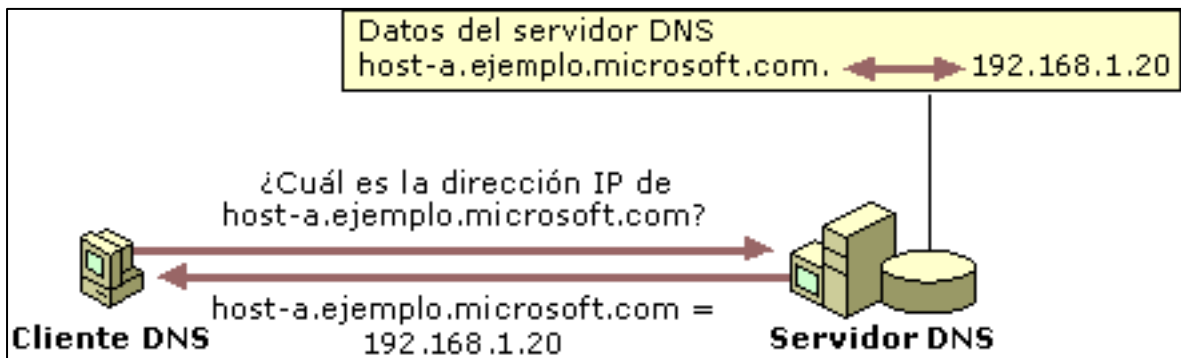


Definición de DNS

DNS es una abreviatura para Sistema de nombres de dominio (*Domain Name System*), un sistema para asignar nombres a equipos y servicios de red que se organiza en una jerarquía de dominios. La asignación de nombres DNS se utiliza en las redes TCP/IP, como Internet, para localizar equipos y servicios con nombres sencillos. Cuando un usuario escriba un nombre DNS en una aplicación, los servicios DNS podrán traducir el nombre a otra información asociada con el mismo, como una dirección IP

El gráfico siguiente muestra un uso básico de DNS, consistente en la búsqueda de la dirección IP de un equipo basada en su nombre.



Integración con DNS

Active Directory utiliza el Sistema de nombres de dominio (DNS, *Domain Name System*). DNS es un servicio estándar de Internet que traduce nombres legibles de equipos host, como mipc.microsoft.com, a direcciones IP numéricas. Esto permite que los procesos que se ejecutan en equipos de redes TCP/IP puedan realizar la identificación y conexión.

Los nombres de dominio de DNS están basados en una estructura jerárquica de nombres DNS que es una estructura de árbol invertida: un único dominio raíz, bajo el que puede haber dominios primarios y secundarios (ramas y hojas). Por ejemplo, un nombre de dominio de Windows 2000 como secundario.primario.microsoft.com identifica a un dominio "secundario", que depende de un dominio denominado "primario", que a su vez es un dominio secundario del dominio raíz microsoft.com.

Active Directory está integrado con DNS de las siguientes formas:

1. Active Directory y DNS tienen la misma estructura jerárquica. Aunque son independientes y se implementan de forma distinta para propósitos diferentes, el espacio de nombres de una organización para DNS y Active Directory tienen una estructura idéntica. Por ejemplo, microsoft.com es un dominio DNS y un dominio de Active Directory.
2. Las zonas DNS se pueden almacenar en Active Directory. Si utiliza el servicio DNS de Windows 2000, los archivos de zona primaria se pueden almacenar en Active Directory para su replicación en otros controladores de dominio de Active Directory.
3. Los clientes de Active Directory utilizan DNS para buscar controladores de dominio. Para localizar un controlador de dominio determinado, los clientes de Active Directory envían una consulta al servidor DNS que tienen configurado para obtener determinados registros de recursos.

Microsoft DNS

El Sistema de nombres de dominio (DNS) es un servicio de nombres estándar para TCP/IP e Internet. El servicio DNS permite registrar y resolver los nombres de dominio DNS a los equipos cliente en la red. Estos nombres se utilizan para la búsqueda y el acceso a recursos que ofrecen otros equipos en la red o en otras redes como Internet.

Para Abrir la Consola de DNS

La consola DNS es una herramienta administrativa que permite administrar sólo servidores DNS de Windows 2000. Para obtener más información, consulte los temas relacionados.

Configurar un servidor principal nuevo

Hay varias situaciones en las que podría agregar y configurar un servidor DNS nuevo para la red:

- Cuando agregue un servidor DNS nuevo a la red y configure una zona nueva para utilizarla por primera vez.
- Cuando haya creado una zona en otro servidor DNS y agregue un servidor nuevo que también necesite cargar y proporcionar servicio en la zona.
- Cuando tenga un servidor DNS configurado con una o más zonas pero necesite agregar una zona nueva para otro nombre de dominio, como un subdominio.

