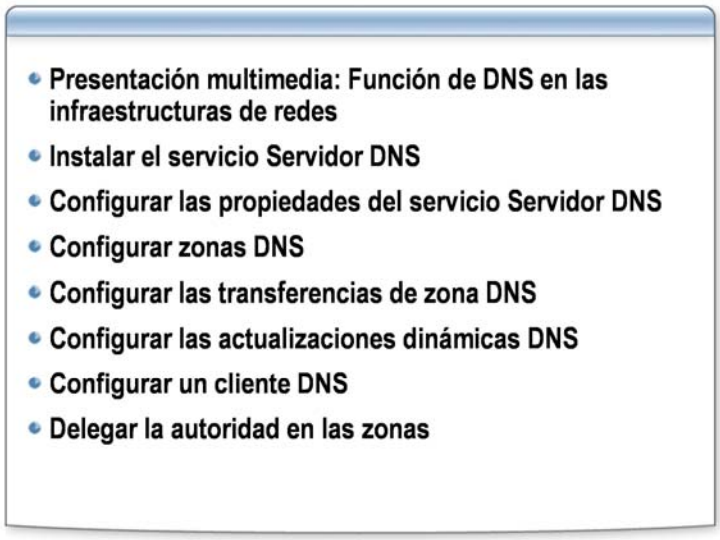
Resolución de nombres de host mediante el Sistema de nombres de dominio (DNS)

Contenido

Introducción



Introducción

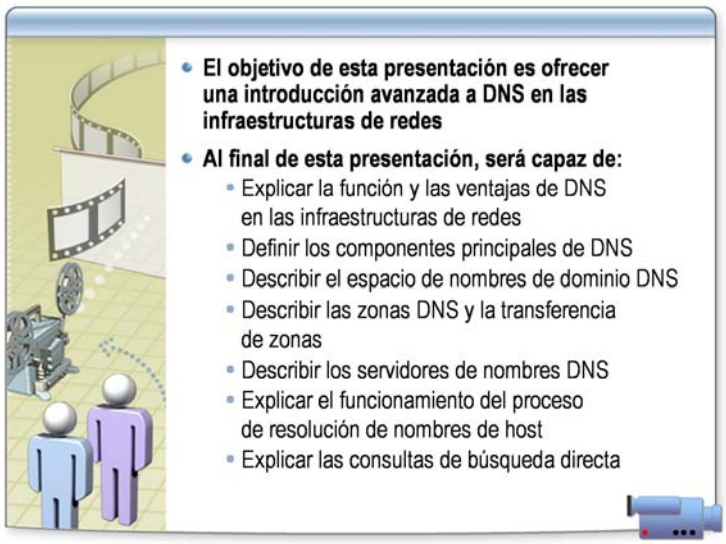
Una solución de red tiene que incluir el Sistema de nombres de dominio (DNS) para conectar los componentes de la infraestructura de redes. Un factor importante en la conexión de componentes es la resolución de los nombres de host en direcciones de Protocolo Internet (IP, *Internet Protocol*). En este módulo, aprenderá cómo resolver nombres de host mediante DNS.

Objetivos

Después de finalizar este módulo, será capaz de:

- Describir la función del Sistema de nombres de dominio (DNS, *Domain Name System*) en las infraestructuras de redes
- Instalar el servicio Servidor DNS.
- Configurar las propiedades del servicio Servidor DNS.
- Configurar zonas DNS.
- Configurar las transferencias de zona DNS.
- Configurar las actualizaciones dinámicas DNS.
- Configurar un cliente DNS.
- Delegar la autoridad en las zonas.

Presentación multimedia: Función de DNS en las infraestructuras de redes



Ubicación del archivo

Para iniciar la presentación *Función de DNS en las infraestructuras de redes*, abra el archivo media30_1.htm que se puede encontrar dentro del fichero media30.zip.

Objetivos

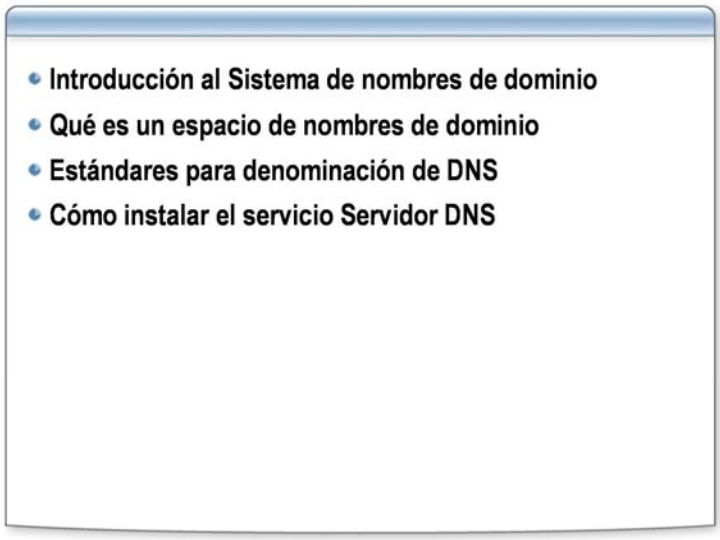
Al final de esta presentación, será capaz de:

- Explicar la función y las ventajas de DNS en las infraestructuras de redes.
- Definir los componentes principales de DNS.
- Describir el espacio de nombres de dominio DNS.
- Describir las zonas DNS y la transferencia de zonas.
- Describir los servidores de nombres DNS.
- Explicar el funcionamiento del proceso de resolución de nombres de host.
- Explicar las consultas de búsqueda directa.

Puntos clave

- DNS es un sistema de base de datos distribuido que puede servir como fundamento para la resolución de nombres en una red IP.
- La mayor parte del software de comunicación de redes, como los programas de correo electrónico y los exploradores Web, emplean DNS para localizar servidores y resolver el nombre descriptivo de un equipo en su dirección IP, o buscar la asignación correspondiente.
- El espacio de nombres de dominio proporciona la estructura de una base de datos DNS distribuida.
- Los dominios pueden organizarse en zonas, que son áreas discretas o contiguas del espacio de nombres de dominio.
- Los datos de la asignación entre nombres y direcciones IP de todos los equipos de una zona se almacenan en un archivo de base de datos de zonas, en un servidor de nombres DNS.

