101100.00010011.00000000.00000000
  - Nmb: 11111111.11111111.11111110.00000000
  - @R1: 10101100.00010011.00000000.00000000, es decir, **172.19.0.0 /23**
  - @B1: 10101100.00010011.00000001.11111111, es decir, **172.19.1.255 /23**

  Nuestra primera red empieza, por tanto, en **172.19.0.0** y termina en **172.19.1.255** con una máscara **/23**.

  Debemos calcular nuestra segunda red de 450 puestos.

  - @B1: 10101100.00010011.00000001.11111111 a la que se agrega 1
  - Nmb: 11111111.11111111.11111110.00000000
  - @R2: 10101100.00010011.00000010.00000000, es decir, **172.19.2.0 /23**
  - @B2: 10101100.00010011.00000011.11111111, es decir, **172.19.3.255 /23**

Nuestra segunda red empieza, por tanto, en **172.19.2.0** y termina en **172.19.3.255** con una máscara **/23**.

Ahora debemos recalcular nuestra máscara de subred para una red de 60 puestos.

- **1.ª etapa**: cálculo del número de bits de la parte host.

(2^n) - 2 □ número de direcciones deseado, es decir (2^n) - 2 □ 60, o sea, n = 6

- **2.ª etapa**: cálculo de la nueva máscara en binario: 32 - 6 = 26 bits.
  - Nueva máscara en binario: 11111111 . 11111111. 11111111 . 11000000, es decir, una máscara /26
- **3.ª etapa**: cálculo de la primera red con la máscara **/26**.
  - @B2: 10101100.00010011.00000011.11111111 a la que se agrega 1
  - Nmb: 11111111.11111111.11111111.11000000
  - @R3: 10101100.00010011.00000100.00000000, es decir, **172.19.4.0 /26**
  - @B3: 10101100.00010011.00000100.00111111, es decir, **172.19.4.63 /26**

Nuestra tercera red empieza, por tanto, en **172.19.4.0** y termina en **172.19.4.63** con una máscara **/26**.

A continuación recalculamos nuestra máscara de subred para una red de 20 puestos.

- **1.ª etapa**: cálculo del número de bits de la parte host.

Calculamos que n es el número de bits de la parte host con la siguiente fórmula:

(2^n) - 2 ≥ número de direcciones deseado, es decir, (2^n) - 2 ≥ 20, o sea n = 5

- **2.ª etapa**: cálculo de la nueva máscara en binario: 32 - 5 = 27 bits.
  - Nueva máscara en binario: 11111111 . 11111111. 11111111 . 11100000, es decir, una máscara /27
- **3.ª etapa**: cálculo de la primera red con la máscara /27.
  - @B3: 10101100.00010011.00000100.00111111 a la que se agrega 1
  - Nmb: 11111111.11111111.11111111.11100000
  - @R4: 10101100.00010011.00000100.01000000, es decir, **172.19.4.64 /27**
  - @B4: 10101100.00010011.00000100.01011111, es decir, **172.19.4.95 /27**

Nuestra cuarta red empieza, por tanto, en **172.19.4.64** y termina en **172.19.4.95** con una máscara **/27**.

Validación de conocimientos adquiridos: preguntas/respuestas

1. Preguntas

Puede validar los conocimientos adquiridos respondiendo a las siguientes preguntas.

1 ¿Cuál es la característica de una dirección de red?

2 Enumere las distintas clases de direcciones IPv4, en forma de tabla. Precise su naturaleza (pública/privada).

3 Divida la red 172.25.0.0/16 en 3 subredes.

4 ¿A qué se corresponde la notación CIDR?

5 ¿Para qué sirve la tecnología NAT?

6 Enumere los mecanismos de transición IPv4 - IPv6.

7 Defina los distintos tipos de direcciones IPv6.

8 ¿Cuáles son las direcciones IPv6 equivalentes a las siguientes direcciones IPv4: dirección de bucle invertido, dirección APIPA, dirección de multidifusión?

9 ¿Cuáles son las características de una dirección global unicast IPv6?

2. Resultados

Consulte las siguientes páginas para comprobar sus respuestas.

Por cada respuesta correcta, cuente un punto.

Número de puntos: /9

Para superar este capítulo, su puntuación mínima debería ser de 7 sobre 9.

3. Respuestas

1 ¿Cuál es la característica de una dirección de red?

La característica de una dirección de red es la siguiente: posee todos los bits de la parte host a cero. Recordemos que la máscara de subred permite determinar la parte de red y la parte host de una dirección IP.

2 Enumere las distintas clases de direcciones IPv4, en forma de tabla. Precise su naturaleza (pública/privada).

Clase	Primer byte en decimal	Máscara de subred por defecto	Pública / Privada
A	1.0.0.0 – 126.255.255.255	255.0.0.0	Pública
	10.0.0.0 – 10.255.255.255		Privada
B	128.0.0.0 – 191.255.255.255	255.255.0.0	Pública
	172.16.0.0 – 172.31.255.255		Privada
C	192.0.0.0 – 223.255.255.255	255.255.255.0	Pública
	192.168.0.0 – 192.168.255.255		Privada

3 Divida la red 172.25.0.0/16 en 3 subredes.

Nueva máscara en notación CIDR / 18

1.ª red: ***172.16.0.0****, dirección de difusión:* ***172.16.63.255***

2.ª red: ***172.16.64.0****, dirección de difusión:* ***172.16.127.255***

3.ª red: ***172.16.128.0****, dirección de difusión:* ***172.16.191.255***

4 ¿A qué se corresponde la notación CIDR?

La notación CIDR es otra manera de escribir la máscara de subred, se corresponde con el número de bits a 1. Por ejemplo, 255.255.0.0 se escribe en notación CIDR /16.

5 ¿Para qué sirve la tecnología NAT?

La tecnología NAT es un mecanismo que permite a las direcciones privadas (no enrutables en Internet) acceder a Internet utilizando la dirección IPv4 pública del router del sitio.

6 Enumere los mecanismos de transición IPv4 - IPv6.

Los mecanismos que permiten a una red IPv4 comunicarse con una red IPv6 son: los mecanismos ISATAP, Teredo, 6to4 y el Port Proxy.

7 Defina los distintos tipos de direcciones IPv6.

Existen tres tipos de direcciones IPv6: Monodifusión, Multidifusión, Anycast.

8 ¿Cuáles son las direcciones IPv6 equivalentes a las siguientes direcciones IPv4: dirección de bucle invertido, dirección APIPA, dirección de multidifusión?

La correspondencia es la siguiente:

***IPv4**: Dirección de bucle invertido 127.0.0.1 - **IPv6** : ::1*

***IPv4**: Dirección APIPA 169.254.0.0/16 - **IPv6** dirección de enlace local: FE80::/64*

***IPv4**: Multidifusión 224.0.0.0/4 - **IPv6** : FF00::/8*

9 ¿Cuáles son las características de una dirección global unicast IPv6?

Una dirección global Unicast se corresponde con una dirección IPv4 pública y permite designar a un equipo en la red Internet.

Caracterizadas por el prefijo 2000::/3, es posible reservarlas desde 1999. Algunos bloques se reservan para la implementación del túnel 6to4 (por ejemplo, el bloque 2002::/16).

Requisitos previos y objetivos

1. Requisitos previos

Tener nociones acerca del direccionamiento IP.

Conocer los distintos parámetros que componen una configuración IP.

Conocer la diferencia entre un direccionamiento estático y dinámico.

2. Objetivos

Definición del rol DHCP.

Presentación de las funcionalidades ofrecidas por el servicio.

Gestión de la base de datos.

Implementar el mantenimiento del servidor DHCP.

Implementar un agente de retransmisión DHCP.

Introducción

El servidor DHCP (*Dynamic Host Configuration Protocol*) es un rol muy importante en una arquitectura de red. Su papel es la distribución de la configuración IP, permitiendo así a los equipos conectados a la red dialogar entre ellos.

Rol del servicio DHCP

DHCP es un protocolo que permite asegurar la configuración automática de las interfaces de red. Esta configuración comprende un direccionamiento IP, una máscara de subred y, también, una puerta de enlace y servidores DNS. Existen otros parámetros suplementarios que también pueden distribuirse (servidores WINS…).

El tamaño de las redes actuales obliga, cada vez más, a eliminar el direccionamiento estático coordinado por un administrador sobre cada máquina por un direccionamiento dinámico realizado mediante un servidor DHCP. Éste presenta la ventaja de que ofrece una configuración completa a cada máquina que realice la petición pero también es imposible encontrar dos configuraciones idénticas (dos direcciones IP idénticas distribuidas). El conflicto de IP se evita, de este modo, y la administración se ve ampliamente simplificada.

El servidor es capaz de realizar una distribución de configuración IPv4 o IPv6.

1. Funcionamiento de la concesión de una dirección IP

Si la interfaz de red está configurada para obtener un contrato DHCP, obtendrá un contrato mediante un servidor DHCP. Esta acción se realiza mediante el intercambio de varias tramas entre el cliente y el servidor.

La máquina envía, por multidifusión (envío de un *broadcast*), una trama (**DHCP Discover**) sobre el puerto 67.

Todos los servidores que reciben la trama envían una oferta DHCP al cliente (**DHCP Offer**), el cual puede, evidentemente, recibir varias ofertas. El puerto utilizado para recibir la oferta es el 68.

El cliente retiene la primera oferta que recibe y difunde por la red una trama (**DHCP Request**). Ésta compone la dirección IP del servidor y la que se le acaba de proponer al cliente, con el objetivo de aceptar el contrato enviado por el servidor seleccionado y, también, para informar al resto de servidores DHCP de que sus contratos no han sido seleccionados.

El servidor envía una trama de acuse de recibo (**DHCP ACK**, *Acknowledgement*) que asigna al cliente la dirección IP y su máscara de subred así como la duración del contrato y, eventualmente, otros parámetros.

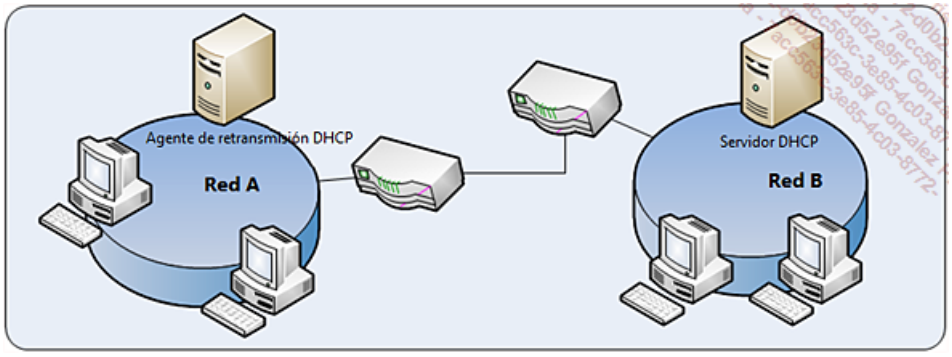
La lista de opciones que el servidor DHCP puede aceptar está definida en la RFC 2134.

Un contrato DHCP (configuración asignada a un puesto) tiene una duración de validez, variable de tiempo que define el administrador. Alcanzado el 50% de la duración del contrato, el cliente solicita una renovación del contrato que se le ofreció. Esta solicitud se realiza únicamente al servidor que envió el contrato. Si éste no renueva el contrato, la próxima solicitud se realizará alcanzado el 87,5% de la duración del contrato. Una vez finalizado el mismo, si el cliente no consigue obtener una renovación o una nueva concesión, su dirección se deshabilita y pierde la capacidad de utilizar la red TCP/IP.

2. Uso de una retransmisión DHCP

El hecho de utilizar tramas de tipo *broadcast* hace que las tramas no puedan circular por los routers. Esto implica tener un servidor por cada subred IP. Esta obligación de tener varios servidores puede suponer un coste excesivo para la empresa. Para solventar este problema conviene implementar un servidor de retransmisión DHCP, que permite transferir las solicitudes de contrato a un servidor presente en otra red.

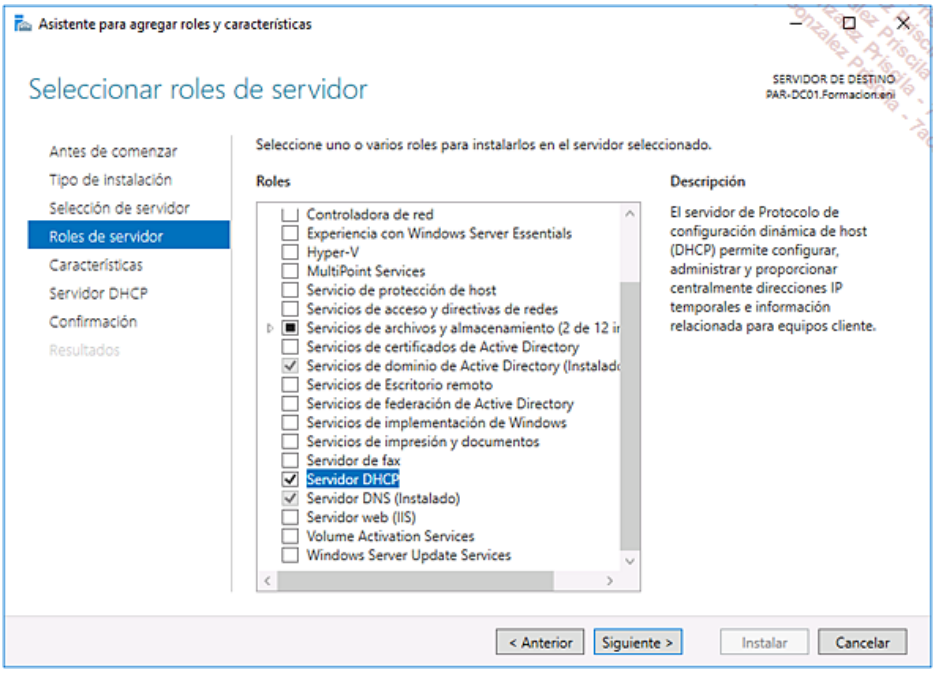
La retransmisión DHCP se instala sobre la red A y permite recuperar las solicitudes de DHCP realizadas sobre la subred IP. Transfiere, a continuación, las distintas solicitudes que recibe al servidor DHCP presente en la red B.



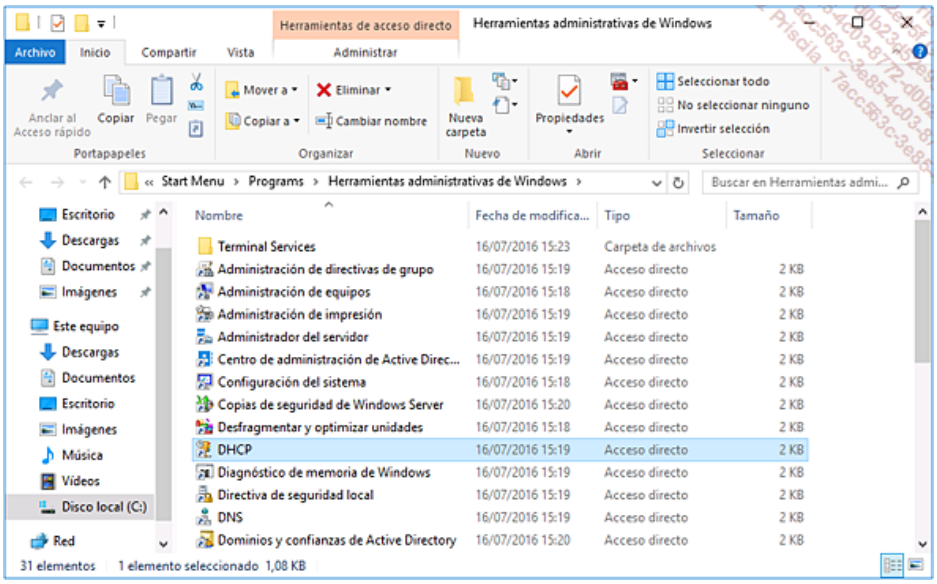
Conviene, no obstante, asegurar que la tasa de transferencia de la línea y el tiempo de respuesta son aceptables.

Instalación y configuración del rol DHCP

Como con los demás servicios que pueden agregarse al servidor, DHCP es un rol. Su instalación se realiza mediante la consola Administrador del servidor marcando el rol en la ventana de selección de rol.



Una vez realizada la instalación, la consola se encuentra en las Herramientas administrativas.



El rol se ha instalado pero todavía no está configurado.

1. Agregar un nuevo ámbito

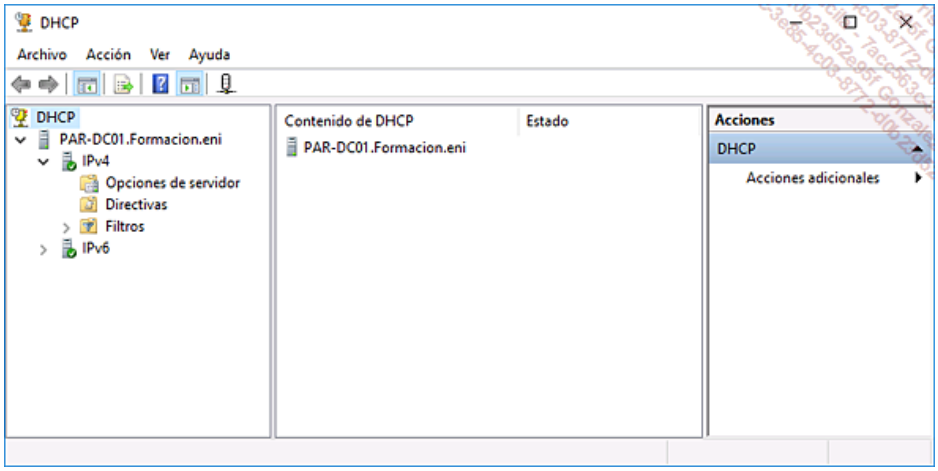
Un ámbito DHCP está formado por un pool de direcciones IP (por ejemplo, 172.16.0.10 a 172.16.0.200), cuando un cliente realiza una solicitud, el servidor DHCP le asigna una de las direcciones del pool.

La franja de direcciones IP disponibles en el ámbito es, necesariamente, contigua. Para evitar la distribución de algunas direcciones IP es posible realizar exclusiones de una dirección o un tramo. Estas últimas pueden asignarse a un puesto de forma manual, sin riesgo de que se produzca un conflicto de IP, puesto que el servidor no distribuirá estas direcciones.

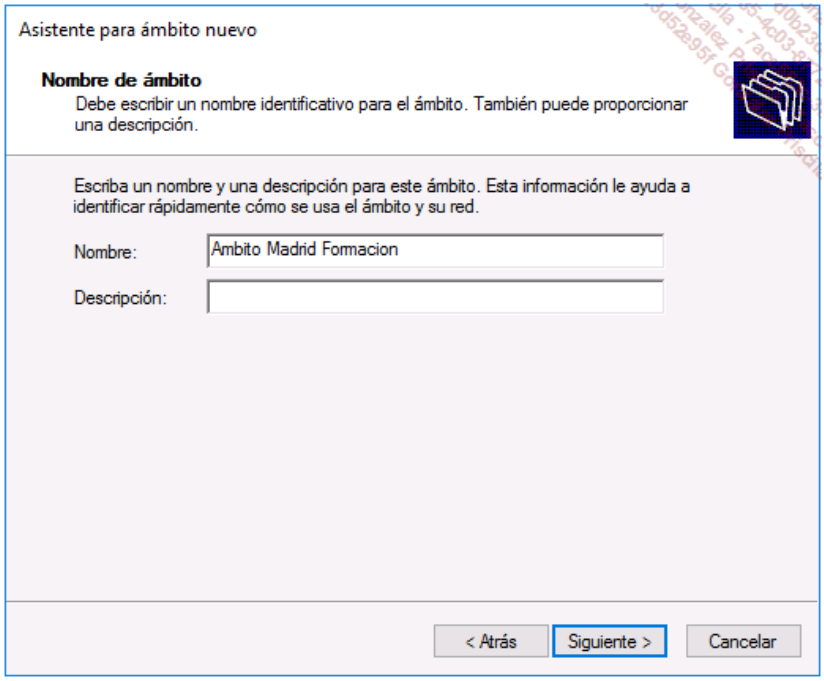
Uso de la regla 80/20 para los ámbitos

Es posible tener dos servidores DHCP activos en la red, dividiendo el pool de direcciones en dos. La regla del 80/20 permite, en un primer momento, equilibrar el uso de los servidores DHCP, aunque, también, poder tener dos servidores sin riesgo de conflicto de IP. El servidor 1 distribuye el 80% del pool de direcciones mientras que el servidor 2 está configurado para distribuir las direcciones restantes (20%).

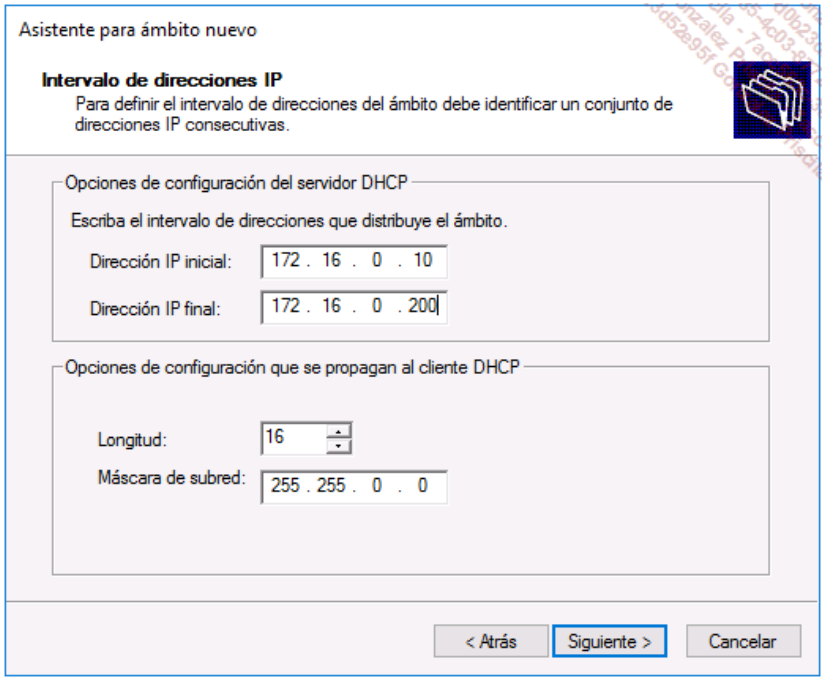
Desplegando **PAR-DC01.Formacion.eni** y, a continuación, **IPv4** podemos ver que no existe ningún ámbito. Debemos crear uno para que el servidor pueda distribuir rangos de direcciones.



De este modo, haciendo clic con el botón derecho sobre IPv4, es posible crear un nuevo ámbito. Éste tendrá un nombre que debemos indicar en el asistente de creación.

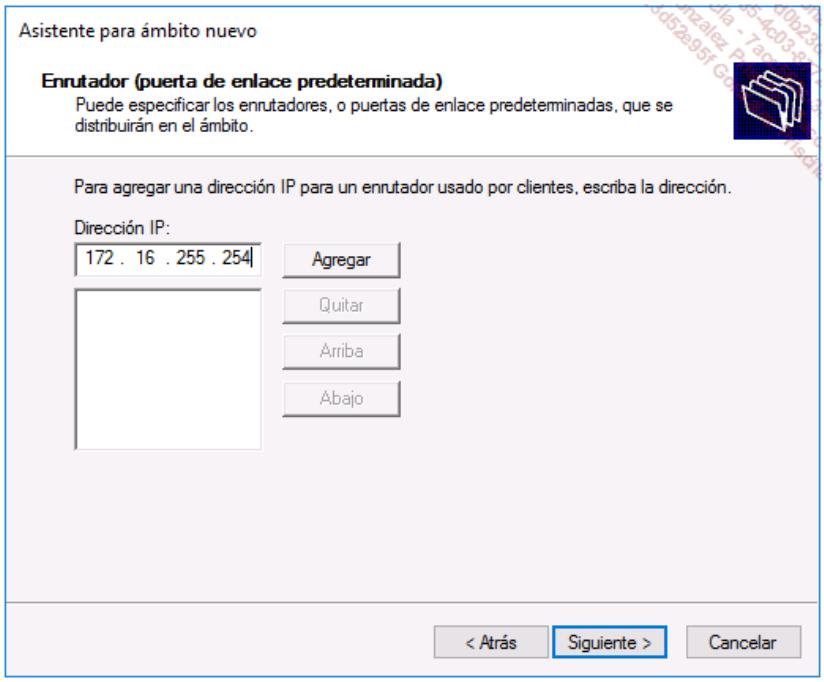


A continuación es preciso definir el rango de direcciones disponibles (de 172.16.0.10 a 172.16.0.200).



Es posible tener, en este rango, ciertas direcciones que es preciso excluir, pues están asignadas a impresoras… Es posible configurar la lista de exclusión, que contiene una dirección o un rango de direcciones que no pueden configurarse en el rango direccionable.

Un contrato contiene, también, una duración cuyo valor por defecto es de 8 días. Evidentemente, es posible aumentar o disminuir este valor. A continuación, es posible indicar la dirección de la o las puertas de enlace que deben utilizarse. También puede indicarse el o los servidores DNS que se desean configurar. Estas opciones (DNS, puerta de enlace predeterminada…) se distribuyen, a continuación, al cliente que realiza la petición de contrato de modo que es preferible asegurarse de toda la información indicada.

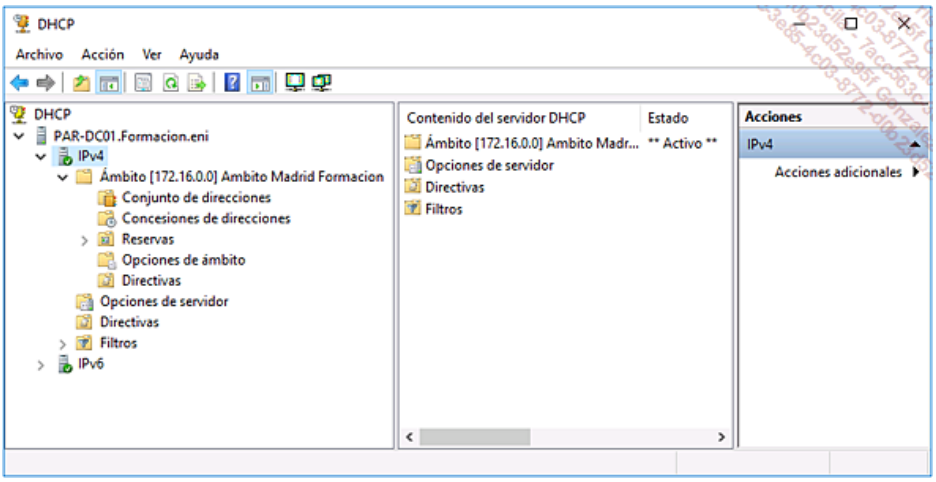


En un dominio Active Directory es necesario proceder a autorizar el servidor DHCP. Los servidores DHCP Microsoft no autorizados verán cómo Active Directory detiene su servicio.

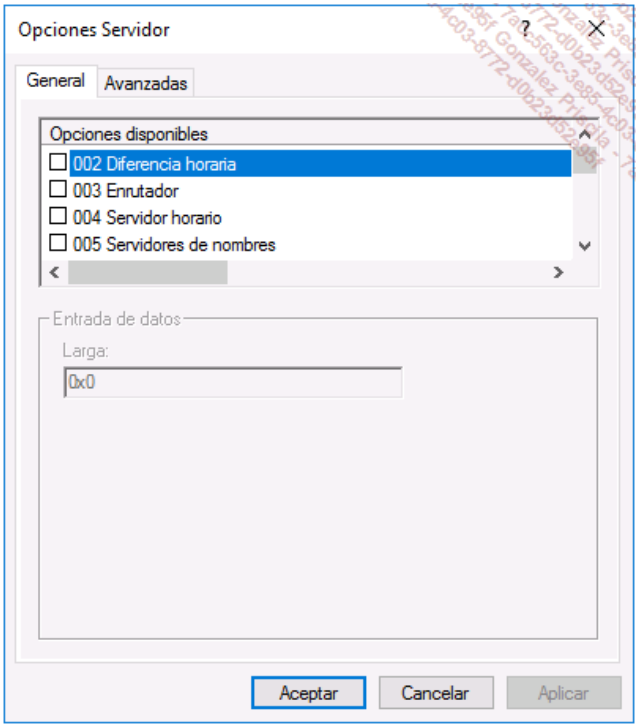
2. Configuración de las opciones DHCP

Las opciones permiten distribuir opciones suplementarias en el contrato, tales como el nombre del dominio DNS y la dirección del servidor DNS. Existen tres tipos de opciones:

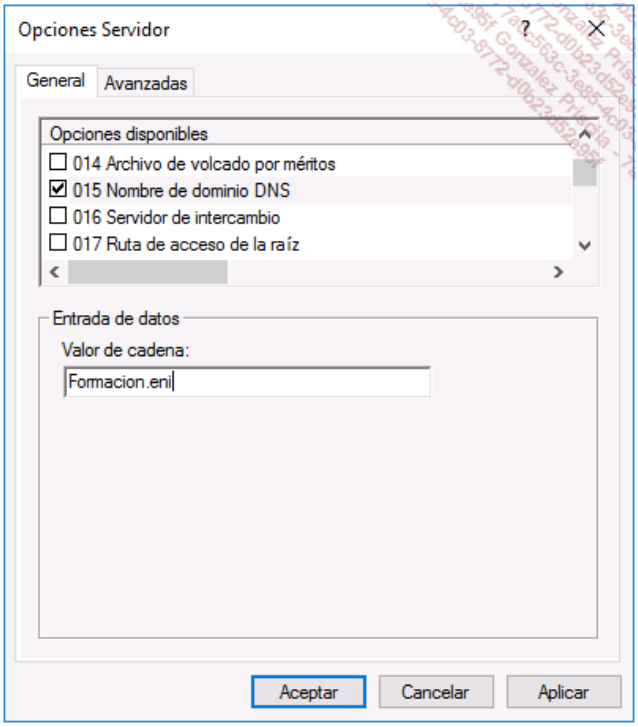
- **Opciones de servidor**: se aplican a todos los ámbitos del servidor así como a las reservas. **Si la misma opción se configura en las opciones del ámbito, es ésta última la que se aplica, mientras que la opción del servidor se ignora**.



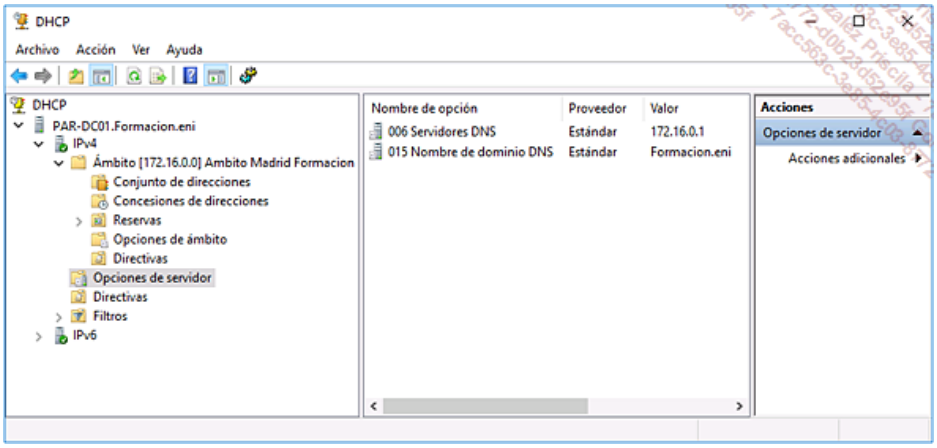
Haciendo clic con el botón derecho en **Opciones de servidor** y seleccionando la opción **Configurar opciones** en el menú contextual se muestra una ventana que permite configurar la opción deseada.



De este modo, la opción **015 Nombre de dominio DNS** permite configurar el nombre del dominio DNS; en nuestro caso Formacion.eni.



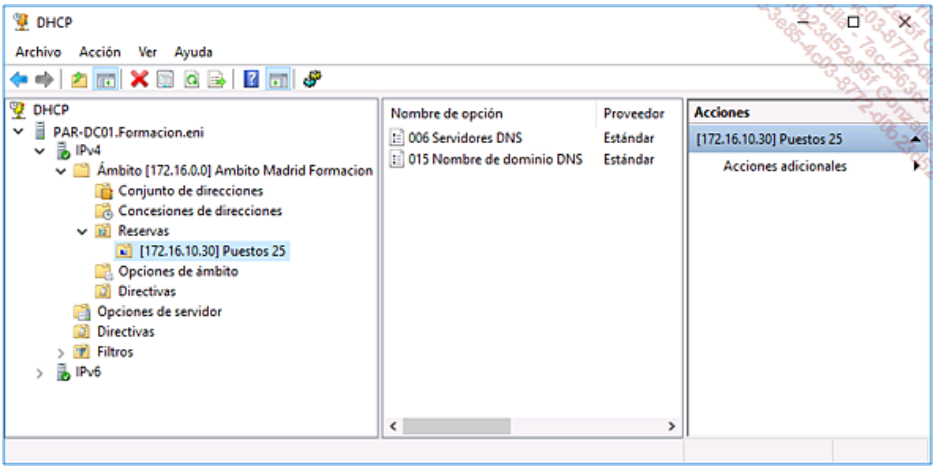
Las opciones también aparecen en opciones de ámbito y en las opciones de reservas.



- **Opciones de ámbito**: se aplican únicamente al ámbito. Cada uno posee sus opciones, las cuales pueden ser diferentes de un ámbito a otro.

No obstante, si se configura una misma opción en las opciones de servidor y de ámbito, la opción de ámbito resulta prioritaria sobre la del servidor.

- **Opciones de reservas**: se aplican únicamente a las reservas, cada reserva puede tener opciones diferentes.



3. Reserva de contrato DHCP

Las reservas DHCP permiten asegurar que un cliente configurado para recibir un contrato tendrá, sistemáticamente, la misma configuración. Esto resulta muy útil para las impresoras de red que se quieren mantener con un direccionamiento dinámico. Esto permite asegurar que tendrán siempre la misma dirección IP. En caso de que existan varios servidores DHCP en una misma red, la reserva debe crearse de forma duplicada en los demás servidores.

La creación de una reserva requiere introducir los siguientes datos:

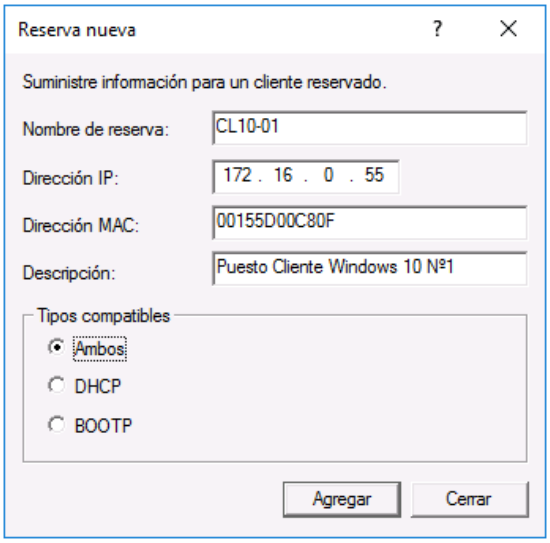
- **El nombre de la reserva**: este campo contiene, por lo general, el nombre del puesto o de la impresora afectada por esta reserva.
- **La dirección IP**: indica la dirección que se distribuye al cliente.
- **La dirección MAC**: debe indicarse la dirección MAC de la interfaz de red que hace la petición.

En la consola DHCP, haga clic con el botón derecho en **Reservas** y, a continuación, seleccione **Reserva nueva**.

De este modo, la reserva de la dirección IP para CL10-01 requiere la configuración de la ventana **Reserva nueva** tal y como se indica a continuación:

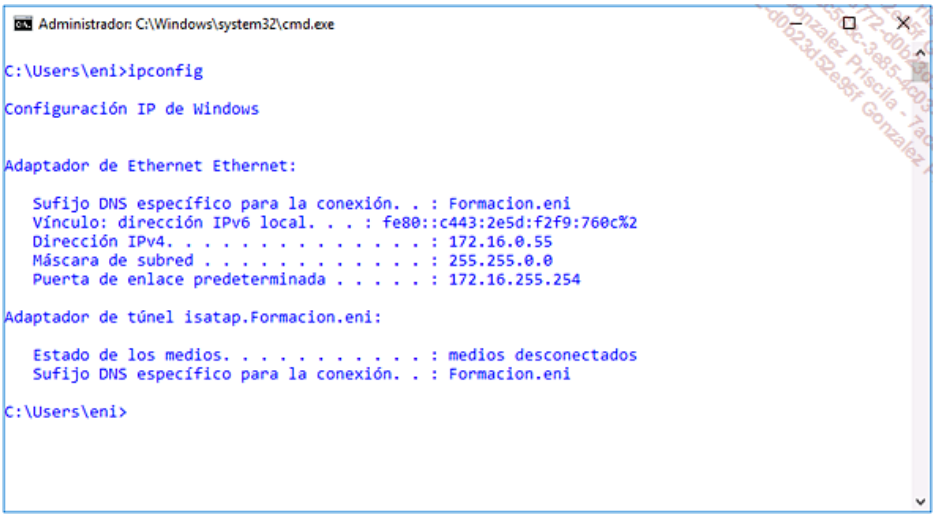
- **Nombre de reserva**: CL10-01
- **Dirección IP**: 172.16.0.55
- **Dirección MAC**: escriba la dirección MAC de la máquina CL10-01 (ejecute el comando `ipconfig /all` sobre el puesto cliente).

La descripción es un campo opcional. Permite agregar alguna información suplementaria.

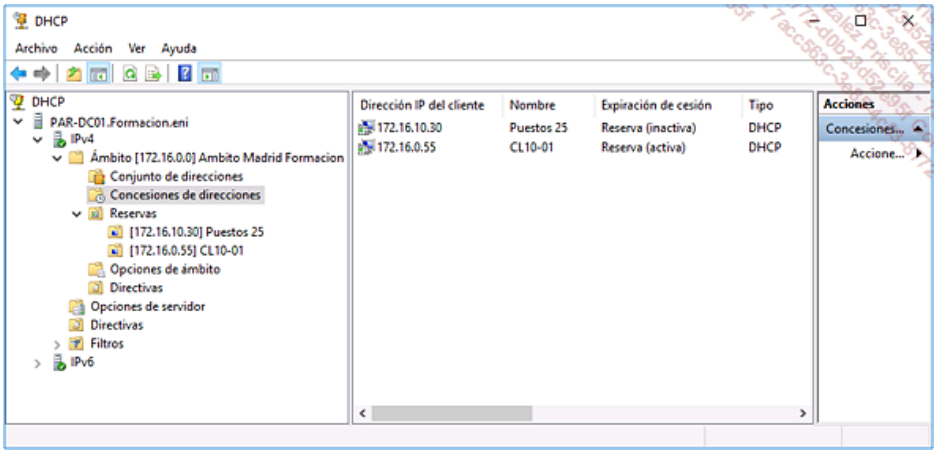


En el puesto cliente, es preciso ejecutar el comando `ipconfig /release` en una ventana de comandos DOS para liberar el comando DHCP en curso. El comando `ipconfig /renew` permite realizar una nueva petición de configuración al servidor.

Comprobamos que la dirección IP asignada es la reservada.



La reserva aparece marcada como activa en la consola DHCP.



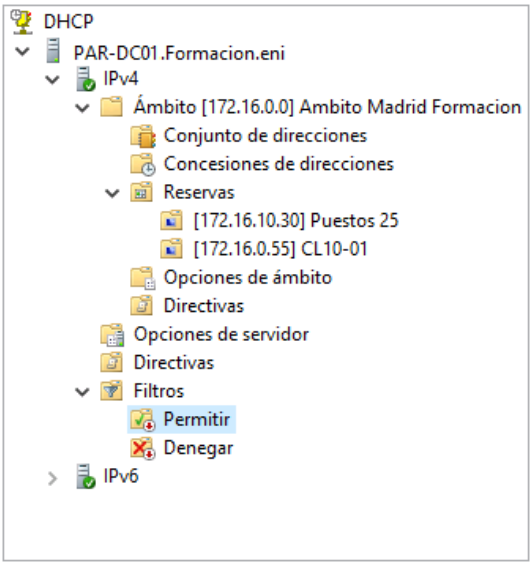
Una novedad aparecida con Windows Server 2012 es la implementación de filtros en el servicio DHCP.

4. Implementación de filtros

Los filtros permiten crear listas verdes y listas de exclusión. La lista verde permite, a todas las interfaces de red cuyas direcciones MAC pertenecen a ella, obtener un contrato DHCP. Está representada por la carpeta **Permitir** en el nodo **Filtros**. La lista de exclusión, a diferencia de la lista verde, prohíbe el acceso al servicio a todas las direcciones MAC referenciadas. Está representada por la carpeta **Denegar**.

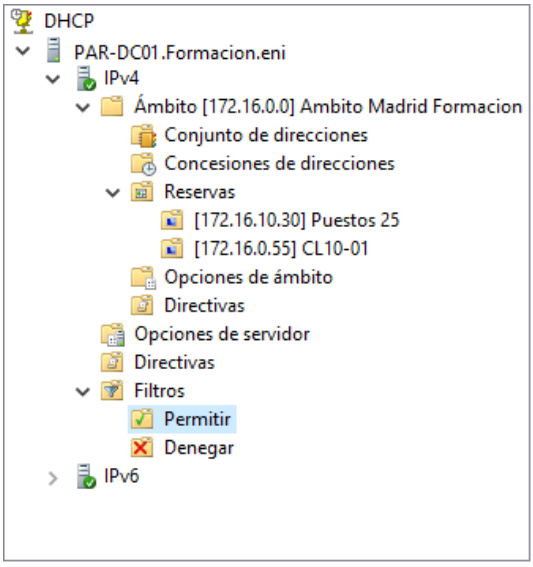
Esta funcionalidad vuelve más pesada las tareas de administración, puesto que es necesario introducir a mano la dirección MAC de una nueva máquina para que pueda recibir un contrato.

Se recomienda crear filtros antes de habilitar la funcionalidad, pues en caso contrario, ninguna máquina de su red podrá solicitar un contrato DHCP.

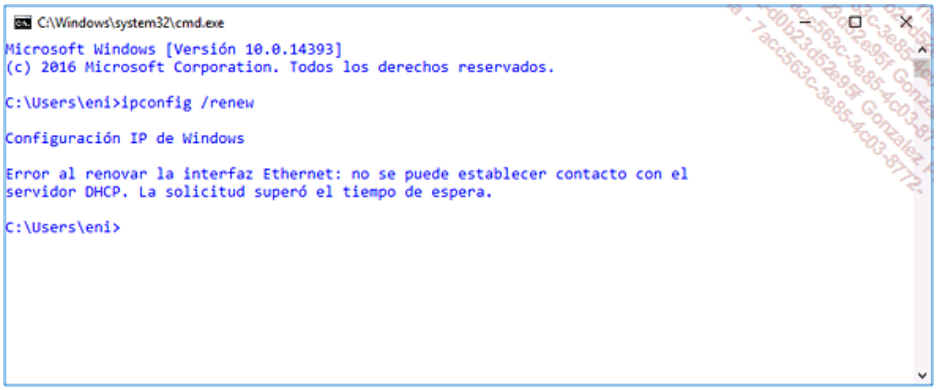


Por defecto, ambas listas estás deshabilitadas.

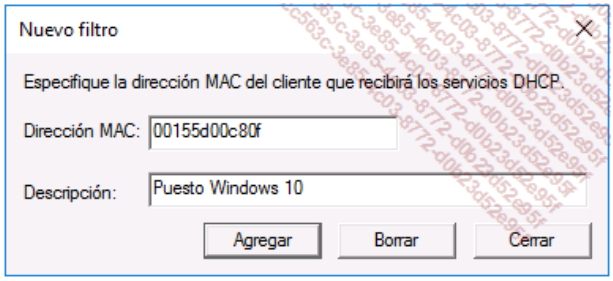
Para habilitar una de las listas, haga clic con el botón derecho sobre el nodo **Permitir** y, a continuación, seleccione **Activar**. Realice la misma operación para la lista **Denegar**.



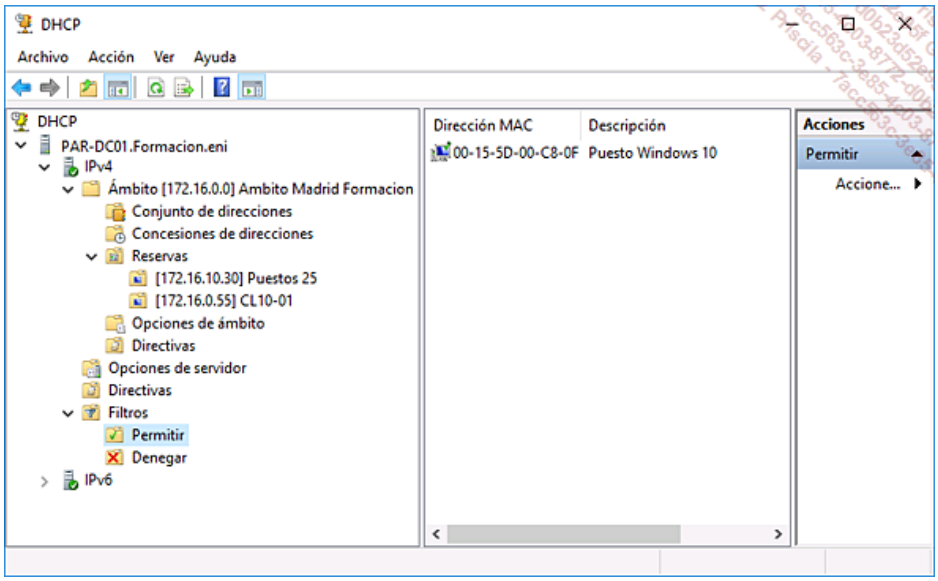
De este modo, si el contrato se libera sobre el puesto (`ipconfig /release`) y, a continuación, se renueva (`ipconfig /renew`), aparece un mensaje de error sobre el puesto informándonos de que el servidor DHCP no ha respondido.



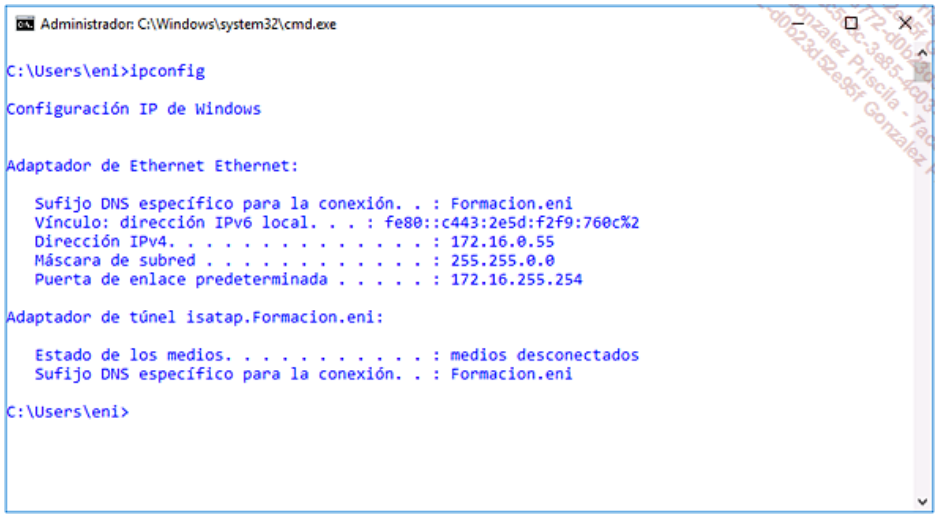
Es, por tanto, necesario crear un nuevo filtro; para ello es preciso hacer clic con el botón derecho en **Permitir** y, a continuación, seleccionar la opción **Nuevo filtro**. Escriba la dirección MAC de CL10-01 y una descripción del nuevo filtro.



Una vez agregado, el filtro aparece en el nodo **Permitir**.



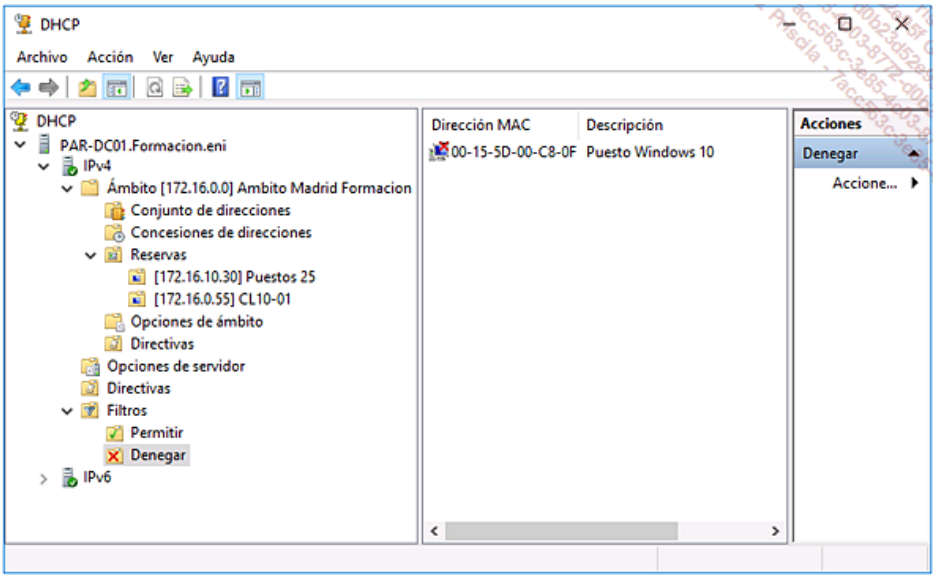
La solicitud de contrato se acepta y el puesto recibe una configuración.



Es, evidentemente, posible pasar un filtro de una lista a otra. Si hace clic con el botón derecho sobre el filtro creado anteriormente, verá la opción **Mover a denegados**.

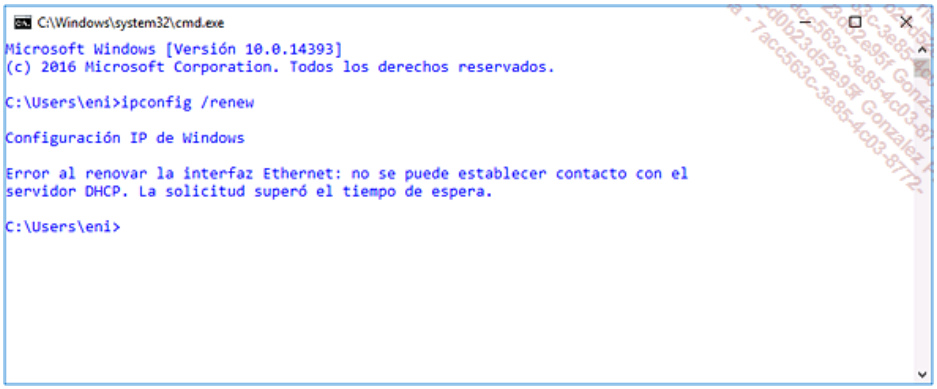
En la carpeta **Permitir**, haga clic con el botón derecho en el filtro que acaba de crear y, a continuación, seleccione **Mover a denegados**.

Es posible realizar la misma operación para desplazar un filtro desde la lista de exclusión a la lista verde.



La máquina no puede obtener un contrato nuevo.

Como ocurría hace un momento, el servidor ya no responde a la máquina.



Base de datos DHCP

La base de datos DHCP permite registrar información (dirección MAC…) tras la distribución de un contrato nuevo.

1. Presentación de la base de datos DHCP

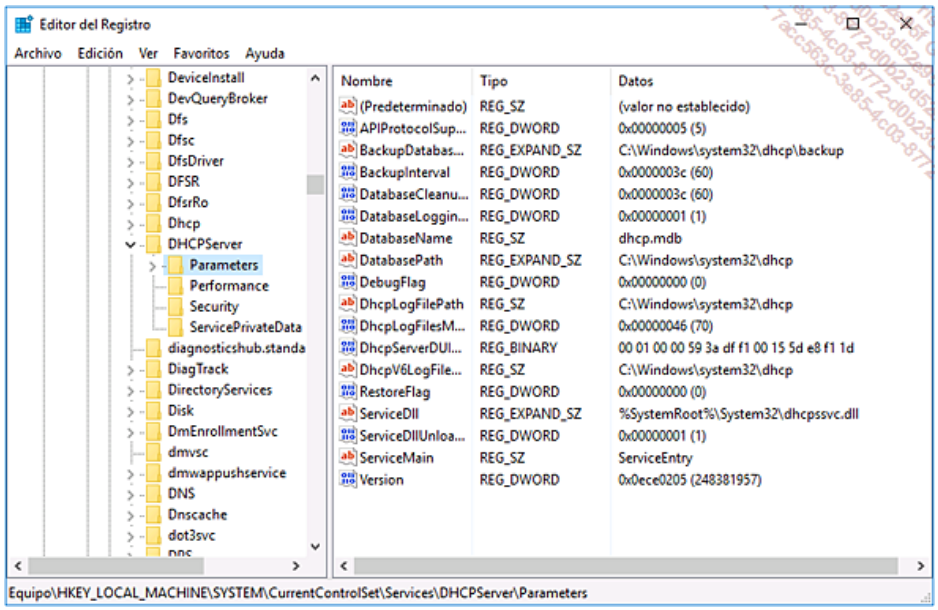
La base de datos almacena un número ilimitado de registros, el tamaño del archivo depende del número de equipos presentes en la red. Por defecto, se almacena en la carpeta Windows\System32\Dhcp.

Esta carpeta contiene varios archivos:

- **Dhcp.mdb**: base de datos del servicio DHCP. Posee un motor de tipo Exchange Server JET.
- **Dhcp.tmp**: este archivo se utiliza como archivo de intercambio cuando se realiza el mantenimiento de los índices sobre la base de datos.
- **J50.log**: permite registrar las transacciones.
- **J50.chk**: archivo con los puntos de verificación.

Con cada operación (nueva petición, renovación o liberación de contrato), la base de datos se actualiza y se crea una entrada en la base de datos de registro.

La información en la base de datos del registro puede encontrarse accediendo a la clave:HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DHCPServer\Parameters.



2. Copia de seguridad y restauración de la base de datos

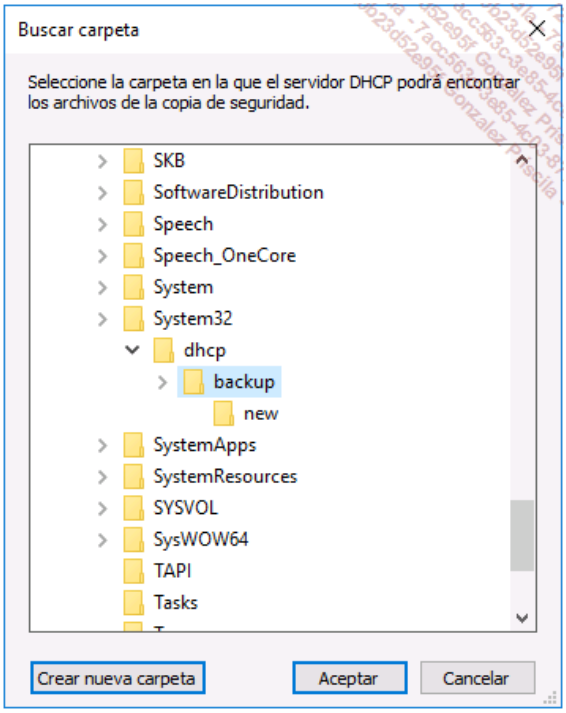
Es posible realizar una copia de seguridad de la base de datos de forma manual (copia de seguridad asíncrona) o automática (copia de seguridad síncrona).

La copia de seguridad síncrona se realiza por defecto en la carpeta Windows\system32\Dhcp\Backup. Se recomienda mover esta carpeta a otro volumen con el objetivo de que no se elimine cuando se realiza una reinstalación. La copia de seguridad asíncrona se realiza manualmente en el momento deseado. Esta operación requiere, al menos, permisos de administración o un usuario miembro del grupo Administradores de DHCP.

Tras la operación de copia de seguridad (síncrona o asíncrona), todos los elementos vinculados con el servidor están incluidos en la copia de seguridad. Encontramos los siguientes elementos:

- Todos los ámbitos presentes en el servidor.
- Las reservas creadas.
- Los contratos distribuidos.
- Las opciones configuradas.
- Las claves de registro y la información de configuración.

Tras la ejecución de la operación de restauración (clic con el botón derecho sobre el servidor y, a continuación, **Restaurar** en el menú contextual), debe seleccionarse la carpeta que contiene la copia de seguridad.



A continuación, se detienen los servicios DHCP y se restablece la base de datos. Como con la copia de seguridad, la operación debe realizarse con permisos de administrador.

3. Reconciliación y desplazamiento de la base de datos

La operación de reconciliación permite arreglar ciertos problemas principalmente tras la restauración de la base de datos. En efecto, los contratos DHCP se registran en dos lugares:

- En la base de datos de forma detallada.
- En la base de datos de registro de forma resumida.

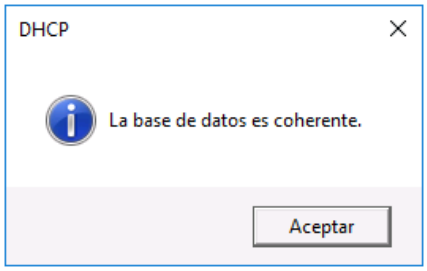
Cuando se realiza una operación de reconciliación, las entradas contenidas en la base de datos y en la base de datos de registro se comparan. Esto permite buscar eventuales incoherencias (entradas en la base de datos que no están presentes en la base de datos de registro y viceversa).

Ejemplo

En la base de datos de registro se ha asignado la dirección IP 172.16.0.88, mientras que en la base de datos posee el estado libre. Realizando una reconciliación, se crea la entrada en la base de datos.

Seleccionando la opción **Reconciliar** en el menú contextual del ámbito (clic con el botón derecho sobre el ámbito deseado), se muestra una ventana. Basta con hacer clic en el botón **Comprobar** para ejecutar la verificación.

A continuación, se muestra una ventana con el resultado de la operación.

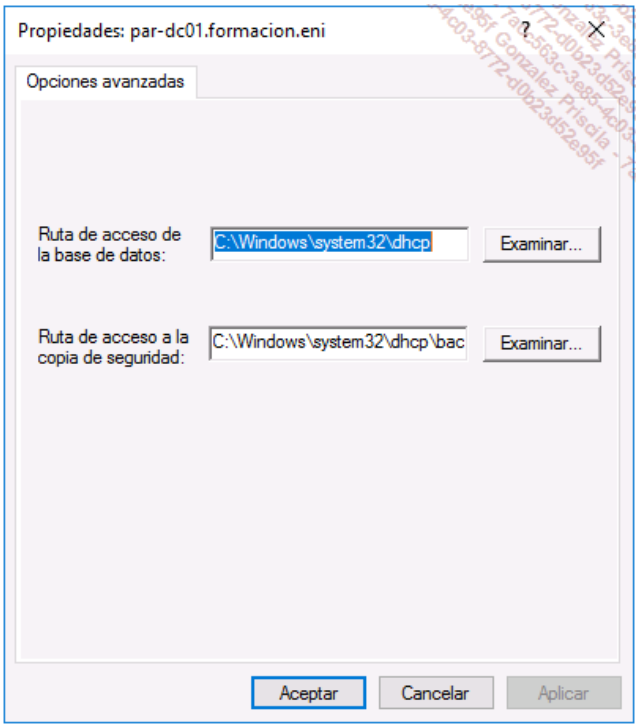


Es posible ejecutar esta operación sobre todos los ámbitos seleccionando la opción **Reconciliar todos los ámbitos...** en el menú contextual del nodo IPv4.

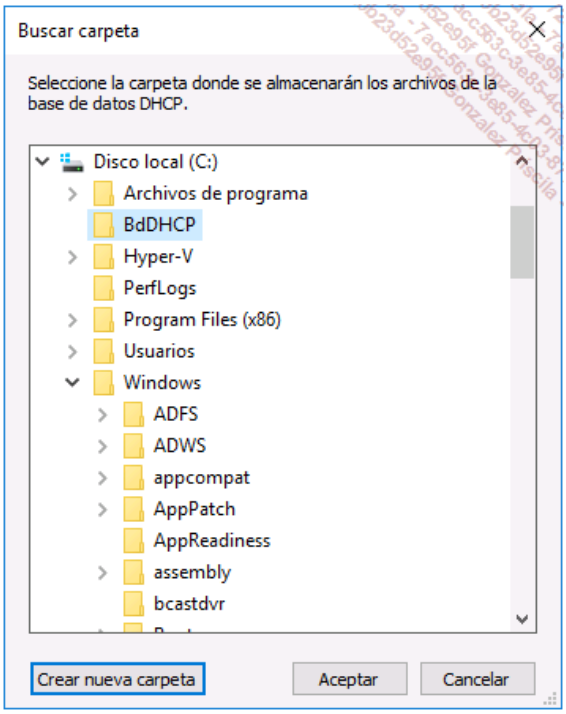
Hemos visto antes que el desplazamiento de la base de datos a otro volumen permite realizar una reinstalación del servidor sin pérdida de datos. En caso de migración del servidor DHCP, es posible utilizar ambas soluciones.

Primera solución: se crea cierto número de reservas y exclusiones de direcciones IP. No es apropiado implementar un nuevo ámbito sobre el servidor DHCP y a continuación crear las reservas y exclusiones. Esto puede resultar engorroso y generar errores más o menos inmanejables para el sistema de información. Es, por tanto, necesario realizar una copia de seguridad del antiguo servidor y, a continuación, realizar la restauración sobre el nuevo o desplazar la base de datos sobre otro volumen.

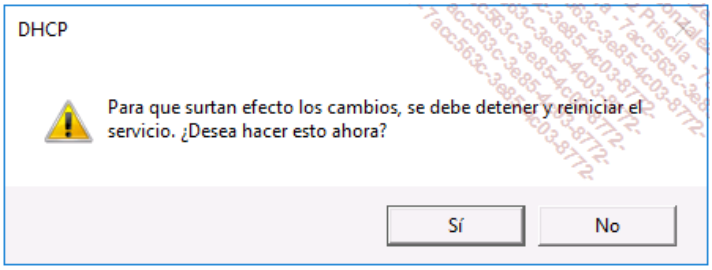
Para desplazar esta base de datos es preciso acceder a las propiedades del servidor (clic con el botón derecho sobre el servidor y, a continuación, seleccionar **Propiedades** en el menú contextual).



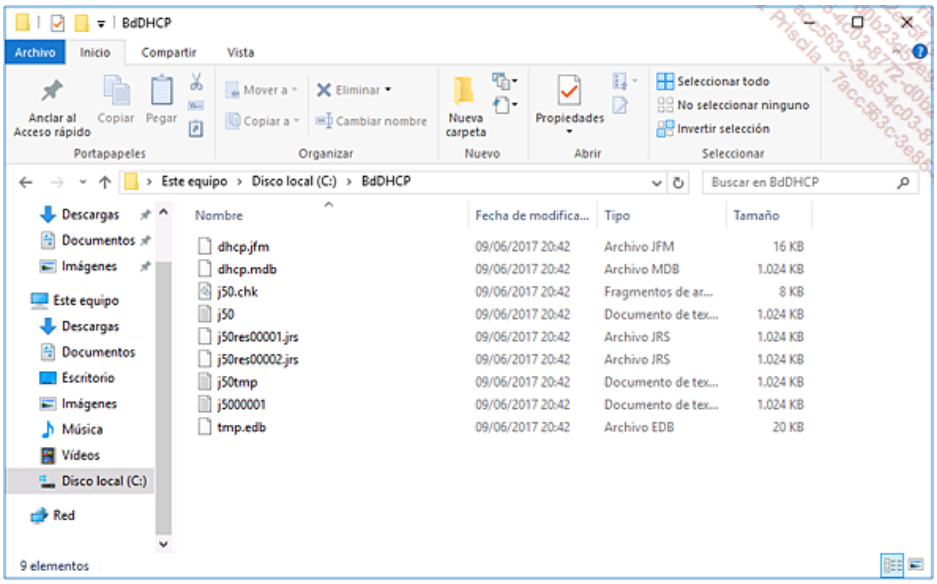
El botón **Examinar...** permite seleccionar otra carpeta.



Tras el reinicio del servicio, se tienen en cuenta los cambios.



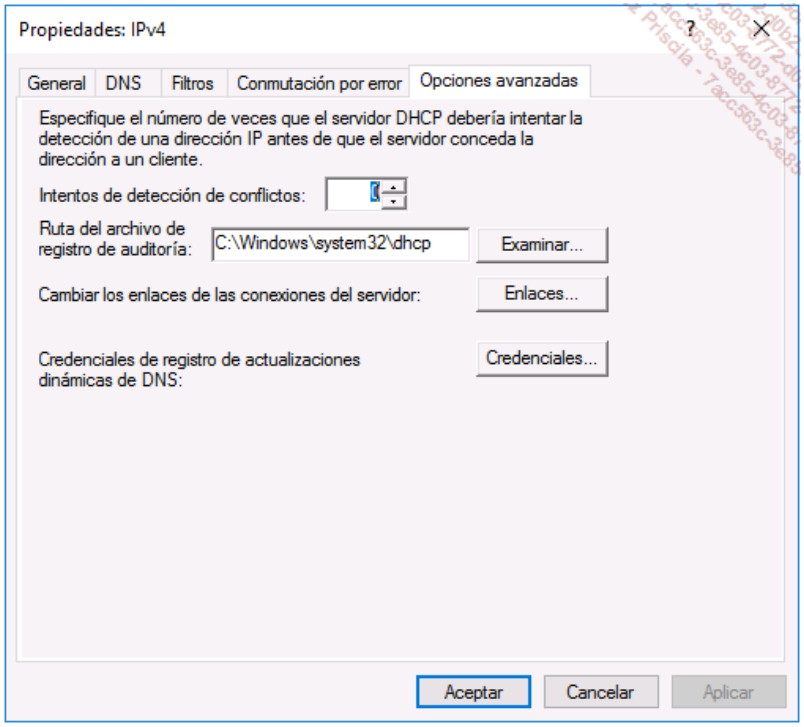
La base de datos se ha desplazado correctamente.



Si tras el reinicio del servicio no aparece el ámbito, copie todos los archivos alojados en la carpeta Windows\System32\dhcp en la nueva carpeta. El servicio debería detenerse y reiniciarse a continuación una vez finalizada la copia.

Segunda solución: no se realiza ninguna reserva en el servidor, o se crea un número muy reducido. La creación de un nuevo ámbito puede resultar abordable. No obstante, esta solución, si se implementa incorrectamente, puede causar grandes inconvenientes en el funcionamiento del sistema de información. En efecto, el nuevo servidor no tiene ninguna información acerca de los rangos DHCP que han sido distribuidos antes de la creación, y existe el riesgo de distribuir direcciones ya atribuidas a un puesto cliente. En este caso es necesario solicitar al servidor DHCP que realice una comprobación antes de atribuir una dirección.

En las propiedades del nodo **IPv4** (clic con el botón derecho sobre **IPv4** y, a continuación, **Propiedades**), existe una pestaña llamada **Opciones avanzadas**. Basta con configurar el número de intentos de detección de conflicto que debe realizar el servidor para evitar los inconvenientes ligados a los conflictos de IP.



Se distribuyen nuevos rangos sin riesgo de conflicto IP.

Alta disponibilidad del servicio DHCP

El servicio DHCP es un servicio importante en una red informática. En caso de que se detenga, no se asignan más contratos DHCP y las máquinas van perdiendo, progresivamente, acceso a la red. Para evitar esta situación es posible instalar un segundo servidor DHCP y compartir el rango de direcciones IP distribuidas (generalmente el 80% en el primer servidor y el 20% en el segundo). La segunda solución consiste en instalar un clúster DHCP, solución eficaz pero que exige ciertas competencias.

Desde la aparición de Windows Server 2012 es posible trabajar con dos servidores DHCP sin tener que montar un *clúster*. De este modo, existe un servicio DHCP disponible ininterrumpidamente sobre la red. Si alguno de los servidores no se encuentra en línea, las máquinas cliente pueden contactar con el otro servidor.

Ambos servidores replican la información de los contratos IP entre ellos, con el objetivo de permitir al otro servidor retomar la responsabilidad de la gestión de las solicitudes de los clientes. En caso de que se configure en modo equilibrio de carga, las solicitudes de los clientes se dirigen a ambos servidores.

La conmutación por error DHCP puede contener dos servidores como máximo y ofrece el servicio solo para extensiones IPv4.

La implementación de la alta disponibilidad se aborda en la parte práctica de este capítulo.

Trabajos prácticos: Instalación y configuración del rol DHCP

Los trabajos prácticos consisten en la instalación del servidor DHCP, de un agente de retransmisión y de la funcionalidad de alta disponibilidad, así como su configuración.

1. Agregar y configurar el rol DHCP

Objetivo: realizar la instalación del rol DHCP y la creación de un agente de retransmisión DHCP.

Máquinas virtuales: PAR-DC01 y CL10-01.

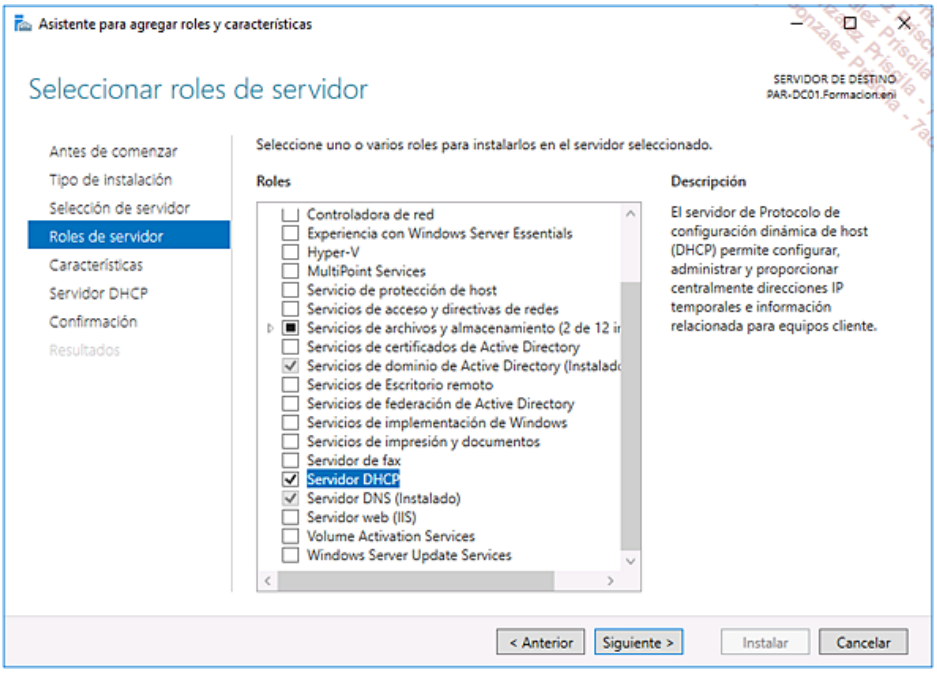
En **PAR-DC01**, abra la consola **Administrador del servidor** y, a continuación, haga clic en **Agregar roles y características**.

En la ventana **Antes de comenzar**, haga clic en **Siguiente**.

Deje marcada la opción **Instalación basada características o en roles** y, a continuación, haga clic en **Siguiente**.

En **Seleccionar servidor de destino**, deje **PAR-DC01** marcado y, a continuación, haga clic en **Siguiente**.

Marque la opción **Servidor DHCP** y, a continuación, haga clic en el botón **Agregar características** en la ventana emergente.



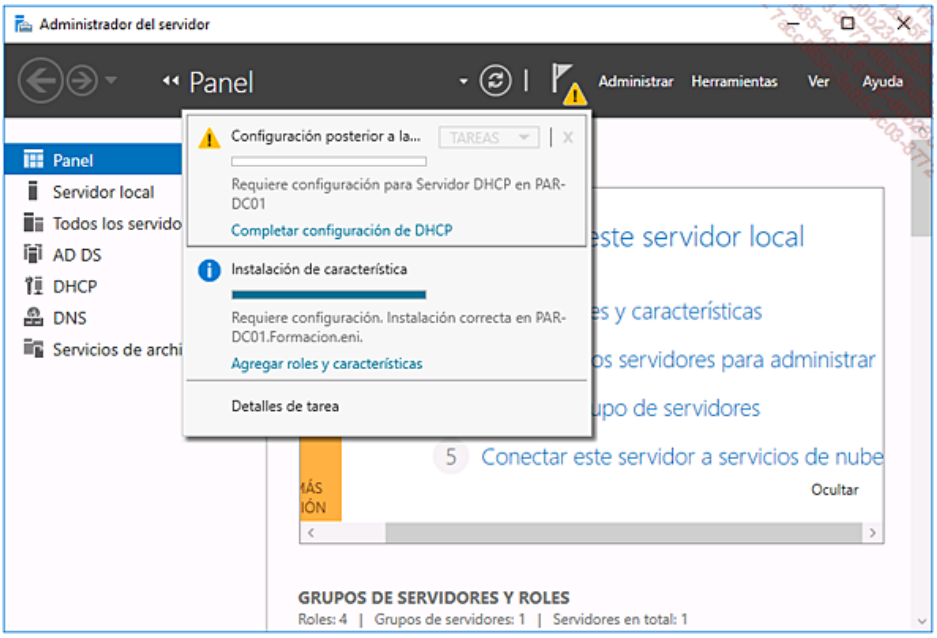
Haga clic en **Siguiente** en la ventana **Seleccionar características**.

Haga clic en **Siguiente** y, a continuación, en **Instalar**.

Espere a que finalice la instalación y haga clic en **Cerrar**.

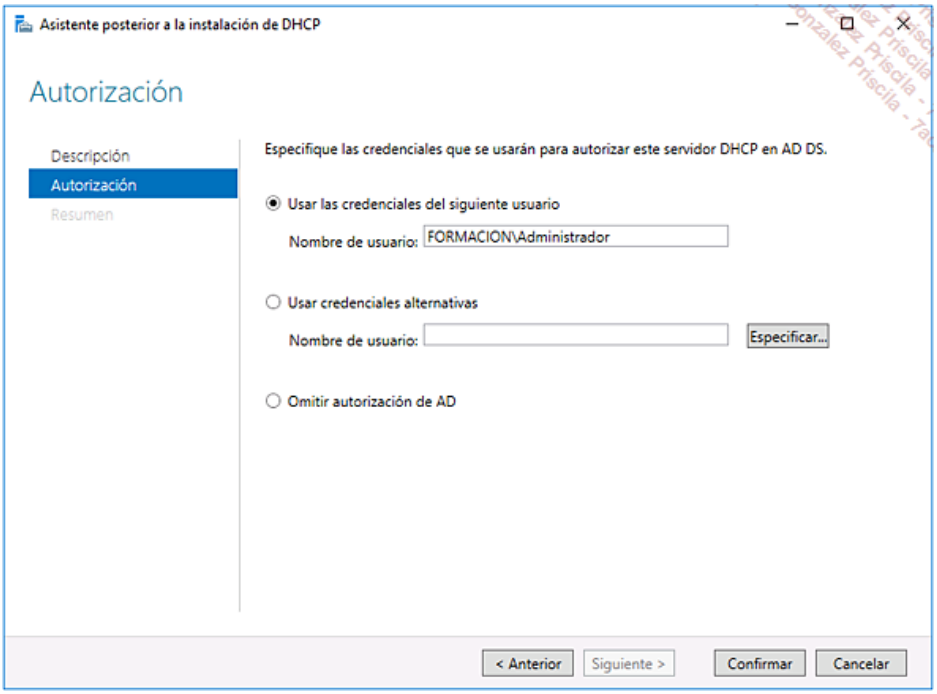
En la consola **Administrador del servidor**, haga clic en el icono que representa una bandera.

Haga clic en el enlace **Completar configuración de DHCP**.



Se abre el asistente de configuración, haga clic en **Siguiente**.

En la ventana **Autorización**, verifique que se utiliza la cuenta **FORMACION\Administrador** y, a continuación, haga clic en **Confirmar**.



Haga clic en **Cerrar** para cerrar el asistente.

Abra la consola **DHCP** presente en las Herramientas administrativas.

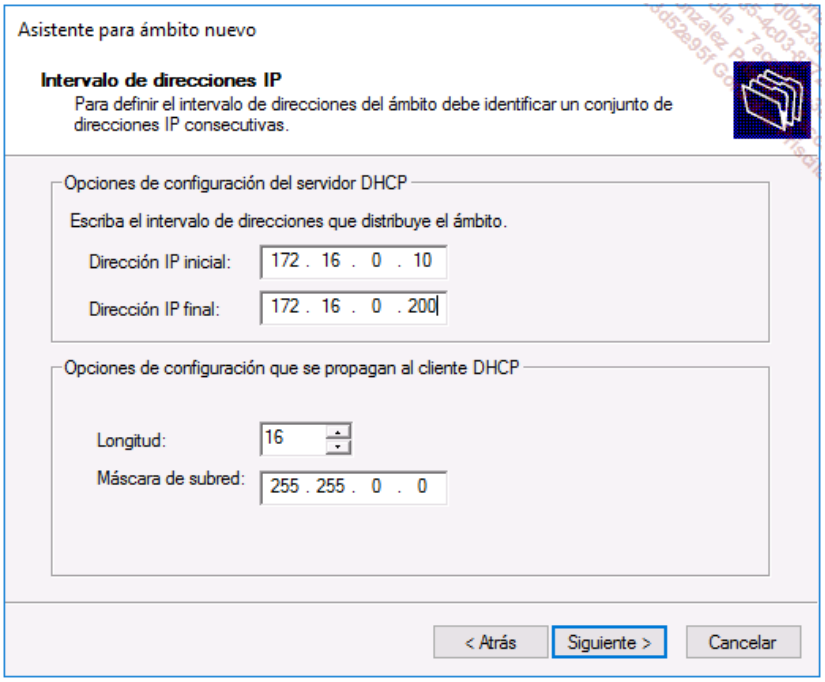
Despliegue **PAR-CD01.Formacion.eni** en el panel de navegación y, a continuación, realice la misma operación con **IPv4**.

Haga clic con el botón derecho en **IPv4** y, a continuación, en el menú contextual, haga clic en **Nuevo ámbito...**.

Haga clic en **Siguiente** en la ventana de **Bienvenida**.

En el campo **Nombre**, escriba **Ámbito Madrid Formación** y, a continuación, haga clic en **Siguiente**.

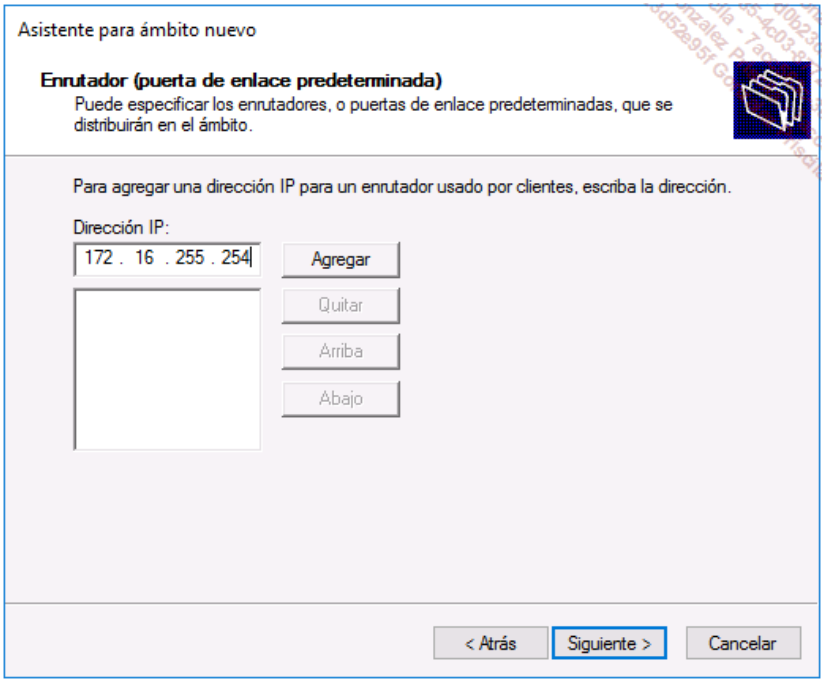
Escriba **172.16.0.10** en **Dirección IP inicial** y, a continuación, **172.16.0.200** en **Dirección IP final**.



En las ventanas **Agregar exclusiones y retraso** y **Duración de la concesión**, haga clic en **Siguiente**.

Marque la opción **Configura restas opciones ahora** y haga clic en **Siguiente**.

Escriba **172.16.1.255.254** en el campo **Dirección IP**. Valide la información haciendo clic en **Agregar** y **Siguiente**.

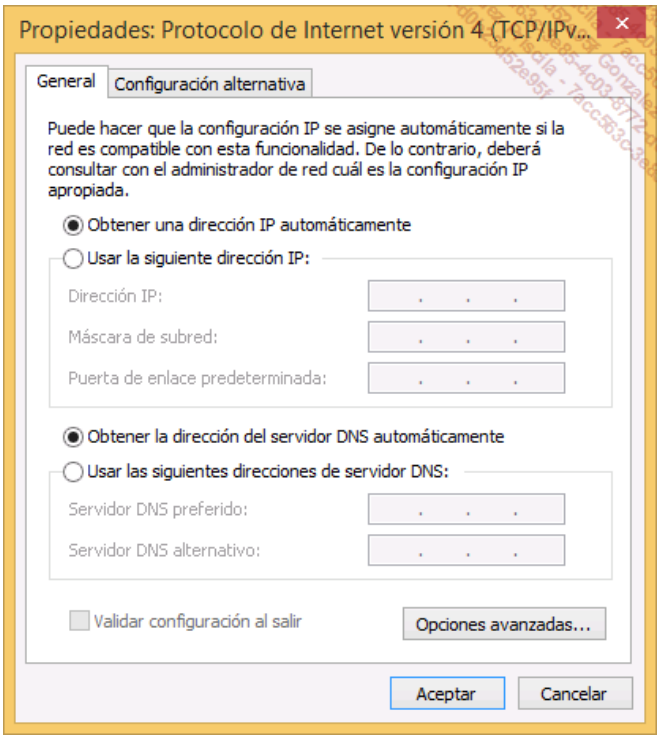


En la ventana **Nombre de dominio y servidores DNS**, verifique que la dirección IP configurada es **172.16.0.1** y, a continuación, haga clic dos veces en **Siguiente**.

En la ventana **Activar ámbito**, haga clic en **Siguiente**.

Haga clic en **Finalizar** para cerrar el asistente.

Verifique en el equipo **CL10-01** el direccionamiento de la tarjeta de red para que esté configurado para **Obtener una dirección IP automáticamente**.

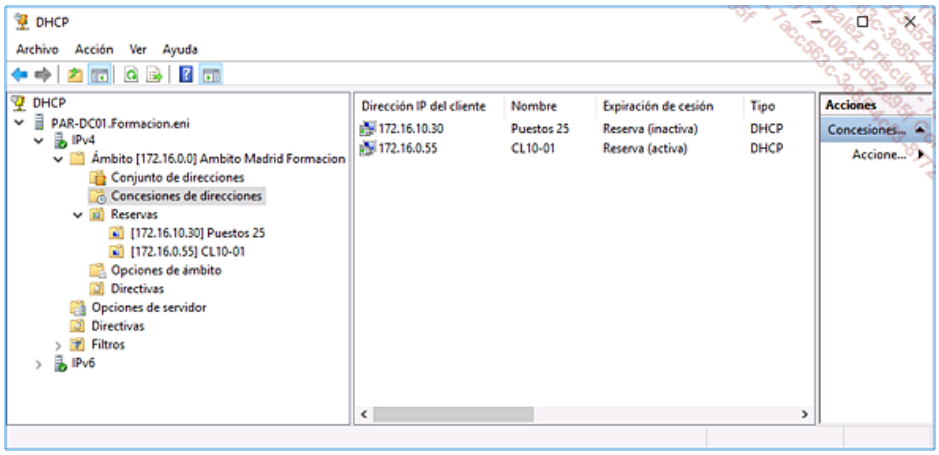


- Marque esta opción si no estuviera marcada.

Utilice el comando `ipconfig` para comprobar la configuración en curso.

- Si la dirección configurada es una dirección APIPA (196.254.x.x), realice una nueva petición de contrato mediante el comando `ipconfig /renew`.

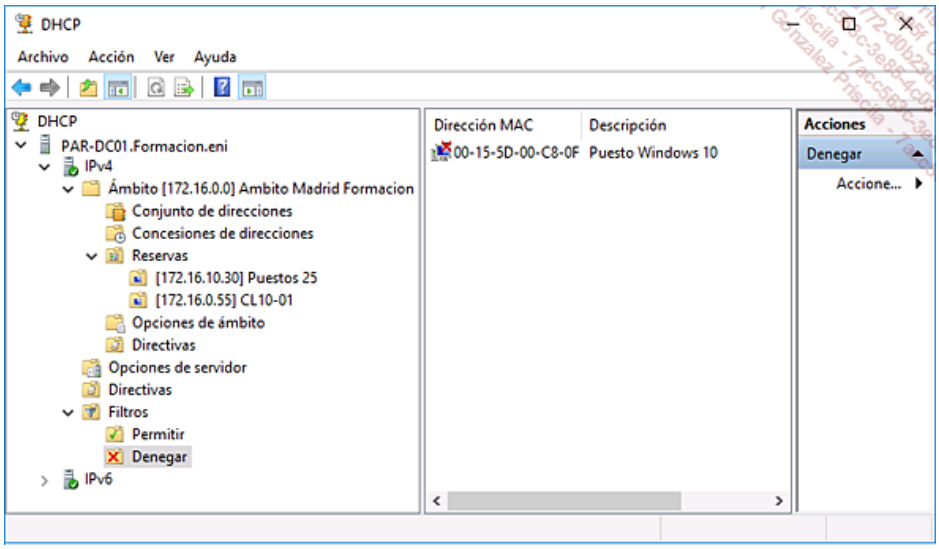
Los contratos distribuidos aparecen en el nodo **Concesiones de direcciones** de la consola DHCP.



Despliegue **Filtros** y, a continuación, haga clic con el botón derecho en el nodo **Permitir**. En el menú contextual, seleccione **Habilitar**. Repita la misma operación con **Denegar**.

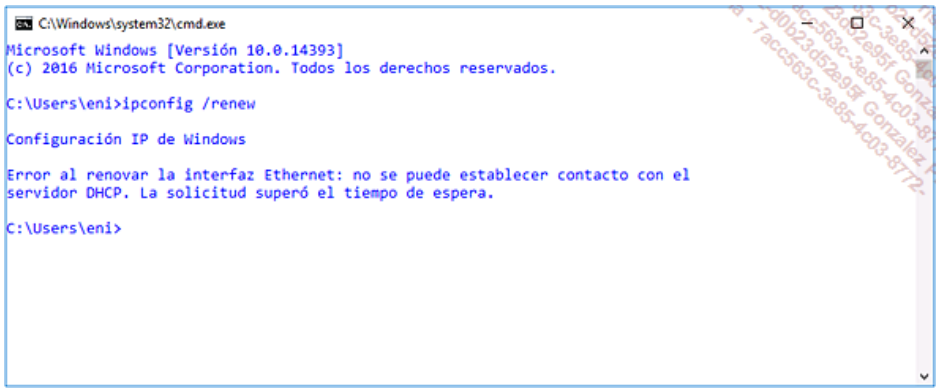
Haga clic en **Conjunto de direcciones** y, a continuación, haga clic con el botón derecho en el correspondiente a **CL10-01**. En el menú contextual, seleccione **Agregar un filtro** y, a continuación, **Denegar**.

Elimine el contrato asignado a **CL10-01** y, a continuación, verifique la presencia del equipo en la lista de exclusión.



En **CL10-01**, abra una ventana de comandos DOS y, a continuación, escriba `ipconfig /release`.

Escriba `ipconfig /renew` para solicitar un nuevo contrato.



No se devuelve ninguna respuesta al cliente puesto que está incluido en la lista de exclusión.

Deshabilite las listas **Permitir** y **Denegar** y, a continuación, vuelva a ejecutar el comando `ipconfig /renew` en **CL10-01**.

2. Implementación de un agente de retransmisión DHCP

Objetivo: implementar y configurar el agente de retransmisión DHCP para los sitios de Sevilla y Valencia.

Máquinas virtuales: PAR-DC01, SRV-RTR y CL10-02.

Las direcciones de red son las dos primeras redes de 450 puestos.

Sevilla: Dirección de red **172.19.0.0 /23**

Valencia: Dirección de red **172.19.2.0 /23**

Utilice el script PowerShell que encontrará en la página Información para crear los dos conmutadores Sevilla y Valencia en el servidor Host Hyper-V.

Si no lo estuviera, incluya **SRV-RTR** en el dominio **Formacion.eni**.

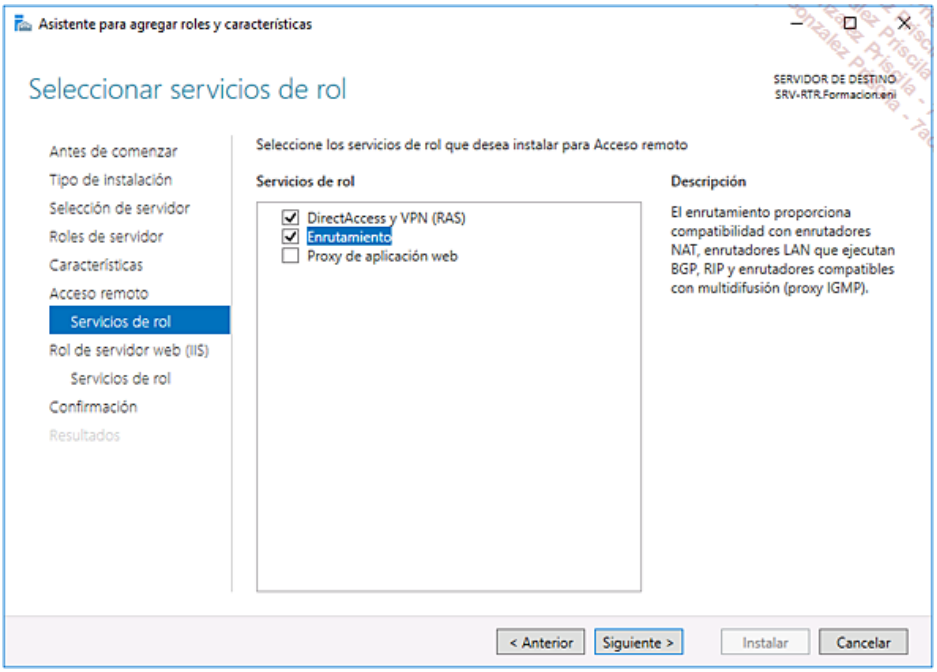
En **SRV-RTR**, abra la consola **Administrador del servidor** y, a continuación, haga clic en **Agregar roles y características**.

En la ventana **Antes de comenzar**, haga clic en **Siguiente**.

Deje la opción por defecto en la ventana **Seleccionar tipo de instalación** y, a continuación, haga clic en **Siguiente**.

Verifique la selección de **SRV-RTR.Formacion.eni** y, a continuación, haga clic en **Siguiente**.

Marque la opción **Acceso remoto** y a continuación haga clic en **Agregar características**. Haga clic tres veces en **Siguiente** y a continuación, en **Servicios de rol**, marque la opción **Enrutamiento**.



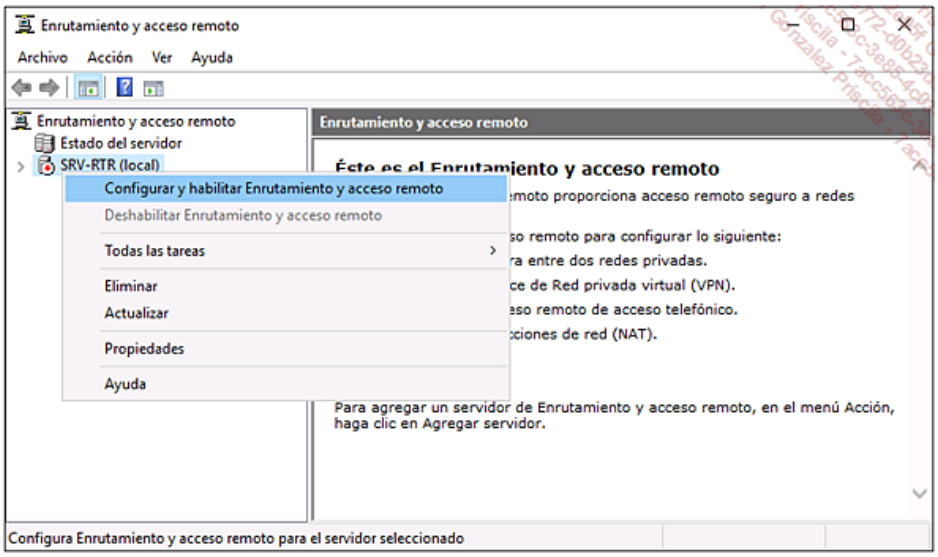
Haga clic en **Agregar características** y, a continuación, en el botón **Siguiente** y en instalar.

La instalación está en curso…

Al final de la instalación, haga clic en **Cerrar**.

En el **Administrador del servidor**, haga clic en **Herramientas** y a continuación en **Enrutamiento y acceso remoto**.

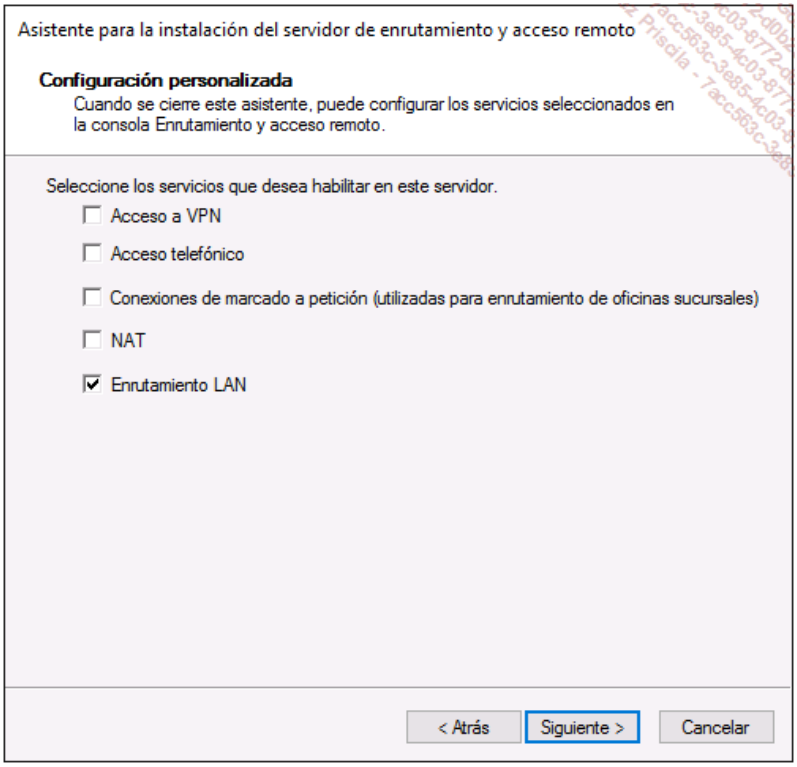
En la consola **Enrutamiento y acceso remoto**, haga clic con el botón derecho en **SRV-RTR** y, a continuación, en **Configurar y habilitar Enrutamiento y acceso remoto**.