Para configurar por primera vez una zona y un servidor nuevo, es mejor utilizar la lista de comprobación que proporciona la Ayuda de DNS para iniciar la distribución de DNS

Agregar un servidor principal para una zona existente

El servidor principal de una zona actúa como punto de actualización de la zona. Las zonas recién creadas son siempre de este tipo. En Windows 2000 Server puede utilizar las zonas principales de una de las dos maneras siguientes: como zonas principales estándar o zonas principales integradas en Active Directory.

En las zonas de tipo principal estándar sólo un servidor puede alojar y cargar la copia maestra de la zona. Si crea una zona y la mantiene como zona principal estándar, no se admitirán servidores principales adicionales para la zona. Sólo se permite a un único servidor aceptar las actualizaciones dinámicas y procesar los cambios de zona.

El modelo principal estándar implica un único punto de error. Por ejemplo, si por cualquier razón no está disponible en la red el servidor principal de una zona, no se podrán realizar actualizaciones dinámicas en dicha zona. Tenga en cuenta que las consultas de nombres en la zona no se verán afectadas y podrán continuar sin interrupción, siempre que los servidores secundarios de la zona estén disponibles para contestarlas.

No obstante, en Windows 2000 Server podrá agregar más servidores principales para una zona mediante las características de duplicación y almacenamiento integrado en directorios del servicio DNS. Para ello, debe cambiar una zona e integrarla en Active Directory.

Puede integrar una zona existente en Active Directory cambiando el tipo de la zona en el servidor principal de origen en que se creó por primera vez. Cuando haya cambiado el tipo de zona de **Principal estándar** a **Integrada en Active Directory**, podrá agregar la zona a otros servidores DNS configurándolos para utilizar la opción **Inicio desde DS** cuando se inicie el servicio DNS.

Cuando la opción **Inicio desde DS** está activada, otros servidores DNS que funcionen como parte del espacio de nombres del dominio de Active Directory (como los controladores de dominio de Active Directory) podrán consultar el directorio y cargar automáticamente todas las zonas integradas en directorios, almacenadas en la base de datos de directorios. No es necesario ningún otro paso. Con la opción **Inicio desde DS**, cualquier servidor DNS que funcione como parte de Active Directory será también, de forma predeterminada, un servidor principal de las zonas integradas en directorios.

Actualizar los servidores existentes

Puede ser necesario actualizar la configuración de los servidores DNS por varias razones:

- Para cambiar el nombre de equipo (host) del servidor.
- Para cambiar el nombre de dominio DNS principal del equipo servidor.
- Para cambiar la dirección IP del equipo servidor.
- Para quitar un servidor DNS de la red.
- Para cambiar el servidor principal de una zona (sólo para zonas principales estándar).

En las secciones siguientes se tratarán estas razones.

Cambiar el nombre de equipo (host) del servidor

Si necesita cambiar el nombre host de un servidor DNS (pero no su nombre de dominio DNS principal), realice los cambios siguientes en la zona en la que el servidor está configurado como un servidor autoritativo de la zona.

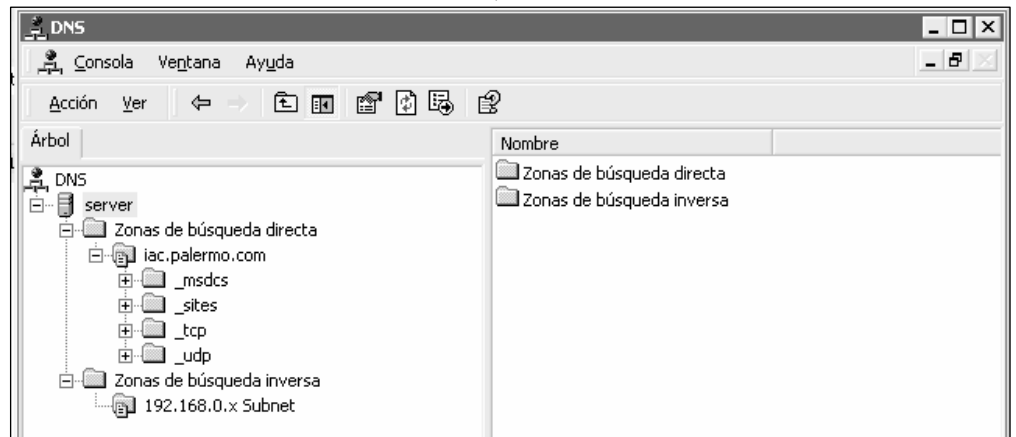
1. Cambie el nombre de equipo del servidor en las Propiedades del sistema.
2. Reinicie el equipo para iniciar las siguientes actualizaciones dinámicas de DNS:
 - a. Agregue los nuevos registros de recursos (RR) de puntero (PTR) y de direcciones host (A) de la dirección IP y el nuevo nombre del servidor.