Lección: Instalar el servicio Servidor DNS



Introducción

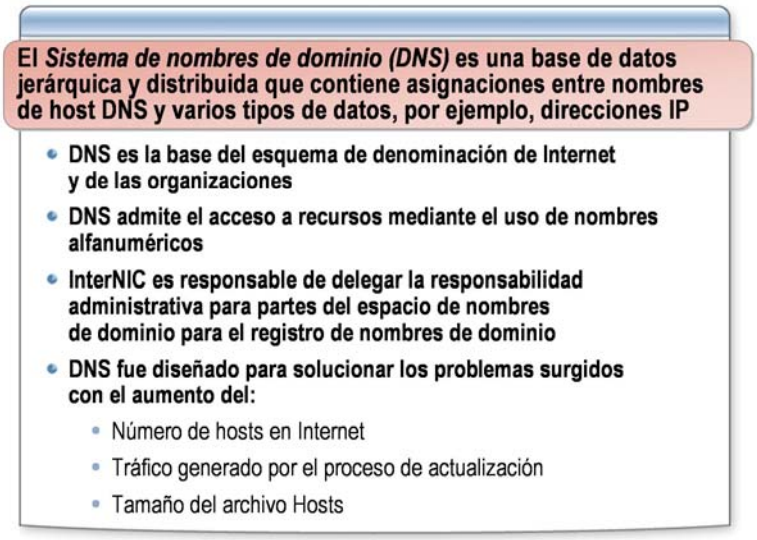
El primer paso para poder resolver nombres de host es instalar el servicio Servidor DNS.

Objetivos de la lección

Después de finalizar esta lección, será capaz de:

- Explicar la finalidad y conceptos básicos de DNS.
- Explicar qué es un espacio de nombres de dominio.
- Definir los estándares para denominación de DNS.
- Instalar el servicio Servidor DNS.

Introducción al Sistema de nombres de dominio



Introducción

DNS es un servicio de resolución de nombres. DNS resuelve direcciones legibles para las personas (como www.microsoft.com) en direcciones (como 192.168.0.1).

Definición

El *Sistema de nombres de dominio (DNS)* es una base de datos jerárquica y distribuida que contiene asignaciones entre nombres de host DNS y direcciones IP. DNS permite la localización de equipos y servicios mediante nombres alfanuméricos, que son fáciles de recordar. DNS permite también el descubrimiento de servicios de red, como servidores de correo electrónico y controladores de dominio en el servicio de directorio Active Directory®.

Finalidad de DNS

DNS es la base del esquema de denominación de Internet y del esquema de denominación de dominios de Active Directory de una organización. DNS admite el acceso a recursos mediante el uso de nombres alfanuméricos. Sin DNS, el usuario tendría que localizar las direcciones IP de los recursos para tener acceso a ellos. Puesto que las direcciones IP de los recursos pueden cambiar, sería difícil mantener una lista exacta de las direcciones IP que les corresponden. DNS permite a los usuarios centrarse en nombres alfanuméricos, que permanecen relativamente constantes en una organización, en vez de hacerlo en direcciones IP.

Con DNS, los nombres de host residen en una base de datos que puede distribuirse entre varios servidores, disminuyendo la carga en cualquier servidor y proporcionando la capacidad de administrar este sistema de denominación en función de las particiones. DNS admite nombres jerárquicos y permite el registro de varios tipos de datos además de la asignación entre nombres de host y direcciones IP que se utilizan en los archivos Hosts. Puesto que la base de datos DNS está distribuida, su tamaño es ilimitado y el rendimiento no disminuye mucho cuando se agregan más servidores.

InterNIC

El sistema de denominación conceptual en el que se basa DNS es una estructura de árbol jerárquica y lógica conocida como el espacio de nombres de dominio. El Centro de información de redes en Internet (InterNIC) administra la raíz o nivel máximo del espacio de nombres de dominio.

InterNIC es responsable de delegar la responsabilidad administrativa para partes del espacio de nombres de dominio y para el registro de nombres de dominio. Los nombres de dominio se administran mediante el uso de un sistema de base de datos distribuida de información de nombres almacenados en servidores de nombres, que se encuentran en toda la red. Cada servidor de nombres tiene archivos de base de datos que contienen información registrada para una región seleccionada dentro de la jerarquía de árbol de dominios.

Nota Para obtener más información acerca de InterNIC, puede visitar el sitio http://www.internic.net.

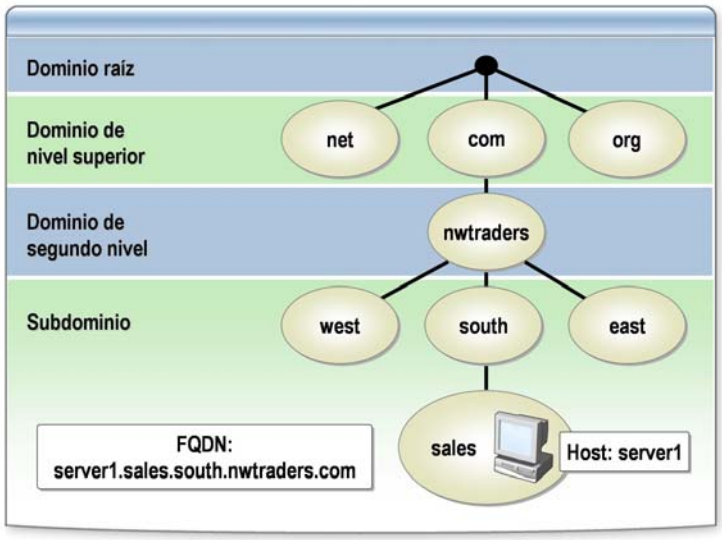
Historia de DNS

DNS nació en los primeros momentos de Internet, cuando era una pequeña red que el Departamento de defensa de los Estados Unidos estableció para fines de investigación. Los nombres de host de los equipos de esta red se administraban mediante el uso de un único archivo de hosts que se encontraba en un servidor administrado centralmente. Cada sitio que tenía que resolver nombres de host en la red descargaba este único archivo.