Haga clic en **Siguiente**.

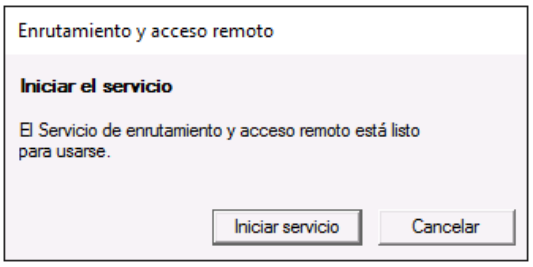
Seleccione **Configuración personalizada**, y a continuación haga clic en **Siguiente**.

Seleccione **Enrutamiento LAN**.

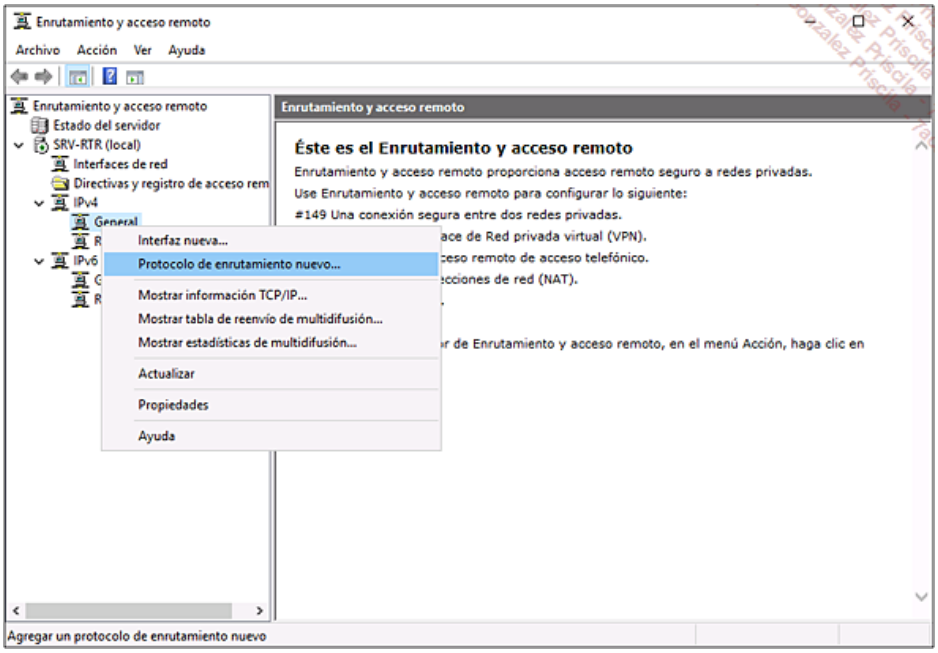


Haga clic en **Siguiente** y, a continuación, en **Finalizar**.

Haga clic en **Iniciar servicio**.



En el panel de navegación, despliegue **SRV-RTR (local)**, despliegue **IPv4**, haga clic con el botón derecho en **General** y, a continuación, haga clic en **Protocolo de enrutamiento nuevo**.

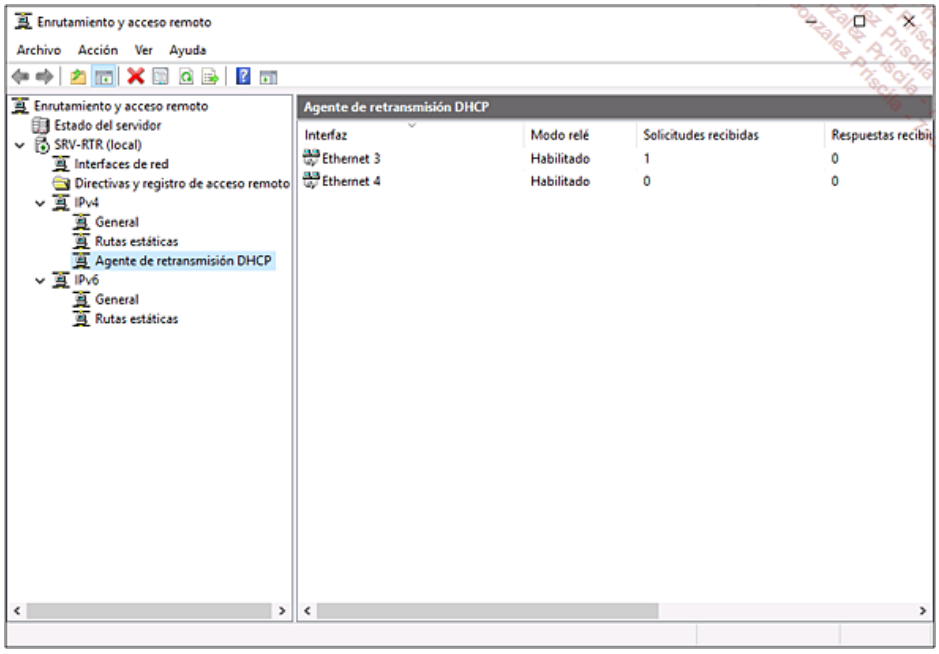


Seleccione **DHCP Relay Agent** y haga clic en **Aceptar**.

En el nodo IPV4 se ha agregado un nuevo elemento, **Agente de retransmisión DHCP**.

Seleccione el nodo del árbol **Agente de retransmisión DHCP** y, a continuación, haga clic con el botón derecho en **Interfaz nueva**.

Agregue las dos interfaces correspondientes a las ciudades de **Sevilla** y **Valencia**.



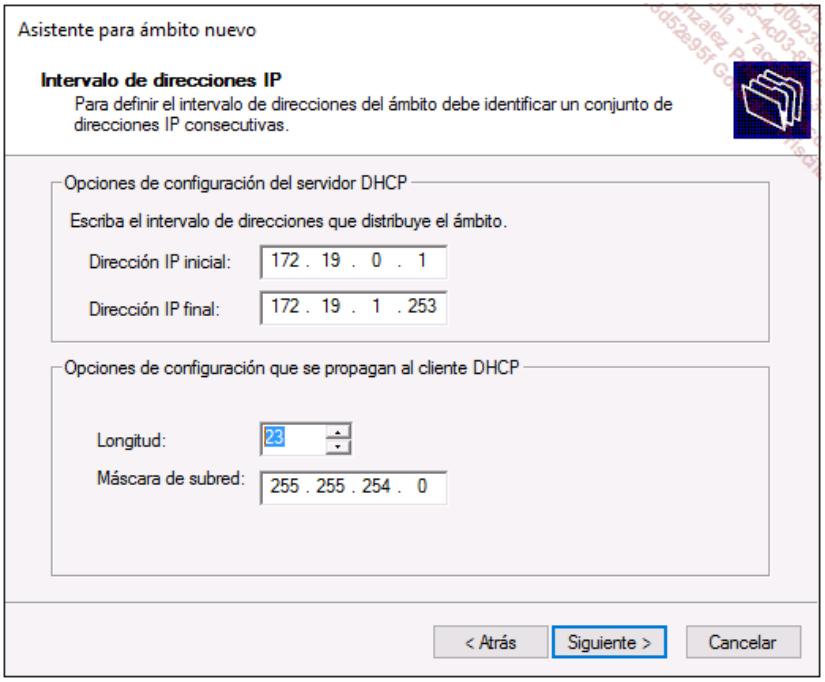
En el nodo **Agente de retransmisión DHCP**, haga clic con el botón derecho y seleccione **Propiedades**.

Agregue la dirección IPv4 del servidor PAR-DC01 172.16.0.1, haga clic en **Agregar** y después en **Aceptar**.

En **PAR-DC01**, abra la consola **Administrador del servidor**, haga clic en **Herramientas** y después en **DHCP**.

Despliegue el árbol de la consola **DHCP** y a continuación, en el nodo **IPv4**, haga clic con el botón derecho y seleccione **Ámbito nuevo**. En el asistente, introduzca los siguientes parámetros:

- **Nombre de ámbito**: Ámbito Sevilla Formación
- **Dirección inicial**: 172.19.0.1
- **Dirección final**: 172.19.1.253
- **Longitud**: 23



Agregue el ámbito de Valencia con los siguientes parámetros:

- **Nombre de ámbito**: Ámbito Valencia Formación
- **Dirección inicial**: 172.19.2.0
- **Dirección final**: 172.19.2.253
- **Longitud**: 23

En **CL10-02**, compruebe que la configuración IPv4 del equipo sea una configuración de tipo automático con DHCP.

Desplace la máquina **CL10-02** al conmutador virtual **Valencia**. El cliente recupera una dirección IPv4 en la red **172.19.2.0 / 23**.

3. Alta disponibilidad del servicio DHCP

Objetivo: implementar alta disponibilidad para asegurar la continuidad del servicio aun en el caso de que uno de los servidores falle.

Máquinas virtuales: PAR-DC01 y PAR-DC02.

En **PAR-DC02**, abra el **Administrador del servidor** y, a continuación, haga clic en **Agregar roles y características**.

En la ventana **Antes de comenzar**, haga clic en **Siguiente**.

Deje la opción por defecto en la ventana **Seleccionar tipo de instalación** y, a continuación, haga clic en **Siguiente**.

El servidor de destino es **PAR-DC02.Formacion.eni**, haga clic en **Siguiente**.

Marque la opción **Servidor DHCP** y, a continuación, haga clic en **Agregar características**.

Haga clic tres veces en **Siguiente** y, a continuación, en **Instalar**.

La instalación está en curso…

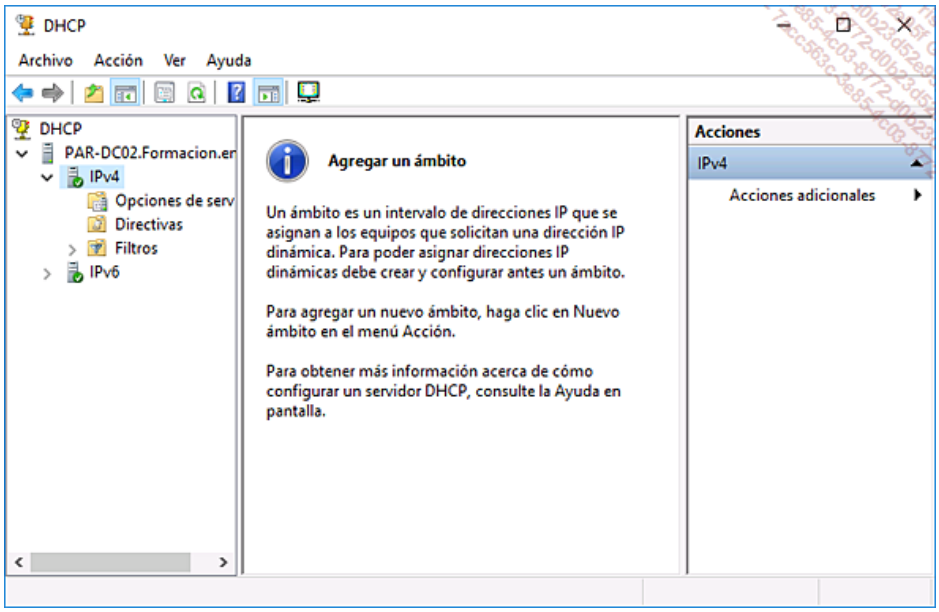
Al finalizar la instalación, haga clic en **Cerrar**.

En el **Administrador del servidor**, haga clic en la bandera y, a continuación, en **Completar configuración de DHCP**.

Haga clic en **Siguiente** en la ventana **Descripción** y, a continuación, **Confirmar** en **Autorización**.

En la interfaz Windows, haga clic en **DHCP**.

Haga doble clic en **PAR-DC02.Formacion.eni** y, a continuación, en **IPv4**.



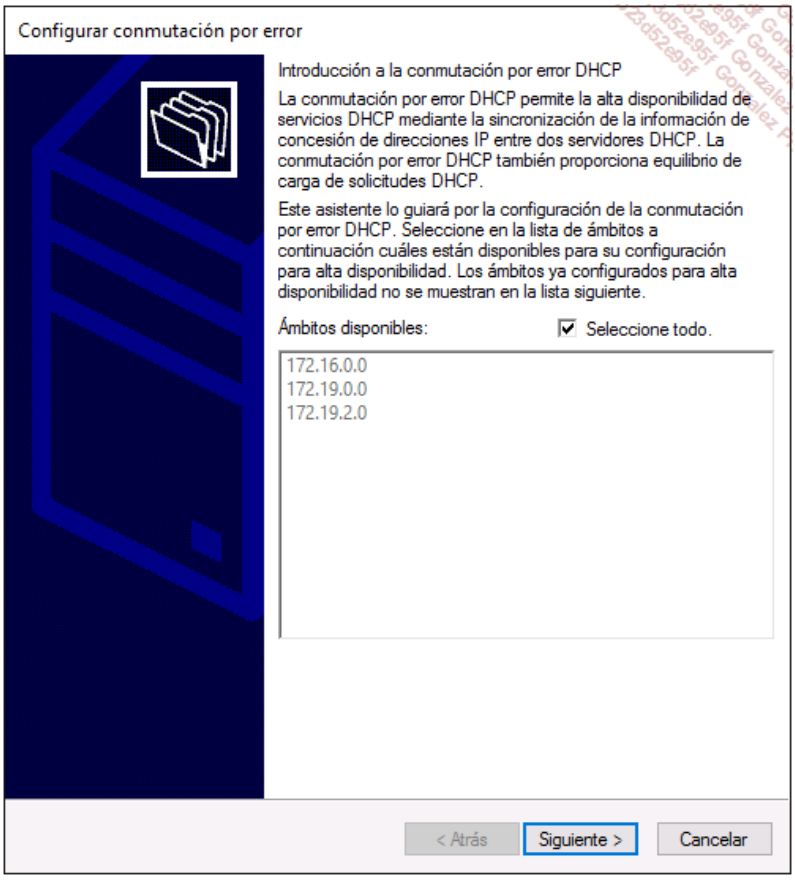
No existe ningún ámbito.

En **PAR-DC01**, haga clic en **DHCP** en las Herramientas administrativas.

Haga doble clic en **PAR-DC01.Formacion.eni** y, a continuación, en **IPv4**.

Haga clic con el botón derecho en **IPv4** y, a continuación, haga clic en **Configurar conmutaciónpor error**.

Existen tres ámbitos en el DHCP. Haga clic en **Siguiente** en la ventana **Introducción a la conmutación por error DHCP**.



En la ventana **Servidor asociado**, haga clic en **Agregar servidor**.

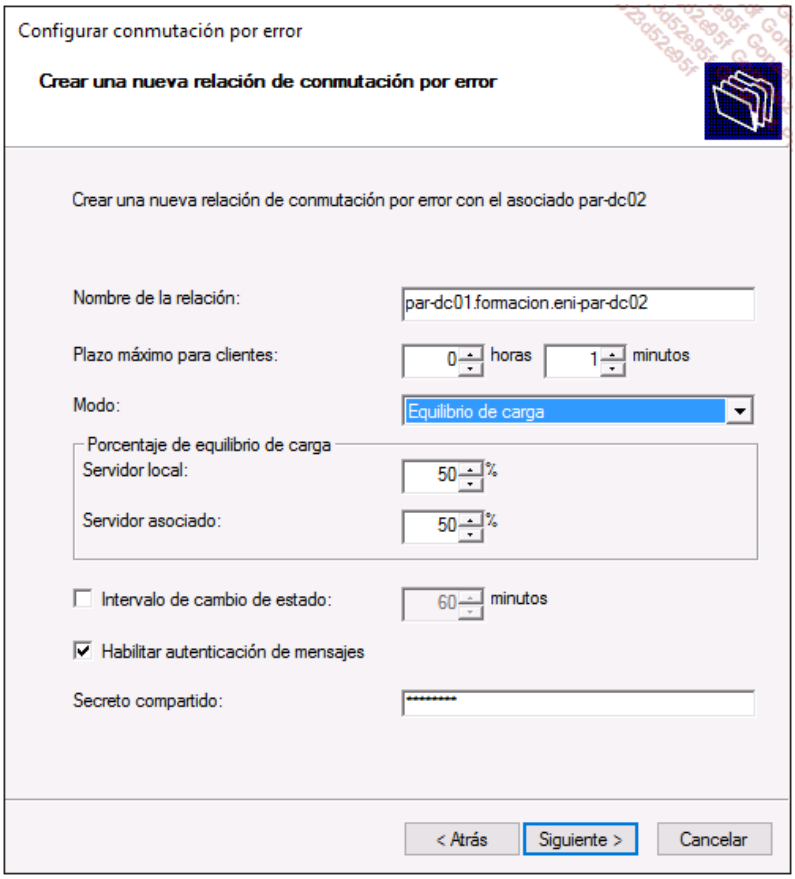
Si **PAR-DC02.Formacion.eni** no aparece, seleccione el servidor con ayuda del botón **Examinar** y, a continuación, haga clic en **Aceptar**.

Haga clic en **Siguiente** para validar el servidor asociado.

Escriba **P@rtDHCP** en el campo **Secreto compartido**.

Modifique el valor del campo **Plazo máximo para clientes** a **1 minuto**.

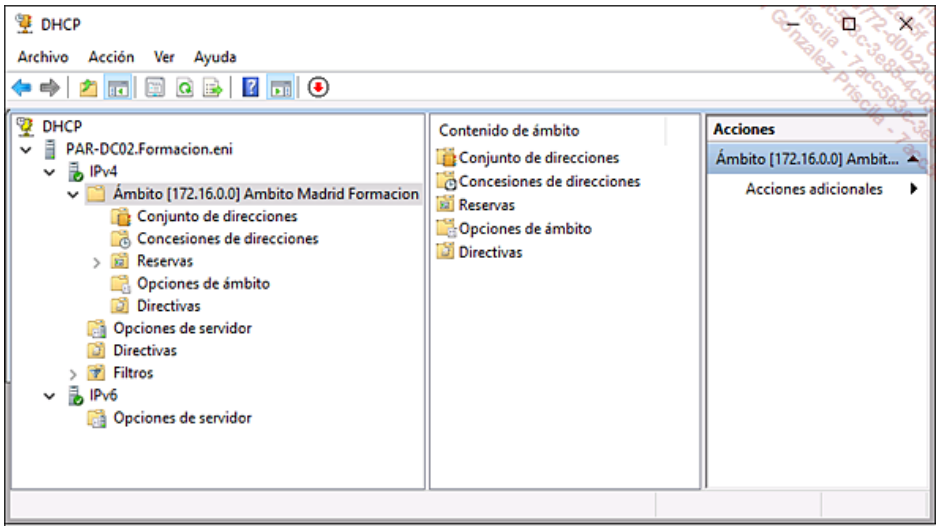
En producción, este retardo sería algo mayor.



Haga clic en **Siguiente** y, a continuación, en **Finalizar**.

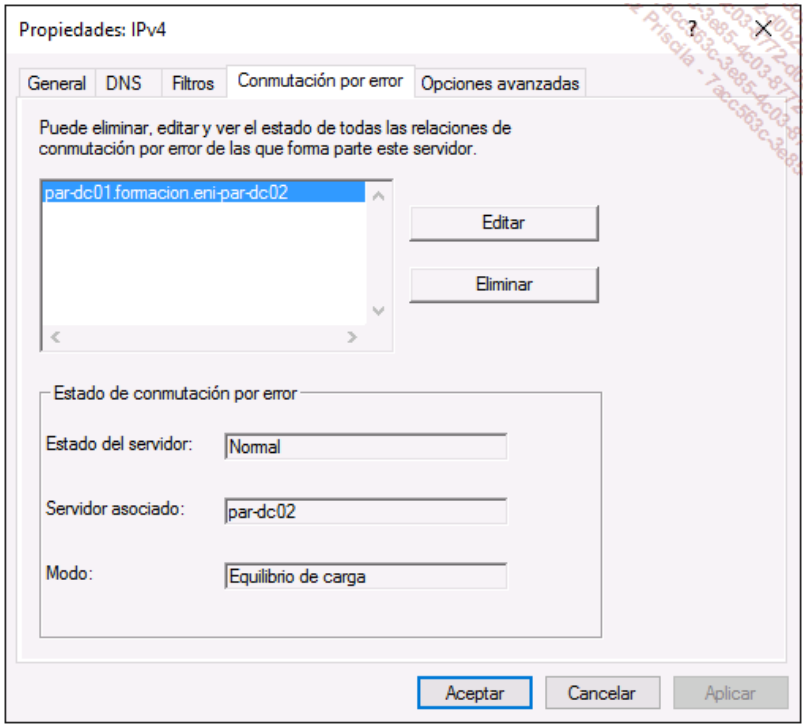
Verifique que las etapas muestran el estado **Correcto** y, a continuación, haga clic en **Cerrar**.

En **PAR-DC02**, acceda a la consola DHCP, ahora aparece el ámbito.



Haga clic con el botón derecho en **IPv4** y, a continuación, seleccione **Propiedades**.

Seleccione la pestaña **Conmutación por error**.



Haga clic en **Editar** para visualizar las propiedades que se pueden modificar.

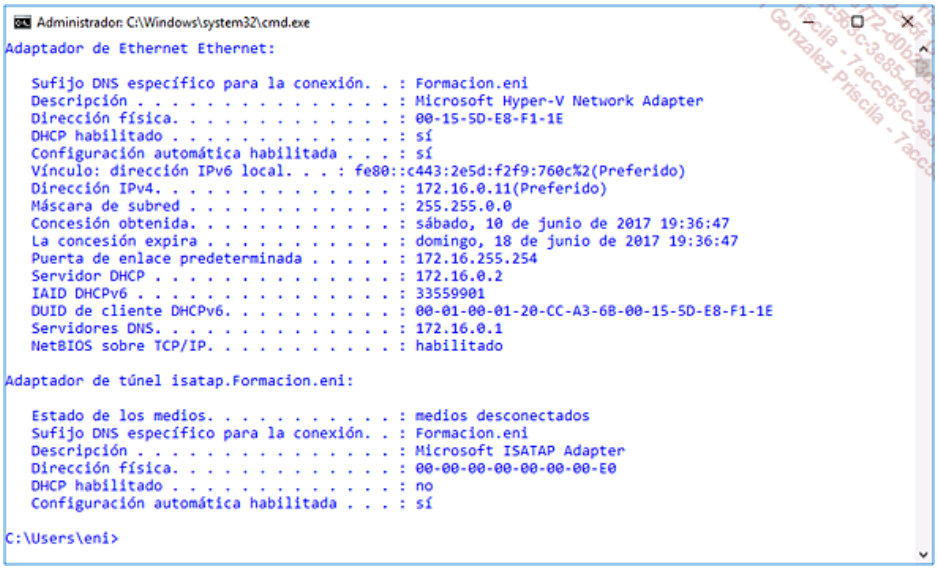
Modifique el campo **Servidor local** para que el porcentaje sea igual a **0**.

Ejecute un `ipconfig /all` en **CL10-01**.

El servidor DHCP que distribuye el contrato es **PAR-DC01**.

Escriba `ipconfig /release` y presione la tecla [Enter] del teclado. Escriba, a continuación, `ipconfig /renew` en una ventana de comandos DOS y presione la tecla [Enter].

Utilice el comando `ipconfig /all` para visualizar el nuevo resultado.



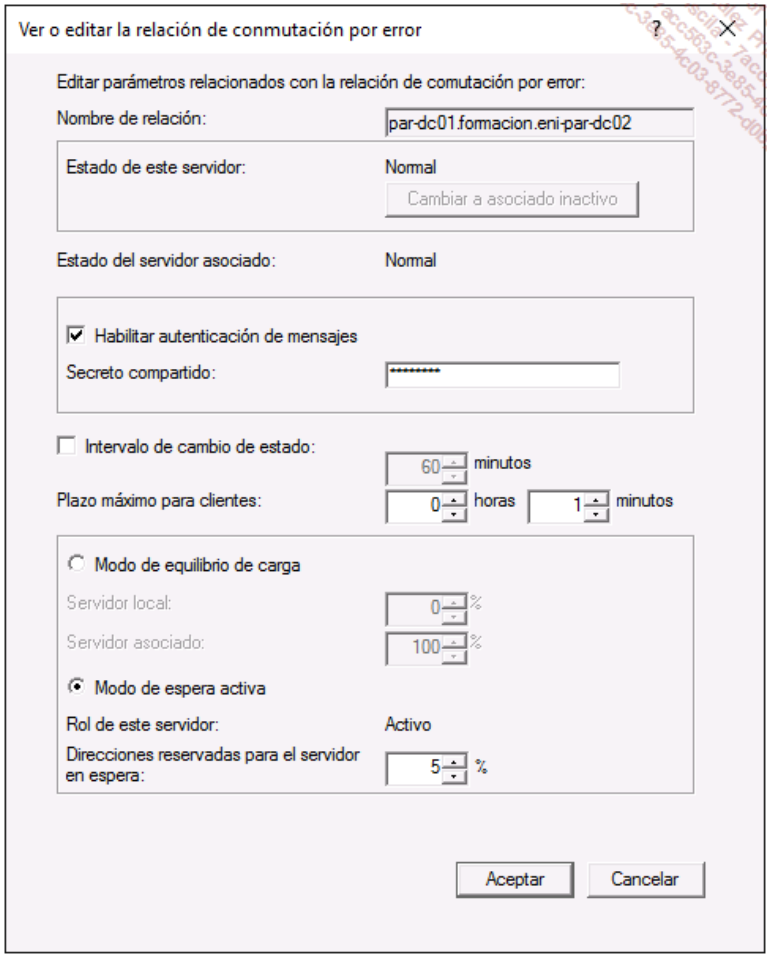
El servidor DHCP que ha distribuido la dirección IP es, efectivamente, **PAR-DC02** (172.16.0.2).

La conmutación por error puede utilizarse, también, en el modo de Espera activa.

En **PAR-DC01**, haga clic con el botón derecho en **IPv4** y, a continuación, seleccione **Propiedades**.

Seleccione **Conmutación por error** y, a continuación, haga clic en **Editar**.

Marque la opción **Modo de espera activa** y, a continuación, haga clic en **Aceptar**.



Haga clic en **Aceptar**. Este servidor tiene el rol **Activo**.

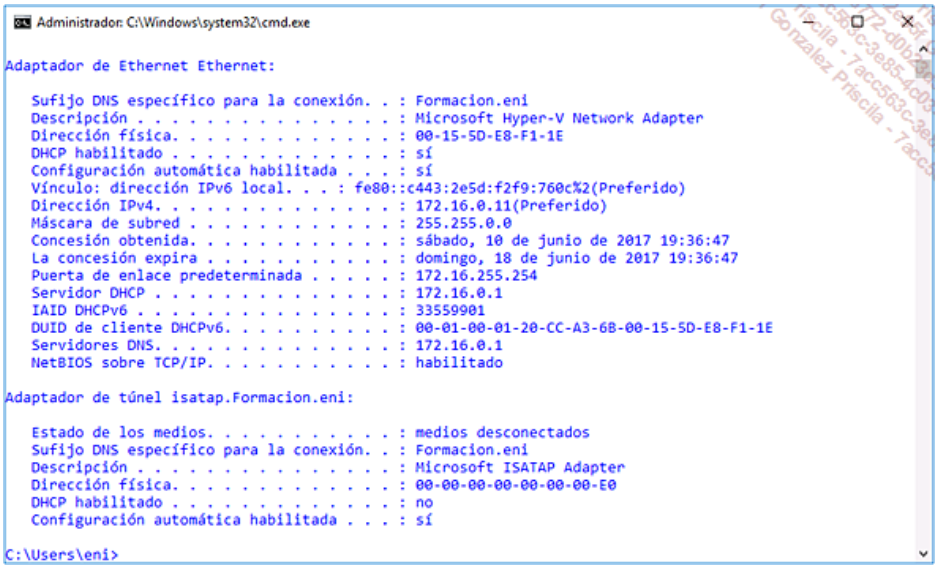
El segundo servidor tiene el rol **Espera**.

Escriba `ipconfig /all` en una ventana de comandos del equipo **CL10-01**.

El servidor DHCP es siempre **PAR-DC02.Formacion.eni**.

Escriba `ipconfig /release` y presione la tecla [Enter] del teclado. Escriba, a continuación, `ipconfig /renew` en la ventana de comandos DOS y presione la tecla [Enter].

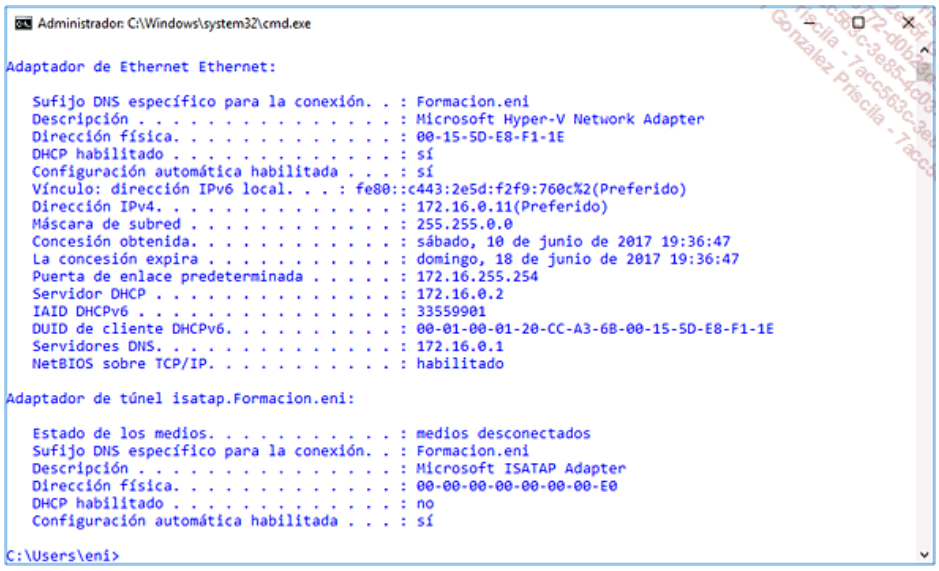
Esta operación permite establecer un contrato DHCP utilizando PAR-DC01.



En **PAR-DC01**, abra la consola **DHCP**.

Haga clic en **PAR-DC01.Formacion.eni**, seleccione **Todas las tareas** y, a continuación, haga clic en **Detener**.

En **CL10-01**, escriba `ipconfig /release` y presione la tecla [Enter] del teclado. Escriba, a continuación, `ipconfig /renew` en la ventana de comandos DOS y presione la tecla [Enter].



El servidor auxiliar ha remplazado al servidor Activo, actualmente fuera de servicio.

Validación de conocimientos adquiridos: preguntas/respuestas

1. Preguntas

Puede validar los conocimientos adquiridos respondiendo a las siguientes preguntas.

1. ¿Cuál es el objetivo del protocolo DHCP?
2. ¿Qué tipo de trama envía el cliente para descubrir el servidor DHCP?
3. ¿Cuáles son los puertos utilizados por el servidor y el cliente DHCP?
4. ¿En qué momento intenta renovar su contrato el equipo cliente?
5. ¿Por qué utilizar una retransmisión DHCP?
6. ¿Qué contiene un ámbito DHCP?
7. ¿Es posible crear varios ámbitos?
8. ¿Cuál es la utilidad de realizar exclusiones?
9. ¿Cuáles son los tres tipos de opciones que pueden configurarse mediante la consola DHCP?
10. ¿Cuáles son los parámetros utilizados durante la implementación de una reserva?
11. ¿Cuál es la función de los filtros?
12. ¿Dónde se encuentra el archivo Dhcp.mdb?
13. Tras la distribución de un contrato DHCP, ¿dónde se escribe la información?
14. ¿Qué es la función de conmutación por error en el servidor DHCP?

2. Resultados

Consulte las siguientes páginas para comprobar sus respuestas.

Por cada respuesta correcta, cuente un punto.

Número de puntos: /14

Para superar este capítulo, su puntuación mínima debería ser de 11 sobre 14.

3. Respuestas

1. ¿Cuál es el objetivo del protocolo DHCP?

   El objetivo del protocolo DHCP es la distribución de configuraciones IP. Permite, de este modo, evitar conflictos de direccionamiento IP.

2. ¿Qué tipo de trama envía el cliente para descubrir el servidor DHCP?

   El cliente envía una trama DHCP Discover con el objetivo de encontrar un servidor DHCP. Esta trama es de tipo broadcast.

3. ¿Cuáles son los puertos utilizados por el servidor y el cliente DHCP?

   Se utilizan los puertos UDP 67 y UDP 68.

4. ¿En qué momento intenta renovar su contrato el equipo cliente?

   El contrato DHCP se asigna al equipo por una duración de x días. Se realizan varios intentos de renovación del contrato. El primero tiene lugar cuando se alcanza el 50% de la duración del contrato. El siguiente, alcanzado el 87,5%, y el último alcanzado el 100%. Una vez expira el contrato, el puesto no puede acceder a la red puesto que no posee configuración IP.

5. ¿Por qué utilizar una retransmisión DHCP?

   Un equipo que se encuentre fuera de la red local no puede recibir el contrato DHCP. El DHCP Discover se basa en una trama de tipo broadcast, lo que impide que se intercambie esta información a través de un router. Es, por tanto, necesario instalar un servidor DHCP en cada red local. No obstante, también es posible implementar una retransmisión DHCP que sirve como enlace entre las dos redes locales separadas por un router.

6. ¿Qué contiene un ámbito DHCP?

   Un ámbito DHCP contiene un pool de direcciones distribuibles pero, también, las reservas y exclusiones configuradas.

7. ¿Es posible crear varios ámbitos?

   Sí, es posible crear varios ámbitos en el servidor DHCP.

8. ¿Cuál es la utilidad de realizar exclusiones?

   Tras la configuración del DHCP, se crea un rango de direcciones IP distribuibles. Es posible excluir aquellas direcciones correspondientes a impresoras… De este modo, estas direcciones no se distribuirán.

9. ¿Cuáles son los tres tipos de opciones que pueden configurarse mediante la consola DHCP?

   Existen tres tipos de opciones presentes en el DHCP, las opciones de servidor, de ámbito o de reserva. De ello se deduce que un ámbito puede

poseer opciones diferentes a las del servidor.

10 ¿Cuáles son los parámetros utilizados durante la implementación de una reserva?

Tras la implementación de una reserva existen tres parámetros importantes, principalmente la dirección IP y la dirección MAC; el nombre de la reserva, si bien es menos importante que los dos parámetros anteriores, permite conocer muy fácilmente (si la nomenclatura se ha escogido cuidadosamente) el destinatario de la reserva.

11 ¿Cuál es la función de los filtros?

Un filtro permite autorizar o no la distribución de configuración IP. Esta seguridad no es óptima, puesto que es posible suplantar la dirección MAC de forma bastante sencilla.

12 ¿Dónde se encuentra el archivo Dhcp.mdb?

Este archivo se encuentra en la carpeta C:\Windows\System32\Dhcp.

13 Tras la distribución de un contrato DHCP, ¿dónde se escribe la información?

La información se escribe en la base de datos del servidor DHCP y también en la base de datos de registro. En caso de restauración de la base de datos, conviene realizar una reconciliación.

14 ¿Qué es la función de conmutación por error en el servidor DHCP?

La conmutación por error permite asegurar una alta disponibilidad en caso de que falle algún servidor. Existen dos modos de trabajo:

- *El modo de equilibrio de carga, que permite repartir la carga de trabajo sobre los dos servidores.*
- *El modo de espera activa, que permite tener un servidor activo y otro en espera. Éste se activa en caso de que falle su servidor asociado.*

Requisitos previos y objetivos

1. Requisitos previos

Poseer nociones acerca del funcionamiento del protocolo DNS.

2. Objetivos

Configuración del rol DNS.

Presentación de los distintos tipos de registros.

Administración y mantenimiento del servidor DNS.

Optimizar la resolución de nombres DNS.

Securizar el servidor DNS.

Introducción

El rol DNS es, junto a Active Directory, un elemento esencial. En efecto, permite la resolución de nombres en direcciones IP. La parada del servicio DNS impediría cualquier resolución y, por tanto, supondría un riesgo de mal funcionamiento a nivel de las aplicaciones que deseen acceder a recursos compartidos (aplicaciones que acceden a una base de datos, por ejemplo).

Instalación de DNS

Como con Active Directory o DHCP, DNS es un rol en Windows Server 2016. Existen dos formas de instalarlo: agregar el rol desde la consola **Administrador del servidor** o realizando una promoción de un servidor como controlador de dominio.

DNS (*Domain Name System*) es un sistema basado en una base de datos distribuida y jerárquica. Esta última está separada de manera lógica. De este modo, los nombres públicos (ediciones-eni.com) son accesibles por cualquiera, sea cual sea su localización geográfica.

Es, naturalmente, más fácil recordar un nombre de dominio o un nombre de equipo que una dirección IP, además IPv6 favorece todavía más el uso de un nombre en lugar de una dirección IP.

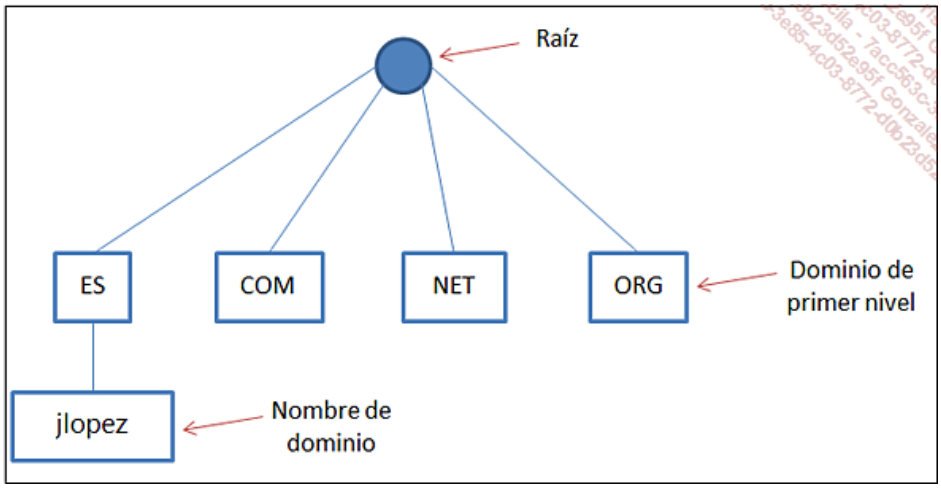
1. Visión general del espacio de nombres DNS

DNS está basado en un sistema jerárquico. El servidor raíz permite redirigir las consultas hacia otros DNS justo por encima. Se representa mediante un punto. Debajo de él se encuentran los distintos dominios de primer nivel (es, net, com…). Cada uno de estos dominios está administrado por un organismo (ESNIC para los dominios .es), mientras que IANA (*Internet Assigned Numbers Authority*) gestiona, por su lado, los servidores raíz.

En un segundo nivel se encuentran los nombres de dominio que están reservados para empresas o particulares (ediciones-eni). Estos nombres de se reservan en un proveedor de acceso que puede, a su vez, albergar su servidor web o, simplemente, proveerle un nombre de dominio.

En cada nivel se encuentran servidores DNS distintos, cada uno con autoridad en su zona. Los servidores raíz contienen, únicamente, la dirección y el nombre de los servidores de primer nivel. Ocurre igual con todos los servidores de cada nivel.

Es posible, para una empresa o un particular, agregar, al nombre de dominio que ha reservado, registros o subdominios (por ejemplo mail.jlopez.es, que permite transferir todo el tráfico de correo electrónico a un router, en particular el correspondiente a la IP pública).



Cada servidor DNS puede resolver únicamente aquellos registros de su zona. El servidor de la zona ES puede resolver el registro jlopez, pero no sabe resolver el nombre de dominio shop.jlopez.es.

2. Separación entre DNS privado/público

Un sistema DNS está compuesto de dos partes, el DNS privado, que tiene como objetivo resolver nombres DNS en una red local, y el servidor DNS sobre las redes públicas que resuelve los nombres DNS accesibles sobre Internet (servidores web…).

Es, por tanto, necesario escoger la política deseada para ambos servidores. El espacio de nombres interno (privado) puede, de este modo, ser idéntico al espacio de nombres externo (público). Cada servidor posee sus propios registros. Esta solución es válida para redes de tamaño restringido. Es habitual encontrar un espacio de nombres interno diferente al externo. El espacio de nombres se encuentra, de este modo, completamente separado en dos partes bien distintas. Por último, una solución híbrida consiste en definir a nivel de los DNS privados subdominios del espacio público.

3. Despliegue de DNS

Tras la implementación de una solución DNS es importante tener en cuenta ciertos parámetros. Es necesario, en primer lugar, conocer el número de zonas DNS configuradas en un servidor así como el número aproximado de registros (con el objetivo de fraccionar, si fuera necesario, los registros en varias zonas). A continuación es, también, necesario conocer el número de servidores que se quiere instalar y configurar, en función, evidentemente, del número de clientes que se comunicarán con los servidores. Puede resultar útil instalar un servidor suplementario en el caso de que el número de puestos cliente sea importante, con el objetivo de poder evitar la sobrecarga de los servidores. Además, agregar un servidor extra permite, también, asegurar la continuidad del servicio si el primer servidor sufriera cualquier fallo en su funcionamiento. Es necesario conocer la ubicación de los servidores, es frecuente encontrar, como mínimo, un servidor DNS por localización (si la red de la empresa se extendiera en cuatro agencias, es decir cuatro redes locales vinculadas mediante enlaces WAN, sería prudente tener, al menos, cuatro servidores DNS). Esto está, evidentemente, sujeto al tamaño del sitio.

Por último, pueden presentarse otras incógnitas, tales como la integración o no con Active Directory. Tras la creación de una zona, el almacenamiento de ésta puede realizarse de dos maneras:

- **Uso de un archivo de texto**: el conjunto de registros se almacena en un archivo. Dicho archivo puede, evidentemente, modificarse mediante un editor de texto.
- **Active Directory**: los registros DNS están contenidos en la base de datos de Active Directory. Para realizar una modificación es necesario acceder a la consola DNS. No obstante la integración de la zona en Active Directory requiere que el rol DNS esté instalado sobre el controlador de dominio, sin lo cual es imposible realizar la operación. Esta última opción ofrece un importante beneficio a los administradores. En efecto, además de asegurar las actualizaciones dinámicas, la replicación se realiza al mismo tiempo que la de Active Directory. Los administradores no tienen, por tanto, que administrar nada más.

Configuración del rol

Una vez instalado, es necesario realizar a la configuración del rol. En el caso de una instalación a partir de la promoción del servidor como controlador de dominio, la creación de la zona se realiza automáticamente.

1. Componentes del servidor

Una solución DNS está formada por varios componentes. Los servidores DNS, para comenzar, tienen como función responder a las consultas de sus clientes, pero también alojar y administrar una o varias zonas. Éstas contienen varios registros de recursos. Los servidores DNS públicos gestionan, a su vez, zonas y registros de recursos. No obstante, estos últimos se refieren únicamente a recursos que deben estar accesibles desde Internet. Por último, los clientes DNS tienen la función de enviar al servidor DNS las distintas peticiones de resolución.

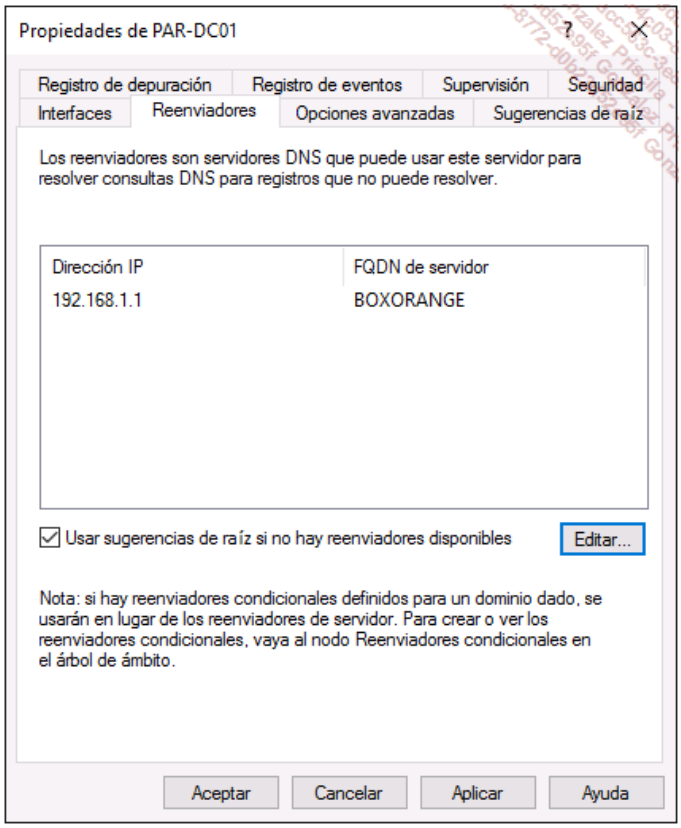
2. Consultas realizadas por el DNS

Una consulta permite solicitar una resolución de nombres a un servidor DNS. De este modo, éste es capaz de ofrecer dos tipos de respuestas, aquellas con autoridad y aquellas sin autoridad. Un servidor provee una respuesta con autoridad si la consulta se refiere a un recurso presente en una zona sobre la que tiene autoridad. En caso contrario, no puede responder al cliente. Utiliza, en tal caso, un reenviador o indicaciones de raíces que permiten obtener dicha respuesta. Pueden utilizarse dos tipos de peticiones, iterativas o recursivas.

Con las consultas iterativas, el puesto cliente envía a su servidor DNS una consulta para resolver el nombre www.jlopez.es, por ejemplo. El servidor consulta al servidor raíz. Éste la redirige al servidor con autoridad en la zona ES. Puede, a su vez, conocer la dirección IP del servidor DNS con autoridad en la zona jlopez. La consulta de esta última permite resolver el nombre www.jlopez.es. El servidor DNS interno responde a la consulta que ha recibido anteriormente de su cliente.

Con las consultas recursivas, el equipo cliente desea resolver el nombre www.jlopez.es, y envía la petición a su servidor DNS. Al no tener autoridad en la zona jlopez.es, el servidor necesita un servidor externo para realizar la resolución. La solicitud se reenvía, entonces, al reenviador configurado por el administrador (el servidor DNS de FAI que posee una caché más amplia, por ejemplo). Si no tiene la respuesta en caché, el servidor DNS de FAI realiza una consulta iterativa y, a continuación, transmite la respuesta al servidor que le ha realizado la petición. Este último puede, ahora, responder a su cliente.

La siguiente captura de pantalla muestra la configuración de un reenviador :



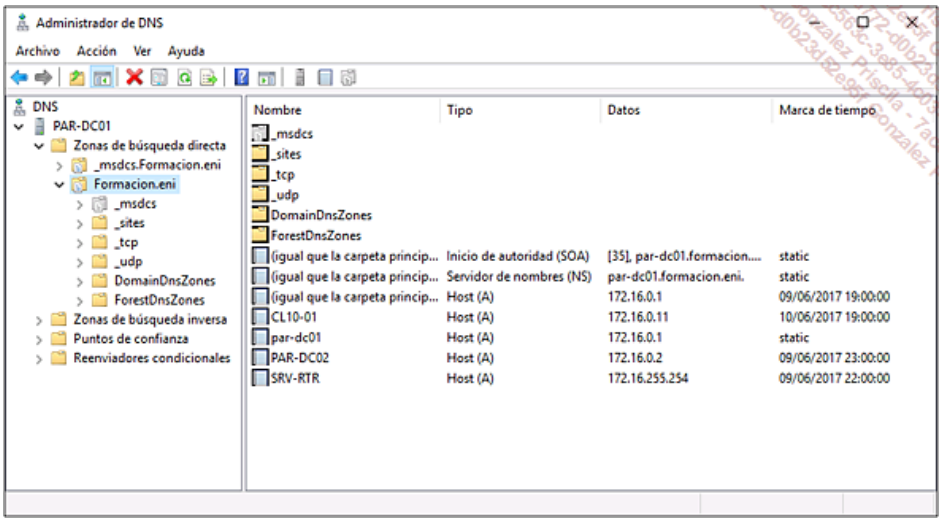
Para toda aquella consulta sobre la que el servidor no tenga autoridad, se utiliza el reenviador. En ciertos casos (aprobación de bosque AD, etc.) es necesario que la petición de resolución que se envía a otro servidor DNS se redirija en función del nombre de dominio (para el dominio eni.es podría enviarse al servidor SRVDNS1, por ejemplo). El reenviador condicional permite realizar esta modificación y, de este modo, dirigir las consultas hacia el servidor adecuado si la condición (nombre de dominio) se valida.

3. Registrar recursos en el servidor DNS

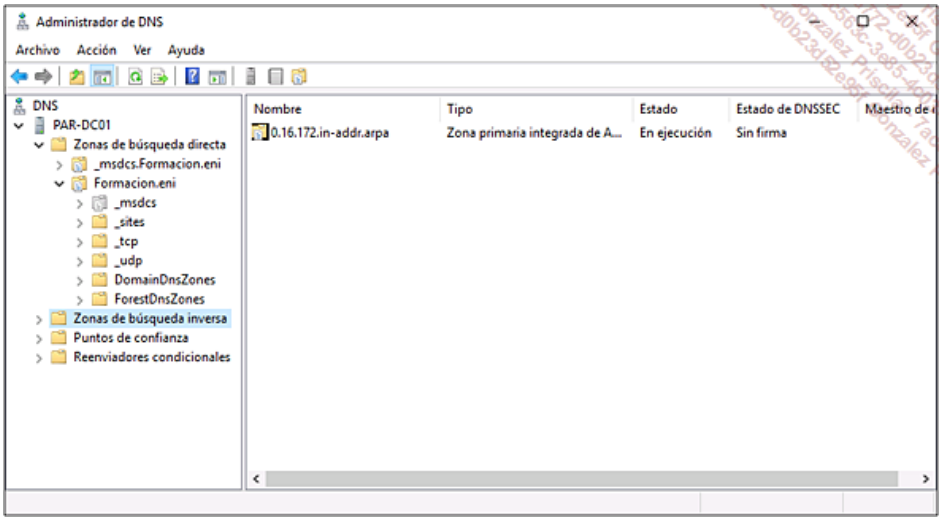
Es posible crear varios tipos de registros en el servidor DNS, los cuales permiten resolver un nombre de equipo, una dirección IP o, simplemente, encontrar un controlador de dominio, un servidor de nombres o un servidor de mensajería.

La siguiente lista muestra los registros más habituales:

- **Registros A y AAAA (*Address Record*)**: permiten establecer la correspondencia entre el nombre de un puesto y su dirección IPv4. El registro AAAA permite resolver el nombre de un puesto en su dirección IPv6.
- **CNAME (*Canonical Name*)**: se crea un alias hacia el nombre de otro puesto. El puesto afectado está accesible mediante su nombre o mediante su alias.
- **MX (*Mail Exchange*)**: define los servidores de correo para el dominio.
- **NS (*Name Server*)**: define los servidores de nombres del dominio.
- **SRV**: permite definir un servidor específico para una aplicación, en particular para el reparto de carga.



- **PTR (*Pointer Record*)**: asociando una dirección IP a un registro de nombre de dominio se realiza la operación opuesta a un registro de tipo A. Se crea este registro en la zona de búsqueda inversa.



- **SOA (*Start Of Authority*)**: el registro ofrece información general sobre la zona (servidor principal, e-mail de contacto, período de expiración…).

4. Funcionamiento del servidor de caché

El almacenamiento en caché supone un ahorro importante en el tiempo de respuesta, y las búsquedas DNS se ven mejoradas. Este almacenamiento en caché proviene de la resolución de un nombre, en efecto, cuando el servidor responde a su cliente, la información se envía y aloja en caché.

Un servidor de caché no contiene ningún dato, este tipo de servidor puede servir de reenviador. Un cliente alberga, a su vez, datos en caché. Para administrar esta información pueden utilizarse dos comandos: `ipconfig /displaydns` permite visualizar la caché, `ipconfig /flushdns` elimina la información contenida en la caché.

Configuración de las zonas DNS

Las zonas DNS son puntos esenciales en una arquitectura DNS. Estas últimas contienen todos los registros necesarios para el correcto funcionamiento del dominio AD.

1. Visión general de las zonas DNS

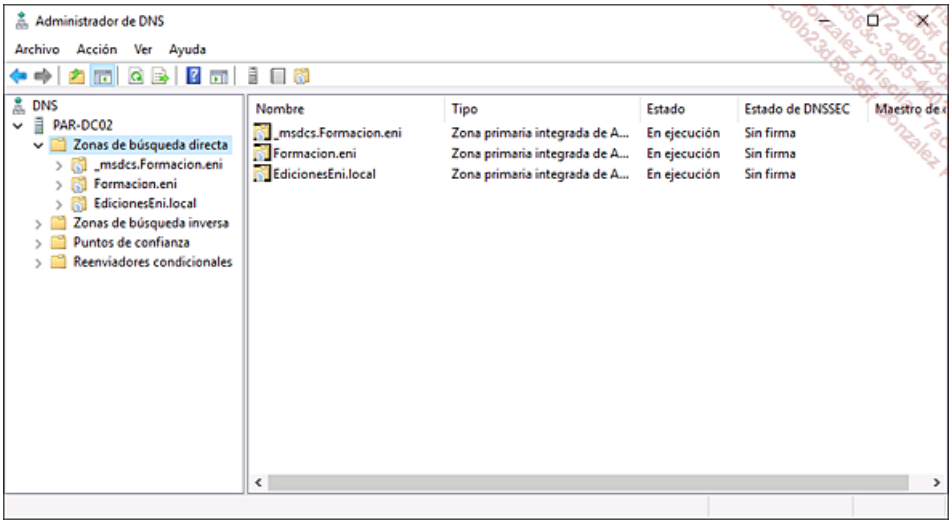
Es posible crear, en un servidor DNS, tres tipos de zona: una zona primaria, una zona secundaria o una zona de stub.

La zona primaria posee permisos de lectura y de escritura sobre el conjunto de los registros que contiene. Este tipo de zona puede integrarse en Active Directory o, simplemente, estar contenida en un archivo de texto. En el caso de que la zona no esté integrada con Active Directory es necesario configurar la transferencia de zona.

La zona secundaria es una simple copia de una zona primaria. Es imposible escribir sobre este tipo de zona, al ser de solo lectura. Es imposible integrarla en Active Directory es obligatorio realizar una transferencia de zona.

Una zona de stub es una copia de una zona, no obstante esta última contiene únicamente registros necesarios para la identificación del servidor DNS que tiene autoridad sobre la zona que acaba de agregarse.

Veamos un ejemplo: el servidor PAR-DC01 tiene autoridad sobre la zona Formacion.eni. El servidor PAR-DC02 tiene autoridad sobre la zona Formacion.eni y EdicionesEni.local.



Se crea una zona de stub para poder conocer el o los servidores que contienen los registros del dominio EdicionesEni.local.

Una vez el servidor PAR-DC01 recibe una petición de resolución para el dominio EdicionesEni.local, la solicitud se redirige hacia el o los servidores DNS configurados en la zona de stub. De este modo puede llevarse a cabo la resolución.

La integración de la zona en Active Directory requiere la instalación del rol DNS sobre un controlador de dominio. Este tipo de zona aporta ciertos beneficios en la gestión del rol DNS.

Actualización con varios maestros: a diferencia de los servidores que alojan zonas primarias y secundarias, las zonas integradas en Active Directory pueden ser modificadas por el conjunto de servidores. En el caso de un sitio remoto, los registros pueden actualizarse sin tener que conectarse con el servidor remoto.

Replicación de zona DNS: la replicación de zona integrada en Active Directory afecta, únicamente, al atributo modificado. También existe una diferencia en el proceso de replicación. Se realiza una transferencia de zona entre las zonas estándar, mientras que las zonas integradas en Active Directory se replican mediante el controlador de dominio.

Actualización dinámica: la integración en Active Directory asegura una mejor seguridad impidiendo cualquier modificación fraudulenta de los registros.

2. Zonas de búsqueda directa y zonas de búsqueda inversa

Las zonas de búsqueda directa permiten resolver un nombre en una dirección IP. Es posible encontrar registros de tipo A, CNAME, SRV... La zona de búsqueda inversa permite resolver una dirección IP en un nombre Es posible encontrar registros de tipo SOA, NS y, principalmente, PTR. Las zonas de búsqueda inversa no se crean por defecto, aunque se recomienda crearlas. Algunas pasarelas de seguridad utilizan la zona de búsqueda inversa para confirmar que la dirección IP que envía los mensajes está asociada correctamente con un dominio.

3. Delegación de zona DNS

La delegación permite realizar el enlace entre las distintas capas DNS, esta operación consiste en identificar el servidor DNS responsable del

dominio de nivel inferior. La delegación de una zona ofrece, a su vez, la posibilidad a otra persona de administrar la zona en cuestión. La carga de red puede verse, así, reducida, y los clientes podrán dirigir sus solicitudes al otro servidor.

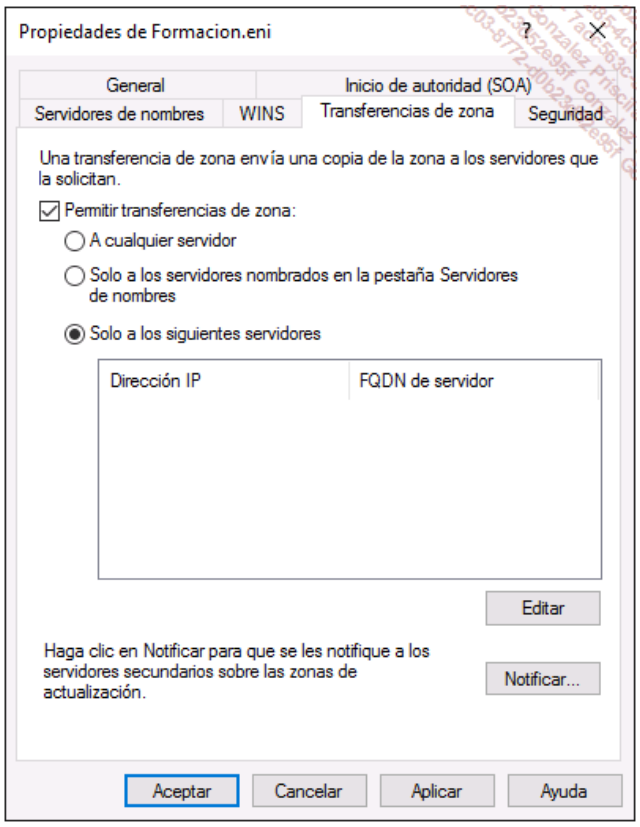
Configuración de la transferencia de zona

Una transferencia de zona consiste en replicar una zona de un servidor a otro. Esto se realiza con el objetivo de poder realizar resoluciones en mejores condiciones.

1. Presentación de la transferencia de zona

Se utiliza una transferencia de zona cuando las zonas no se encuentras en Active Directory. Se realiza, generalmente, entre una zona primaria y una zona secundaria. Existen varios tipos de transferencia de zona: la transferencia de zona integral, que consiste en copiar una zona entera de un servidor a otro o la transferencia de zona incremental, que permite replicar únicamente aquellos registros modificados. El servidor maestro avisa a los servidores secundarios mediante un mensaje DNS Notify, a continuación los servidores secundarios consultan al servidor principal para obtener la actualización.

Para configurar la transferencia de una zona DNS, hay que modificar las propiedades de la zona DNS tal y como muestra la siguiente pantalla.



Cuando la zona está integrada en Active Directory, ésta se replica al mismo tiempo que el directorio Active Directory. Se habla, en este caso, de replicación con varios maestros, todos los servidores DNS pueden realizar modificaciones.

2. Protección de la transferencia de zona

Es importante proteger nuestro servidor DNS, el cual contiene información acerca de los distintos controladores de dominio… Para asegurar una transferencia de zona hacía un servidor autorizado es importante escribir en las propiedades la lista de servidores hacia las que se autoriza la replicación.

Por defecto, no es posible realizar la transferencia de zona, estando, por defecto, deshabilitadas.

Para asegurar una protección tras una transferencia de zona a través de la red es posible utilizar protocolos de tipo IPsec (*Internet Protocol Security*). La protección de datos a través de la red requiere intercambiar datos confidenciales a través del DNS; en caso contrario, bastaría con proteger únicamente la transferencia de zona.

Administración y resolución de errores del servidor DNS

El servicio DNS debe supervisarse para asegurar el correcto funcionamiento de dicho rol. Cualquier error en el mismo podría provocar una incidencia en el funcionamiento de las aplicaciones y demás roles.

Presentación de las características de caducidad y borrado

Si no se realiza ninguna limpieza en un servidor DNS, éste terminará, rápidamente, lleno de registros obsoletos, lo cual puede provocar resoluciones incorrectas y, por tanto, algún problema derivado.

Para evitarlo es posible utilizar varios componentes. El tiempo de vida (TTL, *Time To Live*), el borrado y la caducidad forman parte de estos componentes. El TTL indica un valor durante el que el registro DNS será válido, siendo imposible borrarlo. La caducidad es el mecanismo que permite mantener la coherencia de datos en el servidor DNS. Los datos que hayan alcanzado su fecha de caducidad se eliminarán. Por último, el borrado es la operación que consiste en eliminar estos registros que han alcanzado su fecha de caducidad.

Tras agregar un registro en una zona principal, se le agrega un timestamp para el proceso de bloqueo. Cuando un administrador agrega un registro, este timestamp es igual a 0. De este modo, es imposible aplicar una caducidad a un registro estático.


La caducidad y el borrado deben habilitarse previamente.

Implementar la seguridad de los servidores DNS

El servicio DNS es un servicio crítico que a menudo es víctima de ataques. Por este motivo, los administradores disponen de diversas opciones para dotar de seguridad a los servidores DNS:

- DNSSEC
- Bloqueo de la caché DNS
- Pool de socket DNS

1. Implementar DNSSEC

Un método de ataque frecuente consiste en interceptar y falsificar la respuesta a una petición DNS de una organización. Si una persona malintencionada puede modificar la respuesta de un servidor DNS o enviar una respuesta falsa para dirigir los equipos clientes hacia sus propios servidores, podrá acceder a información sensible. Todos los servicios que se basan en DNS para la conexión inicial, tales como los servidores web de comercio electrónico y los servidores de correo electrónico, son vulnerables. DNSSEC está pensado para proteger a los clientes, enviando peticiones DNS e impidiendo que se acepten respuestas DNS falsas.

Cuando un servidor DNS que alberga una zona firmada digitalmente recibe una petición, reenvía las firmas digitales con los registros solicitados. Un resolutor o un servidor diferente pueden obtener la clave pública del par clave pública/privada de un anclaje de veracidad, y a continuación confirmar que las respuestas son auténticas y no han sido falsificadas. Para ello, el resolutor o el servidor debe estar configurado con un anclaje de veracidad para la zona firmada o para un padre de la zona firmada.

Anclaje de veracidad

Un anclaje de veracidad es una entidad que establece la autoridad, representada por una clave pública. La zona ***TrustAnchors*** registra las claves públicas preconfiguradas que están asociadas a una zona específica. El anclaje de veracidad es un registro de recurso DNSKEY o DS. Si el servidor DNS es un controlador de dominio, las zonas integradas en Active Directory pueden distribuir los anclajes de veracidad.

La tabla NRPT directiva de resolución de nombres

La tabla de directiva de resolución de nombres NRPT contiene las reglas que controlan el comportamiento de los clientes DNS en lo relativo al envío de peticiones DNS y el tratamiento de las respuestas. Para configurar NRPT, se recomienda utilizar la directiva de grupo; sin esta tabla el equipo cliente acepta respuestas sin validar.

Registros de recursos

La validación de las respuestas DNS se realiza asociando una parte de las claves privada y pública (generada por el administrador) a una zona DNS y definiendo registros de recursos DNS suplementarios para firmar y publicar claves.

Registros de recursos	Rol
DNSKEY	Este registro publica la clave pública de la zona que permite verificar la autoridad de una respuesta respecto a la clave privada conservada en el servidor DNS. Estas claves requieren el reemplazo periódico por sustitución de clave (este proceso se realiza automáticamente por parte de Windows Server 2016). Cada zona posee varios registros DNSKEY que se dividen a continuación en claves ZSK y claves KSK.
DS (*Delegation Signer*)	Se trata de un registro de delegación que contiene el hash de la clave pública de una zona hija. Este registro está firmado por la clave privada de la zona padre. Si una zona hija de una zona padre firmada está también firmada, los registros DS de la zona hija deben agregarse manualmente a la zona padre para permitir la creación de una cadena de aprobación.
Ressource Record Signature	Este registro contiene una firma para un juego de registros DNS. Permite comprobar la autoridad de una respuesta.
Next Secure (NSEC)	Cuando la respuesta DNS no contiene ningún dato para proporcionar al cliente, este registro autentica el hecho de que el host no existe.
NSEC3	Esta versión hash del registro NSEC está pensada para impedir los ataques alfabéticos enumerando la zona.

Windows Server 2016 dispone de otras mejoras, como las actualizaciones dinámicas de DNS cuando las zonas se firman con DNSSEC, la distribución de los anclajes automáticamente con Active Directory... Es posible utilizar scripts PowerShell para implementar DNSSEC.

2. El bloqueo de la caché DNS

El bloqueo de la caché es una funcionalidad de seguridad de Windows Server 2016 que le permite controlar el momento en que la información de la caché puede borrarse. Cuando un servidor DNS recursivo responde a una petición, pone los resultados en caché para poder responder más rápidamente si recibe otra petición que pide la misma información. El periodo de tiempo durante el cual el servidor DNS conserva la información en su caché viene determinado por el valor del tiempo de vida (TTL, *Time to Live*) de los registros de recurso. La información de la caché puede borrarse antes de que expire el tiempo de vida si se recibe información actualizada sobre este registro. Si un usuario malintencionado borra con éxito la información de la caché, entonces el usuario malintencionado podría redirigir todo el tráfico de la red hacia un sitio malintencionado. Cuando habilita el bloqueo de la caché, el servidor DNS prohíbe que se borren los registros de la caché durante el tiempo de vida definido.

Debe configurar el bloqueo de la caché como un valor de porcentaje. Por ejemplo, si el valor del bloqueo de la caché está definido al 50 %, entonces el servidor DNS no reemplazará una entrada de la caché durante la mitad del tiempo de vida. Por defecto, el valor del porcentaje de bloqueo de la caché es igual a 100. Esto significa que las entradas alojadas en la caché no se borrarán durante todo el tiempo de vida.

La configuración del bloqueo se realiza mediante PowerShell con el cmdlet `Set-DnsServerCache -LockingPercent`.

```
Set-DnsServerCache -LockingPercent 90
```

Por defecto, el valor es igual a 100 %; es preferible configurar un valor igual o mayor al 90 %. Tras la modificación, es necesario reiniciar el servicio DNS.

3. El pool de sockets DNS

El pool de sockets DNS permite a un servidor DNS utilizar los puertos origen de forma aleatoria durante la emisión de paquetes DNS. Cuando el servicio DNS arranca, el servidor escoge un puerto de origen de un pool de sockets disponibles para enviar peticiones. El pool de sockets DNS hace que los ataques por falsificación de caché sean más difíciles, pues un usuario malintencionado debería adivinar a la vez el puerto origen de una petición DNS y un ID de transacción aleatorio para poder llevar a cabo el ataque con éxito. Desde Windows Server 2012, el pool de sockets DNS está activo por defecto.

Cuando configure el pool de sockets DNS, puede escoger un tamaño comprendido entre 0 y 10 000. Cuanto mayor sea el valor, mayor será la protección contra los ataques por usurpación de dirección DNS. Si el servidor DNS ejecuta Windows Server 2016, también puede configurar una lista de exclusión de pool de sockets DNS.

La configuración del tamaño del pool de sockets DNS se configura mediante la herramienta dnscmd:

```
Dnscmd /config /SocketPoolSize 5000
```

Por defecto, el tamaño del pool sockets DNS es de 2500. Tras su modificación es necesario reiniciar el servicio DNS.

La directiva de respuestas para un servidor DNS

Una mejora importante aportada por Windows Server 2016 a los servidores DNS consiste en poder crear directivas DNS. De este modo, resulta posible modificar el comportamiento del servidor DNS en función de las peticiones recibidas. Por ejemplo, cuando se pide al servidor DNS proveer la dirección IP de un servidor web, una regla DNS permite proporcionar la dirección IP del Data center más cercano al cliente.

1. Escenarios de uso

Es posible implementar muchas directivas DNS en función de las necesidades. He aquí algunos ejemplos de uso posibles:

- **Alta disponibilidad**: los clientes se redirigen al servidor de aplicaciones que esté disponible en un clúster de conmutación por error.
- **Gestión del tráfico**: los clientes se redirigen al centro de datos o al servidor más cercano.
- **DNS Split-Brain**: los registros DNS están repartidos en distintos ámbitos de zona, los clientes reciben una respuesta en función de si son internos o externos.
- **Filtrado**: las peticiones DNS se bloquean si provienen de una lista de direcciones IP o de nombres de dominio completos (FQDN) malintencionados.

2. Objetos DNS correspondientes

En función de los escenarios enunciados anteriormente, existen distintos objetos para configurar las directivas de resoluciones DNS:

- **Subred del cliente**: se utiliza como identificador la subred o la red IPv4 o IPv6 a partir del cual se envían las peticiones DNS a un servidor DNS. Por ejemplo, en ciertos casos se podría querer que los empleados de una empresa pudieran resolver el nombre de un sitio web, el de su compañía (por ejemplo, www.ediciones-eni.com), con una dirección IP interna, pero para un cliente externo que realizara la misma petición en una red diferente, el servidor DNS devolvería una dirección IP diferente para el mismo nombre DNS (www.ediciones-eni.com).
- **Alcance de la recurrencia**: esta directiva DNS permite definir la manera en la que el servidor DNS va a gestionar la recursividad para una petición DNS. Esto significa que es posible habilitar la recursividad para una zona y deshabilitarla para una zona DNS.
- **Zona extendida**: esta directiva permite gestionar las transferencias de zona en función de las redes de origen, por ejemplo.

3. Configuración y administración de las directivas DNS

Una de las novedades en Windows Server 2016 es la introducción de las directivas DNS que pueden aplicarse al servidor DNS o a una zona DNS. Tiene la posibilidad de combinar varias reglas, ya sea a nivel de zona DNS o bien de servidor DNS.

Para crear estas reglas, está obligado a utilizar Windows PowerShell en versión 5.0 o superior. En estas directivas, el parámetro `-Action` es importante, admite como valor **ALLOW**, **DENY** o **IGNORE** y permite determinar la manera en la que el servidor DNS gestionará esta regla.

A continuación se muestran algunos ejemplos de directivas DNS con IPv4, que también funcionan con IPv6:

Gestión del tráfico

El siguiente ejemplo permite devolver una dirección IP diferente para una misma petición, en función de la red de origen de la petición realizada por los clientes.

```
Add-DnsServerClientSubnet -Name "Madrid_ssred" -IPv4Subnet "172.16.0.0/16"
Add-DnsServerClientSubnet -Name "Barcelona_ssred" -IPv4Subnet "172.17.44.0/24"
Add-DnsServerZoneScope -ZoneName "Formacion.eni" -Name "MadridZoneScope"
Add-DnsServerZoneScope -ZoneName "Formacion.eni" -Name "BarcelonaZoneScope"
Add-DnsServerResourceRecord -ZoneName "Formacion.eni" -A -Name "www"
-IPv4Address "172.17.97.97" -ZoneScope "BarcelonaZoneScope"
Add-DnsServerResourceRecord -ZoneName "Formacion.eni" -A -Name "www"
-IPv4Address "172.21.21.21" -ZoneScope "MadridZoneScope"
Add-DnsServerQueryResolutionPolicy -Name "MadridPolicy" -Action ALLOW
-ClientSubnet "eq,Madrid_ssred" -ZoneScope "MadridZoneScope,1"
-ZoneName "Formacion.eni"
Add-DnsServerQueryResolutionPolicy -Name "BarcelonaPolicy" -Action ALLOW
-ClientSubnet "eq,Barcelona_ssred" -ZoneScope "BarcelonaZoneScope,1"
-ZoneName Formacion.eni
```

Bloqueo de peticiones para un nombre de dominio

Puede utilizar una directiva de resolución de peticiones DNS para bloquear las peticiones correspondientes a un dominio. El siguiente comando PowerShell indica al servidor DNS que ignore todas las peticiones DNS para el nombre de dominio **Formacion.msft**:

```
Add-DnsServerQueryResolutionPolicy -Name "BlockFormacionDNS" -Action IGNORE
-FQDN "EQ,*.Formacion.msft"
```

Bloqueo de peticiones a partir de una subred

También puede bloquear las peticiones que provengan de una subred específica. El siguiente script crea un objeto de subred 172.0.33.0/24 antes de crear una directiva para ignorar todas las peticiones provenientes de esta subred:

```
Add-DnsServerClientSubnet -Name "red_06" -IPv4Subnet 172.0.33.0/24
Add-DnsServerQueryResolutionPolicy -Name "BlockRedRed06"
-Action IGNORE
-ClientSubnet "EQ, red_06"
```

Autorizar la recursividad para los clientes internos

Puede controlar la recursividad mediante una directiva de resolución de peticiones DNS. El siguiente ejemplo puede utilizarse para habilitar la recursividad a los clientes internos, deshabilitando esta posibilidad a los clientes externos en un escenario Split-Brain DNS.

```
Set-DnsServerRecursionScope -Name . -EnableRecursion $False
Add-DnsServerRecursionScope -Name "Clientes Internos" -EnableRecursion $True
Add-DnsServerQueryResolutionPolicy -Name "SplitBrainPolicy" -Action ALLOW
- ApplyOnRecursion -RecursionScope "Clientes_Internos" -ServerInterfaceIP
"EQ,10.0.0.34"
```

El primer comando PowerShell permite deshabilitar la recursividad del servidor DNS. Se utiliza el "." para hacer referencia a los 13 servidores Root. El segundo permite habilitar la recursividad para los clientes internos. Por último, se aplica esta directiva al servidor DNS sobre una de sus interfaces, aquí sobre la interfaz **10.0.0.34**.

Directiva de transferencia de zona a nivel de servidor

Puede controlar la transferencia de zona de una manera más granular mediante las directivas de transferencia de zona DNS. El siguiente script de ejemplo puede utilizarse para autorizar las transferencias de zona de cualquier servidor DNS hacia una subred determinada:

```
Add-DnsServerClientSubnet -Name "RedPermitida" -IPv4Subnet 172.21.33.0/24
Add-DnsServerZoneTransferPolicy -Name "BARCELONA_Policy" -Action ALLOW
-ClientSubnet "eq,RedPermitida"
```

La primera línea del script crea un objeto de subred llamado **RedPermitida** con la dirección de la red 172.21.33.0/24. La segunda línea crea una directiva de transferencia de zona para autorizar las transferencias de zona hacia cualquier servidor DNS de la subred creada previamente.

Trabajos prácticos: Instalación y configuración del rol DNS

Los trabajos prácticos permiten instalar, crear y configurar el rol DNS.

1. Configuración del registro de los recursos

Objetivo: realizar la creación del registro y, a continuación, la creación de una zona de búsqueda inversa.

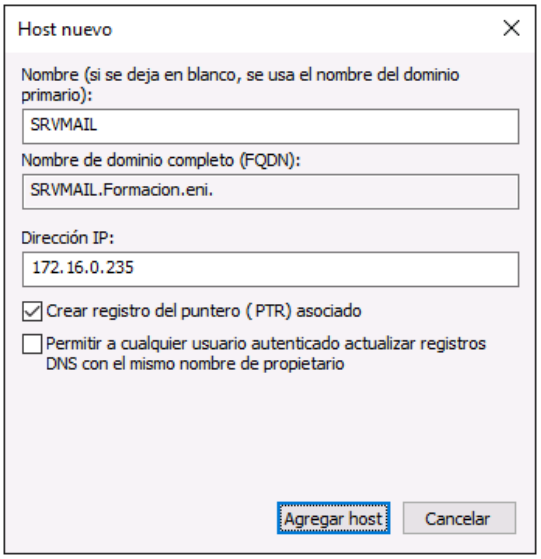
Máquina virtual: PAR-DC01.

Abra una sesión en **PAR-DC01** como administrador y, a continuación, abra la consola **Administrador de DNS**.

Despliegue **PAR-DC01**, **Zonas de búsqueda directa** y, a continuación, **Formacion.eni**.

Haga clic con el botón derecho en **Formacion.eni** y, a continuación, en **Nuevo host (A o AAAA)**.

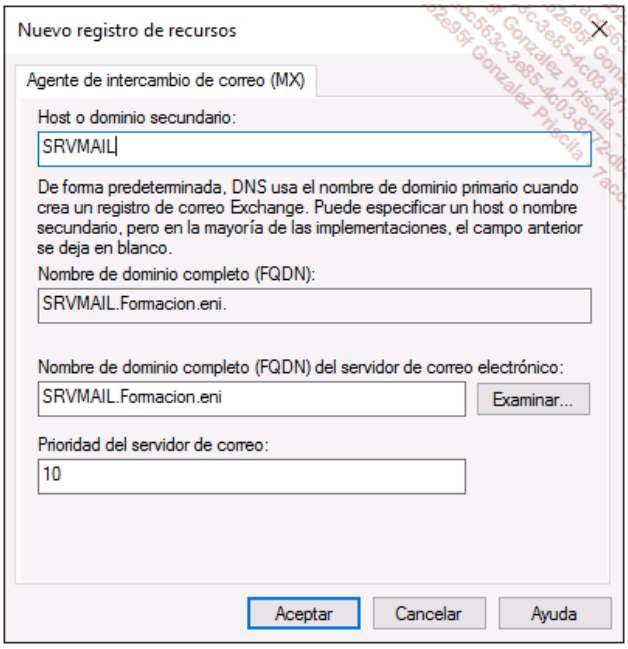
Escriba **SRVMAIL** en el campo **Nombre** y, a continuación, **172.16.0.235** en el campo **Dirección IP**.



Haga clic en **Agregar host** y, a continuación, en **Aceptar** en la ventana que aparece.

Haga clic con el botón derecho en **Formacion.eni** y, a continuación, haga clic en **Nuevo intercambio de correo (MX)**.

Escriba **SRVMAIL** en el campo **Host o dominio secundario** y, a continuación, **SRVMAIL.formacion.eni** en el campo **Nombre de dominio completo (FQDN) del servidor de correo electrónico**.



Haga clic con el botón derecho en **Zonas de búsqueda inversa** y, a continuación, seleccione **Nueva zona**.

Haga clic en **Siguiente** en la ventana de bienvenida y, a continuación, seleccione **Zona principal**.

Valide las opciones haciendo clic en **Siguiente**.

En las ventanas **Ámbito de replicación de la zona de Active Directory** y **Zona de búsqueda inversa IPv4** deje las opciones por defecto y, a continuación, haga clic en **Siguiente**.

Escriba **172.16.0** en el campo **Id. de red** y, por último, haca clic en **Siguiente**.

Solo están autorizadas las actualizaciones dinámicas seguras, deje la opción por defecto y, a continuación, haga clic en **Siguiente**.

Haga clic en **Finalizar** para realizar la creación de la zona.

2. Caducidad y borrado de los registros

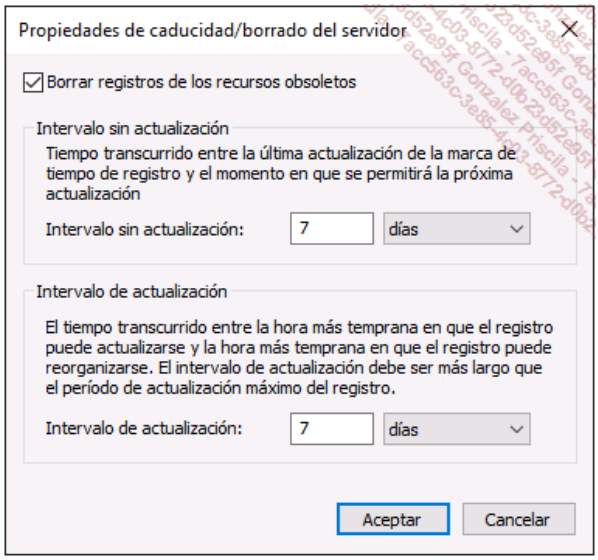
Objetivo: configurar las funcionalidades de tiempo de vida, borrado y caducidad con el fin de asegurar la eliminación de registros obsoletos.

Máquina virtual: PAR-DC01.

En **PAR-DC01**, abra la consola **Administrador de DNS**.

Haga clic con el botón derecho en **PAR-DC01** y, a continuación, en el menú contextual, seleccione **Establecer caducidad/borrado para todas las zonas**.

Marque la opción **Borrar registros de los recursos obsoletos** y, a continuación, haga clic en **Aceptar**.

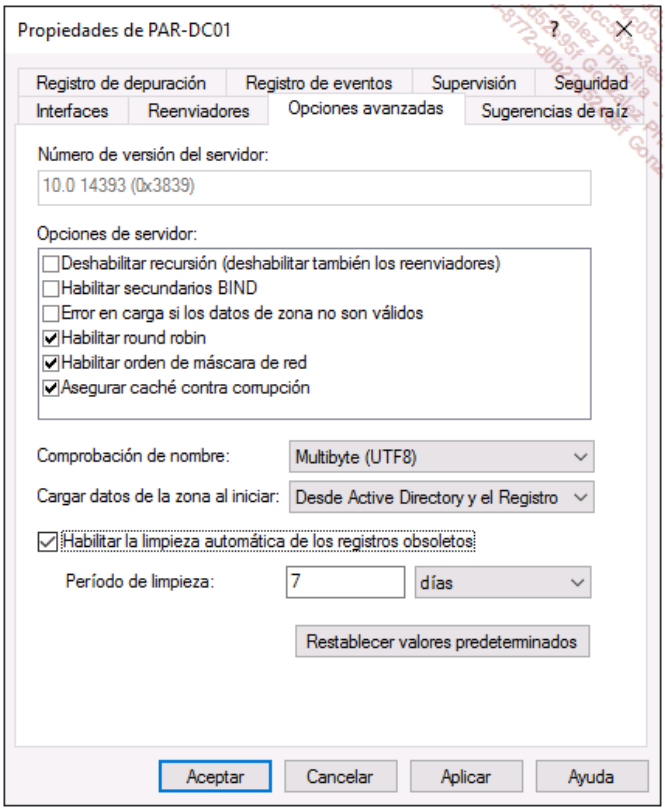


Se abre una ventana, marque **Aplicar esta configuración a las zonas integradas en Active Directory existentes**.

El valor **7 días** es un valor por defecto que puede modificarse.

Haga clic con el botón derecho en **PAR-DC01** y, a continuación, seleccione **Propiedades** en el menú contextual.

Haga clic en la pestaña **Opciones avanzadas** y, a continuación, marque la opción **Habilitar la limpieza automática de los registros obsoletos**.



El valor del borrado debe coincidir con el configurado para la caducidad.

Haga clic en **Aceptar**.

Ahora están configuradas las características de caducidad y borrado.

3. Configuración de un reenviador condicional

Objetivo: creación de un reenviador con el objetivo de redirigir aquellas consultas relativas al dominio Formatica.msft hacia el dominio PAR-SRV1.

Máquinas virtuales: PAR-DC01, PAR-SRV1.

En **PAR-SRV1**, abra una sesión como administrador de dominio.

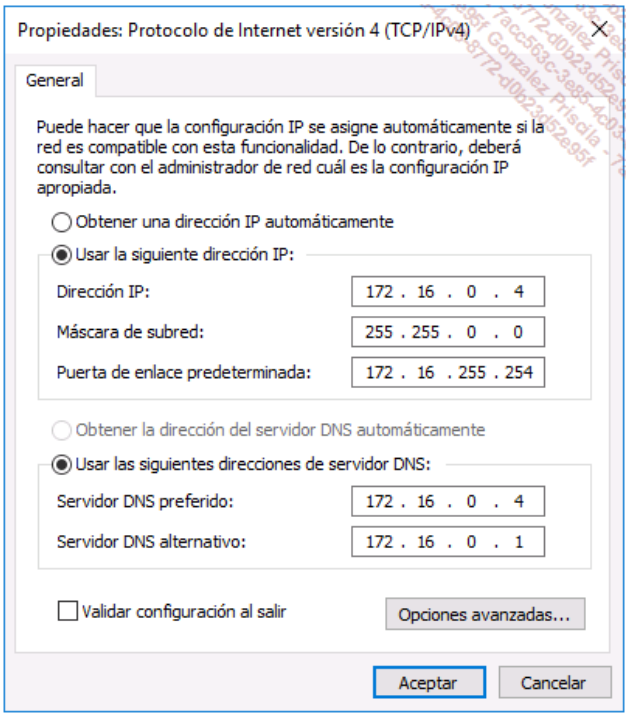
Abra la consola **Centro de redes y recursos compartidos**.

Haga clic en **Cambiar configuración del adaptador**.

Haga clic con el botón derecho sobre la tarjeta de red y, a continuación, seleccione la opción **Propiedades** en el menú contextual.

Haga doble clic en **Protocolo de Internet versión 4 (TCP/IPv4)**.

Modifique la configuración IP de la máquina para que posea su dirección IP en el campo **Servidor DNS preferido**. La dirección del servidor**PAR-DC01** debe configurarse en el campo **Servidor DNS alternativo**.

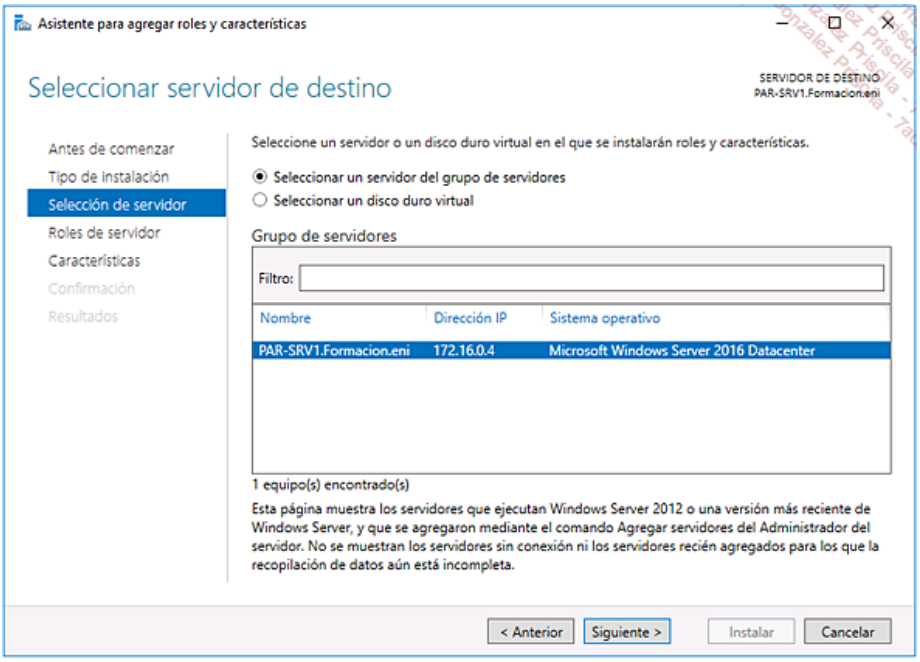


Haga clic en **Aceptar**.

Abra la consola **Administrador del servidor** y, a continuación, haga clic en el enlace **Agregar roles y características**.

Se abre el asistente, haga clic en **Siguiente**.

En las ventanas **Seleccionar tipo de instalación** y **Seleccionar servidor de destino**, haga clic en **Siguiente** dejando el valor por defecto.



Marque el rol **Servidor DNS** y, a continuación, haga clic en **Agregar características**.

Haga clic tres veces en **Siguiente** y, a continuación, en **Instalar**.

Cierre la ventana una vez termine la operación.

Abra la consola **DNS** desde las Herramientas administrativas y, a continuación, despliegue **PAR-SRV1**.

Haga clic con el botón derecho en las **Zonas de búsqueda directa** y, a continuación, seleccione **Nueva zona**.

En la ventana de bienvenida, haga clic en **Siguiente**.

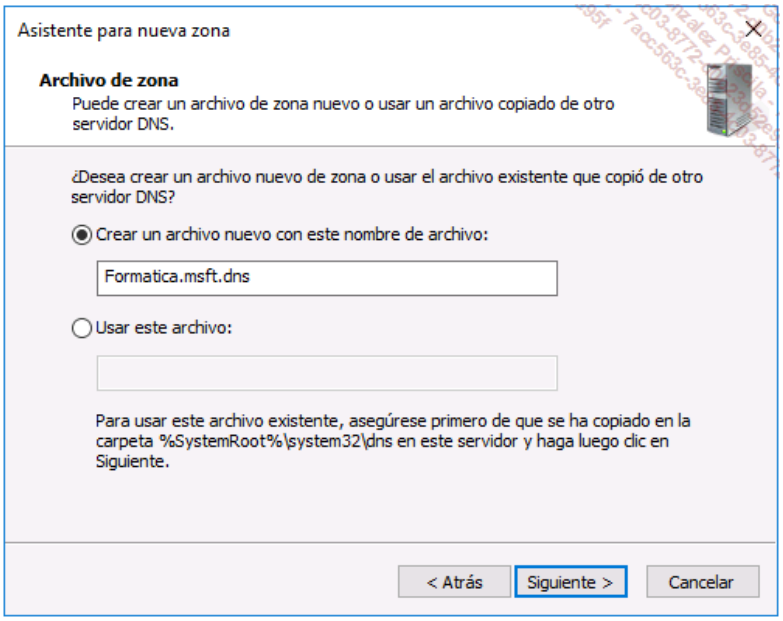
Compruebe que está marcada la **Zona principal** y, a continuación, haga clic en **Siguiente**.

En el campo **Nombre de zona**, escriba **Formatica.msft** y, a continuación, haga clic en **Siguiente**.

La zona no puede integrarse en Active Directory, pues el servidor no es un controlador de dominio.

Se crea, entonces, un archivo, el cual contiene todos los registros de la zona.

Haga clic en **Siguiente** en la ventana **Archivo de zona**.



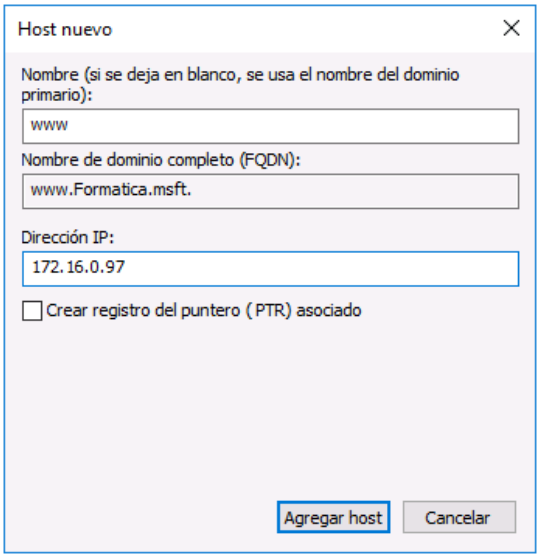
Deje marcada la opción **No permitir las actualizaciones dinámicas** y, a continuación, haga clic en **Siguiente**.

Haga clic en **Finalizar** para realizar la creación de la zona.

Despliegue la zona **Formatica.msft** y, a continuación, haga clic con el botón derecho sobre la zona.

En el menú contextual, seleccione **Nuevo host (A o AAAA)**.

Escriba **www** en el campo **Nombre** y, a continuación, **172.16.0.97** en el campo **Dirección IP**.



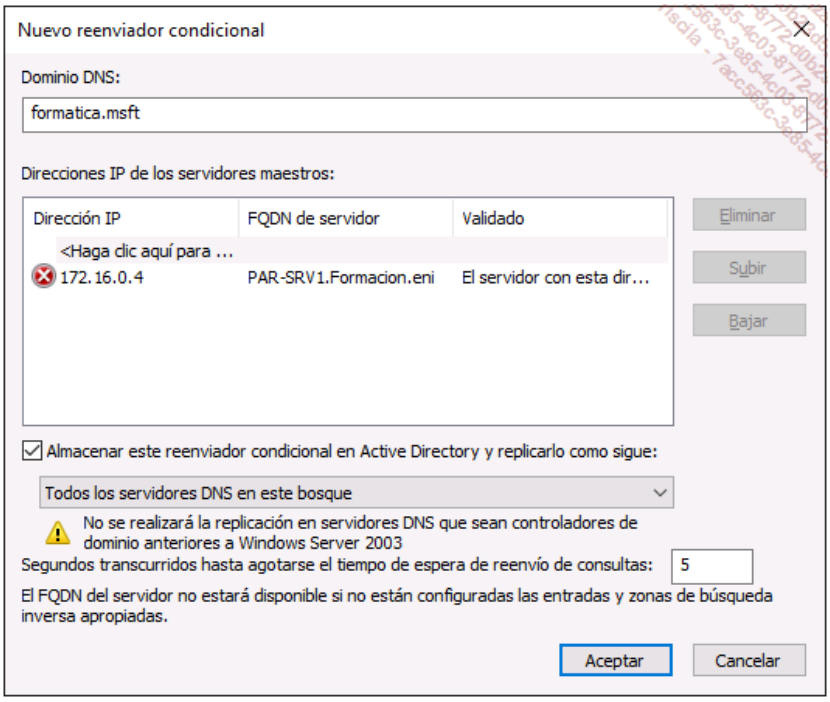
Haga clic en **Agregar host** y, a continuación, en **Finalizar**.

En **PAR-DC01**, abra la consola **Administrador de DNS** y, a continuación, haga clic con el botón derecho en **Reenviadores condicionales**.

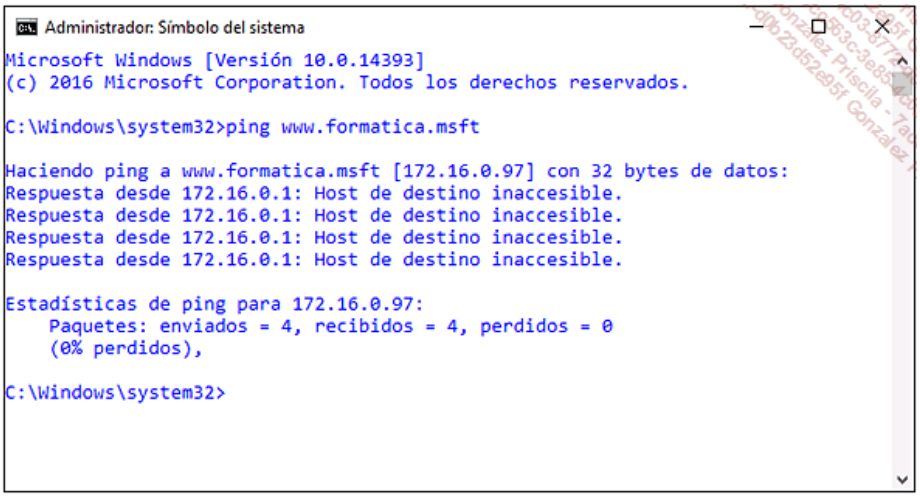
En el menú contextual, seleccione **Nuevo reenviador condicional**.