- b. Quite los RR PTR y A antiguos de la dirección IP, y el nombre antiguo del servidor.
3. Actualice los RR (NS) del servidor de nombres en las zonas en las que el servidor esté configurado como autoritativo para que apunte al nuevo RR A agregado en el paso 2.
4. Si el servidor es el servidor principal de una zona estándar, revise el nombre en el campo propietario del RR de inicio de autoridad (SOA) de la zona (si la zona está integrada en directorios, no será necesario este paso).
5. Compruebe las zonas para asegurarse de que se actualice el nombre de servidor para los registros de delegación (RR NS o A) utilizados.

Cambiar el nombre de dominio DNS principal del servidor

Cuando cambie el nombre de dominio DNS de un equipo, la capacidad de cambiar el nombre de dominio DNS principal del servidor puede depender de si utiliza o no el equipo como controlador de dominio.

Si ejecuta el equipo servidor como controlador de dominio, el nombre de dominio DNS principal del equipo servidor se establece para que sea igual al nombre del dominio de Active Directory en el que se promocionó el servidor a controlador de dominio. Para cambiar este



nombre, antes debe degradar al servidor para que deje de ser un controlador de dominio. Para un servidor que cambie el nombre de dominio DNS principal en esta situación, el proceso de agregar y eliminar los RR PTR y A del servidor se realiza automáticamente cuando se incorpore a un dominio de Active Directory o cuando lo abandone. En este caso, puede que sólo sea necesaria la actualización manual de los RR (NS) del servidor de nombres de los dominios principales DNS nuevos y antiguos.

Para cambiar el nombre de dominio DNS de un equipo del servidor DNS que no utilice Active Directory, como un servidor miembro del dominio o un servidor independiente, pueden ser necesarios algunos cambios adicionales y administración manual. Por ejemplo, si los nombres de dominio DNS nuevos y antiguos están en dos zonas diferentes, como Zona A (la zona antigua) y Zona B (la zona nueva), tendrá que realizar los cambios siguientes:

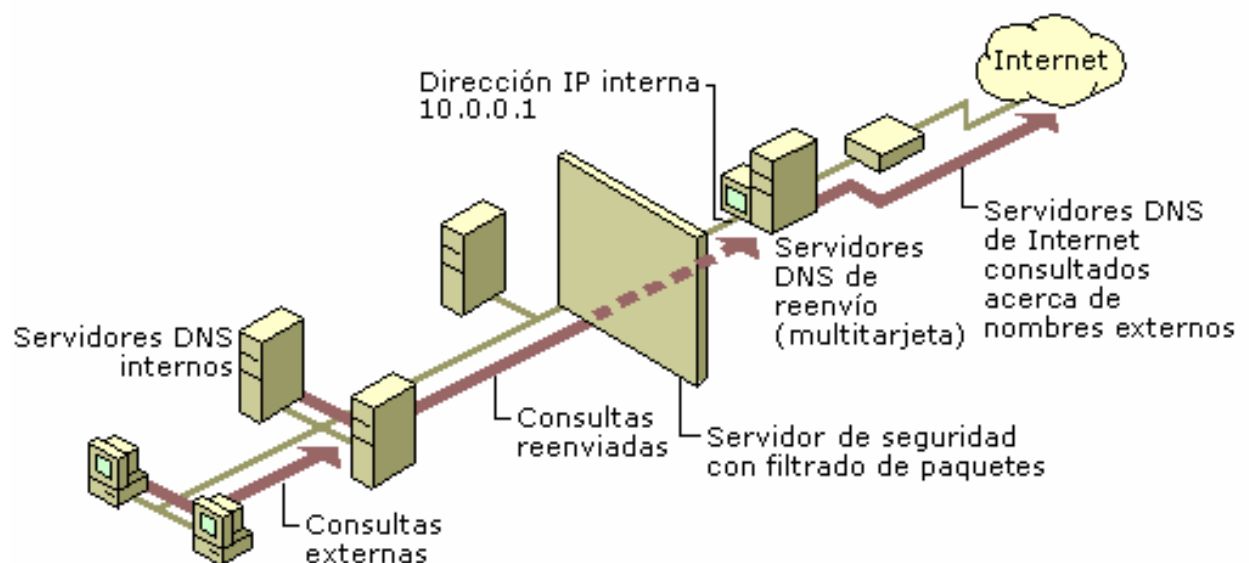
1. Cambie el **Sufijo DNS principal de este equipo** en las Propiedades del sistema y reinicie el equipo.
2. En la Zona A, quite el RR (A) host del servidor.
3. En la Zona B, agregue el RR A del servidor.
4. Actualice todos los RR del servidor de nombres (NS) y de inicio de autoridad (SOA) en las zonas que contengan el nombre del servidor DNS cuyo nombre se cambió.