A medida que el número de hosts de Internet creció, el tráfico que se generaba con el proceso de actualización aumentaba, además del tamaño del archivo de hosts. Se hizo necesaria la existencia de un nuevo sistema que ofreciera características como escalabilidad, administración descentralizada y compatibilidad con varios tipos de datos.

DNS se introdujo en 1984 y se convirtió en este nuevo sistema.

Qué es un espacio de nombres de dominio



Introducción

Un espacio de nombres DNS incluye el dominio raíz, dominios de nivel superior, dominios de nivel secundario y, posiblemente, subdominios. Juntos, el espacio de nombres DNS y el nombre de host conforman el nombre de dominio completo (FQDN).

Finalidad de un espacio de nombres de dominio

El espacio de nombres DNS permite mostrar nombres de recursos para organizarlos en una estructura lógica que los usuarios pueden entender fácilmente. Gracias a la estructura jerárquica del espacio de nombres DNS, la organización y localización de recursos se simplifica en gran medida.

Espacio de nombres de dominio

El *espacio de nombres de dominio* es un árbol de nombres jerárquico que DNS utiliza para identificar y localizar un host dado en un dominio en relación a la raíz del árbol.

Los nombres de la base de datos DNS establecen una estructura de árbol lógica conocida como *espacio de nombres de dominio*. El nombre de dominio identifica la posición de un dominio en el árbol de nombres en relación a su dominio principal. Para utilizar y administrar un servicio DNS, el espacio de nombres de dominio hace referencia a cualquier estructura de árbol de nombres de dominio en su totalidad, desde la raíz de nivel superior del árbol a las ramas de los niveles inferiores. El árbol debe cumplir las convenciones aceptadas para representar nombres DNS. La convención principal es simplemente ésta: para cada nivel de dominio, se utiliza un punto (.) con el fin de separar cada subdominio descendente de su dominio de nivel primario.

Dominio

Un *dominio*, en DNS, es cualquier árbol o subárbol dentro del espacio de nombres de dominio general. Aunque los nombres para dominios DNS se utilizan para denominar dominios de Active Directory, son diferentes de los dominios de Active Directory y no deben confundirse.

Dominio raíz

Éste es el nodo raíz del árbol DNS. No tiene asignado nombre (nulo). A veces se representa en nombres DNS mediante un punto (.) para designar que el nombre se encuentra en la raíz o nivel más alto de la jerarquía de dominios.

Dominio de nivel superior

Es la parte posterior (extremo derecho) de un nombre de dominio. Normalmente, un dominio de nivel superior se establece como un código de nombre de dos o tres caracteres que identifica el estado organizativo o geográfico para el nombre de dominio. En el ejemplo www.microsoft.com, el nombre de dominio de nivel superior es la parte ".com" del mismo, que indica que este nombre ha sido registrado por una organización para uso comercial.

Nota Un espacio de nombres corporativo interno, como puede ser un bosque de Active Directory, no tiene que finalizar en un dominio de nivel superior válido. Se puede utilizar para fines internos el dominio corp.ejemplo.local u otro espacio de nombres que no esté reconocido en Internet.

Dominio de segundo nivel

Un nombre de dominio de segundo nivel es un nombre único de longitud variable que InterNIC registra formalmente para un profesional u organización que se conecta a Internet. En el ejemplo de www.microsoft.com, el nombre de segundo nivel es la parte ".Microsoft" del mismo, que InterNIC registra y asigna a Microsoft Corporation.

Subdominio

Además de un nombre de segundo nivel que esté registrado con InterNIC, una gran organización puede subdividir su nombre de dominio registrado agregando subdivisiones o departamentos representados por una parte de nombre independiente. A continuación, se muestran ejemplos de nombres de subdominio:

- .sales.microsoft.com
- .finance.microsoft.com
- .corp.ejemplo.local

Nombre de dominio completo

Un *nombre de dominio completo (FQDN)* es un nombre de dominio DNS que se ha determinado de forma inequívoca para indicar con una certeza absoluta su ubicación en el árbol del espacio de nombres de dominio.

Ejemplo

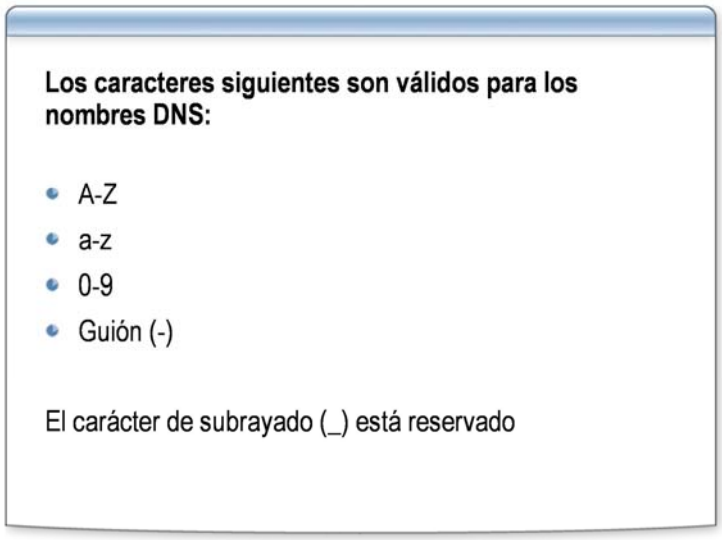
La ilustración de la diapositiva muestra el espacio de nombres DNS de una compañía que está conectada a Internet.