En el campo **Dominio DNS** escriba **Formatica.msft** y, a continuación, 172.16.0.4 en **Direcciones IP de los servidores maestros**.

Marque la opción **Almacenar este reenviador condicional en Active Directory y replicarlo como sigue**. Deje el valor por defecto en la lista desplegable y, a continuación, haga clic en **Aceptar**.



Abra una ventana de comandos DOS y, a continuación, escriba `ping www.formatica.msft`.



La resolución se realiza correctamente, no se obtiene ninguna respuesta dado que la dirección indicada no existe en la maqueta.

4. Creación de una zona secundaria y zona de stub

Objetivo: creación de una zona secundaria para el dominio demo.local y de una zona de stub para el dominio Formatica.msft.

Máquinas virtuales utilizadas: PAR-DC01, PAR-SRV1 y PAR-SRV2.

Si la máquina **PAR-SRV2** es miembro del dominio, apague la máquina y realice un punto de control de las máquinas **PAR-DC01** y **PAR-SRV2**.

En **PAR-SRV2**, inicie una sesión como administrador de dominio.

Saque la máquina del dominio **Formacion.eni** y reinicie.

En **PAR-SRV2**, inicie una sesión como administrador local.

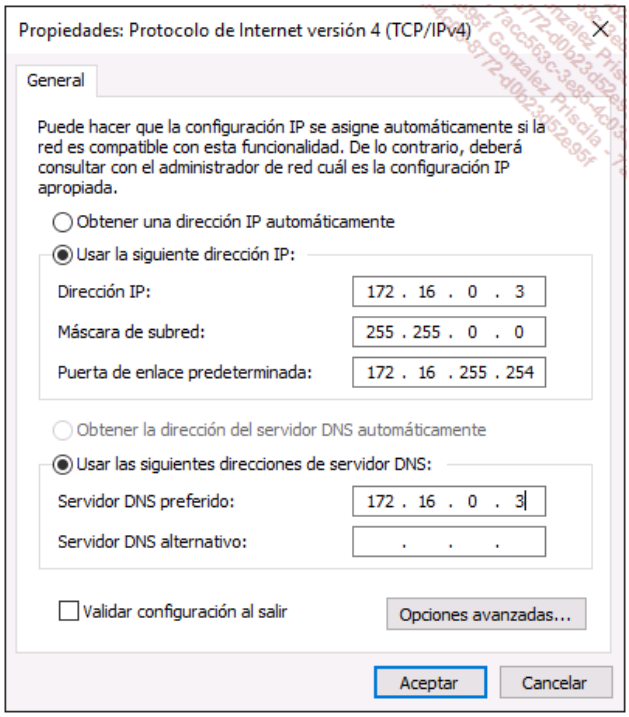
Abra la consola **Centro de redes y recursos compartidos**.

Haga clic en **Cambiar configuración del adaptador**.

Haga clic con el botón derecho en la tarjeta de red y, a continuación, seleccione la opción **Propiedades** en el menú contextual.

Haga doble clic en **Protocolo de Internet versión 4 (TCP/IPv4)**.

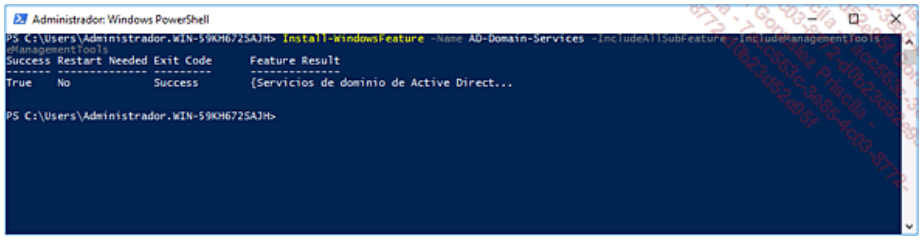
Modifique la configuración IP de la máquina para que posea su dirección IP en el campo **Servidor DNS preferido**.



Haga clic en **Aceptar**.

Abra una ventana de comandos PowerShell como Administrador y ejecute el siguiente comando:

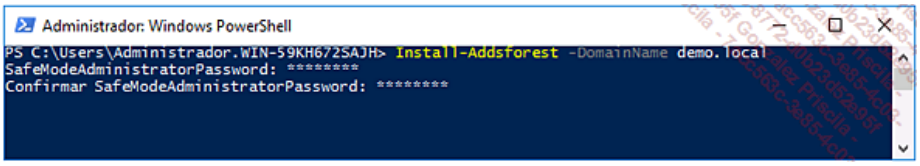
```
Install-WindowsFeature -Name AD-Domain-Services -IncludeAllSubFeature
-IncludeManagementTools
```



Abra una ventana de comandos PowerShell como Administrador y ejecute el siguiente comando:

```
Install-Addsforest -DomainName demo.local
```

Introduzca como contraseña de restauración **Pa$$w0rd** y seleccione **T** para la instalación del dominio Active Directory.

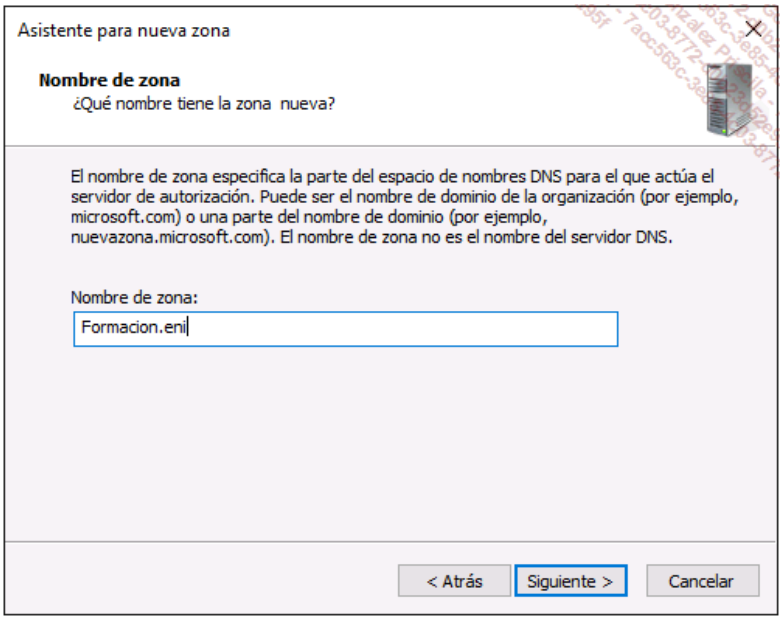


Inicie una sesión como Administrador del dominio (**DEMO\Administrador**) con la contraseña **Pa$$w0rd** y, a continuación, abra la consola **Administrador de DNS**.

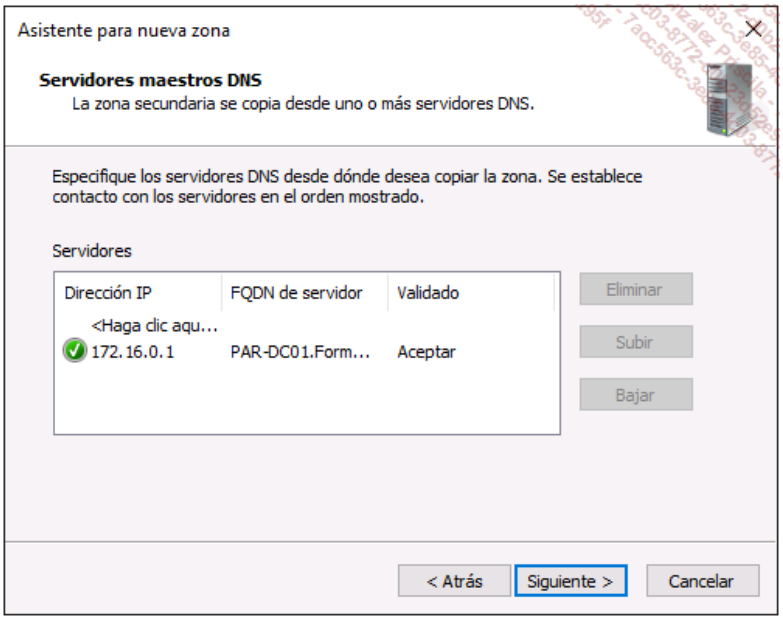
Despliegue **PAR-SRV2** y, a continuación, haga clic con el botón derecho en **Zonas de búsqueda directas** y seleccione **Nueva zona**.

En el asistente de creación de una nueva zona, haga clic en **Siguiente** y, a continuación, marque **Zona secundaria** antes de pasar a la siguiente pantalla.

En el campo **Nombre de zona**, introduzca **Formacion.eni** y, a continuación, haga clic en **Siguiente**.



En la ventana **Servidores maestros DNS**, introduzca la dirección IPv4 de la máquina **PAR-DC01**.

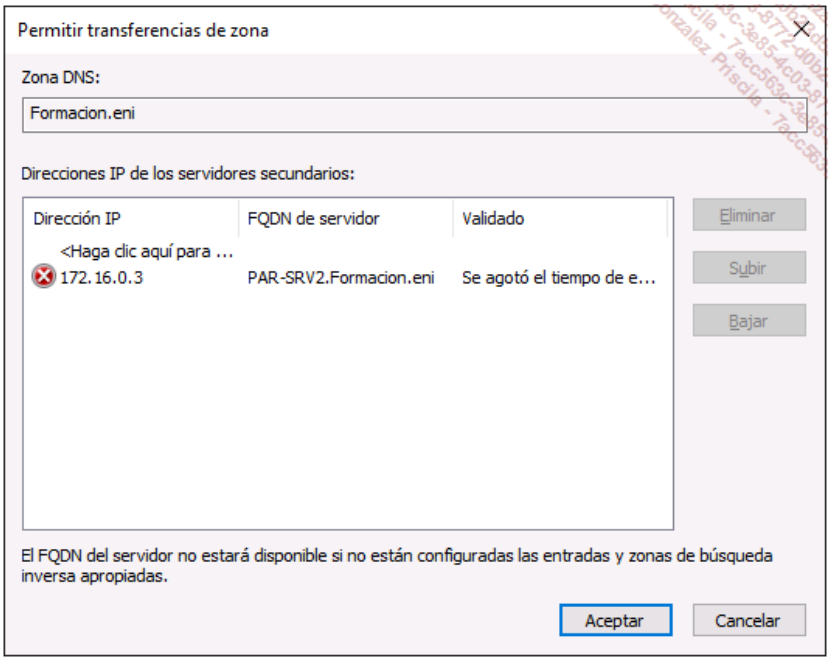


Haga clic en **Siguiente** y, a continuación, en **Finalizar**.

Cambie a la máquina **PAR-DC01**, abra la consola **Administrador de DNS**.

Despliegue **PAR-DC01**, **Zonas de búsqueda directa - Formacion.eni**, haga clic con el botón derecho en **Propiedades**, seleccione la pestaña **Transferencia de Zona**, marque la opción **Permitir transferencia de zona**, y marque **solo a los siguientes servidores**.

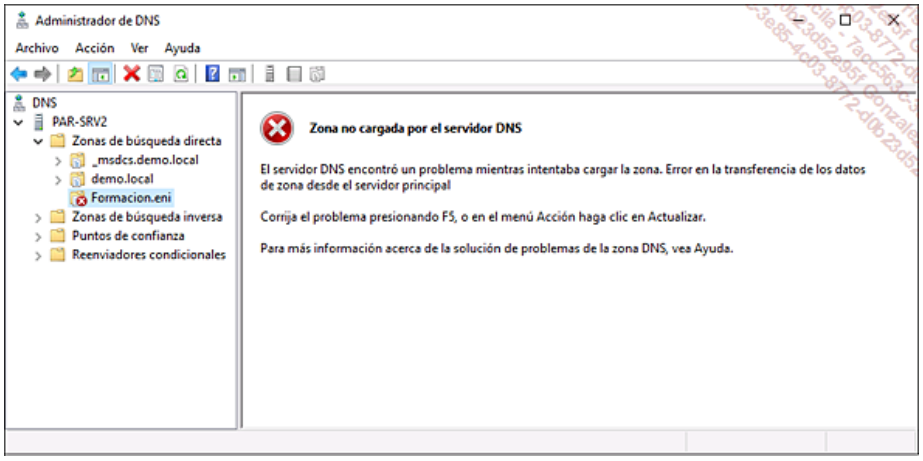
Haga clic en **Modificar** y agregue la dirección IPv4 de **PAR-SRV2**.



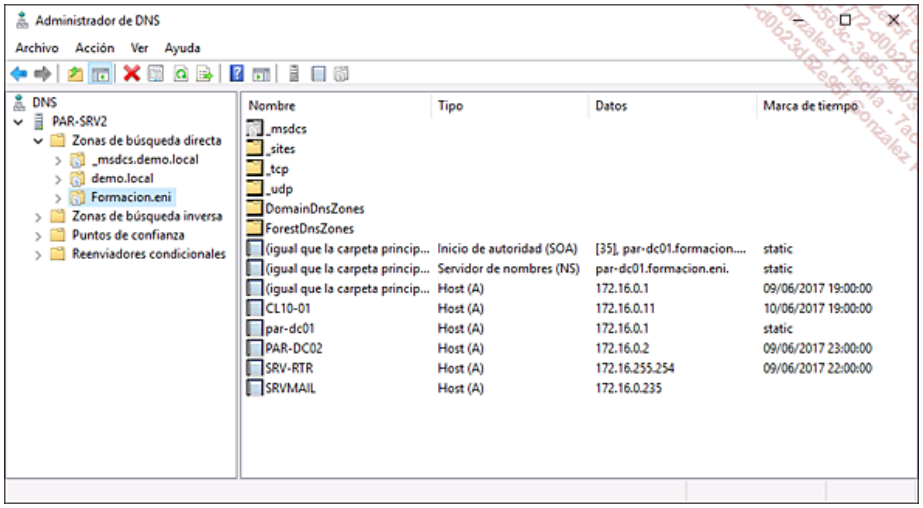
Haga clic dos veces en **Aceptar**.

Cambie a la máquina **PAR-SRV2**, abra la consola **Administrador de DNS**.

Despliegue **PAR-SRV2**, **Zonas de búsqueda directa - Formacion.eni**; debe aparecer un error.



Haga clic con el botón derecho en **Formacion.eni** y seleccione **Transferir desde Maestro**.

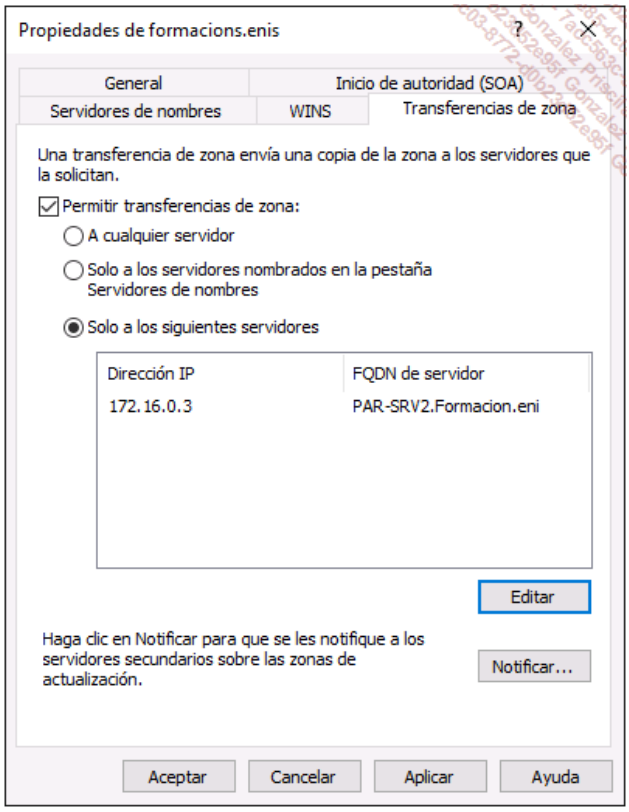


Queremos recuperar la zona Formacion.eni como solo lectura en el controlador de dominio PAR-SRV2 del dominio demo.local.

Cambie a la máquina **PAR-SRV1**, despliegue **PAR-SRV1**, **Zonas de búsqueda directa - Formatica.msft**, haga clic en **Propiedades**, seleccione la pestaña **Transferencias de zona**, marque la opción **Permitir transferencias de zona**, y seleccione **Solo a los siguientes servidores**.

Haga clic en **Modificar** y agregue la dirección IPv4 de **PAR-SRV2**.

Haga clic en **Aceptar**.



Haga clic en **Aceptar**.

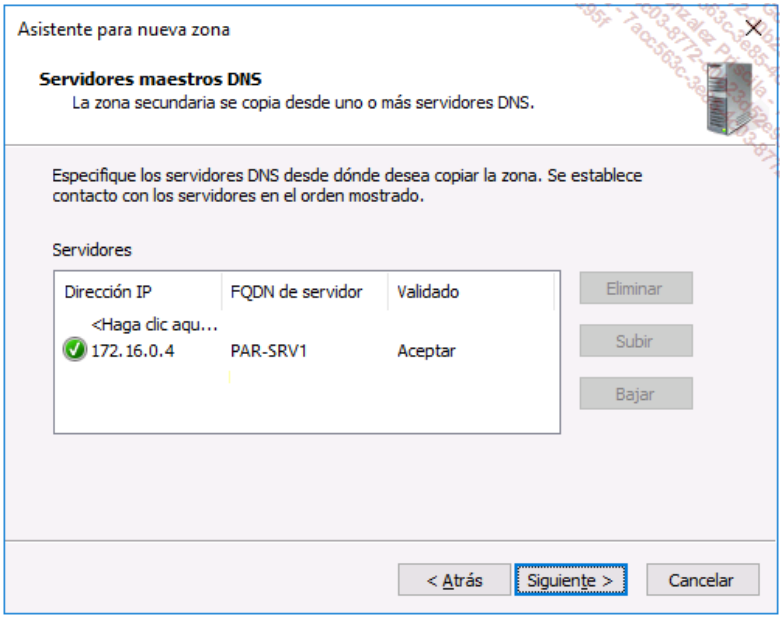
En la máquina **PAR-SRV2**, abra la consola **Administrador de DNS**.

Despliegue **PAR-SRV2** y, a continuación, haga clic con el botón derecho en **Zonas de búsqueda directa** y seleccione **Zona nueva**.

En el asistente de creación de nueva zona, haga clic en **Siguiente**, seleccione a continuación **Zona secundaria** antes de pasar a la siguiente pantalla.

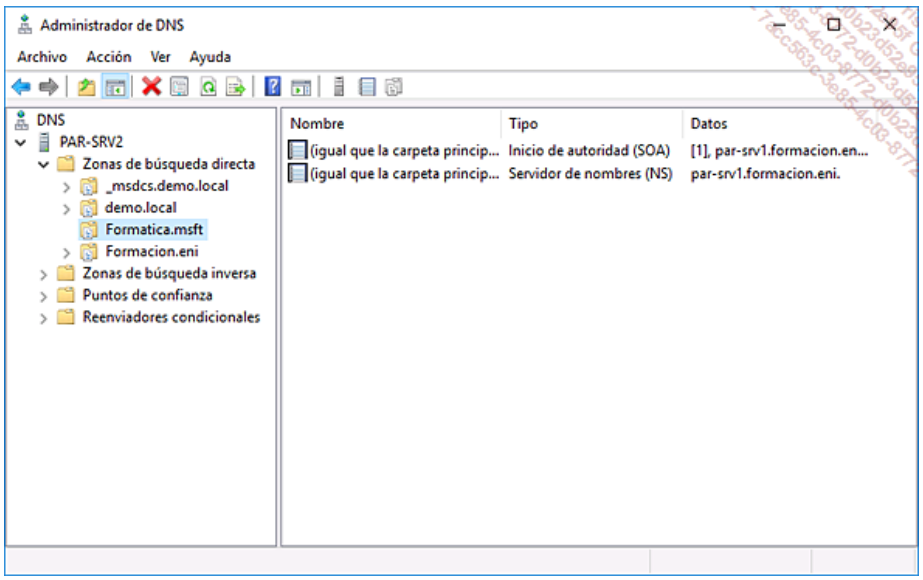
En el campo **Nombre de zona**, escriba **Formacion.eni** y haga clic en **Siguiente**.

En la ventana **Servidores maestros DNS**, introduzca la dirección IPv4 de la máquina **PAR-SRV1**.



Haga clic en **Siguiente** y en **Finalizar**.

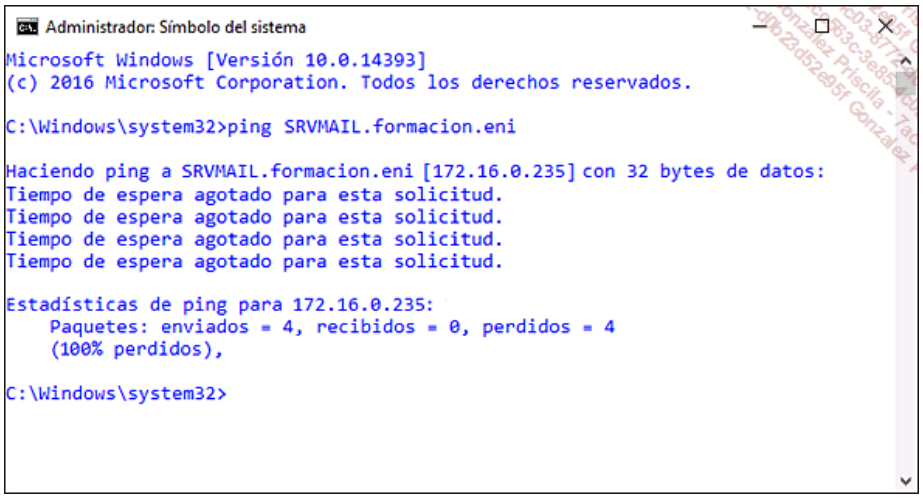
Haga clic con el botón derecho en **Formatica.msft** y seleccione **Transferir desde maestro**.



Acabamos de recuperar la zona de stub Formatica.msft en el controlador de dominio PAR-SRV2 del dominio demo.local.

Abra una ventana de comandos y compruebe el siguiente comando:

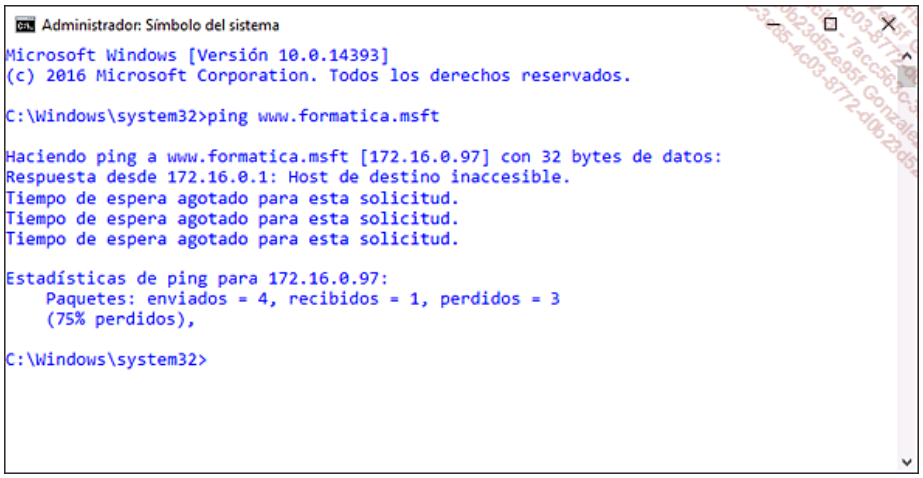
```
ping srvmail.formacion.eni
```



La resolución de nombres funciona; en cambio, el ping no funciona, pues no tenemos ninguna máquina activa con esta dirección IPv4.

Abra una ventana de comandos y compruebe el siguiente comando:

```
ping www.formatica.msft
```



La resolución de nombres funciona también aquí.

5. Implementación de DNSSEC y de reglas DNS

Objetivo: Securizar la infraestructura de resolución de nombres e implementar reglas de respuestas DNS en función de diversos criterios.

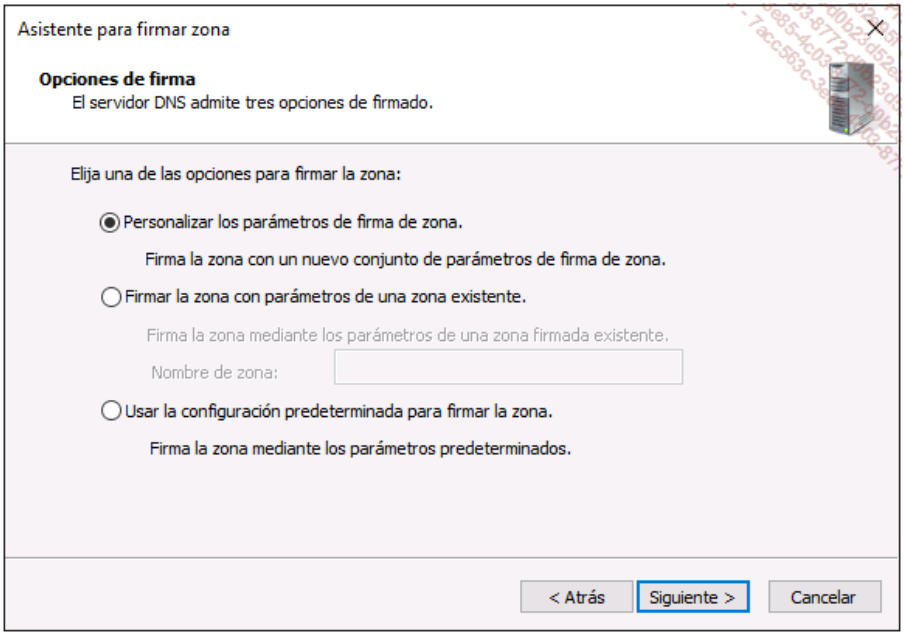
Máquinas virtuales utilizadas: PAR-DC01, PAR-DC02, SRV-RTR, CL10-01 y CL10-02.

En **PAR-DC01**, inicie una sesión como administrador de dominio y abra la consola **Administrador de DNS**.

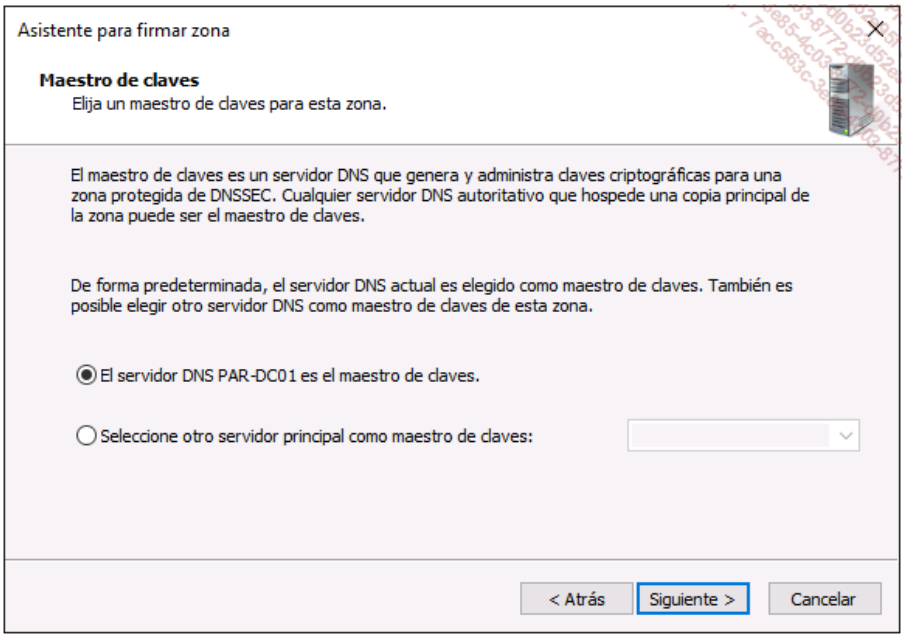
Despliegue **PAR-DC01**, **Zonas de búsqueda directa - Formacion.eni**, haga clic con el botón derecho en **DNSSEC** y seleccione **Firmar la zona**.

Haga clic en **Siguiente**.

Seleccione **Personalizar los parámetros de firma de zona**.

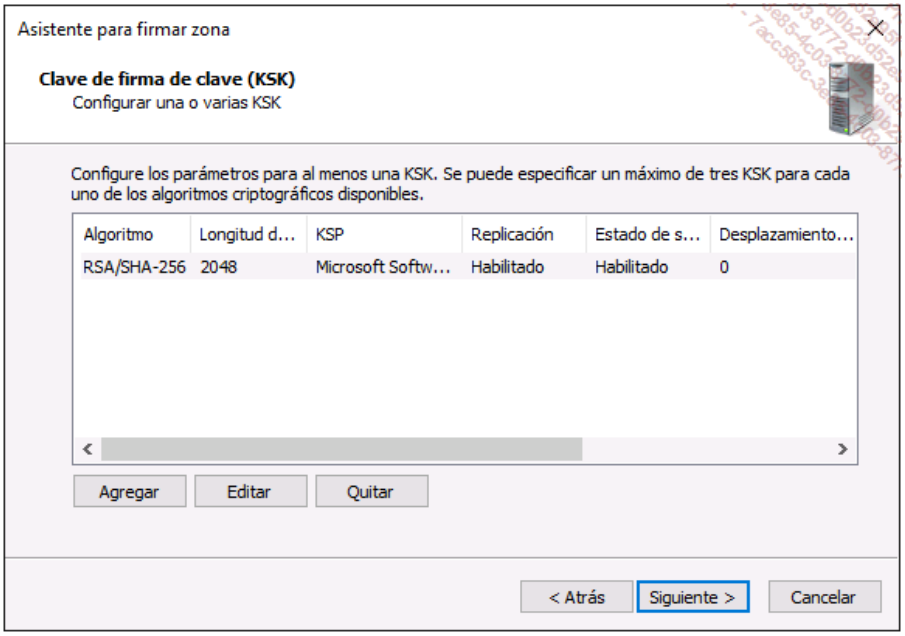


Haga clic en **Siguiente**.



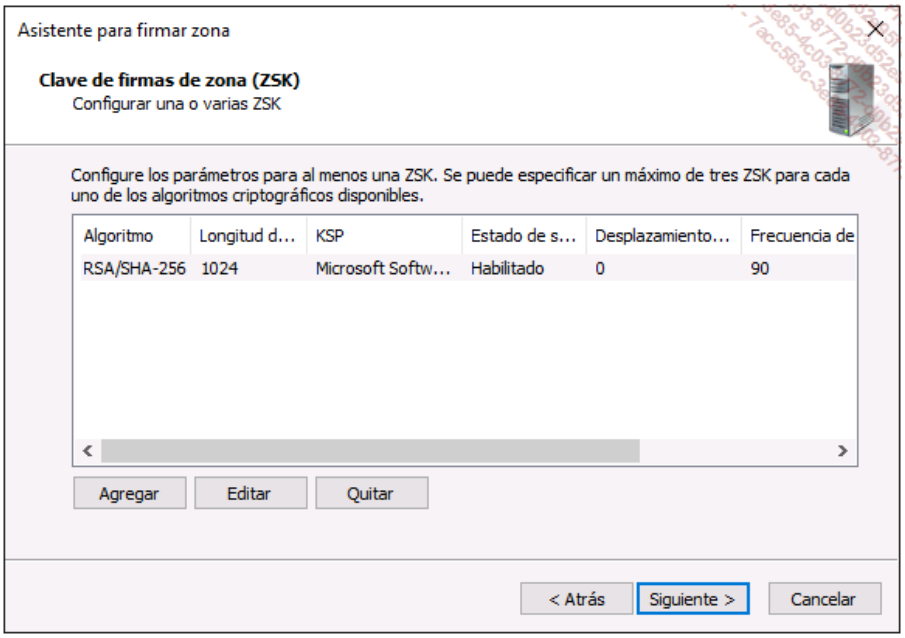
Haga clic dos veces en **Siguiente**.

En la etapa de configuración de la clave **KSK**, haga clic en **Agregar**, deje la información por defecto y haga clic en **Aceptar**.



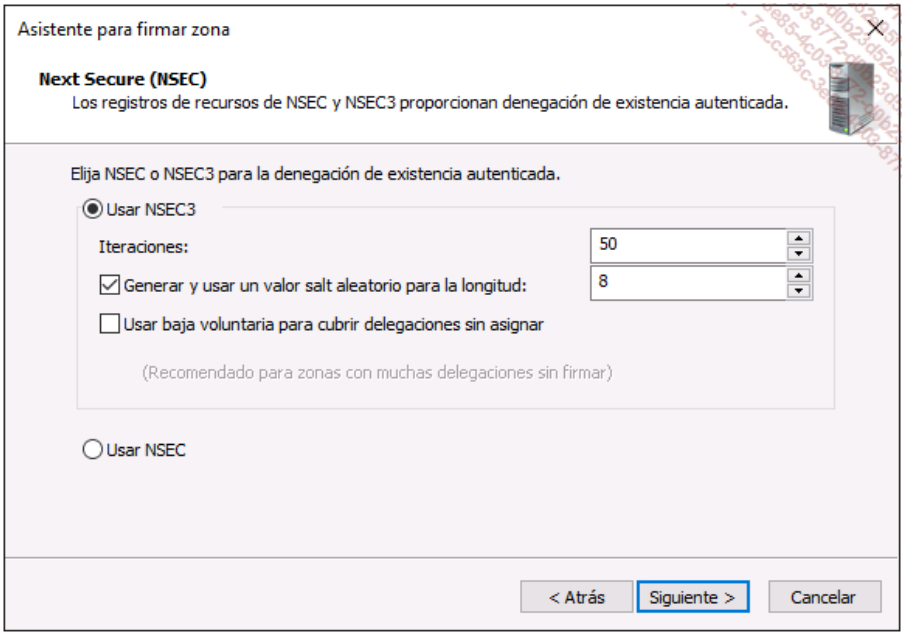
Haga clic dos veces en **Siguiente**.

En la etapa de configuración de la **clave ZSK**, haga clic en **Agregar**, deje la información por defecto y haga clic en **Aceptar**.



Haga clic en **Siguiente**.

Asegúrese de que está marcada la opción **Usar NSEC3**.

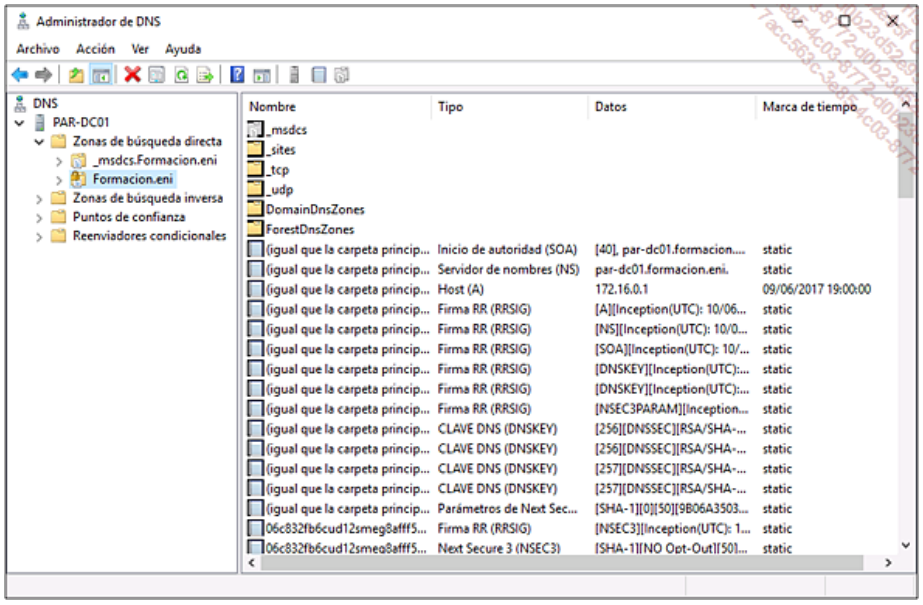


Haga clic en **Siguiente**.

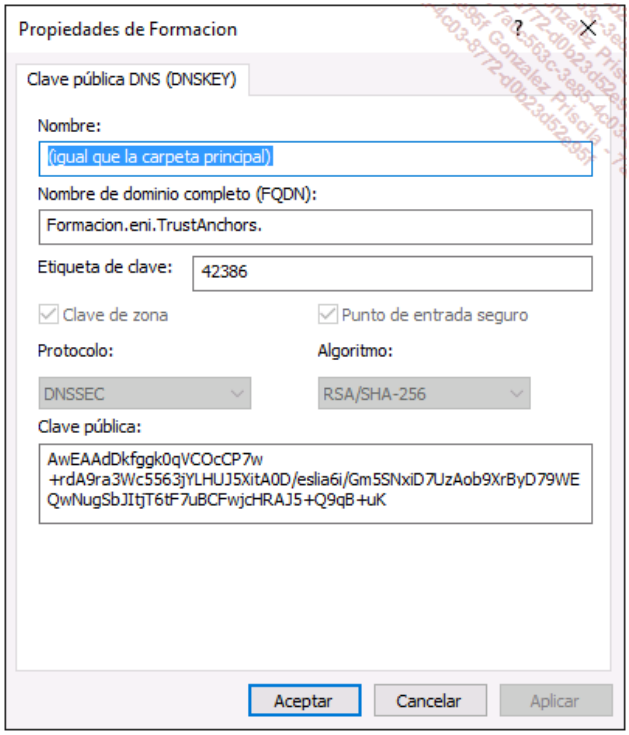
Seleccione **Habilitar la distribución de anclajes de veracidad para esta zona**.

Haga clic tres veces en **Siguiente** y luego en **Finalizar**.

La zona DNS **Formacion.eni** está ahora firmada con DNSSEC.

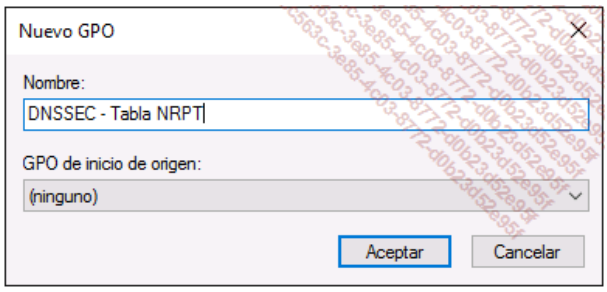


Despliegue **PAR-DC01**, **Zonas de búsqueda directa - Puntos de confianza - eni - formacion** y haga clic con el botón derecho en el primer registro para ver la clave pública correspondiente.



Abra la consola **Administración de directivas de grupo**.

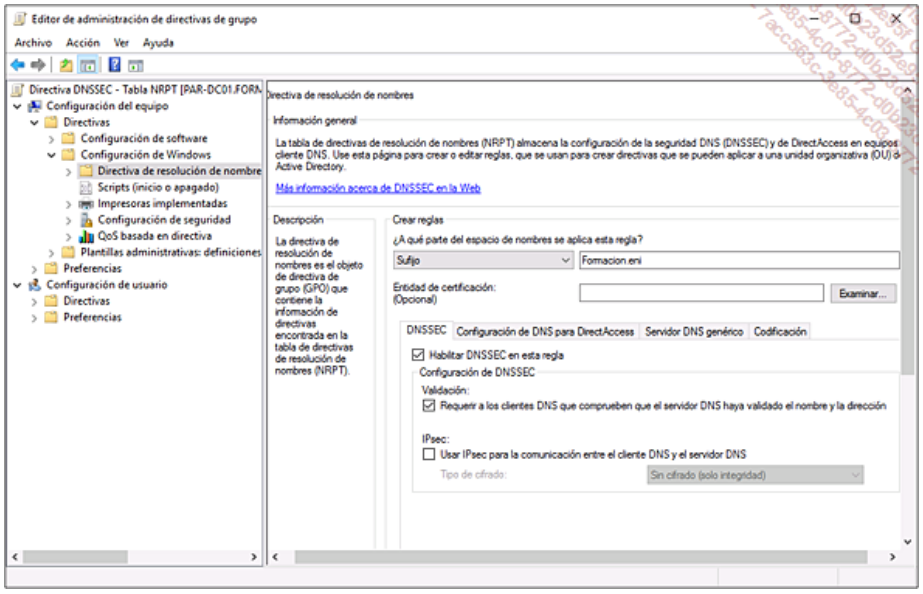
Despliegue **Formacion.eni**, haga clic con el botón derecho en **Crear un GPO en este dominio y vincularlo aquí**, en el campo nombre escriba **DNSSEC - Tabla NRPT** y haga clic en **Aceptar**.



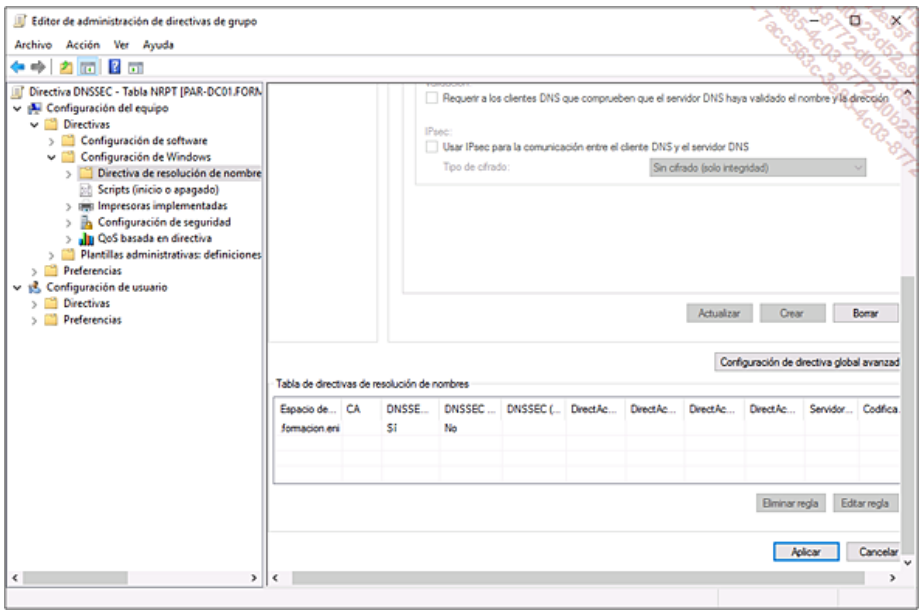
Edite la directiva de grupo creada y navegue hasta **Configuración del equipo - Directivas - Configuración de Windows - Directiva de**

resolución de nombres.

Informe el **sufijo DNS** con el valor **Formacion.eni**, marque **Habilitar DNSSEC en esta regla** y en los parámetros de la regla marque**Requerir a los clientes DNS que comprueben que el servidor DNS haya validado el nombre y la dirección**.



Haga clic en **Crear** y en **Aplicar**.



Si no lo hubiera hecho, una **SRV-RTR** al dominio **Formacion.eni**.

Inicie una sesión como **administrador@formacion.eni** (o como FORMACION\administrador) en el servidor **SRV-RTR**.

Abra la consola **Administrador del servidor**.

Haga clic en el enlace **Agregar roles y características** y, a continuación, en la ventana **Antes de comenzar**, haga clic en **Siguiente**.

Deje la opción por defecto en la ventana **Seleccionar tipo de instalación** y, a continuación, haga dos veces clic en **Siguiente**.

En la ventana **Seleccionar roles de servidor**, marque **Acceso remoto** y, a continuación, haga clic en el botón **Agregar características**.

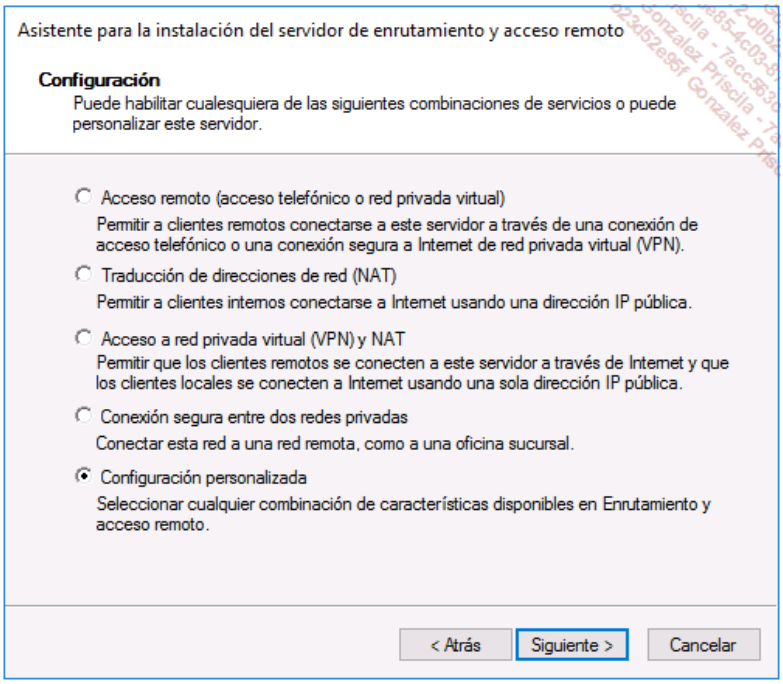
Haga clic tres veces en **Siguiente** y a continuación, en la ventana **Servicios de rol**, marque **Enrutamiento** y haga clic en **Siguiente**.

Haga clic dos veces en **Siguiente** (los **servicios de rol IIS** deben dejarse marcados por defecto) y, a continuación, haga clic en **Instalar**.

Una vez terminada la instalación, abra la consola **Enrutamiento y acceso remoto** desde las **Herramientas administrativas**.

Haga clic con el botón derecho en **SRV-RTR** y, a continuación, en el menú contextual, haga clic en **Configurar y habilitar Enrutamiento y el acceso remoto**.

En la ventana **Bienvenida**, haga clic en **Siguiente** y, a continuación, marque **Configuración personalizada**.

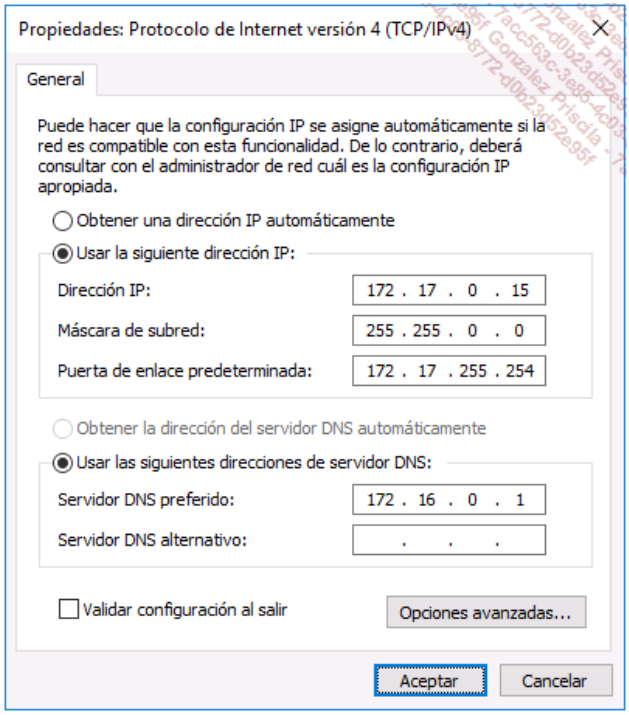


Haga clic en **Siguiente** para validar esta opción.

En la ventana **Configuración personalizada**, marque **Enrutamiento** y, a continuación, haga clic en **Siguiente**.

Iniciar servicio y haga clic en **Finalizar**.

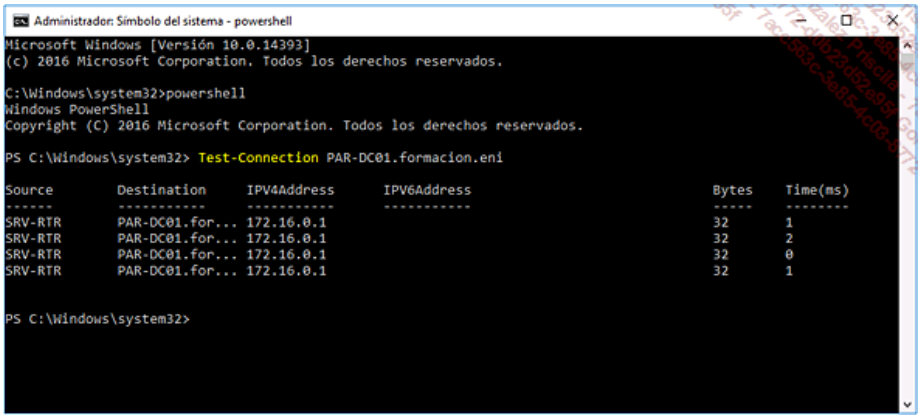
Desplace la máquina **CL10-02** hasta el conmutador de **BARCELONA**, modifique la dirección IPV4 del cliente de la siguiente manera:



A continuación, haga clic en **Aceptar**.

Abra una consola PowerShell como Administrador y ejecute el siguiente comando:

```
Test-connection PAR-DC01.formacion.eni
```



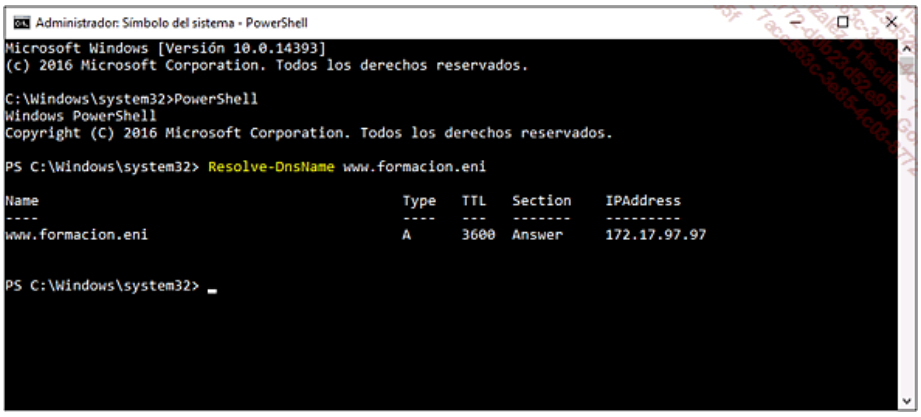
El enrutamiento funciona; a continuación, vamos a configurar las reglas DNS en función de las redes de proveniencia de las peticiones de los clientes.

Cambie a la máquina **PAR-DC01** y, a continuación, abra una consola PowerShell como administrador y ejecute los siguientes comandos:

```
Add-DnsServerClientSubnet -Name "Madrid_ssred" -IPv4Subnet "172.16.0.0/16"
Add-DnsServerClientSubnet -Name "Barcelona_ssred" -IPv4Subnet "172.17.0.0/16"
Add-DnsServerZoneScope -ZoneName "formacion.eni" -Name "MadridZoneScope"
Add-DnsServerZoneScope -ZoneName "formacion.eni" -Name "BarcelonaZoneScope"
Add-DnsServerResourceRecord -ZoneName "formacion.eni" -A -Name "www"
-IPv4Address "172.17.97.97" -ZoneScope "BarcelonaZoneScope"
Add-DnsServerResourceRecord -ZoneName "formacion.eni" -A -Name "www"
-IPv4Address "172.16.21.21" -ZoneScope "MadridZoneScope"
Add-DnsServerQueryResolutionPolicy -Name "MadridPolicy" -Action ALLOW
-ClientSubnet "eq,Madrid_ssred" -ZoneScope "MadridZoneScope,1" -ZoneName
"formacion.eni"
Add-DnsServerQueryResolutionPolicy -Name "BarcelonaPolicy" -Action ALLOW
-ClientSubnet "eq,Barcelona_ssred" -ZoneScope "BarcelonaZoneScope,1" -ZoneName
"formacion.eni"
```

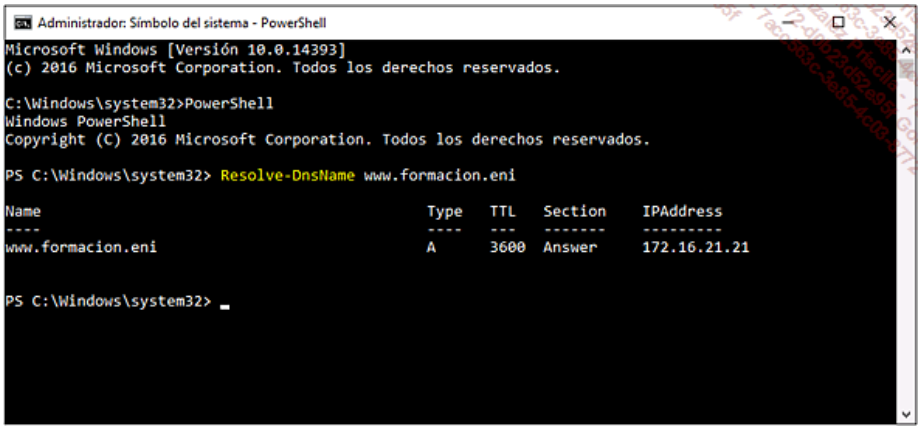
En **CL10-02**, abra una consola PowerShell como administrador y ejecute el siguiente comando:

```
Resolve-DNSName www.formacion.eni
```



En **CL10-01**, abra una consola PowerShell como administrador y ejecute el siguiente comando:

```
Resolve-DNSName www.formacion.eni
```



Las reglas de respuesta DNS aplicadas sobre la máquina **PAR-DC01** funcionan correctamente, pues, en función de la subred del cliente DNS, el servidor devuelve una dirección IPv4 diferente.

A continuación puede restablecer el conjunto de máquinas virtuales para que la máquina **PAR-SRV2** vuelva a ser miembro del dominio**Formacion.eni** al igual que **PAR-DC01**.

Validación de conocimientos adquiridos: preguntas/respuestas

1. Preguntas

Puede validar los conocimientos adquiridos respondiendo a las siguientes preguntas.

1. ¿Cuál es el rol del protocolo DNS?
2. ¿Por qué se dice que el sistema DNS es jerárquico?
3. ¿Se encuentra la misma información en un DNS privado que en un DNS público?
4. ¿Es posible almacenar zonas DNS?
5. ¿Cuáles son los requisitos previos para unir una zona a AD?
6. ¿Cuáles son las ventajas de integrar la zona en Active Directory?
7. ¿Qué dos componentes utiliza el servidor DNS cuando no puede resolver un nombre?
8. ¿Qué tipos de registros pueden crearse en un servidor DNS?
9. Enumere los distintos tipos de zona que es posible crear.
10. ¿Sobre qué propiedad de un registro se basa el borrado?
11. ¿Cuál es el mecanismo que permite securizar el proceso de resoluciones?
12. ¿Para qué sirven las reglas DNS?

2. Resultados

Consulte las siguientes páginas para comprobar sus respuestas.

Por cada respuesta correcta, cuente un punto.

Número de puntos: /12

Para superar este capítulo, su puntuación mínima debería ser de 10 sobre 12.

3. Respuestas

1. ¿Cuál es el rol del protocolo DNS?

   El protocolo DNS tiene como rol la resolución de nombres en direcciones IP y viceversa.

2. ¿Por qué se dice que el sistema DNS es jerárquico?

   DNS se compone de varios niveles, y cada uno de ellos se encarga de realizar la resolución. Es posible encontrar, por ejemplo, la raíz que posee en su base de datos la dirección IP de los servidores de primer nivel (es, com…). Cada nivel posee, por tanto, una parte del nombre DNS.

3. ¿Se encuentra la misma información en un DNS privado que en un DNS público?

   No, un servidor DNS privado contiene los registros que permiten resolver nombres de recursos locales al dominio mientras que el DNS público contiene, por su lado, registros de recursos que están accesibles desde el exterior.

4. ¿Es posible almacenar zonas DNS?

   Es posible almacenar zonas DNS en dos lugares: en un archivo de texto (C:\Windows\System32\dns) o en el directorio Active Directory.

5. ¿Cuáles son los requisitos previos para unir una zona a AD?

   El registro de una zona en Active Directory requiere que la zona sea de tipo primario. Es necesario, a su vez, que el servidor esté instalado sobre un controlador de dominio.

6. ¿Cuáles son las ventajas de integrar la zona en Active Directory?

   La integración en Active Directory permite una replicación al mismo tiempo que Active Directory (además de transferir la zona) y, a su vez, proteger las actualizaciones dinámicas.

7. ¿Qué dos componentes utiliza el servidor DNS cuando no puede resolver un nombre?

   Cuando un servidor no puede resolver un nombre puede, en función de la configuración realizada por el administrador, utilizar el o los reenviador(es) o las indicaciones de las raíces.

8. ¿Qué tipos de registros pueden crearse en un servidor DNS?

   Es posible crear varios registros. Los hosts (A o AAAA) permiten resolver un nombre en una dirección IP. Los punteros (PTR) permiten resolver una dirección IP en un nombre. Los registros de tipo CNAME ofrecen la posibilidad de implementar alias hacia un equipo o servidor. Por último, los registros de tipo NS permiten definir los distintos servidores DNS.

9. Enumere los distintos tipos de zona que es posible crear.

   Las zonas principales permiten al servidor tener permisos de lectura y de escritura en la zona. Este tipo de zona puede integrarse en Active Directory. Una zona secundaria no puede modificarse, los registros son de solo lectura y es necesario realizar una transferencia de zona para

proceder a la actualización de los registros. Este tipo de zona no puede integrarse en Active Directory. La zona de stub no contiene más que ciertos registros (A, NS y SOA) de una zona, lo que evita un acoplamiento completo de la zona.

10 ¿Sobre qué propiedad de un registro se basa el borrado?

Para realizar el borrado, un servidor DNS utiliza el timestamp con el objetivo de saber si el registro está obsoleto.

11 ¿Cuál es el mecanismo que permite securizar el proceso de resoluciones?

Para securizar la infraestructura DNS, es posible implementar DNSSEC, que permite asegurar que la información transmitida por el servidor DNS es segura y fiable. Esto consiste en firmar digitalmente los registros de la zona DNS.

12 ¿Para qué sirven las reglas DNS?

Las reglas DNS nos permiten configurar las respuestas de nuestro servidor DNS en función de distintos criterios, como la red de origen, el horario de la petición, el dominio interrogado...

Requisitos previos y objetivos

1. Requisitos previos

Poseer conocimientos de administración.

Poseer buenos conocimientos en redes.

2. Objetivos

Instalar y configurar IPAM.

Describir las funcionalidades de IPAM.

Presentación

IPAM (*IP Address Management*) es una funcionalidad integrada en los sistemas operativos Windows Server 2012. Ofrece la posibilidad de descubrir, supervisar, auditar y administrar uno o varios direccionamientos IP. IPAM permite también realizar la administración y la supervisión de servidores DHCP (*Dynamic Host Configuration Protocol*) y DNS (*Domain Name Service*).

Los siguientes componentes están incluidos en esta funcionalidad:

- **Descubrir automáticamente la infraestructura de direcciones IP**: descubre controladores de dominio, servidores DHCP y servidores DNS en el dominio afectado.
- **Visualización, creación de informes y administración personalizada del espacio de direccionamiento IP**: ofrece los detalles de seguimiento y de uso detallado de las direcciones IP. Los espacios de direccionamiento IPv4 e IPv6 están organizados por bloques de direcciones IP, por rangos de direcciones IP y por direcciones IP individuales.
- **Auditoría de las modificaciones de configuración del servidor y seguimiento del uso de las direcciones IP**: muestra los eventos operacionales del servidor IPAM y DHCP administrado. También se realiza un seguimiento de las direcciones IP, ID de cliente, nombre de host o nombre de usuario. Los eventos del contrato DHCP y los eventos de inicio de sesión de usuario se recogen en los servidores NPS (*Network Policy Server*), sobre los controladores de dominio y sobre los servidores DHCP.

Antes de desplegar la funcionalidad IPAM, es necesario pensar qué estrategia de despliegue se quiere escoger. Tenemos a nuestra disposición dos maneras de desplegar: el método distribuido mediante un servidor IPAM en cada sitio de la empresa o el método centralizado con un servidor para el conjunto de la empresa.

IPAM realiza tentativas periódicas de localización de los controladores de dominio, de los servidores DNS y DHCP. Esta operación de localización afecta, evidentemente, a los servidores que se encuentran en el ámbito de las directivas de grupo. Para poder ser gestionadas por IPAM y autorizar el acceso a este último, debe realizarse la configuración de los parámetros de seguridad y de los puertos del servidor.

La comunicación entre el servidor IPAM y los servidores administrados se realiza mediante WMI o RPC.

Especificaciones de IPAM

El alcance de los servidores IPAM está limitado únicamente a un único bosque Active Directory. Se tienen en cuenta los servidores NPS, DNS y DHCP Windows Server 2008 o superior, miembros de un dominio Active Directory. En cambio, algunos elementos de red (WINS - *Windows Internet Naming Service, proxy*…) no están soportados. Desde Windows Server 2012 R2 es posible utilizar una base de datos SQL en lugar de la base de datos interna proporcionada por defecto.

Un servidor IPAM puede gestionar 150 servidores DHCP y 500 servidores DNS (6000 ámbitos y 150 zonas DNS).

Con la instalación de IPAM, se instalan también las siguientes funcionalidades:

- **Herramientas de administración del servidor remoto**: instalación de las herramientas DHCP, DNS y del cliente IPAM que permiten realizar la administración remota de los servidores DHCP, DNS e IPAM.
- **Base de datos interna Windows**: base de datos interna que puede instalarse mediante los roles y características internas.
- **Servicio de activación de procesos Windows**: elimina la dependencia con el protocolo HTTP generalizando el modelo del proceso IIS.
- **Administración de las directivas de grupo**: instala la consola MMC que permite administrar las directivas de grupo.
- **.NET Framework**: instalación de la funcionalidad .NET Framework 4.5.

Características de IPAM

Una vez instalada la funcionalidad, se crean los siguientes grupos locales:

- **Usuarios IPAM**: los miembros tienen la posibilidad de mostrar toda la información del descubrimiento del servidor, así como aquella información asociada al espacio de direccionamiento IP y la administración del servidor. El acceso a la información de seguimiento de las direcciones IP le está prohibido.
- **Administrador IPAM MSM (*Multi-Server Management*)**: además de los permisos de usuario IPAM, puede realizar tareas de administración del servidor y tareas de administración propias de IPAM.
- **Administradores IPAM ASM (*Address Space Management*)**: además de los permisos de usuario IPAM, puede realizar tareas de direccionamiento IP y tareas de administración propias de IPAM.
- **Administrador de Auditoría IPAM IP**: los miembros de este grupo pueden realizar tareas de administración propias de IPAM, así como mostrar la información de seguimiento de la dirección IP.
- **Administradores IPAM**: los administradores IPAM tienen acceso a todos los datos IPAM y pueden, a su vez, realizar todas las tareas IPAM.

Las tareas IPAM se ejecutan, regularmente, en función de una periodicidad y se definen en el planificador de tareas (Microsoft / Windows / IPAM):

- **DiscoveryTask**: permite descubrir de forma automática servidores DC, DHCP y DNS.
- **AddressUtilizationCollectionTask**: recoge los datos de uso del espacio de direccionamiento IP para los servidores DHCP.
- **AuditTask**: recoge información de auditoría de servidores DHCP, IPAM, NPS y DC, así como de los contratos DHCP.
- **ConfigurationTask**: recoge información de configuración de los servidores DHCP, DNS para ASM y MSM.
- **ServerAvailabilityTask**: recupera el estado de los servidores DHCP y DNS.

La instalación y configuración de la funcionalidad IPAM se realiza en los trabajos prácticos.

Novedades aportadas por Windows Server 2016

Con Windows Server 2016, Microsoft ha aportado mejoras a las funcionalidades existentes e incluye novedades en IPAM 2016.

1. Gestión mejorada de las direcciones IP

Las siguientes características mejoran las funcionalidades de gestión del direccionamiento IPAM:

- **IPAM**, en su versión 2016, soporta en lo sucesivo las siguientes máscaras de subred **/31**, **/32** y **/128**. Observe que el soporte de las máscaras de subred se corresponde con las direcciones de bucle /32 para IPv4 y /128 para IPv6.
- Microsoft ha introducido los dos nuevos cmdlets **IpamFreeSubnet** e **IpamFreeRange**. El primero permite buscar las subredes libres en un rango IP y el segundo es complementario, pues permite renovar un rango de direcciones IP disponible para una subred.

2. Gestión mejorada del servicio DNS

Se han agregado nuevas características en Windows Server 2016; en particular, aquellas que permiten gestionar los servicios DNS:

- La gestión de zonas DNS y el registro de los recursos.
- La posibilidad de actuar sobre las **zonas secundarias** y **zonas de stub** como la transferencia desde el DNS maestro.
- La gestión de los redirectores.

Despliegue de IPAM y configuración

IPAM posee una funcionalidad de descubrimiento automático que simplifica la identificación inicial de los servidores que pueden administrarse con IPAM. Sin embargo, son necesarias ciertas tareas de configuración para preparar el entorno.

1. Instalación

La implementación de IPAM implica varias etapas importantes:

- Examinar la funcionalidad IPAM y alinear los objetivos de despliegue.
- Confirmar que los requisitos previos del sistema y del entorno se cumplen.
- Desarrollar un plan de despliegue.
- Desplegar los servidores IPAM.
- Desplegar los clientes IPAM.
- Asignar los roles de administración IPAM.
- Utilizar IPAM para gestionar la infraestructura IP.

Una vez decidida la topología IPAM que se va a utilizar (distribuida, centralizada, híbrida), puede desplegar servidores IPAM siguiendo las etapas siguientes:

- Instalar la funcionalidad IPAM en el servidor. Puede instalarla a través del administrador del servidor o utilizando el siguiente cmdlet:

```
Install-WindowsFeature IPAM – IncludeManagementTools
```

- Configurar cada servidor IPAM para crear las autorizaciones, los recursos compartidos de archivos y parámetros en los servidores gestionados. Esta etapa se lleva a cabo mediante un objeto de directiva de grupo (GPO).

  El uso de un objeto GPO ofrece varias ventajas respecto a la configuración manual:

  - La configuración de la GPO aplicada está menos sujeta al error de configuración humano.
  - La configuración de la GPO se aplica automáticamente a los servidores cuando se encuentran en estado "Administrado".
  - La configuración se elimina fácilmente deshabilitando o eliminando el vínculo con la GPO.

- Configurar y ejecutar el descubrimiento del servidor. Debe configurar el ámbito de descubrimiento de los servidores que desea administrar seleccionando el dominio o los dominios Active Directory sobre los que se desarrollará el descubrimiento. También puede agregar manualmente un servidor en la gestión de IPAM especificando el nombre de dominio completo (FQDN) del servidor que desea administrar.

Es posible administrar y gestionar un servidor IPAM de manera remota instalando las herramientas RSAT. Para los clientes Windows 8, 8.1, y 10, la funcionalidad se habilita automáticamente, a diferencia de lo que ocurre con los servidores 2012, 2012 R2 y 2016, donde hay que instalar la característica **RSAT / IPAM Management Client**.

2. Administración

La configuración de la administración puede resultar una tarea compleja según cómo se despliegue su infraestructura IPAM. Un servidor IPAM puede administrar varios dominios y bosques de Active Directory, y también es posible limitar un servidor IPAM a roles específicos o limitar los servidores administrados.

Podemos utilizar la administración basada en roles para gestionar los diversos servidores IPAM.

- **Roles**. Un rol es una colección de operaciones IPAM. Puede asociar un rol a un **usuario** o un **grupo de Windows** mediante una directiva de acceso. Existen ocho roles de Administrador integrados para una mayor granularidad, pero también puede crear roles personalizados para responder a las necesidades propias de su empresa. Puede crear y modificar roles en el nodo de control de acceso en la consola de administración de IPAM.
- **Ámbito del acceso**: el ámbito del acceso determina los distintos objetos a los que tendrá acceso un usuario. Por ejemplo, puede crear ámbitos de acceso basados en la localización geográfica. Puede crear y modificar ámbitos de acceso desde el nodo de control de acceso en la consola de administración de IPAM.
- **Directivas de acceso**. Una directiva de acceso combina un rol con un ámbito de acceso para asignar autorizaciones a un usuario o un grupo. Por ejemplo, puede definir una directiva de acceso de un usuario con un rol llamado **Admin Block IP** y un ámbito de acceso llamado **Global\Barcelona**. Como consecuencia, este usuario tendrá autorización para modificar y eliminar los bloques de direcciones IP que estén asociadas al ámbito de acceso **Barcelona**. Puede crear y modificar directivas de acceso desde el nodo de control de acceso en la consola de administración de IPAM.

Tras la instalación de un servidor IPAM, se crean ciertos grupos de seguridad que permiten realizar esta gestión basada en roles. La siguiente tabla muestra estos grupos de seguridad.

Grupos de seguridad	Descripciones

Administrador IPAM DNS	Los miembros de este grupo pueden administrar los servidores DNS y sus registros de recursos y de zonas DNS asociadas.
Administrador IPAM MSM	Los miembros de este grupo pueden administrar servidores DHCO, ámbitos, políticas y servidores DNS.
Administrador IPAM ASM	Los miembros de este grupo pueden realizar tareas sobre el espacio de direccionamiento IP, además de las tareas habituales en la administración de IPAM.
Administrador IP Address Record	Los miembros de este grupo pueden administrar las direcciones IP, incluidas las direcciones no asignadas, y los miembros pueden crear y eliminar instancias de direccionamiento IP.
Administrador IPAM	Los miembros de este grupo poseen permisos para ver todos los datos de IPAM y realizar todas las tareas de IPAM.
Administrador IPAM DHCP	Administran completamente los servidores DHCP.
Administrador de reservas IPAM DHCP	Administran las reservas DHCP.
Administrador de ámbitos IPAM DHCP	Administran los ámbitos DHCP.
Administrador de recursos DNS	Administran los registros de recursos DNS.

3. Configuración

Puede configurar IPAM en función de su entorno y proporcionar el nivel de facilidad en la administración que necesite. En la mayoría de los casos, puede configurar IPAM utilizando los objetos GPO desplegados durante el proceso de instalación.

Cuando ponga en marcha un servidor IPAM, se crearán tres objetos de directiva de grupo en alguno de los dominios que escoja, y se vinculan estos objetos de directiva de grupo con la raíz del dominio en la consola de administración de las directivas de grupo. Cuando seleccione**Configuración de la directiva de grupo**, tendrá que proporcionar un prefijo para los objetos de directiva de grupo con el objetivo de poder identificarlos fácilmente en la consola GPMC.

Los objetos GPO creados son:

- **<Prefijo>_DHCP**. Este objeto GPO se utiliza para aplicar parámetros que permiten a IPAM supervisar, administrar y recopilar información de los servidores DHCP a través de la red. Despliega IPAM, crea las tareas planificadas y agrega las reglas de cortafuegos de tráfico entrante para la gestión remota del registro de eventos (RPC-EMAP y RPC), la gestión de los servicios remotos (RPC-EMAP y RPC) y el servidor DHCP (RPCSS-In y RPC -In).
- **<Prefijo>_DNS**. Este objeto GPO se utiliza para aplicar los parámetros que permiten a IPAM supervisar y recopilar información desde los servidores DNS administrados en la red. Despliega IPAM, crea las tareas planificadas y agrega las reglas de cortafuegos de tráfico entrante para RPC (TCP, entrante), el mapeo del punto final RPC (TCP, entrante), la gestión remota del registro de eventos (RPC-EMAP y RPC) y la gestión de los servicios remotos (RPC-EMAP y RPC).
- **<Prefijo>_DC_NPS**. Este objeto GPO se utiliza para aplicar los parámetros que permitirán a IPAM recopilar información desde los controladores de dominio administrados. Despliega IPAM, crea tareas planificadas y agrega las reglas de cortafuegos de tráfico entrante para la administración remota del registro de eventos (RPC-EMAP y RPC) y la gestión de servicios remotos (RPC-EMAP y RPC).

Tras aplicar los objetos GPO anteriores, que nos permiten descubrir los servidores DHCP y DNS en nuestro entorno, tendremos que utilizar el siguiente comando PowerShell para crear los objetos GPO anteriores:

```
Invoke-IpamGpoProvisioning -Domain formacion.eni -GpoPrefixName
IPAM_ENI -IpamServerFqdn PAR-SVR1.formacion.eni -DelegatedGpoUser
administrador
```

Trabajos prácticos

1. Implementación de IPAM

Objetivo: implementar y configurar la funcionalidad IPAM.

Máquinas virtuales utilizadas: PAR-DC01, PAR-SRV1 y CL10-02.

Si todavía no se hubiera hecho, una **PAR-SRV1** al dominio **Formacion.eni**.

En **PAR-SRV1**, abra la consola **Administrador del servidor** y, a continuación, haga clic en **Agregar roles y características**.

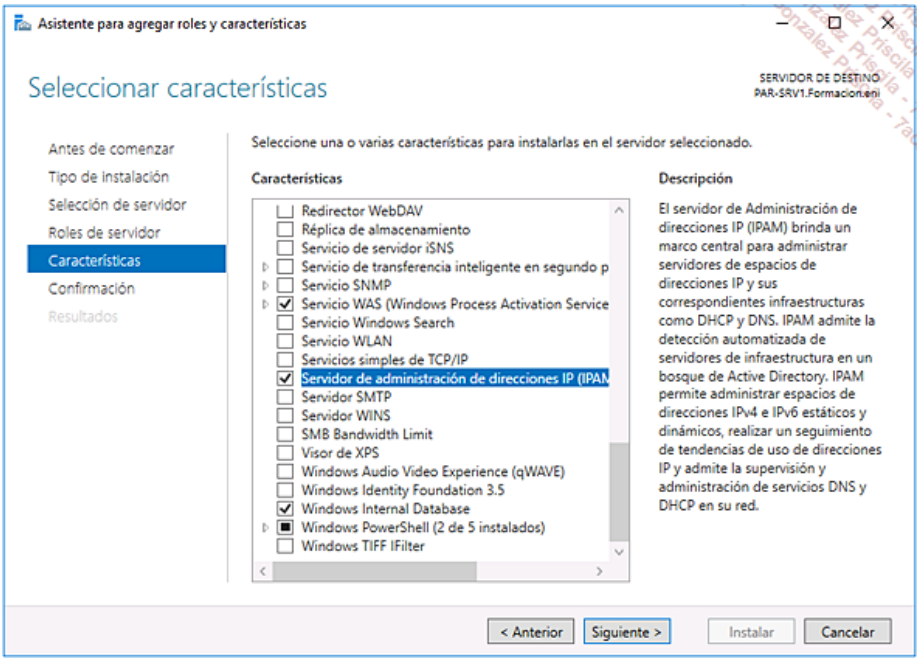
IPAM no debe instalarse en un controlador de dominio, se utiliza PAR-SRV1 para desplegar la funcionalidad.

En la ventana **Antes de comenzar**, haga clic en **Siguiente**.

Deje marcada la opción por defecto en la ventana **Seleccionar el tipo de instalación** y, a continuación, haga clic en **Siguiente**.

Compruebe que está marcado **PAR-SRV1.Formacion.eni** y haga clic en **Siguiente**.

En la ventana que permite seleccionar las características, marque la característica **Servidor de administración de direcciones IP (IPAM)**.



Haga clic en el botón **Agregar características** y, a continuación, en el botón **Siguiente**.

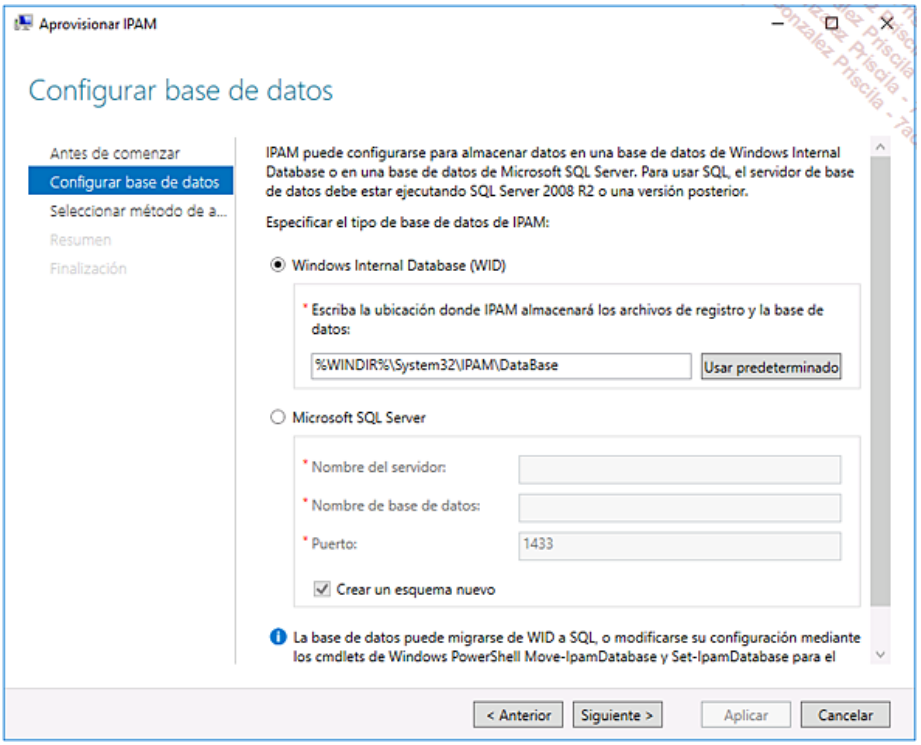
Ejecute la instalación haciendo clic en **Instalar**.

Una vez instalada la característica, acceda a **Administrador del servidor** y, a continuación, haga clic en **IPAM** para mostrar la página de presentación.

Haga clic en el vínculo **Aprovisionar el servidor IPAM**.

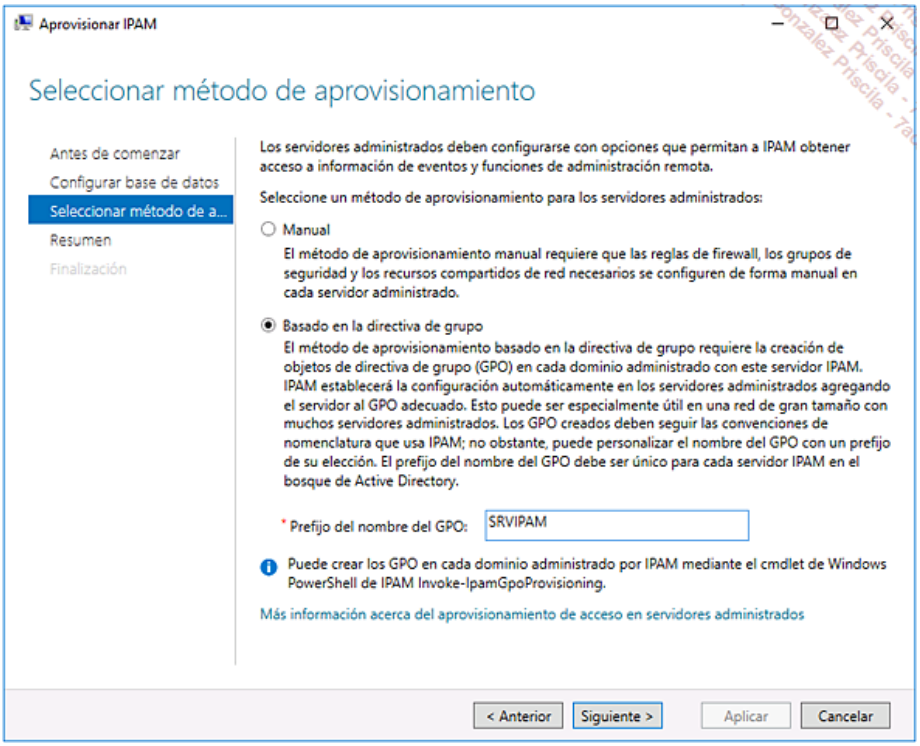
Haga clic en **Siguiente** en la ventana **Antes de comenzar**.

La elección de la base de datos se va a realizar sobre una base de datos interna. No obstante, en un entorno de producción (y en función del número de equipos), es preferible almacenar la información en una base de datos SQL.



Seleccione un método de aprovisionamiento **Basado en la directiva de grupo**.

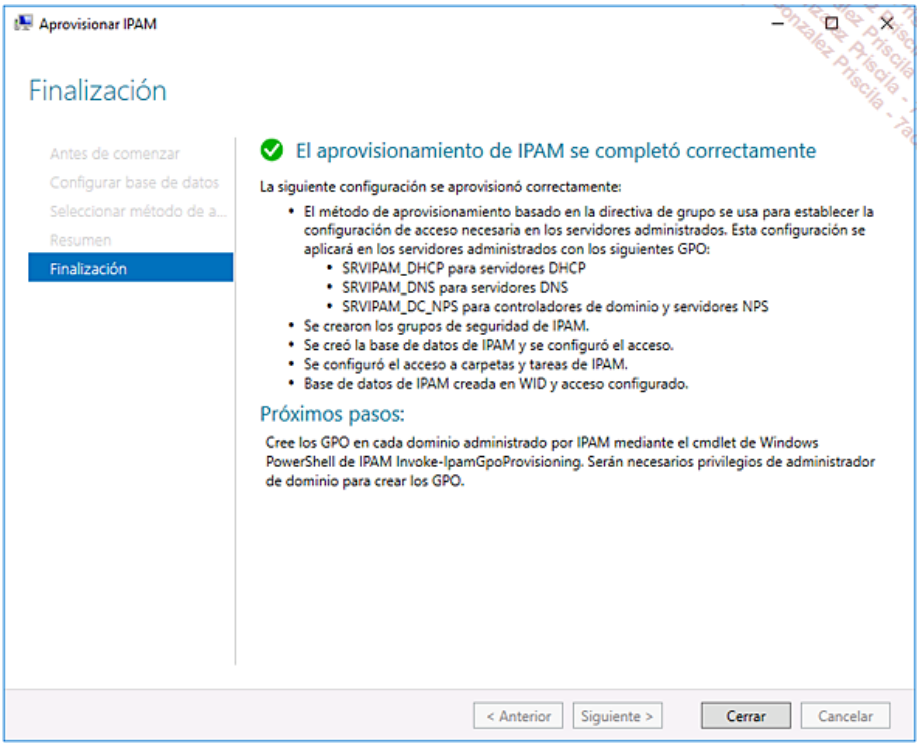
En el campo **Prefijo del nombre del GPO**, escriba **SRVIPAM** y, a continuación, valide haciendo clic en **Siguiente**.



Confirme la configuración haciendo clic en **Aplicar**.

El aprovisionamiento está en curso…

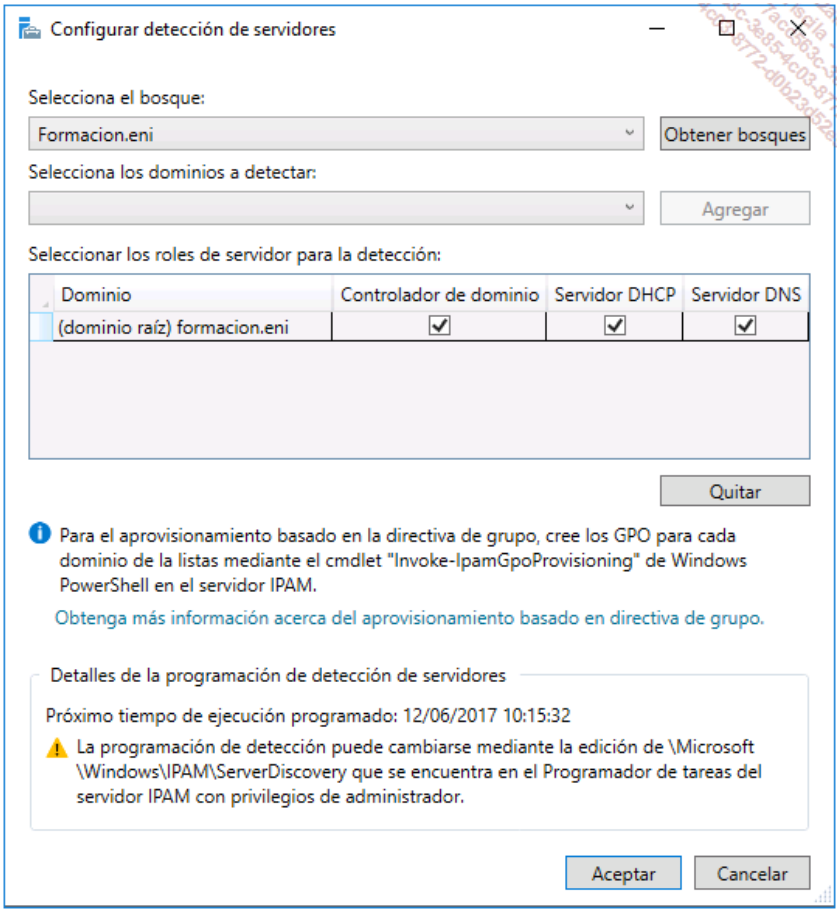
Verifique, al finalizar, la presencia de un mensaje que indica que **El aprovisionamiento de IPAM se completó correctamente** y, a continuación, haga clic en **Cerrar**.



Haga clic en **Configurar detección de servidores**.

Haga clic en **Obtener bosques** para agregar **Formacion.eni** en el ámbito.

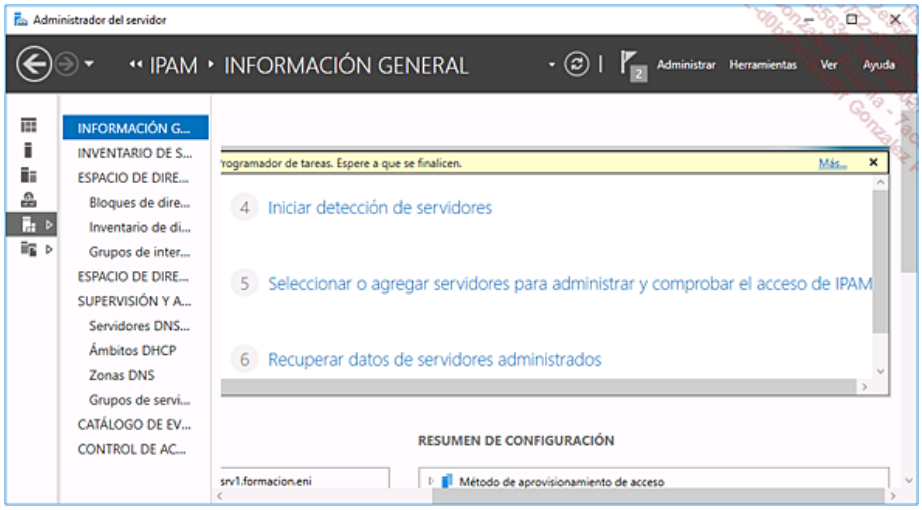
Configure los roles que quiere descubrir desmarcando aquellos que no desee.



Haga clic en **Aceptar**.

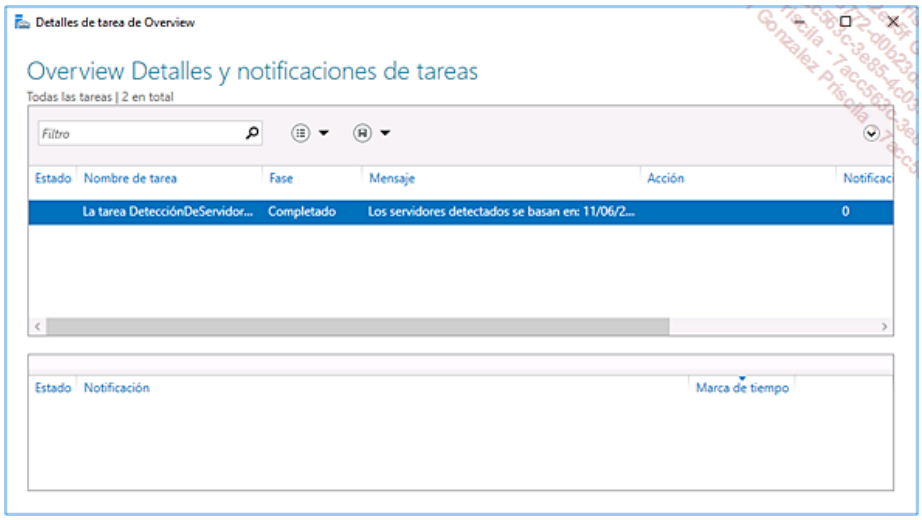
En la ventana **INFORMACIÓN GENERAL**, haga clic en **Iniciar detección de servidores**.

Haga clic en **Más** en la banda amarilla con el objetivo de obtener más detalles.



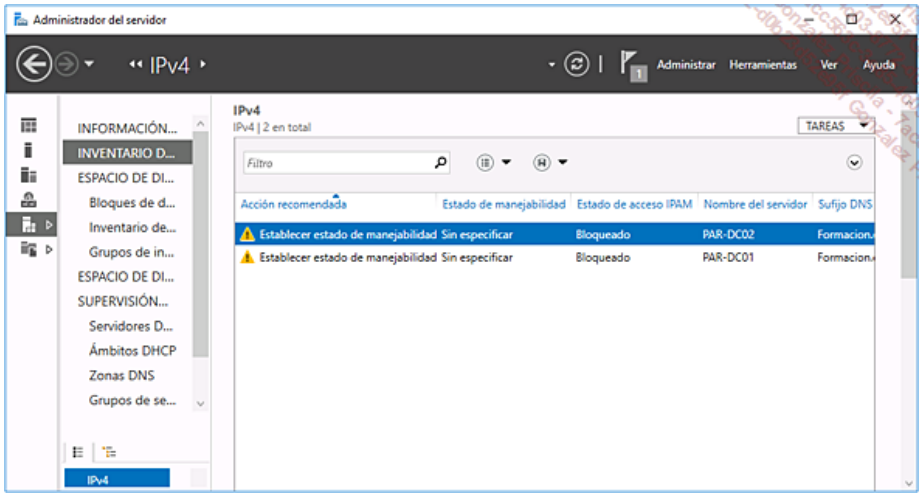
Espere a que finalice la ejecución.

Cuando el campo **Fase** tenga el valor **Completado**, cierre la ventana **Detalles de tarea**.



Haga clic en **Seleccionar o agregar servidores para administrar y comprobar el acceso de IPAM**.

El servidor o los servidores tienen el estado **Bloqueado** en **Estado de acceso IPAM** y **Sin especificar** en **Estado de manejabilidad**.



Si no se muestra ningún servidor, haga clic en **Actualizar IPv6** (junto al identificador de notificación).

A continuación es preciso otorgar a **PAR-SRV1** los permisos para administrar los distintos servidores. Se utilizan objetos de directiva de grupo para autorizar el acceso a los servidores DHCP y DNS.

Abra una consola PowerShell como administrador en **PAR-SRV1**.

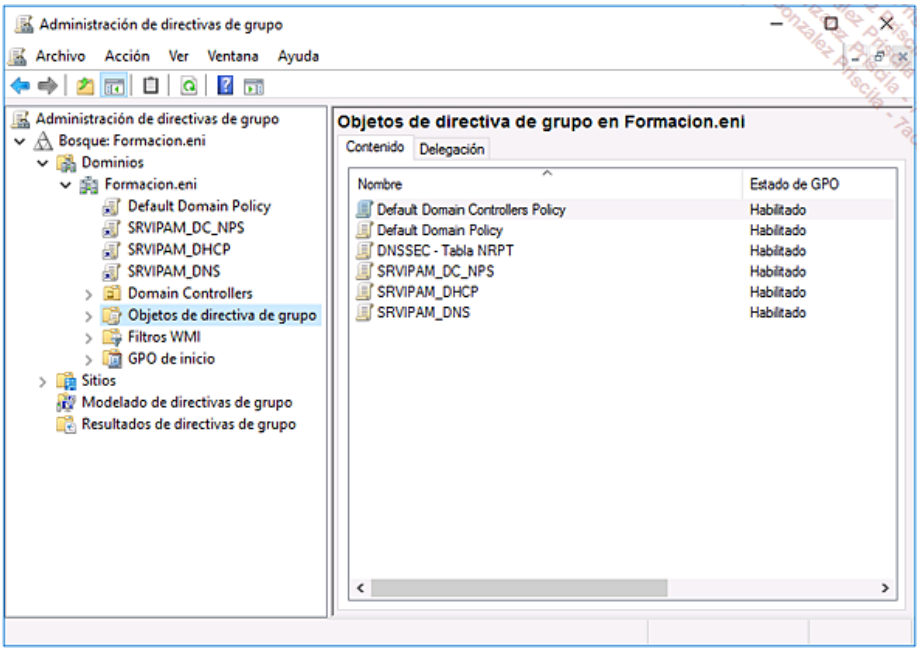
Escriba el siguiente comando y, a continuación, presione [Enter]:

```
Invoke-IpamGpoProvisioning -Domain 'Formacion.eni' -GpoPrefixName 'SRVIPAM'
-IpamServerFqdn 'par-srv1.formacion.eni' -DelegatedGpoUser
'FORMACION\Administrador'
```

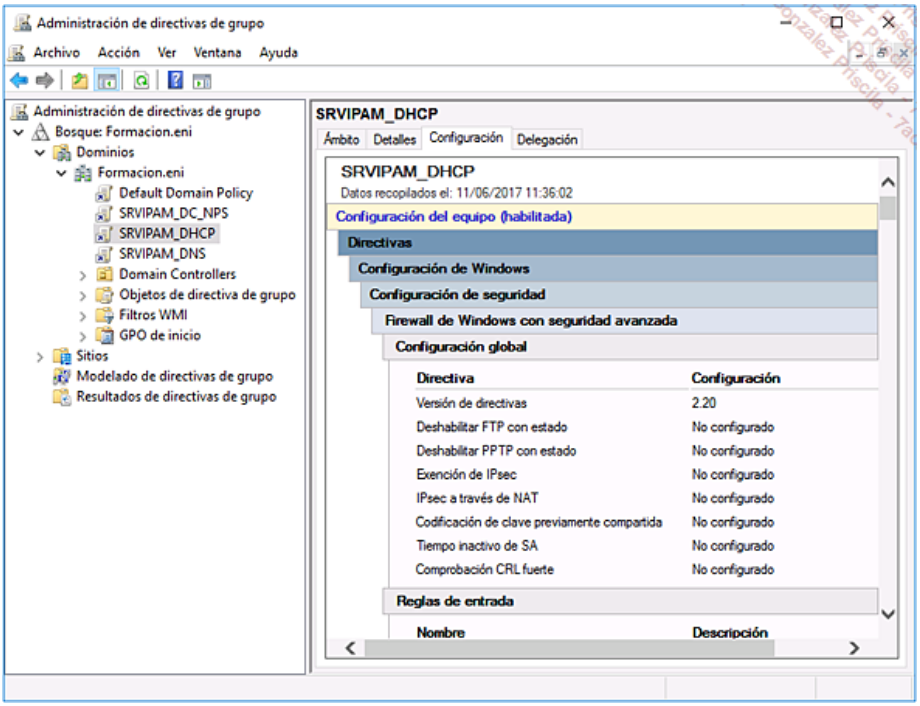
Es posible descargar el script desde la página Información.