Utilizar reenviadores

Se puede configurar los servidores DNS para enviar todas las consultas recursivas a una lista seleccionada de servidores, conocidos como reenviadores. Los servidores utilizados en la lista de reenviadores proporcionan una búsqueda recursiva de cualquier consulta recibida por un servidor DNS para la que no pueda producir una respuesta basada en sus zonas locales. Durante el proceso de reenvío, un servidor DNS configurado para usar reenviadores (uno o más servidores basados en la lista de reenviadores) se comportará en esencia como un cliente DNS para sus reenviadores.

Ventajas del uso de reenviadores

Los reenviadores son especialmente útiles cuando el acceso a los servidores DNS remotos requiera el uso de un vínculo lento, como una red interna de alta velocidad vinculada a Internet a través de una conexión de velocidad relativamente baja. El uso de reenviadores en esta situación puede reducir de dos maneras el costoso tráfico a través del vínculo de baja velocidad:



Administrar registros de recursos

Después de crear una zona, es necesario agregarle registros de recursos adicionales. Los registros de recursos (RR) más comunes para agregar son:

- **Host (A)** para asignar un nombre de dominio DNS a una dirección IP que utiliza un equipo.
- **Alias (CNAME)** para asignar un nombre de dominio DNS con alias a otro nombre canónico o principal.
- **Agente de intercambio de correo (MX)** para asignar un nombre de dominio DNS al nombre de un equipo que intercambia o reenvía el correo.
- **Puntero (PTR)** para asignar un nombre de dominio DNS inverso basado en la dirección IP de un equipo que señala al nombre de dominio DNS directo de ese equipo.
- **Ubicación de servicios (SRV)** para asignar un nombre de dominio DNS a una lista especificada de equipos host de DNS que ofrecen un tipo específico de servicio, como los controladores de dominio de Active Directory.
- Otros registros de recursos según sean necesarios.

Registros de recursos de host (A)

Los registros de recursos de host (A) se utilizan en una zona para asociar nombres de dominio DNS de equipos (o hosts) a sus direcciones IP y se pueden agregar a una zona de varias formas:

- Puede crear manualmente un RR A para un equipo cliente TCP/IP estático con la consola DNS.
- Los equipos que ejecutan Windows 2000 utilizan el servicio Cliente de DHCP para registrar y actualizar dinámicamente sus propios registros de recursos A en DNS cuando ocurre un cambio en la configuración IP.
- Los equipos cliente habilitados para DHCP que ejecuten versiones anteriores de sistemas operativos de Microsoft pueden hacer que un servidor proxy registre y actualice sus registros de recursos A si obtienen su concesión de IP de un servidor DHCP calificado (sólo el servicio DHCP que proporciona Windows 2000 Server compatibiliza actualmente esta característica).

El registro de recursos de host (A) no es requerido para todos los equipos, pero es necesario para los equipos que comparten recursos en una red. Cualquier equipo que comparta recursos y tenga que identificarse por su nombre de dominio DNS, tiene que utilizar registros de recursos A para facilitar la resolución de nombres DNS a la dirección IP del equipo.

La mayor parte de los RR A requeridos en una zona puede incluir otros servidores o estaciones de trabajo que comparten recursos, otros servidores DNS, servidores de correo electrónico y servidores Web. Estos registros de recursos contienen la mayoría de los registros de recursos de la base de datos de una zona.

Registros de recursos de alias (CNAME)

Los registros de recursos de alias (CNAME) también se llaman, en ocasiones, *nombres canónicos*. Estos registros permiten utilizar más de un nombre para señalar a un único host, lo que facilita tareas como alojar un servidor FTP y un servidor Web en el mismo equipo. Por ejemplo, los nombres de servidor conocidos (ftp, www) se registran utilizando los RR CNAME que asignan el nombre host de DNS, como "servidor-1", al equipo servidor que aloja estos servicios.