El dominio raíz y los dominios de primer nivel .net, .com y .org representan el espacio de nombres Internet, la parte del espacio de nombres bajo control administrativo del cuerpo gubernamental de Internet.

El dominio de segundo nivel, nwtraders, y sus subdominios west, south, east y el subdominio sales representan todos el espacio de nombres privado, bajo el control administrativo de la compañía, Northwind Traders.

El nombre de dominio completo para el host server1, server1.sales.south.nwtraders.com, indica exactamente dónde reside este host en el espacio de nombres en relación a la raíz.

Estándares para denominación de DNS



Propósito de los estándares para denominación de DNS

Los estándares para denominación de DNS están diseñados para permitir la coherencia entre cualquier implementación de DNS. Dichos estándares son las reglas globales, por lo que independientemente de quién implemente DNS, su implementación puede interoperar con otras. Gracias a los estándares de denominación de DNS, las organizaciones que implementan un espacio de nombres DNS también pueden utilizar el mismo espacio de nombres en Internet.

Estándares para denominación de DNS

Los estándares para denominación de DNS admiten un subconjunto limitado del juego de caracteres ASCII para DNS. En el documento de Solicitud de comentarios (RFC, *Request for Comments*) 1123 se especifican los caracteres siguientes como válidos para nombres DNS.

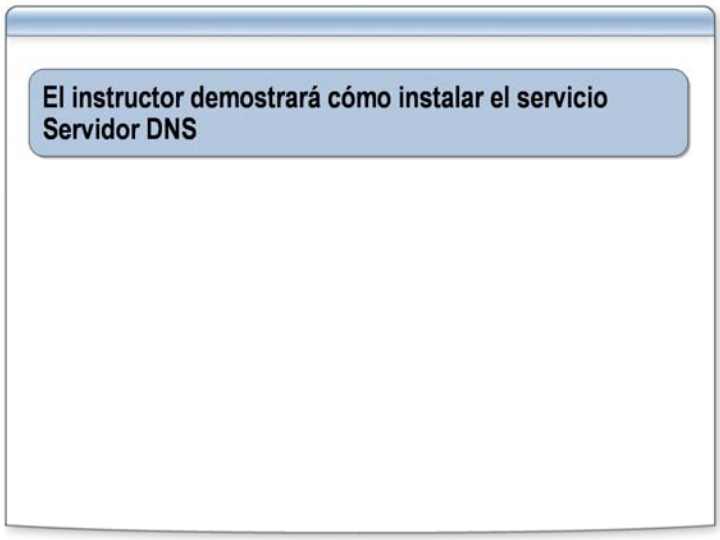
- A-Z
- a-z
- 0-9
- Guión (-)

  Todos los caracteres no válidos se sustituyen por guiones. Por ejemplo, si se utiliza un carácter de subrayado en el nombre del equipo, éste será sustituido por un guión.

Aunque los servidores DNS que ejecutan Microsoft® Windows® 2000 y versiones posteriores incluyen compatibilidad para caracteres ASCII extendidos y Unicode, se recomienda limitar los nombres DNS a los caracteres especificados en el documento RFC 1123.

El carácter de subrayado (_) está reservado para fines especiales en registros SRV. Para obtener más información, consulte el documento RFC 2782.

Cómo instalar el servicio Servidor DNS



Introducción

El primer paso para crear una solución DNS para resolver nombres de host es instalar el servicio Servidor DNS.

Nota Es recomendable que inicie sesión con una cuenta que no tenga credenciales administrativas y que ejecute el comando **Ejecutar como** con una cuenta de usuario que disponga de las credenciales administrativas apropiadas para realizar esta tarea.

Recomendación

Para instalar el servicio Servidor DNS es necesario disponer de derechos administrativos.

Procedimiento para instalar el servicio Servidor DNS

Para instalar un servidor DNS:

Nota Para fines instructivos, este procedimiento sólo explica la instalación de un servicio Servidor DNS. Si desea aprender y practicar la configuración del servidor DNS, consulte la lección Configurar las propiedades del servicio Servidor DNS en este módulo.

1. Inicie sesión con una cuenta de usuario no administrativa.
2. Haga clic en **Inicio** y, después, haga clic en **Panel de control**.
3. En el Panel de control, abra **Herramientas administrativas**, haga clic con el botón secundario del *mouse* (ratón) en **Administre su servidor** y seleccione **Ejecutar como**.
4. En el cuadro de diálogo **Ejecutar como**, seleccione **El siguiente usuario**, escriba una cuenta de usuario y una contraseña que tenga los permisos apropiados para completar la tarea y, después, haga clic en **Aceptar**.
5. En la ventana **Administre su servidor**, haga clic en **Agregar o quitar función**.

6. En la página **Pasos preliminares**, haga clic en **Siguiente**.
7. En la página **Función del servidor**, seleccione **Servidor DNS** y haga clic en **Siguiente**.
8. En la página **Resumen de las selecciones**, haga clic en **Siguiente**.
9. Si se le pide, introduzca el CD de Microsoft Windows Server 2003.
10. En la página **Asistente para configurar un servidor DNS**, haga clic en **Cancelar**.

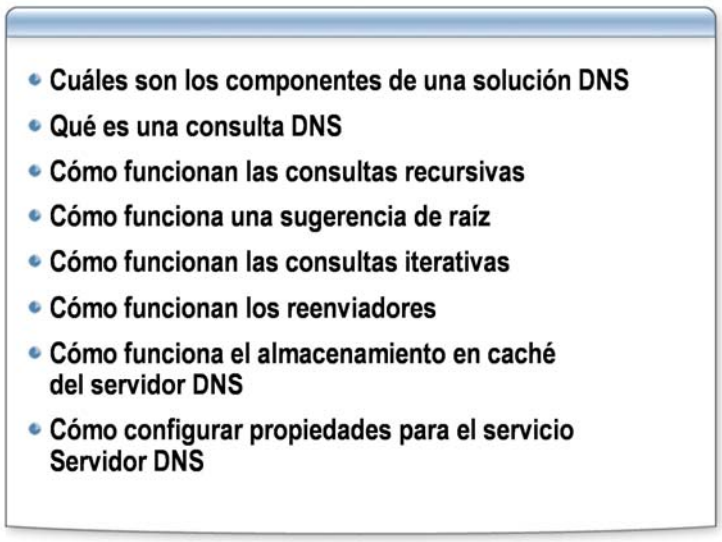
Nota El servicio DNS se configurará en un ejercicio posterior.