Pulse la tecla **S** y, a continuación, valide presionando la tecla [Enter].

Aparecen nuevas directivas en la consola **Administración de directivas de grupo**.

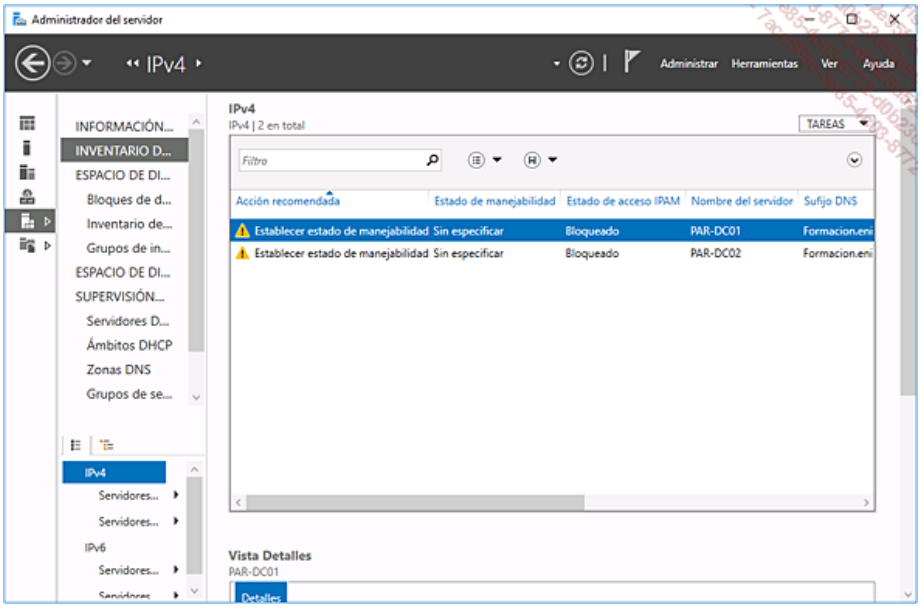


La directiva **SRVIPAM_DHCP** contiene los siguientes parámetros:

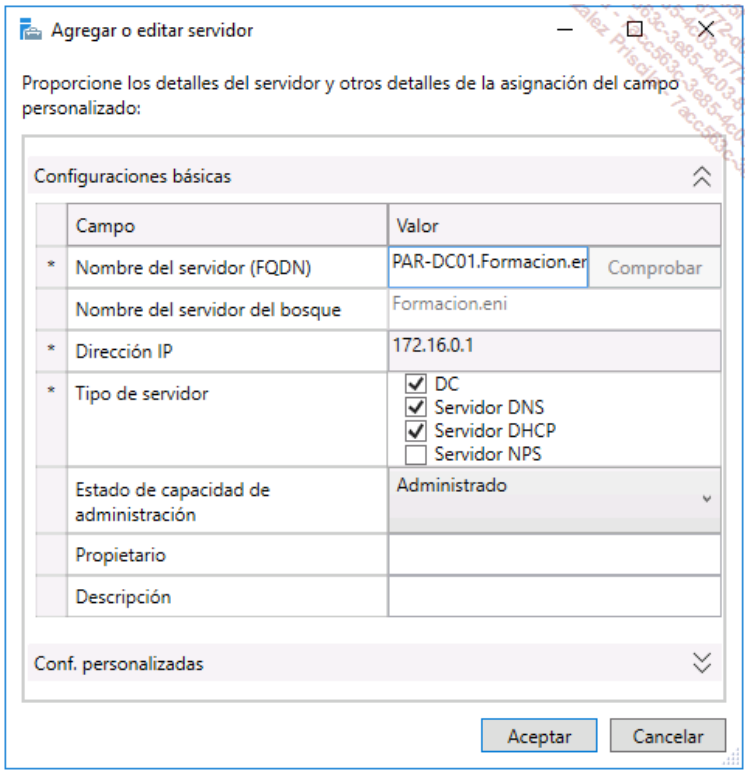


Las directivas están vinculadas, por defecto, a la raíz del dominio. Es posible moverlas si fuera necesario.

En la consola de configuración de IPAM, haga clic con el botón derecho en la fila **PAR-DC01** y, a continuación, seleccione **Editar servidor**.



Asegúrese de que la opción **DHCP** está marcada y, a continuación, en la lista desplegable **Estado de capacidad de administración**, seleccione **Administrado**.



Haga clic en **Aceptar**.

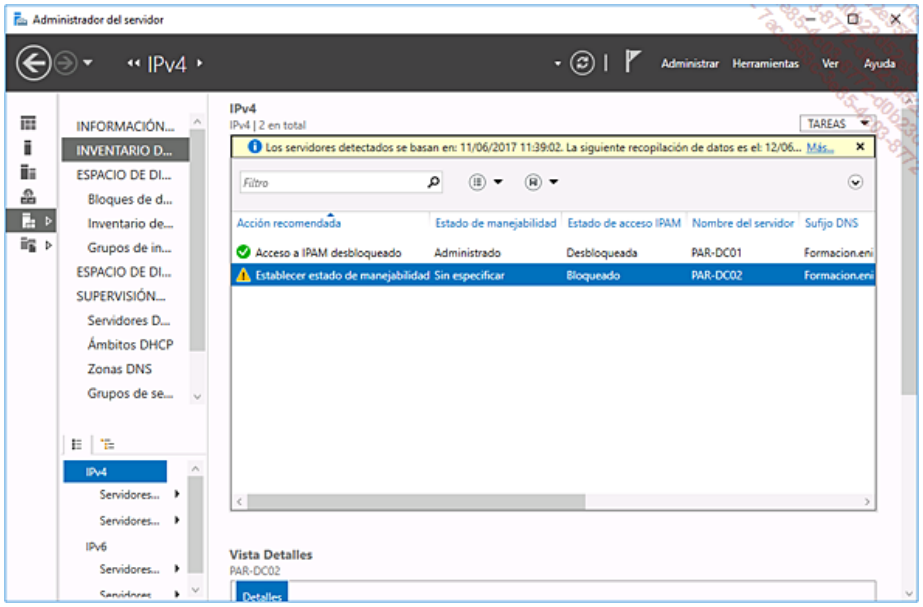
Resulta inútil reproducir estas acciones en PAR-DC02, pues el único servidor DHCP es PAR-DC01.

En el servidor **PAR-DC01**, abra una ventana de línea de comandos DOS y, a continuación, escriba el comando **`gpupdate /force`**. Esto permite aplicar las directivas de grupo creadas anteriormente utilizando el comando PowerShell.

Actualice la consola IPAM; el campo **Estado de acceso IPAM** está ahora **Desbloqueado**.

Si no fuera el caso, haga clic con el botón derecho en **PAR-DC01** y seleccione **Actualizar**.

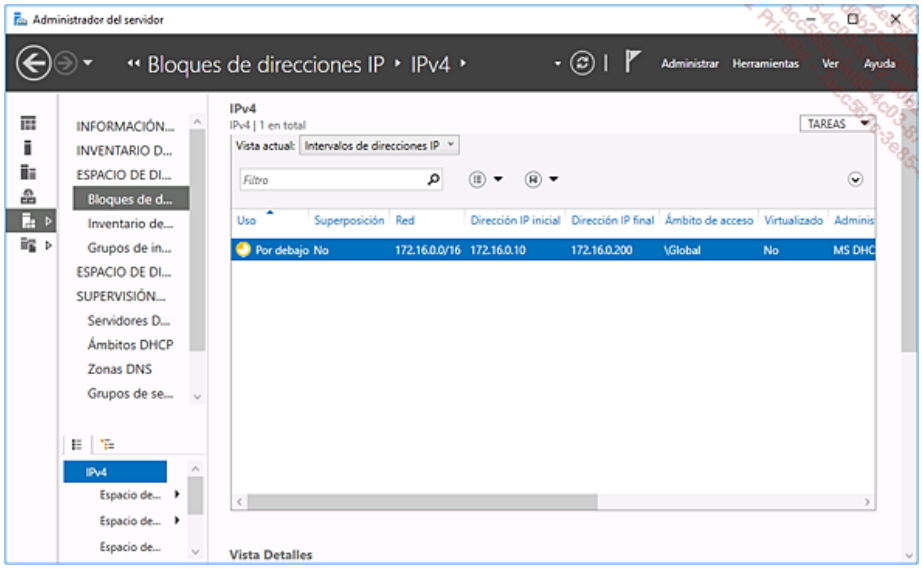
Pueden necesitarse varios minutos para aplicar la directiva.



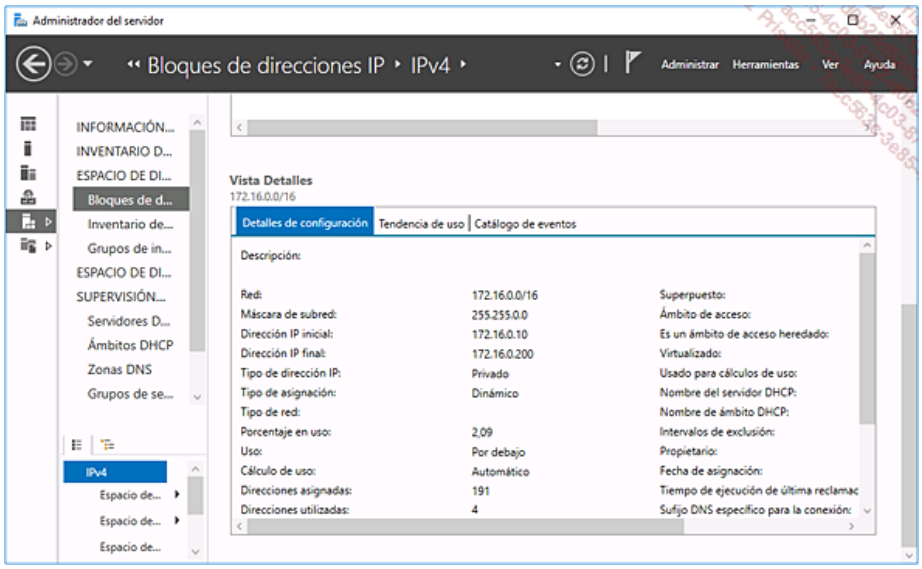
En el panel **INFORMACIÓN GENERAL**, haga clic en **Recuperar datos de servidores administrados**.

Espere a que finalice la recuperación (concesión en curso...).

En el panel de navegación IPAM, haga clic en **Bloques de direcciones IP**.



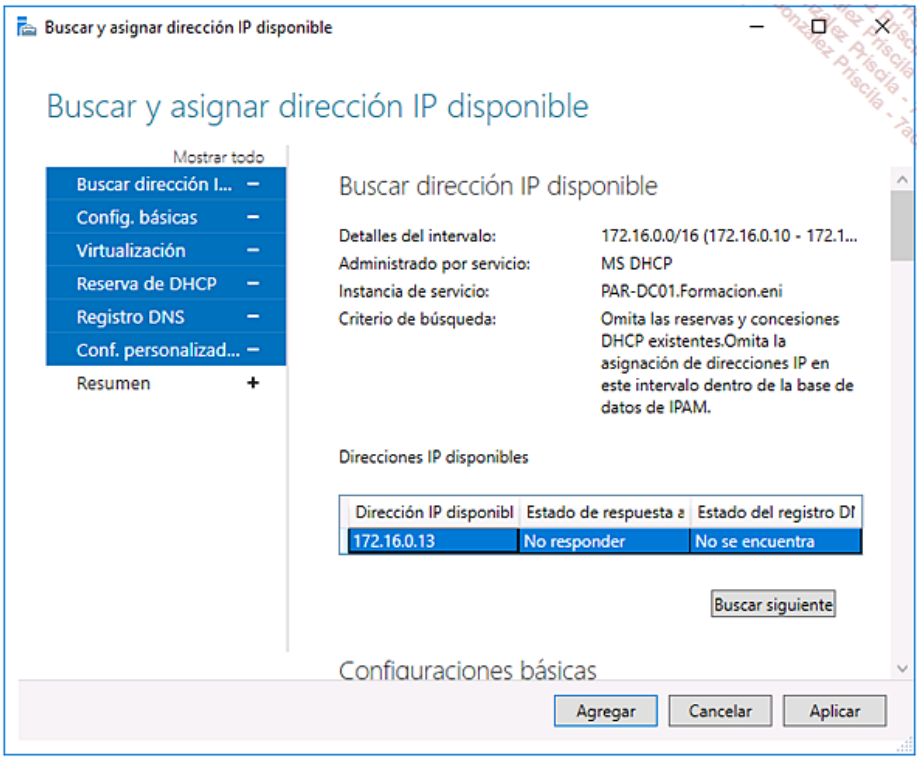
Muestre el contenido de la pestaña **Detalles de configuración**, examine la información mostrada.



La información proveniente del DHCP se recupera correctamente.

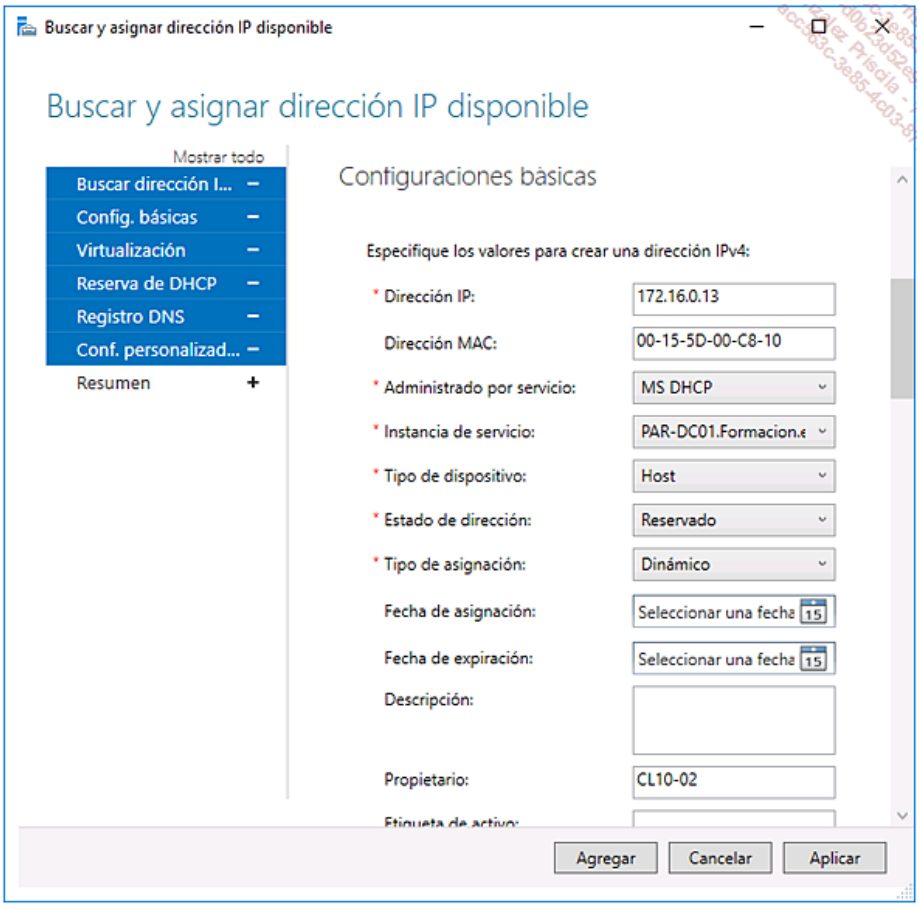
Haga clic con el botón derecho sobre el rango de direcciones IP y, a continuación, en el menú contextual, haga clic en **Buscar y asignar dirección IP disponible**...

Pasados algunos segundos, se propone una dirección IP y, a continuación, se realizan las comprobaciones.



Haga clic en la sección **Configuraciones básicas** y, a continuación, en el campo **Dirección MAC**, escriba la dirección MAC de **CL10-02**.

Seleccione **Reservado** en el campo **Estado de dirección** y, a continuación, **CL10-02** en el campo **Propietario**.

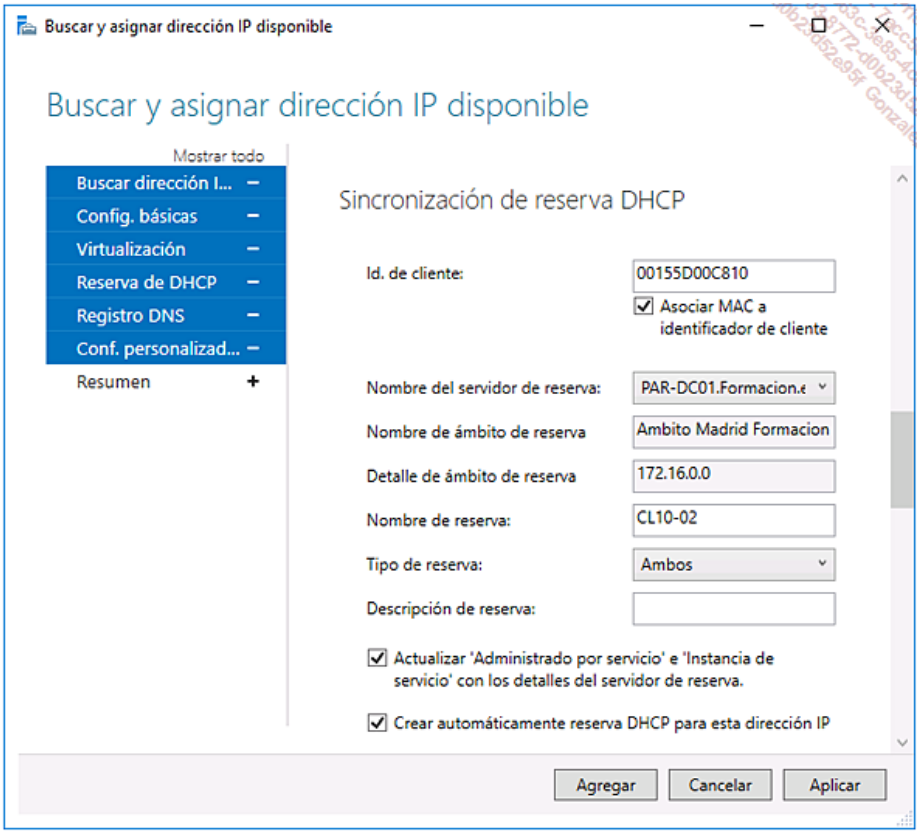


Seleccione el menú **Sincronización de reserva DHCP**.

En la lista desplegable **Nombre del servidor de reserva**, seleccione **PAR-DC01.Formacion.eni**.

Escriba **CL10-02** en el campo **Nombre de reserva** y, a continuación, **Ambos** en la lista desplegable **Tipo de reserva**.

En el campo **Id. de cliente**, marque la opción **Asociar MAC a identificador de cliente**.



En la zona **Sincronización de registro DNS**, escriba **CL10-02** en el campo **Nombre de dispositivo**.

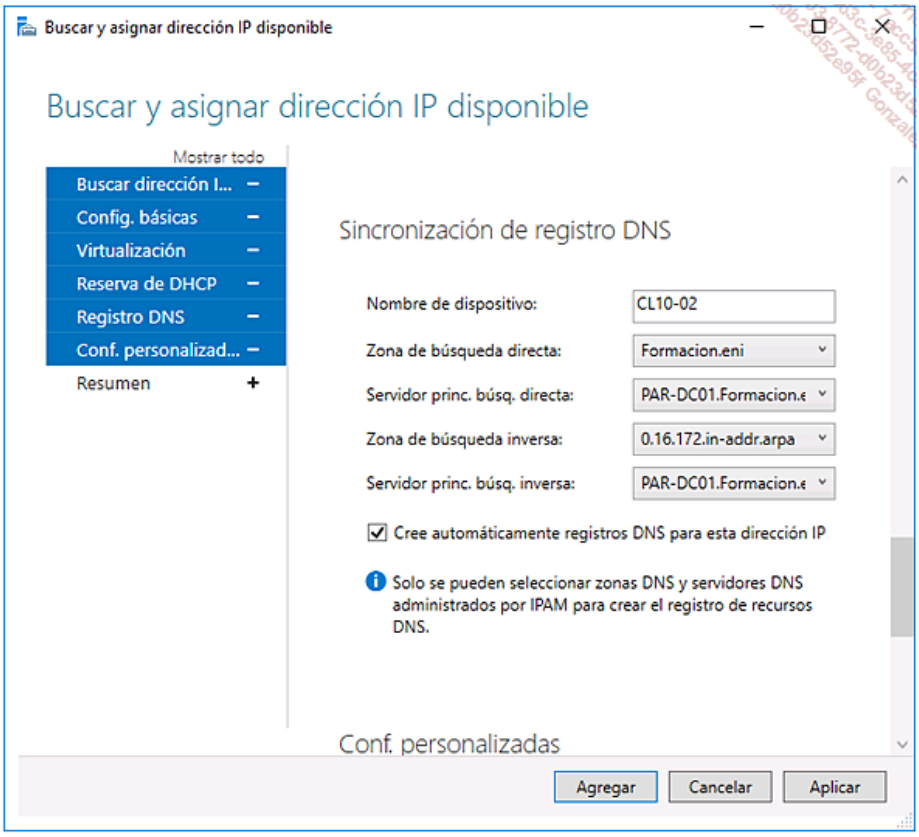
En el campo **Zona de búsqueda directa**, escriba **Formacion.eni**.

En el campo **Servidor princ. búsq. directa**, escriba **PAR-DC01.Formacion.eni**.

En el campo **Zona de búsqueda inversa**, escriba **0.16.172.in-addr.arpa**.

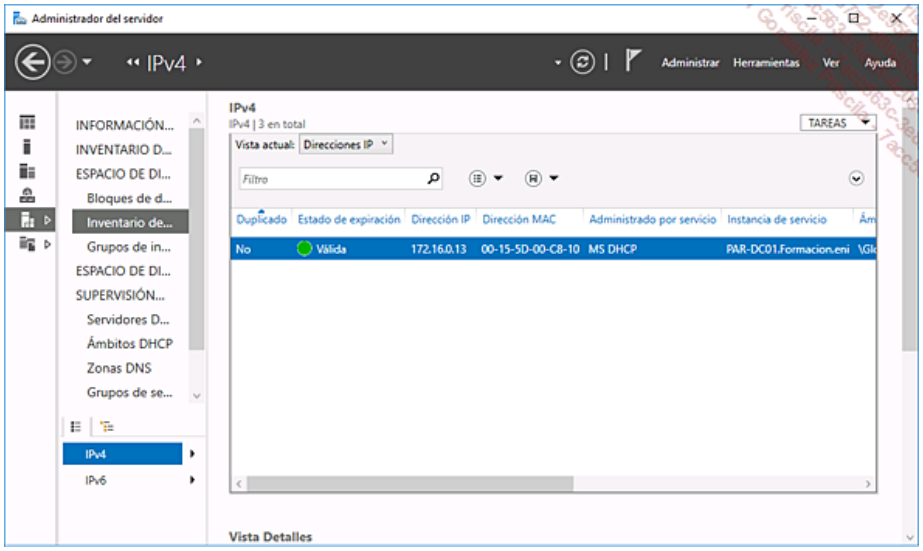
En el campo **Servidor princ. búsq. inversa**, escriba **PAR-DC01.Formacion.eni**.

Marque la opción **Cree automáticamente registros DNS para esta dirección IP**.



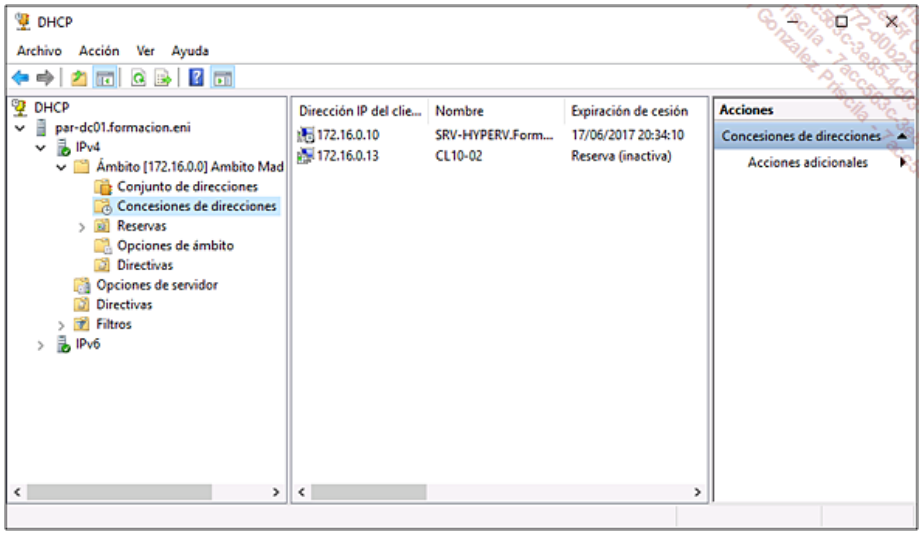
Haga clic en los botones **Aplicar** y, a continuación, **Aceptar**.

En la lista desplegable **Vista actual**, seleccione **Direcciones IP**.

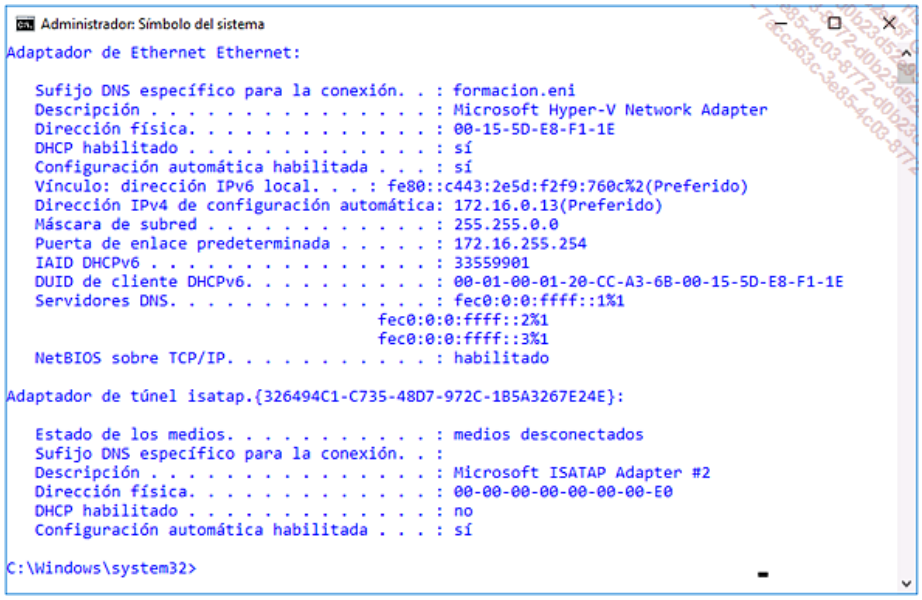


Haga clic con el botón derecho en la entrada creada anteriormente y, a continuación, seleccione la opción **Crear reserva DHCP**.

La reserva se ha creado correctamente en la consola DHCP.



En el puesto **CL10-02**, renueve el contrato DHCP ejecutando los comandos **`ipconfig /release`** y, a continuación, **`ipconfig /renew`**.



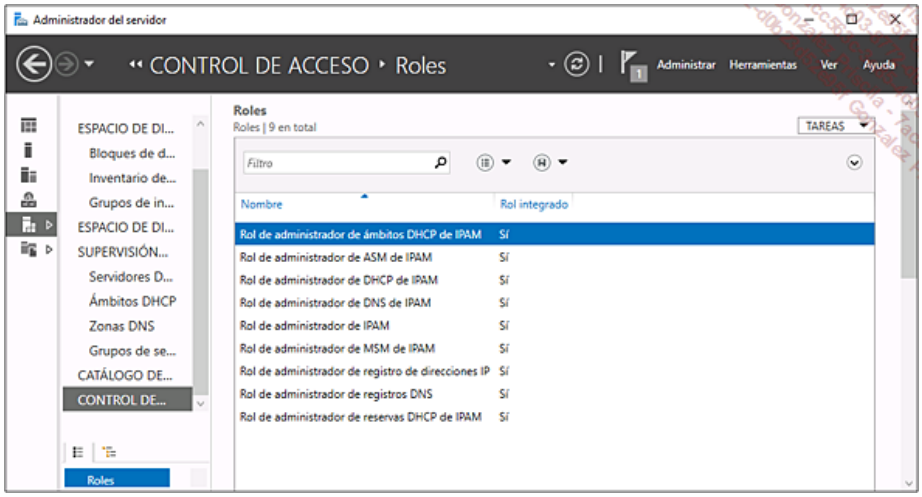
La reserva se ha tenido en cuenta.

2. Uso y administración de IPAM

Objetivo: creación de un rol personalizado y delegación de la administración para el servidor IPAM.

Máquinas virtuales utilizadas: PAR-DC01, PAR-SRV1.

En **PAR-SRV1**, abra la consola **Administrador del servidor** y, a continuación, haga clic en **IPAM** y seleccione **CONTROL DE ACCESO**.

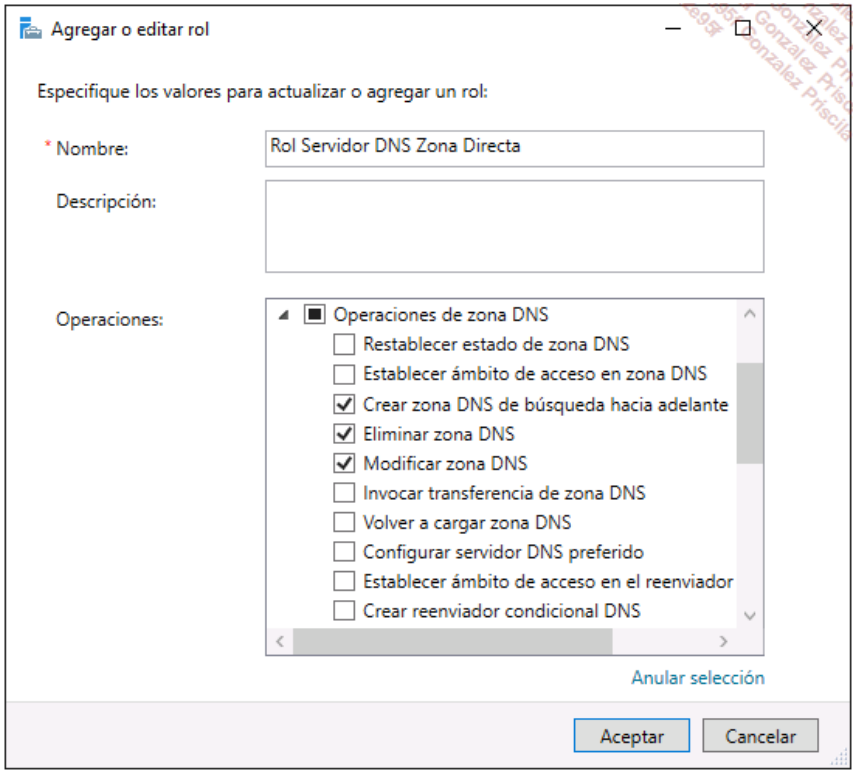


Haga clic con el botón derecho en **Roles** y **Agregar rol de Usuario**.

En el campo **Nombre**, escriba **Rol Servidor DNS Zona Directa**.

Despliegue el nodo **Operaciones de zona DNS** y marque las siguientes acciones:

- Crear zona DNS de búsqueda hacia adelante
- Eliminar zona DNS
- Modificar zona DNS



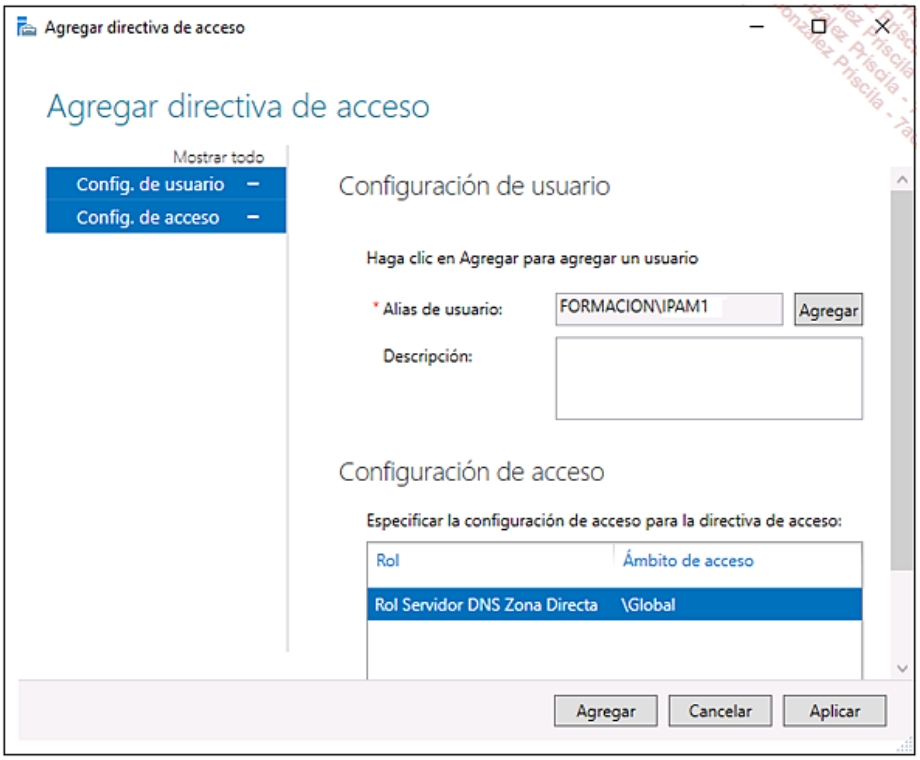
Haga clic en **Aceptar**.

Haga clic con el botón derecho en **Directiva de acceso** y **Agregar directiva de acceso**.

En el campo **Alias de usuario**, haga clic en **Agregar** y, a continuación, haga clic en **Ubicaciones** y seleccione **Todo el directorio** y en**Aceptar**.

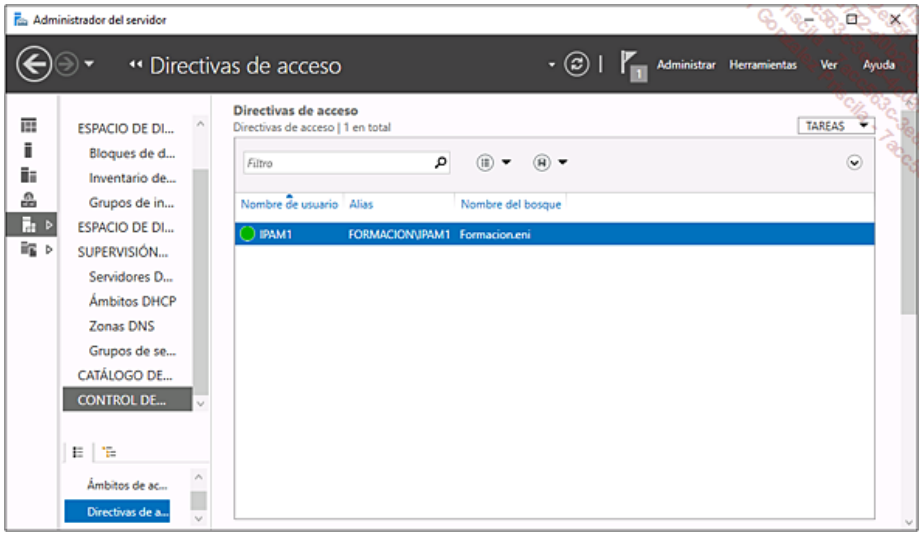
Escriba **IPAM1** y, a continuación, haga clic en **Comprobar nombres** y en **Aceptar**.

En la sección **Configuración de acceso**, haga clic en **Nuevo** y en la lista desplegable seleccione **Rol Servidor DNS Zona Directa** y haga clic en **Agregar configuración**.



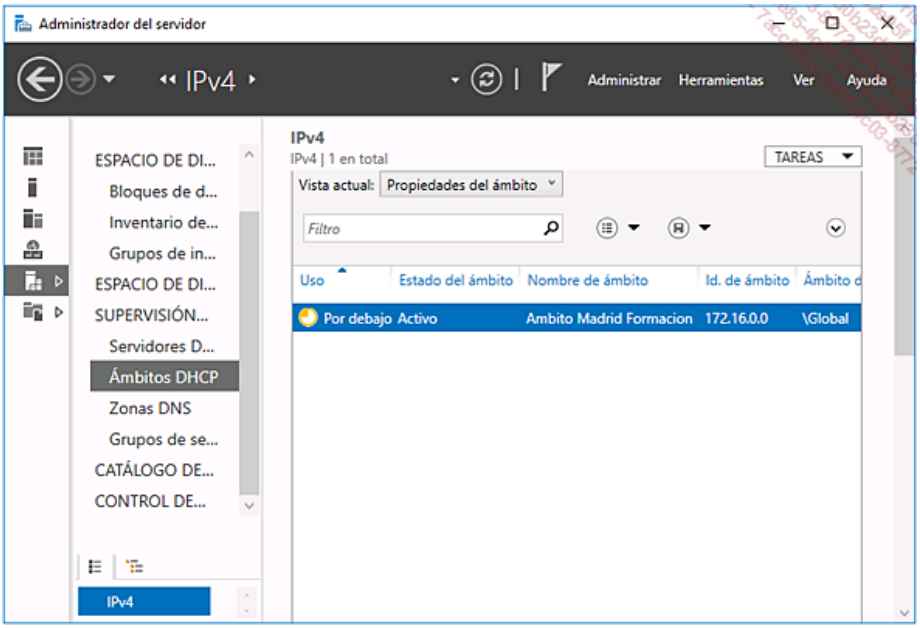
Haga clic en **Aceptar**.

La directiva de acceso para el usuario **IPAM1** del dominio **Formacion.eni** está ahora operacional.

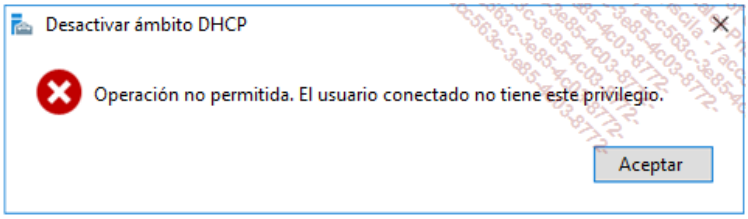


Inicie una sesión en el equipo **PAR-SRV1** con el usuario **IPAM1** y la contraseña **Pa$$w0rd**.

En **PAR-SRV1**, abra la consola **Administrador del servidor** y, a continuación, haga clic en **IPAM** y seleccione **Ámbitos DHCP**.

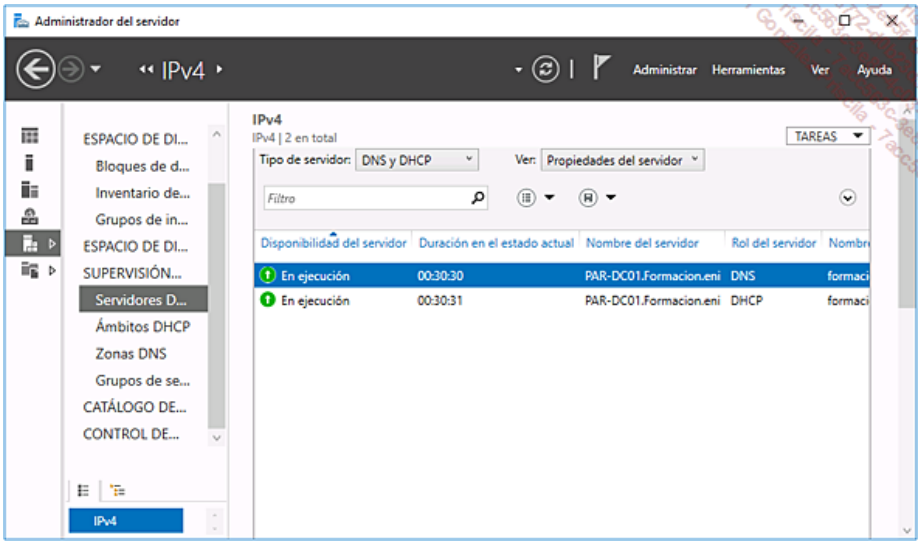


Haga clic con el botón derecho en **Por debajo** y haga clic en **Desactivar ámbito DHCP**.

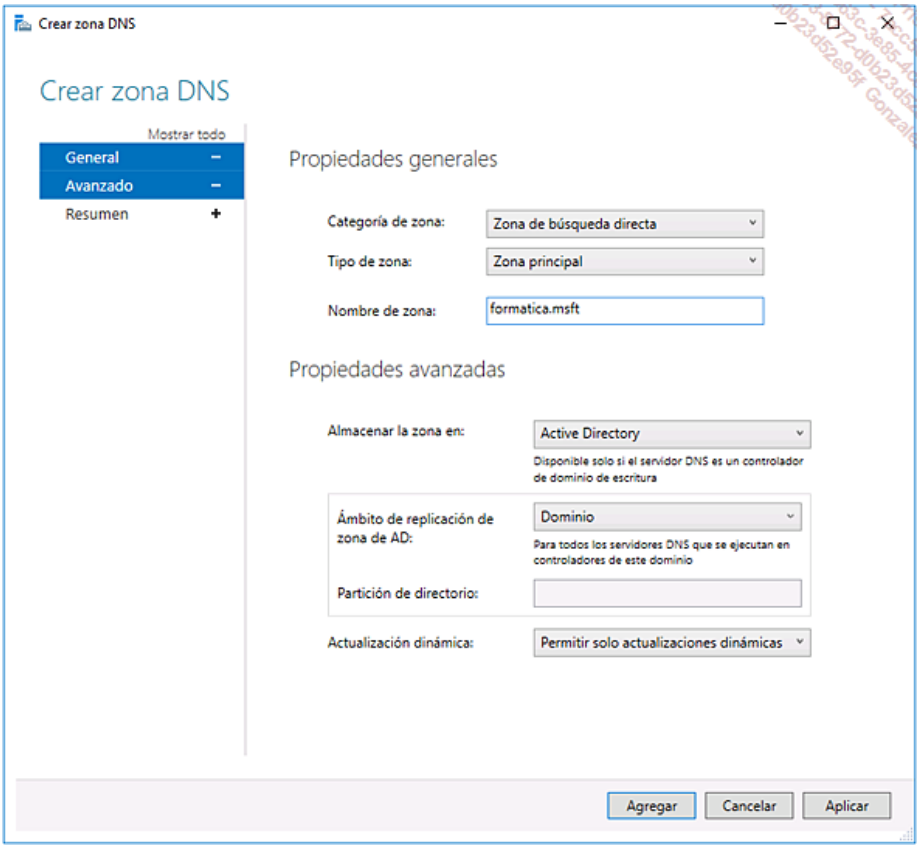


El comportamiento es normal, el usuario IPAM1 no dispone de permisos sobre los servidores DHCP.

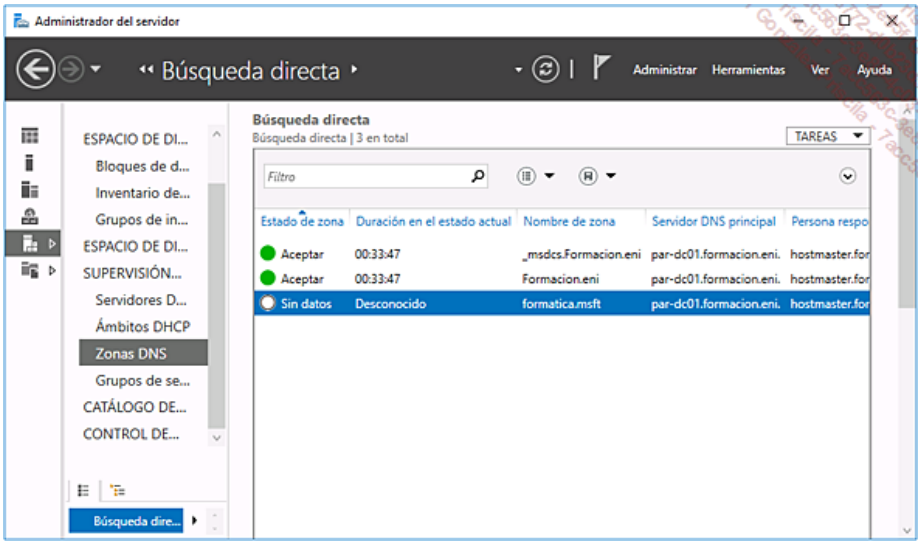
En **PAR-SRV1**, abra la consola **Administrador del servidor** y, a continuación, haga clic en **IPAM** y seleccione **Servidores DNS y DHCP**.



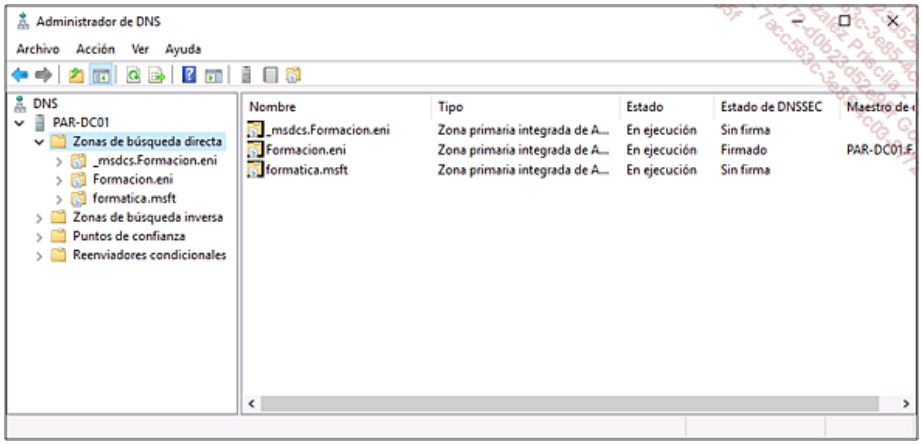
Haga clic con el botón derecho y seleccione **Crear zona DNS**; en el campo **Nombre de zona**, escriba **formatica.msft**.



Haga clic en **Aceptar**; la zona que acabamos de crear aparece en el servidor IPAM.



En **PAR-DC01**, abra la consola DNS y compruebe la existencia de la zona.



El usuario IPAM1 ha obtenido permisos para crear una zona DNS mediante el servidor IPAM.

Validación de conocimientos adquiridos: preguntas/respuestas

1. Preguntas

1 Describa brevemente la función IPAM.

2 ¿Cuáles son los métodos de aprovisionamiento de IPAM?

3 ¿Cuáles son las novedades aportadas con Windows Server 2016?

4 Cite dos grupos de seguridad que se creen automáticamente durante la instalación de IPAM.

5 ¿Cuáles son las funcionalidades de un servidor IPAM?

6 ¿Cuáles son las ventajas de la administración basada en los roles?

2. Resultados

Consulte las siguientes páginas para comprobar sus respuestas.

Por cada respuesta correcta, cuente un punto.

Número de puntos: /6

Para superar este capítulo, su puntuación mínima debería ser de 4 sobre 6.

3. Respuestas

1 Describa brevemente la función IPAM.

IPAM permite controlar los servicios de servidores que proporcionan la distribución de la configuración de la red (DHCP, NPS). También permite implementar una reserva IP, buscar una dirección disponible o crear un registro.

2 ¿Cuáles son los métodos de aprovisionamiento de IPAM?

Para realizar el aprovisionamiento de IPAM, es posible utilizar el método manual, aunque esto implica crear recursos compartidos manualmente, así como las reglas de cortafuegos sobre cada servidor que se ha de administrar. El segundo método es por directiva de grupo; durante el proceso de aprovisionamiento se utilizará un prefijo para crear directivas de grupo para configurar los servidores.

3 ¿Cuáles son las novedades aportadas con Windows Server 2016?

Las novedades aportadas por Windows Server 2016 se centran en la gestión mejorada del servicio DNS (DNSSEC) y en las mejoras en la parte de red con la gestión y el soporte de las subredes o la posibilidad de encontrar subredes libres.

4 Cite dos grupos de seguridad que se creen automáticamente durante la instalación de IPAM.

Existen 9 grupos de seguridad provisionados en el momento de la instalación de IPAM:

- *Administrador IPAM DNS*
- *Administrador IPAM MSM*
- *Administrador IPAM ASM*
- *Administrador IP Address Record*
- *Administrador IPAM*
- *Administrador IPAM DHCP*
- *Administrador de reservas IPAM DHCP*
- *Administrador de ámbito IPAM DHCP*
- *Administrador de recursos DNS*

5 ¿Cuáles son las funcionalidades de un servidor IPAM?

Un servidor IPAM permite a los administradores de una empresa supervisar y configurar de manera centralizada una infraestructura DHCP y DNS con el descubrimiento automático del espacio de direccionamiento, con la creación de informes y la posibilidad de auditar los seguimientos de las modificaciones realizadas sobre la infraestructura.

6 ¿Cuáles son las ventajas de la administración basada en los roles?

La administración basada en roles permite a los administradores realizar la delegación de la administración y, por tanto, confiar tareas de responsabilidad a otros administradores.

Requisitos previos y Objetivos

1. Requisitos previos

Poseer conocimientos acerca del protocolo VPN.

Tener nociones sobre DirectAccess.

2. Objetivos

Configuración de una infraestructura de red.

Presentación de los métodos de autenticación.

Presentación y configuración del acceso VPN.

Introducción

En nuestros días, el acceso remoto es algo habitual, y numerosas personas trabajan desde casa y se conectan a la empresa mediante una conexión VPN.

Componentes de una infraestructura de acceso de red

Una infraestructura de acceso de red contiene varios componentes. Encontramos un servidor VPN que permite crear un túnel a través de Internet. El usuario puede, de este modo, conectarse de manera remota a la red de la empresa y trabajar como si estuviera conectado a la red física. El servidor AD DS (Active Directory) garantiza la autenticación cuando algún usuario intenta conectarse de manera remota. Existe una entidad emisora de certificados (rol AD CS - *Active Directory Certificates Services*) que asegura el despliegue y gestión de los certificados necesarios para realizar la autenticación y la conexión a la red. Se requiere, a su vez, la asignación de un contrato DHCP para poder acceder a los datos, y el servidor DHCP tiene como función entregar dicho contrato cuando se acepta una conexión remota entrante.

Es posible proteger esta conexión entrante asegurando el estado de salud de los equipos (antivirus habilitado y actualizado, firewall habilitado…). Para ello, debe instalarse un servidor NAP.

1. Presentación del rol Servicios de acceso y directivas de redes

El rol Servicios de acceso y directivas de redes provee los componentes necesarios para asegurar la conectividad de red. Además de validar el estado de salud del equipo, es posible instalar un servidor RADIUS (802.1x). Éste protege la conexión VPN o Wi-Fi utilizando una autenticación basada en un certificado o una contraseña. Es necesario, para ello, utilizar clientes (componentes de red, conexión Wi-Fi…) RADIUS.

Es conveniente comprobar que se soporta esta norma antes de comprar cualquier material hardware.

El acceso remoto se gestiona mediante el rol Acceso remoto. Éste permite establecer la conexión utilizando una de las dos tecnologías siguientes:

- **Acceso VPN**: este tipo de conexión se establece a través de una red pública (Internet). Se crea un túnel entre los dos puntos asegurando una conexión segura entre ambos. Es posible, a su vez, utilizar este tipo de conexión para enlazar las distintas sedes de la empresa. Cada una permite, de este modo, acceder a los recursos de red de la otra.
- **DirectAccess**: a diferencia del acceso VPN, que requiere que el usuario establezca manualmente la conexión, DirectAccess realiza la conexión a la red de la empresa sin intervención alguna por parte del usuario. Además de la consulta de páginas de Internet, el ancho de banda utilizado no es el de la empresa sino el del usuario. Esto permite ahorrar en ancho de banda de Internet de la empresa.

Un router lógico puede, a su vez, configurarse para vincular dos redes diferentes. Esto tiene la misma función que un router hardware. Es, por tanto, posible implementar la traducción NAT (*Network Address Translation*) que permite compartir la conexión a Internet en el interior de la red utilizando un direccionamiento privado (RFC 1918).

2. Autenticación y autorización de red

En una red informática, la autenticación y la autorización son dos puntos diferentes. La autenticación consiste en verificar la información (nombre de usuario y contraseña) enviados a los servidores VPN. Este envío lo realiza un cliente, la información puede estar cifrada o no. La autorización es el hecho de autorizar una conexión entrante una vez realizada la autenticación. Es, por tanto, posible que la autenticación funcione sin que la conexión esté autorizada, en cuyo caso la conexión no se establecerá. La autorización se verifica mediante las propiedades de la cuenta de usuario y las directivas de acceso remoto. No obstante, en caso de utilizar un servidor RADIUS, éste tiene como función realizar la autenticación y la autorización.

3. Métodos de autenticación

Los métodos de autenticación se negocian, por lo general, una vez establecida la conexión. Es posible utilizar varios métodos diferentes:

- **PAP**: el protocolo PAP (*Password Authentication Protocol*) es uno de los protocolos menos seguros, puesto que utiliza contraseñas sin cifrar. Este último se utiliza si no se puede negociar ningún método seguro. Ofrece, no obstante, la ventaja de que tiene en cuenta sistemas operativos de cliente antiguos que no permiten utilizar un método más seguro.
- **CHAP** (*Challenge Handshake Authentication Protocol*): este protocolo es de tipo pregunta/respuesta. La respuesta utiliza el protocolo MD5 (protocolo de hash) para cifrar la respuesta enviada.
- **MS-CHAP v2** (*Microsoft Challenge Handshake Authentication Protocol*): este protocolo utiliza una contraseña cifrada para asegurar la autenticación.
- **EAP** (*Extensible Authentication Protocol*): el modelo de autenticación se negocia entre el cliente y el servidor (RADIUS o servidor de acceso remoto). Es posible que este protocolo utilice certificados digitales para asegurar la autenticación.

4. Visión general de la PKI

Una PKI (*Public Key Infrastructure* - infraestructura de clave pública) permite asegurar los datos o la comunicación. La solución contiene varios componentes necesarios para el funcionamiento del rol.

Una entidad emisora de certificados permite emitir y administrar un certificado digital. Éste puede asignarse a un usuario, a un equipo o a un servicio. Un certificado digital permite, como un pasaporte o un carnet de identidad, justificar la identidad de un objeto (usuario, etc.). Contiene claves necesarias para realizar la autenticación. Los modelos de certificado permiten emitir un certificado copiando las distintas propiedades del modelo. Emitido con una duración previa definida, puede resultar necesario revocar el certificado antes de su fecha de expiración. La lista de revocación permite enumerar los certificados revocados y prohibir su uso. Desde Windows Server 2008, el servicio de rol OCSP (*Online Certificate Status Protocol*) permite verificar la revocación de un certificado sin que el usuario tenga que descargar una lista completa de

revocaciones.

Existen dos tipos de entidades de certificación:

Entidad de Certificación (AC)	Ventajas	Inconvenientes
Privada	• Ofrece un mayor control sobre la gestión de los certificados • Menor coste respecto a una entidad de certificación pública • Plantillas personalizadas • Inscripción automática	• Por defecto, no están aprobados por los clientes externos (navegadores web, sistemas operativos) • Requiere una mayor administración
Pública	• Confianza por numerosos clientes externos (navegadores web, sistemas operativos) • Requiere una administración mínima	• Mayor coste respecto a una AC privada. El coste está basado por certificado • La obtención de un certificado es más lenta

Las entidades de certificación llamadas privadas entregan certificados llamados autofirmados que solo están aprobados y reconocidos por la entidad de certificación que los ha emitido.

5. Integración de DHCP con enrutamiento y acceso remoto

La integración del protocolo DHCP permite asignar un contrato DHCP tras la conexión remota. Es, no obstante, posible configurar un pool de direcciones sobre el servidor VPN para realizar la distribución de la configuración de red (el servidor DHCP deja de ser necesario para las conexiones remotas).

El servidor de acceso remoto realiza una petición de diez direcciones cuya atribución realiza un servidor DHCP. La primera dirección la utiliza el propio servidor para su interfaz mientras que las nueve restantes sirven para los clientes que se conectan.

Tras la desconexión de la sesión remota, el contrato se libera. No obstante, si se utilizan las diez direcciones, se provee otro lote de diez direcciones. Es posible asignar las opciones únicamente a los equipos que se conectan de manera remota utilizando la clase de enrutamiento y de acceso remoto (es preciso crear una directiva en el DHCP).

Configuración del acceso VPN

Una solución VPN está compuesta por un servidor y, también, por un cliente VPN. Ambos se comunican mediante un protocolo de tunneling.

1. Las conexiones VPN

En una conexión VPN los datos están cifrados para evitar que puedan ser interceptados a lo largo de su camino por la red de Internet. Para realizar el descifrado de los mismos es necesario poseer la clave de cifrado. Esto hace que sea imposible que cualquier persona que intercepte la trama sea capaz de descifrarla. Es posible establecer una conexión VPN en dos escenarios diferentes. El acceso remoto permite a los usuarios trabajar desde fuera de la empresa y acceder a los datos como si estuvieran en ella. La conexión de sitio a sitio consiste en configurar una conexión VPN entre dos routers. De este modo, dos sedes separadas geográficamente se verían enlazadas en la misma red. Como con el acceso remoto, los datos están cifrados, lo que permite asegurar la confidencialidad de los datos.

2. Protocolos utilizados para el túnel VPN

Existen varios protocolos (PPTP, L2TP o SSTP) que pueden utilizarse en la configuración del acceso remoto. El protocolo PPTP encapsula las tramas PPP en datagramas IP. A continuación, el túnel se gestiona mediante una conexión TCP (*Transmission Control Protocol*). El cifrado se realiza mediante el protocolo MPPE (*Microsoft Point-to-Point Encryption*). Las claves de cifrado se generan mediante el proceso de autenticación MS-CHAPv2 o EAP-TLS.

L2TP es una combinación de dos protocolos (PPTP y L2F). No obstante, a diferencia de PPTP, no se utiliza el cifrado MPPE, pues se reemplaza por IPsec en modo transporte. Se habla, así, de L2TP/IPsec. No obstante, es necesario que tanto el servidor como el cliente interpreten ambos protocolos. Los clientes deben ejecutar, como mínimo, Windows XP y los servidores Windows Server 2003. La encapsulación se realiza en dos capas:

- Encapsulación L2TP
- Encapsulación IPsec

Los algoritmos AES (*Advanced Encryption Standard*) o 3DES (*Triple Data Encryption Standard*) se utilizan para cifrar los mensajes L2TP. La clave de cifrado se genera mediante IKE.

SSTP es el protocolo de tunneling que aparece con Windows Server 2008. Este último presenta la ventaja de utilizar el protocolo HTTPS (puerto 443). Este puerto está, a menudo, abierto en los firewall, lo que permite al cliente poder conectarse en la mayoría de casos. Las tramas PPP se encapsulan en tramas IP. El cifrado se realiza mediante el protocolo SSL.

3. Presentación de la funcionalidad VPN Reconnect

Desde Windows Server 2008 R2, la funcionalidad VPN Reconnect permite asegurar que la conexión se restablece si hubiera sido interrumpida. La reconexión se realiza automáticamente sin que el usuario tenga que realizar ninguna acción. En el caso de una conexión VPN establecida, por ejemplo, en un tren, la conexión se podría cortar cuando el tren pasara por un túnel. Una vez el tren saliese del túnel, la conexión se restablecería de manera automática sin intervención alguna por parte del usuario. En las versiones anteriores, habría sido necesario que el usuario se reconectara.

No obstante, deben cumplirse algunos requisitos previos:

- Cliente que ejecute Windows 7 como mínimo
- Servidor con Windows Server 2008, 2012 R2 o 2016
- Instalación de una solución PKI (infraestructura de clave pública)

4. Configuración del servidor

Una solución VPN necesita asegurar ciertos requisitos previos. El servidor VPN precisa dos interfaces de red. Es necesario diferenciar la interfaz conectada a la red privada de aquella conectada a la red pública. La elección se realiza en la configuración del servidor.

A continuación, es necesario indicar si la atribución de direcciones IP tras la conexión de los equipos cliente se realiza mediante un servidor DHCP o desde el pool de direcciones creado por el administrador.

La autenticación de las peticiones de conexión de los clientes VPN puede llevarse a cabo mediante un servidor RADIUS o por el servidor de acceso remoto. Esta elección se realiza en la configuración del servidor VPN.

Es posible realizar otras operaciones tales como la configuración de la funcionalidad VPN Reconnect o la definición del número de puertos VPN.

5. Presentación del kit CMAK

El kit CMAK (*Connection Manager Administration Kit*) permite crear conexiones predefinidas. Una vez ejecutado el asistente de creación del kit CMAK, se crea un archivo ejecutable. Esta herramienta puede distribuirse a continuación en los equipos cliente con el objetivo de crear las conexiones de acceso remoto en los equipos. El usuario no tiene más que ejecutar el archivo para que la conexión se cree automáticamente. Esta última está preconfigurada, de modo que el usuario no tiene que indicar el nombre del servidor…

La funcionalidad no está incluida por defecto, y es necesario instalarla antes de poder crear los perfiles.

Visión general de las políticas de seguridad

El servidor de acceso remoto determina si la conexión está autorizada o no en función de las directivas de red. Es, así, posible agregar en estas reglas restricciones de día y hora, de desconexión en caso de inactividad…

Las directivas de red son reglas que contienen un conjunto de condiciones y de parámetros que indican las personas autorizadas a conectarse. De este modo, el servidor autoriza o no la conexión en función del estado de salud del equipo que se conecta.

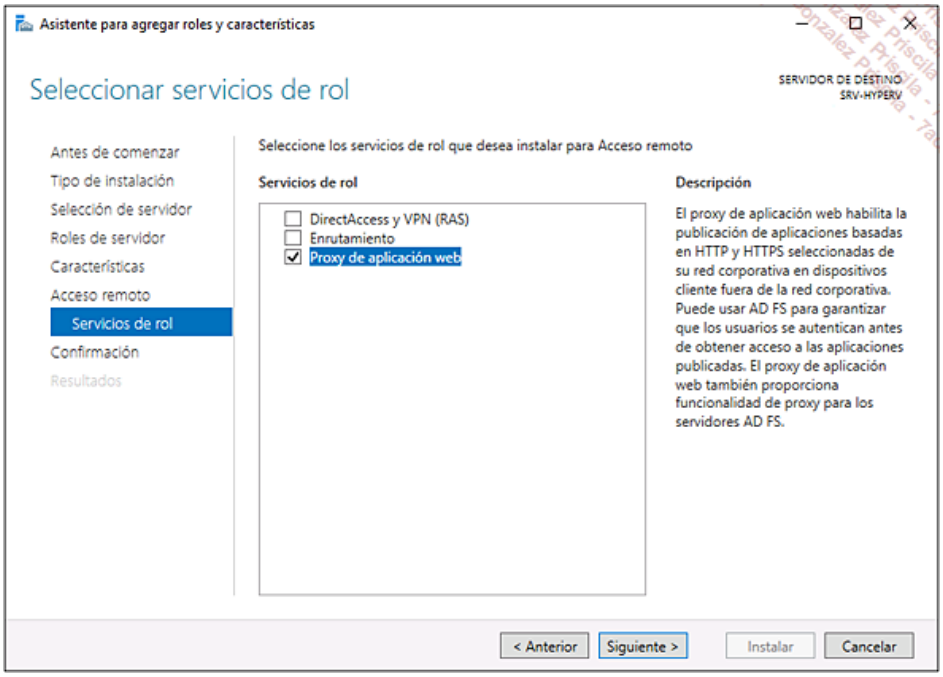
Como con un firewall, las reglas son analizadas. Cuando alguna regla se corresponde con la solicitud de conexión, se aplican los parámetros definidos. La verificación de las reglas se realiza en orden, por lo que es importante verificar la concordancia de las distintas reglas (si la regla 1 aplica, las siguientes reglas no se tendrán en cuenta).

Una regla posee varias prioridades. Éstas se dividen en cuatro categorías:

- Visión general: esta categoría permite habilitar o no la directiva así como la autorización o la denegación del acceso. Es posible configurar la regla para ignorar las propiedades de marcado de la cuenta de usuario afectada (solo se utilizan los parámetros de la directiva de red).
- Condiciones: esta categoría permite definir la condición que debe respetarse para que se esté en conformidad con la directiva de red.
- Restricciones: las restricciones permiten agregar criterios que las solicitudes de conexión deben respetar obligatoriamente. En caso contrario, la consulta se rechaza. No obstante, si las condiciones no se respetan, la solicitud de conexión se rechaza sin evaluar las directivas suplementarias.
- Opciones: tras la aceptación de la solicitud de conexión se aplican ciertos parámetros a la misma. La pestaña **Opciones** permite definir estos valores.

Presentación del Web Application Proxy y del proxy RADIUS

El Web Application Proxy es un nuevo servicio de rol de acceso remoto. Aparecido con Windows Server 2012 R2, provee un servicio de proxy inverso.



Útil para las aplicaciones web, puede utilizarse con AD FS. Este último caso aporta una seguridad suplementaria. En efecto, el riesgo de exposición en Internet de la o las aplicaciones se gestiona configurando ciertas funcionalidades de AD FS (Workplace Join, autenticación fuerte…).

Con Windows Server 2016, Microsoft ha aportado nuevas funcionalidades al Web Application Proxy:

- La capacidad de trabajar con un dominio genérico de aplicaciones se utiliza en escenarios SharePoint. Se trata de incluir un carácter genérico (*) para reemplazar un dominio específico, como, por ejemplo, para el siguiente dominio: http://*.sp-apps.ediciones-eni.com. Esta dirección de sitio Sharepoint se utiliza para la publicación externa de aplicaciones.
- La preautenticación para la publicación HTTP.
- La posibilidad de redirección HTTP hacia HTTPS.
- La publicación HTTP.
- La publicación de aplicaciones para el rol Remote Desktop Gateway.

Gracias a ello, aseguramos que únicamente aquellas personas autorizadas acceden a las aplicaciones.

Desde hace varios años es posible utilizar NPS como servidor RADIUS. Es posible, también, utilizarlo como proxy RADIUS para asegurar que se enrutan los mensajes RADIUS entre los distintos clientes RADIUS que tienen el rol de servidor de acceso y los servidores RADIUS que tienen el rol de autenticar a los usuarios.

Por ello, NPS se convierte en el punto central cuando se intenta realizar una conexión y posee el rol de proxy RADIUS.

Un proxy RADIUS puede utilizarse en varios escenarios:

- Desea proveer a sus clientes servicios de acceso remoto externalizados (VPN, por ejemplo). Los servidores de directorio están, por su parte, gestionados por los clientes. En función del nombre de dominio y del nombre de usuario informado el servidor proxy redirigirá la petición de conexión al servidor RADIUS del cliente correspondiente.
- Es preciso procesar muchas conexiones. Para evitar una sobrecarga en alguno de los servidores, conviene repartir a los usuarios sobre el conjunto de servidores. Para ello, conviene enviar las tramas al proxy RADIUS, que repartirá la carga entre los distintos servidores RADIUS.

Soporte del enrutamiento y acceso remoto

El soporte de la parte de enrutamiento es un elemento importante. En efecto, el fallo de un router o de un servidor con el rol puede provocar errores en las aplicaciones o en el trabajo del usuario. Es, por tanto, necesario asegurar el correcto funcionamiento de este rol.

1. Configuración de los logs de acceso remoto

Los logs se habilitan mediante las opciones del servidor en la consola Enrutamiento y acceso remoto. Es posible habilitar varios niveles de eventos, y es posible obtener más o menos información.

Hay cuatro niveles disponibles:

- **Sólo registrar errores**: solamente se utiliza el log del sistema, y los errores encontrados se anotan.
- **Registrar errores y advertencias**: se utiliza el log del sistema pero, a diferencia del nivel anterior, se anotan los errores y advertencias.
- **Registrar todos los eventos**: este nivel permite recuperar el máximo de información.
- **No registrar ningún evento**: no registra ninguna información en los logs.

Es posible utilizar el comando `netsh` para habilitar el seguimiento de ciertos componentes:

```
netsh ras set tracing componente enabled/disabled
```

componente debe reemplazarse por uno de los componentes presentes en la lista de componentes del servicio de enrutamiento y acceso remoto. Éste está presente en la clave HKEY_Local_machine\software\Microsoft\tracing.

2. Resolución de problemas en VPN

Cuando la conexión VPN no se establece, es necesario conocer de dónde viene el problema. En efecto, puede deberse a una configuración errónea del equipo, a la presencia de un firewall o, simplemente, a un problema a nivel de firewall.

Es, por tanto, necesario, en primer lugar, asegurar que el servidor responde, utilizando los comandos ping o tracert. A continuación, puede ser necesario asegurar la validez de la información indicada (que la cuenta de usuario esté habilitada, que la cuenta no esté bloqueada, que no exista restricción horaria…).

El problema puede, no obstante, provenir del servidor VPN, en cuyo caso el administrador debería verificar el estado del servicio de enrutamiento y la presencia de eventos relacionados en el registro.

Enrutamiento y protocolos

El servicio de enrutamiento y acceso remoto (RRAS) obtiene su nombre de los dos servicios de red principales que proporciona.

Un router es un dispositivo que gestiona el flujo de datos entre los segmentos de la red, o las subredes. Un router dirige los paquetes entrantes y salientes en función de la información acerca del estado de sus propias interfaces de red y de una lista de orígenes y de destinos posibles para el tráfico de red.

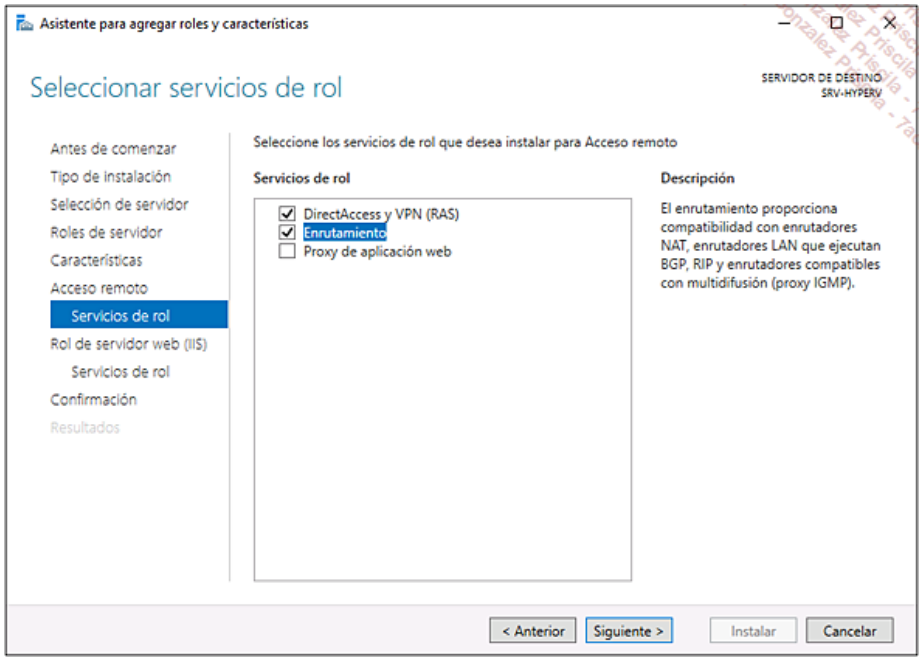
En general, los routers hardware dedicados gestionan mejor las exigencias de enrutamiento más costosas y los routers software (menos costosos) gestionan cargas de enrutamiento más ligeras.

Una solución de enrutamiento por software como RRAS, en esta versión de Windows, puede resultar ideal para una pequeña red segmentada con un tráfico relativamente bajo entre las distintas subredes. Los entornos de red corporativos con un gran número de segmentos de red y una amplia gama de restricciones de rendimiento pueden requerir diversos routers hardware que desempeñen diversos roles en el conjunto de la red.

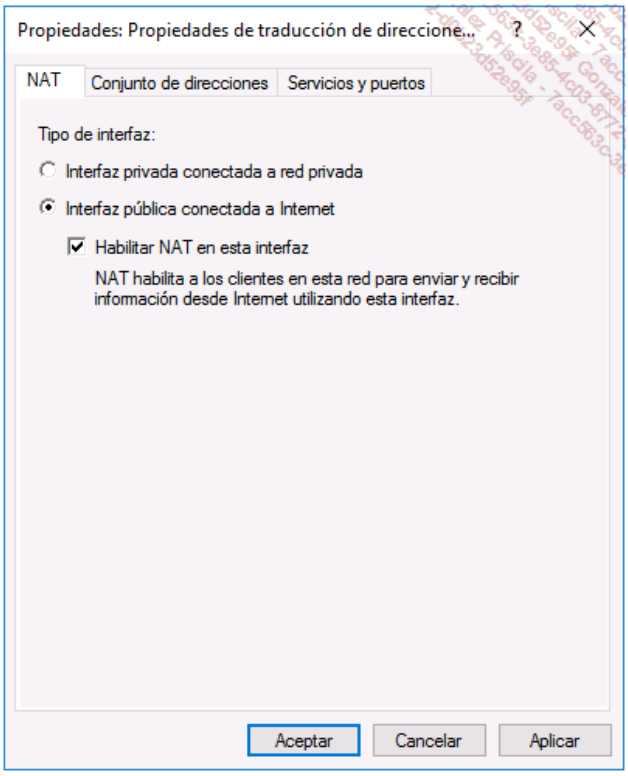
1. La traducción de direcciones NAT

La traducción de direcciones es un mecanismo que permite a las direcciones IPv4 privadas (no enrutables en Internet) acceder a Internet utilizando la dirección IP pública de la empresa. En este caso concreto, hablamos más bien de PAT, pues el router mantiene una tabla de asociación entre la dirección IPv4 interna y la dirección IPv4 pública con un número de puerto asociado. Con el direccionamiento IPv6, el protocolo NAT deja de ser necesario, pues el espacio de direccionamiento es ampliamente más importante.

Para habilitar NAT en Windows Server 2016, debe instalarse el rol de acceso remoto.



A continuación, hay que agregar las interfaces expuestas para habilitar el NAT.

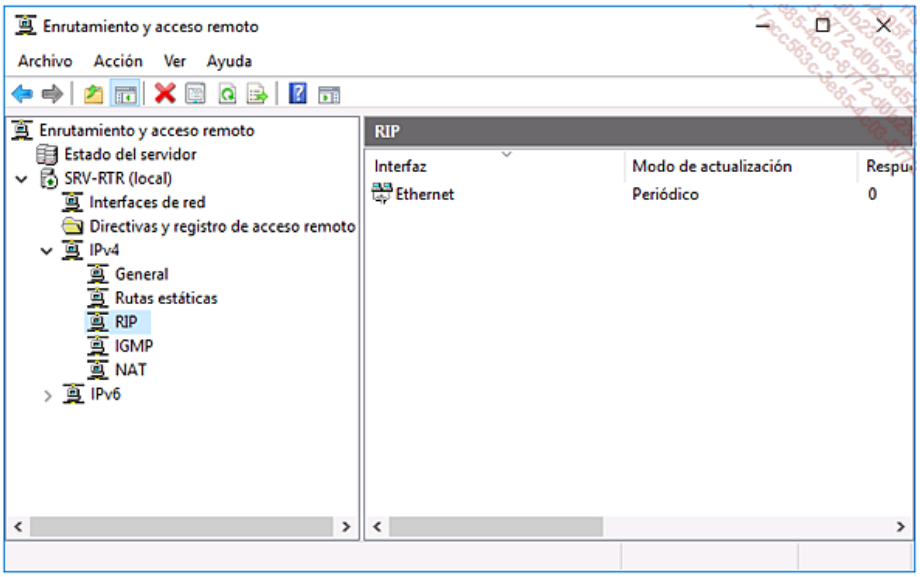


En la consola de administración del acceso remoto, es posible mostrar la tabla de mapeo entre las direcciones IP internas e IP externas.

2. Protocolo de enrutamiento RIP

Routing Information Protocol (RIP, protocolo de información de enrutamiento) es un protocolo de enrutamiento IP de tipo vector de distancias que se basa en el algoritmo de determinación de rutas descentralizadas de Bellman-Ford. Permite a cada router comunicar a los routers vecinos la métrica, es decir, la distancia que los separa de una red IP determinada en cuanto al número de saltos o "hops" (en inglés).

Para cada red IP conocida, cada router conserva la dirección del router vecino cuya métrica es menor. Estas mejores rutas se difunden cada 30 segundos. Windows Server 2016 soporta la versión 2 del protocolo RIP.



Para realizar la configuración con Windows Server 2016 en la consola de Enrutamiento y acceso remoto en el nodo IPv4 y RIP, se agregan las interfaces que se expondrán hacia los demás nodos, también configurados con RIP. Cada router RIP anuncia a sus vecinos las redes a las que está conectado.

3. El protocolo BGP

Border Gateway Protocol (BGP) es un protocolo de intercambio de enrutamiento utilizado en particular en la red Internet. Su objetivo es

intercambiar información de enrutamiento entre routers.

A diferencia de los protocolos de enrutamiento interno, BGP no utiliza una métrica clásica, sino que fundamenta sus decisiones de enrutamiento en las rutas recorridas, los atributos de los prefijos y un conjunto de reglas de selección definidas por el administrador de cada sistema autónomo.

BGP tiene en cuenta el enrutamiento sin distinción de clase y utiliza la agregación de las rutas para limitar el tamaño de la tabla de enrutamiento.

Cuando instala una pasarela RAS, debe especificar si BGP está habilitado para cada elemento mediante el comando `Enable-RemoteAccessRoutingDomain`. Para instalar el acceso remoto como router LAN con extensión BGP sin funcionalidades multitenant, puede utilizar el comando `Install-RemoteAccess – VpnTypeRoutingOnly`.

El siguiente ejemplo de código muestra cómo instalar RAS en modo multitenant con todas las funcionalidades RAS (VPN punto a sitio, VPN sitio a sitio y enrutamiento BGP) habilitados para ambos sitios, Madrid y Valencia:

```
$Madrid_RoutingDomain = "Madrid"
$Valencia_RoutingDomain = "Valencia"

Install-RemoteAccess -MultiTenancy

Enable-RemoteAccessRoutingDomain -Name $Madrid_RoutingDomain -Type All
-PassThru
Enable-RemoteAccessRoutingDomain -Name $ValenciaG_RoutingDomain -Type All
-PassThru
```

En Windows Server 2016 existen diversos escenarios en los que puede desplegarse BGP:

- Router VPN sitio a sitio con una pasarela BGP como dispositivo de cada sitio.
- Múltiples compañías conectadas por VPN sitio a sitio a un Data center cloud.
- Varios puntos de acceso distintos de pasarelas de terceros para BGP y VPN.

BGP se implementa y gestiona con Windows PowerShell en Windows Server.

Configuración de DirectAccess

Implementando DirectAccess, el administrador se aísla de problemas vinculados con una incorrecta manipulación del usuario o configuración del cliente. En efecto, éste se conecta de manera automática al servidor.

1. Presentación de DirectAccess

DirectAccess permite, a diferencia de otros tipos de servidor, evitar al usuario tener que establecer la conexión con el servidor. En efecto, ésta se establece automáticamente. Se utilizan varios protocolos, entre ellos HTTPS e IPv6. El uso del protocolo HTTPS permite atravesar con mayor facilidad los firewalls.

Implementando este tipo de servidor VPN el administrador se asegura de que los equipos remotos están actualizados, en efecto esta funcionalidad permite administrar los equipos remotos como un equipo local. Es posible configurar un acceso bidireccional que permita al equipo remoto acceder a la red local, y viceversa. Además, implementando DirectAccess, el cliente separa el tráfico de intranet hacia la empresa del tráfico de Internet. El ancho de banda de Internet de la empresa no se utiliza en los clientes conectados remotamente.

2. Componentes de DirectAccess

Una solución DirectAccess está compuesta por varios componentes, entre ellos un rol DirectAccess. Este rol puede instalarse en cualquier servidor del dominio, y tiene como objetivo proveer servicios de autenticación y funcionar como extremo del túnel IPsec.

Desde Windows Server 2012, se ha simplificado el asistente de instalación, y ya no es necesario poseer una infraestructura de clave pública (PKI) así como cuatro direcciones IPv4 públicas consecutivas. El asistente se ha visto también mejorado y permite, en lo sucesivo, seleccionar la mejor solución de despliegue.

El cliente DirectAccess es una estación de trabajo que ejecuta Windows 8 (versión Enterprise) o Windows 7 (Enterprise o Ultimate). Es preciso que la máquina sea miembro del dominio. La conexión al servidor se realiza utilizando los protocolos IPv6 e IPsec. Es posible utilizar los protocolos de transición IPv6/IPv4, si se implementan las soluciones 6to4 o Teredo. No obstante, si los protocolos de transición estuvieran bloqueados, la conexión podría establecerse utilizando los protocolos IP y HTTPS.

Se requiere un servidor de ubicación de red. Éste lo utiliza el cliente DirectAccess. En efecto, si existe la posibilidad de establecer una conexión HTTPS, el equipo está en la red local y el cliente DirectAccess se deshabilita. En caso contrario, el equipo está fuera de la red local. Este servidor se instala con el rol Servidor Web.

Debe instalarse un dominio Active Directory, cuyo nivel funcional debe ser, como mínimo, Windows Server 2003. Se utilizan directivas de grupo para desplegar las opciones de DirectAccess.

Windows Server 2012 aporta una novedad a nivel del sistema de PKI. En efecto, ya no es obligatorio, lo que simplifica la implementación y la administración de la funcionalidad. No obstante, es imposible utilizar ciertas funcionalidades tales como la protección de acceso mediante un servidor NAP (*Network Access Protection*), la autenticación de dos factores o el *tunneling* forzado.

3. La tabla de directivas de resolución de nombres

La tabla de directivas de resolución de nombres está integrada directamente en Windows Server 2012/2012 R2 y Windows 8/8.1. Consiste en separar el tráfico de Internet del tráfico de intranet. De este modo, existe una lista de reglas que contiene, por cada regla, un espacio de nombres DNS y el comportamiento del cliente DNS.

Cuando la conexión DirectAccess se encuentra activa (equipo ubicado fuera de la intranet), se comprueba el espacio de nombres en las distintas reglas. Si se encuentra alguna correspondencia, se aplican los parámetros de la regla. Si no se encuentra ninguna correspondencia, se utilizan los servidores DNS configurados en los parámetros TCP/IP.

Como hemos visto antes, el cliente DirectAccess intenta conectarse con el servidor NLS para saber si está conectado en la intranet o desde Internet. El servidor NLS se ubica en un servidor web (o en el servidor DirectAccess), y puede accederse utilizando el protocolo HTTPS. Este servidor debe estar accesible desde cualquier sitio de la empresa, pues de lo contrario el cliente DirectAccess puede presentar un comportamiento anormal (conexión del equipo mientras está ubicado en la red intranet, por ejemplo).

En caso de que el equipo se conecte a la red desde Internet, el cliente DirectAccess no recibe ninguna respuesta del servidor NLS. Utiliza, entonces, la tabla NRPT para redirigir las consultas hacia el servidor DNS adecuado.

4. Requisitos previos para la implementación de DirectAccess

La funcionalidad DirectAccess requiere que se respeten algunos requisitos previos. En primer lugar, el servidor DNS debe estar unido al dominio y ejecutar, como mínimo, el sistema operativo Windows Server 2008 R2. A diferencia de Windows Server 2008, DirectAccess ya no requiere dos direcciones IPv4 públicas consecutivas. Es posible implementar una solución de alta disponibilidad instalando y utilizando un sistema de reparto de carga (8 nodos como máximo).

Como el servidor, el cliente debe ser miembro del dominio. Es preciso asegurar, antes de implementar DirectAccess, que se tiene instalada la versión adecuada de Windows 7/8/8.1/10 (Windows 7 Enterprise o Ultimate, Windows 8 u 8.1 Enterprise, Windows 10 Enterprise o Education).

Por último, es necesario disponer de un controlador de dominio Active Directory, un servidor DNS y, para un uso completo, una infraestructura de PKI. Puede resultar necesario implementar los protocolos de transición IPv4/IPv6 adecuados.

Presentación del rol Network Policy Server

NPS permite a los administradores implementar las directivas de acceso de red (autenticación y autorización de las solicitudes de conexión). Es posible, a su vez, configurar un proxy RADIUS que asegure la transmisión de las peticiones hacia otros servidores RADIUS.

Es posible utilizar un servidor NPS como servidor RADIUS, para ello es preciso configurar los clientes RADIUS (punto de acceso Wi-Fi, switch, servidor VPN…). A continuación, es necesario implementar las distintas directivas de red útiles para realizar la autorización de las peticiones de conexión. Si el servidor es miembro del dominio, puede utilizarse AD DS para proveer la base de las cuentas de usuario. De este modo, el usuario puede utilizar su nombre de usuario y su contraseña para acceder a la red. NPS puede, a su vez, servir como servidor de directivas NAP. El servidor recupera la información de conformidad enviada por los clientes y autoriza, o no, el acceso a la red. Este acceso se autoriza si el estado de conformidad respeta las restricciones de seguridad definidas por el administrador (antivirus actualizado, etc.). El cliente NAP está integrado en los sistemas operativos desde Windows XP SP3.

Una vez realizada la instalación del rol es posible proceder a su configuración mediante la consola que se agrega durante la instalación o mediante el comando `netsh`. Es, también, posible utilizar cmdlets de PowerShell.

Configuración del servidor RADIUS

RADIUS es un protocolo que permite realizar la autenticación y la autorización con el objetivo de autorizar o no un acceso a la red.

1. Nociones acerca del cliente RADIUS

Un cliente RADIUS se considera como tal cuando envía peticiones de conexión a un servidor con el rol servidor RADIUS. De este modo, los distintos dispositivos de acceso a la red (puntos de acceso Wi-Fi, switches…) compatibles con la norma 802.1x están considerados como servidores RADIUS.

2. Directiva de solicitud de conexión

Una directiva de solicitud de conexión es un conjunto de condiciones y de parámetros que permiten designar un servidor RADIUS responsable de la autenticación y de la autorización. Una directiva está compuesta por una condición, la cual comprende uno o varios atributos RADIUS. En el caso de que existan varias condiciones, es necesario que todas se respeten para que la directiva pueda aplicarse. El servidor NPS procede a escuchar el tráfico RADIUS a través de los puertos 1812, 1813, 1645 y 1646.

Las RFC 2865 y 2866 normalizan los puertos 1812 y 1813 para realizar la autenticación (el primero) y la gestión de cuentas (el segundo).

Método de autenticación NPS

Antes de autorizar o rechazar el acceso, el servidor NPS autentica y autoriza la solicitud de conexión. La autenticación permite asegurar la identificación de un usuario o un equipo que intenta conectarse a la red. Esta identificación se aprueba mediante la información de identificación proporcionada (contraseña, certificado digital…).

1. Configurar las plantillas NPS

Es posible utilizar plantillas NPS para elaborar elementos de configuración (RADIUS, clave compartida…). Estos últimos pueden utilizarse a nivel del rol NPS o exportarse a otro servidor.

La gestión de estas plantillas se realiza mediante la consola NPS. Es posible agregar, eliminar, modificar o duplicar las distintas plantillas. El objetivo de esta funcionalidad es crear plantillas que permitan reducir el tiempo de administración de los distintos servidores NPS de una empresa.

Están disponibles las siguientes plantillas:

- **Claves compartidas**: permite especificar una clave compartida que se reutilizará en uno o varios servidores RADIUS.
- **Cliente RADIUS**: define la configuración del cliente RADIUS que debe utilizarse.
- **Servidor RADIUS remoto**: ofrece la posibilidad al administrador de configurar los parámetros de servidores RADIUS.
- **Política de conformidad**: indica los parámetros de directiva de conformidad a utilizar.

2. Autenticación

La autenticación basada en una contraseña no se considera como la más segura. Es preferible implementar una autenticación basada en certificados digitales. El servidor NPS acepta varios métodos de autenticación. Es posible utilizar, de este modo, varios protocolos.

MS-CHAP Versión 2

El protocolo MS-CHAP Versión 2 consiste en una autenticación mutua cifrada mediante una contraseña cifrada de sentido único. Está compuesta por un servidor responsable de realizar la autenticación así como un cliente. La versión 1 o MS-CHAP utiliza, por su parte, contraseñas irreversibles y cifradas. Es preferible utilizar MS-CHAPv2.

CHAP

CHAP (*Challenge Handshake Authentication Protocol*) es un protocolo que utiliza el esquema de codificación MD5 (*Message Digest 5*) para realizar el cifrado de la respuesta. Este protocolo lo utiliza un servidor con el rol de Servicio de enrutamiento y acceso remoto. La contraseña es de tipo cifrado irreversible. No obstante, este protocolo posee el inconveniente de que no permite al usuario modificar su contraseña si expira durante el proceso de autenticación.

PAP

Este protocolo se considera como el menos seguro puesto que utiliza contraseñas sin cifrar. Se utiliza, por lo general, si el cliente y el servidor no pueden comunicarse por ningún otro método de autenticación más seguro. No se recomienda utilizar este protocolo pues un análisis de las tramas intercambiadas permite obtener la contraseña.

Un certificado digital es como un "carnet de identidad" virtual, que entrega la entidad emisora de certificados y permite asegurar la autenticación. Implementándolo con el servidor NPS, es posible autenticar una cuenta de usuario o un equipo y, por tanto, evitar el uso de contraseñas. Se utilizan, para ello, los protocolos PEAP y EAP-TLS para permitir a NPS realizar una autenticación basada en un servidor. El uso del protocolo EAP-TLS permite al cliente y al servidor autenticarse mutuamente, hablamos por tanto de autenticación mutua.

Supervisión y mantenimiento del rol NPS

En ciertos casos puede resultar útil analizar el servidor NPS. Para ello es necesario configurar el registro de eventos. La información que ofrecen estos registros de eventos puede resultar útil para analizar un problema de conexión, o para realizar una auditoría de seguridad.

El análisis puede realizarse de dos formas, utilizando el registro de eventos o registrando las peticiones de autenticación y las cuentas utilizadas. Con el primer método, los registros se almacenan en los registros de sistema y de seguridad. Permite realizar una auditoría de las conexiones y, por tanto, resolver problemas más fácilmente.

El segundo método consiste, por su parte, en registrar las solicitudes de autenticación en archivos de texto o en una base de datos. Este método permite realizar un análisis de las conexiones y su facturación. La base de datos puede, evidentemente, alojarse en un servidor remoto o de manera local.

Trabajos prácticos: Configuración del acceso remoto

Estos trabajos prácticos permiten configurar un acceso VPN y, a continuación, implementar la funcionalidad DirectAccess.

1. Configuración de un servidor VPN

Objetivo: instalación y configuración del servidor VPN.

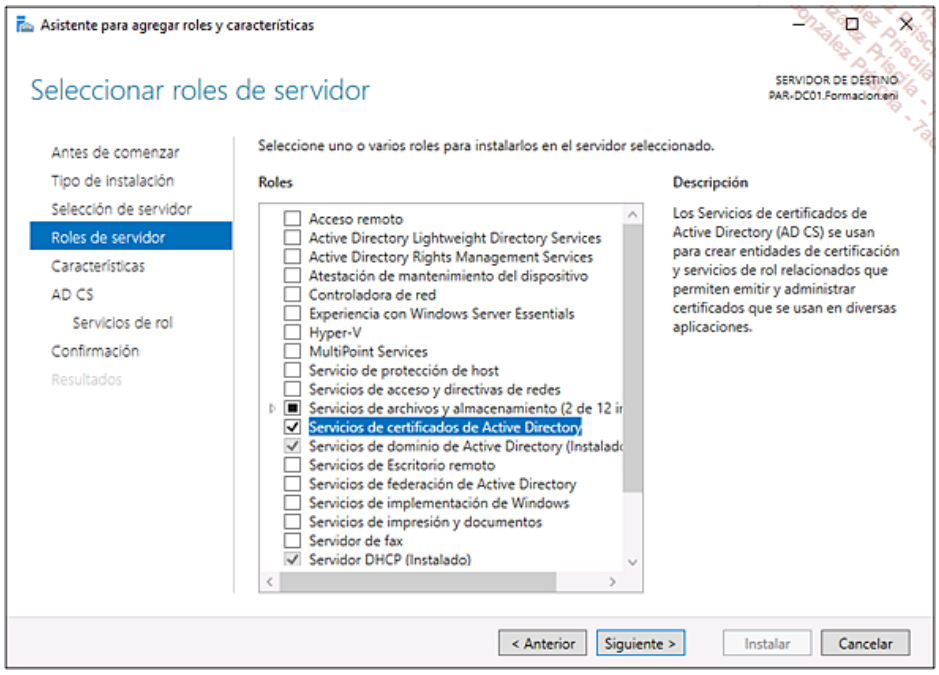
Máquinas virtuales: PAR-DC01, SRV-RTR y CL10-02.

En **PAR-DC01**, abra la consola **Administrador del servidor**.

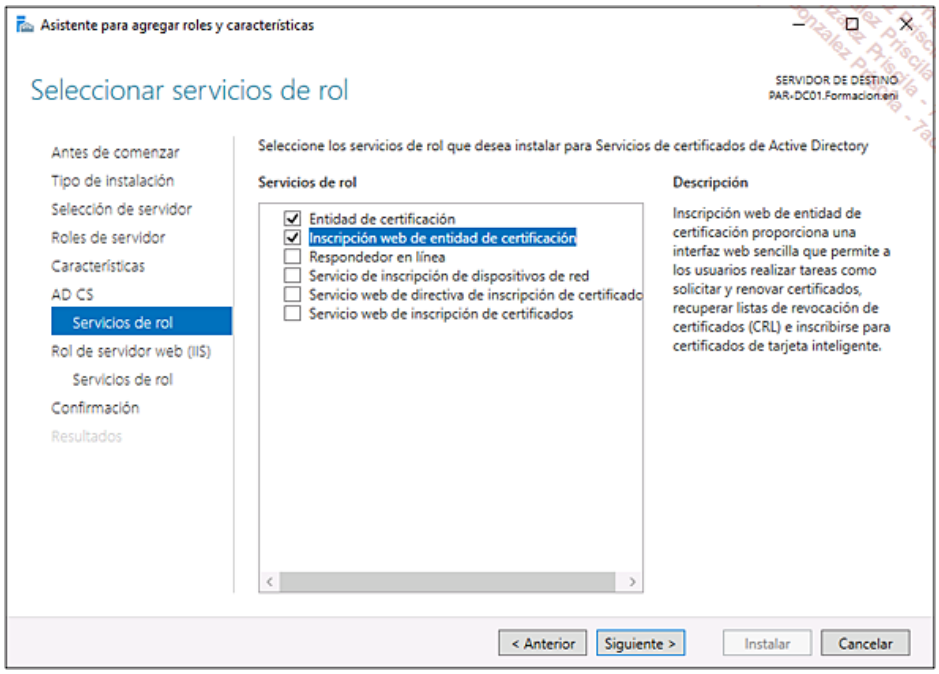
Haga clic en **Agregar roles y características** y, a continuación, haga clic en **Siguiente** en la ventana **Antes de comenzar**.

En la ventana **Seleccionar tipo de instalación**, deje la opción por defecto y, a continuación, haga clic dos veces en **Siguiente**.

Marque la opción **Servicios de certificados de Active Directory** y, a continuación, haga clic en el botón **Agregar características** en la ventana que se muestra.