Se recomienda utilizar los RR CNAME en los casos siguientes:

- Cuando se necesita cambiar el nombre a un host especificado en un RR A de la misma zona.
- Cuando se necesita resolver un nombre genérico de un servidor conocido como www en un grupo de equipos individuales (cada uno con RR A individuales) que proporcionan el mismo servicio. Por ejemplo, un grupo de servidores Web redundantes.

Cuando cambie el nombre de un equipo con un RR A existente en la zona, podrá utilizar un RR CNAME de forma temporal con el objeto de permitir un período de gracia para que los usuarios y los programas dejen de especificar el nombre de equipo antiguo y usen el nuevo. Para ello, tiene que hacer lo siguiente:

- Para el nombre de dominio DNS nuevo del equipo, se agrega un RR A nuevo a la zona.
- Para el nombre de dominio DNS antiguo, se agrega un RR CNAME que señala al RR A nuevo.

- El RR A original del nombre de dominio DNS antiguo (y su RR PTR asociado, si procede) se quita de la zona.

Cuando utilice un RR CNAME para asignar un alias o cambiar el nombre a un equipo, establezca un límite temporal en la frecuencia con la que utiliza el registro en la zona antes de quitarlo de DNS. Si olvida eliminar el RR CNAME y después se elimina su RR A asociado, el RR CNAME puede desperdiciar recursos del servidor al intentar resolver consultas de un nombre que ya no se utiliza en la red.

El uso más común o popular de un RR CNAME es el de proporcionar un nombre de dominio con un alias de DNS permanente para la resolución de nombres genérica de un nombre basado en servicios, como `www.example.microsoft.com`, a varios equipos o direcciones IP utilizados en un servidor Web. Por ejemplo, a continuación se muestra la sintaxis básica del uso de un RR CNAME.

nombreAlias IN CNAME nombreCanónicoPrincipal

En este ejemplo, un equipo denominado `host-a.example.microsoft.com` necesita funcionar como un servidor Web denominado "`www.example.microsoft.com`." y como un servidor FTP denominado "`ftp.example.microsoft.com`". Para conseguir el uso deseado para denominar este equipo, puede agregar y utilizar las entradas CNAME siguientes en la zona `example.microsoft.com`:

```
host-a IN A 10.0.0.20
ftp IN CNAME host-a
www IN CNAME host-a
```

Si decide posteriormente mover el servidor FTP a otro equipo independiente del servidor Web en el "host-a", basta con cambiar el RR CNAME en la zona por `ftp.example.microsoft.com` y agregar un RR A adicional a la zona del equipo nuevo que aloja el servidor FTP.

Registros de recursos del agente de intercambio de correo (MX)

El RR del agente de intercambio de correo (MX) es usado por las aplicaciones de correo electrónico para ubicar el servidor de correo electrónico en función del nombre de dominio DNS utilizado en la dirección de destino para el destinatario de un mensaje de correo electrónico. Por ejemplo, se puede utilizar una consulta DNS del nombre "`example.microsoft.com`" para buscar un RR MX y habilitar una aplicación de correo electrónico para reenviar o intercambiar correo electrónico con un usuario con la dirección de correo electrónico "`user@example.microsoft.com`".

El RR MX muestra el nombre de dominio DNS del equipo o equipos que procesan correo en un dominio. Si hay varios RR MX, el servicio Cliente DNS intenta entrar en contacto con los servidores de correo en el orden de preferencia desde el valor más bajo (prioridad más alta) al valor más alto (prioridad más baja). A continuación se muestra la sintaxis básica que se utiliza en un RR MX.

nombreDeDominioDeCorreo IN MX preferencia hostServidorDeCorreo

Al utilizar los RR MX que se muestran debajo en la zona `example.microsoft.com`, el correo dirigido a `user@example.microsoft.com` se entrega primero, si es posible, en

user@mailserver0.example.microsoft.com. Si este servidor no está disponible, el cliente de resolución puede utilizar en su lugar user@mailserver1.example.microsoft.com.

```
@      IN MX 1  mailserver0
@      IN MX 2  mailserver1
```

Tenga en cuenta que el uso del símbolo arroba (@) en los registros indica que el nombre de dominio DNS del servidor de correo es el mismo que el nombre de origen de la zona (example.microsoft.com).