11. En la página **Asistente para configurar su servidor**, haga clic en **Finalizar**.

Ejercicio: Instalar el servicio Servidor DNS

Objetivo	En este ejercicio, instalará el servicio Servidor DNS.
Instrucciones	Para completar este ejercicio, consulte el documento *Valores del plan de implementación*, incluido en el apéndice al final del cuaderno de trabajo. Debe haber iniciado sesión con una cuenta que no tenga credenciales administrativas y ejecutar el comando **Ejecutar como** con una cuenta de usuario que disponga de las credenciales administrativas apropiadas para realizar la tarea.
Situación de ejemplo	El departamento de laboratorio ha sido diseñado para utilizar un servidor DNS corporativo para la resolución de nombres. La ingeniera de sistemas ha aprobado un nuevo servidor DNS para cada subred del departamento. Tendrá que instalar el servicio Servidor DNS para su subred.
Ejercicio	**Instalar el servicio Servidor DNS** ■ Complete esta tarea desde los equipos de ambos alumnos. ■ Nombre de usuario: **nwtraders***NombreDeEquipo*__Admin__ ■ Contraseña: **P@ssw0rd** ■ Para el ejercicio, no configure el servidor DNS en este momento.

Lección: Configurar las propiedades del servicio Servidor DNS



Introducción

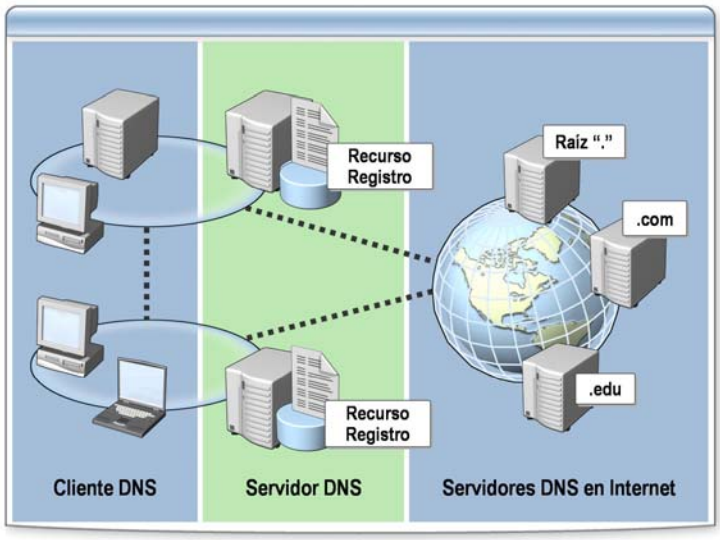
Una solución DNS está compuesta por el servidor DNS, clientes DNS y los recursos a los que hacen referencia los registros de recursos en DNS. Tras la instalación del servicio Servidor DNS, el paso siguiente es configurar correctamente el servidor DNS para su entorno.

Objetivos de la lección

Después de finalizar esta lección, será capaz de:

- Explicar cuáles son los componentes de una solución DNS.
- Definir qué es una consulta DNS.
- Describir cómo funcionan las consultas recursivas.
- Describir cómo funcionan las sugerencias de raíz.
- Explicar cómo funcionan las consultas iterativas.
- Describir cómo funcionan los reenviadores.
- Definir cómo funciona el almacenamiento en caché del servidor DNS.
- Configurar las propiedades para el servicio Servidor DNS.

Cuáles son los componentes de una solución DNS



Componentes de DNS

Los componentes de una solución DNS se describen en la tabla siguiente.

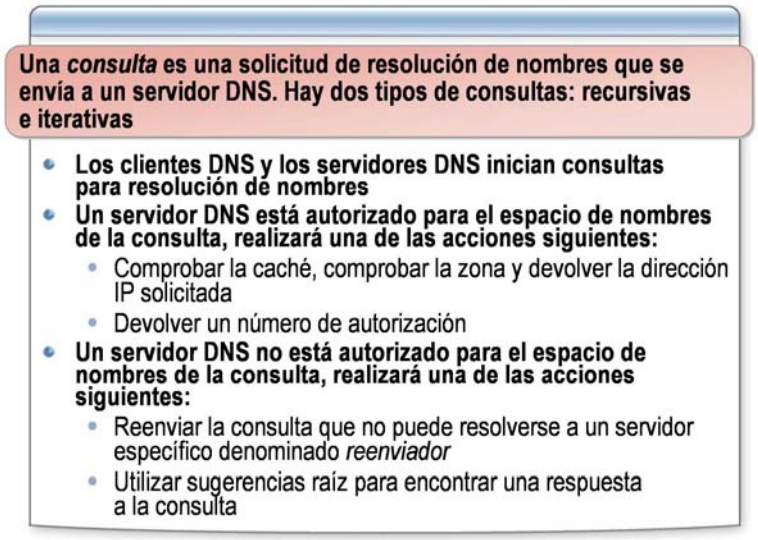
Componente	Descripción
Servidor DNS	• Equipo que ejecuta el servicio DNS • Aloja un espacio de nombres o parte de un espacio de nombres (dominio) • Autorizado para un espacio de nombres o dominio • Resuelve las consultas de resolución de nombres que los clientes DNS (Cliente DNS = Solucionador) envían
Cliente DNS	• Equipo que ejecuta el servicio Cliente DNS
Registros de recursos DNS	• Entradas en la base de datos DNS que asignan nombres de host a recursos

Nota En este curso, se hace referencia al servidor de nombres como *servidor DNS*.