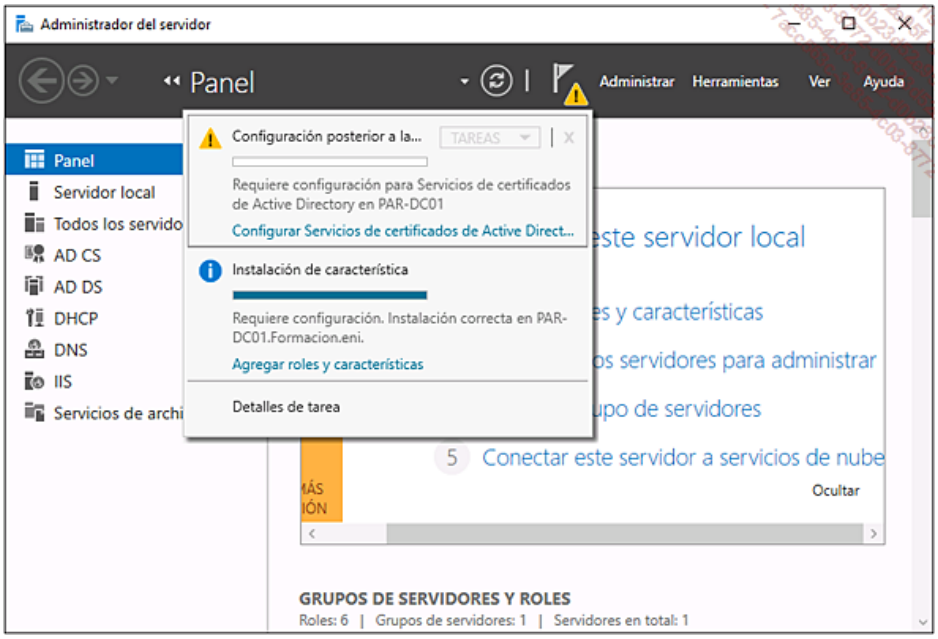


Haga clic tres veces en **Siguiente** y, a continuación, en la ventana **Servicios de rol**, marque la opción **Inscripción web de entidad de certificación**.

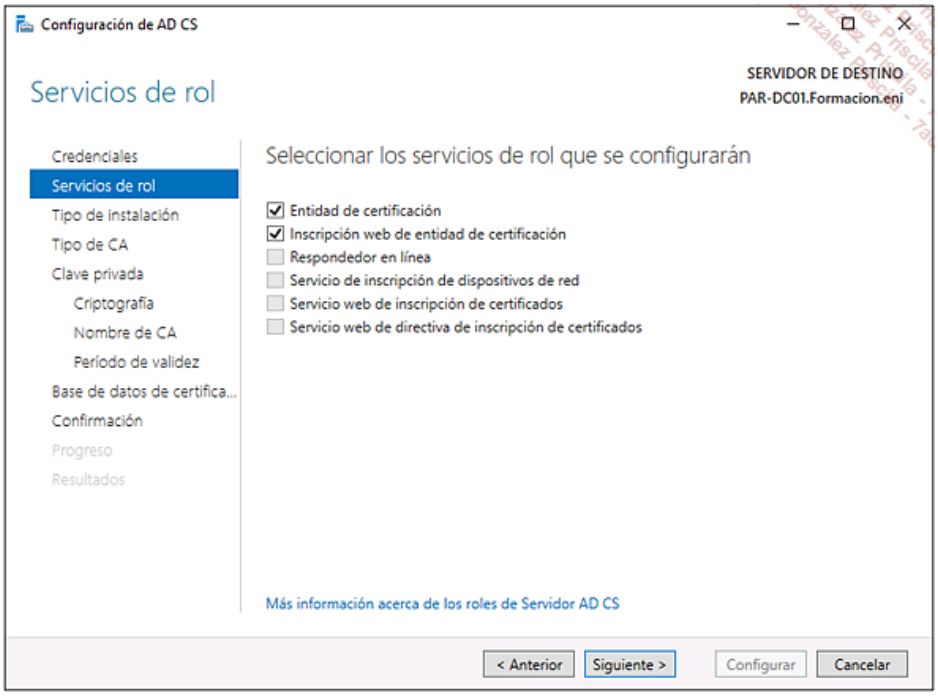


Valide la selección haciendo clic tres veces en **Siguiente**, y, a continuación, ejecute la instalación mediante el botón **Instalar**.

Haga clic en **Cerrar** y, a continuación, en la consola **Administrador del servidor**, haga clic en **Notificaciones** y, a continuación, en**Configurar Servicios de certificados de Active Directory**.

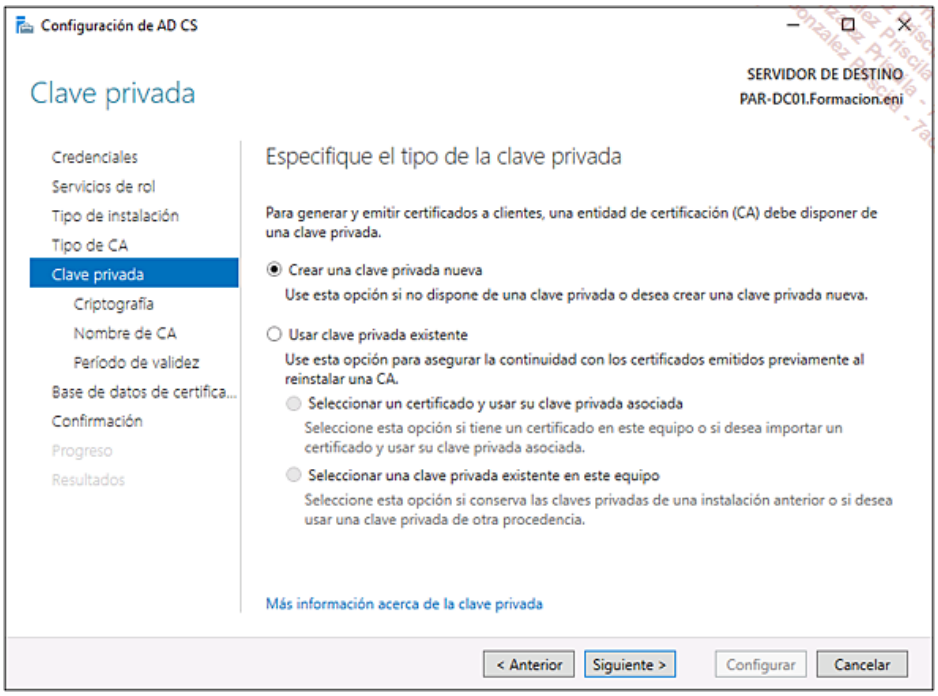


Haga clic en **Siguiente** en la ventana **Credenciales** y, a continuación, marque los dos servicios de rol.



En las ventanas **Tipo de instalación** y **Tipo de CA**, deje la opción por defecto (**CA empresarial**, **CA raíz**) y, a continuación, haga clic en**Siguiente**.

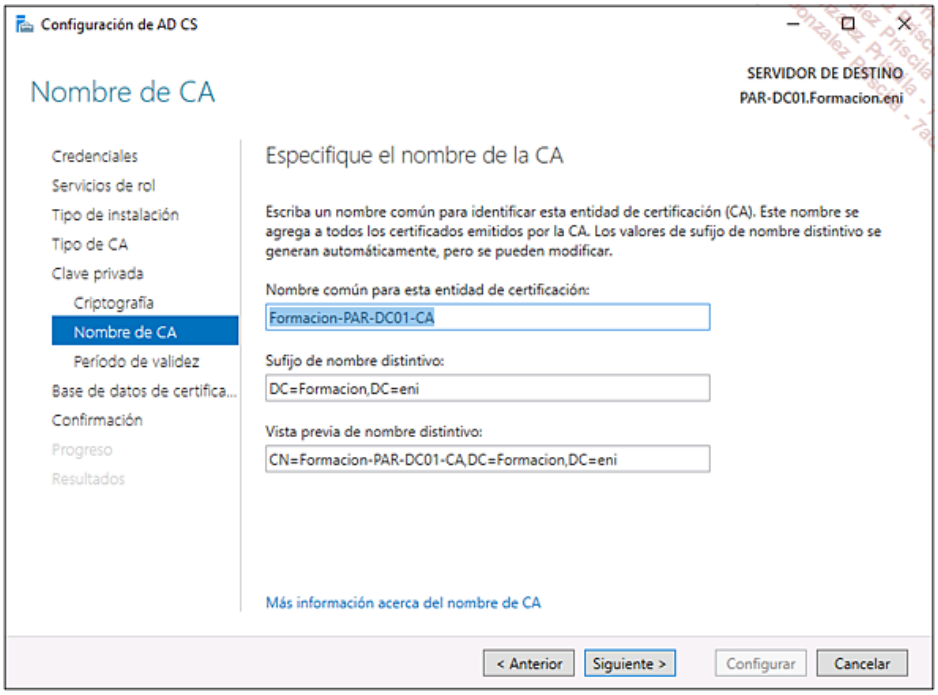
Marque la opción **Crear una clave privada nueva** y, a continuación, haga clic en **Siguiente**.



Deje las opciones por defecto en la ventana **Criptografía para la CA**.

El nombre de la entidad emisora de certificados se configura automáticamente, puede ser necesario modificarla (acceder desde el exterior…).

Deje las opciones por defecto y, a continuación, haga clic en **Siguiente**.



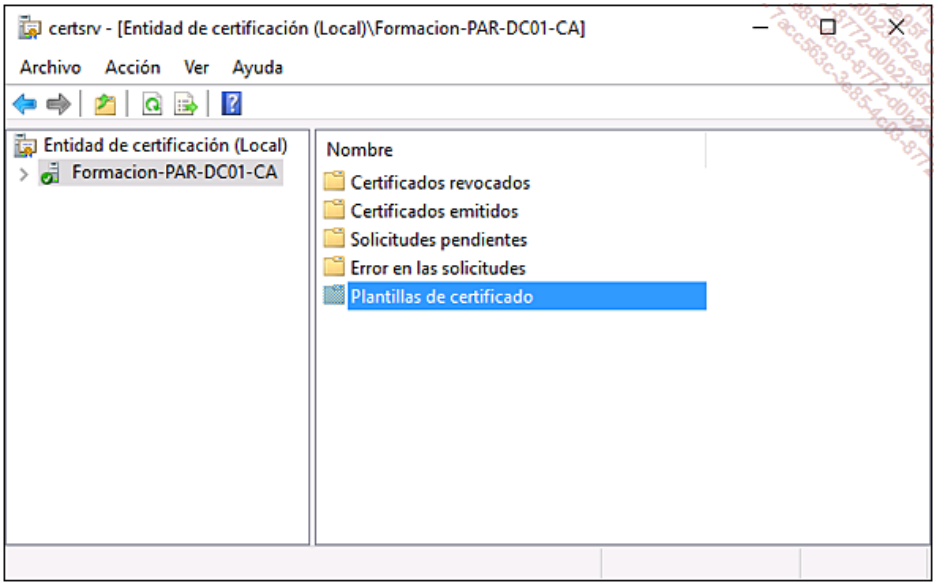
Configure un período de validez de 2 años en la ventana **Período de validez**.

Haga clic tres veces en **Siguiente** y, a continuación, en **Configurar**.

Haga clic en **Cerrar** para cerrar el asistente

En las Herramientas administrativas, abra la consola **Entidad de certificación**.

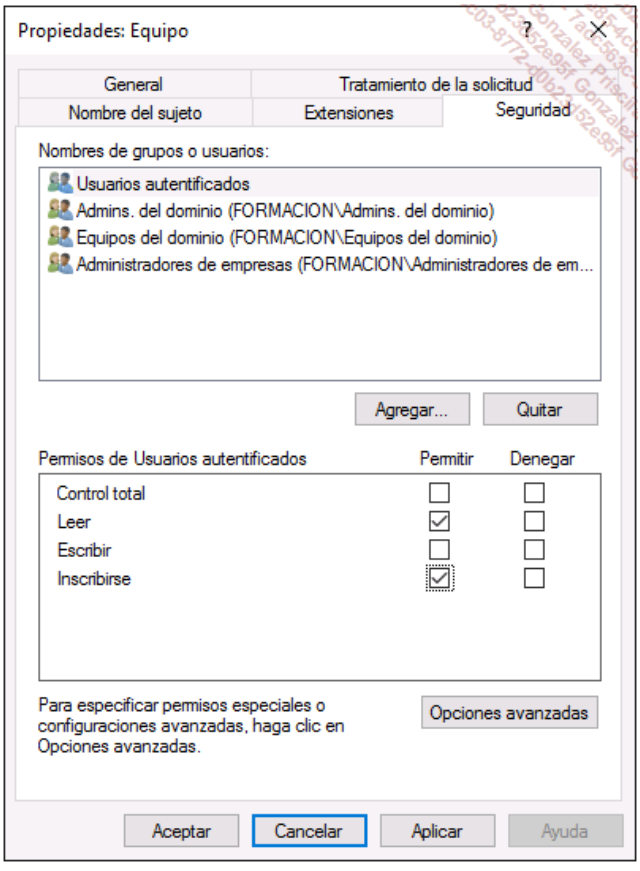
Despliegue el nodo **Formacion-PAR-DC01-CA** y, a continuación, haga clic con el botón derecho en **Plantillas de certificado** y seleccione**Administrar**.



Haga clic con el botón derecho en **Equipo** y, a continuación, haga clic en **Propiedades**.

En la ventana emergente **Propiedades: Equipo**, haga clic en la pestaña **Seguridad** y, a continuación, seleccione **Usuarios autenticados**.

Marque la opción **Permitir** para el permiso **Inscribirse** y, a continuación, haga clic en **Aceptar**.



Cierre la ventana **Consola de plantillas de certificado** y, a continuación, haga clic con el botón derecho en **Formacion-PAR-DC01-CA**, seleccione **Todas las tareas** y, a continuación, **Detener servicio**.

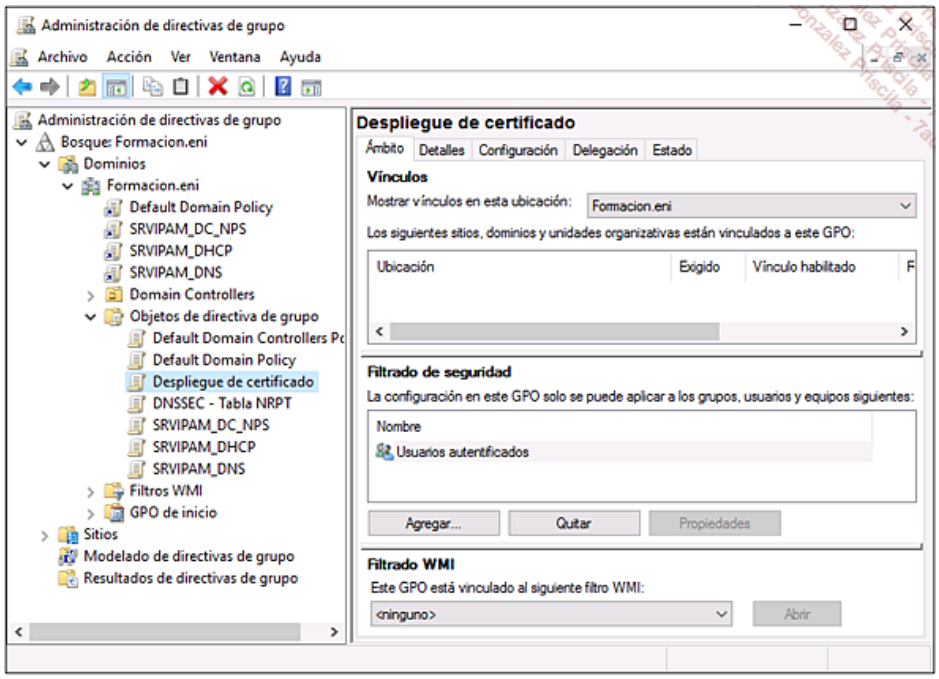
Repita la operación seleccionando, esta vez, la opción **Iniciar servicio**.

Cierre la consola **certsrv** (consola que permite administrar la entidad de certificación) y, a continuación, abra la consola **Administración de directivas de grupo**.

Despliegue el nodo **Bosque: Formacion.eni**, **Dominios** y, por último, **Formacion.eni**.

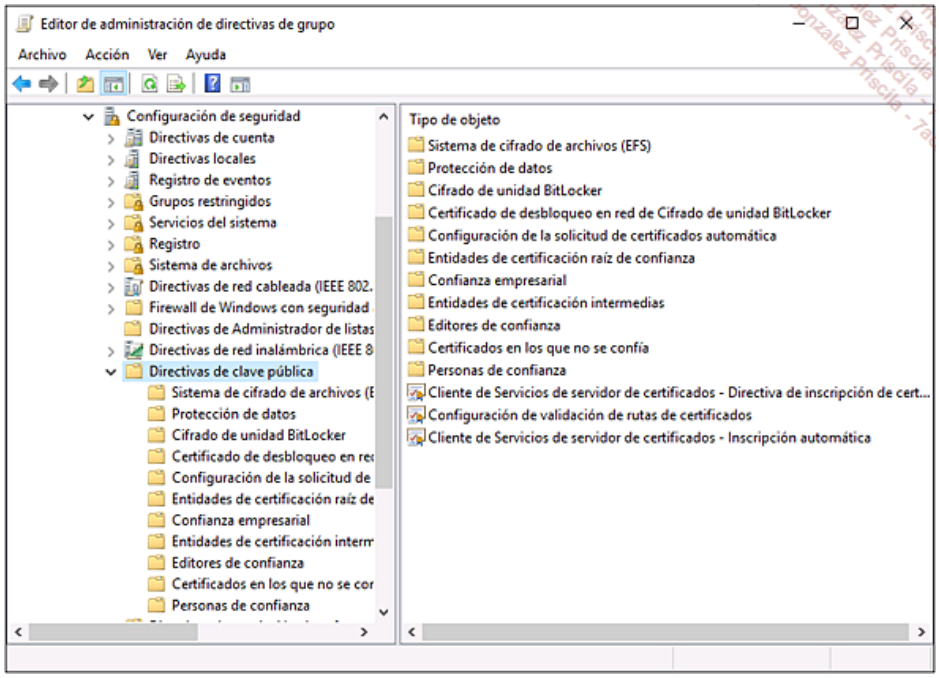
Haga clic con el botón derecho en **Objetos de directiva de grupo** y, a continuación, seleccione la opción **Nuevo** en el menú contextual.

Escriba **Despliegue de certificado** en el campo **Nombre** y, a continuación, haga clic en **Aceptar**.



Haga clic con el botón derecho en la directiva que acaba de crear y, a continuación, haga clic en **Editar**.

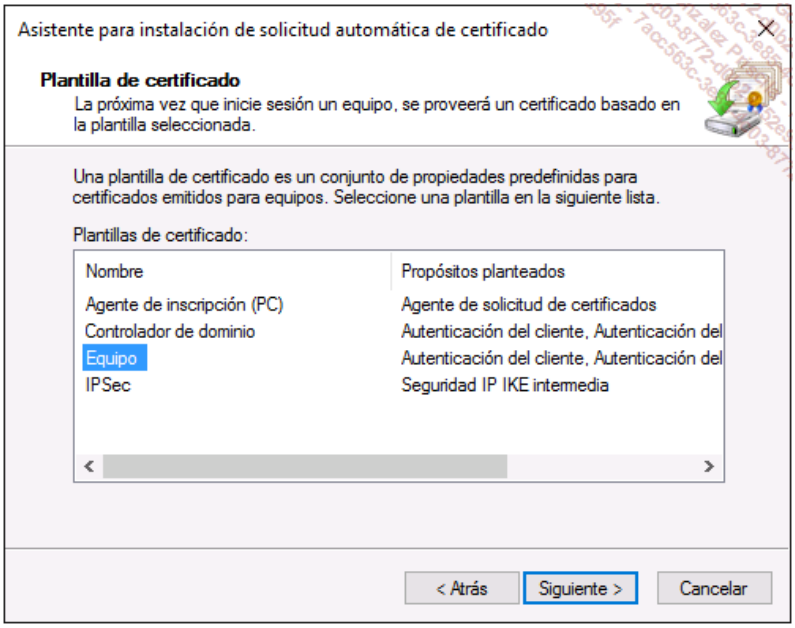
En la consola **Editor de administración de directivas de grupo** despliegue los nodos **Configuración del equipo, Directivas**, **Configuración de Windows**, **Configuración de seguridad** y, a continuación, **Directivas de clave pública**.



Haga clic con el botón derecho en la carpeta **Configuración de la solicitud de certificados automática** y, a continuación, en el menú contextual, seleccione **Nuevo** y, por último, **Solicitud de certificados automática**.

Se abre el asistente, haga clic en **Siguiente**.

En la ventana **Plantilla de certificado**, seleccione **Equipo** y, a continuación, haga clic en **Siguiente**.

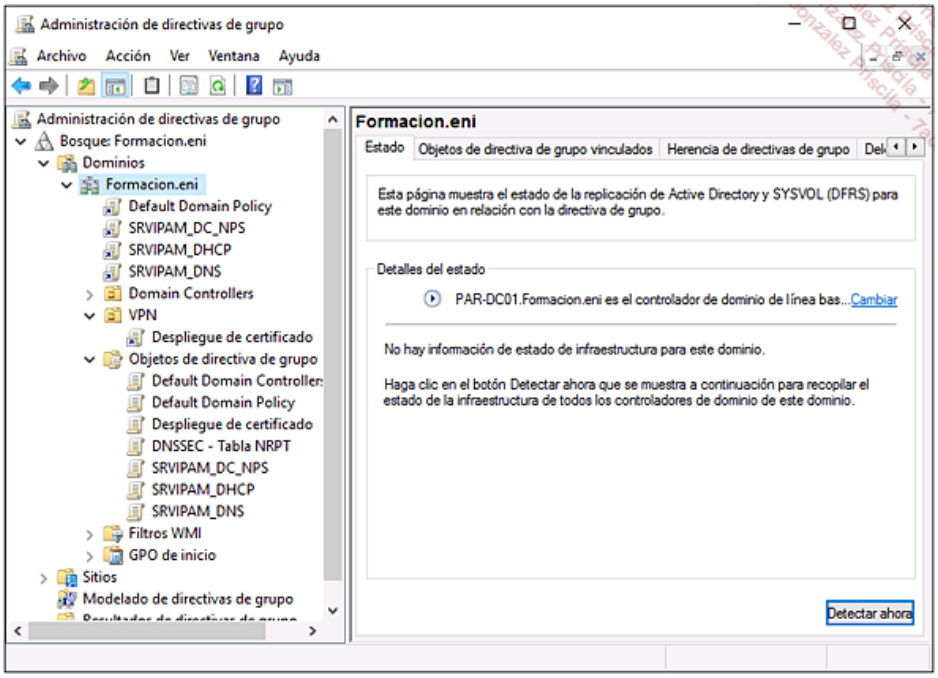


Haga clic en el botón **Finalizar** para cerrar el asistente.

Cierre la consola **Editor de administración de directivas de grupo** y, a continuación, en la consola **Administración de directivas de grupo**, haga clic con el botón derecho en la raíz del dominio **Formacion.eni**.

En el menú contextual, seleccione la opción **Nueva unidad organizativa** y, a continuación, escriba **VPN** en el campo **Nombre**.

Vincule la directiva de grupo **Despliegue de certificado** con la unidad organizativa **VPN**.



Si no lo hubiera hecho, una **SRV-RTR** al dominio **Formacion.eni**.

Inicie una sesión como **administrador@formacion.eni** (o como FORMACION\administrador) en el servidor **SRV-RTR**.

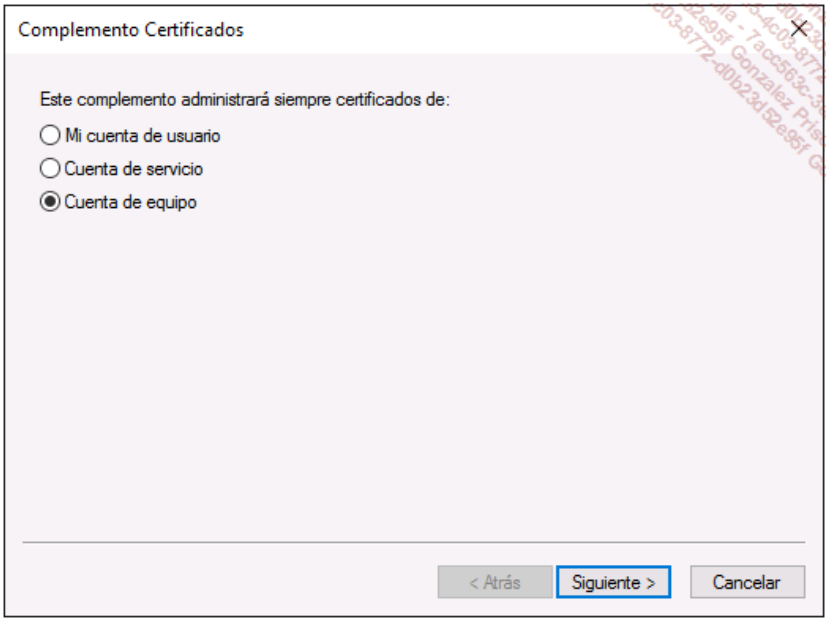
Sitúe el ratón en la zona inferior izquierda para mostrar la interfaz Windows, haga clic con el botón derecho y, a continuación, seleccione, en el menú contextual, la opción **Ejecutar**.

Escriba **mmc** y, a continuación, presione la tecla [Enter].

Haga clic en **Archivo** y, a continuación, en **Agregar o quitar complemento**.

En la ventana **Agregar o quitar complementos**, seleccione **Certificados** y, a continuación, haga clic en **Agregar**.

Se abre un asistente, marque la opción **Cuenta de equipo** y, a continuación, haga clic en **Siguiente**.



Deje la opción por defecto en la ventana **Seleccionar equipo** y, a continuación, haga clic en **Finalizar**.

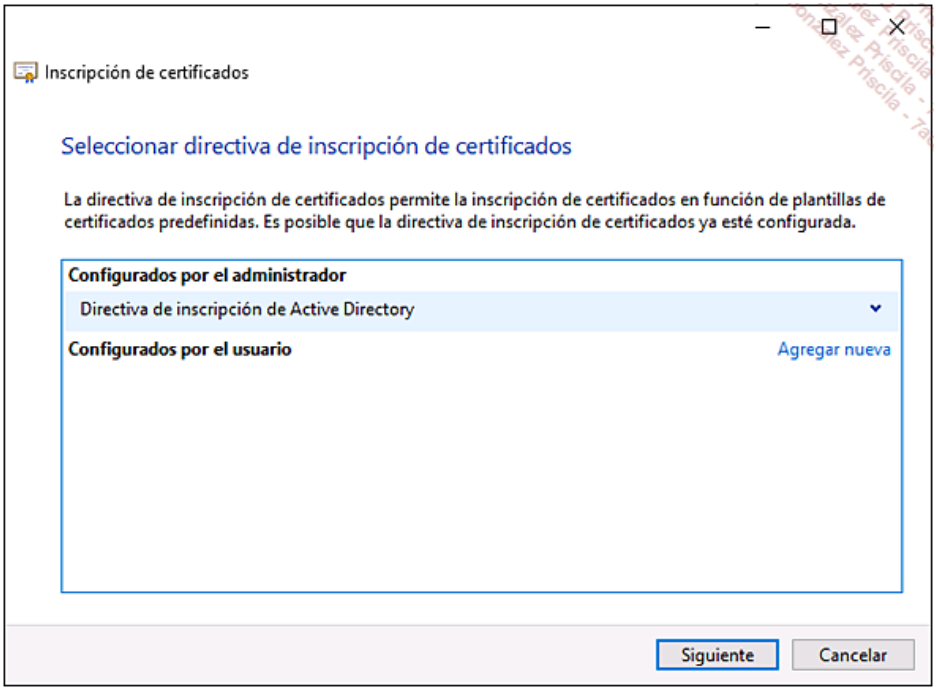
Haga clic en **Aceptar** para cerrar la ventana de selección de complementos.

Despliegue el nodo **Certificados** y, a continuación, haga clic con el botón derecho en **Personal**.

En el menú contextual, seleccione **Todas las tareas** y, a continuación, **Solicitar un nuevo certificado**.

Haga clic en **Siguiente** en la ventana **Antes de comenzar**.

Haga clic en **Directiva de inscripción de Active Directory** y, a continuación, haga clic en **Siguiente**.



En la ventana **Solicitar certificados**, marque **Equipo** y, a continuación, haga clic en **Inscribir**.

Verifique que el estado es igual a **Correcto** y, a continuación, haga clic en **Finalizar**.

Si no lo hubiera hecho, una **CL10-02** al dominio **Formacion.eni**.

El conmutador virtual debe ser idéntico al que utiliza PAR-DC01.

En **PAR-DC01**, abra la consola **Usuarios y equipos de Active Directory** y, a continuación, mueva la cuenta de equipo de **CL10-02** a la unidad organizativa **VPN**.

Inicie una sesión como **administrador@formacion.eni** (o como **FORMACION\administrador**) en el equipo **CL10-02**.

Abra una ventana de comandos DOS y, a continuación, ejecute el comando `gpupdate /force`.

Cierre la ventana de comandos y, a continuación, abra una consola MMC.

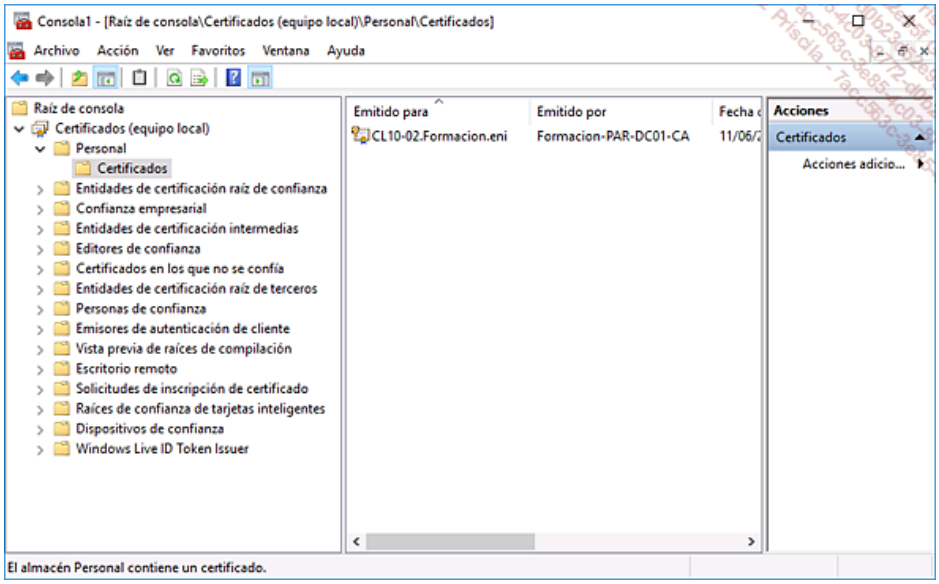
Agregue el complemento **Certificados**.

Se abre un asistente, marque **Cuenta de equipo** y, a continuación, haga clic en **Siguiente**.

Deje la opción por defecto en la ventana **Seleccionar equipo** y, a continuación, haga clic en **Finalizar**.

Despliegue los nodos **Certificados** y, a continuación, **Personal**.

Verifique la presencia del certificado emitido por **Formacion-PAR-DC01-CA**.



En **SRV-RTR**, abra la consola **Administrador del servidor**.

Haga clic en el vínculo **Agregar roles y características** y, a continuación, en la ventana **Antes de comenzar**, haga clic en **Siguiente**.

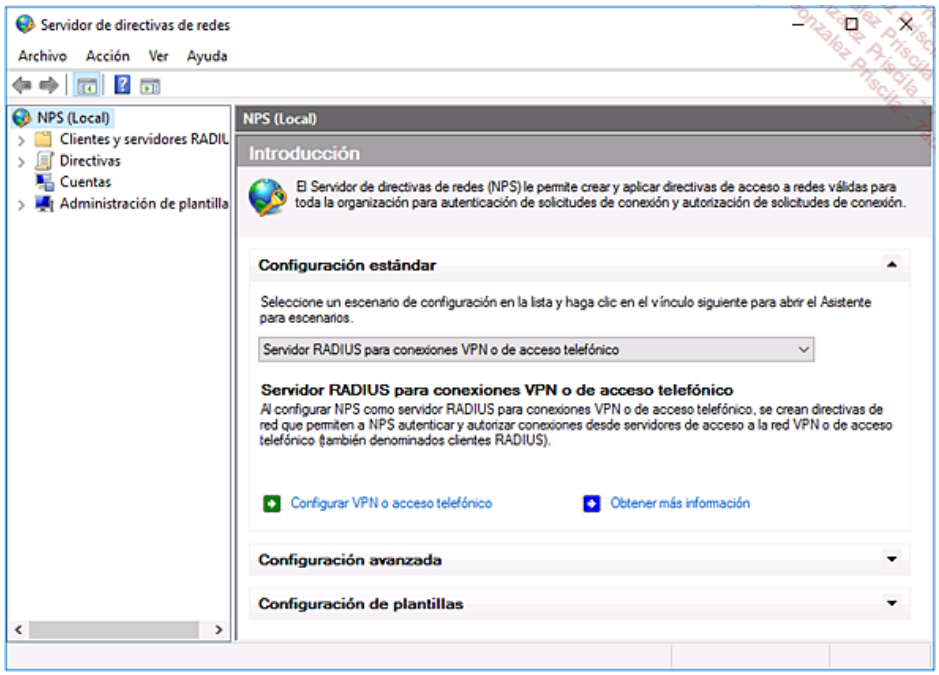
Deje la opción por defecto en la ventana **Seleccionar tipo de instalación** y, a continuación, haga clic dos veces en **Siguiente**.

En la ventana **Seleccionar roles de servidor**, marque **Servicios de acceso y directivas de redes** y, a continuación, haga clic en el botón**Agregar características**.

Haga clic tres veces en **Siguiente** y, a continuación, en la ventana **Seleccionar servicios de rol**, compruebe que está marcada la opción**Servidor de directivas de redes**.

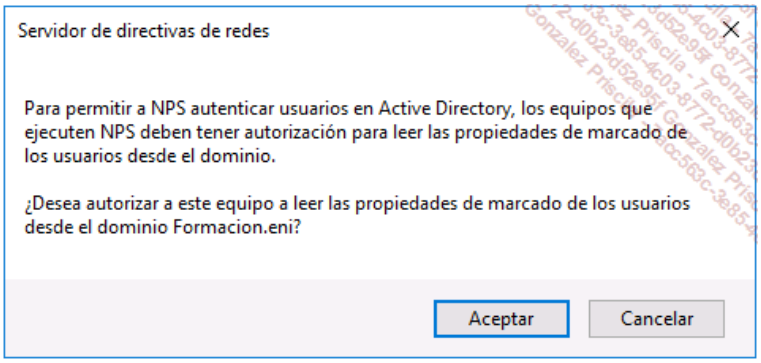
Haga clic en **Siguiente** y, a continuación, en **Instalar**.

Una vez terminada la instalación, abra la consola **Servidor de directivas de redes** desde las herramientas administrativas.



Haga clic con el botón derecho en **NPS (Local)** y, a continuación, seleccione **Registrar servidor en Active Directory** en el menú contextual.

Aparece un mensaje, haga clic en **Aceptar**.



Abra la consola **Administrador del servidor**.

Haga clic en el vínculo **Agregar roles y características** y, a continuación, en la ventana **Antes de comenzar**, haga clic en **Siguiente**.

Deje la opción por defecto en la ventana **Seleccionar tipo de instalación** y, a continuación, haga clic dos veces en **Siguiente**.

En la ventana **Seleccionar roles de servidor**, marque **Acceso remoto** y, a continuación, haga clic en el botón **Agregar características**.

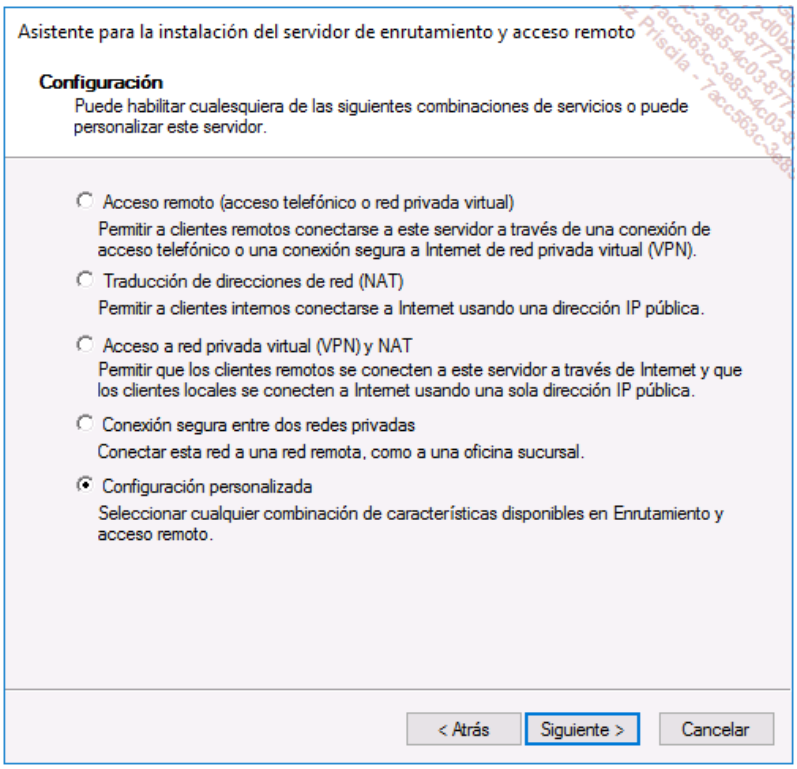
Haga clic tres veces en **Siguiente** y, a continuación, en la ventana **Seleccionar servicios de rol**, marque **Enrutador** y, a continuación, haga clic en **Siguiente**.

Haga clic dos veces en **Siguiente** (los **Servicios de rol IIS** deben dejarse por defecto) y, a continuación, haga clic en **Instalar**.

Una vez terminada la instalación, abra la consola **Enrutamiento y acceso remoto** desde las Herramientas administrativas.

Haga clic con el botón derecho en **SRV-RTR** y, a continuación, en el menú contextual, haga clic en **Configurar y habilitar Enrutamiento y acceso remoto**.

En la ventana de **bienvenida**, haga clic en **Siguiente** y, a continuación, marque la opción **Configuración personalizada**.



Haga clic en **Siguiente** para validar la opción seleccionada.

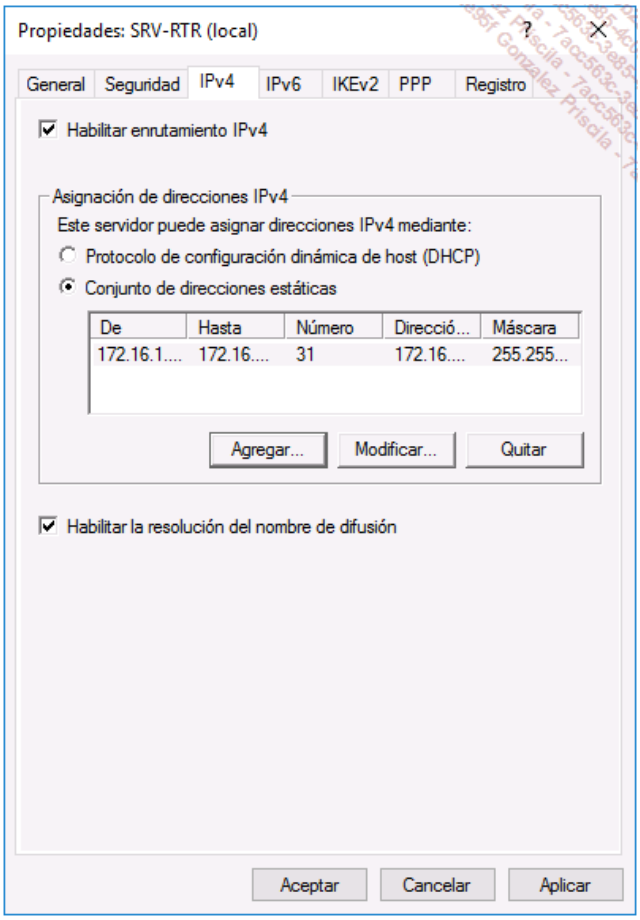
En la ventana **Configuración personalizada**, marque la opción **Acceso a VPN** y, a continuación, haga clic en **Siguiente**.

Haga clic en **Finalizar** para cerrar el asistente y, a continuación, en **Iniciar servicio** en la ventana que aparece.

Haga clic con el botón derecho en **SRV-RTR (local)** y, a continuación, en el menú contextual, seleccione **Propiedades**.

Seleccione la pestaña **IPv4** y, a continuación, marque la opción **Conjunto de direcciones estáticas**.

Haga clic en **Agregar** y, a continuación, escriba **172.16.1.200** en el campo **Dirección IP inicial** y **172.16.1.230** en **Dirección IP final**.



Haga clic en **Aceptar**.

Ahora es preciso crear una directiva de red para los clientes que se conectan mediante VPN.

Desde **PAR-DC01**, abra la consola **Usuarios y equipos de Active Directory** y, a continuación, en la unidad organizativa **VPN** cree un grupo llamado **G_Acceso_VPN**.

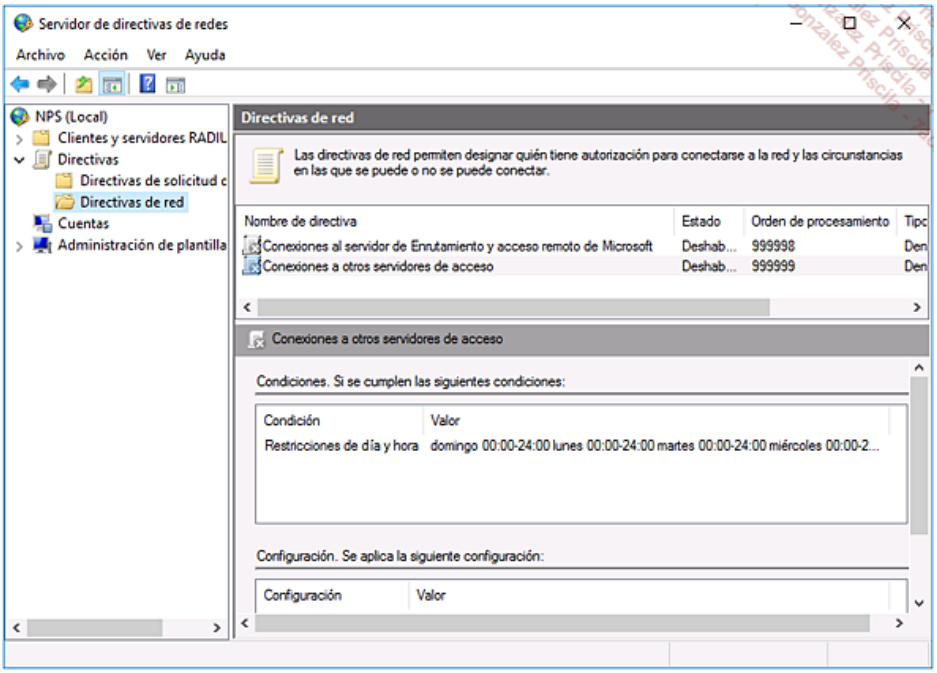
El grupo de seguridad tiene un ámbito global. Los usuarios se añadirán más adelante.

Cree un usuario **Vpn Test (vpntest)** y agréguelo al grupo **G_Acceso_VPN**.

En la consola **Servidor de acceso a redes**, en el servidor **SRV-RT**, despliegue **Directivas** y, a continuación, haga clic en **Directivas de red**.

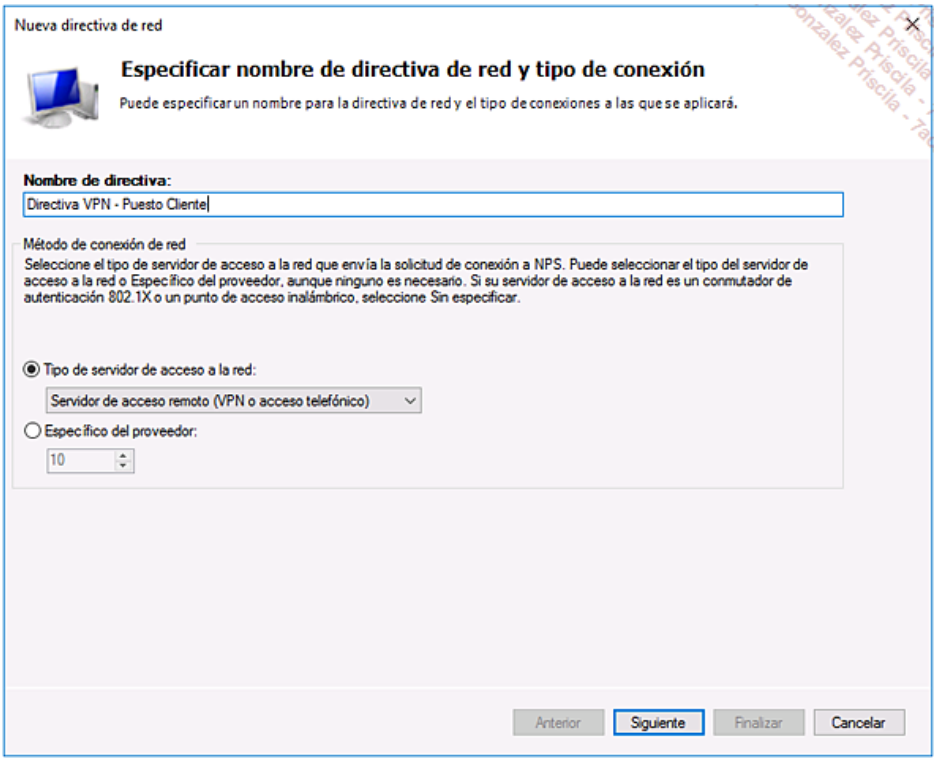
Haga clic con el botón derecho en la primera directiva de red y, a continuación, seleccione la opción **Deshabilitar** en el menú contextual.

Repita la misma operación para la segunda directiva.



Haga clic con el botón derecho en la carpeta **Directivas de red** y, a continuación, seleccione **Nuevo**.

En el campo **Nombre**, escriba **Directiva VPN - Puesto Cliente** y, a continuación, en la lista desplegable **Tipo de servidor de acceso a la red** seleccione **Servidor de acceso remoto (VPN o acceso telefónico)**.

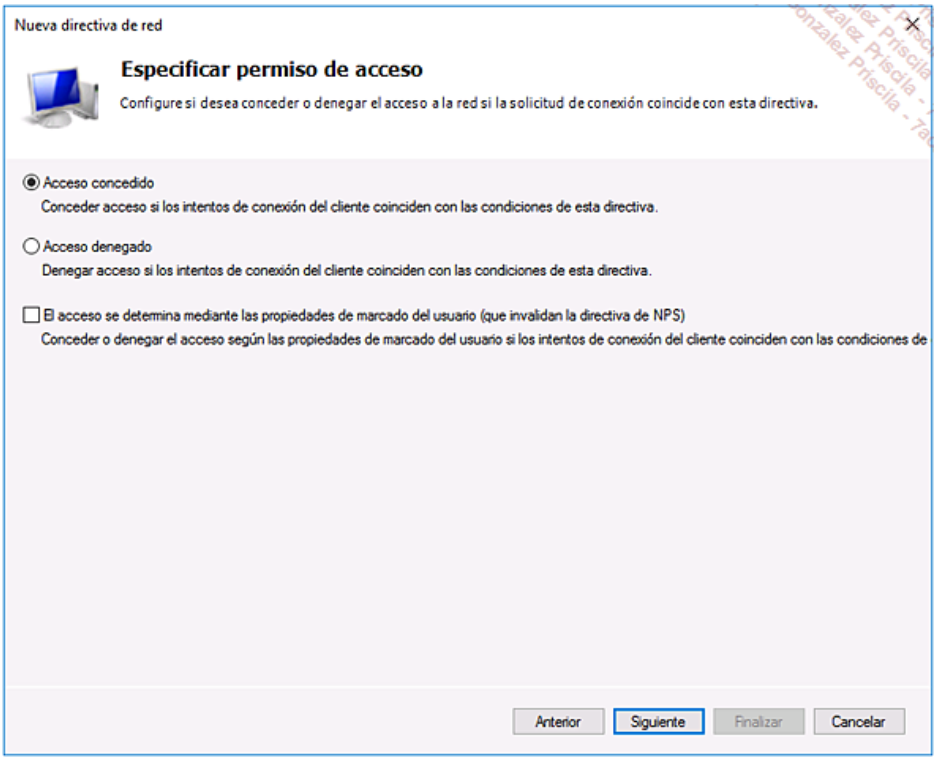


Haga clic en **Siguiente** para validar los cambios.

En la página **Especificar condiciones**, haga clic en **Agregar** y, a continuación, seleccione **Grupos de Windows** en la ventana que se muestra.

Haga clic en **Agregar** y, a continuación, en **Agregar grupos**. En la ventana que se muestra, escriba **G_Acceso_VPN** y, a continuación, haga clic en **Comprobar nombres**.

Haga clic en **Siguiente** y, a continuación, indique la autorización **Acceso concedido**. Valide haciendo clic en **Siguiente**.



En la ventana **Configurar métodos de autenticación**, desmarque la opción **Autenticación cifrada de Microsoft (MS-CHAP)** y, a continuación, haga clic en **Siguiente**.

Haga clic en **Siguiente** hasta la última ventana y, a continuación, en el botón **Finalizar** para cerrar el asistente.

El servidor VPN está, ahora, configurado.

2. Configuración del cliente VPN

Objetivo: configurar el cliente VPN y, a continuación, comprobar su conexión.

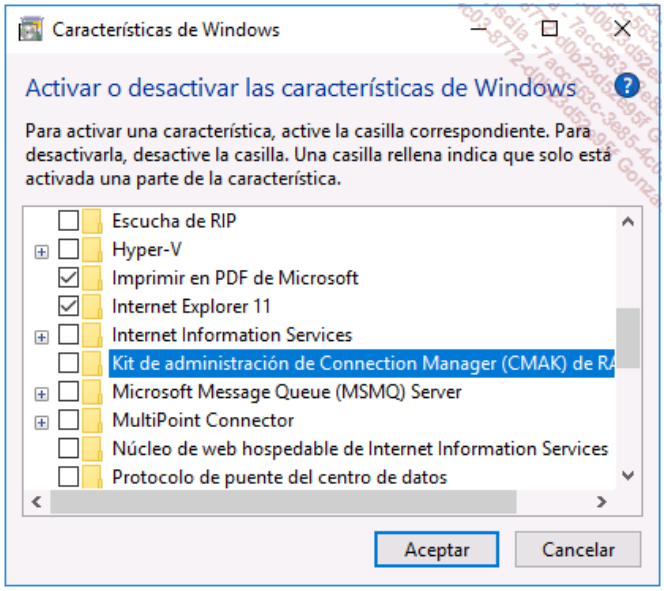
Máquinas virtuales: PAR-DC01, SRV-RTR y CL10-02.

En **CL10-02**, conéctese como administrador de dominio.

Sitúe el ratón en la zona inferior izquierda para mostrar la interfaz del menú inicio. Haga clic con el botón derecho en la interfaz y, a continuación, en el menú contextual, seleccione **Panel de control**.

Haga clic en **Programas** y, a continuación, en **Activar o desactivar las características de Windows**.

Marque la opción **Kit de administración de Connection Manager (CMAK) de RAS**, y, a continuación, haga clic en **Aceptar**.



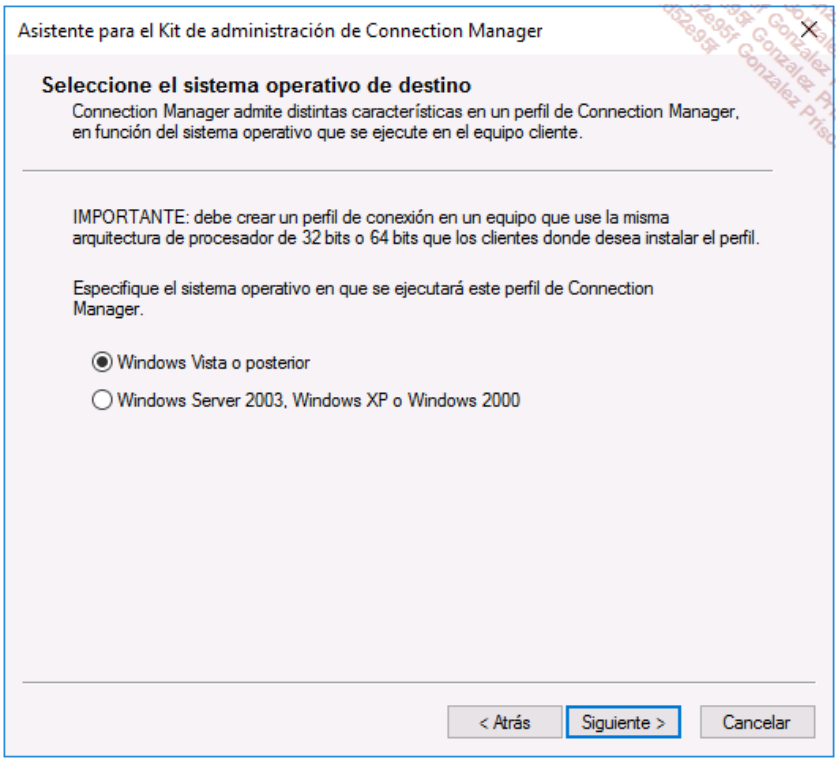
Haga clic en **Cerrar**.

Cambie la interfaz del panel de control al modo **Iconos grandes**.

Haga clic en **Herramientas administrativas** y, a continuación, haga doble clic en **Kit de administración de Connection Manager**.

En la ventana de **bienvenida**, haga clic en **Siguiente**.

Deje la opción **Windows Vista o posterior** marcada y, a continuación, haga clic en **Siguiente**.



En la ventana **Crear o modificar un perfil de Connection Manager**, deje la opción **Perfil nuevo** marcada y, a continuación, haga clic en**Siguiente**.

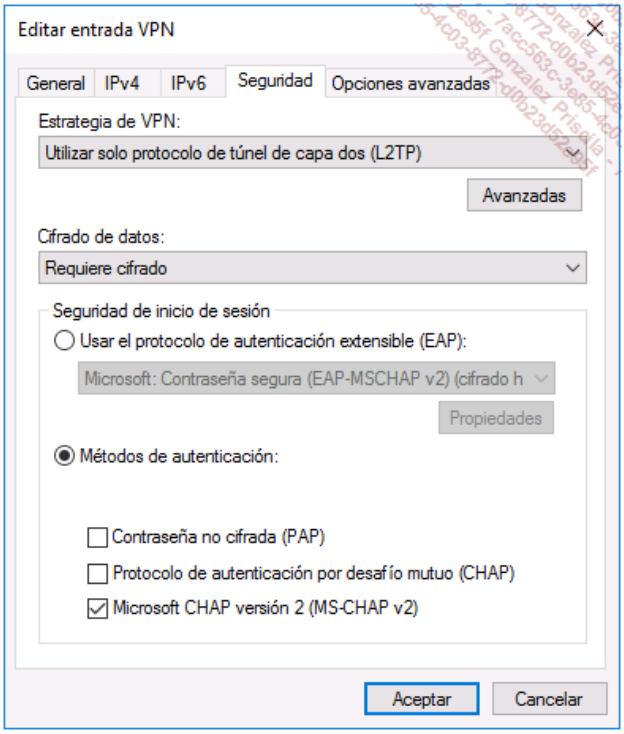
Escriba **Conexión VPN Formacion.eni** en el campo **Nombre de servicio** y, a continuación, **VPN** en **Nombre de archivo**. Haga clic en**Siguiente** para validar la información introducida.

En la pantalla **Especificar un nombre de dominio**, haga clic en **No agregar un nombre de territorio al nombre de usuario**, y, a continuación, dos veces en **Siguiente**.

En la pantalla **Agregar compatibilidad para conexiones VPN**, marque la opción **Libreta de teléfonos de este perfil**. A continuación, en el campo **Usar siempre el mismo servidor VPN**, escriba **172.17.255.254**, y haga clic en **Siguiente**.

Haga clic en **Editar** en la pantalla **Crear o modificar una entrada VPN** y, a continuación, seleccione la pestaña **Seguridad**.

En la lista desplegable **Estrategia de VPN**, seleccione **Utilizar solo protocolo de túnel de capa dos (L2TP)**.



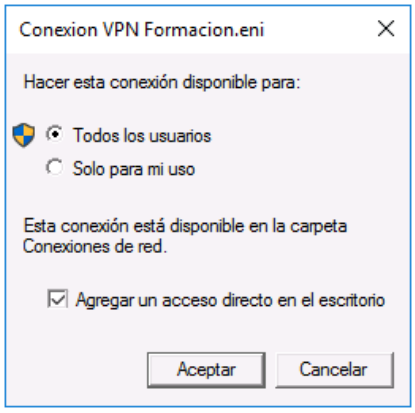
Valide la información indicada haciendo clic en **Aceptar**.

Haga clic en **Siguiente** y, a continuación, desmarque la opción **Descargar automáticamente actualizaciones de la libreta de teléfonos** en la pantalla **Agregar una libreta de teléfonos personalizada**.

Haga clic en **Siguiente** hasta que finalice el asistente y, a continuación, en **Finalizar**.

Vaya a la carpeta C:\Program Files\CMAK\Profiles\Windows Vista and above\VPN y, a continuación, haga doble clic en **VPN.exe**.

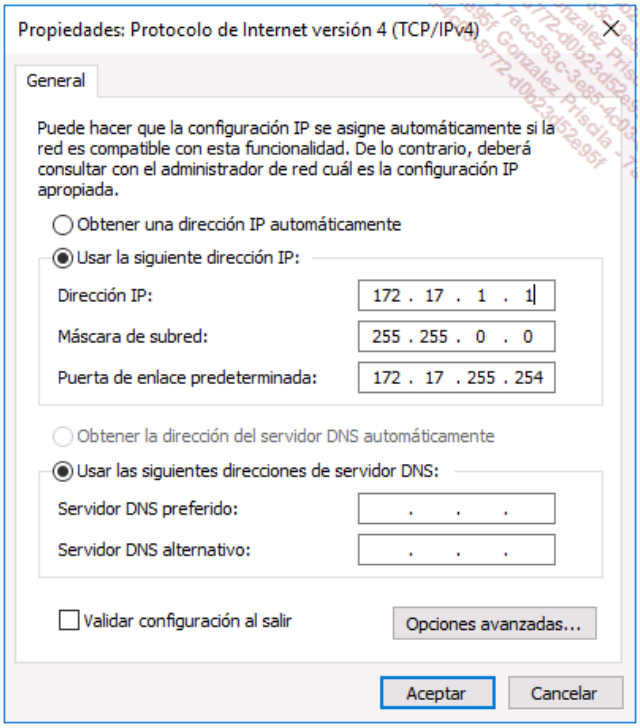
Haga clic en **Sí** en el mensaje de advertencia y, a continuación, marque **Todos los usuarios** y **Agregar un acceso directo en el escritorio**.



Cierre todas las ventanas y, a continuación, inicie una sesión como **emartinez**.

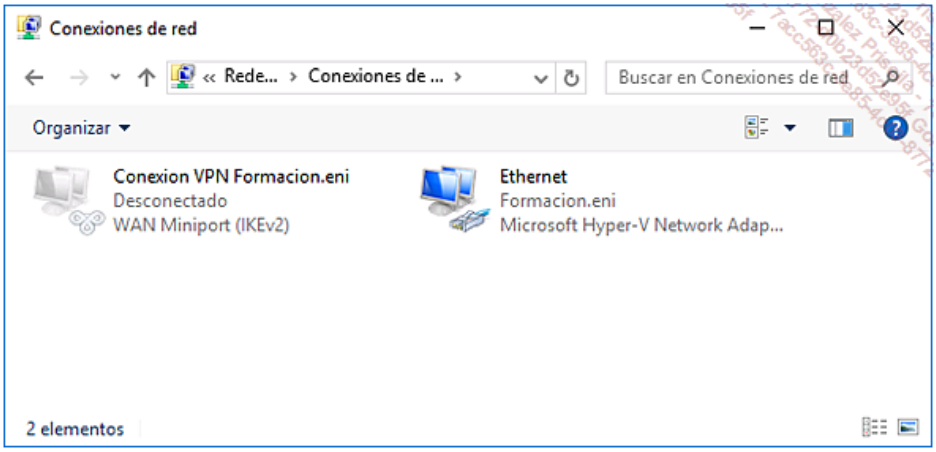
Modifique la configuración IP de la tarjeta de red como se indica a continuación (es necesario informar las credenciales del administrador de dominio):

- **Dirección IP**: 172.17.1.1
- **Máscara de subred**: 255.255.0.0
- **Puerta de enlace predeterminada**: 172.17.255.254

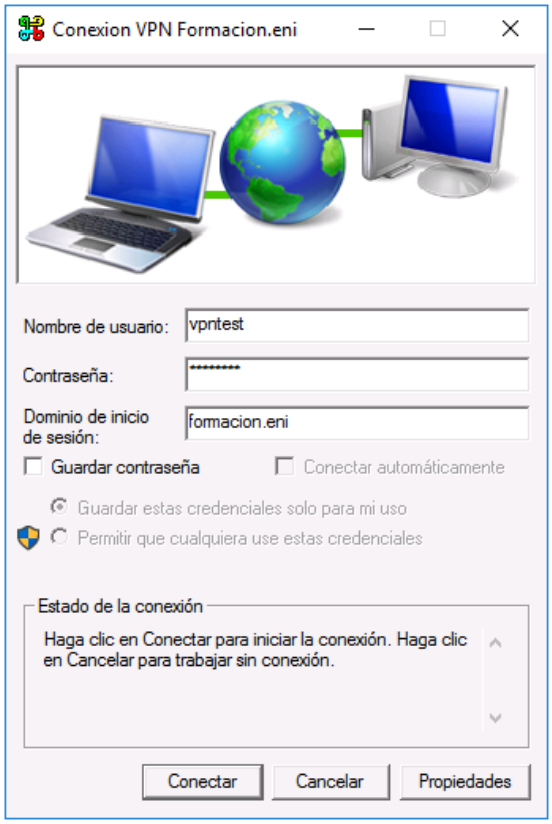


Modifique el conmutador virtual de la máquina **CL10-02** para utilizar el conmutador llamado **BARCELONA** utilizado por **SRV-RTR**.

En la ventana **Conexiones de red**, haga doble clic en el icono **Conexión VPN Formacion.eni** y, a continuación, en el panel **Red**, haga clic en **Conexión VPN Formacion.eni** y, a continuación, en **Conectar**.



Escriba **vpntest** en el campo **Nombre de usuario** y, a continuación, **Pa$$w0rd** en **Contraseña** y **Formacion.eni** en el campo **Dominio de inicio de sesión**.



Haga clic en **Conectar** para iniciar la conexión VPN.

Ejecute la combinación de teclas [Windows] + i en la ventana **Configuración de Windows**, ejecute la búsqueda con la palabra **VPN** y, a continuación, haga clic en **Cambiar redes privadas virtuales (VPN)**.

Haga clic en **Conexion VPN Formacion.eni** y, a continuación, en **Opciones avanzadas** y obtenga las propiedades de la conexión VPN.

En caso de que falle la conexión, deshabilite el Firewall y renueve la conexión.

La máquina cliente está, ahora, conectada con la red de la empresa mediante un túnel VPN.

3. Configuración de DirectAccess

Objetivo: configurar la funcionalidad DirectAccess

Máquinas virtuales: PAR-DC01, SRV-RTR y CL10-02.

Si ha seguido los dos trabajos prácticos anteriores, realice las siguientes tres manipulaciones. En caso contrario, puede ignorarlas.

En **SRV-RTR**, abra la consola **Enrutamiento y acceso remoto** y, a continuación, haga clic con el botón derecho en **SRV-RTR (local)**.

Seleccione la opción **Deshabilitar Enrutamiento y acceso remoto** para detener el servicio.

En **PAR-DC01**, abra la consola **Administrador de directivas de grupo** y, a continuación, deshabilite la directiva de grupo **Despliegue de certificado** vinculada a la unidad organizativa **VPN**.

Modifique el conmutador virtual de la estación **CL10-02** para que utilice el configurado en **PAR-DC01**. Modifique la configuración de red de manera tal que la obtenga mediante DHCP. Si no ha realizado el trabajo práctico anterior, es necesario crear una unidad organizativa llamada **VPN** en la raíz del dominio **Formacion.eni**. Puede crearse mediante la consola **Usuarios y equipos de Active Directory**. A continuación, cree un grupo global de seguridad llamado **G_Acceso_VPN** (el cual estará presente en la unidad organizativa que acaba de crear).

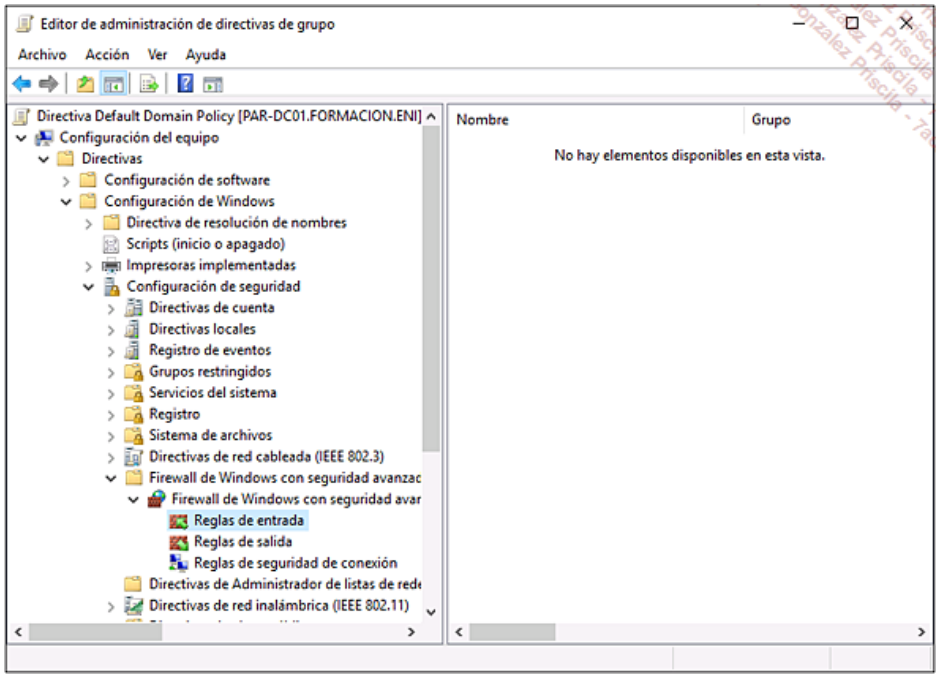
En **PAR-DC01**, abra la consola **Usuarios y equipos de Active Directory** y, a continuación, despliegue el nodo **Formacion.local** y haga clic en la unidad organizativa **VPN**.

Haga doble clic en el grupo **G_Acceso_VPN**, seleccione la cuenta de usuario que ha agregado en el trabajo práctico anterior y haga clic en**Eliminar**. Agregue la cuenta de equipo **CL10-02** al grupo.

Abra la consola **Administración de directivas de grupo**, haga clic con el botón derecho en la directiva de grupo **Default Domain Policy** y, a continuación, seleccione la opción **Editar**.

Se abre la consola **Editor de administración de directivas de grupo**, despliegue los nodos **Configuración del equipo**, **Directivas**,**Configuración de Windows**, **Configuración de seguridad**, **Firewall de Windows con seguridad avanzada**.

Haga clic con el botón derecho en **Reglas de entrada** y, a continuación, haga clic en **Nueva regla**.

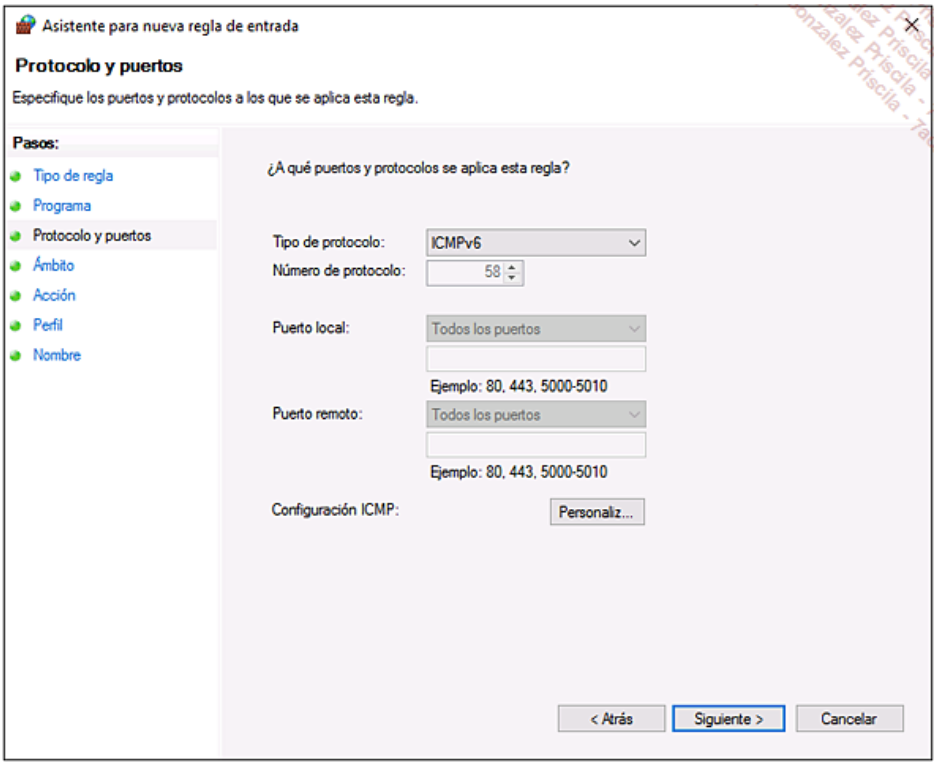


En la pantalla **Tipo de regla**, seleccione **Personalizada** y, a continuación, haga clic dos veces en **Siguiente**.

En la lista desplegable **Tipo de protocolo**, seleccione **ICMPv6** y, a continuación, haga clic en el botón **Personaliz...**.

Marque la opción **Tipos de ICMP específicos** y, a continuación, **Petición eco**.

Haga clic en **Aceptar** y, a continuación, **Siguiente**.



Haga clic en **Siguiente** en las ventanas **Ámbito**, **Acción** y **Perfil**.

Escriba **Autorizar - ICMPv6 - De entrada** en el campo **Nombre** y, a continuación, haga clic en **Finalizar**.

Haga clic con el botón derecho en **Reglas de salida** y, a continuación, haga clic en **Nueva regla**.

En la pantalla **Tipo de regla**, seleccione **Personalizada** y, a continuación, haga clic dos veces en el botón **Siguiente**.

En la lista desplegable **Tipo de protocolo**, seleccione **ICMPv6** y, a continuación, haga clic en el botón **Personaliz...**.

Marque la opción **Tipos de ICMP específicos** y, a continuación, **Petición eco**.

Haga clic en **Aceptar** y, a continuación, dos veces en **Siguiente**.

Seleccione la opción **Permitir la conexión** y, a continuación, haga clic dos veces en **Siguiente**.

Escriba **Autorizar - ICMPv6 - De salida** en el campo **Nombre** y, a continuación, haga clic en **Finalizar**.

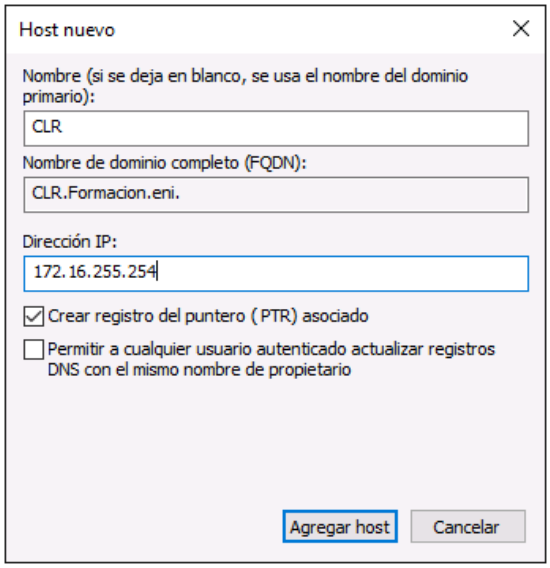
Cierre las consolas **Editor de administración de directivas de grupo** y **Administración de directivas de grupo**.

Abra la consola **Administrador del servidor**, haga clic en **Herramientas** y, a continuación, **DNS**.

Despliegue los nodos **PAR-DC01**, **Zonas de búsqueda directa** y **Formacion.eni**.

Haga clic con el botón derecho en **Formacion.eni** y, a continuación, seleccione **Host nuevo (A o AAAA)**.

Escriba **CRL** en el campo **Nombre** y **172.16.255.254** en el campo **Dirección IP**.



Haga clic en el botón **Agregar host**.

Repita la misma operación para el host **NLS** con dirección IP **172.16.255.254**.

Haga clic en **Aceptar** para validar el mensaje informativo.

Cierre la consola DNS y abra una ventana de comandos DOS.

Escriba el comando `dnscmd /config /globalqueryblocklist wpad`.

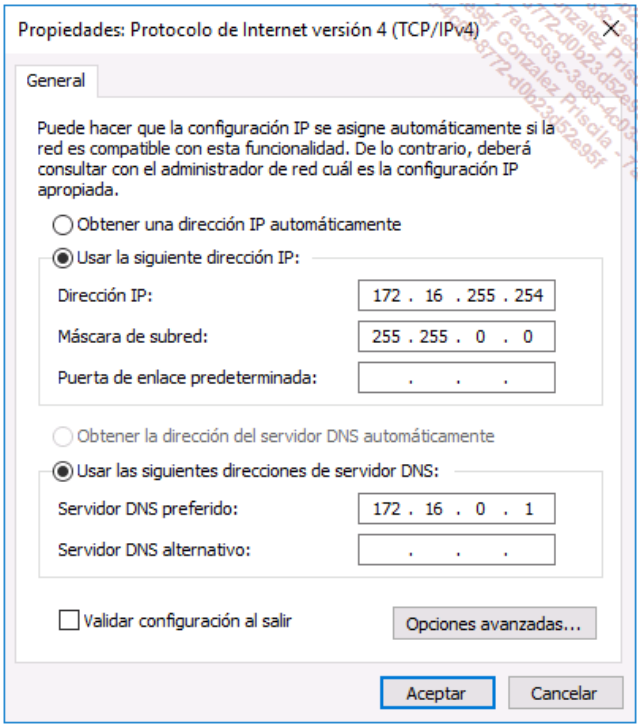
Este comando permite eliminar el nombre ISATAP de la lista roja de consultas globales DNS

Aparece el mensaje **El comando se ha ejecutado correctamente**.

En **SRV-RTR**, acceda al panel de control y, a continuación, a la consola **Centro de redes y recursos compartidos**.

Haga clic en **Cambiar configuración del adaptador** y, a continuación, acceda a las propiedades de la tarjeta Ethernet que está conectada a la red local 172.16.255.254.

Seleccione **Protocolo de Internet versión 4 (TCP/IPv4)** y, a continuación, haga clic en **Propiedades** y **Opciones avanzadas**.



Seleccione la pestaña **DNS** y, a continuación, escriba **Formacion.eni** en el campo **Sufijo DNS para esta conexión**.

Haga clic en **Aceptar** para validar todas las ventanas.

Es, ahora, momento de ocuparse de la parte correspondiente a los certificados digitales.

Si no estuviera hecho, instale una **entidad de certificación** en **PAR-DC01**.

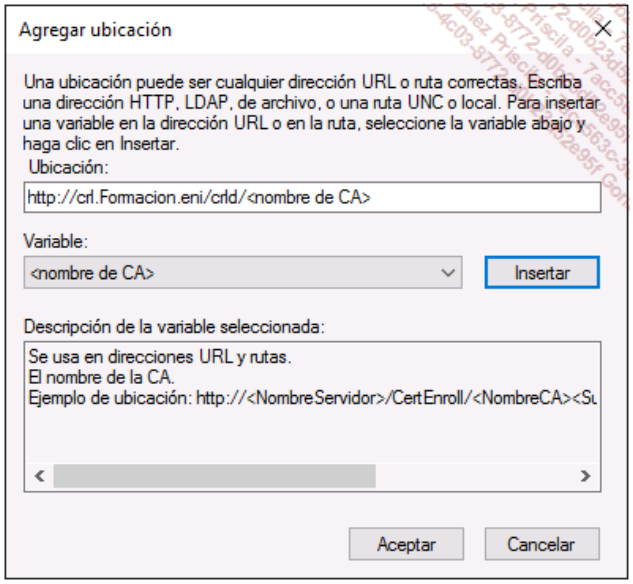
En **PAR-DC01**, abra la consola **Administrador del servidor**, haga clic en **Herramientas** y, a continuación, seleccione **Entidad de certificación**.

Haga clic con el botón derecho en **Formation-PAR-DC01-CA** y, a continuación, seleccione **Propiedades**.

Seleccione la pestaña **Extensiones** y, a continuación, haga clic en el botón **Agregar**.

Escriba **http://crl.Formacion.eni/crld/** en el campo **Ubicación** y, a continuación, seleccione **<nombre de CA>** en la lista desplegable**Variable**.

Haga clic en **Insertar**.



Seleccione **<sufijo de nombre de lista CRL>** en la lista desplegable **Variable** y, a continuación, haga clic en **Insertar**.

Seleccione **<diferencias entre listas CRL permitidas>** en la lista desplegable **Variable** y, a continuación, haga clic en **Insertar**.

Escriba **.crl** al final del campo **Ubicación**.

Haga clic en **Aceptar** y, a continuación, marque las opciones **Incluir en las CRL.Usada para encontrar la ubicación de diferencias CRL.** e**Incluir en la extensión CDP de los certificados emitidos**.

Haga clic en **Aplicar** y, a continuación, en **No** en la ventana emergente que propone reiniciar los servicios de certificados de Active Directory.

Haga clic en el botón **Agregar** y, a continuación, en el campo **Ubicación**, escriba **\\SRV-RTR\crldist$**.

Seleccione **<nombre de CA>** en la lista desplegable **Variable** y, a continuación, haga clic en **Insertar**.

Seleccione **<sufijo de nombre de lista CRL>** en la lista desplegable **Variable** y, a continuación, haga clic en **Insertar**.

Seleccione **<diferencias entre listas CRL permitidas>** en la lista desplegable **Variable** y, a continuación, haga clic en **Insertar**.

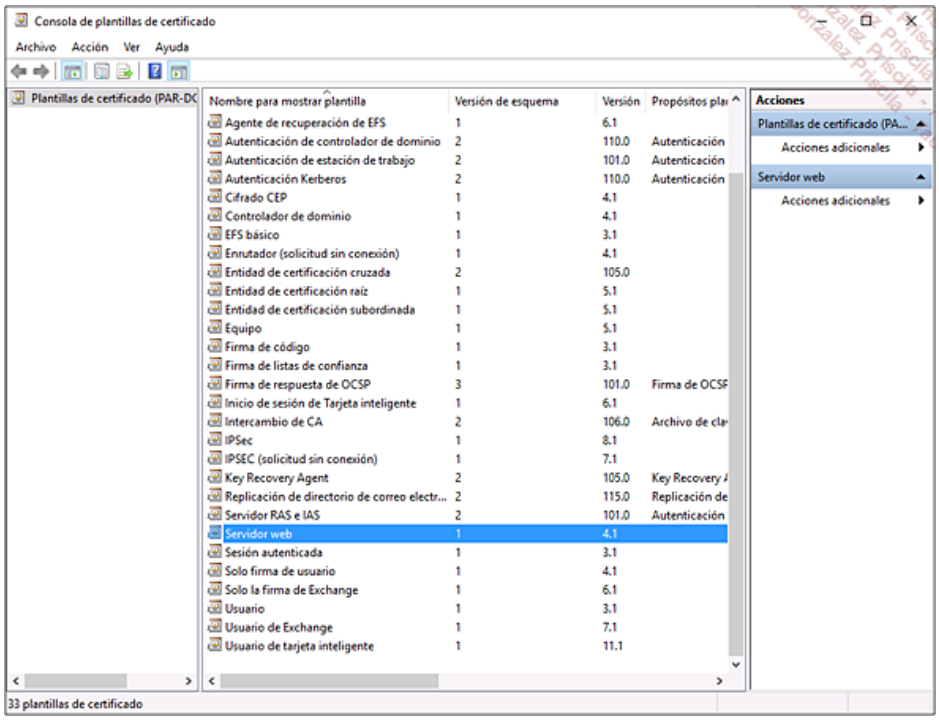
Escriba **.crl** al final del campo **Ubicación** y, a continuación, haga clic en **Aceptar**.

Marque las opciones **Publicar las listas de revocación de certificados (CRL) en esta ubicación** y **Publicar diferencias CRL en esta ubicación** y, a continuación, haga clic en **Aceptar**.

Haga clic en **Sí** para reiniciar los servicios de certificados de Active Directory.

Despliegue **Formacion-PAR-DC01-CA** y, a continuación, haga clic con el botón derecho en **Plantillas de certificado**. Seleccione**Administrar** en el menú contextual.

Haga clic con el botón derecho en **Servidor web** y, a continuación, haga clic en **Plantilla duplicada**.



Seleccione la pestaña **General** y, a continuación, escriba **Certificado SRV Web Formación**.

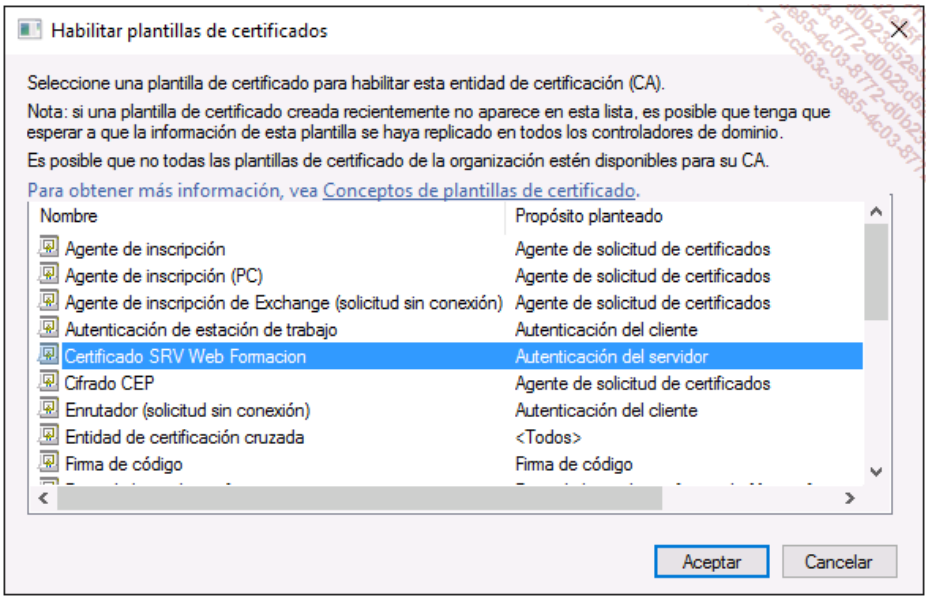
Haga clic en la pestaña **Tratamiento de la solicitud** y, a continuación, marque **Permitir que la clave privada se pueda exportar**.

Haga clic en la pestaña **Seguridad**, seleccione **Usuarios autentificados** y, a continuación, en **Permisos** seleccione **Inscribirse**.

Haga clic en **Aceptar** y, a continuación, cierre la **Consola de plantillas de certificado**.

En la consola **Entidad de certificación**, haga clic con el botón derecho en **Plantillas de certificado** y, a continuación, seleccione las opciones **Nuevo - Plantilla de certificado que se va a emitir** en el menú contextual.

Seleccione la plantilla que acaba de crear y, a continuación, haga clic en **Aceptar**.



Haga clic con el botón derecho en **Formacion-PAR-DC01-CA** y, a continuación, en el menú contextual, seleccione **Todas las tareas** y, a continuación, **Detener servicio**.

Repita la operación seleccionando, esta vez, la opción **Iniciar servicio**.

Cierre la consola **Entidad de certificación** y, a continuación, abra la consola **Administración de directivas de grupo**.

Despliegue los nodos **Bosque: Formacion.eni**, **Dominios** y, a continuación, **Formacion.eni**.

Haga clic con el botón derecho en **Default Domain Policy** y, a continuación, haga clic en **Editar**.

Despliegue los nodos **Configuración del equipo**, **Directivas**, **Configuración de Windows**, **Configuración de seguridad** y **Directivas de clave pública**.

Haga clic con el botón derecho en **Configuración de la solicitud de certificados automática**, y, a continuación, seleccione **Nuevo - Solicitud de certificados automática**.

Se abre un asistente, haga clic en **Siguiente**.

En la **Plantilla de certificado**, seleccione **Equipo** y, a continuación, haga clic en **Siguiente** y **Finalizar**.

Ahora es posible solicitar un certificado para **SRV-RTR**.

En **SRV-RTR**, abra una ventana de comandos DOS y, a continuación, escriba el comando `gpupdate /force`.

Escriba, a continuación, **mmc** y con ayuda de la opción **Agregar o quitar complemento** (menú **Archivo**) agregue **Certificados**.

Se abre un asistente, seleccione **Cuenta de equipo** y, a continuación, haga clic sucesivamente en **Siguiente**, **Finalizar** y, a continuación,**Aceptar**.

Despliegue los nodos **Certificados (este equipo)**, **Personal** y, por último, **Certificados**.

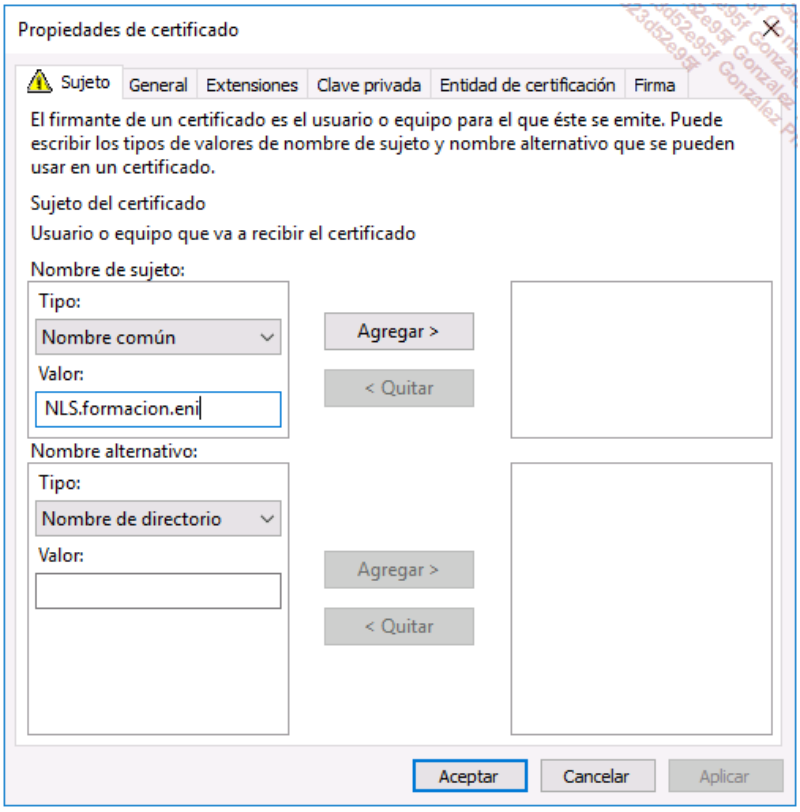
Haga clic con el botón derecho en **Certificados** y, a continuación, en el menú contextual seleccione **Todas las tareas** y, a continuación,**Solicitar un nuevo certificado**.

Haga clic dos veces en **Siguiente**. En la pantalla **Solicitar certificados** haga clic en **Certificado SRV Web Formación**.

Haga clic en **Se necesita más información para inscribir este certificado**.

Seleccione la pestaña **Objeto**, y, a continuación, seleccione **Nombre común** en la lista desplegable **Tipo**.

En el campo **Valor**, escriba **NLS.Formacion.eni** y, a continuación, haga clic en **Agregar**.



Haga clic en **Aceptar**, a continuación en **Inscribir** y, por último, **Finalizar**.

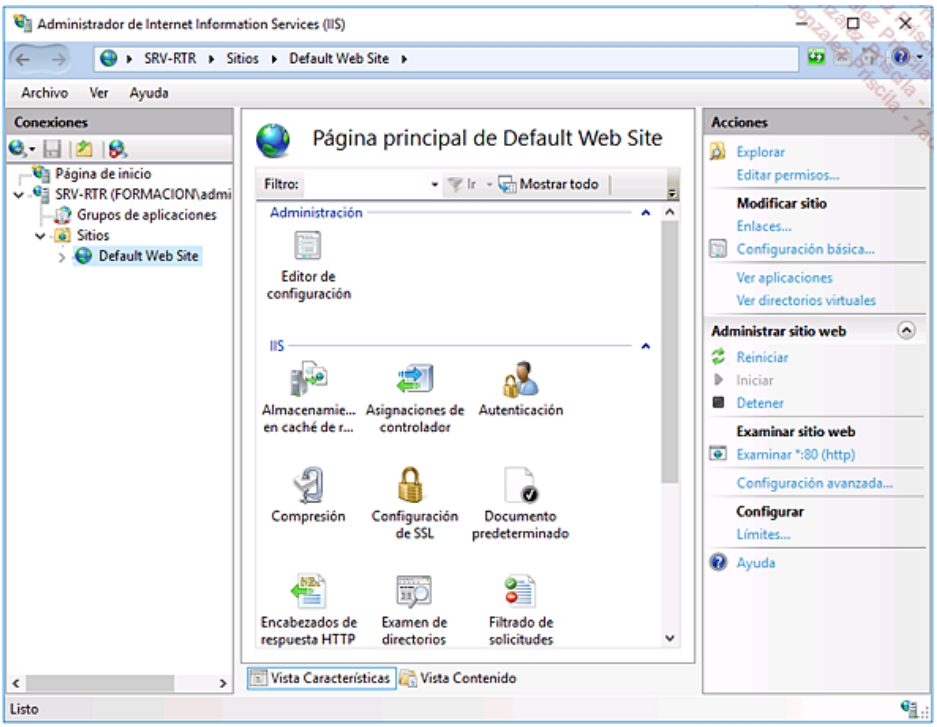
Aparece un nuevo certificado en la consola MMC.

Si no lo hubiera hecho, instale el rol **IIS** en **SRV-RTR**.

En **SRV-RTR**, abra la consola **Administración de Internet Information Services (IIS)**.

Haga clic en **Sitios** y, a continuación, en **Default Web Site**.

En el panel **Acciones**, haga clic en **Enlaces** y, a continuación, en **Agregar**.



En la lista desplegable **Tipo**, seleccione **HTTPS** y, a continuación, en **Certificado SSL** seleccione **NLS.Formacion.eni**.

Haga clic en **Aceptar** y, a continuación, en **Cerrar**.

Cierre la consola **Administrador de Internet Information Services (IIS)**.

Ya es posible configurar DirectAccess.

Abra una consola **MMC** y, a continuación, agregue el complemento **Certificados**.

Se abre un asistente, marque **Cuenta de equipo** y, a continuación, haga clic en **Siguiente**, **Finalizar** y, a continuación, **Aceptar**.

En el árbol que muestra la consola, despliegue los nodos **Certificados (equipo local)**, **Personal** y, por último, **Certificados**.

Haga clic con el botón derecho en **Certificados** y, a continuación, seleccione **Todas las tareas - Solicitar un nuevo certificado**.

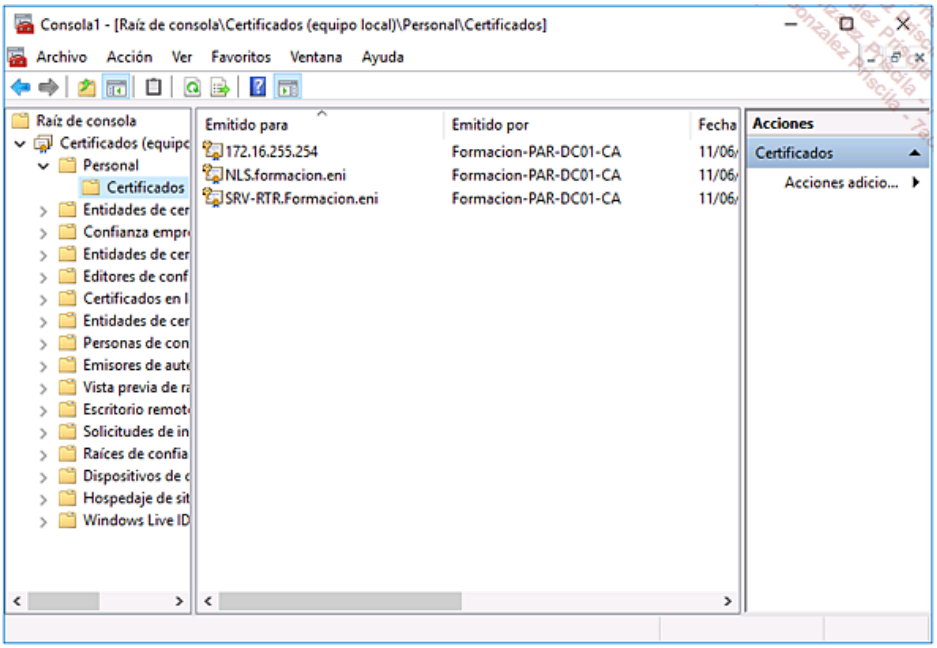
Haga clic dos veces en **Siguiente**, marque **Certificado SRV Web Formación** y, a continuación, haga clic en **Se necesita más información para inscribir este certificado**.

Seleccione **Nombre común** en la lista desplegable **Tipo** y, a continuación, escriba **172.16.255.254** en el campo **Valor**.

Haga clic en los botones **Agregar**, **Aceptar** y, a continuación, **Inscribir**.

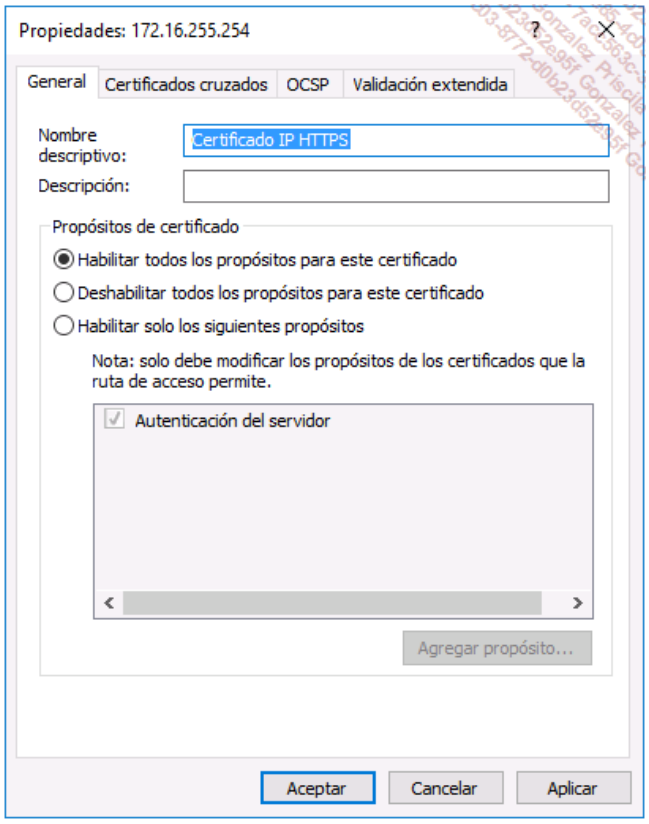
Haga clic en **Finalizar** para cerrar el asistente.