Ejemplo

Los componentes de una solución DNS son los clientes DNS, los servidores DNS y los registros de recursos DNS. Los registros de recursos se encuentran en la base de datos de servidores DNS. También, si su solución DNS está conectada a Internet, pueden utilizarse los servidores DNS de Internet.

Qué es una consulta DNS



Definición

Una *consulta* es una solicitud de resolución de nombres que se envía a un servidor DNS. Hay dos tipos de consultas: recursivas e iterativas.

Nota Las consultas recursivas e iterativas se explicarán posteriormente en esta lección.

Finalidad de una consulta DNS

La finalidad de una solución DNS es permitir a los usuarios el acceso a los recursos mediante nombres alfanuméricos. Una consulta DNS se genera cuando el solucionador de cliente DNS pide al servidor DNS la dirección IP del nombre proporcionado. La consulta DNS es la manera en la que el servicio o aplicación obtiene la dirección IP del recurso para poder tener acceso a él.

Cómo se inician las consultas DNS

Los clientes DNS y los servidores DNS inician consultas para resolución de nombres. Un sistema de cliente puede emitir una consulta a un servidor DNS, que puede emitir después consultas a otros servidores DNS.

Servidores DNS autorizados y no autorizados

Un servidor DNS puede estar autorizado o no para el espacio de nombres de la consulta. Estar *autorizado* quiere decir que un servidor DNS aloja una copia principal o secundaria de una zona DNS.

Si el servidor DNS está autorizado para el espacio de nombres de la consulta, el servidor DNS realizará una de las acciones siguientes:

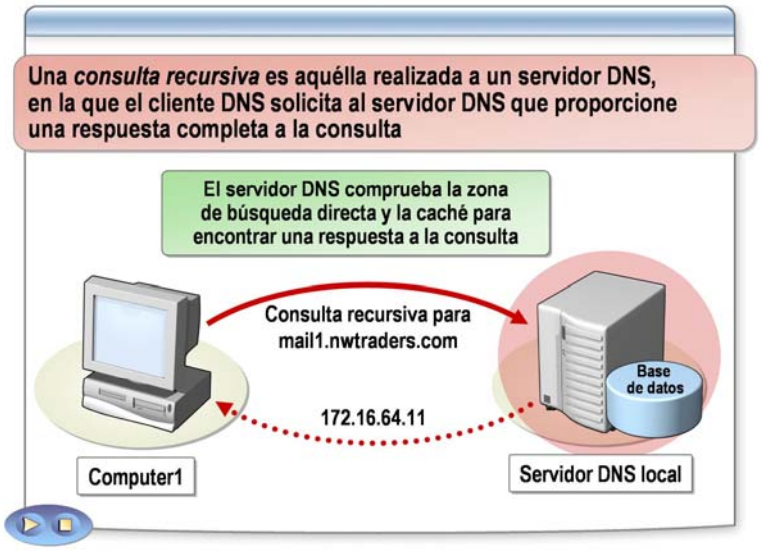
- Comprobar la caché, comprobar la zona y devolver la dirección IP solicitada.
- Devolver un número de autorización.

Si el servidor DNS local *no está autorizado* para el espacio de nombres de la consulta, realizará una de las acciones siguientes:

- Reenviar la consulta que no puede resolverse a un servidor específico denominado reenviador.
- Utilizar direcciones reconocidas de varios servidores raíz para subir en el árbol DNS y localizar una respuesta para la consulta. Este proceso se denomina también *sugerencias de raíz*.

Nota Los reenviadores se explican más adelante en esta lección. Para obtener más información acerca de las sugerencias de raíz, consulte la lección Configurar las zonas DNS en este módulo.

Cómo funcionan las consultas recursivas



Definición

Una *consulta recursiva* es aquélla realizada a un servidor DNS, en la que el cliente DNS solicita al servidor DNS que proporcione una respuesta completa a la consulta. La única respuesta aceptable a una consulta recursiva es la respuesta completa o una que indique que el nombre no se pudo resolver. Una consulta recursiva no puede redirigirse a otro servidor DNS.

Finalidad de una consulta recursiva

Mediante una consulta recursiva, el cliente DNS puede confiar en el servidor DNS para localizar la asignación entre el nombre de host y la dirección IP. El cliente DNS pregunte al servidor DNS la asignación y acepta su respuesta.

Consulta recursiva

Las consultas recursivas pueden ser iniciadas por un cliente DNS o por un servidor DNS que se configuren como reenviadores. Una consulta recursiva deja al servidor consultado la responsabilidad de devolver una respuesta final.

La respuesta a una consulta recursiva siempre será positiva o negativa (dependiendo de si la referencia se ha encontrado o no). En una consulta recursiva, se pide al servidor DNS consultado que responda con una de las respuestas siguientes:

- Los datos solicitados.
- Un error que establece que los datos del tipo solicitado no existen.
- Una respuesta que establece que el nombre de dominio especificado no existe.

Cómo funciona una consulta recursiva

Los pasos siguientes describen cómo funciona una consulta recursiva de un cliente al servidor DNS configurado de dicho cliente:

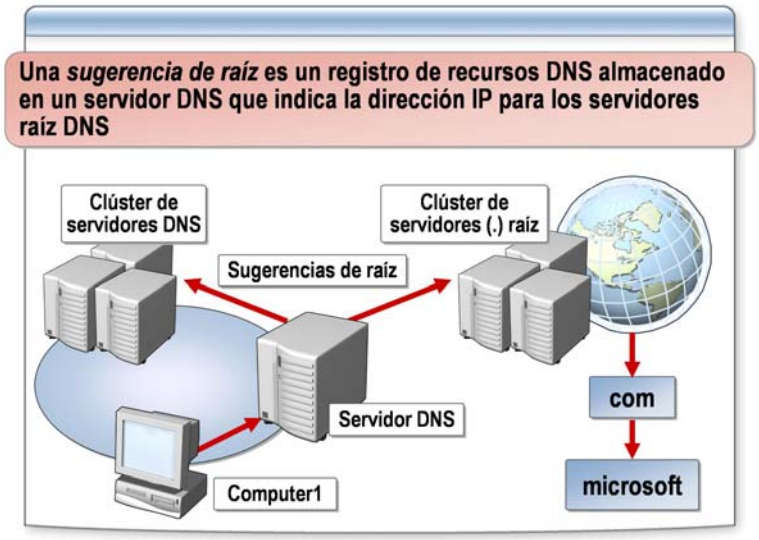
1. El cliente envía una consulta recursiva al servidor DNS local.
2. El servidor DNS local comprueba la zona de búsqueda directa y la caché para una respuesta a la consulta.
3. Si se encuentra la respuesta a la consulta, el servidor DNS la devuelve al cliente.
4. Si *no* se encuentra respuesta, el servidor DNS utiliza una dirección de reenviador o sugerencias de raíz para localizar una.

Ejemplo

En la ilustración, el cliente DNS pregunta al servidor DNS la dirección IP del nombre para mostrar proporcionado. Entonces, el cliente DNS acepta la respuesta del servidor DNS.

El cliente DNS, utilizando el servicio de resolución DNS, envía una consulta DNS al servidor DNS para obtener la dirección IP de mail1.nwtraders.msft. El servidor DNS comprueba la caché para localizar el registro. Si la caché no contiene el registro, el servidor DNS localiza el servidor DNS autorizado para el dominio nwtraders.msft. Si el servidor DNS está autorizado para el dominio, éste busca la zona para el registro de recursos. Si el registro existe, el servidor devuelve la dirección IP para el registro consultado. Si no existe, el servidor DNS informa al cliente de que el registro no se encontró.

Cómo funciona una sugerencia de raíz



Definición

Una *sugerencia de raíz* es un registro de recursos DNS almacenado en un servidor DNS que indica la dirección IP para los servidores raíz DNS.

Función de una sugerencia de raíz

Cuando el servidor DNS recibe una consulta DNS, comprueba la caché. Entonces, el servidor DNS intenta localizar el servidor DNS autorizado para el dominio consultado. Si el servidor DNS no tiene la dirección IP del servidor DNS autorizado para dicho dominio y si el servidor DNS está configurado con las direcciones IP de las sugerencias de raíz, el servidor DNS consultará a un servidor raíz el dominio a la izquierda del dominio raíz de la consulta.

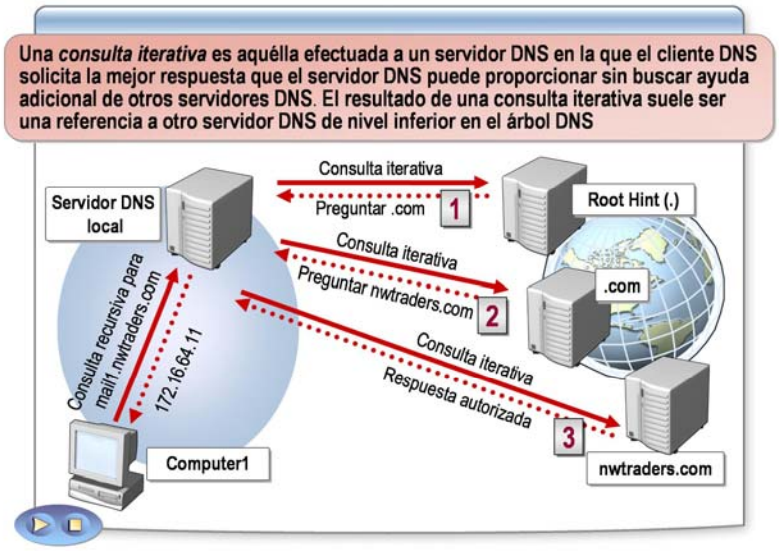
El servidor raíz DNS devuelve entonces la dirección IP del dominio a la izquierda del dominio raíz y el servidor DNS continúa analizando el nombre de dominio completo hasta localizar el dominio autorizado.

Las sugerencias de raíz se almacenan en el archivo Cache.dns, que se encuentra en la carpeta %SystemRoot%\System32\Dns.

Función de las sugerencias de raíz dentro de una organización

En circunstancias normales, las sugerencias de raíz indican las direcciones IP para los servidores raíz DNS que InterNIC mantiene en Internet. Las sugerencias de raíz también apuntan a un servidor DNS local. Si las sugerencias de raíz apuntan a un servidor local, los únicos nombres que estarán disponibles para resolución son aquéllos a los que el servidor DNS puede hacer referencia (normalmente, sólo direcciones locales). Esta configuración a veces puede utilizarse para incrementar la seguridad, puesto que en ella sólo pueden resolverse los dominios internos.

Cómo funcionan las consultas iterativas



Definición

Una *consulta iterativa* es aquélla efectuada a un servidor DNS en la que el cliente DNS solicita la mejor respuesta que el servidor DNS puede proporcionar sin buscar ayuda adicional de otros servidores DNS. Las consultas iterativas se denominan a veces consultas no recursivas. El resultado de una consulta iterativa suele ser una referencia a otro servidor DNS de nivel inferior en el árbol DNS. Una referencia no sería una respuesta aceptable a una consulta recursiva.

Finalidad de una consulta iterativa

El objetivo de una consulta iterativa es que el servidor DNS, que ahora puede utilizar la consulta recursiva del cliente, es responsable de encontrar una respuesta a la pregunta del cliente. El servidor DNS buscará una respuesta en su propia base de datos e incluso consultará servidores DNS de diferentes niveles del espacio de nombres de dominio para localizar el servidor DNS autorizado para la consulta original.

Consulta iterativa

Un servidor DNS suele efectuar una consulta iterativa a otros servidores DNS después de haber recibido una consulta recursiva por parte de un cliente. En una consulta iterativa, el servidor de nombres consultado devuelve al solicitante la mejor respuesta que tiene actualmente. Las respuestas a consultas iterativas pueden ser:

- Respuestas positivas.
- Respuestas negativas.
- Referencias a otros servidores.