Ahora aparece un nuevo certificado en la consola MMC.



Haga clic con el botón derecho en el certificado que acaba de crear y, a continuación, en el menú contextual, seleccione **Propiedades**.

En el campo **Nombre descriptivo**, escriba **Certificado IP-HTTPS** y, a continuación, haga clic en **Aceptar**.



Cierre la consola **Certificados**.

A continuación, es posible crear el punto de distribución de CRL para certificados.

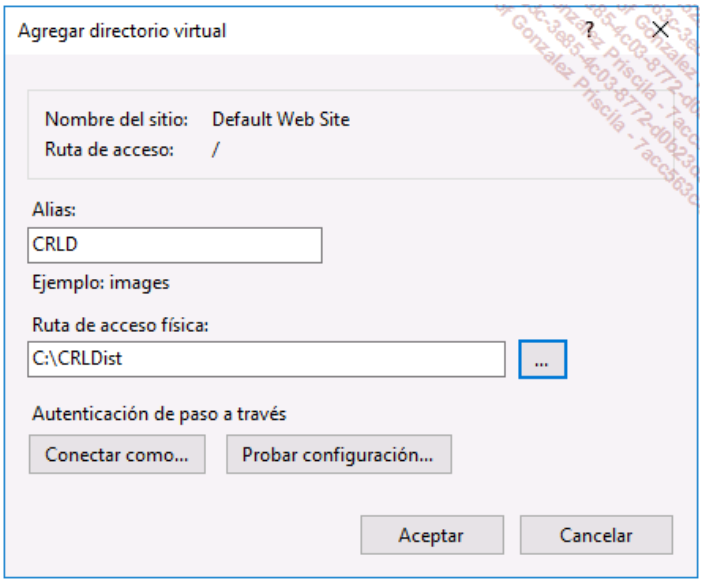
En **SRV-RTR**, abra la consola **Administrador de Internet Information Services (IIS)**.

Despliegue el nodo **Sitios** y, a continuación, haga clic con el botón derecho en **Default Web Site**. En el menú contextual, haga clic en**Agregar directorio virtual**.

En la ventana **Agregar directorio virtual**, escriba **CRLD** en el campo **Alias** y, a continuación, haga clic en el botón ... situado a la derecha del campo **Ruta de acceso física**.

Haga doble clic en **Disco local (C:)** y, a continuación, haga clic en el botón **Crear nueva carpeta**.

Escriba **CRLDist** y, a continuación, presione la tecla [Enter].



Haga clic dos veces en **Aceptar** para cerrar las ventanas.

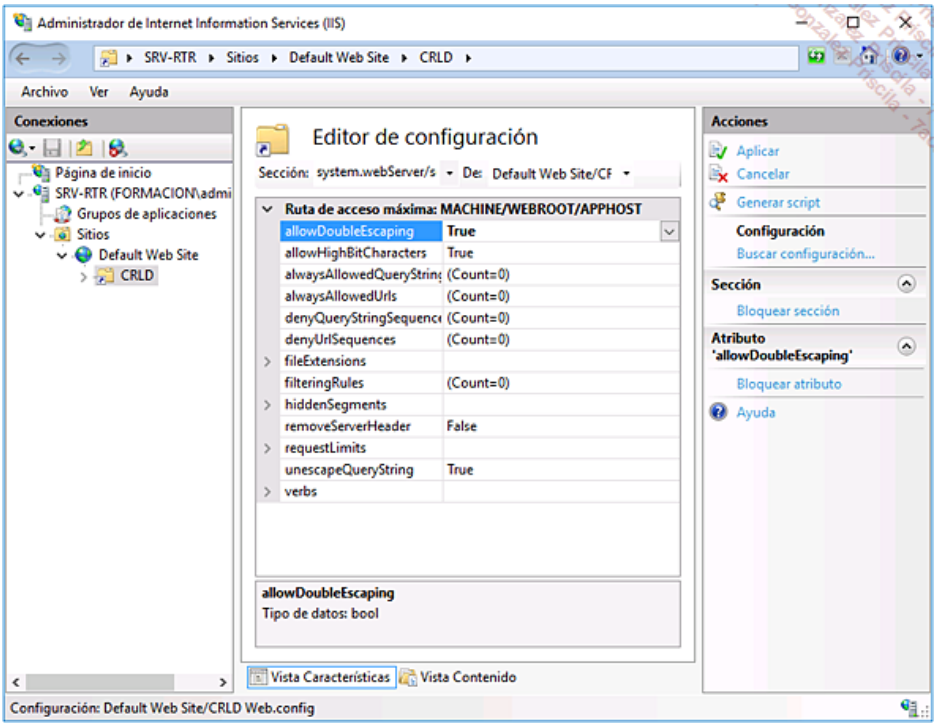
Haga doble clic en **Examen de directorios** en el panel central de la consola **Administrador de Internet Information Services (IIS)** y, a continuación, seleccione **Habilitar** en el panel **Acciones**.

Seleccione la carpeta **CRLD** y, a continuación, en el panel central de la consola, haga doble clic en el icono **Editor de configuración**.

En la lista desplegable **Sección**, despliegue **system.webServer**, **security**, y, a continuación, haga clic en **requestFiltering**.

En la lista desplegable **allowDoubleEscaping**, seleccione el valor **True**.

Haga clic en **Aplicar** en el panel de **Acciones**.



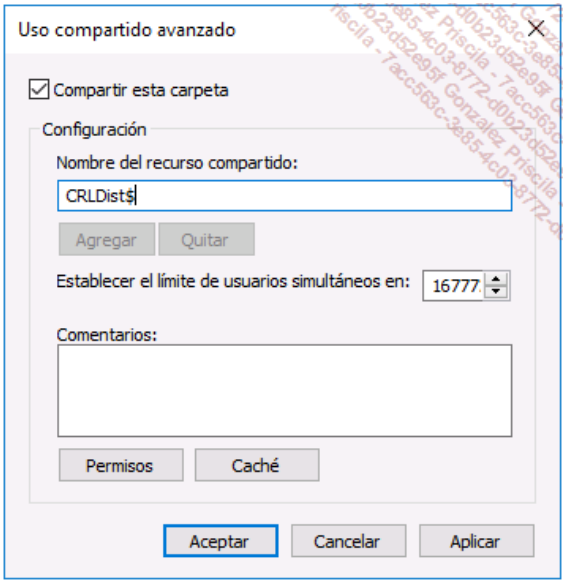
Es necesario compartir el punto de distribución de CRL.

Abra un explorador de Windows y, a continuación, haga doble clic en **Disco local (C:)**.

Haga clic con el botón derecho en la carpeta **CRLDist** y, a continuación, haga clic en **Propiedades**.

Seleccione la pestaña **Compartir** y, a continuación, haga clic en **Uso compartido avanzado**.

Marque la opción **Compartir esta carpeta** y, a continuación, agregue un **$** al final de la ruta.



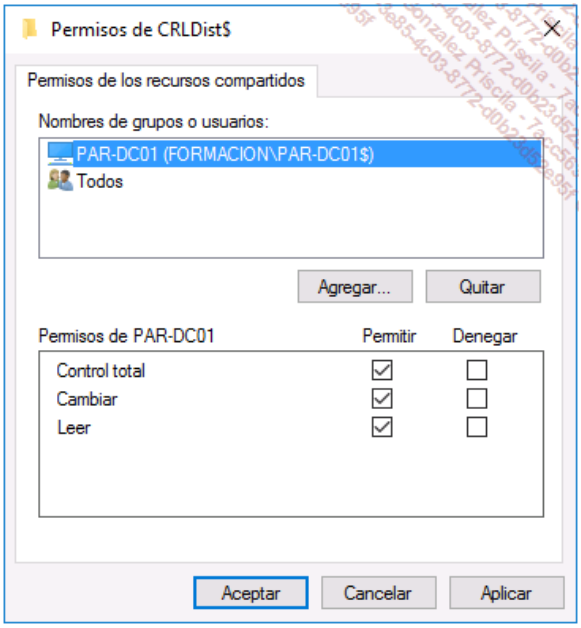
Haga clic en **Permisos** y, a continuación, en **Agregar**.

Haga clic en el botón **Tipos de objeto** y, a continuación, seleccione **Equipos**.

Haga clic en **Aceptar** y, a continuación, escriba **PAR-DC01** en el campo **Escriba los nombres de objeto que desea seleccionar**.

Haga clic en **Comprobar nombres** y, a continuación, en **Aceptar**.

Seleccione **PAR-DC01** y, a continuación, marque **Control total** en la columna **Permitir**.



Haga clic dos veces en **Aceptar** y, a continuación, seleccione la pestaña **Seguridad**.

Haga clic en el botón **Editar** y, a continuación, en **Agregar**.

Haga clic en el botón **Tipos de objeto** y, a continuación, seleccione **Equipos**.

Haga clic en **Aceptar** y, a continuación, escriba **PAR-DC01** en el campo **Escriba los nombres de objeto que desea seleccionar**.

Haga clic en **Comprobar nombres** y, a continuación, en **Aceptar**.

Seleccione **PAR-DC01** y, a continuación, marque **Control total** en la columna **Permitir**.

Ahora es momento de publicar la lista de revocación de certificados.

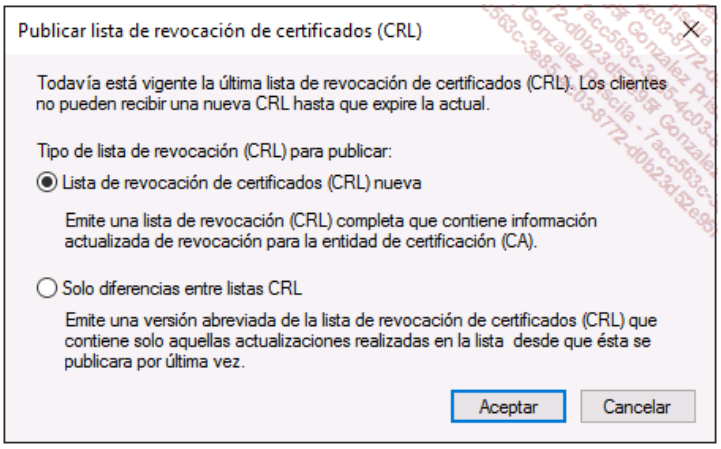
En **PAR-DC01**, abra la consola **Entidad de certificación**.

Despliegue el nodo **Formacion-PAR-DC01-CA** y, a continuación, haga clic con el botón de derecho en **Certificados revocados**.

En el menú contextual, seleccione **Todas las tareas** y, a continuación, **Publicar**.

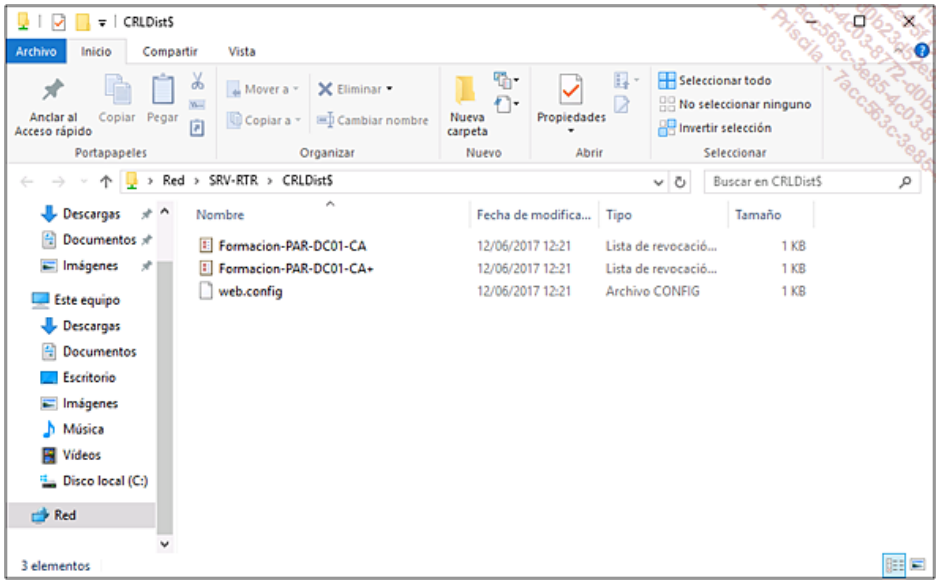
Marque la opción **Lista de revocación de certificados (CRL) nueva** en el cuadro de diálogo **Publicar lista de revocación de certificados**

(CRL).



Valide haciendo clic en **Aceptar**.

Acceda al recurso compartido **\\SRV-RTR\CRLDist$** y compruebe la presencia de los archivos.



A continuación, es posible configurar DirectAccess.

Si no lo hubiera hecho, instale el rol **Acceso remoto** en **SRV-RTR**.

Configure la segunda tarjeta de red en el servidor **SRV-RTR** (con dirección IP 172.17.255.254) para que tenga la dirección IP 131.0.0.1 y la máscara de subred 255.255.0.0.

La tarjeta de red debe estar conectada a un conmutador diferente al utilizado por la primera tarjeta de red (un conmutador de tipo privado, por ejemplo).

En **SRV-RTR**, abra la consola **Enrutamiento y acceso remoto**.

Compruebe que **SRV-RTR** está deshabilitado, en caso contrario haga clic con el botón derecho en **SRV-RTR (local)** y seleccione**Deshabilitar enrutamiento y acceso remoto**.

Desde el **Administrador del servidor** haga clic en **SRV-RTR** y, a continuación, haga clic con el botón derecho en **SRV-RTR** y abra la consola **Administración del acceso remoto**.

Haga clic en **Configuración** en el panel izquierdo. A continuación, haga clic en **Ejecutar el asistente para introducción** en el panel central.

Se abre un asistente, ejecute **Implementar solo DirectAccess**.

Verifique que está marcada la opción **Tras un dispositivo perimetral (con dos tarjetas de red)** y, a continuación, escriba **131.0.0.1** en el campo de texto.

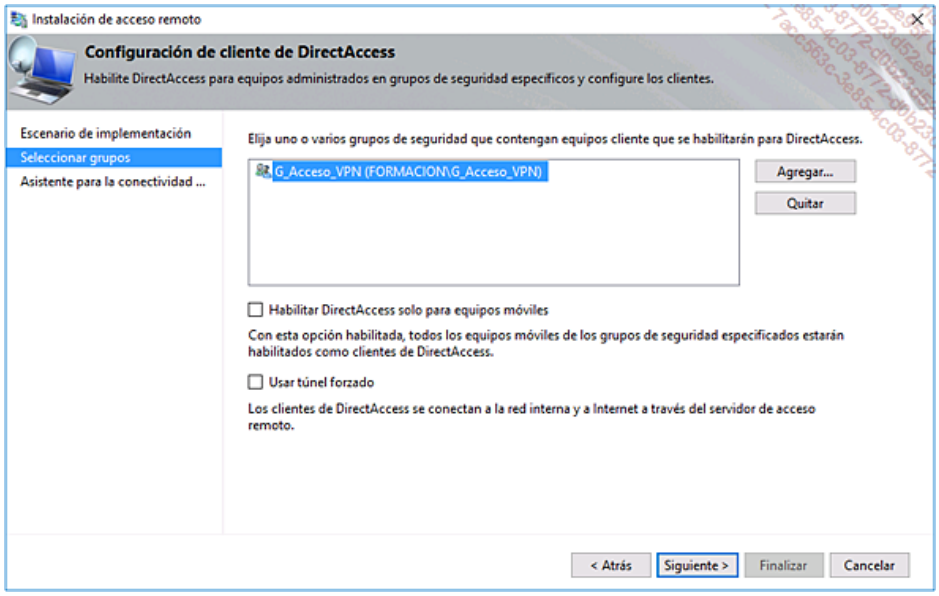
Haga clic en **Siguiente** y, a continuación, en **Finalizar**.

En la consola **Administración de acceso remoto**, en **Etapa 1**, haga clic en **Editar**, y, a continuación, en **Siguiente**.

En la ventana de selección de grupos, haga clic en **Agregar**.

Escriba **G_Acceso_VPN** y, a continuación, haga clic en **Aceptar**.

Desmarque la opción **Habilitar DirectAccess solo para equipos móviles** y, a continuación, elimine el grupo **Equipos del dominio**.



Haga clic en **Siguiente** y, a continuación, en **Finalizar**.

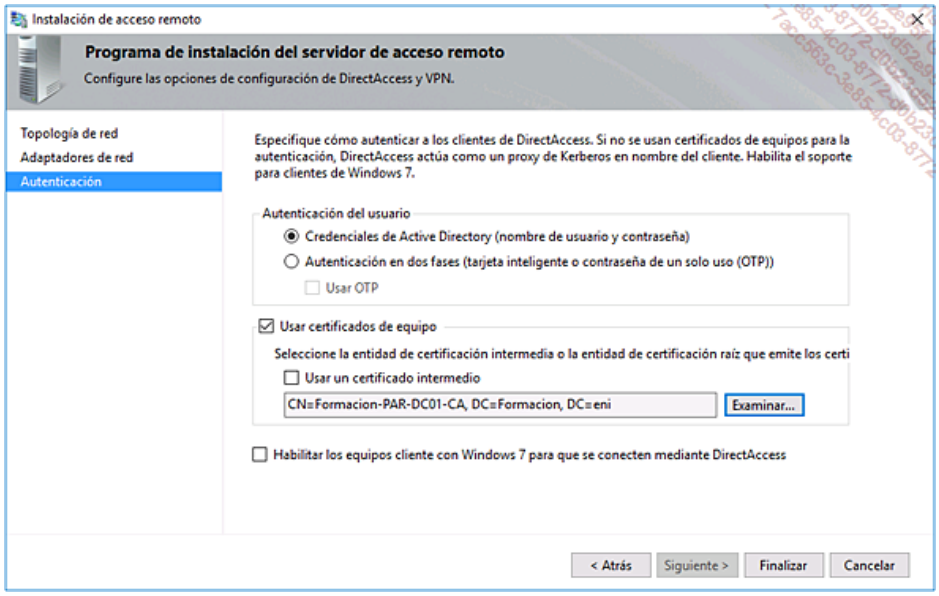
En la consola **Administración de acceso remoto**, en **Etapa 2**, haga clic en **Editar**.

Haga clic en **Siguiente** y, a continuación, compruebe que se está utilizando la tarjeta Ethernet correcta.

Valide la información haciendo clic en **Siguiente**.

Haga clic en el botón **Examinar** presente en la zona **Usar certificados de equipo**.

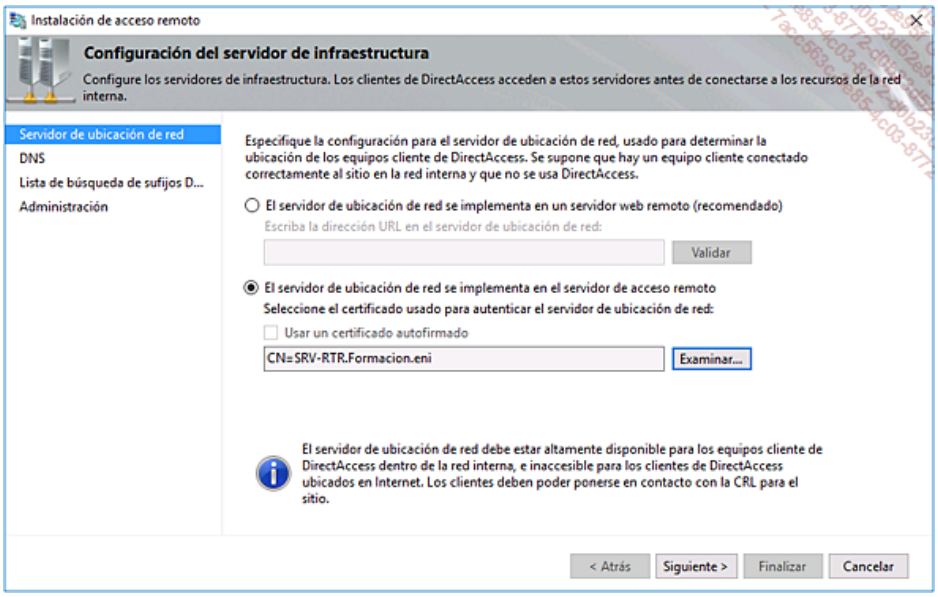
Seleccione **Formacion-PAR-DC01-CA** y, a continuación, haga clic en **Aceptar**.



Haga clic en **Finalizar**.

En la consola **Administración de acceso remoto**, haga clic en el enlace **Editar** presente en la **Etapa 3**.

En la ventana **Servidor de ubicación de red**, marque la opción **El servidor de ubicación de red se implementa en el servidor de acceso remoto**. Con ayuda del botón **Examinar**, seleccione el certificado **SRV-RTR**.



Haga clic tres veces en **Siguiente** y, a continuación, en **Finalizar**.

En la consola **Administración de acceso remoto**, haga clic en el enlace **Editar** presente en la **Etapa 4**.

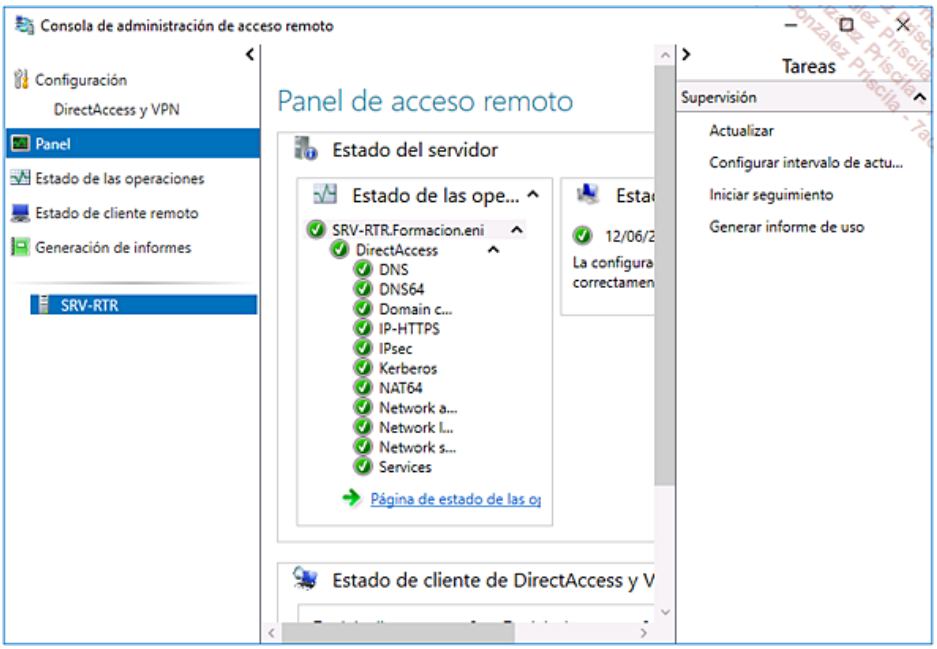
En la pantalla **Instalación del servidor de aplicaciones DirectAccess**, haga clic en **Finalizar**.

Aplique los cambios haciendo clic en **Finalizar** en la consola **Administración de acceso remoto** y, a continuación, en **Aplicar** en la ventana emergente.

Una vez finalizada la operación, haga clic en **Cerrar**.

En **SRV-RTR**, abra una ventana de comandos DOS y, a continuación, ejecute el comando `gpupdate /force`.

Haga clic en **Panel** en la **Consola de administración de acceso remoto**.



4. Configuración del cliente DirectAccess

Objetivo: configuración de la funcionalidad DirectAccess

Máquinas virtuales: PAR-DC01, SRV-RTR y CL10-02.

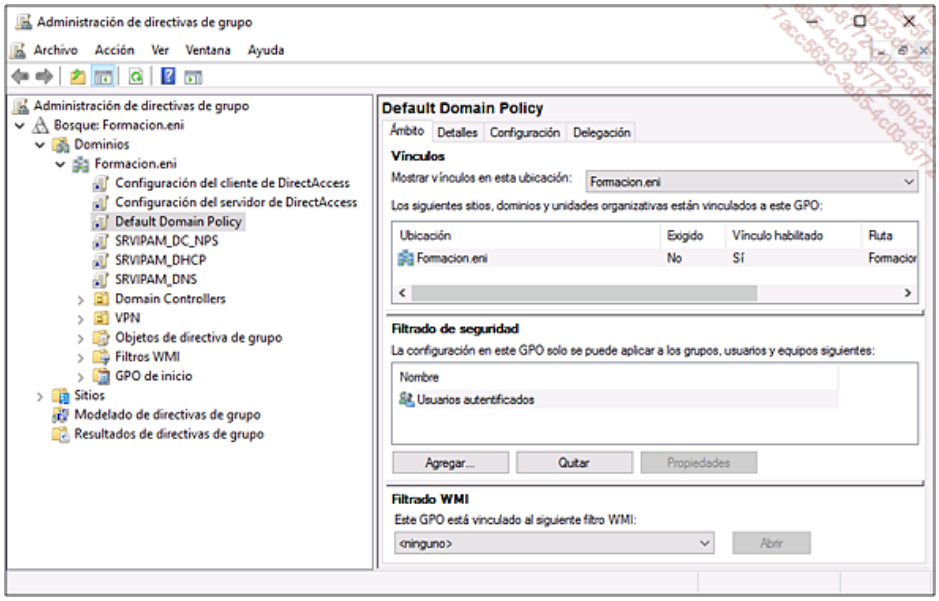
En **CL10-02**, inicie una sesión como administrador (administrador@formacion.eni).

Abra una ventana de comandos DOS y, a continuación, ejecute el comando `gpupdate /force`.

Compruebe que CL10-02 está configurado con direccionamiento dinámico y ubicado sobre el mismo conmutador virtual que PAR-DC01.

Compruebe que se esté aplicando la directiva de grupo **Configuración del cliente DirectAccess**.

Esta GPO se ha creado automáticamente.

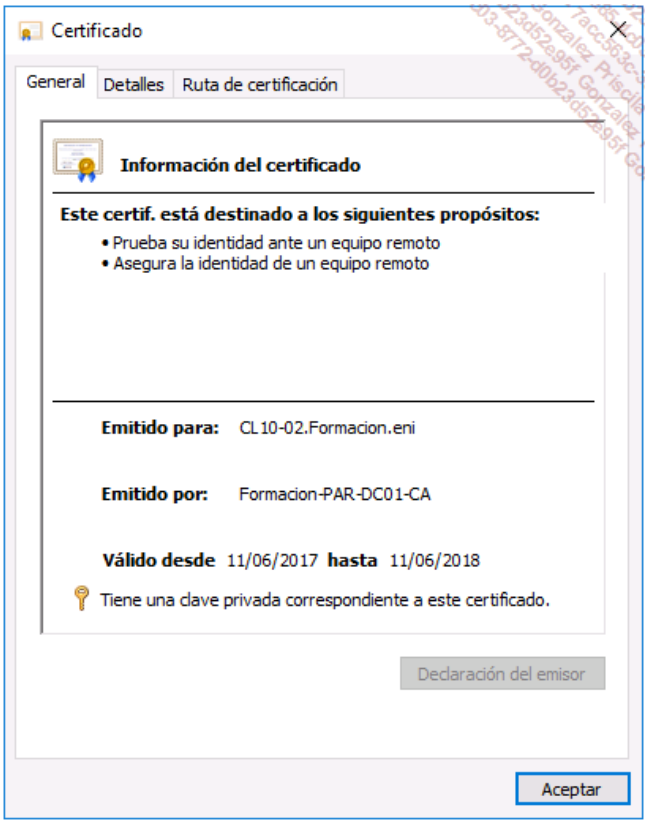


En **CL10-02**, abra una consola MMC y, a continuación, agregue el complemento **Certificados**.

En el asistente, seleccione la opción **Cuenta de equipo**, a continuación haga clic en **Siguiente** y en **Finalizar**.

Despliegue los nodos **Certificados**, **Personal** y, por último, **Certificados**.

Compruebe que existe un certificado con el nombre **CL10-02.Formacion.eni** con el rol **Asegura la identidad de un equipo remoto**.



El certificado es necesario para identificar la máquina instalada.

Abra un navegador de Internet y, a continuación, acceda a la URL: **http://SRV-RTR.Formacion.eni**.

Esta operación permite comprobar la conectividad con el servidor de la empresa. La estación **CL10-02** debe utilizar el mismo conmutador que**SRV-RTR** para estar conectada a la red 131.0.0.0. Para ello, configure el mismo conmutador virtual que para **SRV-RTR**.

Edite la configuración de la tarjeta de red de **CL10-02** para que esté configurada tal y como se indica más abajo. A continuación, cambie el conmutador virtual.

- **Dirección IP**: 131.0.0.2
- **Máscara de subred**: 255.255.0.0
- **Puerta de enlace predeterminada**: 131.0.0.1
- **Servidor DNS primario**: 131.0.0.1

En **Internet Explorer**, elimine la información en caché (archivos temporales, etc.).

Esto permite asegurar que el acceso funciona y que la página no se muestra porque está alojada en la caché local del equipo.

Abra un navegador de Internet y, a continuación, acceda a la URL: **http://SRV-RTR.Formacion.eni**.

La página se muestra.

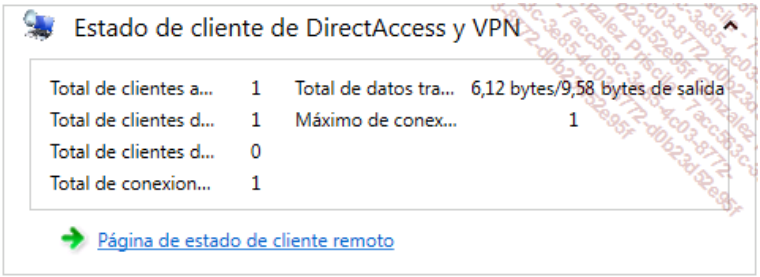
Abra una ventana de comandos DOS y, a continuación, ejecute el comando: `ping SRV-RTR.formacion.eni`

Se devuelve una respuesta.

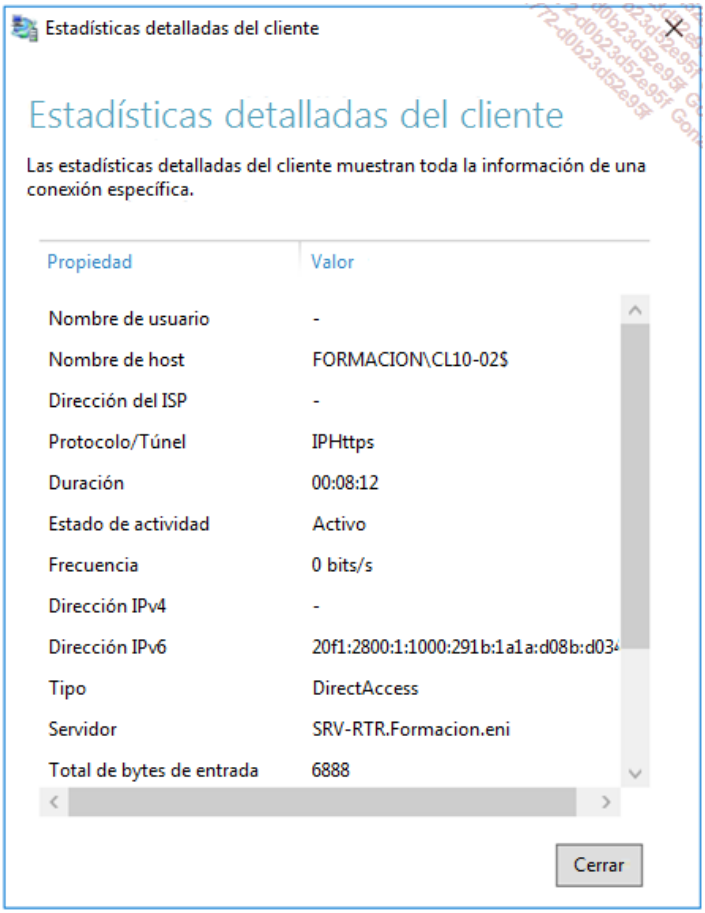
Escriba el comando `netsh name show effectivepolicy` para comprobar la configuración de la tabla de directivas de resolución de nombres DNS.

Abra una consola **PowerShell** y, a continuación, escriba el comando `Get-DAClientExperienceConfiguration`.

En la máquina **PAR-DC01**, en la **Consola de administración de acceso remoto**, seleccione **Panel** y, a continuación, observe la presencia de un cliente DirectAccess.



Haga clic en **Estado de cliente remoto** y, a continuación, doble clic en **FORMACION\CL10-02$** y observe las estadísticas detalladas.


Estadísticas detalladas del cliente
Estadísticas detalladas del cliente
Las estadísticas detalladas del cliente muestran toda la información de una conexión específica.
Propiedad
Valor
Nombre de usuario
-
Nombre de host
FORMACION\CL10-02$
Dirección del ISP
-
Protocolo/Túnel
IPHttps
Duración
00:08:12
Estado de actividad
Activo
Frecuencia
0 bits/s
Dirección IPv4
-
Dirección IPv6
20f1:2800:1:1000:291b:1a1a:d08b:d03
Tipo
DirectAccess
Servidor
SRV-RTR.Formacion.eni
Total de bytes de entrada
6888
Cerrar

Validación de conocimientos adquiridos: preguntas/respuestas

1. Preguntas

Puede validar los conocimientos adquiridos respondiendo a las siguientes preguntas.

1. ¿Cuál es el rol de un servidor VPN?
2. ¿Qué permite hacer el rol Servicios de acceso y directivas de redes?
3. ¿Cuál es la misión de un servidor RADIUS?
4. ¿Cuáles son las dos tecnologías que es posible implementar con el rol Acceso remoto?
5. ¿Cuál es la diferencia entre la autenticación y la autorización?
6. Nombre algunos métodos de autenticación.
7. ¿Por qué conviene implementar una PKI?
8. ¿Qué dos formas existen de distribuir una configuración IP?
9. ¿Cuál es la ventaja de utilizar SSTP?
10. Presente brevemente la funcionalidad VPN Reconnect.
11. ¿Por qué conviene utilizar un kit CMAK?
12. Nombre alguna de las ventajas ofrecidas por DirectAccess.
13. ¿Es necesario disponer de dos direcciones IP y una PKI para implementar DirectAccess?
14. Tras implementar un servidor RADIUS es preciso configurar, también, el cliente RADIUS. ¿Qué elementos pueden utilizarse como cliente RADIUS?
15. NPS realiza autenticación, ¿dónde se almacenan las cuentas (equipo, usuario…) que permiten realizar la autenticación?
16. ¿Qué número tiene la norma RADIUS?
17. ¿Qué contiene una directiva de solicitud de conexión?
18. ¿Cuál es la utilidad de un proxy RADIUS?

2. Resultados

Consulte las siguientes páginas para comprobar sus respuestas.

Por cada respuesta correcta, cuente un punto.

Número de puntos: /18

Para superar este capítulo, su puntuación mínima debería ser de 13 sobre 18.

3. Respuestas

1. ¿Cuál es el rol de un servidor VPN?

   El rol del servidor VPN es crear un túnel seguro entre un equipo y el servidor en el interior de una red pública (Internet).

2. ¿Qué permite hacer el rol Servicios de acceso y directivas de redes?

   Este rol permite tener los componentes necesarios para asegurar el correcto funcionamiento de la conectividad de red.

3. ¿Cuál es la misión de un servidor RADIUS?

   Un servidor RADIUS permite dotar de seguridad una red Wi-Fi o una VPN realizando una autenticación basada en un certificado o contraseña.

4. ¿Cuáles son las dos tecnologías que es posible implementar con el rol Acceso remoto?

   El rol Acceso remoto ofrece la posibilidad de implementar un acceso VPN tradicional o un servidor DirectAccess.

5. ¿Cuál es la diferencia entre la autenticación y la autorización?

   La autenticación es una operación que consiste en verificar las credenciales utilizadas mientras que una autorización permite, por su parte, comprobar si la cuenta está autorizada o no para acceder a un determinado recurso.

6. Nombre algunos métodos de autenticación.

   Es posible utilizar varios métodos de autenticación (PAP, CHAP, MS-CHAPv2, EAP…).

7. ¿Por qué conviene implementar una PKI?

   Una PKI o Public Key Infrastructure consiste en implementar un servidor que permite distribuir y gestionar certificados digitales. Esta solución permite asegurar los datos.

8. ¿Qué dos formas existen de distribuir una configuración IP?

Cuando se implementa una conexión VPN es necesario distribuir una configuración IP a los equipos. Para ello, puede utilizarse un servidor DHCP. La segunda manera consiste en configurar, en el servidor VPN, un pool de direcciones remotas.

9 ¿Cuál es la ventaja de utilizar SSTP?

El protocolo SSTP es, como L2TP o PPTP, un protocolo que permite implementar un túnel VPN. Este protocolo tiene una ventaja importante: utiliza HTTPS y, por tanto, el puerto 443. De este modo resulta más fácil atravesar los cortafuegos.

10 Presente brevemente la funcionalidad VPN Reconnect.

VPN Reconnect es una funcionalidad que consiste en restablecer la conexión VPN en caso de corte. De este modo, el usuario no tiene que volver a conectar manualmente.

11 ¿Por qué conviene utilizar un kit CMAK?

Un kit CMAK contiene la configuración esencial para realizar una conexión VPN, de modo que el usuario no tenga más que informar las credenciales.

12 Nombre alguna de las ventajas ofrecidas por DirectAccess.

Es posible citar varias ventajas, tales como la conexión sin intervención por parte del usuario, la integración en el sistema operativo o, simplemente, la separación de los tráficos de Internet e intranet.

13 ¿Es necesario disponer de dos direcciones IP y una PKI para implementar DirectAccess?

No, desde Windows Server 2012 ya no es necesario instalar una PKI o disponer de dos direcciones IPv4 consecutivas.

14 Tras implementar un servidor RADIUS es preciso configurar, también, el cliente RADIUS. ¿Qué elementos pueden utilizarse como cliente RADIUS?

Un servidor VPN, un conmutador o un punto de acceso Wi-Fi son equipos que pueden configurarse como cliente RADIUS.

15 NPS realiza autenticación, ¿dónde se almacenan las cuentas (equipo, usuario…) que permiten realizar la autenticación?

Estas cuentas pueden provenir de una base de datos local o, con mayor frecuencia, de un directorio Active Diretory.

16 ¿Qué número tiene la norma RADIUS?

El número de la norma RADIUS es 802.1x.

17 ¿Qué contiene una directiva de solicitud de conexión?

Una solicitud de conexión contiene condiciones pero, también, parámetros (información de servidor RADIUS, etc.).

18 ¿Cuál es la utilidad de un proxy RADIUS?

Un proxy RADIUS se utiliza con varios roles (AD FS, etc.) y permite asegurar que solo las personas autorizadas pueden acceder a la aplicación.

Requisitos previos y objetivos

1. Requisitos previos

Poseer nociones acerca de la administración del sistema.

2. Objetivos

Instalar y configurar un espacio de nombres DFS.

Instalar y configurar Branchcache.

Introducción

El sistema de archivos es uno de los aspectos esenciales en una empresa, que evoluciona de manera cotidiana. Mal administrado, este sistema puede volverse, rápidamente, indomable.

El sistema DFS

DFS es un sistema que facilita la administración de un sistema de archivos. Ofrece, a la empresa, una tolerancia a fallos redirigiendo a los usuarios a otro servidor en caso de producirse algún error. El acceso a un recurso compartido se realiza, obligatoriamente, mediante una ruta UNC (*NombreDeServidor**NombreDeRecursoCompartido*). En caso de remplazar un servidor de archivos es necesario proceder a la actualización de todos los nombres. Esta etapa puede resultar, en ciertos casos, muy costosa. Un espacio de nombres DFS permite, en tal caso, facilitar la tarea del administrador, pues la ruta UNC no contiene el nombre del servidor afectado. La replicación DFS complementa a la solución replicando los datos en otros servidores. De este modo, se asegura la tolerancia a fallos.

Tras la instalación del rol DFS es posible seleccionar dos servicios de rol.

- **Espacio de nombres o DFS-N**: permite instalar la consola y las herramientas necesarias para la administración del espacio de nombres.
- **Replicación DFS o DFS-R**: instala un motor de replicación multimaestro que permite replicar las distintas carpetas contenidas en el espacio de nombres. La replicación puede planificarse con un uso del ancho de banda distinto en función de la hora. Además, es posible implementar la compresión diferencial remota para replicar únicamente la parte de un archivo que se haya modificado desde la última replicación. La replicación no está, obligatoriamente, vinculada con el espacio de nombres, por lo que puede funcionar de manera autónoma sin problema alguno.

1. Presentación del espacio de nombres DFS

Un espacio de nombres simplifica la gestión de un sistema de archivos representando, de manera virtual, los recursos compartidos de red. Este espacio de nombres puede ser de tipo autónomo o estar basado en un dominio (se apoya, en tal caso, en Active Directory).

Espacio basado en un dominio

Este tipo de espacio de nombres simplifica la alta disponibilidad. En efecto, no es necesario *clusterizar* los servidores con este tipo de espacio de nombres. La ruta UNC está compuesta por un nombre de dominio Active Directory más el nombre del espacio de nombres (por ejemplo: \\Formacion.local\DocsFormacion).

Existen dos modelos disponibles: Windows 2000 o Windows Server 2008, este último ofrece la posibilidad de utilizar ABE (*Access Based Enumeration*, enumeración basada en el acceso) así como de aumentar el número de destinos de la carpeta (posibilidad de tener hasta 50.000 destinos de carpeta). ABE ofrece la ventana de mostrar únicamente las carpetas a las que el usuario tiene acceso.

No obstante, la selección del modo Windows Server 2008 supone respetar los siguientes requisitos previos:

- Nivel funcional del bosque igual a Windows Server 2003 o superior.
- Nivel funcional del dominio igual a Windows Server 2008.
- Todos los servidores de espacios de nombres deben ejecutar Windows Server 2008.

Espacio de nombres autónomo

Este tipo de espacio de nombres se utiliza, por lo general, cuando la empresa no posee un dominio Active Directory. La alta disponibilidad se asegura mediante un clúster de conmutación por error.

2. La replicación DFS

La replicación DFS es un mecanismo que permite replicar las distintas carpetas sobre uno o varios servidores. Este tipo de replicación ofrece la ventaja de utilizar la compresión diferencial remota, que es un protocolo de tipo cliente-servidor que permite la detección de las modificaciones (agregar/quitar/modificar) operadas sobre un archivo con el objetivo de replicar únicamente este bloque de datos modificados. Este protocolo se utiliza en archivos con un tamaño mínimo de 64 KB.

Tras la replicación, se crea una carpeta intermedia, con una copia comprimida del archivo, y a continuación se envía el archivo. El servidor que recibe los datos almacena, a su vez, el archivo en una carpeta intermedia. Cuando se termina la descarga el archivo se descomprime y, a continuación, se ubica en la carpeta adecuada. Estas carpetas temporales están presentes, por lo general, en DFSrPrivate\Staging.

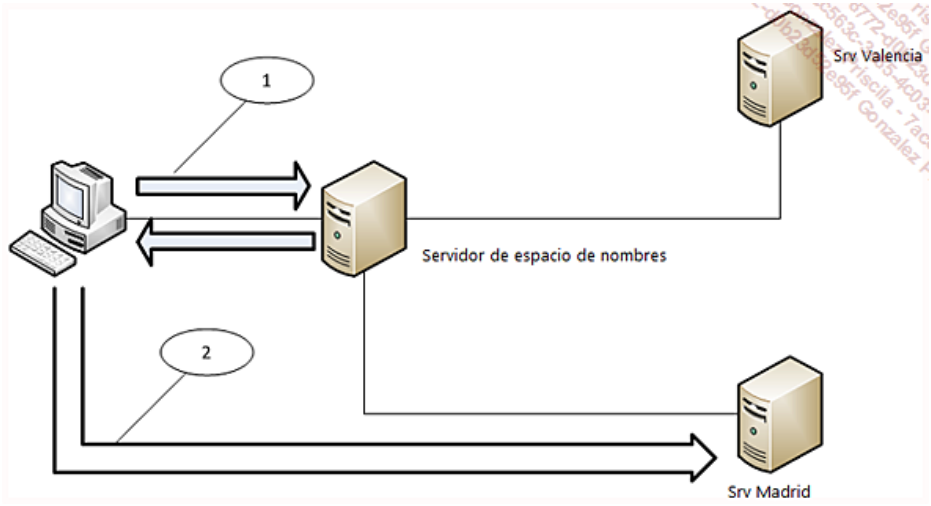
En caso de producirse algún conflicto en la replicación, la persona que ha realizado la última modificación aporta los cambios. Si el conflicto afecta al nombre del archivo, el primer usuario que realiza la modificación aporta los cambios. Se produce una copia de los archivos que han "perdido en la resolución del conflicto" en la ruta DFSrPrivate\ConflictandDeleted.

3. Funcionamiento del espacio de nombres

Para facilitar la compresión del funcionamiento del espacio de nombres, vamos a estudiar un ejemplo.

Un usuario llamado Nicolás trabaja en la sede de la empresa Formacion. La empresa está compuesta por una sede social en Madrid así como una agencia en Valencia. Los usuarios utilizan el espacio de nombres para acceder a los distintos recursos compartidos.

El equipo cliente del usuario contacta al servidor del espacio de nombres (1) que le envía una lista ordenada (en función de los criterios configurados por los administradores) de los servidores que contienen carpetas compartidas (destinos de carpeta) a los que el usuario puede acceder. El equipo cliente intenta acceder al primer servidor (2) de la lista (los demás se contactan únicamente si el primer servidor está en fuera de servicio).



En la etapa 2, el usuario tiene la posibilidad de acceder a los demás servidores puesto que se ha implementado la replicación entre los dos servidores.

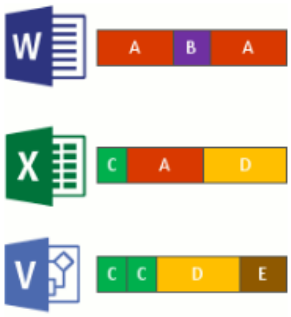
4. La desduplicación de datos

Windows Server 2012 R2 ofrece la posibilidad de habilitar la desduplicación de datos. Esta funcionalidad no puede utilizarse en una partición de sistema. El objetivo de esta funcionalidad es optimizar el espacio de disco. De este modo, un bloque idéntico en varios archivos se almacena una única vez.

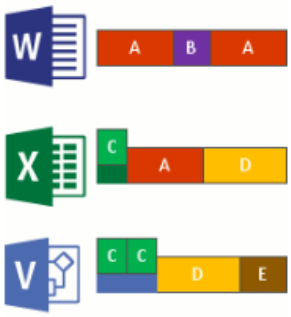
Principio de funcionamiento de la desduplicación:

- **Análisis de los archivos en el volumen**: el sistema analiza los archivos en la partición.

- **Segmenta los archivos en trozos de tamaño variable**:



- **Identificación de los bloques idénticos**:



- **Ordenación y compresión**: los bloques de tamaño variable se agrupan y comprimen en función de su tamaño.

- **Reemplazo del flujo de archivos**: los archivos se reemplazan por un vínculo entre los distintos bloques que componen un archivo y el volumen de almacenamiento de los bloques variables.

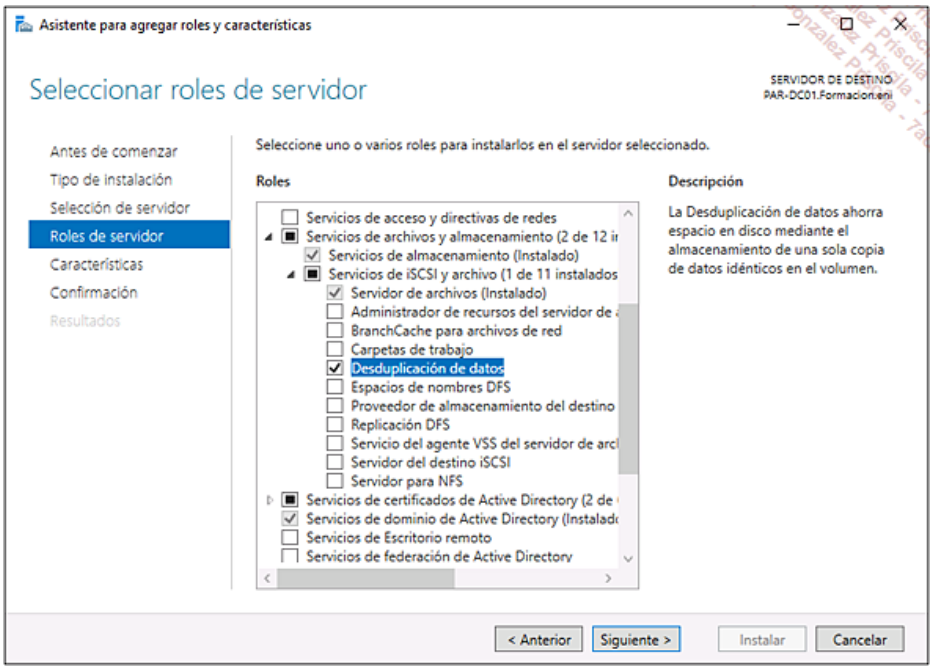
El rol de desduplicación presenta diversos parámetros de configuración en función del tipo de archivo que se quiera optimizar.

Tipo de configuración	Tipo de trabajo	Funcionamiento
Default	Servidor de archivos • Carpetas de trabajo • Redirección del perfil • Recursos compartidos de archivos orientados al desarrollo	• Optimización en segundo plano • Parámetros por defecto: ▪ Edad mínima de los archivos = 3 días ▪ Optimización de los archivos en uso = No ▪ Optimización de los archivos parciales = No
Hyper-V	Virtualización del puesto de trabajo (VDI)	• Optimización en segundo plano • Parámetros por defecto: ▪ Edad mínima de los archivos = 3 días ▪ Optimización de los archivos en uso = Sí ▪ Optimización de los archivos parciales = Sí • Optimización interna por Hyper-V
Copia de seguridad	Copias de seguridad de las aplicaciones	• Prioridad a la optimización • Parámetros por defecto: ▪ Edad mínima de los archivos = 0 días ▪ Optimización de los archivos en uso = Sí ▪ Optimización de los archivos parciales = No • Optimización interna por Hyper-V y compatibilidad con DPM

La desduplicación de datos ofrece varias ventajas, entre ellas la optimización del espacio en disco, cuyo consumo se ve reducido.

La primera etapa de la implementación es la instalación de la funcionalidad. Ésta puede realizarse mediante la consola **Administrador del servidor**.

En esta consola, haga clic en el enlace **Agregar roles y características** y, a continuación, seleccione el servicio de rol **Desduplicación de datos**.



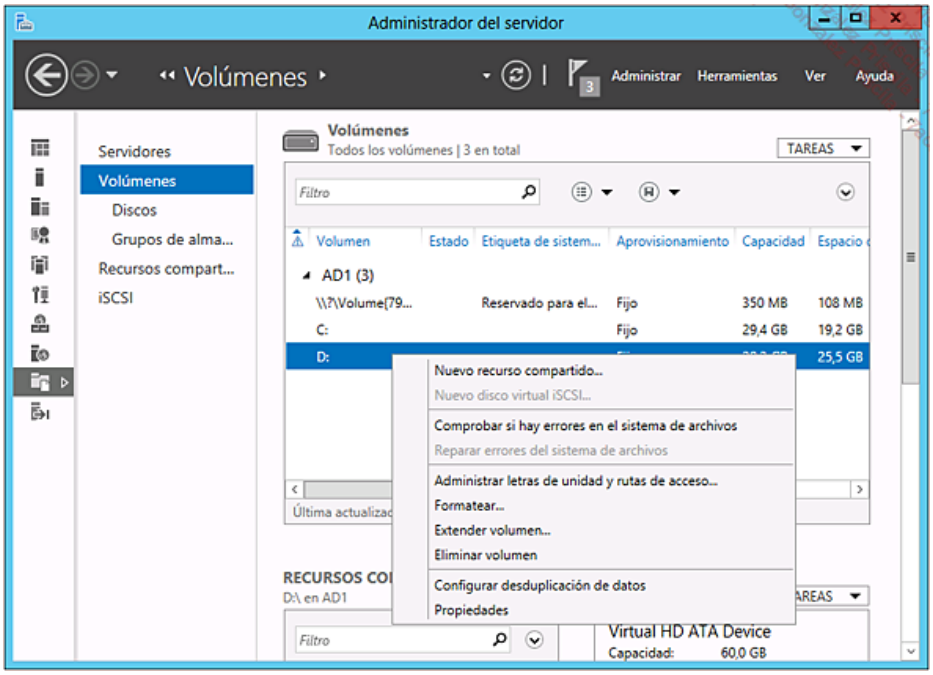
Es, a su vez, posible realizar la instalación mediante el comando PowerShell:

```
Import-Module ServerManager
Add-WindowsFeature -name FS-Data-Deduplication
Import-Module Deduplication
```

A continuación, es necesario habilitar la funcionalidad en el volumen deseado. Esta etapa puede realizarse mediante la interfaz gráfica.

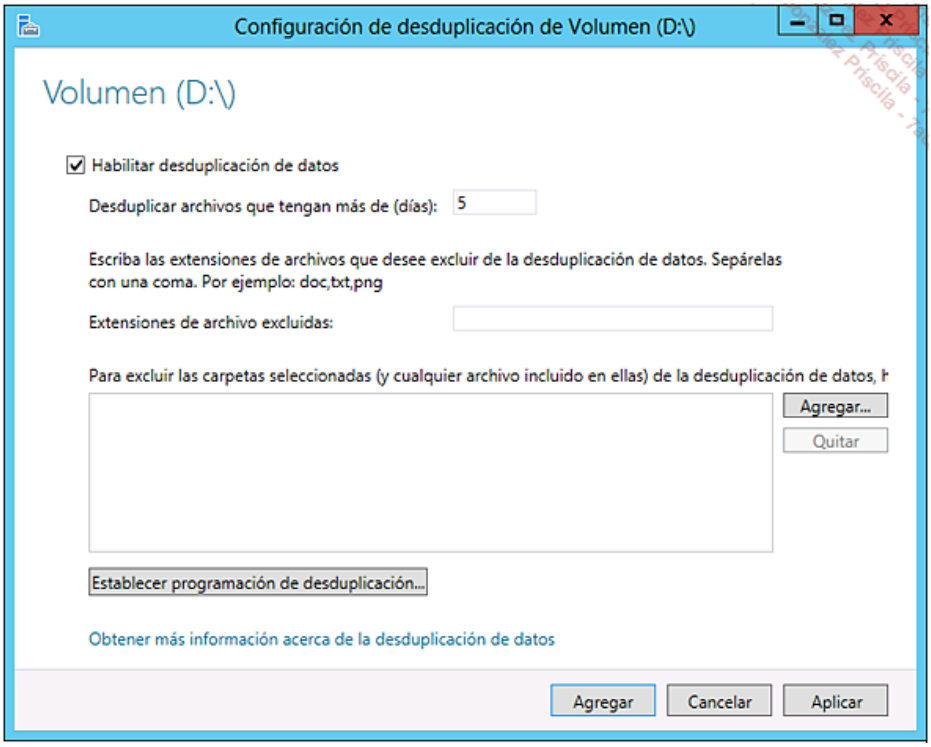
En el **Panel**, seleccione **Servicios de archivos y almacenamiento**.

Seleccione **Volúmenes** y, a continuación, haga clic con el botón derecho en el volumen deseado (todos, salvo el volumen del sistema).



Haga clic en **Configurar desduplicación de datos**.

Marque la opción **Habilitar desduplicación de datos** y, a continuación, configure las opciones como desee.



Como con la instalación, la etapa de activación puede realizarse por línea de comandos:

```
Enable-DedupVolume D:
```

Con Windows server 2016 se han aportado muchas mejoras a la desduplicación:

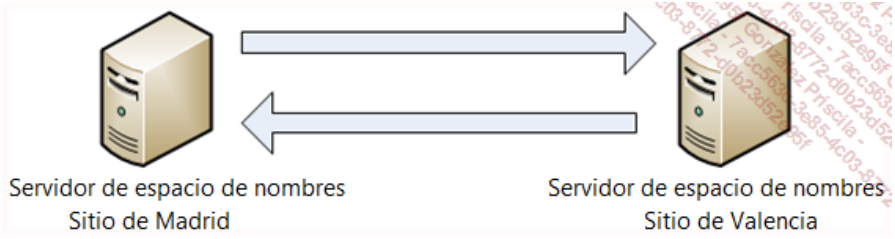
- El tamaño de los volúmenes se ha aumentado hasta los 64 TB frente a los 10 TB de Windows Server 2012 R2.
- En Windows Server 2012 R2, el pipeline de uso de la desduplicación de datos utiliza un thread único y una fila de espera de E/S para cada volumen. Esta nueva versión permite ejecutar varios threads en paralelo mediante varias filas de espera de E/S para cada volumen, alcanzando rendimientos que antes no eran posibles salvo dividiendo los datos en varios volúmenes de menor tamaño.
- En Windows Server 2012 R2, los archivos muy voluminosos no son buenos candidatos a la desduplicación de datos debido a una disminución en el rendimiento del pipeline de procesamiento de la desduplicación. En Windows Server 2016, la desduplicación de archivos de hasta 1 TB se desarrolla con muy buen rendimiento, lo que permite a los administradores, por ejemplo, duplicar archivos muy voluminosos ejecutando tareas de copia de seguridad.
- Nano Server es una nueva opción de despliegue sin interfaz gráfica que necesita muy pocos recursos del sistema, arranca considerablemente más rápido y requiere menos actualizaciones y reinicios que un servidor Core. La desduplicación de los datos está completamente soportada en los servidores Nano.
- El soporte de Cluster OS Rolling Upgrade para los clústeres de conmutación por error.

5. Escenarios DFS

El sistema DFS permite trabajar con varios escenarios.

Compartición de archivos entre distintas sedes

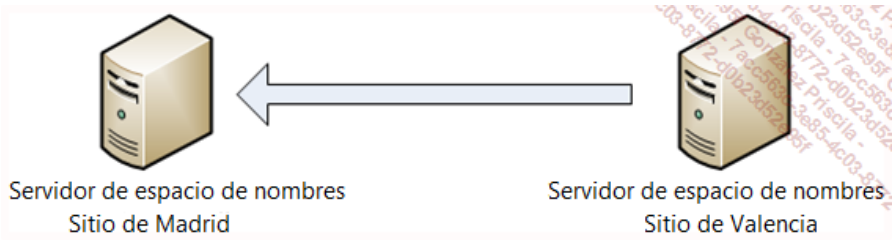
Los archivos se intercambian entre dos o más sitios de la empresa. Esta solución permite realizar una replicación bidireccional que asegura tener todos los servidores actualizados. Además, las personas en itinerancia de un sitio tienen un acceso a los distintos archivos de forma más sencilla. Observe que las modificaciones se replican únicamente cuando se cierra un archivo.



Este escenario no se recomienda para archivos de tipo base de datos o archivos abiertos durante un gran periodo de tiempo (por ejemplo, un archivo Excel de seguimiento en producción que esté abierto durante todo el día por parte del equipo de servicio en producción).

Recopilación de datos

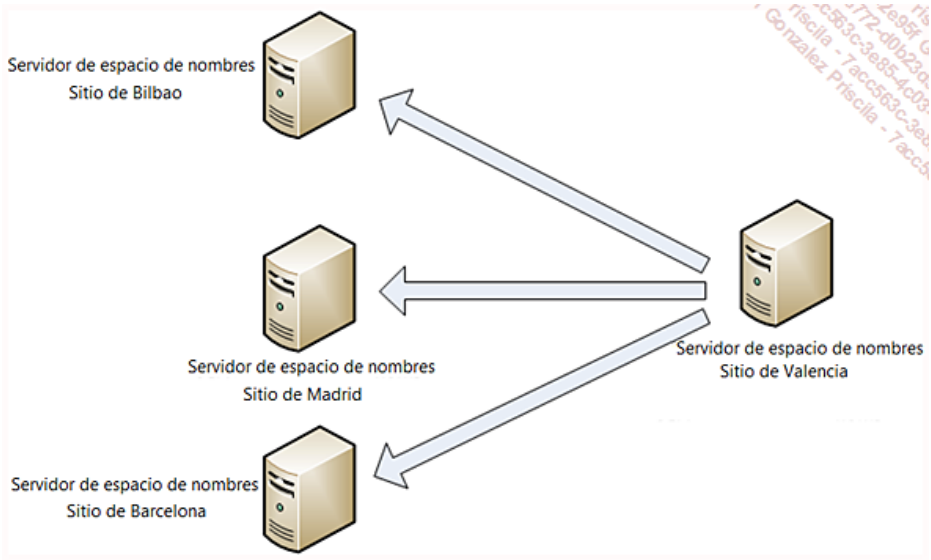
El escenario de recopilación de datos consiste en recuperar los datos de un sitio para replicarlos en otro sitio. La replicación es de tipo unidireccional. Puede consistir en replicar los datos en un sitio concentrador con el objetivo de poder realizar una copia de seguridad.



De este modo, los datos están presentes en ambos sitios, lo que permite una tolerancia a fallos en caso de ocurrir cualquier problema en el primer servidor, con un coste hardware menor en los sitios remotos (ya no es necesario realizar una copia de seguridad de los archivos en cada sede puesto que se consolidan en el sitio central).

Publicación de datos

Esta solución consiste en replicar los documentos en varios servidores (por ejemplo, un archivo de catálogo que se replica desde la sede matriz hacia el conjunto de agencias regionales).



De este modo, cada departamento comercial puede acceder a los archivos de catálogo en su servidor local.

Configuración del espacio de nombres

La configuración de un espacio de nombres es un conjunto de etapas que consiste en crear el espacio de nombres, crear las carpetas en el espacio de nombres y, por último, los destinos de estas carpetas. Éstas pueden apuntar sobre una carpeta compartida que ya exista o sobre una carpeta creada y compartida a tal efecto. A continuación es posible realizar otras operaciones de tipo ABE, tales como la configuración del orden de referencias.

1. Implementar el servicio DFS

La primera etapa es la creación del espacio de nombres. Esta etapa puede ejecutarse mediante el asistente. Debe indicarse información como el tipo de espacio de nombres (autónomo o basado en un dominio), el modo (Windows 2000, Windows Server 2008) así como el nombre del servidor y el nombre del espacio de nombres.

A continuación, es necesario indicar las carpetas, ligadas ellas mismas a uno o varios destinos de carpeta. Si los usuarios deben acceder por defecto a su servidor local, es necesario tener un destino por cada sitio.

Hemos visto más arriba que el servidor provee al cliente una lista ordenada, el administrador tiene la posibilidad de indicar el orden deseado (servidor del sitio en primer lugar, orden aleatorio, excluir destinos que estén fuera del sitio del cliente, etc.). Esta etapa se puede configurar en las propiedades del espacio de nombres.

2. Optimización de un espacio de nombres

Además de las operaciones que consisten en renombrar o desplazar una carpeta creada en el espacio de nombres, es posible deshabilitar las referencias a una carpeta. Esta etapa consiste en impedir a un equipo acceder a una carpeta compartida en un servidor. Resulta muy útil cuando se modifican los servidores de archivos y se encuentran en plena migración. Es posible modificar el valor de la caché de referencia, cuyo valor es de 5 minutos (300 segundos) por defecto. Este valor se renueva cuando el equipo utiliza una referencia. Esto permite, por tanto, utilizar la lista de referencias de forma indefinida.

Con el uso de un espacio de nombres basado en Active Directory, los servidores de dicho espacio de nombres consultan a Active Directory para obtener los datos más recientes relativos al espacio de nombres. Es posible utilizar dos modos:

- **Optimizar para coherencia**: se trata del modo por defecto, consiste en preguntar al controlador de dominio que posee el rol de Maestro emulador de PDC cuando se realiza cualquier modificación del espacio de nombres.
- **Optimizar para escalabilidad**: todos los servidores del espacio de nombres consultan a su controlador de dominio a intervalos periódicos.

Configuración y mantenimiento de DFS-R

Una mala replicación puede generar enormes problemas, por lo que se recomienda asegurar un correcto funcionamiento de esta funcionalidad.

1. Funcionamiento de la replicación

Un grupo de replicación consiste en agrupar un conjunto de servidores que participan en la replicación de una o varias carpetas. Tras la creación del grupo es necesario realizar una elección entre un grupo de replicación multiuso, que permite realizar una replicación entre dos servidores como mínimo (este tipo de grupo puede utilizarse en la mayoría de escenarios DFS), y el grupo de replicación para la recopilación de datos, que permite realizar una replicación de tipo bidireccional entre dos servidores (por ejemplo, un servidor en la sede matriz y otro en alguna sede deslocalizada).

Tras la configuración de la replicación es necesario seleccionar una topología. Podemos escoger entre tres topologías distintas:

- **Concentrador y radio**: esta topología requiere, como mínimo, tres servidores en el mismo grupo de replicación. Esta topología se utiliza en el escenario de publicación (envío de un archivo de un sitio principal hacia sedes regionales).
- **Malla completa**: los miembros realizan replicaciones entre ellos en función de las modificaciones aportadas.
- **Sin topología**: esta opción permite realizar la configuración de la topología más adelante.

2. Proceso de replicación inicial

Tras la configuración de la replicación, el asistente solicita un miembro principal. Se trata del servidor que posee los archivos a replicar más actualizados. En caso de conflicto, este servidor impone su autoridad. El inicio de la replicación inicial no es inmediato, es necesario, previamente, realizar una replicación de los parámetros DFS así como de los parámetros de la topología en el conjunto de los controladores de dominio. A continuación, puede comenzar la replicación inicial entre el miembro principal y los demás servidores. Tras la recepción, los archivos presentes en un miembro de recepción pero no presentes en el miembro principal se mueven a la carpeta DFSrPrivate\PreExisting del miembro de recepción. A continuación, se suprime la designación del miembro principal, y el servidor que poseía esta función ya no tiene autoridad sobre los demás servidores, y se convierte en un servidor más del miembro, al mismo nivel que el resto de servidores.

BranchCache

BranchCache es una tecnología de Microsoft que trata de reducir los flujos de red WAN (*Wide Area Network*) intersitio, permitiendo la puesta en caché de aquellos archivos que se utilizan con mayor frecuencia.

1. Presentación de BranchCache

La tecnología BranchCache nace con el sistema operativo Windows Server 2008 R2 y el cliente Windows 7. La necesidad fue creciendo con el aumento de las estructuras organizativas que trabajaban con sitios remotos (filiales, usuarios remotos, adjuntos…) mientras que los servidores se encuentran en la sede de la empresa. Cada usuario que quería acceder a los recursos alojados en un sitio remoto experimentaba velocidades de transferencia muy lentas a través de una conexión de red intersitio.

Microsoft ha renovado la implementación de la tecnología BranchCache en el sistema operativo Windows Server 2012 R2 como funcionalidad de servidor. BranchCache permite poner en caché los recursos consultados por los usuarios a través de los siguientes protocolos:

- **SMB** (*Server Message Block*): este protocolo se utiliza para los recursos compartidos en una red de Microsoft. Todo recurso consultado por un usuario remoto a través de un recurso compartido de red puede, potencialmente, ponerse en caché si se ha implementado BranchCache.
- **BITS** (*Background Intelligent Transfer Service*): este protocolo lo utilizan las aplicaciones (por ejemplo: Windows Update) para transferir, como tarea de fondo, datos de un servidor a sus clientes utilizando aquellos momentos en los que el ancho de banda no está muy solicitado. Los datos transferidos a través del componente Windows BITS pueden ponerse en caché sobre una infraestructura BranchCache.
- **HTTP/HTTPS** (*HyperText Transfer Protocol*): estos protocolos se utilizan para acceder a contenido web, securizado o no, desde un servidor web como Microsoft IIS (*Internet Information Services*). Todo el contenido recuperado a través de un flujo web HTTP o HTTPS puede almacenarse en un servidor de caché de una infraestructura BranchCache para que los usuarios puedan acceder más rápidamente al contenido del sitio Internet.

Cuando un usuario intenta leer el contenido de un recurso a través de alguno de estos protocolos, BranchCache se encarga de poner en caché el archivo en el caso de que algún otro usuario de la red lo necesite. En la actualidad, solo los clientes Windows 7, 8, 8.1 o 10 pueden utilizar las funcionalidades de BranchCache instaladas en los servidores desde Windows Server 2008 R2 hasta Windows Server 2016. El uso de la funcionalidad BranchCache reduce así el tráfico en las redes WAN asegurando una interconexión intersitio.

a. Funcionamiento de BranchCache

La tecnología BranchCache requiere agregar un servicio de rol BranchCache para archivos de la red en el servidor de archivos o el servidor web, accesibles por los usuarios. A continuación, debe configurarse un objeto GPO para habilitar BranchCache en el servidor.

Si la infraestructura de red utiliza el modo de caché hospedada, debe agregarse la funcionalidad del servidor BranchCache para transformar el servidor situado en el sitio remoto en un servidor de caché para los usuarios. También es necesario crear un objeto GPO para configurar el cortafuegos del servidor de caché y, de este modo, autorizar a aceptar el tráfico HTTP entrante.

Cuando se agrega la funcionalidad BranchCache en un servidor de caché, se crea el servicio de Windows BranchCache con un tipo de arranque automático. El rol de este servicio es poner en caché los recursos consultados por los equipos cliente.

Cuando se configura un sitio remoto para utilizar el modo de caché distribuida, los equipos cliente realizan peticiones de tipo multicast a la red para saber qué puesto de la red posee una copia en caché del recurso solicitado por el usuario. Para no bloquear las peticiones multicast de los puestos cliente, el administrador del sitio remoto debe configurar un objeto GPO para autorizar el tráfico HTTP y WS-Discovery en el cortafuegos de los clientes Windows.

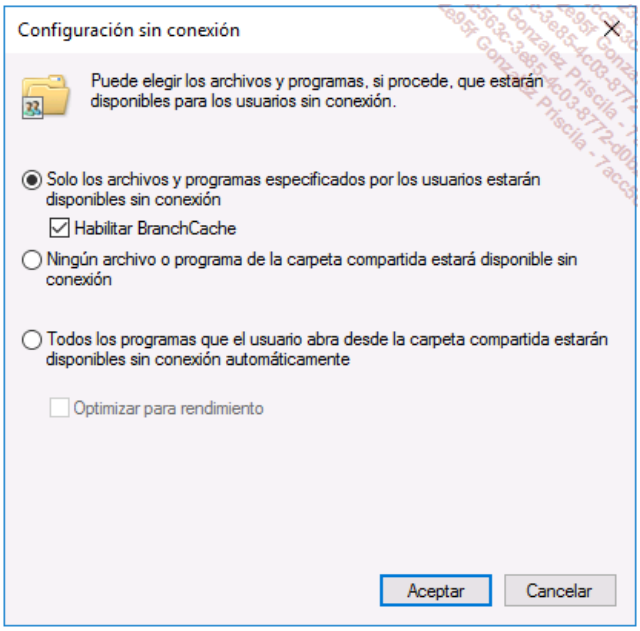
Los clientes que trabajan con Windows 8, Windows 8.1 o Windows 10 poseen, de manera nativa, un cliente BranchCache visible como un servicio de Windows. Por defecto, este servicio está detenido y el tipo de arranque está configurado a **Manual**.

Cuando se crea una directiva de grupo para habilitar BranchCache en los equipos cliente Windows 8.1 o 10, el servicio de Windows arranca en un modo de funcionamiento de caché hospedada. Esto quiere decir que los clientes empiezan buscando un servidor de caché en la red local. Si el servidor de caché no existe, los clientes pasan a un modo de funcionamiento de caché distribuida. Esta configuración automática de los clientes Windows puede configurarse mediante un objeto GPO para definir previamente el modo de caché distribuida u hospedada.

b. Administración de BranchCache

Las carpetas compartidas

Para agregar el servicio de rol BranchCache en un servidor web, no se requiere ninguna configuración adicional. Sin embargo, para un servidor de archivos, las carpetas compartidas en la red deben configurarse para indicar a los usuarios que los archivos pueden estar alojados en caché. La configuración de una carpeta compartida puede realizarla BranchCache a través de sus propiedades:



La activación de BranchCache

Para utilizar BranchCache en los equipos cliente, en primer lugar hay que habilitarlo. La activación de esta funcionalidad se puede llevar a cabo de dos maneras:

- A través de las directivas de grupo (GPO): basta con editar una GPO vinculada a una OU que contenga los equipos correspondientes. Los parámetros de activación de BranchCache y la configuración del modo de caché se encuentran en la siguiente ubicación:**Configuración del equipo - Directivas - Plantillas administrativas - Red - BranchCache**.
- Mediante comandos PowerShell: los siguientes comandos PowerShell permiten configurar BranchCache en un cliente o un servidor Windows.

Comprobar el modo de caché utilizado por un cliente:

```
Get-BCClientConfiguration
```

Configurar un equipo cliente Windows 8.1 o 10 para que utilice el modo de caché hospedada:

```
Enable-BCHostedClient -ServerNames <Nombre del servidor de caché>
```

Configurar un equipo cliente Windows 8.1 o 10 para utilizar el modo de caché distribuida:

```
Enable-BCDistributed
```

Configurar un servidor para que sea servidor de caché y registrar el punto de conexión del servicio (SCP - Service Connection Point) en Active Directory:

```
Enable-BCHostedServer -RegisterSCP
```

Para obtener más información, consulte el sitio de Microsoft en la siguiente dirección: http://technet.microsoft.com/en-us/library/hh848394%28v=wps.620%29.aspx

Configuración del cortafuegos

Cuando los equipos cliente utilizan el modo de caché hospedada, el administrador debe configurar un objeto GPO que permita configurar el cortafuegos autorizando el puerto entrante 80:

- **BranchCache - Recuperación de contenido**: permite transferir los datos en caché del servidor hasta los puestos cliente a través del protocolo de transporte HTTP.
- **BranchCache - Detección del mismo nivel**: permite descubrir los equipos cliente que hospedan un contenido en caché a través del protocolo WS-Discovery.

Cuando los puestos cliente utilizan el modo de caché distribuida, el administrador debe configurar un objeto GPO que permita configurar el cortafuegos autorizando el puerto entrante 3702.

Publicación de hash

Cuando un servidor de archivos posee el rol BranchCache para archivos de red, es posible crear una directiva de grupo cuyo objetivo sea habilitar la generación de hash para los datos compartidos (los hash representan información de contenido).

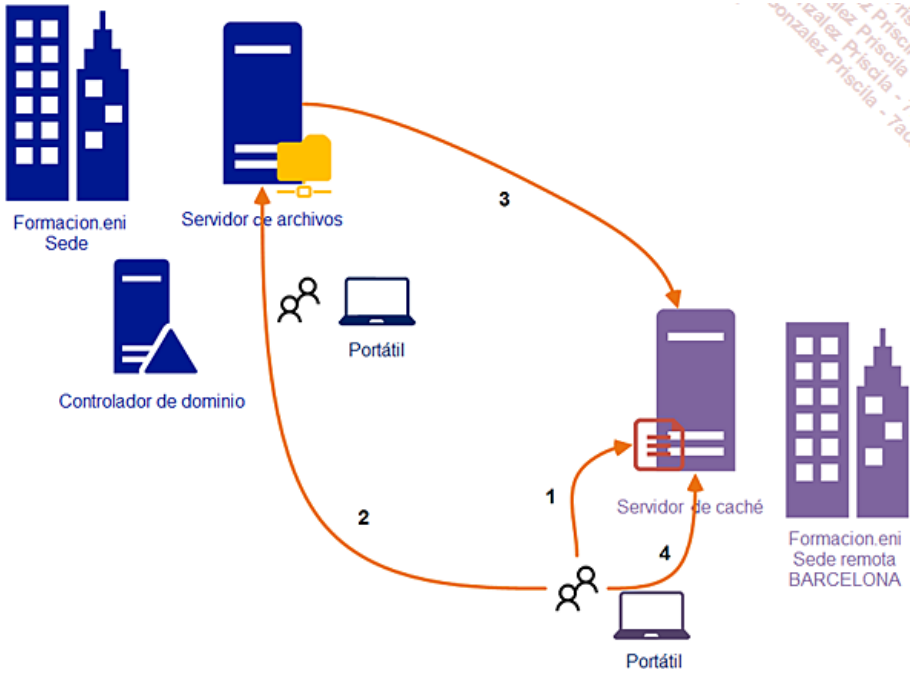
2. Los distintos modos de caché

Una infraestructura BranchCache puede configurarse según dos modos de caché: la caché hospedada o la caché distribuida.

a. Modo de caché hospedada BranchCache

El modo de caché hospedada consiste en implementar un servidor de caché en el sitio remoto. Cada recurso consultado por los usuarios en el servidor de archivos de la sede (también funciona si se trata de un acceso HTTP/HTTPS a un servidor web) puede alojarse en caché localmente en el servidor de caché. El objetivo de esto es evitar que otros usuarios tengan que descargar de nuevo el archivo que ya se ha consultado a través de un flujo WAN interconectando ambos sitios, y acceder en su lugar a través de la red local del sitio replicado. Este modo de funcionamiento de la caché se utiliza con la tecnología BranchCache cuando el sitio remoto contiene varios puestos de usuario.

Esquema de una infraestructura BranchCache que utiliza el modo de caché hospedada:

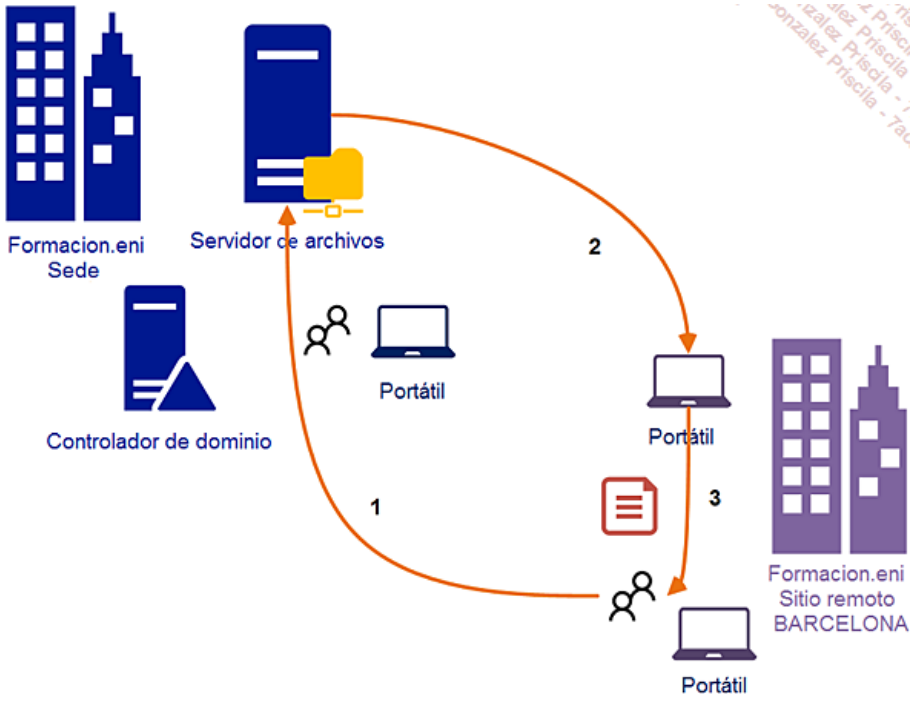


1. Un usuario del sitio remoto de Barcelona de la empresa Formacion.eni trata de acceder a un archivo compartido en el servidor de archivos de la sede. El equipo cliente consulta primero si existe una copia del archivo en la caché del servidor de caché.
2. Si el archivo solicitado por el usuario no figura en el servidor de caché, el puesto cliente se conecta directamente al servidor de archivos de la sede para recuperar el recurso solicitado.
3. El recurso solicitado se copia en el servidor de caché a través del flujo WAN. El usuario accede a continuación a su archivo.
4. Otro usuario intenta acceder al mismo archivo solicitado previamente por su colega. El puesto cliente de este usuario consulta el contenido del servidor de caché para acceder a la copia en caché del recurso solicitado.

b. Modo de caché distribuida BranchCache

El modo de caché distribuida consiste en autorizar a los puestos cliente a poner en caché localmente en su disco una copia de los recursos consultados en el servidor de archivos de la sede (funciona también cuando se trata de un acceso HTTP/HTTPS a un servidor web). Este modo de caché no requiere un servidor de caché en el sitio remoto. Se recomienda utilizar este modo con la tecnología BranchCache únicamente cuando el sitio remoto contiene pocos puestos de usuario.

Esquema de una infraestructura BranchCache que utiliza el modo de caché distribuida:

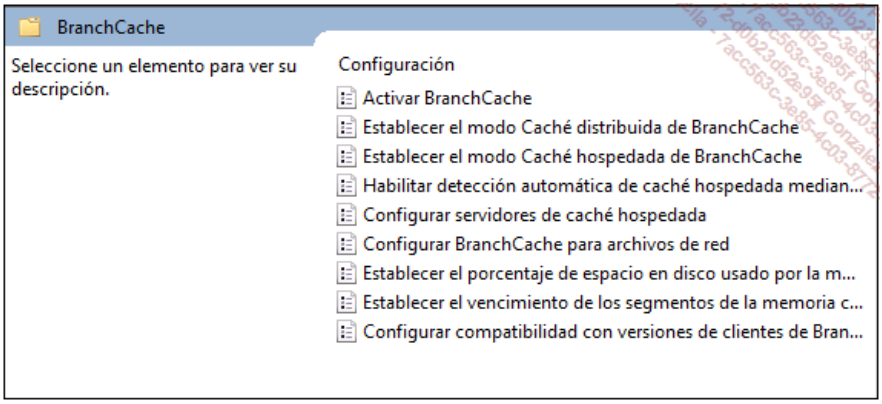


1. Un usuario del sitio remoto de Barcelona de la empresa Formacion.eni trata de acceder a un archivo compartido en el servidor de archivos de la sede central.
2. El archivo solicitado por el usuario se descarga en local en el puesto cliente y el usuario accede a su archivo.
3. Otro usuario trata de acceder al mismo archivo solicitado previamente por su colega. El puesto cliente de este usuario realiza una petición multicast para saber qué puesto cliente de la red posee una copia en su caché local. Una vez recuperada la información, el puesto cliente consulta el contenido de la caché de su colega para acceder a la copia del archivo solicitado.

3. Desplegar BranchCache

Para desplegar BranchCache configurando los puestos cliente de los sitios remotos que usarán esta tecnología, hay que utilizar objetos de directiva de grupo, o bien ejecutar manualmente comandos PowerShell o Netsh en cada puesto.

Para configurar BranchCache utilizando las directivas de grupo, hay que configurar la siguiente sección en los parámetros de un GPO:**Configuración del equipo - Directivas - Plantillas administrativas - Red - BranchCache**.



La sección BranchCache permite:

- Habilitar BranchCache.
- Definir el modo de caché (distribuida u hospedada).
- Habilitar el descubrimiento automático.
- Configurar los servidores de caché hospedada.
- Configurar BranchCache para los archivos de red.
- Definir el porcentaje de espacio en disco asignado para la caché de un cliente.
- Definir el tiempo de vida de los segmentos en la caché de datos.
- Configurar la versión de BranchCache.

Trabajos prácticos: Gestión del servidor de archivos

Estos trabajos prácticos muestran cómo instalar y configurar las funcionalidades que permiten administrar un sistema de archivos.

1. Instalación y configuración del servidor DFS

Objetivo: instalar y configurar un espacio de nombres DFS.

Máquinas virtuales: PAR-DC01 y PAR-SRV2

Inicie una sesión como administrador en **PAR-DC01** y **PAR-SRV2**.

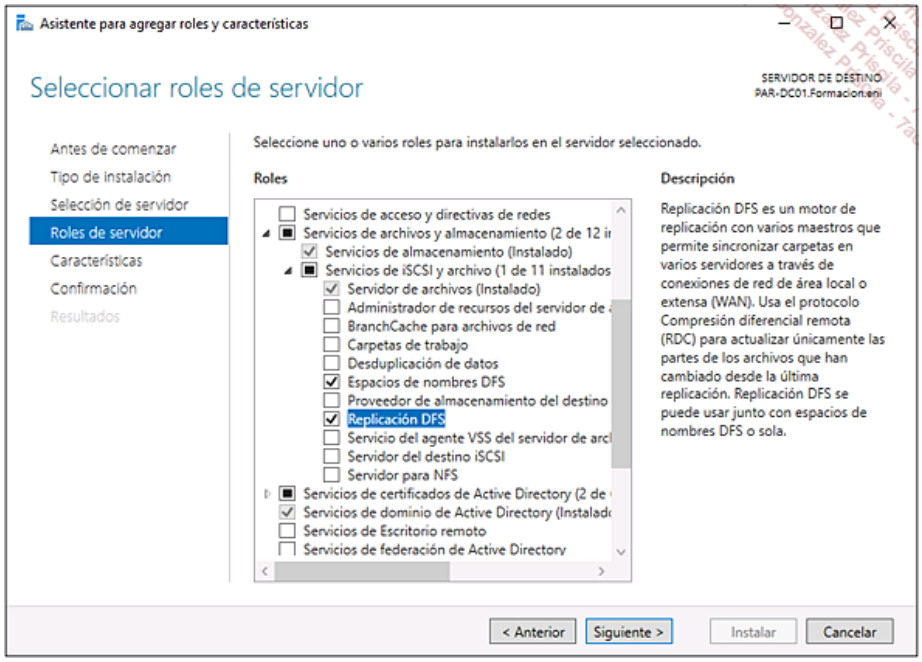
En **PAR-DC01**, abra la consola **Administrador del servidor** y, a continuación, haga clic en **Agregar roles y características**.

En la ventana **Seleccione el tipo de instalación**, deje la opción por defecto y, a continuación, haga clic en **Siguiente**.

Haga clic en **Siguiente** en la ventana de selección del servidor de destino.

Despliegue los roles **Servicios de archivos y almacenamiento** y, a continuación, **Servicios de iSCSI y archivo**.

Marque **Espacios de nombres DFS** y **Replicación DFS** y, a continuación, haga clic en **Agregar funcionalidades** en la ventana emergente.



Valide haciendo clic en **Siguiente**.

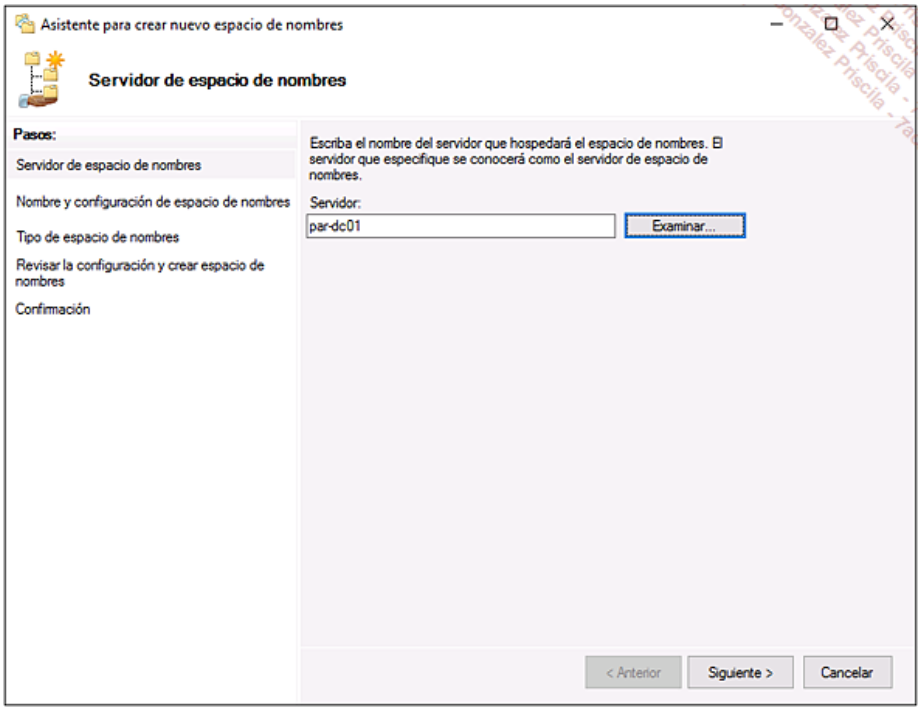
Haga clic en **Siguiente** en la ventana **Seleccionar funcionalidades** y, a continuación, en **Instalar**.

Haga clic en **Cerrar** al finalizar la instalación y, a continuación, repita la misma operación con el servidor **PAR-SRV2**.

En **PAR-DC01**, haga clic en **Administración de DFS** en las Herramientas administrativas.

Haga clic en **Nuevo espacio de nombres** (panel **Acciones**) en la consola que acaba de abrir.

Mediante el botón **Examinar** en la ventana **Servidor de espacio de nombres**, seleccione **PAR-DC01** y, a continuación, haga clic en**Siguiente**.



En el campo **Nombre** del espacio de nombres, escriba **DocsCertificaciones**.

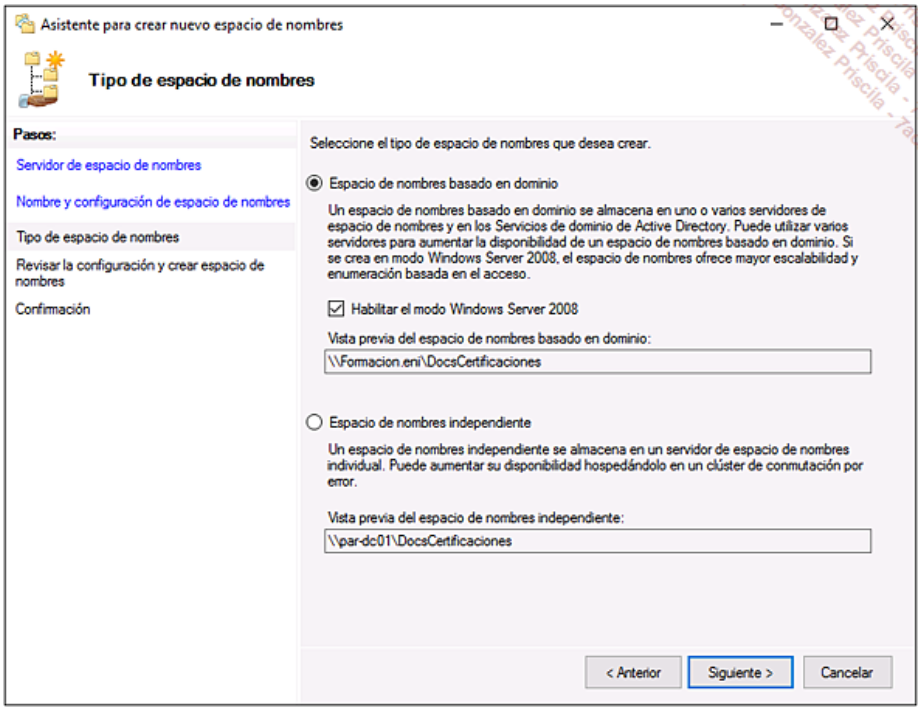
Haga clic en el botón **Editar configuración**.

Este menú permite configurar la ruta de acceso local a la carpeta compartida y, también, sus permisos.

En la zona **Permisos de la carpeta compartida**, haga clic en el botón de radio que autoriza a los administradores con permisos de control total y, a los demás usuarios, con permisos de lectura/escritura.

En la ventana **Tipo de espacio de nombres**, deje la configuración por defecto y pulse en **Siguiente**.

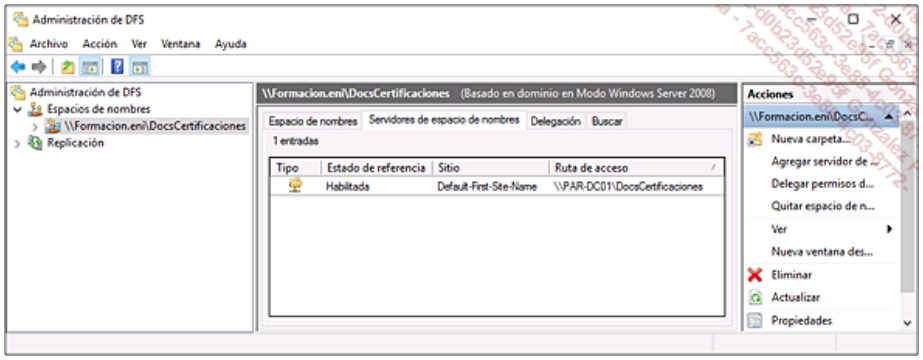
Habilitando el modo Windows Server 2008 se habilitan funcionalidades suplementarias tales como la enumeración basada en el acceso.



Haga clic en **Crear** para iniciar la creación.

Si no aparece ningún error, cierre el asistente.

Despliegue el nodo **Espacios de nombres** y, a continuación, seleccione el espacio de nombres y haga clic en la pestaña **Servidores de espacio de nombres**.



En el panel **Acciones**, haga clic en **Agregar servidor de espacio de nombres**.

Mediante el botón **Examinar**, seleccione el servidor **PAR-SRV2**.

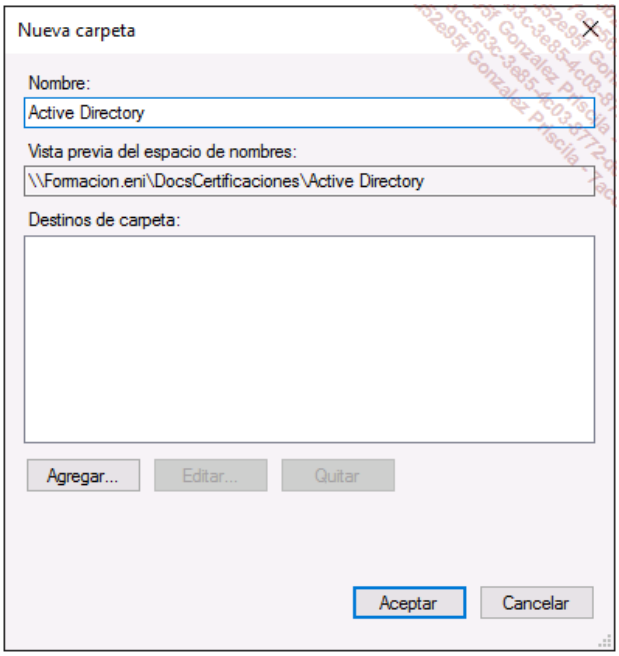
Haga clic en el botón **Editar configuración**.

En **Permisos de carpeta compartida**, haga clic en la opción que autoriza a los administradores con permisos de control total y a los demás usuario con permisos de lectura/escritura y, a continuación, haga clic dos veces en **Aceptar**.

Se ha agregado el servidor al espacio de nombres.

Haga clic en la pestaña **Espacio de nombres** y, a continuación, en **Nueva carpeta** en el panel **Acciones**.

Escriba **Active Directory** en el campo **Nombre** y, a continuación, haga clic en **Agregar**.

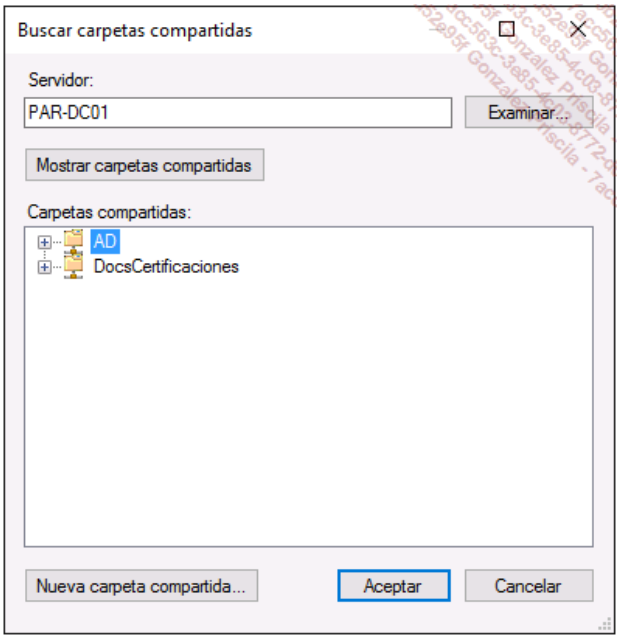


En la ventana **Agregar destino de carpeta**, haga clic en **Examinar**.

Haga clic en **Nueva carpeta compartida**.

En **Nombre del recurso compartido** escriba **AD** y, a continuación, mediante el botón **Examinar**, cree una carpeta compartida en C: con el nombre **ActiveDirectory**.

Haga clic en **Aceptar** y, a continuación, marque la opción **Los administradores tienen acceso total; otros usuarios tienen permisos de lectura/escritura**.



Haga clic en **Aceptar** para validar todas las ventanas.

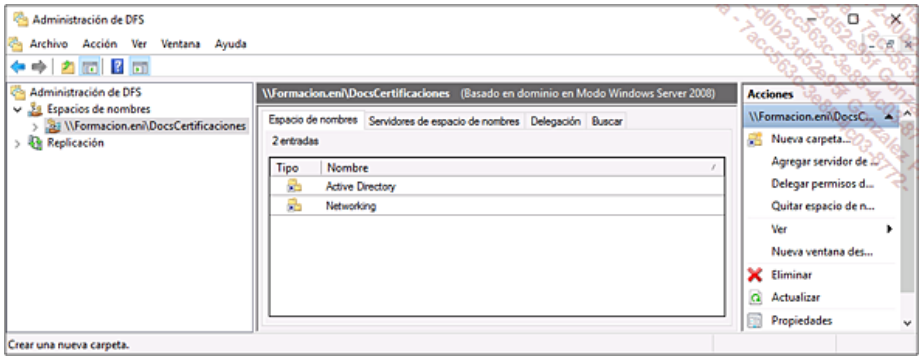
Haga clic, de nuevo, en **Nueva carpeta**.

En el campo **Nombre** escriba **Networking** y, a continuación, haga clic en **Agregar**.

En la ventana **Agregar destino de carpeta**, haga clic en **Examinar**.

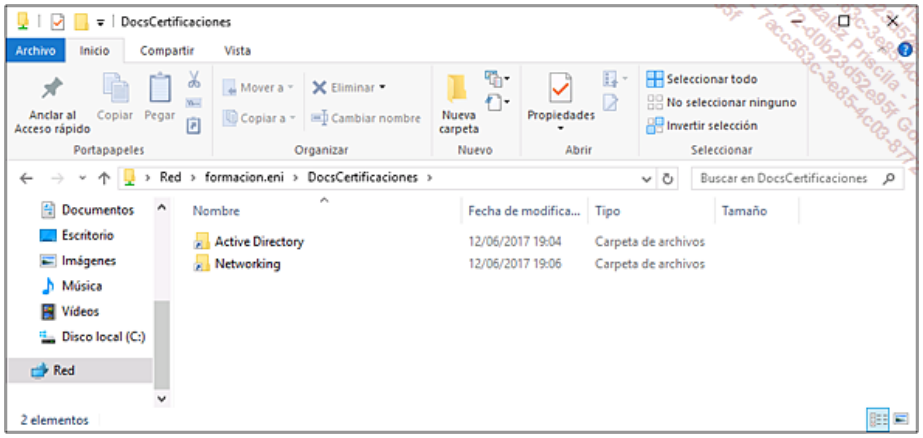
Haga clic en **Examinar** en la ventana **Buscar carpetas compartidas**.

Escriba **PAR-SRV2** y valide la selección haciendo clic en **Comprobar nombres**, a continuación haga clic en **Aceptar**.



Haga clic en **Mostrar carpetas compartidas** y, a continuación, en **DocsCertificaciones**.

Se muestran en la consola las dos carpetas. Existe un acceso a \\formacion.eni\DocsCertificaciones que permite acceder a sus carpetas sin tener por qué conocer el servidor sobre el que están ubicados.



Las dos carpetas presentes en el espacio de nombres se encuentran en dos servidores separados. Es útil activar la replicación DFS para asegurar la disponibilidad de los datos.

2. Configuración de la replicación

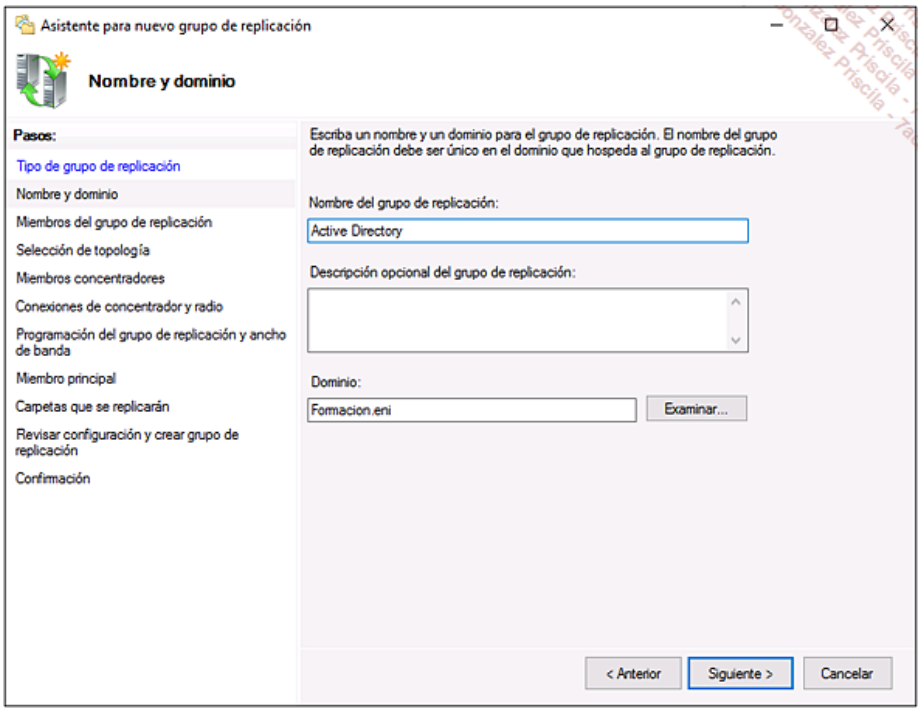
Objetivo: implementar la replicación DFS entre dos servidores.

Máquinas virtuales: PAR-DC01 y PAR-SRV2.

En la consola **Administración DFS**, haga clic en el nodo **Replicación** y, a continuación, en **Nuevo grupo de replicación** en el panel**Acciones**.

En la ventana que permite escoger el tipo de grupo, seleccione **Grupo de replicación multipropósito** y, a continuación, haga clic en**Siguiente**.

En **Nombre del grupo de replicación**, escriba **Active Directory** y, a continuación, valide haciendo clic en **Siguiente**.



Debe agregar los servidores **PAR-DC01** y **PAR-SRV2**. Para realizar esta operación, haga clic en el botón **Agregar**.

Seleccione el tipo de topología **Malla completa** y, a continuación, haga clic en **Siguiente**.

Es posible planificar o limitar el ancho de banda para evitar crear un cuello de botella.

Deje la opción por defecto en la ventana **Programación del grupo de replicación y ancho de banda** y, a continuación, haga clic en**Siguiente**.

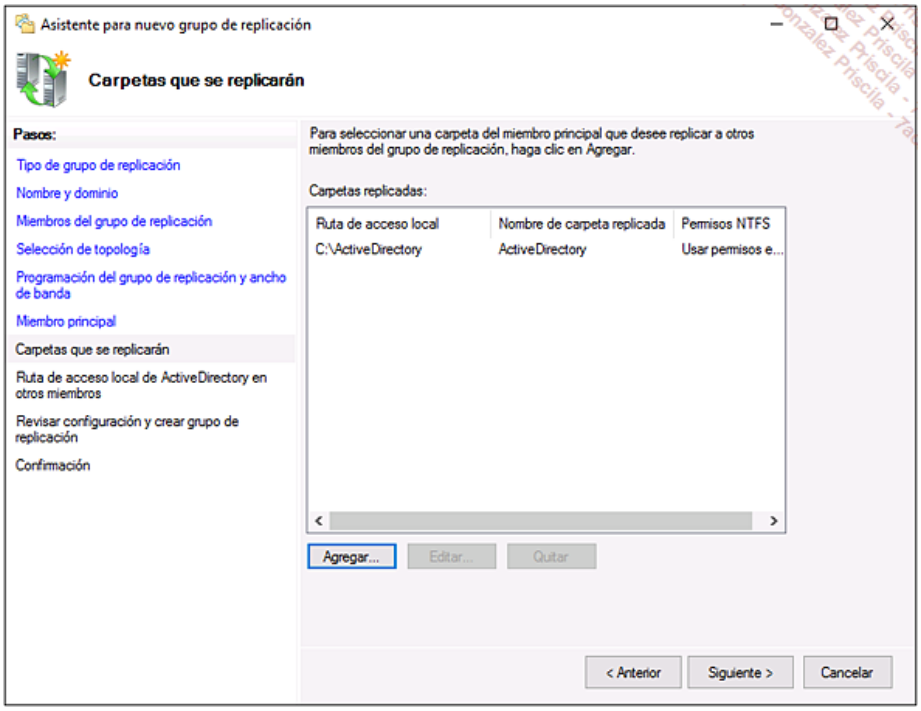
En la lista desplegable que permite escoger el **Miembro principal**, seleccione **PAR-DC01** y, a continuación, haga clic en **Siguiente**.

Es preciso, a continuación, seleccionar las carpetas que se quieren replicar.

Haga clic en el botón **Agregar**.

En la ventana **Carpetas que se replicarán**, haga clic en **Examinar** y, a continuación, seleccione la carpeta **ActiveDirectory**.

Valide haciendo clic en **Aceptar** y, a continuación, haga clic en **Siguiente**.



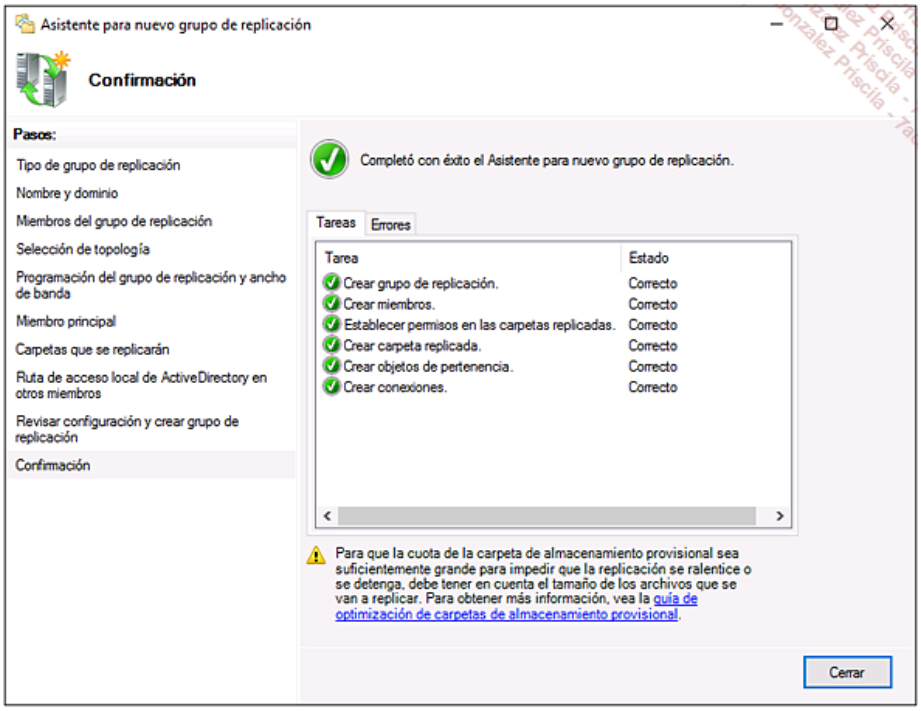
En la ventana **Ruta de acceso local de ActiveDirectory en otros miembros**, haga clic en el botón **Editar**.

Escoja la opción **Habilitada** y, a continuación, haga clic en **Examinar**.

Cree una nueva carpeta llamada **ActiveDirectory** en la partición C: del servidor **PAR-SRV2**.

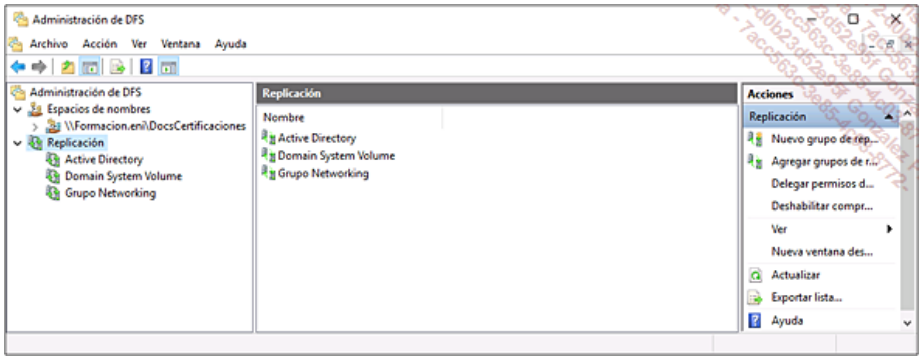
Haga clic en **Siguiente** y, a continuación, en **Crear**.

Si todo queda de color verde, haga clic en **Cerrar**.



La replicación puede llevar cierto tiempo.

Repita la misma operación con la carpeta **Networking**. El miembro principal es **PAR-SRV2**, y el grupo de replicación se denominará **Grupo Networking**.



Acceda, con ayuda del explorador, a la ruta UNC \\formacion.eni\docscertificaciones.

Cree un archivo de texto llamado **Agregar_grupos** en **Active Directory** y, a continuación, otro archivo llamado **Conflicto_IP** en**Networking**.

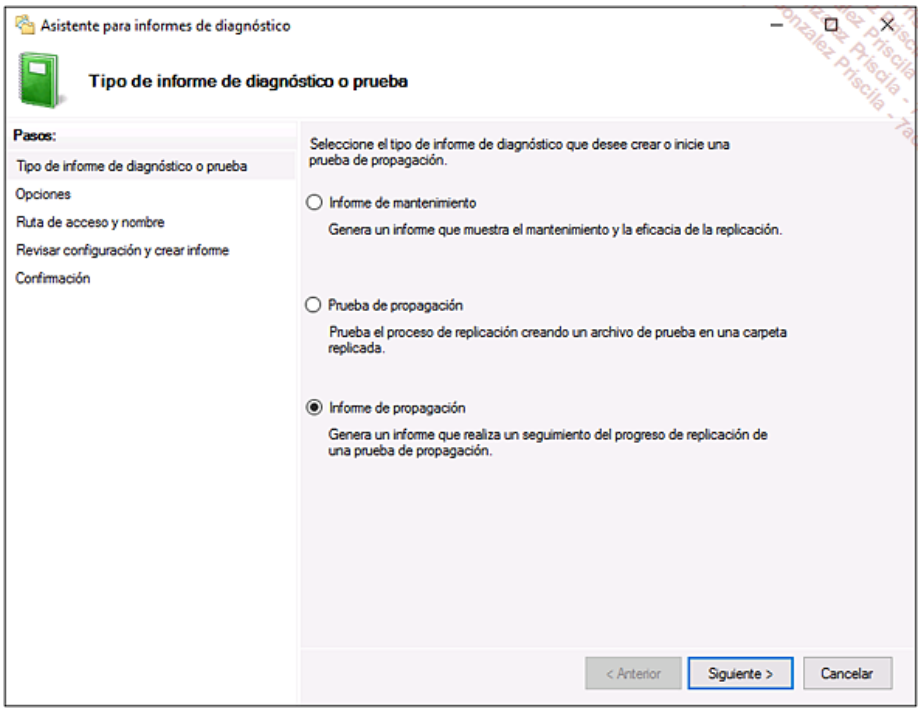
Verifique la presencia de ambos archivos en las carpetas **ActiveDirectory** y **Networking** de ambos servidores.

Se ha realizado la replicación y los archivos están replicados.

Uso de informes

Haga clic en el grupo de replicación **Active Directory** y, a continuación, en el panel **Acciones** haga clic en **Crear informe de diagnóstico**.

Seleccione la opción **Informe de propagación** y, a continuación, haga clic en **Siguiente**.



Deje los valores por defecto y, a continuación, haga clic en **Siguiente**.

Haga clic en el botón **Crear** para iniciar la operación.

Si no ocurre ningún error, haga clic en **Cerrar**.

Haga clic en el grupo de replicación **Active Directory** y, a continuación, en el panel **Acciones** haga clic en **Crear informe de diagnóstico**.

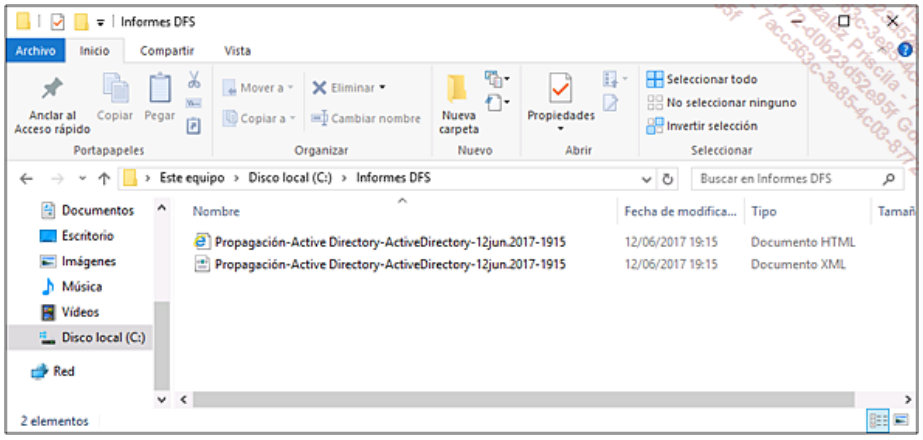
Seleccione la opción **Informe de propagación**.

En la ventana de las opciones del informe, haga clic en **Siguiente**.

La ventana **Ruta de acceso de informe** permite seleccionar la carpeta que va a contener el informe.

Deje la ruta por defecto y, a continuación, haga clic en **Siguiente**.

Haga clic en **Crear** para iniciar la operación de creación. El informe se ejecuta al finalizar el asistente.



Los informes permiten no sólo asegurar el buen funcionamiento del espacio de nombres DFS sino también la replicación. Puede resultar útil planificar la creación de estos informes.

3. Instalación y configuración de BranchCache

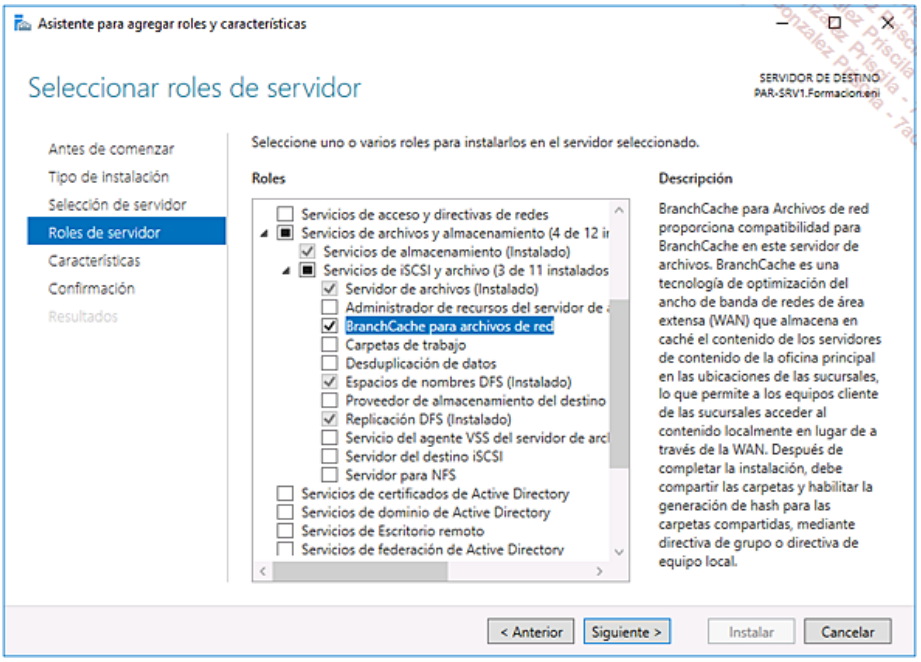
Máquinas virtuales necesarias: PAR-DC01, PAR-SRV1, PAR-SRV2, CL10-01 y CL10-02.

Objetivos: este trabajo práctico tiene como objetivo desplegar y configurar BranchCache utilizando el modo de caché hospedada en una red del sitio remoto.

Una los servidores **PAR-SRV1** y **PAR-SRV2** al dominio Active Directory Formacion.eni.

En **PAR-SRV1**, inicie una sesión como administrador del dominio, abra el Administrador del servidor y haga clic en **Agregar roles y características**.

Haga clic tres veces en **Siguiente**, despliegue el árbol del servicio de rol de archivos **Servicios de archivos y almacenamiento - Servicios de archivos y iSCSI**, y marque la opción **BranchCache para archivos de red**. En la ventana **Asistente para agregar roles y características**, haga clic en **Agregar características**.



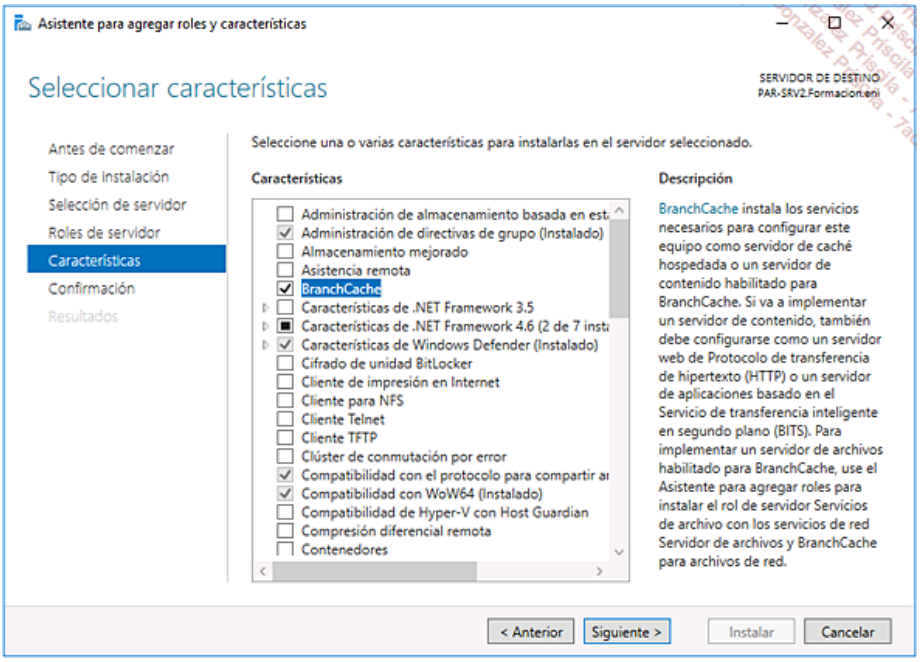
Haga clic dos veces en **Siguiente** y, a continuación, en **Instalar**.

Haga clic en **Cerrar** una vez terminada la instalación.

Configuración del servidor de Caché: PAR-SRV2

En el servidor de caché (situado en el nodo remoto), abra el Administrador del servidor y haga clic en **Agregar roles y características**.

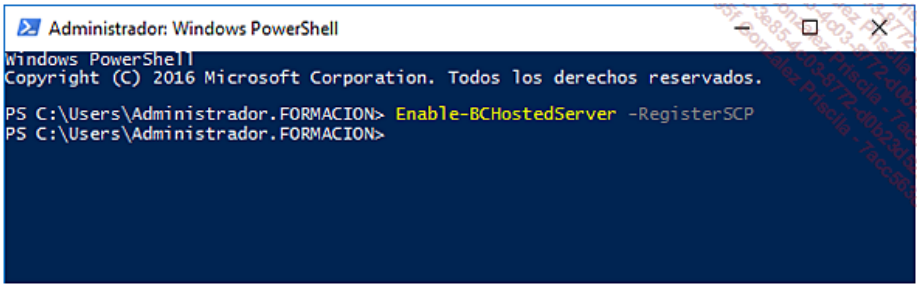
Marque la característica **BranchCache** y, a continuación, haga clic dos veces en **Siguiente** e **Instalar**.



Haga clic en **Cerrar** cuando termine el asistente para instalar la característica.

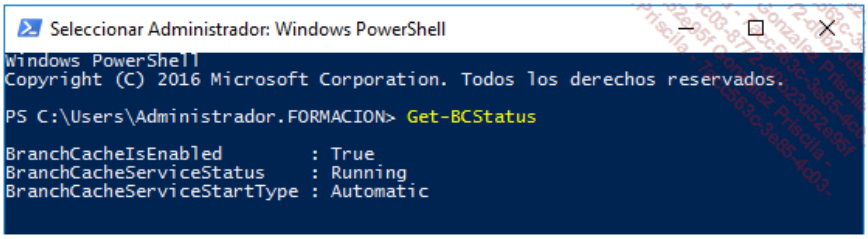
Abra una línea de comandos PowerShell como administrador y escriba el siguiente comando:

```
Enable-BCHostedServer -RegisterSCP
```



Compruebe el estado del servicio en PowerShell con el comando:

```
Get-BCStatus
```



Debe obtener la configuración **`BranchCacheIsEnable True`** y **`BranchCacheService Status Running`**.

Habilitar y configurar BranchCache: PAR-DC01

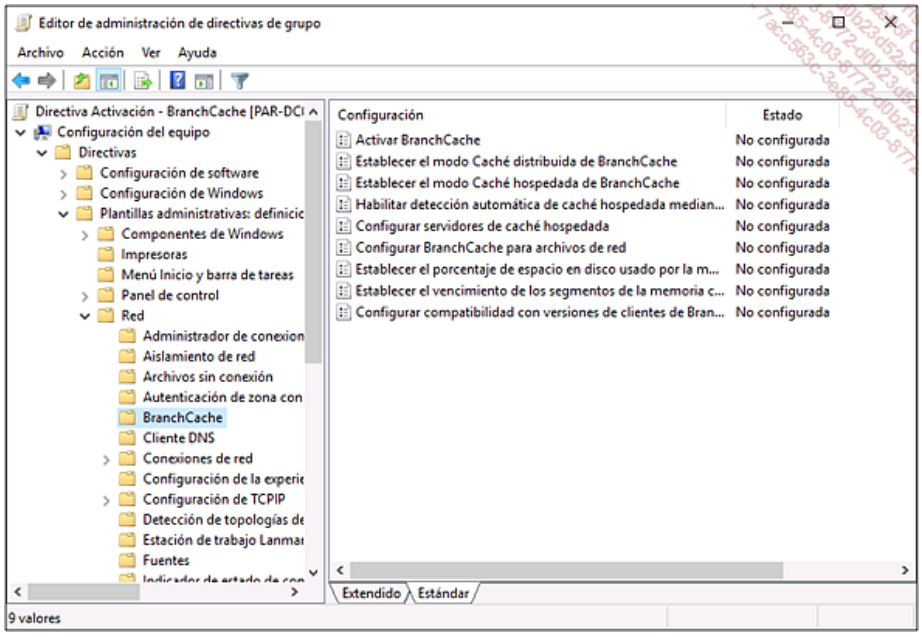
Activación y configuración de la funcionalidad BranchCache mediante una directiva de grupo:

Entre en **PAR-DC01** y abra la consola de administración de directivas de grupo desde el Administrador del servidor, en **Herramientas**.

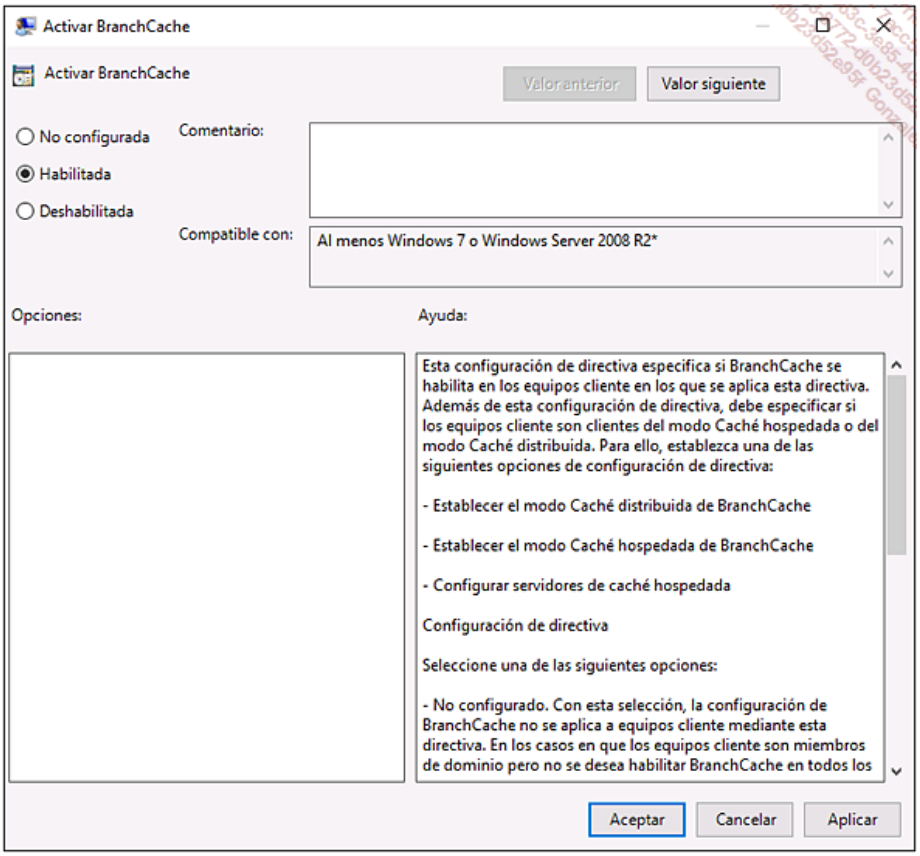
Despliegue el árbol de la consola, haga clic con el botón derecho en la OU **FORMACION\BranchCache_Client** y haga clic en **Crear un GPO en este dominio y vincularlo aquí**.

Llame a la directiva de grupo **Activación - BranchCache** y haga clic en **Aceptar**.

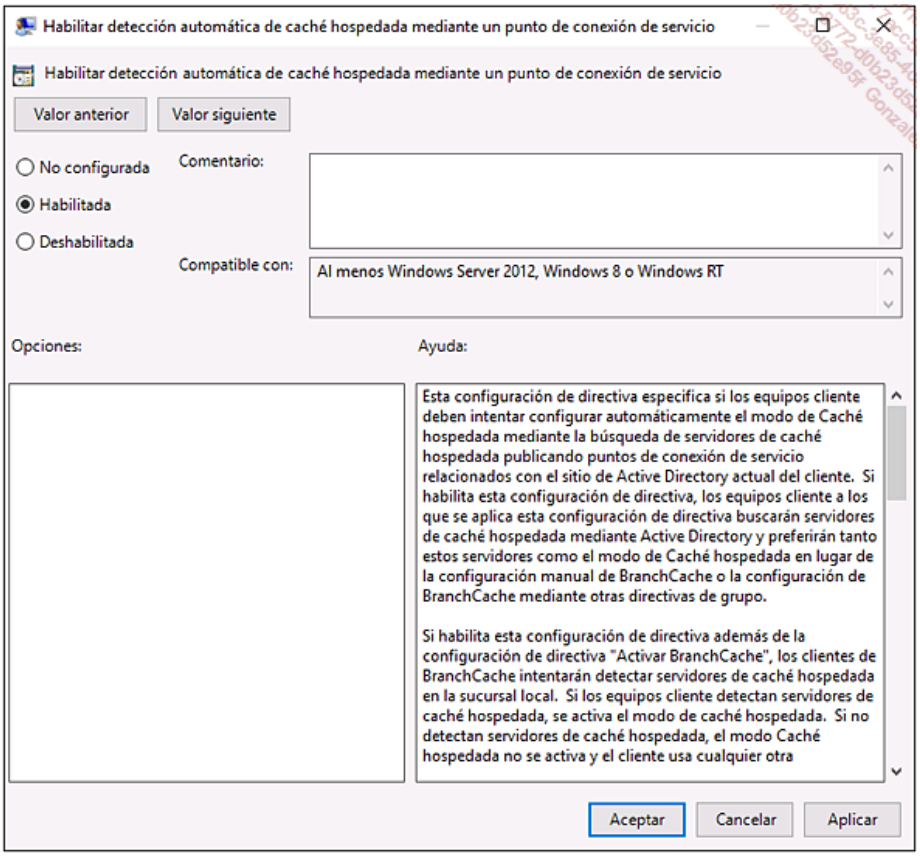
Despliegue el árbol de la consola y seleccione la siguiente carpeta: **Configuración del equipo - Directivas - Plantillas administrativas - Red - BranchCache**.



Haga doble clic en el parámetro **Activar BranchCache** para editarlo y, a continuación, marque la opción **Habilitada** y haga clic en **Aceptar**.



Haga doble clic en el parámetro **Habilitar detección automática de caché hospedada mediante un punto de conexión de servicio** para editarlo y, a continuación, marque la opción **Habilitada** y haga clic en **Aceptar**.



En la consola **Usuarios y equipos de Active Directory**, desplace el equipo cliente **CL10-01** hasta la OU **BranchCache_Client**.

En **CL10-01**, inicie una sesión como administrador del dominio y ejecute en una línea de comandos:

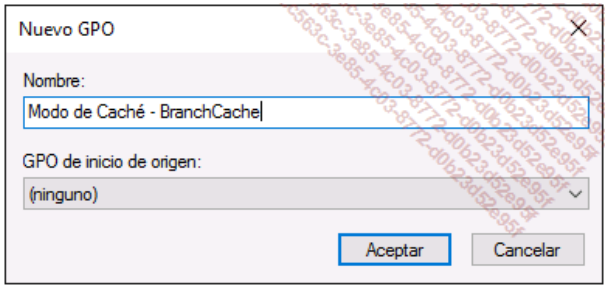
```
gpupdate /force
```

Configurar el modo de caché: PAR-DC01

Entre en **PAR-DC01** y abra la consola de administración de directivas de grupo desde el Administrador del servidor, en **Herramientas**.

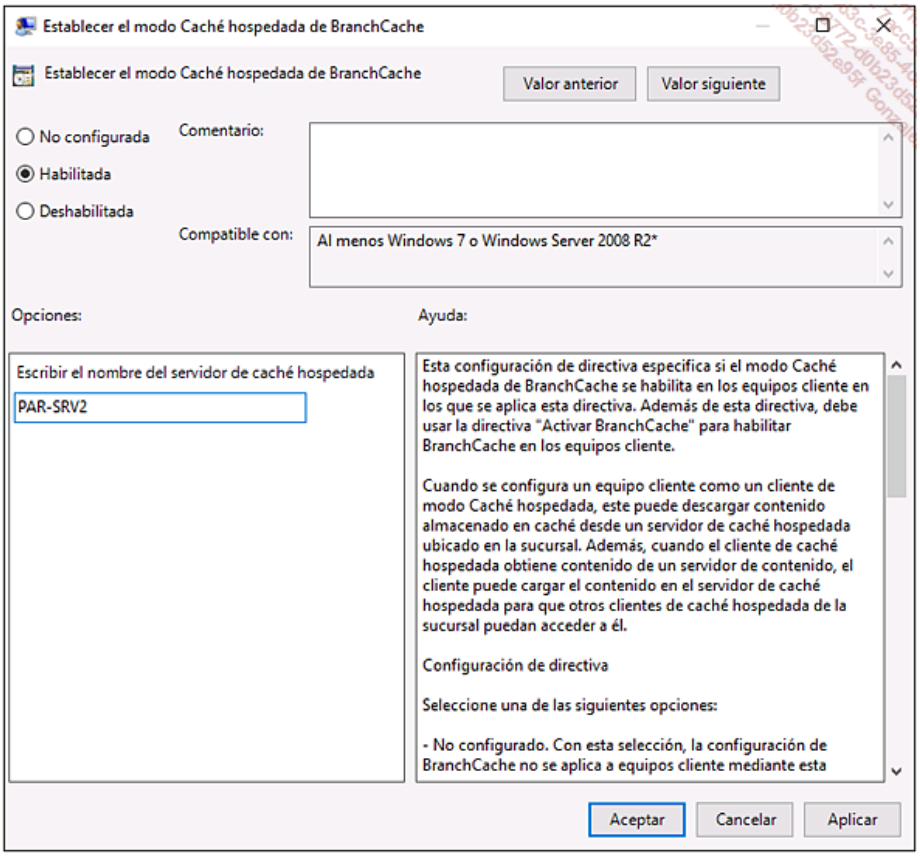
Despliegue el árbol de la consola, haga clic con el botón derecho en la OU **FORMACION\BranchCache_Client** y haga clic en **Crear un GPO en este dominio y vincularlo aquí**.

Llame a la directiva de grupo **Modo de Caché - BranchCache** y haga clic en **Aceptar**.



Despliegue el árbol de la consola y seleccione la siguiente carpeta: **Configuración del equipo - Directivas - Plantillas administrativas - Red - BranchCache**.

Haga doble clic en el parámetro **Establecer el modo Caché hospedada de BranchCache** para editarlo y, a continuación, marque la opción**Habilitada**. Escriba **PAR-SRV2** en el campo **Escribir el nombre del servidor de caché hospedada** y haga clic en **Aceptar**.



Haga doble clic en el parámetro **Configurar BranchCache para archivos de red** para editarlo y, a continuación, marque la opción**Habilitada**. Introduzca el valor **0** en el campo **Escribir la latencia de red de ida y vuelta máxima (milisegundos) tras la cual comienza el almacenamiento en caché** para forzar a BranchCache a que ponga en caché cualquier archivo recuperado de la red. Haga clic en **Aceptar**.

En **CL10-01**, inicie una sesión como administrador del dominio y ejecute en una consola de comandos:

```
gpupdate /force
```

Configurar los recursos compartidos de archivos: PAR-SRV1

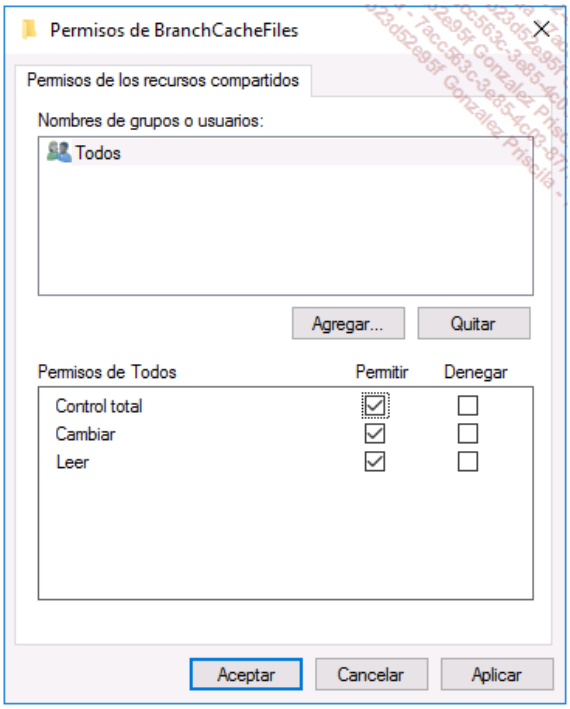
En el servidor de archivos **PAR-SRV1**, cree una nueva carpeta llamada **BranchCacheFiles** en la raíz del disco C:\.

Haga clic con el botón derecho en la carpeta compartida y haga clic en **Propiedades**.

Seleccione la pestaña **Compartir** y haga clic en **Uso compartido avanzado**.

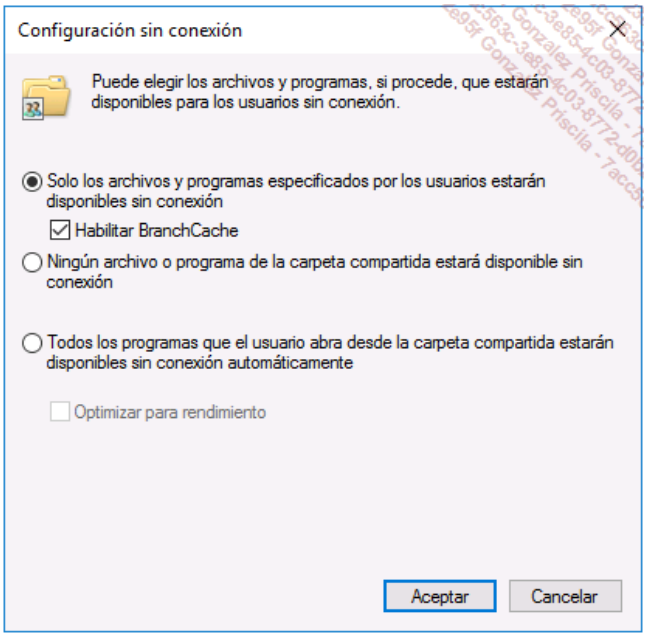
En la ventana **Uso compartido avanzado**, marque la opción **Compartir esta carpeta** y, a continuación, haga clic en **Permisos**.

Marque la opción **Permitir** de la autorización **Control total** para **Todos** y, a continuación, haga clic en **Aceptar**.



En la ventana **Uso compartido avanzado**, haga clic en **Caché**.

En la ventana **Configuración sin conexión**, marque la opción **Habilitar BranchCache** y haga clic en **Aceptar**.



Haga clic dos veces en **Aceptar** para cerrar las ventanas correspondientes a las propiedades de compartición de la carpeta compartida.

Para habilitar BancheCache en las carpetas compartidas existentes, habilite la funcionalidad BranchCache en la pestaña **Caché**.

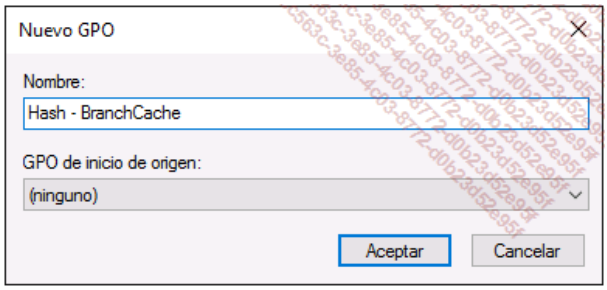
Configurar el hash: PAR-SRV1

Para autorizar a un servidor de archivos que utilice la tecnología BranchCache para generar información de contenido llamada hash, es preciso crear la siguiente direcriva de grupo y aplicarla a los servidores de archivos correspondientes. El servidor de archivos debe ubicarse en una nueva OU llamada **Servidor_BranchCache**.

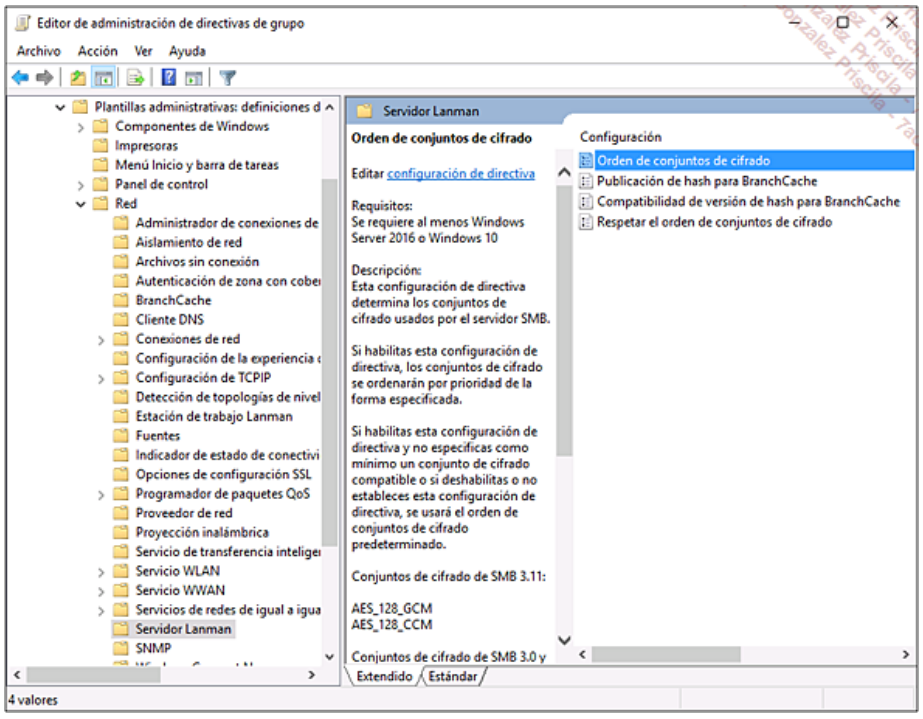
Entre en **PAR-DC01** y abra la consola de **administración de directivas de grupo** desde el Administrador del servidor, en **Herramientas**.

Despliegue el árbol de la consola, haga clic con el botón derecho en la OU **FORMACION\Servidor_BranchCache** y haga clic en **Crear un GPO en este dominio y vincularlo aquí**.

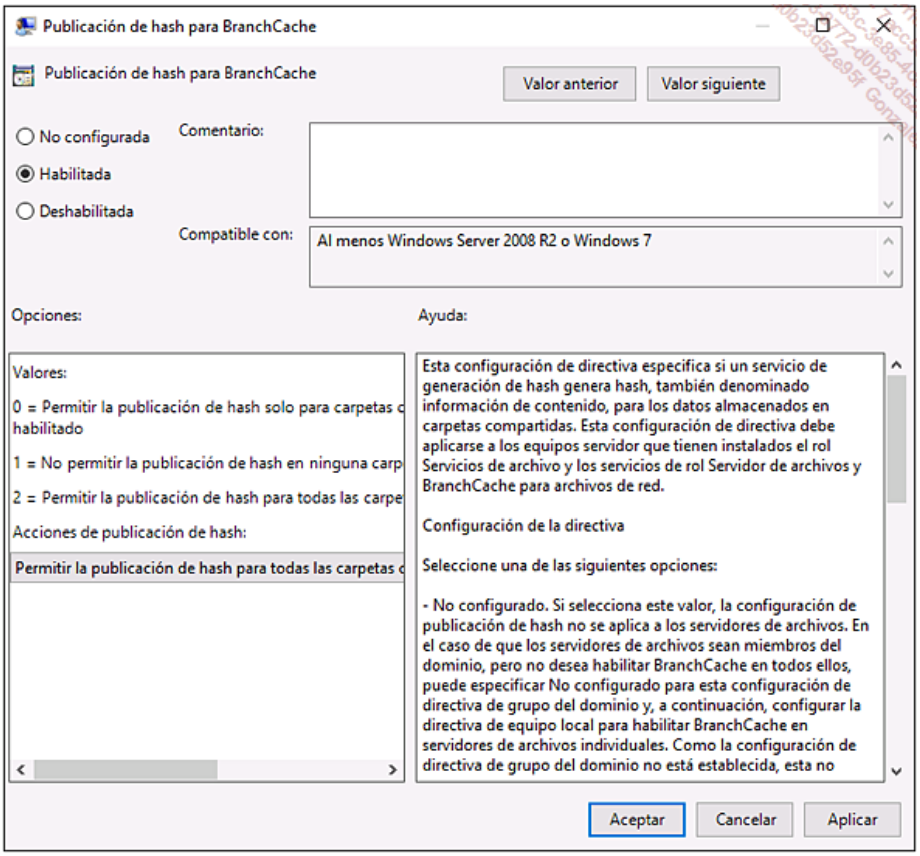
Llame a la directiva de grupo **Hash - BranchCache** y haga clic en **Aceptar**.



Despliegue el árbol de la consola y seleccione la siguiente carpeta: **Configuración del equipo - Directivas - Plantillas administrativas - Red - Servidor Lanman**.



Haga doble clic en el parámetro **Publicación de hash para BranchCache** para editarlo y, a continuación, marque la opción **Habilitada** y seleccione el valor **Permitir la publicación de hash para todas las carpetas compartidas**. A continuación, haga clic en **Aceptar**.



Cierre la consola **Editor de directivas de grupo**.

En la máquina **PAR-SRV1**, ejecute el siguiente comando:

```
gpupdate /force
```

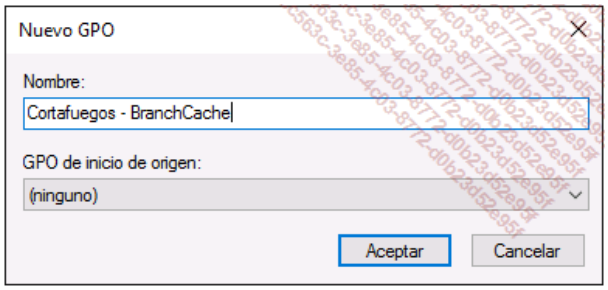
Reinicie la máquina virtual.

Configurar el cortafuegos de los clientes: PAR-DC01

Entre en **PAR-DC01** y abra la consola de **administración de directivas de grupo** desde el Administrador del servidor, en **Herramientas**.

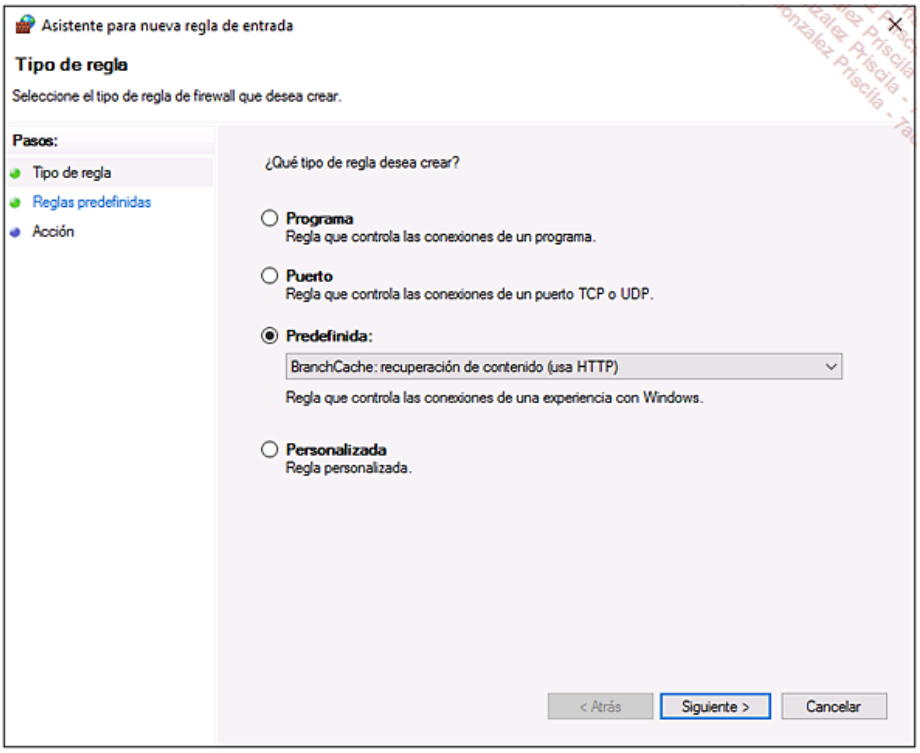
Despliegue el árbol de la consola, haga clic con el botón derecho en la OU **FORMACION\BranchCache_Client** y haga clic en **Crear un GPO en este dominio y vincularlo aquí**.

Llame a la directiva de grupo **Cortafuegos - BranchCache** y haga clic en **Aceptar**:



Despliegue el árbol de la consola y seleccione la siguiente carpeta: **Configuración del equipo - Directivas - Configuración de Windows - Configuración de seguridad - Firewall de Windows con seguridad avanzada - Firewall de Windows con seguridad avanzada - Reglas de tráfico entrante**. Haga clic con el botón derecho en **Reglas de entrada** y, a continuación, en **Nueva regla**.

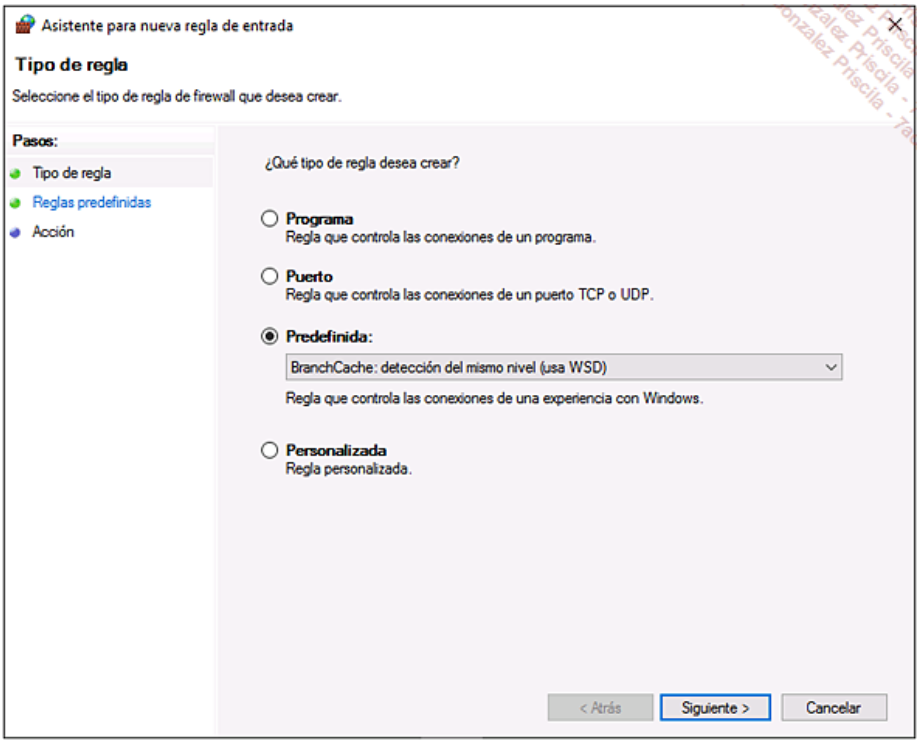
Seleccione la opción **Predefinida** y, a continuación, **BranchCache: recuperación de contenido (usa HTTP)**.



En la ventana **Reglas predefinidas**, compruebe la información mostrada y haga clic en **Siguiente**.

En la ventana **Acción**, marque la opción **Permitir la conexión** y, a continuación, haga clic en **Finalizar**.

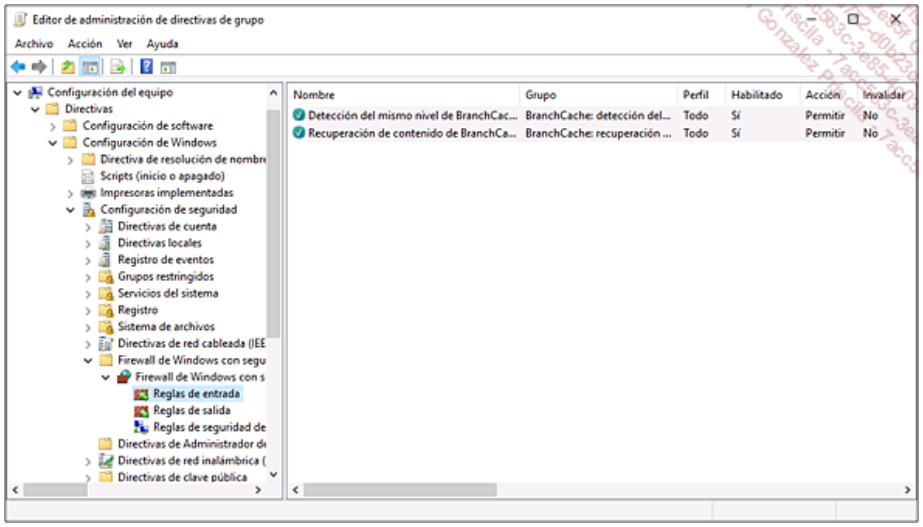
Cree otra nueva regla de tráfico entrante. Marque la opción **Predefinida** y, a continuación, seleccione la regla **BranchCache: detección del mismo nivel (usa WSD)** y haga clic en **Siguiente**.



En la ventana **Reglas predefinidas**, compruebe la información que se muestra y haga clic en **Siguiente**.

En la ventana **Acción**, marque la opción **Autorizar la conexión** y, a continuación, haga clic en **Finalizar**.

Compruebe la presencia de las dos reglas.



En **CL10-01**, inicie una sesión como administrador del dominio y ejecute en una consola de línea de comandos:

```
gpupdate /force
```

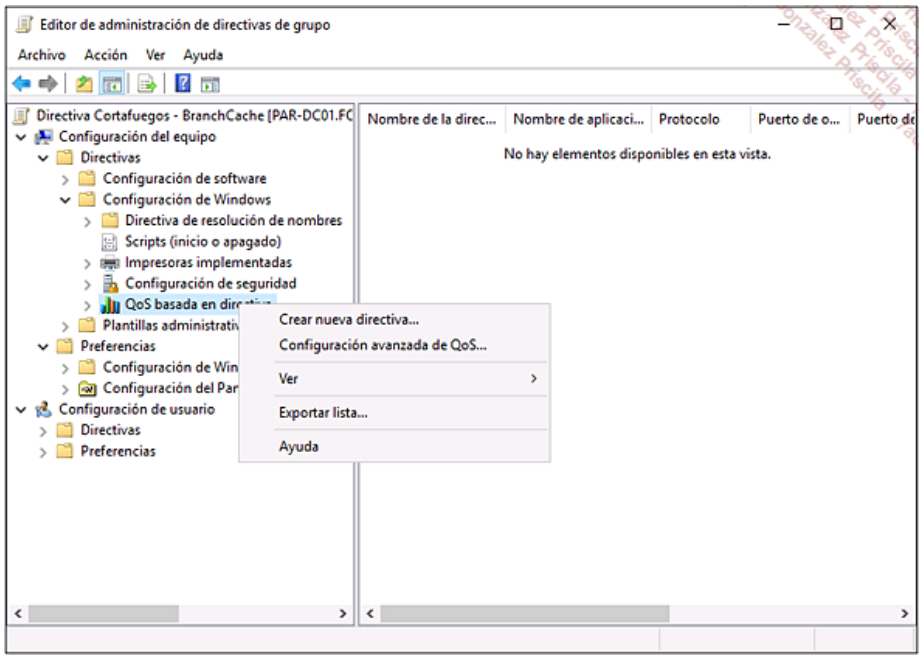
Validación de la configuración: PAR-SRV1

El siguiente procedimiento permite simular una conexión lenta para el sitio remoto. Esta operación debe realizarse únicamente en un entorno de test para validar el funcionamiento de BranchCache en nuestra maqueta.

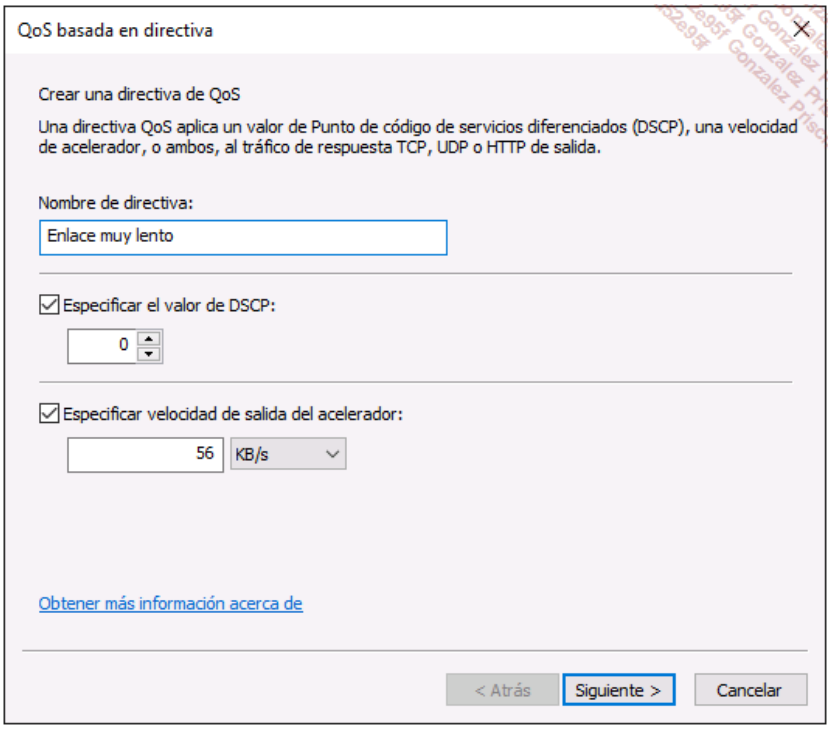
En el servidor de archivos **PAR-SRV1**, escriba el siguiente comando para abrir el **Editor de directivas de grupo local**:

```
gpedit.msc
```

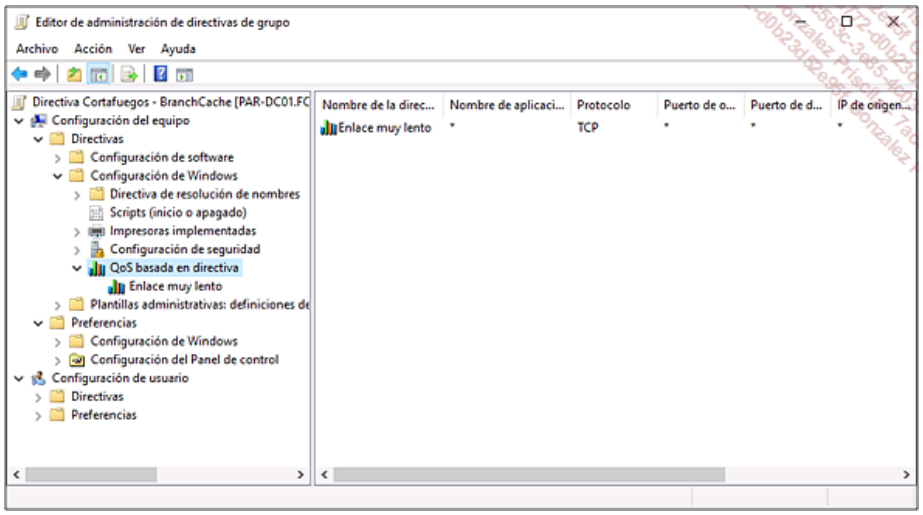
Despliegue el árbol de la consola hasta el siguiente nodo: **Configuración del equipo - Configuración de Windows**. Seleccione **QoS basada en directiva**, haga clic con el botón derecho y haga clic en **Crear nueva directiva**:



En el campo **Nombre de directiva**, escriba **Enlace muy lento**. Marque la opción **Especificar velocidad de salida del acelerador** y escriba el valor **56 KB/s** para simular un sitio remoto conectado a la sede mediante un módem de 56 K. A continuación, haga clic tres veces en**Siguiente** y después en **Finalizar**.



Compruebe que la directiva de QoS llamada **Enlace muy lento** aparece en la consola **Editor de directivas de grupo** y, a continuación, cierre la ventana.



En el servidor de archivos **PAR-SRV1**, copie el archivo Notepad.exe (ubicado en la carpeta de Windows) hasta la carpeta c:\BranchCacheFiles.

Inicie una sesión en **CL10-01** y acceda al recurso compartido \\PAR-DC01\BranchCacheFiles\.

Copie el archivo Notepad.exe al escritorio de la estación **CL10-01**.

El archivo tardará mucho tiempo antes de copiarse en la máquina, pues hemos creado una directiva de QoS para simular un enlace muy lento.

Inicie una sesión en **CL10-02** y acceda al recurso compartido \\PAR-DC01\BranchCacheFiles\.

Copie el archivo Notepad.exe en el escritorio de la estación **CL10-02**.

Validación de conocimientos adquiridos: preguntas/respuestas

1. Preguntas

Puede validar los conocimientos adquiridos respondiendo a las siguientes preguntas.

1. ¿Qué permite hacer la funcionalidad DFS?
2. ¿Cuál es el objetivo de la replicación DFS?
3. ¿Es posible utilizar la replicación DFS sin instalar el espacio de nombres DFS?
4. ¿Cuáles son los dos tipos de espacios de nombres que es posible configurar?
5. ¿Qué aporta el modo Windows Server 2008?
6. ¿Qué es ABE?
7. ¿Qué niveles funcionales son necesarios para implementar el modo Windows Server 2008?
8. ¿Qué ventaja supone utilizar la compresión diferencial remota?
9. ¿Cuál es el objetivo de la carpeta DFSrPrivate\ConflictandDeleted?
10. ¿Cuál es el objetivo de la desduplicación de datos?
11. ¿Es posible utilizar la desduplicación sobre una partición de sistema?
12. ¿Cómo se realizan las operaciones de exportación y de importación de la base de datos?
13. ¿Es necesario instalar el servicio de replicación DFS para asegurar la alta disponibilidad en un espacio de nombres DFS?
14. ¿Qué es la tecnología BranchCache?
15. En la implementación de BranchCache, ¿qué es el modo de caché hospedada?
16. En la implementación de BranchCache, ¿qué es el modo de caché distribuida?

2. Resultados

Consulte las siguientes páginas para comprobar sus respuestas.

Por cada respuesta correcta, cuente un punto.

Número de puntos: /16

Para superar este capítulo, su puntuación mínima debería ser de 14 sobre 16.

3. Respuestas

1. ¿Qué permite hacer la funcionalidad DFS?

   DFS es un sistema que facilita la administración de un sistema de archivos. Ofrece, a una empresa, una tolerancia a fallos redirigiendo a los usuarios hacia otro servidor en caso de producirse algún error grave.

2. ¿Cuál es el objetivo de la replicación DFS?

   La replicación DFS tiene como objetivo replicar los datos de un servidor a otro.

3. ¿Es posible utilizar la replicación DFS sin instalar el espacio de nombres DFS?

   Sí, es posible utilizar la replicación DFS sin tener que configurar un espacio de nombres DFS.

4. ¿Cuáles son los dos tipos de espacios de nombres que es posible configurar?

   Tras la configuración del espacio de nombres, es preciso seleccionar los tipos de espacio de nombres deseados. Existen dos opciones posibles, los espacios de nombres basados en un dominio y los que son autónomos.

5. ¿Qué aporta el modo Windows Server 2008?

   El modo Windows Server 2008 aporta nuevas funcionalidades tales como ABE, aunque también tienen la posibilidad de tener varios destinos de carpeta.

6. ¿Qué es ABE?

   ABE, o Access Based Enumeration, permite mostrar únicamente aquellas carpetas sobre las que el usuario tiene acceso.

7. ¿Qué niveles funcionales son necesarios para implementar el modo Windows Server 2008?

   El modo Windows Server 2008 requiere, como mínimo, un nivel funcional Windows Server 2003 a nivel del bosque y un nivel Windows Server 2008 a nivel del dominio.

8. ¿Qué ventaja supone utilizar la compresión diferencial remota?

   La compresión diferencial remota permite replicar únicamente las modificaciones aportadas.

9. ¿Cuál es el objetivo de la carpeta DFSrPrivate\ConflictandDeleted?

Esta carpeta contiene los archivos que presentaron algún conflicto y lo "perdieron", tras la resolución del mismo.

10 ¿Cuál es el objetivo de la desduplicación de datos?

El objetivo de esta funcionalidad es optimizar el espacio en disco. De este modo, un bloque idéntico contenido en varios archivos se almacena una única vez.

11 ¿Es posible utilizar la desduplicación sobre una partición de sistema?

No, es imposible utilizar la desduplicación en una partición de sistema, solo puede aplicarse en una partición de datos.

12 ¿Cómo se realizan las operaciones de exportación y de importación de la base de datos?

Las operaciones de importación y de exportación de la base de datos se realizan mediante cmdlets de PowerShell. Para realizar la operación de exportación, se utiliza Export-DFSrClone, la importación se opera con Import-DfsrClone.

13 ¿Es necesario instalar el servicio de replicación DFS para asegurar la alta disponibilidad en un espacio de nombres DFS?

Sí, el servicio de replicación DFS es un requisito previo.

14 ¿Qué es la tecnología BranchCache?

La tecnología BranchCache permite reducir los flujos de red poniendo en caché los archivos más utilizados en un servidor o en la caché de los clientes.

15 En la implementación de BranchCache, ¿qué es el modo de caché hospedada?

El modo de caché hospedada funciona con un servidor de caché en el sitio remoto. Cada archivo consultado por los usuarios del sitio remoto puede ponerse en caché en el servidor de caché para que los demás usuarios puedan acceder de manera local al archivo sin tener que utilizar los flujos WAN.

16 En la implementación de BranchCache, ¿qué es el modo de caché distribuida?

El modo de caché distribuida permite autorizar los puestos clientes a poner en caché de manera local los archivos consultados. Cada puesto cliente que realice una petición de acceso a un archivo consultará primero el resto de los equipos de la misma red para saber si alguno posee la copia del archivo en caché.

Requisitos previos y objetivos

1. Requisitos previos

Poseer conocimientos avanzados sobre la red.

Poseer buenos conocimientos del hipervisor Hyper-V.

Poseer nociones de cloud computing.

2. Objetivos

Ser capaz de describir las novedades aportadas por Windows Server 2016.

Ser capaz de configurar las funcionalidades avanzadas de Hyper-V.

Introducción

Microsoft ha introducido nuevas funcionalidades de red en Windows Server 2016 que permiten mejorar el rendimiento de las máquinas virtuales, así como su seguridad. Encontramos **Server Message Block** (SMB), ahora en versión 3.1.1, y nuevas opciones de **Quality of Service** (QoS). Microsoft da soporte a nuevas funcionalidades de las máquinas virtuales ,así como de los hosts Hyper-V, con la funcionalidad de máquina virtual dinámica Queuing (Dynamic VMQ) y el soporte de la asociación de tarjetas de red NIC Teaming para las máquinas virtuales.

Las funcionalidades de red

Los Data Center (centros de datos) están, actualmente, interconectados. También están conectados a la Cloud. Con objeto mejorar su rendimiento de manera global, el NIC Teaming se generaliza para asegurar la redundancia, o bien para aumentar el ancho de banda disponible.

1. NIC Teaming

Se trata de la agrupación lógica de tarjetas de red (creación de un **Team**). En esta asociación, es posible agregar hasta 32 tarjetas de red y utilizarlas como una interfaz de red lógica única. El NIC Teaming asegura la redundancia permitiendo la comunicación de red mediante la interfaz de red lógica, incluso aunque una de las tarjetas falle o si un enlace de red deja de estar disponible.

La asociación de tarjetas de red mejora también el ancho de banda disponible de la interfaz de red lógica única de manera similar a como lo hace la tecnología LACP o la tecnología Etherchannel. Se trata de una funcionalidad que se presentó con Microsoft Windows Server 2012 y que se ha mejorado en la versión 2016.

El host Hyper-V y los equipos virtuales Hyper-V pueden utilizar la funcionalidad de NIC Teaming. Una asociación de tarjetas de red puede contener una única tarjeta de red (aunque en este caso la asociación de tarjetas de red no puede proveer un equilibrio de carga ni una conmutación por error). Sin embargo, puede utilizar un equipo NIC (asociación de tarjetas de red) con un único adaptador de red para separar el tráfico de red cuando utiliza redes de área local virtuales (VLAN).

Si desea mejorar la tolerancia a fallos de la conectividad de red y el rendimiento de su host Hyper-V, debe desplegar varios adaptadores de red y a continuación agruparlos en equipo.

Con Windows Server 2016, ahora puede utilizar la funcionalidad de vSwitch Embedded Teaming (SET) como un conmutador virtual de Microsoft Hyper-V, con un límite de 8 tarjetas de red físicas. Estas tarjetas de red virtuales ofrecen un buen rendimiento y una tolerancia a fallos en caso de que falle algún adaptador de red. También puede utilizar el modo RDMA (*Remote Direct Memory Access*), que puede gestionarse a nivel del conmutador virtual.

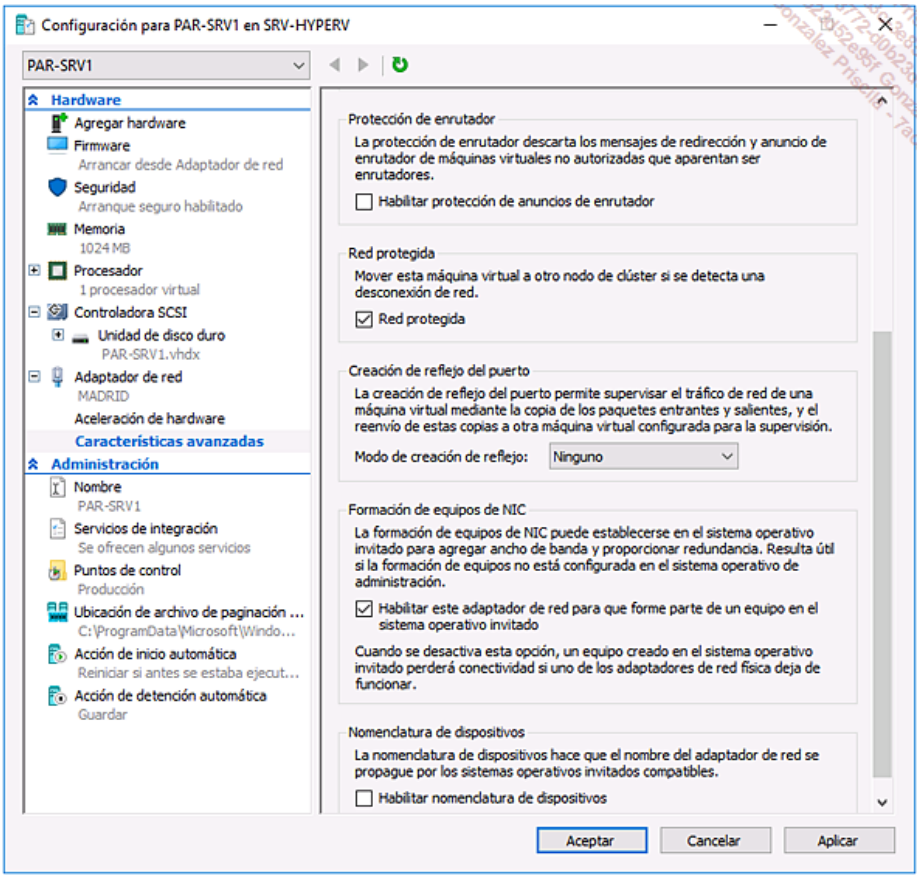
a. Configuración de un host Hyper-V

La configuración de este vSwitch se realiza a través de PowerShell con el siguiente comando:

```
New-VMSwitch -Name SETswitch -NetAdapterName "Ethernet","Ethernet 2"
-EnableEmbeddedTeaming $true
```

b. Configuración de una máquina virtual

Para activar el NIC Teaming para las máquinas virtuales Hyper-V, hay que modificar la configuración de la tarjeta de red en Hyper-V, seleccionar **Características avanzadas** y habilitar la opción **Formación de equipos de NIC**.



También es posible realizar esta operación con Windows PowerShell:

```
Set-VMNetworkAdapter -VMName PAR-SRV1 -AllowTeaming On
```

2. Mejora del protocolo SMB

La última versión de SMB es SMB 3.1.1, incluida con Windows 10 y Windows Server 2016. SMB 3.1.1 es compatible con el cifrado Advanced Encryption Standard (AES) 128 Galois/Counter Mode (GCM), además del sistema 128 AES con encriptación CBC-MAC (CCM) incluido en SMB 3.0, y el protocolo SMB se aplica a un control de integridad preautenticación utilizando el hast Secure Hash Algorithm (SHA) 512. SMB 3.1.1 requiere a su vez una negociación de seguridad aumentada cuando se conecta a través de dispositivos que utilizan SMB 2.x o superior.

Hyper-V soporta ahora el almacenamiento de los archivos de configuración de la máquina virtual, así como los puntos de control de máquinas virtuales. Por el contrario, es obligatorio trabajar sobre servidores de archivos que ejecuten Windows Server 2012 o superior. Las versiones anteriores de Windows Server no soportan los recursos compartidos SMB 3.0.

Se recomienda encarecidamente conectase a un recurso compartido SMB 3.0 o superior a través de una conexión rápida de 1 Gb/s o superior.

Un recurso compartido de archivos SMB 3.0 es una alternativa al almacenamiento de archivos de equipos virtuales sobre dispositivos iSCSI (*Internet Small Computer System Interface*) o redes de almacenamiento Fibre Channel (San). Durante la creación de una máquina virtual en Hyper-V con Windows Server 2012 o superior, puede especificar un recurso compartido de red cuando se selecciona la ubicación de la máquina virtual y la ubicación del disco duro virtual. También puede agregar discos VHD o VHDX almacenados en recursos compartidos de red SMB 3.0 o superior.

a. Mejoras introducidas con SMB 3.0 en Windows Server 2012 R2

He aquí las principales mejoras del protocolo SMB 3.0:

- **Conmutación por error transparente de SMB**. En un clúster de archivos, es posible realizar el mantenimiento de un servidor miembro del clúster de archivos sin interrumpir el acceso a los datos que se encuentran en el recurso compartido.
- **SMB Scale Out**. En un Cluster Shared Volumes (CSV) en versión 2, los recursos compartidos creados permiten un acceso simultáneo a los archivos. Todos los servidores pueden tener acceso a los archivos, lo cual garantiza una alta disponibilidad.

Se han introducido otras mejoras, como el soporte del NIC Teaming para conectarse a un recurso compartido, el Multipathing (varias rutas de red para alcanzar un mismo destino) o el soporte de las tarjetas de red RDMA (*Remote Direct Memory Access*) para reducir la latencia en la red. Del lado de la seguridad, SMB permite la encriptación extremo a extremo de la comunicación entre el cliente y el servidor. Ahora es posible realizar la administración de los recursos compartidos SMB con Windows PowerShell. Por último, la funcionalidad **SMB Directory Leasing**mejora

los tiempos de respuesta de las aplicaciones que se ubican en sitios remotos. Reduce el número de intercambios entre el cliente y el servidor, pues los metadatos se recuperan desde una caché.

b. Mejoras introducidas con SMB 3.1.1 en Windows Server 2016

Un cambio que no aporta ninguna funcionalidad es la notación de la versión de SMB que, en lo sucesivo, utiliza tres letras x.y.z y un número de revisión distinto de cero. A partir de Windows Server 2016, se utilizan tres cifras distintas para indicar la versión de SMB.

Las aportaciones de Windows Server 2016 refuerzan la seguridad con una preautenticación, así como con los protocolos utilizados para encriptar, compatibles con AES-128-GCM. Este protocolo está mejor gestionado en los procesadores modernos, pues poseen instrucciones de hardware para acelerar el procesamiento. Siempre del lado de la seguridad, es posible deshabilitar la integridad y la autenticación previamente activas por defecto en los servidores y clientes SMB 3.1.1. Estas funcionalidades mejoran la compatibilidad con las rutas de red para almacenar los archivos de configuración y los discos duros de nuestras máquinas virtuales, pero cabe destacar cambios en la compartición de datos sensibles de dominios, carpetas SYSVOL y NETLOGON, que requieren ahora, con Windows Server 2016 y Windows 10, una autenticación mutua y autenticada.

Para los clústeres de archivos (*Scale-out File Server* - SoFS), Microsoft es compatible con la funcionalidad Cluster Rolling Upgrade a través de la funcionalidad **Cluster Dialect Fencing**.

Respecto al almacenamiento y los clústeres de almacenamiento, Storage Spaces Direct permite generar sistemas de almacenamiento con una alta disponibilidad y evolutivos con un almacenamiento local. Se trata de un avance importante en el dominio del almacenamiento en los servidores Windows por dos motivos:

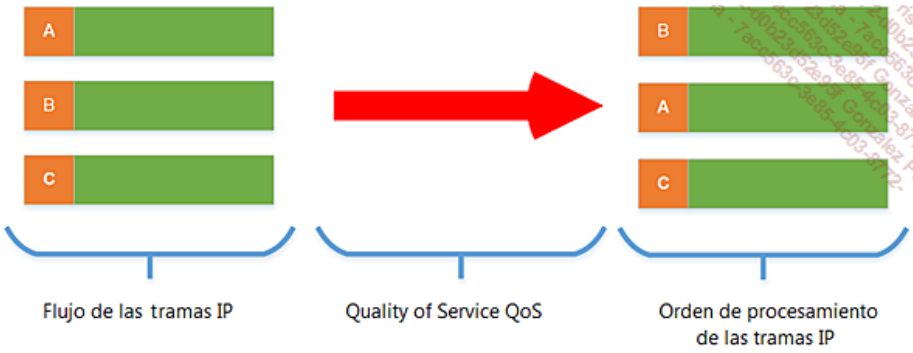
- Facilita el despliegue y la administración de los sistemas de almacenamiento.
- Los espacios de almacenamiento directo se basan en servidores estándar equipados de lectores locales para crear un almacenamiento mutualizado, con alta disponibilidad y evolutivo para obtener un coste netamente inferior respecto a las bahías SAN o NAS tradicionales.

Windows Server 2016 es compatible con otras mejoras de hardware, como la caché de los datos, el cifrado, así como los discos duros SSD con un controlador de tipo NVMe que ofrece una eficacia y un rendimiento sin igual.

3. La Calidad del Servicio QoS

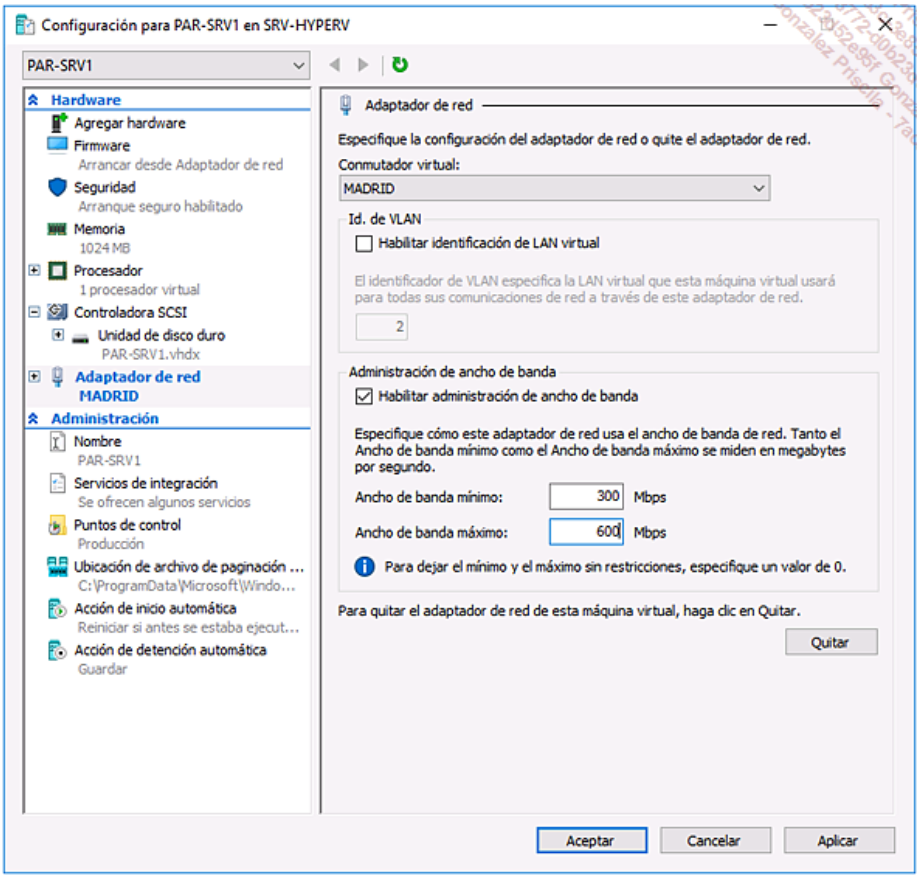
La QoS es un conjunto de tecnologías que permite responder a muchas exigencias de la red en términos de ancho de banda disponible. Con la QoS es posible jerarquizar la red y, por lo tanto, determinar prioridades. Esto quiere decir que el tráfico que posea una prioridad más elevada se tratará y encaminará primero.

Por ejemplo, puede utilizar la QoS para priorizar tráficos de red como la voz o el vídeo en streaming, muy sensibles a la latencia, y para controlar el impacto del tráfico independiente de la latencia de los demás flujos de la red.

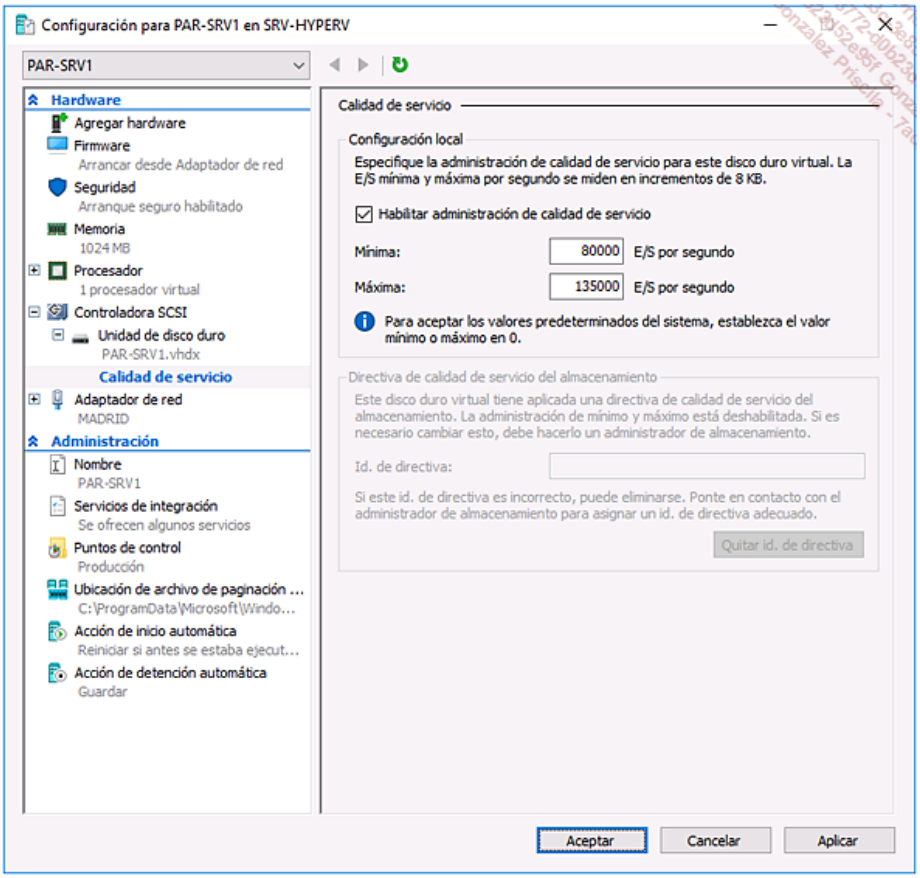


He aquí algunos ejemplos de uso de la funcionalidad QoS:

- **Administrar el ancho de banda**. La funcionalidad QoS permite administrar el ancho de banda para la convergencia de varios tipos de tráfico a través de la tarjeta de red de la máquina virtual. Es posible asignar o definir un ancho de banda mínimo y máximo; esta asignación se realiza únicamente por máquina virtual.
- **Clasificación y etiquetado**. Antes de poder gestionar el ancho de banda para una carga de trabajo, debe clasificar o filtrar este flujo de red con el planificador de paquetes QoS disponible en la funcionalidad Data Center Bridging. Windows Server 2016 simplifica la tarea de administración para que pueda utilizar filtros integrados en Windows PowerShell para clasificar los flujos que se utilizan con más frecuencia.
- **QoS** basada en directivas y **QoS Hyper-V**. La QoS, basada en directivas para administrar el tráfico de red en una red física. Permite especificar la cantidad de ancho de banda de red que debe utilizarse en función de cada tipo de aplicación. Se configura a través de la directiva de grupo AD DS. Aparece una nueva función en QoS llamada QoS Hyper-V, que permite administrar el tráfico en la red virtual.



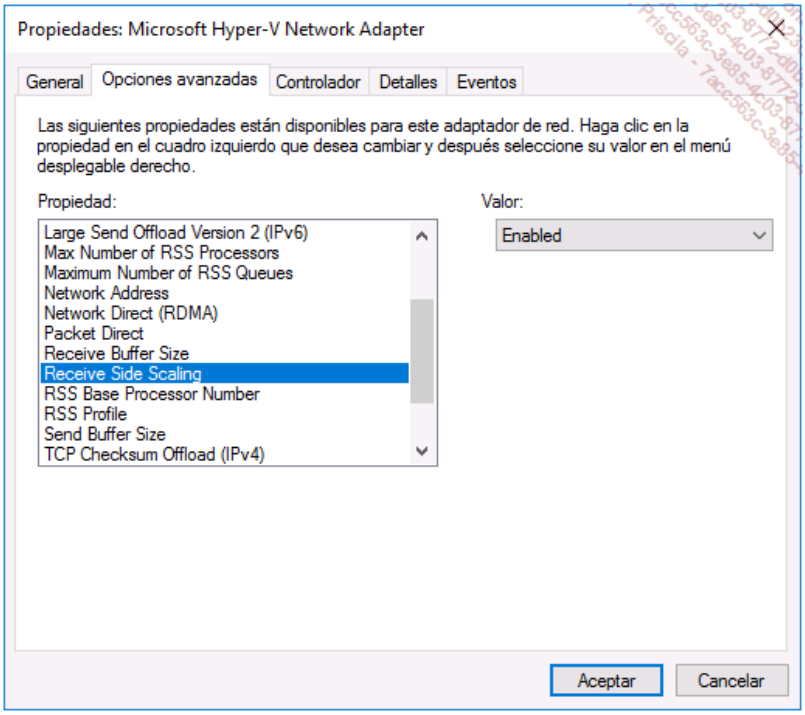
A partir de Windows Server 2012, Hyper-V incluye la posibilidad de definir los parámetros de QoS para el almacenamiento en máquinas virtuales. Los discos duros virtuales se ven impactados por la configuración de los parámetros de QoS. Cuando configura los parámetros de QoS, puede especificar el número máximo de entradas/salidas (IOPS) para el disco duro virtual, lo que minimiza la probabilidad de que un único disco duro virtual consuma la mayoría de la capacidad de las IOPS del almacenamiento subyacente. También puede configurar un disco duro virtual para que se produzca una alerta si el número de E/S es inferior a un determinado umbral. Las E/S se miden en incrementos de 8 kbytes. No es posible configurar el almacenamiento QoS si se utilizan discos duros virtuales compartidos.



Windows Server 2016 utiliza ahora el almacenamiento QoS para gestionar las directivas QoS de Hyper-V y para los servidores de archivos Scale-Out.

4. Compartir el tráfico entrante (RSS, Receive Side Scaling)

La funcionalidad RSS que comparte el tráfico entrante ya existía en Windows Server 2012. Permite a las tarjetas de red distribuir la carga de procesamiento de red en modo núcleo sobre varios cores de procesadores en los equipos multicore. Windows Server 2016 incluye esta funcionalidad en las máquinas virtuales RSS alojadas en un host Hyper-V en versión 2016. Esto permite a las máquinas virtuales soportar mayores cargas de red.



Esta funcionalidad se configura en la tarjeta de red dentro de la configuración avanzada, o también a través de PowerShell con el comando:

```
Enable-NetAdapterRSS -Name "Ethernet0"
```

Aquí se habilita RSS para la tarjeta de red llamada Ethernet0.

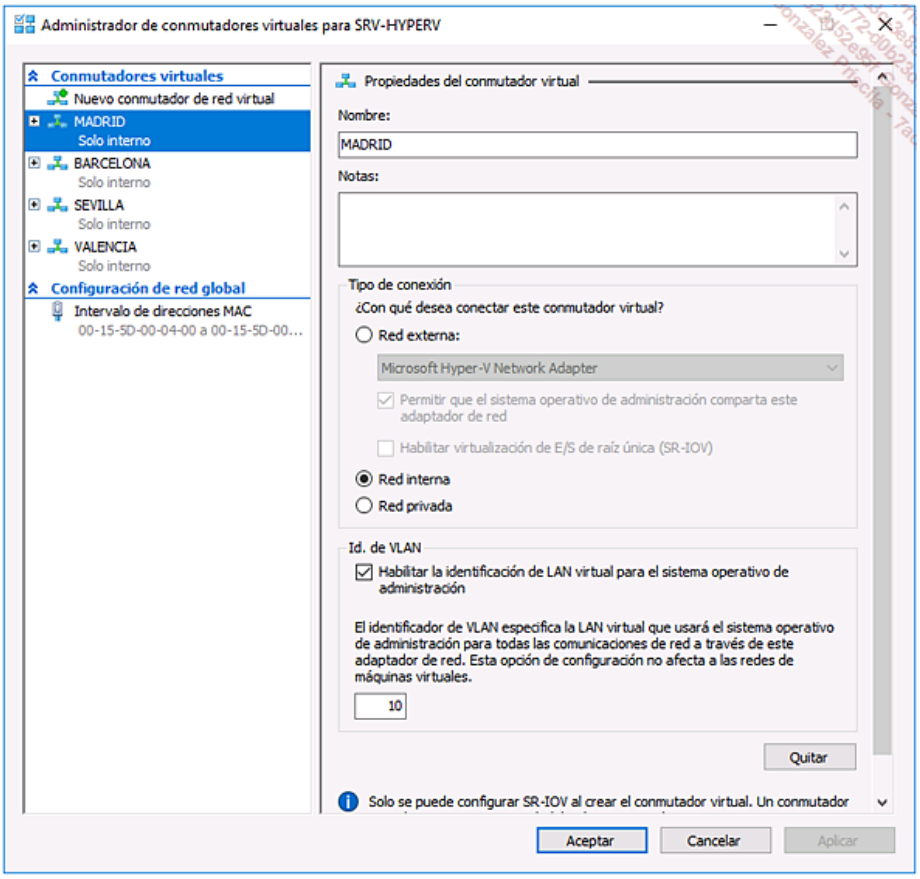
Las funcionalidades de red avanzadas

Los conmutadores virtuales en Hyper-V son dispositivos virtuales que puede gestionar desde el administrador de conmutadores virtuales o mediante PowerShell. Los conmutadores virtuales controlan la circulación del tráfico de red entre los equipos virtuales alojados en un servidor Hyper-V y la forma en la que el tráfico transita entre los equipos virtuales y el resto de la red física.

Este rol Hyper-V de Windows Server 2012 y Windows Server 2016 considera tres tipos de conmutadores virtuales.

- **Red externa**. Este tipo de conmutador le permite mapear una red a una tarjeta de red específica o un equipo adaptador de red (NIC Teaming). Windows Server 2016 permite mapear una red externa con un adaptador inalámbrico si se encuentra instalado el servicio de red local inalámbrica en el servidor Hyper-V y el servidor posee una tarjeta de red compatible.
- **Red interna**. Puede utilizar conmutadores virtuales internos para permitir la comunicación entre equipos virtuales, incluido el propio host Hyper-V.
- **Red privada**. Puede utilizar conmutadores privados para permitir que las máquinas virtuales se comuniquen entre sí únicamente. De este modo, los equipos virtuales no podrán contactar con el host Hyper-V.

Cuando configura una red virtual, también puede configurar un número de VLAN ID.



1. Las funcionalidades de red avanzadas desde Windows Server 2012 y R2

La siguiente tabla muestra las funcionalidades de red presentes desde Windows Server 2012:

Funcionalidades	Descripción
Virtualización de red	Esta funcionalidad permite que las direcciones IP de las VM estén virtualizadas en los entornos que las alojan para que las máquinas virtuales migradas a otro host Hyper-V puedan mantener sus direcciones IP originales.
Administración de ancho de banda	Esta funcionalidad le permite especificar un ancho de banda mínimo y máximo que Hyper-V asignará al adaptador. Hyper-V reserva una cantidad de ancho de banda mínimo para la tarjeta de red.
Protección DHCP (*DHCP guard*)	La protección DHCP elimina los mensajes de servidor DHCP de los equipos virtuales no autorizados que se hacen pasar por servidores DHCP.
Protección router (*Router guard*)	La protección Router guard elimina los mensajes de redirección y de anuncio de router (Enrutamiento y enrutamiento dinámico) de los equipos virtuales no autorizados que se hacen pasar por routers.
Puerto en espejo	Puede utilizar esta funcionalidad para copiar los paquetes entrantes y

	salientes de una tarjeta de red en otra máquina virtual que ha configurado para la supervisión.
Virtual Machine Queue	Esta funcionalidad requiere que el equipo host disponga de una tarjeta de red compatible con esta funcionalidad. VMQ utiliza el filtrado hardware de paquetes para entregar el tráfico de red directamente a un invitado. Esto mejora el rendimiento, pues el paquete no necesita copiarse desde el sistema operativo del host hasta la máquina virtual. Solo los adaptadores de red específicos de Hyper-V soportan esta funcionalidad.
SR-IOV	Esta característica requiere que el hardware y ciertos drivers especiales estén instalados en el sistema operativo invitado. SR-IOV permite a varios equipos virtuales compartir los mismos recursos de hardware (PCI) de interconexión de dispositivos físicos. Si no hay bastantes recursos disponibles, se restablece la conectividad de red para que el conmutador virtual provea esta conectividad. Esta funcionalidad está soportada únicamente en los dispositivos de red específicos de Hyper-V.
VLAN privadas (*Private VLANs*)	Compatibilidad con VLAN privadas que pueden ser de tres tipos: • **Aislada**. Comunica únicamente con los puertos de broadcast en la VLAN privada. • **Broadcast**. Comunica con todos los puertos de la VLAN privada. • **Comunidad**. Comunica con los puertos de la misma comunidad y con los puertos de broadcast de la VLAN privada.
Modo agregación (*Trunk mode*)	El modo Trunk permite transitar a través de un único enlace de red varios paquetes IP de VLAN diferentes.
Funcionalidades aportadas por Windows Server 2012 R2	
Compatibilidad con las ACL	Puede utilizar ACL de puerto extendido en un conmutador virtual Hyper-V para aplicar directivas de seguridad y una protección de cortafuegos a nivel de los conmutadores para los equipos virtuales.
Equilibrio de carga dinámico del tráfico de red	Cuando mapea una red virtual a un equipo de adaptadores de red en un host Hyper-V Windows Server 2012 R2, el tráfico de red se equilibrará de manera continua entre los distintos adaptadores de red, y los flujos de tráfico se desplazarán según sea necesario para mantener este equilibrio.
Enrutamiento avanzado	El módulo de virtualización de red Hyper-V transmite el tráfico de red a través de una encapsulación de enrutamiento genérico de la red de virtualización (**NVGRE**).

2. Las novedades con Windows Server 2016

Las mejoras en las funcionalidades avanzadas de Hyper-V son:

- **Virtualización de las funciones de red**. En la mayoría de los centros de datos, los dispositivos de hardware gestionan ciertas funciones o servicios de red, tales como el equilibrio de la carga de las aplicaciones y la traducción de direcciones de red, los servicios proporcionados por el cortafuegos de los Data centers y los servicios de puerta de enlace para el servicio de acceso remoto. Sin embargo, con las redes definidas por software, cada vez hay más dispositivos virtuales. Las tres funciones están disponibles en Windows Server 2016.
- **Controladora de red**. Utilizando el controlador de red, puede tener una ubicación central para supervisar, administrar, resolver problemas y configurar de manera unificada su entorno físico y virtual.
- **Conmutador integrado de agrupamiento (SET)**. Nueva opción de agrupamiento de tarjetas de red que pueden utilizarse con Hyper-V, que permite mejorar el rendimiento y la tolerancia a fallos respecto al agrupamiento clásico.
- **Colas de espera múltiples para las máquinas virtuales (VMQ)**. Esta funcionalidad asigna varias colas de espera de hardware para cada máquina virtual, mejorando así el rendimiento respecto a Windows Server 2012 R2.

Dynamic VMQ es una mejora introducida con Windows Server 2016. Permite distribuir dinámicamente el tráfico de red en los núcleos del procesador host físico según la carga de la red y el uso del procesador. De este modo, cuando se sobrecarga la red, Dynamic VMQ reparte automáticamente la carga en los demás procesadores. Dispone de un nuevo algoritmo adaptativo que permite modificar la afinidad de procesador de las colas de espera sin tener que eliminarlas y volver a crearlas, como se hacía antes. Esto se traduce en un mejor rendimiento.

3. Hyper-V y los contenedores

Cuando se utilizan contenedores, conviene tener en mente cómo queremos configurar la red para permitir a los clientes acceder a los contenedores. Por ejemplo, si desea virtualizar un servidor web, tendrá que utilizar la traducción de direcciones de red (NAT) disponible en Windows Server 2016 a través de una funcionalidad integrada en el conmutador virtual. Puede crear un switch virtual en el host de un equipo virtual ejecutando el siguiente comando:

```
New-VMSwitch -Name ”SwitchNAT” -SwitchType NAT
```

Software Defined Networking SDN

1. Introducción

SDN permite resolver ciertas limitaciones impuestas por los dispositivos de red físicos y permite a las organizaciones administrar dinámicamente sus redes. SDN utiliza una capa de abstracción software para administrar la red de manera dinámica. Para realizar esta abstracción, se despliegan Appliances o máquinas virtuales cuyo rol va a ser la administración de la red, como haría un **Windows Server Gateway**, que es un router, y una puerta de enlace virtual que permite realizar el enrutamiento entre el centro de datos, el tráfico cloud y sus redes virtuales y físicas.

Cuando implementa SDN, puede gestionar su red, virtualizarla y definir directivas para administrar el tráfico. Para implementar el Software Defined Networking, Microsoft se apoya en diversas soluciones técnicas y en su propia gama de productos:

- El **Network Controller**, un nuevo rol en Windows Server 2016.
- **RRAS Multitenant Gateway**, que permite extender los límites de una red hacia Microsoft Azure o hacia cualquier otro proveedor que ofrezca una infraestructura híbrida bajo demanda.
- Microsoft System Center, que proporciona un cierto número de tecnologías SDN, como los siguientes componentes:
  - **System Center Operation Manager** (SCOM) para monitorizar y administrar un centro de datos y una cloud privada y pública.
  - **System Center Virtual Machine Manager** (SCVMM), que permite configurar y administrar redes virtuales. También permite realizar un control centralizado de las políticas de la red virtual que apuntan hacia nuestras aplicaciones, así como una administración y configuración de los hosts Hyper-V e hipervisores de otros fabricantes.

2. La cloud

La cloud se ha definido por primera vez por el NIST (*National Institute of Standards & Technology*) en 2009 y la versión final data de 2011. La cloud computing debe responder a los siguientes criterios:

- Cinco características:
  - Debe estar accesible en el conjunto de una red.
  - La mutualización de recursos.
  - Debe ser elástica (capacidad para responder rápidamente a un cambio de las necesidades).
  - El servicio debe ser medible.
  - El servicio debe ser de tipo autoservicio.
- Cuatro modelos de despliegue:
  - **Cloud privada**, solución implementada en el seno de una misma empresa.
  - **Cloud comunitaria**, cloud que agrupa a personas de una misma profesión (notarios, hospitales).
  - **Cloud pública**, la más conocida es Internet.
  - **Cloud híbrida**, el hecho de comunicar dos o varios tipos de cloud.
- Tres modelos de servicio:
  - Modelo **SaaS** (*Software as a Service*): uso de una aplicación bajo demanda.
  - Modelo **PaaS** (*Platform as a Service*): hacer disponible una plataforma por software (máquinas virtuales) para el desarrollo.
  - Modelo **IaaS** (*Infrastructure as a Service*): hacer disponible una infraestructura informática, máquinas físicas o virtuales.

La responsabilidad de las empresas que prestan el servicio y de los clientes varía en función de estos tres tipos de modelo de servicio.

3. Despliegue de SDN

La instalación de un Software Defined Networking puede llevarse a cabo mediante un conjunto de scripts PowerShell disponibles en el sitio github de Microsoft/SDN http://aka.ms/Iu57tt.

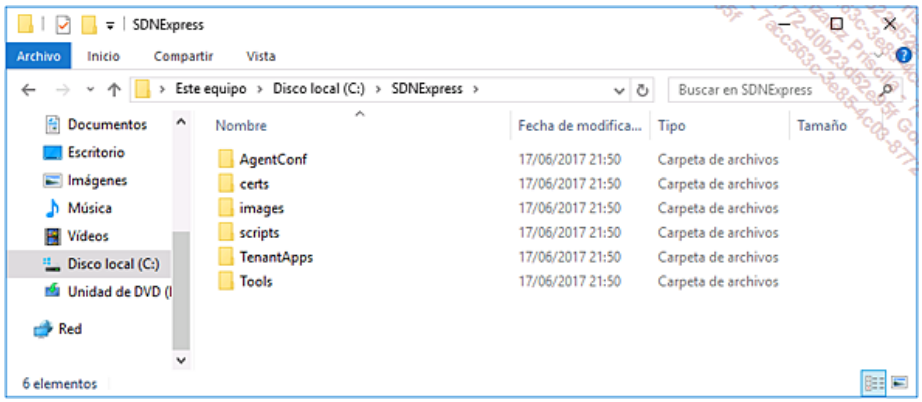
Se requieren varias etapas para desplegar un SDN:

- **Etapa n.° 1**: Instalar la red host y validar la configuración. Durante esta etapa, se habilitan e instalan todos los hosts Hyper-V, se configura la red de administración, se crean la VLAN. Es necesario instalar un dominio de Active Directory (AD DS), comprobar que el conjunto de hosts pueden interconectarse con un nombre plenamente cualificado (FQDN) y que todos los hosts Hyper-V utilizan Kerberos como método de autenticación. Para ello, se emplea el siguiente comando:

```
winrm id -r:"Hyper-V Host FQDN"
```

- **Etapa n.° 2**: Ejecutar los scripts SDN Express y validar la instalación. Es posible descargar los scripts del sitio http://aka.ms/Iu57tt y

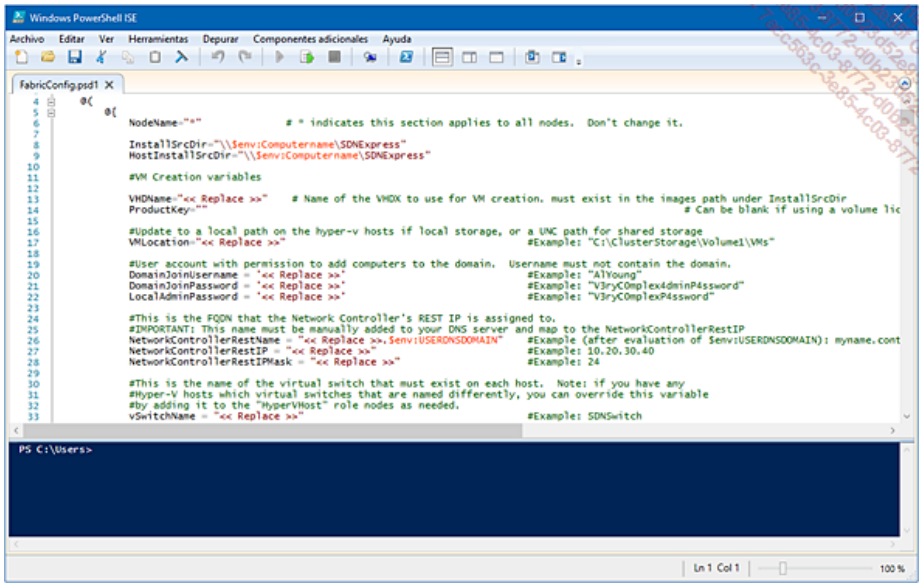
descomprimirlos en la carpeta SDNExpress.



En la carpeta **scripts**, existe un conjunto de scripts que nos permiten configurar SDN.

- **SDNExpress.ps1**. Este script se despliega y configura SDN, incluidos los ordenadores virtuales del controlador de red, las máquinas virtuales de Software Load Balancing y el conjunto de máquinas virtuales para la puerta de enlace.
- **FabricConfig.psd1**. Este script es un archivo de configuración, un modelo que nos permite personalizar nuestro entorno.
- **SDNExpressTenant.ps1**. Este script despliega en un entorno de test un ejemplo de carga de trabajo para un cliente X sobre una red virtual dotada de un VIP Load-balancing. Puede utilizar este script con una opción **Undo** para eliminar la configuración correspondiente.
- **TenantConfig.psd1**. Este script es un archivo de configuración para un cliente.
- **SDNExpressUndo.ps1**. Este script limpia un entorno en función de una fecha de arrranque.
- **SDNExpressEntrepriseExemple.ps1**. Este script provisiona una o varias empresas. El script posee una opción **Undo** para eliminar una configuración.
- **EntrepriseConfig.psd1**. Este script es un archivo de configuración.

A continuación es preciso compartir el archivo c:\SDNExpress, editar y configurar el archivo FabricConfig.psd1, así como reemplazar todos los campos cuyo valor sea **<<Replace>>** con la configuración correspondiente.



Para desplegar SDN con la cuenta de administrador de dominio, se ejecuta el siguiente comando:

```
SDNExpress.ps1 -ConfigurationDataFile FabricConfig.psd1 -Verbose
```

Para eliminar la configuración:

```
SDNExpressUndo.ps1 -ConfigurationDataFile FabricConfig.psd1 -verbose
```

Una vez ejecutado el script sin errores, se comprueba el despliegue de las máquinas virtuales. Asegúrese de que están ejecutándose un Agent Network Controller y un agente SLB (*Software Load Balancing*) en el conjunto de hosts Hyper-V con los siguientes comandos

PowerShell: `Get-Service NCHostAgent` y `Get-Service SlbHostAgent`. Compruebe a su vez la presencia del Network Controller.

- **Etapa n.° 3**: Desplegar un workload con algunas máquinas virtuales.
  - Configurar el archivo TenantConfig.psd1 y reemplazar todos los campos cuyo valor sea **<<Replace>>** con la configuración correspondiente.
  - Ejecutar el script:

```
SDNExpressTenant.ps1 -ConfigurationDataFile TenantConfig.psd1 - Verbose
```

4. Ventajas de la virtualización de redes

La virtualización de redes proporciona una capa de abstracción entre la red física y el tráfico de red, lo que otorga las siguientes ventajas:

- **Una ubicación más flexible de las máquinas virtuales**. La virtualización de la red proporciona la abstracción y separa las direcciones IP usadas en los equipos virtuales de las direcciones IP utilizadas en la red física. De este modo, puede situar una máquina virtual en cualquier host Hyper-V dentro del Data center y asignar direcciones IP donde las restricciones de aislamiento VLAN de la red física no restrinjan su ubicación.
- **Aislamiento de la red mutualizado sin VLAN**. Puede definir e imponer el aislamiento del tráfico de red sin la necesidad de utilizar VLAN o reconfigurar los conmutadores de la red física. Como la virtualización de la red utiliza un identificador de 24 bits para las redes virtuales, frente a un identificador de 12 bits para las redes locales virtuales, ya no está limitado a 4094 identificadores de VLAN. Además, con la virtualización de la red, no es necesaria ninguna reconfiguración del hardware físico cuando desplaza los equipos virtuales existentes o crea uno nuevo.
- **Reutilización de direcciones IP**. Las máquinas virtuales presentes en las distintas redes virtuales pueden utilizar el mismo espacio de direccionamiento IP o superpuesto, incluso durante el despliegue de estas máquinas virtuales en la misma red física. Las redes virtuales están aisladas y pueden utilizar el mismo espacio de direccionamiento sin ningún conflicto o problema.
- **Libre migración a través de las distintas subredes**. Gracias a la virtualización de red, puede desplazar los equipos virtuales utilizando la migración directa entre dos hosts Hyper-V de diferentes subredes sin la necesidad de modificar la dirección IP del equipo virtual.
- **Compatibilidad con el hardware existente**. No es necesario realizar ninguna modificación de la red física existente, incluso el direccionamiento no requiere ninguna modificación.
- La posibilidad de realizar desplazamientos transparentes de máquinas virtuales de una infraestructura compartida como una cloud de servicio **IaaS** hacia una plataforma **IaaS** física, donde la ejecución de máquinas virtuales se alberga en un Data center separado, generalmente accesible a través de Internet.

a. Encapsulación de enrutamiento genérico

Generic Routing Encapsulation (GRE o encapsulación de enrutamiento genérico) es un protocolo de tunneling que permite encapsular cualquier paquete de la capa de red.

GRE ha sido desarrollado por Cisco y permite encapsular una amplia gama de paquetes de distintos protocolos en paquetes IP. Los túneles GRE se construyen para no tener que mantener un estado, lo que significa que cada extremo del túnel no conserva ninguna información de estado o de disponibilidad del extremo remoto.

Windows Server 2016 e Hyper-V utilizan la virtualización de red basada en la encapsulación de enrutamiento genérico (NVGRE) para implementar la virtualización de la red.

Cuando se utiliza virtualización de la red, cada adaptador de red virtual está asociado a dos direcciones IP. Estas dos direcciones son:

- **Dirección del cliente (CA)**. Se trata de la dirección IP que se configura y que utiliza la máquina virtual. Esta dirección se configura en las propiedades del adaptador de red virtual en el sistema operativo de la máquina virtual invitada, sin importar si se utiliza virtualización de la red. Una máquina virtual utiliza la CA cuando se comunica con otro sistema, y, cuando migra una máquina virtual a otro host Hyper-V, la dirección del cliente puede ser la misma.
- **Dirección del proveedor (PA)**. Se trata de la dirección IP que la plataforma de virtualización asigna al host Hyper-V y depende de la infraestructura de red física en la que se está conectando el host Hyper-V. Cuando se utiliza virtualización de la red, y el equipo virtual envía tráfico de red, el host Hyper-V encapsula los paquetes e incluye la PA como dirección de origen a partir de la cual se envían los paquetes. La PA es visible en la red física pero invisible para la máquina virtual. Si migra un equipo virtual a un host Hyper-V diferente, la PA cambia.

Ejemplo de configuración de dos máquinas virtuales con dos clientes:

Empresa	Direcciones Clientes CA	Direcciones Proveedores PA
Empresa n.° 1	WEB : 172.16.0.2 / BDD : 172.16.0.3	WEB : 192.168.1.10 / BDD : 192.168.1.12
Empresa n.° 2	WEB : 172.16.0.2 / BDD : 172.16.0.3	WEB : 192.168.1.10 / BDD : 192.168.1.12

Para habilitar la comunicación entre equipos virtuales, debe configurar una red virtual. Por ejemplo, puede configurar una red virtual para la empresa n.° 1 con el ID de subred virtual 5051 y configurar una red virtual para la empresa n.° 2 con el ID de subred virtual 6055. Creará a su vez directivas de

virtualización de red para ambas empresas y aplicará las directivas a los distintos hosts Hyper-V que alberguen las máquinas virtuales.

Cuando la máquina virtual web de la empresa n.° 1 que está situada en el host Hyper-V 2 interroga al servidor de BDD con la dirección IP CA 172.16.0.3, el proceso se explica a continuación:

- El host 2 procesa las directivas y traduce las direcciones de la siguiente manera:
  - Dirección de origen 172.16.0.2
  - Dirección de destino 172.16.0.3
- Las direcciones se traducen y encapsulan:
  - Encabezado GRE que utiliza el ID de red virtual: 5051
  - Dirección de origen: 192.168.1.10
  - Dirección de destino: 192.168.1.12

El paquete que se encapsula con el protocolo NVGRE contiene el paquete IP original.

En la vuelta, el host Hyper-V 1, dependiendo de las reglas y de las directivas que tiene asignadas, desencapsula el paquete NVGRE y determina, en función del identificador virtual 5051, a qué máquina virtual está destinado el paquete IP.

5. Controladora de red

La controladora de red (*Network Controller*) es una nueva funcionalidad de Windows Server 2016 que permite administrar, configurar, supervisar y resolver los errores de la infraestructura de red física y virtual de su centro de datos utilizando un punto de automatización centralizado y programable. Mediante la controladora de red podrá automatizar la configuración de su infraestructura de red sin tener que realizar una configuración manual de los dispositivos de red y de los servicios.

Es posible desplegar la controladora de red en un dominio Active Directory, en cuyo caso se utiliza Kerberos como motor de autenticación para autenticar tanto a los usuarios como los dispositivos. Sin embargo, puede desplegarse en un entorno autónomo (Workgroup), en cuyo caso se recomienda utilizar una entidad de certificación para permitir esta autenticación.

La controladora de red proporciona un cierto número de funcionalidades con las que puede configurar y administrar los dispositivos y los servicios de redes virtuales y físicas:

- **Administración del cortafuegos**. Puede configurar y administrar las reglas de control de acceso del cortafuegos para sus equipos virtuales.
- **Administración SLB**. Puede configurar varios servidores para repartir la carga y proporcionar una alta disponibilidad.
- **Administración de la red virtual**. Puede implementar la virtualización de red desplegando el Network Controller (*Hyper-V Network Virtualization*) en sus hosts de virtualización o, por el contrario, en las máquinas virtuales.
- **Administración de puertas de enlace RAS**. Puede proporcionar servicios de puerta de enlace a sus clientes desplegando, configurando y administrando los hosts Hyper-V y las máquinas virtuales que son miembro de un pool de puertas de enlace RAS.

a. Despliegue de una controladora de red

- Requisitos previos:
  - Disponible exclusivamente en la versión Datacenter de Windows Server 2016.
  - El puesto o los puestos de administración deben trabajar con Windows 8, 8.1 o Windows 10.
  - Un dominio Active Directory con una infraestructura DNS.
  - Es necesario crear varios grupos de seguridad que permitan administrar y delegar las autorizaciones.
- **Etapa n.° 1**: instalación del rol de controladora de red con el comando PowerShell:

```
Install-WindowsFeature -Name NetworkController -IncludeManagementTools
```

- **Etapa n.° 2**: Creación del nodo o de los nodos
  - Debe crear un nodo para cada equipo o máquina virtual que sea miembro del clúster Network Controller. Utilice el cmdlet `New-NetworkControllerNodeObject` para realizar esta etapa:

```
New-NetworkControllerNodeObject -Name "Node1" -Server
"PAR-SRV2.formacion.eni"
-FaultDomain "fd:/rack1/host1" -RestInterface "Ethernet"
```

- **Etapa n.º 3**: Configuración del clúster
  - Una vez creado el nodo o los nodos del clúster, use el cmdlet `install-NetworkControllerCluster` para configurar el clúster. Los siguientes comandos instalan un clúster de controladores de red en un entorno de pruebas. El soporte a la alta disponibilidad no está disponible, pues se utiliza un único nodo. Se emplea una autenticación basada en Kerberos entre los nodos del clúster.

```
$NodeObject = New-NetworkControllerNodeObject -Name "Node1"
-Server "PAR-SRV2.formacion.eni" -FaultDomain "fd:/rack1/host1"
-RestInterface "Ethernet"
```

```
Install-NetworkControllerCluster -Node $NodeObject
-ClusterAuthentication Kerberos
```

- **Etapa n.º 4**: Configuración de la aplicación
  - La última etapa de despliegue implica la configuración de la aplicación de controladora de red. Se utiliza el cmdlet `Install-NetworkController`. Los siguientes comandos crean un objeto de nodo de controladora de red y a continuación lo almacenan en la variable `$NodeObject`:

```
$NodeObject = New-NetworkControllerNodeObject -Name "Node01" -Server
"PAR-SRV2.formacion.eni" -FaultDomain "fd:/rack1/host1" -RestInterface
Ethernet
```

  - A continuación hay que utilizar los certificados para la máquina virtual o el equipo correspondiente:

```
$Certificate = Get-Item Cert:\LocalMachine\My | Get-ChildItem |
Where-Object {$_.Subject -eq "CN=PAR-SRV2.formacion.eni" }
```

  - El siguiente comando crea un clúster Network Controller utilizando el cmdlet `Install-NetworkControllerCluster`:

```
Install-NetworkControllerCluster -Node $NodeObject
-ClusterAuthentication None
```

El siguiente comando despliega una controladora de red en un entorno de pruebas. Como se utiliza un único nodo en el despliegue, no se soporta la alta disponibilidad. Esta controladora de red no utiliza ninguna autenticación entre los nodos del clúster, ni entre los clientes y la controladora de red. El comando especifica la opción `$Certificate` para encriptar el tráfico entre los clientes y la controladora de red.

```
Install-NetworkController -Node $NodeObject -ClientAuthentication None
-RestIpAddress "10.0.0.1/24" -ServerCertificate $Certificate
```

- **Etapa n.º 5**: Validación del despliegue
  - Para validar el despliegue, debe agregarse una identidad (pareja login / contraseña) a esta controladora de red. Esta etapa se realiza con PowerShell.

```
$cred=New-Object Microsoft.Windows.Networkcontroller.credentialproperties
$cred.type="usernamepassword"
$cred.username="admin"
$cred.value="Pa$$w0rd"
New-NetworkControllerCredential -ConnectionUri https://networkcontroller
-Properties
$cred -ResourceId cred1
```

  - A continuación, para verificar el correcto despliegue, se utiliza el cmdlet: `Get-NetworkControllerCredential`.

```
Get-NetworkControllerCredential -ConnectionUri https://networkcontroller
-ResourceId cred1
```

Y, si todo va bien, debería obtener como respuesta algo similar a lo siguiente:

```
Tags:
ResourceRef: /credentials/cred1
CreatedTime: 1/1/0001 12:00:00 AM
InstanceId: e16ffe62-a701-4d31-915e-7234d4bc5a18
Etag: W/"1ec59631-607f-4d3e-ac78-94b0822f3a9d"
ResourceMetadata:
ResourceId: cred1
Properties: Microsoft.Windows.NetworkController.CredentialProperties
```

El despliegue del Network Controller está ahora validado y es operacional.

b. El cortafuegos con el Network Controller

El cortafuegos de Windows Server 2016 en versión Datacenter le ayuda a instalar y configurar las directivas de cortafuegos que permiten proteger sus redes virtuales del tráfico de red no deseado. Puede administrar las directivas de cortafuegos del Data center utilizando las API de la controladora de red. Esto nos ofrece numerosas ventajas de administración para los sistemas cloud:

- Una solución de cortafuegos basada en aplicaciones que evolucionan con bastante frecuencia y fáciles de administrar, y que además pueden ofrecerse fácilmente a los distintos clientes.
- La posibilidad de desplazar fácilmente las máquinas virtuales de un cliente entre los distintos hosts Hyper-V sin perturbar la configuración del cortafuegos de cada cliente, puesto que:
  - Se despliega como un cortafuegos del agente host del puerto vSwitch.
  - Las reglas de cortafuegos se configuran en cada puerto vSwitch, independientemente del host que ejecuta el equipo virtual.
- La protección de máquinas virtuales, sea cual sea el sistema operativo invitado para cada cliente.

c. Software Load Balancing (SLB)

Puede utilizar el reparto de carga por software (SLB) en un Software Defined Networking para repartir el tráfico de red entre los diversos recursos de red disponibles. Windows Server SLB proporciona las siguientes características:

- Reparto de carga de capa 4 (modelo OSI) para las dos API de uso del tráfico Transmission Control Protocol/User Datagramme Protocol (TCP/UDP).
- Reparto de carga del tráfico para las redes pública e interna.
- Compatibilidad con direcciones IP dinámicas en las VLAN y en redes virtuales Hyper-V.

d. Puerta de enlace RAS

La puerta de enlace RAS es un router BGP lógico. Ha sido diseñado por los proveedores de servicios cloud y las grandes organizaciones que albergan varias redes virtuales de clientes basadas en la virtualización Hyper-V para la red (HVN). La puerta de enlace RAS proporciona las siguientes características:

- **VPN de sitio a sitio**. Permite conectar dos redes situadas en distintas ubicaciones físicas a través de Internet.
- **VPN de punto a sitio**. Ofrece a los empleados de una organización o a los administradores la posibilidad de conectarse a la red privada de la empresa desde ubicaciones remotas.
- **Tunneling GRE**. Permite la conectividad entre las redes virtuales y las redes exteriores.
- **Enrutamiento dinámico con BGP**. Reduce la necesidad de una configuración manual de las rutas definidas en los routers, pues se trata de un protocolo de enrutamiento dinámico, capaz de implementar automáticamente los itinerarios entre los sitios conectados mediante conexiones VPN de sitio a sitio.

Trabajos prácticos

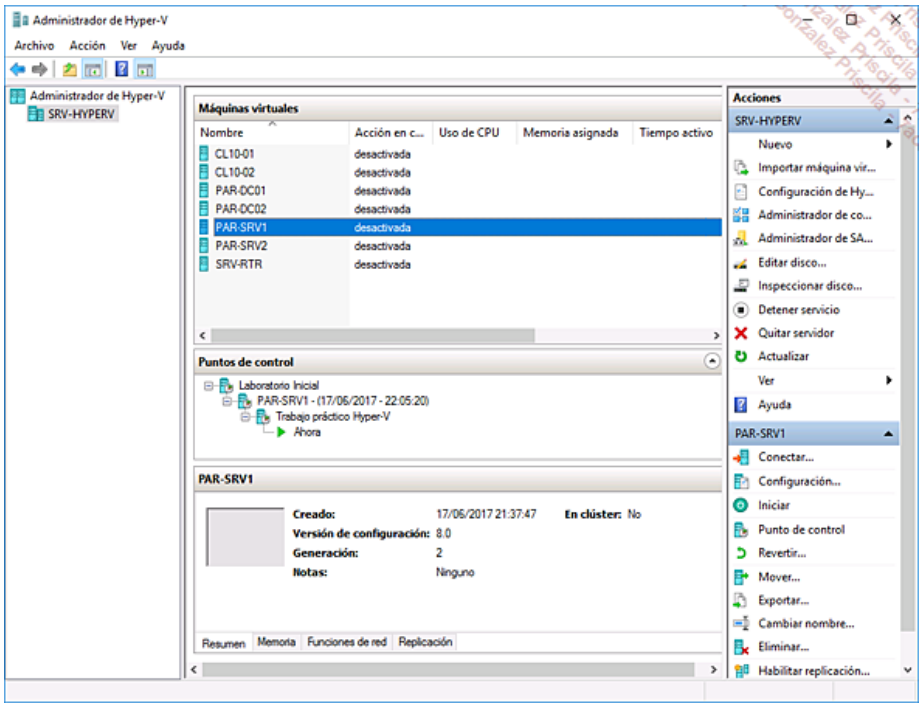
1. Creación de un vSwitch de tipo SET y creación de una asociación de tarjetas de red

Máquinas virtuales necesarias para el trabajo práctico: PAR-SRV1.

Objetivos: este taller tiene como objetivo implementar varias funcionalidades de red avanzadas en nuestro host Hyper-V y nuestras máquinas virtuales.

Antes de comenzar este trabajo práctico, realice un punto de control en la máquina **PAR-SVR1** con el siguiente comando:

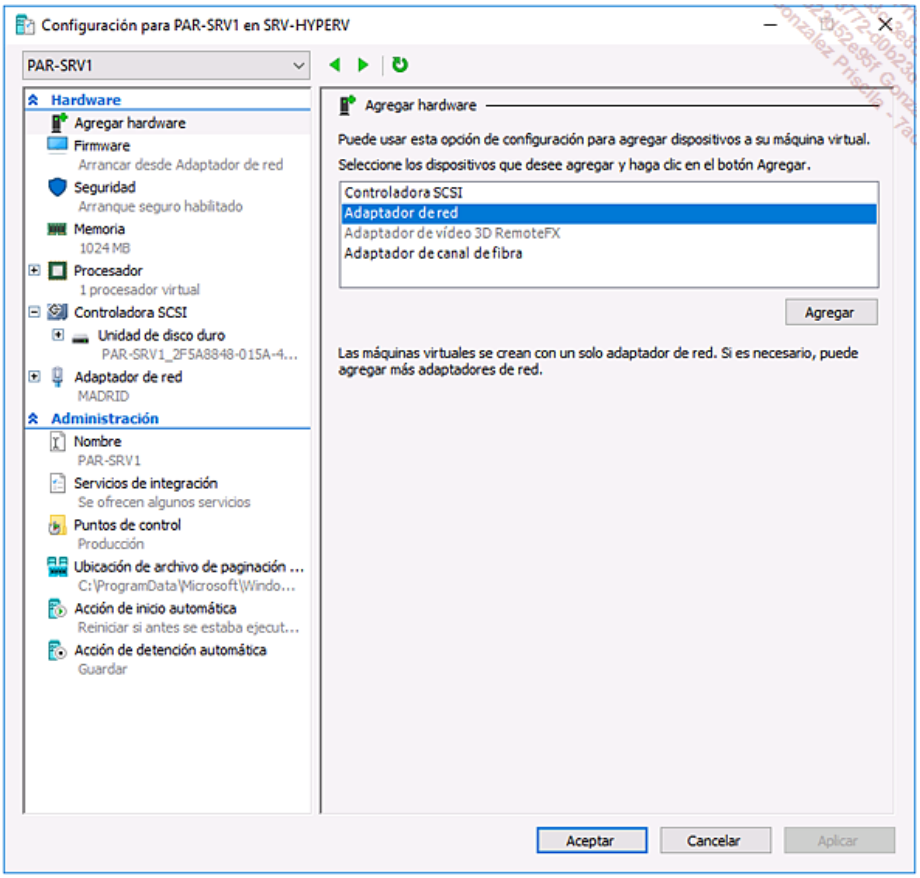
```
CHECKPOINT-VM -Name "PAR-SRV1" -Snapshotname 'Trabajo practico Hyper-V'
```



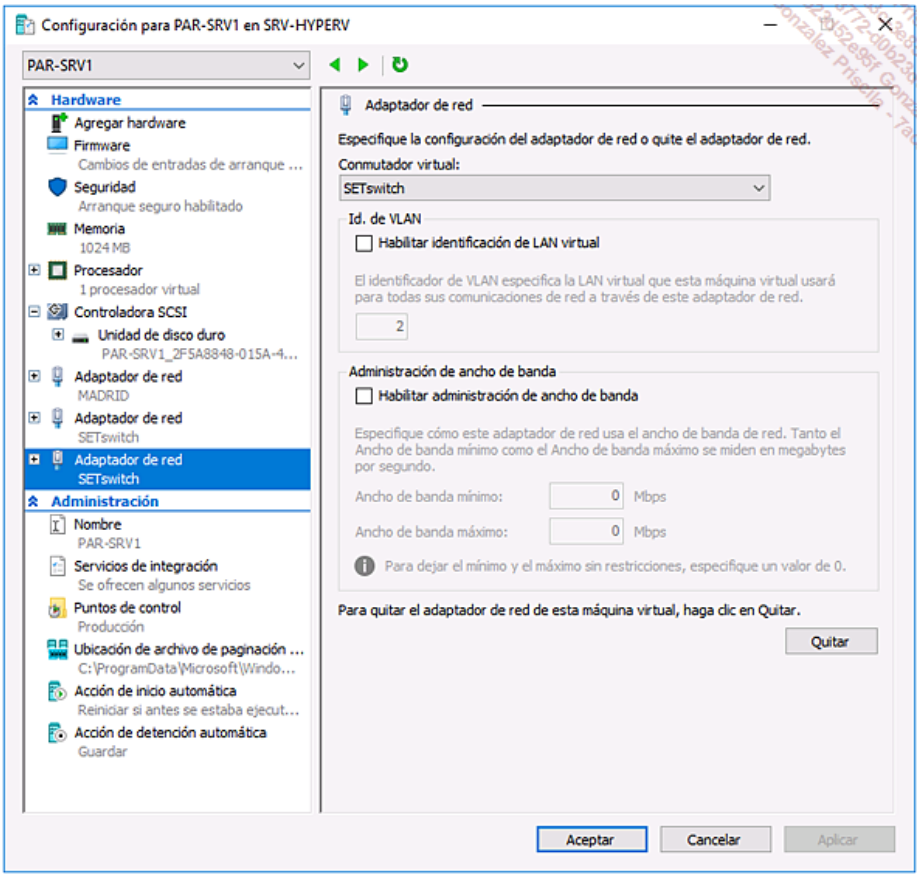
Utilizaremos una única tarjeta de red.

```
New-VMSwitch -Name SETswitch -NetAdapterName "Ethernet"
-EnableEmbeddedTeaming $true
```

Haga clic con el botón derecho en el equipo virtual **PAR-SRV1**, haga clic en **Configuración** y, a continuación, en **Agregar hardware** y seleccione **Adaptador de red**.



Haga clic en **Agregar** y seleccione el conmutador **SETswitch**. Repita esta acción dos veces.



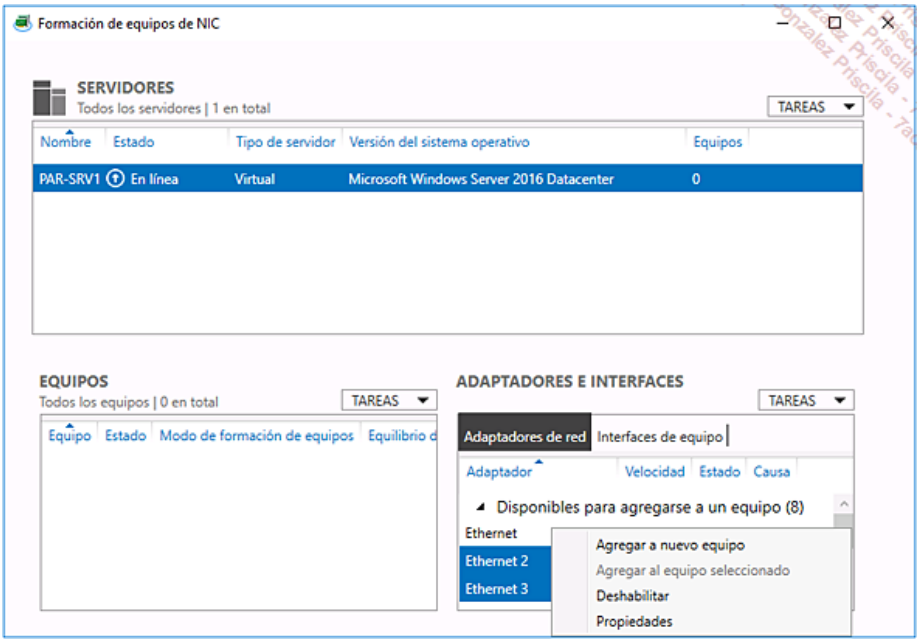
Ejecute el siguiente comando PowerShell en el servidor Hyper-V para conectarse a la máquina **PAR-SRV1**.

Conéctese como administrador local de la máquina con la contraseña: **Pa$$w0rd** y el login **PAR-SRV1\Administrador**.

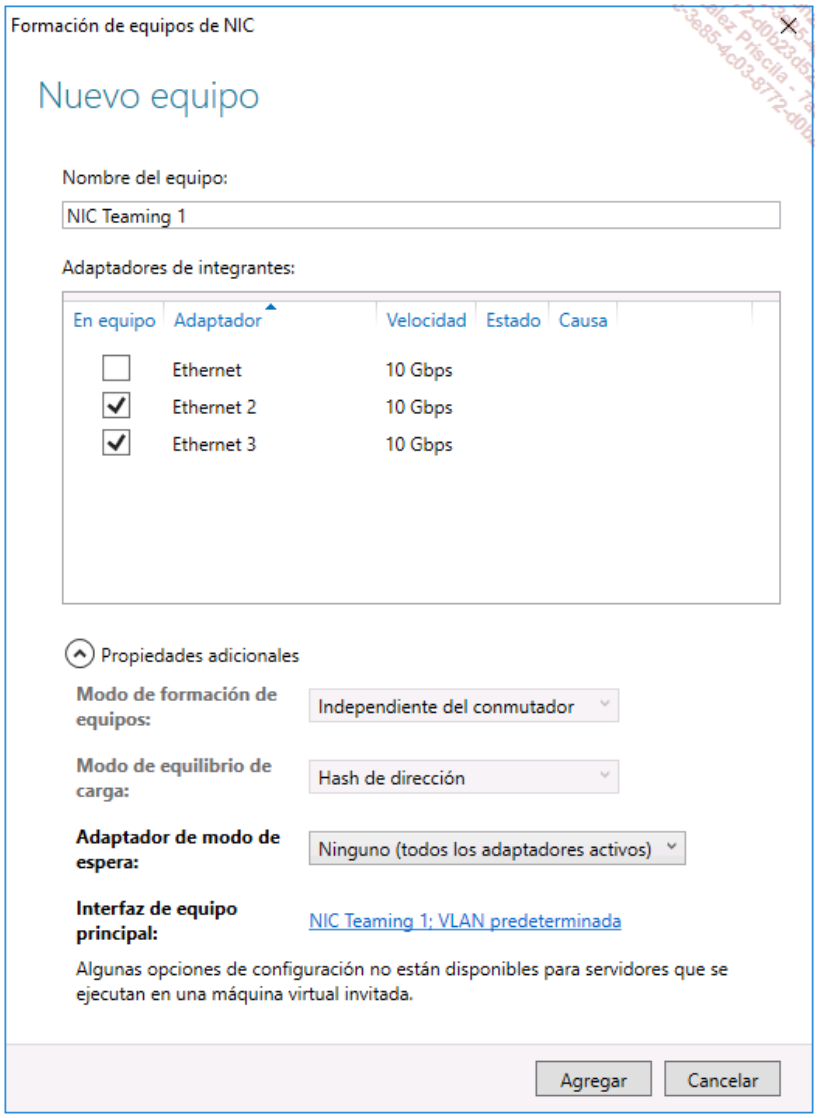
```
$VMName = "PAR-SRV1"
Start-VM -Name $VMName
VMConnect localhost $VMName
```

Abra el Administrador del servidor, seleccione **Configurar este servidor local** y en **Formación de equipos de NIC** haga clic en**Deshabilitado**.

En el asistente **Formación de equipos de NIC**, en la sección **ADAPTADORES E INTERFACES**, seleccione las dos tarjetas de red que acabamos de agregar y a continuación haga clic con el botón derecho.



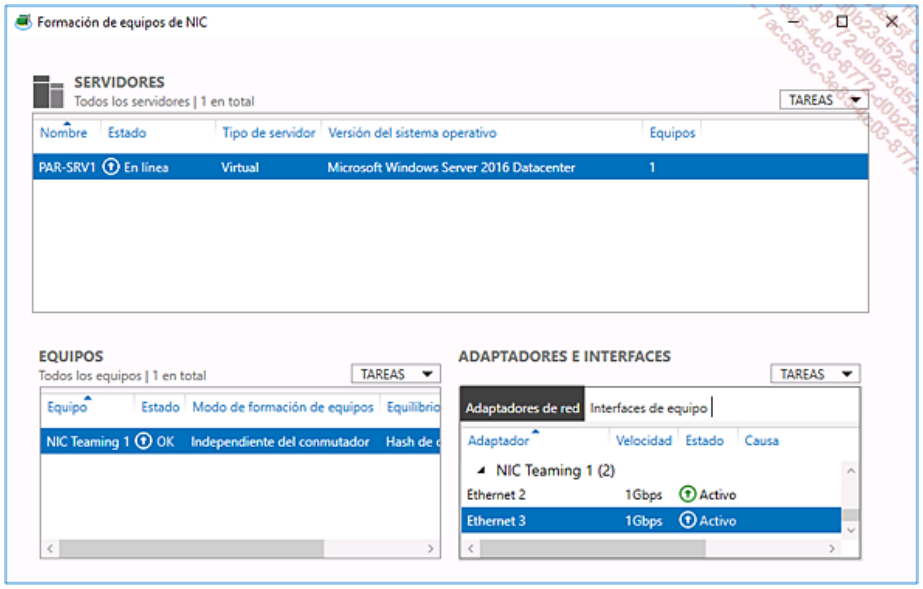
Seleccione **Agregar a nuevo equipo** y escriba el siguiente nombre de equipo: **NIC Teaming 1**.



Si quiere configurar una VLAN específica para esta asociación de tarjetas de red, haga clic en **NIC Teaming 1; VLAN predeterminada**.

Haga clic en **Agregar**.

Compruebe que la asociación de tarjetas de red funciona correctamente.



Al finalizar este trabajo práctico, para restablecer la configuración inicial, ejecute los siguientes comandos:

```
Stop-VM -Name PAR-SRV1
Restore-VMSnapshot -VMName PAR-SRV1 -Name "Trabajo practico Hyper-V"
```

A la pregunta **¿Está seguro de que desea realizar esta acción?** responda **S**.

```
Remove-VMSnapshot -VMName PAR-SRV1 -Name "Trabajo practico Hyper-V"
```

Ejecute el siguiente comando para eliminar el vSwitch de tipo **SET**.

```
Remove-VMSwitch -Name SETswitch -Force
```

Ya no existe ningún snapshot para la máquina **PAR-SRV1** y el vSwitch de tipo **SET** ya no existe.

2. Configuración de la protección para un router y para un DHCP

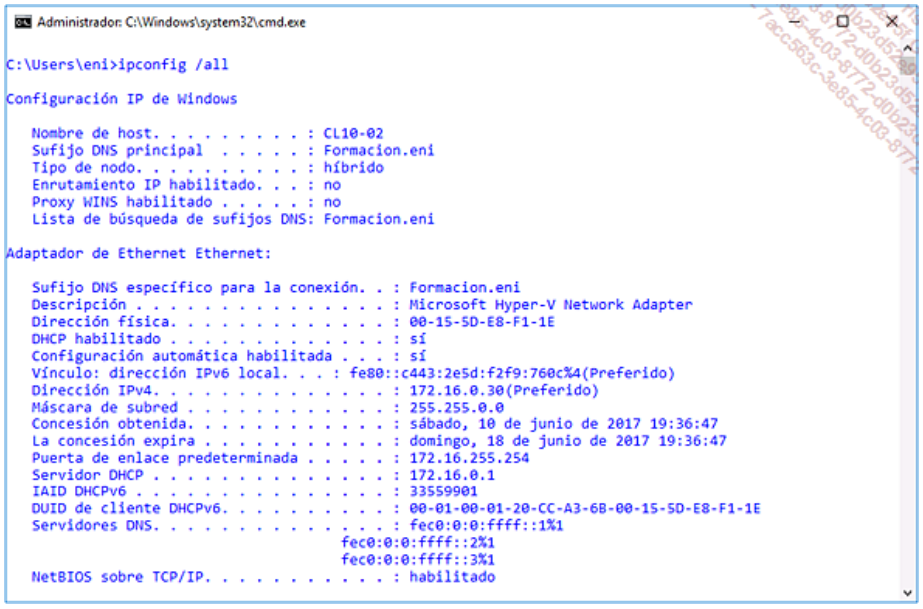
Máquinas virtuales necesarias para el trabajo práctico: PAR-DC01, SRV-RTR y CL10-02

Objetivo: este taller tiene como objetivo implementar las funcionalidades DHCP guard y Router guard.

Ejecute los siguientes comandos para crear un punto de control para las máquinas implicadas en el trabajo práctico:

```
$VMname = ("PAR-DC01","SRV-RTR","CL10-02")
foreach ($item in $VMname)
{
   CHECKPOINT-VM -Name $item -Snapshotname 'Trabajo practico Hyper-V /
DHCP & Router Guard'
}
```

En **PAR-DC01**, compruebe la presencia del servicio DHCP, y en **CL10-02**, compruebe que esta última recupera correctamente una dirección a través de DHCP.



En el host Hyper-V, ejecute el siguiente comando:

```
Set-VMNetworkAdapter -VMName PAR-DC01 -DhcpGuard On
```

En **CL10-02**, libere su contrato DHCP con el comando:

```
ipconfig /release
```

Y realice una nueva petición de dirección IP con el comando:

```
ipconfig /renew
```

El equipo **CL10-02** no logra obtener una respuesta del DHCP, puesto que se ha habilitado DHCP Guard.

Para restablecer la comunicación, ejecute el siguiente comando en el host Hyper-V:

```
Set-VMNetworkAdapter -VMName PAR-DC01 -DhcpGuard off
```

En **CL10-02**, realice una petición de dirección IP con el comando:

```
ipconfig /renew
```

El equipo **CL10-02** obtiene, de nuevo, una respuesta del DHCP.

En **SRV-RTR**, abra la consola **Administrador del servidor**.

Haga clic en la opción **Agregar roles y características** y, a continuación, en la ventana **Antes de comenzar**, haga clic en **Siguiente**.

Deje la opción por defecto en la ventana **Seleccionar tipo de instalación** y, a continuación, haga clic dos veces en **Siguiente**.

En la ventana **Seleccionar roles de servidor**, marque **Acceso remoto** y, a continuación, haga clic en **Agregar características**.

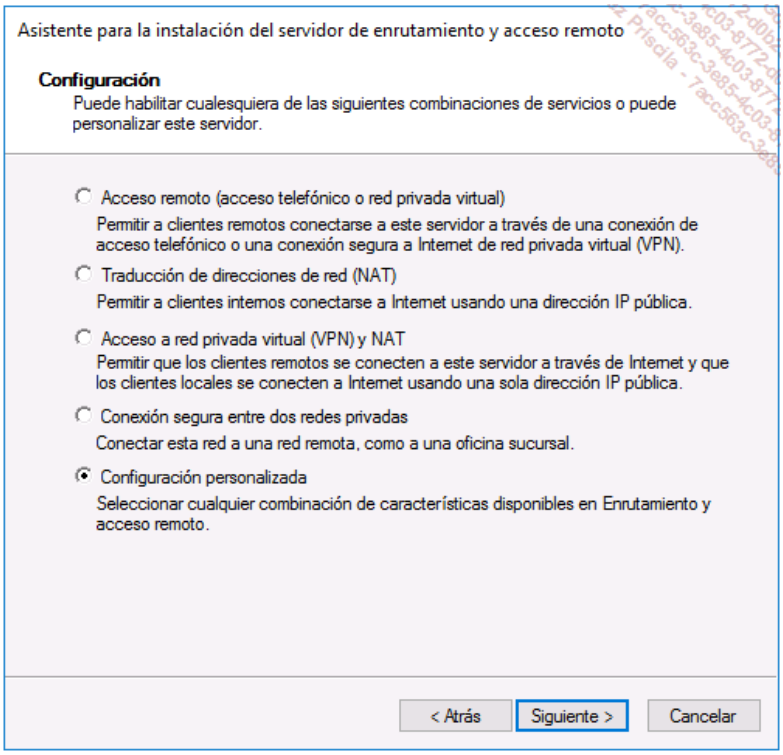
Haga clic tres veces en **Siguiente** y, a continuación, en la ventana **Seleccionar servicios de rol**, marque **Enrutamiento** y haga clic en**Siguiente**.

Haga clic dos veces en **Siguiente** (los **servicios de rol IIS** deben dejarse marcados por defecto) y, a continuación, haga clic en **Instalar**.

Una vez terminada la instalación, abra la consola **Enrutamiento y acceso remoto** desde las **Herramientas administrativas**.

Haga clic con el botón derecho en **SRV-RTR** y, a continuación, en el menú contextual, haga clic en **Configurar y habilitar el enrutamiento y el acceso remoto**.

En la ventana **Bienvenido**, haga clic en **Siguiente** y, a continuación, marque **Configuración personalizada**.



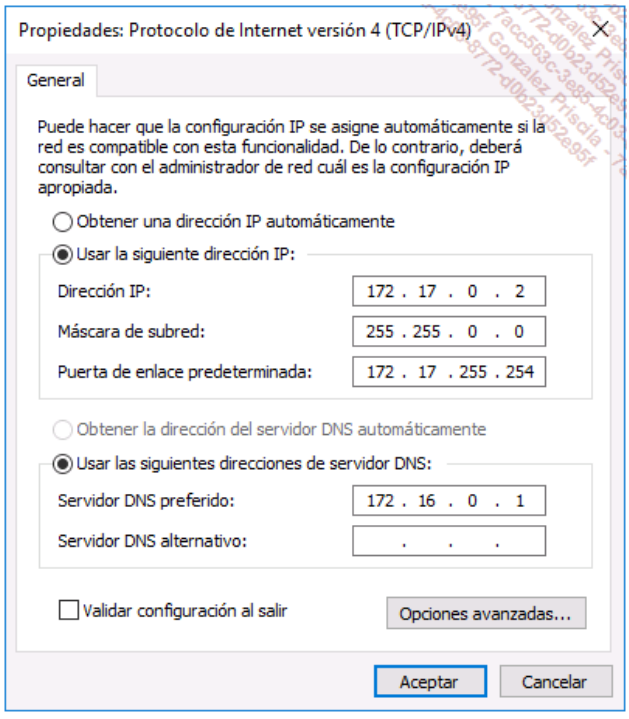
Haga clic en **Siguiente** para validar esta opción.

En la ventana **Configuración personalizada**, marque **Enrutamiento LAN** y, a continuación, haga clic en **Siguiente**.

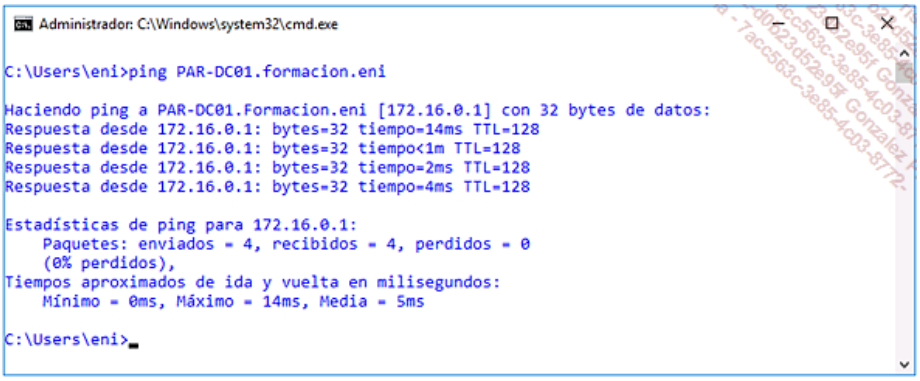
Haga clic en **Finalizar** para cerrar el asistente y, a continuación, en **Iniciar servicio** en la ventana emergente.

Desplace la máquina **CL10-02** del vSwitch MADRID hasta el vSwitch BARCELONA y asígnele la siguiente configuración de red:

- **Dirección IP**: 172.17.0.2
- **Máscara de subred**: 255.255.0.0
- **Servidor DNS**: 172.16.0.1
- **Puerta de enlace**: 172.17.255.254



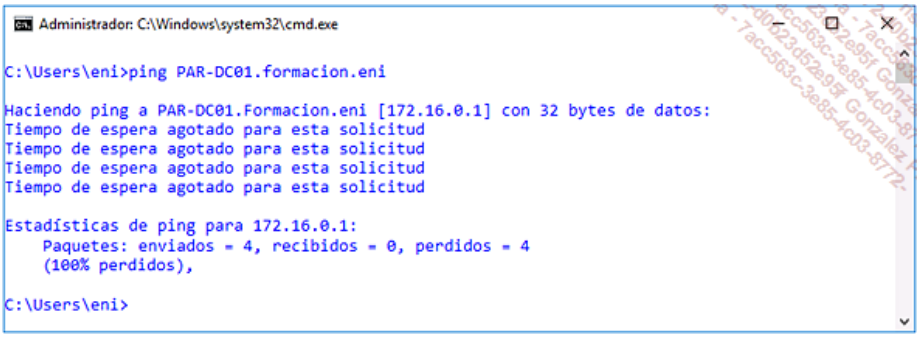
Compruebe la conectividad con la máquina **PAR-DC01** utilizando el comando **`ping`**.



En el host Hyper-V, ejecute el siguiente comando:

```
Set-VMNetworkAdapter -VMName SRV-RTR -RouterGuard on
```

En **CL10-02**, compruebe la conectividad con la máquina **PAR-DC01** utilizando el comando **`ping`**.



La conectividad de red ha dejado de funcionar, puesto que se ha habilitado Routeur Guard en las dos interfaces del router **SRV-RTR**.

Al finalizar este trabajo práctico, para restablecer la configuración inicial, ejecute los siguientes comandos:

```
$VMname = ("PAR-DC01","SRV-RTR","CL10-02")
foreach ($item in $VMname)
{
  Stop-VM -Name $item
}

foreach ($item in $VMname)
{
  Restore-VMSnapshot -VMName $item -Name 'Trabajo practico Hyper-V / DHCP
& Router Guard'
  Remove-VMSnapshot -VMName $item -Name 'Trabajo practico Hyper-V / DHCP
& Router Guard'
}
```

A la pregunta **¿Está seguro de que desea realizar esta acción?** responda **S** tres veces consecutivas, para cada máquina virtual.

3. Despliegue de la controladora de red

Máquinas virtuales necesarias para el trabajo práctico: PAR-DC01 y PAR-SRV2

Objetivos: este taller tiene como objetivo desplegar Network Controller en la máquina **PAR-SRV2**.

Ejecute los siguientes comandos para crear un punto de control para las máquinas implicadas en el trabajo práctico:

```
$VMname = ("PAR-DC01","PAR-SRV2")
foreach ($item in $VMname)
{
   CHECKPOINT-VM -Name $item -Snapshotname 'Trabajo practico Hyper-V /
Network Controller'
}
```

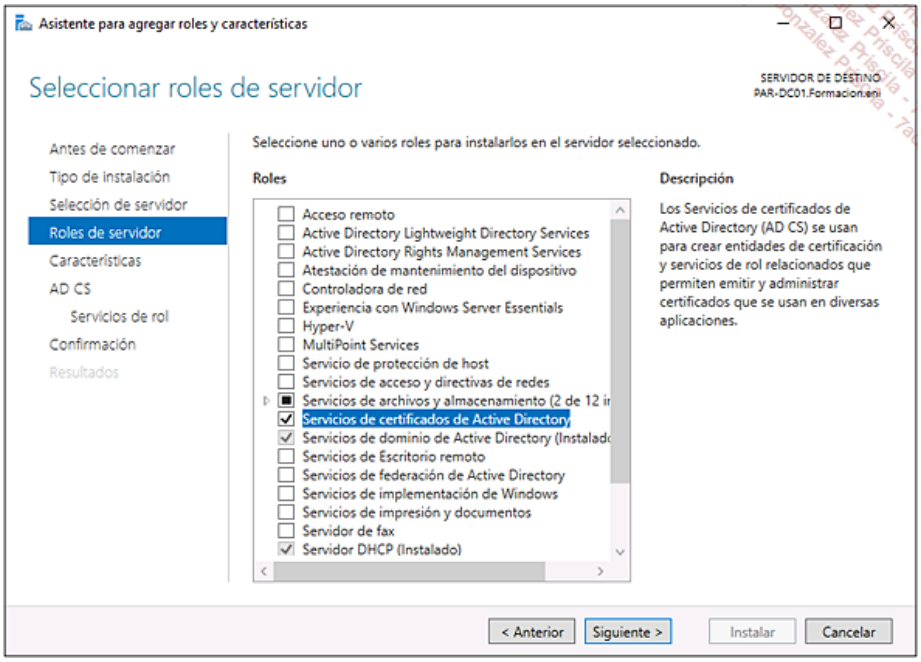
En **PAR-DC01**, abra la consola **Administrador del servidor**. Compruebe que el rol **Servicios de certificados de Active Directory** esté

instalado; en caso contrario, siga estas etapas.

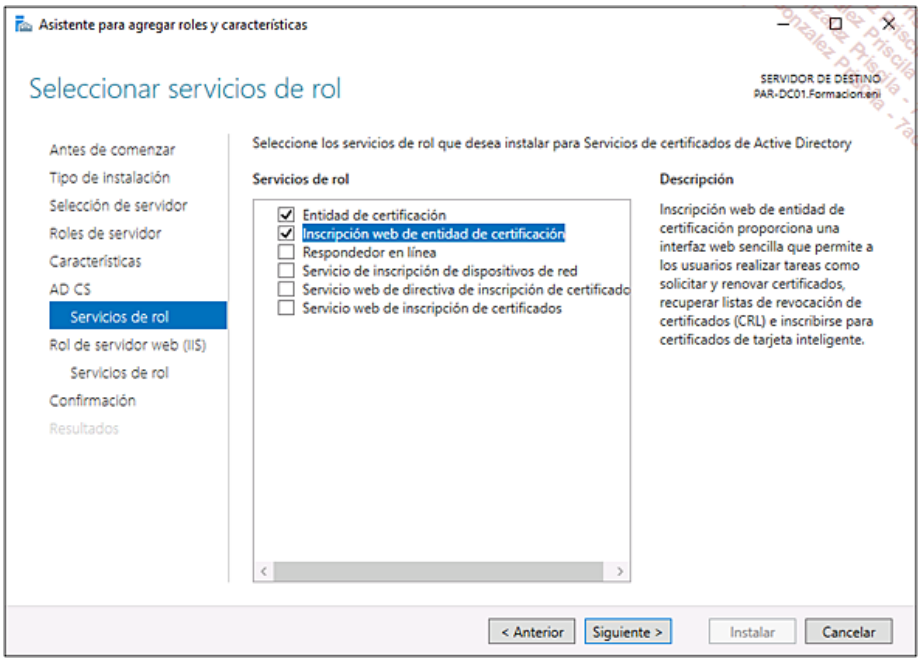
Haga clic en **Agregar roles y características** y, a continuación, haga clic en **Siguiente** en la ventana **Antes de comenzar**.

En la ventana **Seleccionar tipo de instalación** deje la opción por defecto y, a continuación, haga clic dos veces en **Siguiente**.

Marque la opción **Servicios de certificados de Active Directory** y, a continuación, haga clic en el botón **Agregar características** en la ventana emergente.

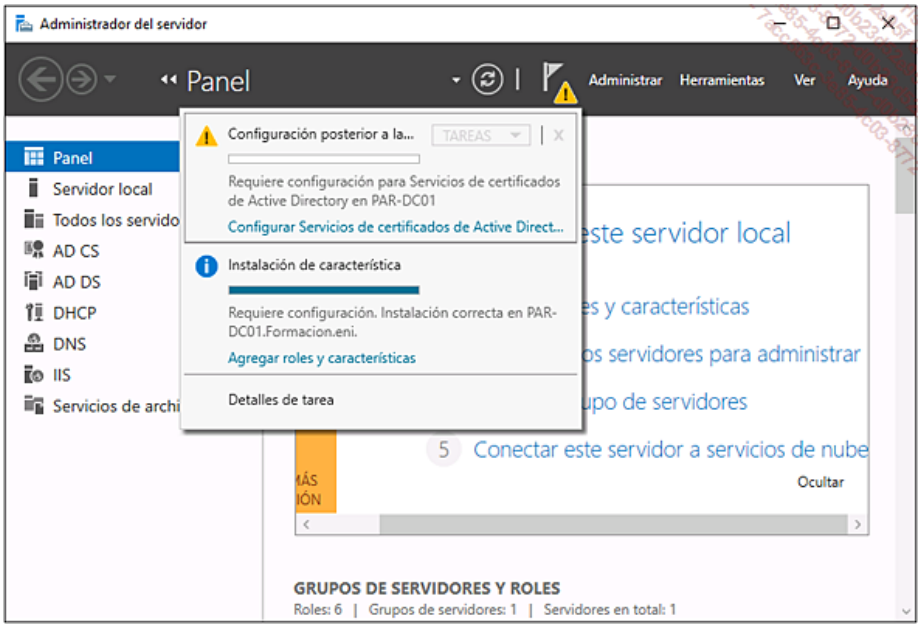


Haga clic tres veces en **Siguiente** y, a continuación, en la ventana **Servicios de rol**, marque **Inscripción web de entidad de certificación**.

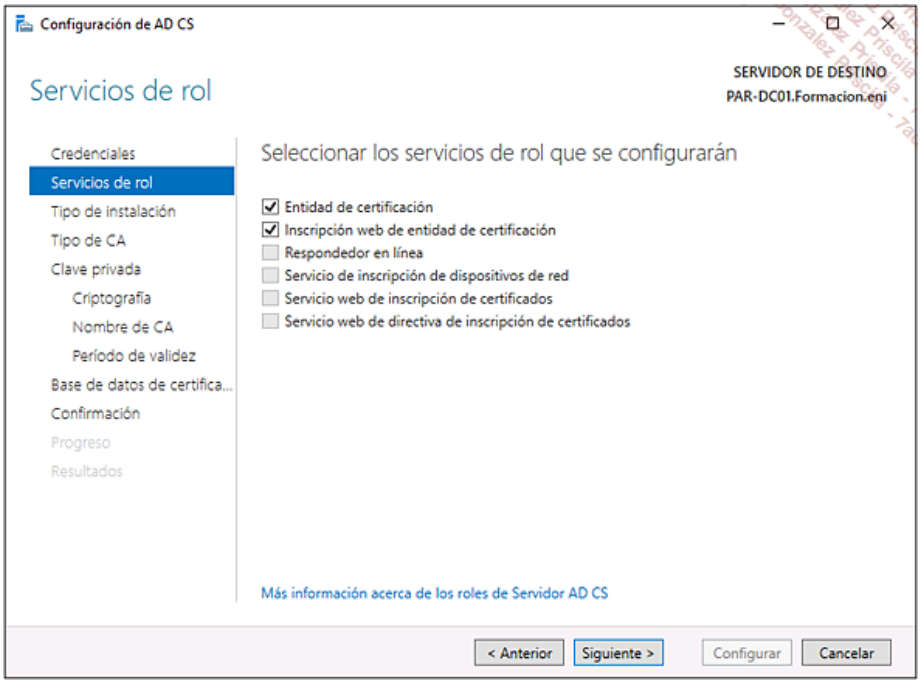


Valide la opción haciendo clic tres veces en **Siguiente** y, a continuación, inicie la instalación mediante el botón **Instalar**.

Haga clic en **Cerrar** y, a continuación, en la consola **Administrador del servidor**, haga clic en **Notificaciones** y en **Configurar Servicios de certificados de Active Directory**.

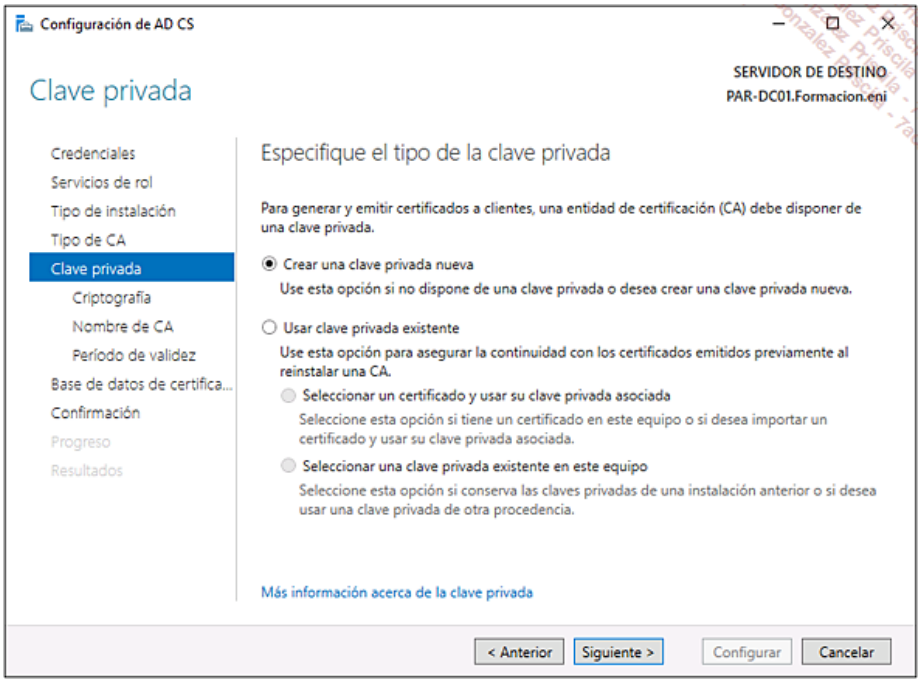


Haga clic en **Siguiente** en la ventana **Credenciales** y, a continuación, marque los dos servicios de rol.



En las ventanas **Tipo de instalación** y **Tipo de AC**, deje la opción por defecto (**CA empresarial**, **CA raíz**) y haga clic en **Siguiente**.

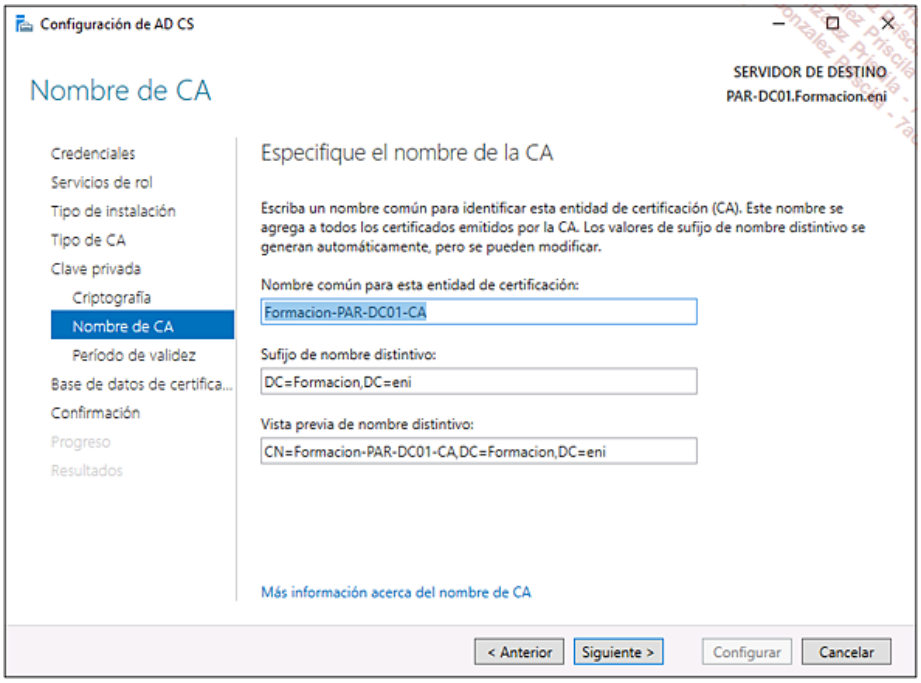
Marque **Crear una clave privada nueva** y, a continuación, haga clic en **Siguiente**.



Deje las opciones por defecto en la ventana **Criptografía para la CA**.

El nombre de la entidad de certificación se configura automáticamente, y puede ser necesario modificarlo (para acceder desde el exterior…).

Deje las opciones por defecto y, a continuación, haga clic en **Siguiente**.



Configure un período de validez de dos años en la ventana **Período de validez**.

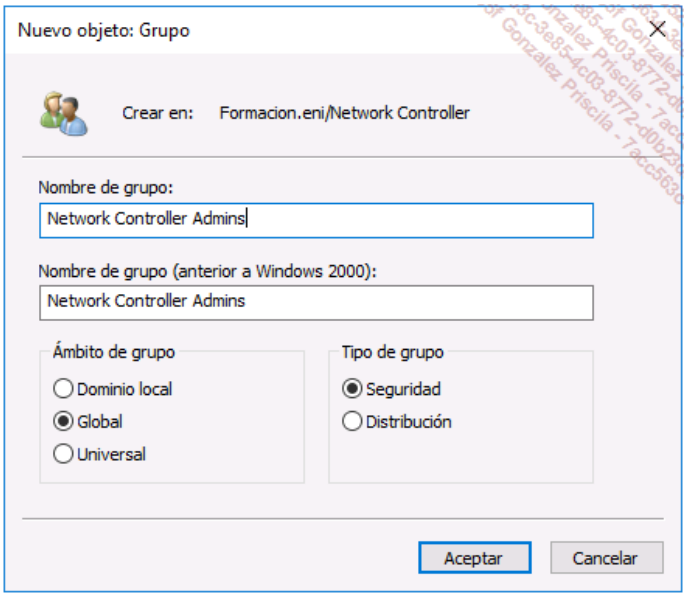
Haga clic tres veces en **Siguiente** y, a continuación, en **Configurar**.

Haga clic en **Cerrar** para cerrar el asistente.

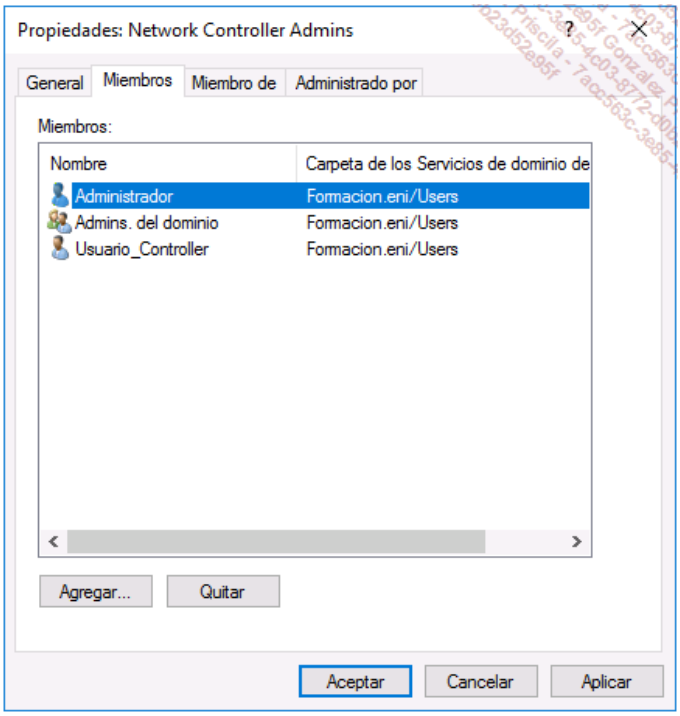
Abra la consola **Usuarios y equipos de Active Directory** y cree una unidad organizativa llamada Network Controller.

Cree dos grupos globales de seguridad llamados:

- Network Controller Admins
- Network Controller Ops



Agregue a los dos grupos que acabamos de crear las cuentas Administrador, Usuario_Controller y Admins. del dominio.



En **PAR-SRV2**, inicie una sesión como FORMACION\Administrador con la contraseña **Pa$$w0rd**. Abra la consola **Administrador del servidor**.

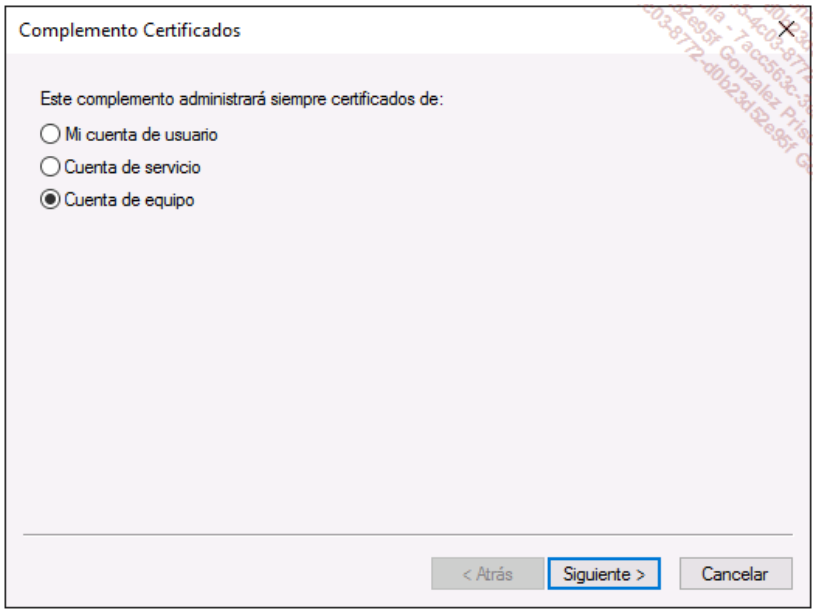
Sitúe el ratón en la parte inferior izquierda para mostrar la interfaz de Windows, haga clic con el botón derecho y, a continuación, seleccione en el menú contextual la opción **Ejecutar**.

Escriba **mmc** y, a continuación, presione la tecla [Enter].

Haga clic en **Archivo** y, a continuación, en **Agregar o quitar complemento**.

En la ventana **Agregar o quitar complementos**, seleccione **Certificados** y, a continuación, haga clic en **Agregar**.

Se abre un asistente, marque **Cuenta de equipo** y, a continuación, haga clic en **Siguiente**.



Deje la opción por defecto en la ventana **Seleccionar equipo** y, a continuación, haga clic en **Finalizar**.

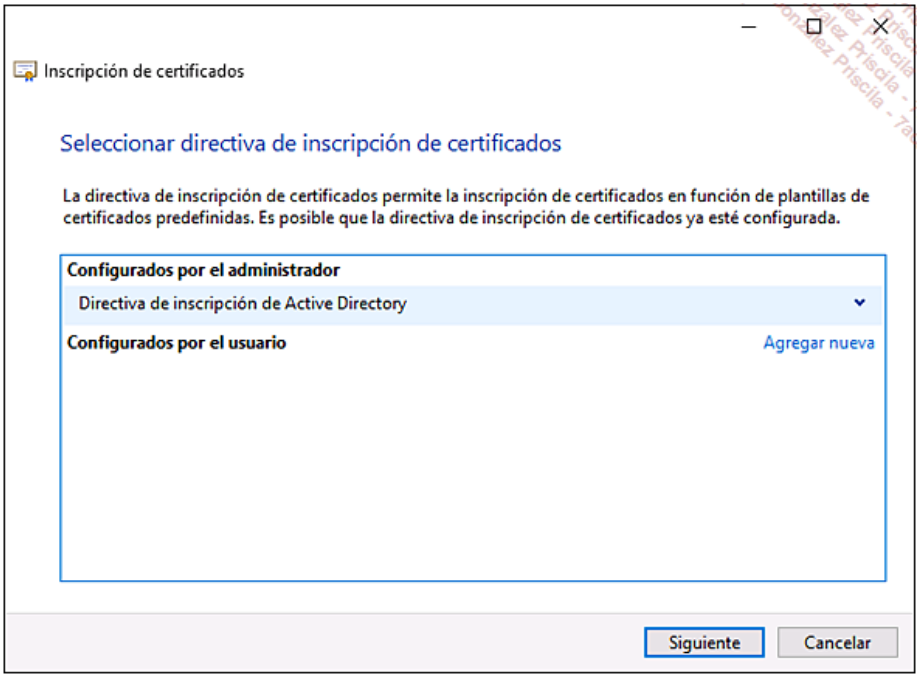
Haga clic en **Aceptar** para cerrar la ventana de selección de complementos.

Despliegue el nodo **Certificados** y, a continuación, haga clic con el botón derecho en **Personal**.

En el menú contextual, seleccione **Todas las tareas** y, a continuación, **Solicitar un nuevo certificado**.

Haga clic en **Siguiente** en la ventana **Antes de comenzar**.

Haga clic en **Directiva de inscripción de Active Directory** y, a continuación, haga clic en **Siguiente**.



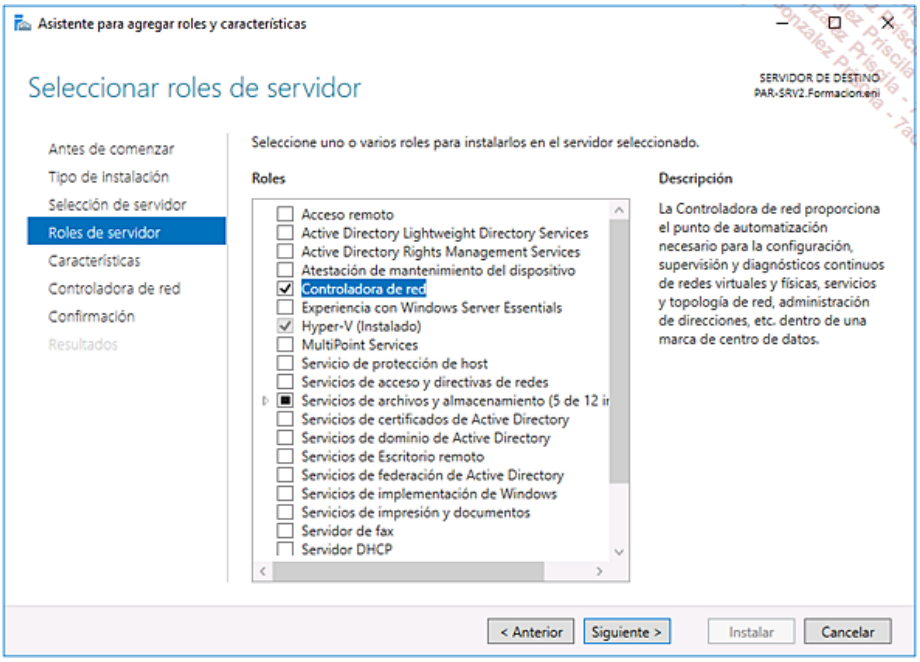
En la ventana **Solicitar certificados**, marque **Equipo** y, a continuación, haga clic en **Inscribir**.

Verifique que el estado es igual a **Correcto** y, a continuación, haga clic en **Finalizar**. Cierre la consola mmc.

Haga clic en **Agregar roles y características** y, a continuación, haga clic en **Siguiente** en la ventana **Antes de comenzar**.

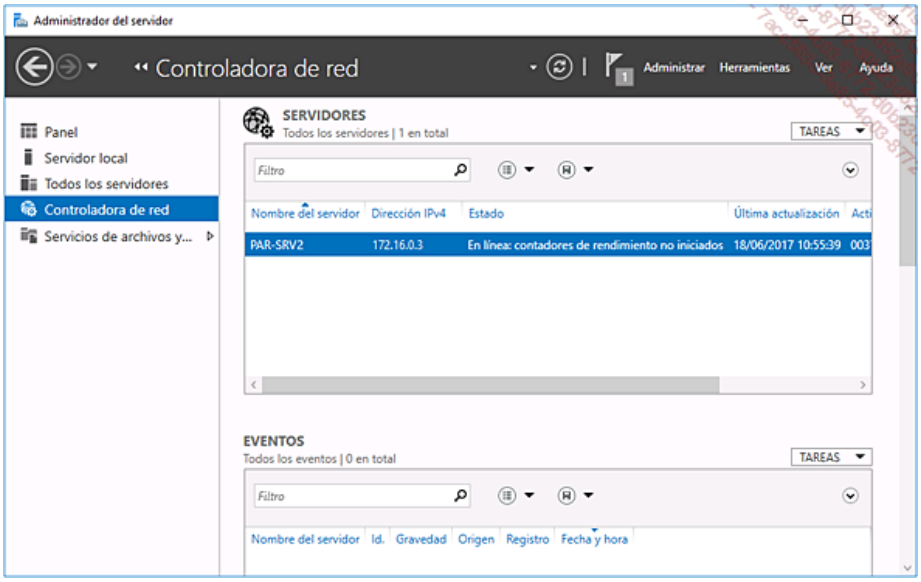
En la ventana **Seleccionar tipo de instalación**, deje la opción por defecto y, a continuación, haga clic dos veces en **Siguiente**.

Marque la opción **Controladora de red** y, a continuación, haga clic en el botón **Agregar características** en la ventana emergente.



Haga clic tres veces en **Siguiente** y, a continuación, en **Instalar**.

La funcionalidad Controladora de red se encuentra ahora instalada.



En **PAR-SRV2**, como administrador, introduzca los siguientes comandos en una consola PowerShell para instalar, configurar y comprobar el despliegue de Network Controller.

- Definir el nodo en la máquina:

```
$node=New-NetworkControllerNodeObject -Name "Node1"
-Server "PAR-SVR2.formacion.eni"
-FaultDomain "fd:/rack1/host1" -RestInterface "Ethernet"
```

- Recuperar el certificado:

```
$Certificate = Get-Item Cert:\LocalMachine\My | Get-ChildItem |
Where-Object {$_.Subject -eq "CN=PAR-SRV2.formacion.eni" }
```

- Crear el clúster:

```
Install-NetworkControllerCluster -Node $node
```

```
-ClusterAuthentication Kerberos -
ManagementSecurityGroup "Formacion\Network Controller Admins"
-CredentialEncryptionCertificate $Certificate
```

- Configurar el nodo:

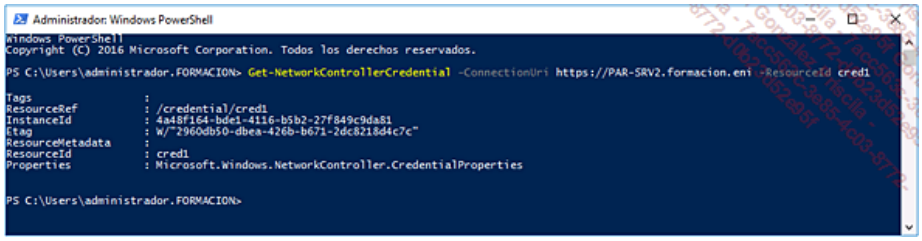
```
Install-NetworkController -Node $node -ClientAuthentication Kerberos
-ClientSecurityGroup "Formacion\Network Controller Ops" -RestIpAddress
"172.16.0.99/24" -ServerCertificate $Certificate
```

- Agregar unas credenciales (login/password) como recurso al clúster PAR-SRV2:

```
$cred=New-Object Microsoft.Windows.Networkcontroller.credentialproperties
$cred.type="usernamepassword"
$cred.username="admin"
$cred.value="Password"
New-NetworkControllerCredential -ConnectionUri
https://PAR-SRV2.formacion.eni -Properties $cred -ResourceId "cred1"
```

- Comprobación del despliegue:

```
Get-NetworkControllerCredential -ConnectionUri
https://PAR-SRV2.formacion.eni -ResourceId cred1
```



Validación de conocimientos adquiridos: preguntas/respuestas

1. Preguntas

1. ¿Cuáles son las mejoras de Windows Server 2016 respecto al protocolo SMB?
2. Enumere los distintos tipos de vSwitchs que existen en Hyper-V con Windows Server 2016.
3. Realice una breve descripción de las funcionalidades Router Guard y DHCP Guard.
4. Enumere los cuatro tipos de clouds.
5. ¿Con qué comando PowerShell damos la posibilidad a los contenedores Hyper-V o a un contenedor de acceder a Internet?
6. ¿Qué es el Software Defined Networking?
7. ¿Cuál es el rol del Network Controller?
8. ¿Para qué sirve la funcionalidad Dynamic Virtual Machine Queue?
9. ¿Para qué sirven los vSwitchs de tipo SET?
10. ¿Cuáles son los "equipos lógicos" que podemos implementar desplegando un Network Controller en un Software Defined Networking?

2. Resultados

Consulte las siguientes páginas para comprobar sus respuestas.

Por cada respuesta correcta, cuente un punto.

Número de puntos /10

Para superar este capítulo, su puntuación mínima debería ser de 8 sobre 10.

3. Respuestas

1. ¿Cuáles son las mejoras de Windows Server 2016 respecto al protocolo SMB?

   La última versión de SMB es SMB 3.1.1, incluida con Windows 10 y Windows Server 2016. Incorpora la compatibilidad del cifrado AES 128 con Galois/Counter Mode (GCM), además del contador 128 AES con encriptación CBC-MAC (CCM) incluido en SMB 3.0.

2. Enumere los distintos tipos de vSwitchs que existen en Hyper-V con Windows Server 2016.

   Existen tres tipos de vSwitchs:

- ***Externo**, que permite a las máquinas virtuales comunicarse con los hosts situados en la red física.*
- ***Interno**, se conecta a una red que pueden utilizar únicamente aquellos equipos virtuales en ejecución dentro del host que administra el conmutador virtual, y entre el host y los equipos virtuales.*
- ***Privado**, se conecta a una red que pueden utilizar únicamente aquellos equipos virtuales en ejecución dentro del host que administra el conmutador virtual, pero no proporciona conexión entre el host y los equipos virtuales.*

3. Realice una breve descripción de las funcionalidades Router Guard y DHCP Guard.

   La funcionalidad Router Guard permite prohibir que una máquina no autorizada que posea la funcionalidad de enrutamiento realice el enrutamiento. DHCP Guard funciona de la misma manera, pero prohíbe al servidor DHCP enviar y recibir peticiones de cliente DHCP.

4. Enumere los cuatro tipos de clouds.

   Existen cuatro tipos de cloud:

- *La **cloud pública**, la más grande y conocida de ellas es **Internet**.*
- *La **cloud privada**, una solución implementada dentro de una misma compañía (SCVMM).*
- *La **cloud comunitaria**, que agrupa a personas de una misma profesión (notarios, hospitales).*
- *La **cloud híbrida**, es el hecho de comunicar dos o más tipos de cloud.*

5. ¿Con qué comando PowerShell damos la posibilidad a los contenedores Hyper-V o a un contenedor de acceder a Internet?

   Para permitir que los conectores accedan a Internet, hay que crear un vSwitch de tipo NAT con el siguiente comando:

```
New-VMSwitch -Name ”SwitchNAT” -SwitchType NAT
```

6. ¿Qué es el Software Defined Networking?

   SDN permite a las organizaciones administrar dinámicamente sus redes. Utiliza una capa de abstracción lógica que permite gestionar la red de manera dinámica. Se implementa entonces la virtualización de red.

7. ¿Cuál es el rol del Network Controller?

   Network Controller es un rol que se instala en Windows Server 2016 y que permite controlar, desplegar y administrar la infraestructura de red, ya sea física o virtual.

8 ¿Para qué sirve la funcionalidad Dynamic Virtual Machine Queue?

VMQ se ha desarrollado para ser una tecnología de virtualización de hardware para la transferencia eficaz del tráfico de red hacia un sistema operativo invitado virtual. Una tarjeta de red compatible con VMQ clasifica las tramas entrantes que se han de enrutar hacia una cola de espera de recepción basándose en filtros que asocian la cola de espera con el adaptador de red virtual de la máquina virtual. Se asigna una cola de espera a cada búfer del dispositivo virtual, evitando así realizar copias de paquetes inútiles y búsquedas de rutas en el conmutador virtual. Esto, a cambio, permite a cada máquina virtual tener su propia tarjeta virtual dedicada. VMQ proporciona colas de espera diferentes para el dispositivo físico. En VMQ estático, el administrador de Hyper-V puede definir manualmente la afinidad del procesador de las colas de espera físicas hacia diferentes núcleos CPU, creando flujos RSS sobre una tarjeta de red por equipo virtual.

9 ¿Para qué sirven los vSwitchs de tipo SET?

El vSwitch de tipo SET permite habilitar el NIC Teaming en las máquinas virtuales y gestionar hasta 8 tarjetas de red físicas en el host Hyper-V.

10 ¿Cuáles son los "equipos lógicos" que podemos implementar desplegando un Network Controller en un Software Defined Networking?

Una vez desplegado el Network Controller, tenemos la posibilidad de desplegar el Software Load Balancing (equilibrio de carga), una puerta de enlace RAS, un router BGP lógico, que proporciona funcionalidades para implementar una VPN sitio a sitio dedicada para los proveedores cloud o de servicios.

Tabla de objetivos

Objetivos	Capítulos	Trabajos prácticos
Implementación del Sistema de nombres de dominio DNS	Configuración y mantenimiento de DNS	
Instalación y configuración de los servidores DNS	Configuración y mantenimiento de DNS	Configuración del registro de los recursos Caducidad y borrado de los registros Implementación de DNSSEC y de reglas DNS
Creación y configuración de los servidores DNS	Configuración y mantenimiento de DNS	Configuración del registro de los recursos Configuración de un reenviador condicional Creación de una zona secundaria y zona de stub Implementación de DNSSEC y de reglas DNS
Implementación de DHCP	Implementar un servidor DHCP	
Instalación y configuración de DHCP	Implementar un servidor DHCP	Agregar y configurar el rol DHCP Alta disponibilidad del servicio DHCP
Administración y mantenimiento de DHCP	Implementar un servidor DHCP	Agregar y configurar el rol DHCP Implementación de un agente de retransmisión DHCP Alta disponibilidad del servicio DHCP
Implementación de la gestión de direcciones IP (IPAM)	IPAM	
Instalación y configuración de la gestión de direcciones IP (IPAM)	IPAM	Implementación de IPAM
Administración de DNS y DHCP con IPAM	IPAM	Implementación de IPAM
Auditoría IPAM	IPAM	Implementación de IPAM Uso y administración de IPAM
Implementación de soluciones de conectividad de red y de acceso remoto	Configuración del acceso remoto	
Implementación de soluciones de conectividad de red	Configuración del acceso remoto	
Implementación de soluciones de red privada virtual (VPN) y DirectAccess	Configuración del acceso remoto	Configuración de un servidor VPN Configuración de DirectAccess Configuración del cliente DirectAccess
Implementación del servidor NPS (Network Policy Server)	Configuración del acceso remoto	
Implementación de soluciones de red centrales y distribuidas	Prever, planificar e implementar el direccionamiento IP	
Implementación del direccionamiento IPv4 e IPv6	Prever, planificar e implementar el direccionamiento IP	Conversión binaria/decimal Direccionamiento IPv6
Implementación del sistema de archivos distribuidos (DFS) y de soluciones de sucursales	Optimización de los servicios de archivos	Instalación y configuración del servidor DFS Configuración de la replicación Instalación y configuración de BranchCache
Implementación de una infraestructura de red avanzada	Hyper-V y Software Defined	

	Networking	
Implementación de soluciones de red de alto rendimiento	Hyper-V y Software Defined Networking	Creación de un vSwitch de tipo SET y creación de una asociación de tarjetas de red
Determinación de los escenarios y requisitos para la implementación de SDN (*Software Defined Network*)	Hyper-V y Software Defined Networking	Configuración de la protección para un router y para un DHCP