Nota Un servidor DNS local suele emitir consultas iterativas a otro servidor DNS de cualquier lugar del espacio de nombres a la vez que intenta resolver una consulta de nombres en nombre de un cliente. Para que quede más claro, es el servicio Cliente DNS en el servidor DNS local el que emite la consulta iterativa.

Referencia

Una *referencia* es una lista de objetivos, que pasan desapercibidos para el usuario, que un cliente recibe de DNS cuando el usuario está teniendo acceso a una raíz o a un vínculo en el espacio de nombres DNS. La información de referencia se almacena en la caché del cliente durante un período especificado en la configuración DNS.

Si el servidor DNS consultado no tiene una coincidencia exacta para el nombre consultado, la mejor información que puede devolver es una referencia. Una referencia apunta a un servidor DNS que está autorizado para un nivel inferior del espacio de nombres de dominio.

El cliente DNS, en el servidor DNS local, puede consultar al servidor DNS para el que obtuvo una referencia. Este proceso continúa hasta que localiza un servidor DNS que esté autorizado para el nombre consultado o bien hasta que se genere un error o se cumpla una condición de tiempo de espera.

Recursividad

La *recursividad* es una función del servidor DNS con la que un servidor DNS emite una serie de varias consultas iterativas a otros servidores DNS al mismo tiempo que responde a una consulta recursiva que emite un cliente DNS.

Los servidores DNS consultados devuelven referencias, que el servidor que realiza la consulta sigue hasta recibir una respuesta definitiva. La recursividad finaliza siempre cuando un servidor propietario del espacio de nombres proporciona una respuesta positiva o negativa.

Cómo funciona una consulta iterativa

En la ilustración, el servidor DNS local no ha conseguido resolver el nombre solicitado utilizando datos almacenados en la caché y no está autorizado para el dominio. Por tanto, comienza el proceso de localizar el servidor DNS autorizado mediante consultas a servidores DNS adicionales. Para localizar el servidor DNS autorizado para el dominio, el servidor DNS resuelve el nombre de dominio completo desde la raíz al host mediante consultas iterativas.
El proceso que se utiliza en este ejemplo es el siguiente:

1. El servidor DNS local recibe una consulta recursiva de un cliente DNS.

   Por ejemplo, el servidor DNS local recibe una consulta recursiva de Computer1 para mail1.nwtraders.com.

2. El servidor DNS local envía una consulta iterativa al servidor raíz para obtener un servidor de nombres autorizado.

3. El servidor raíz responde con una referencia a un servidor DNS cercano al nombre de dominio enviado.

   Por ejemplo, el servidor raíz responde con una referencia al servidor DNS para .com.

4. El servidor DNS local realiza una consulta iterativa al servidor DNS que está más cerca del nombre de dominio enviado.

   Por ejemplo, el servidor DNS local efectúa entonces una consulta iterativa al servidor DNS para .com.

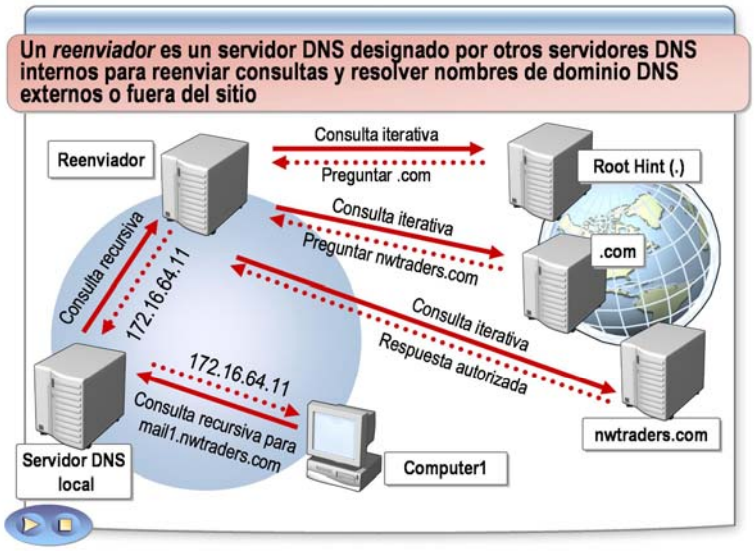
5. El proceso continúa hasta que el servidor DNS local recibe una respuesta autorizada.

   Por ejemplo, el servidor DNS para .com responde con una referencia al servidor DNS para nwtraders.com. Después, el servidor DNS local envía una consulta iterativa al servidor DNS para que nwtraders.com obtenga un nombre autorizado del servidor de nombres autorizados. El servidor DNS local recibe entonces una respuesta autorizada del servidor DNS para nwtraders.com.

6. La respuesta se envía a continuación al cliente DNS.

   Por ejemplo, el servidor DNS local envía esta respuesta autorizada a Computer1, que puede conectarse entonces a mail1.nwtraders.com mediante la dirección IP apropiada.

Cómo funcionan los reenviadores



Definición

Un *reenviador* es un servidor DNS que otros servidores DNS internos designan para reenviar consultas y resolver nombres de dominio DNS externos o fuera del sitio.

Finalidad de los reenviadores

Cuando un servidor de nombres DNS recibe una consulta, intenta localizar la información solicitada dentro de los archivos de su propia zona. Si no lo consigue, bien porque el servidor no esté autorizado para el dominio solicitado o bien porque no tenga el registro de una búsqueda anterior almacenado en la caché, el servidor debe comunicarse con otros servidores de nombres para resolver la solicitud. En una red conectada globalmente como Internet, las consultas DNS que están fuera de una zona local pueden necesitar la interacción con servidores de nombres DNS en vínculos de la red de área extensa (WAN) fuera de la organización. La creación de reenviadores DNS es una manera de designar servidores de nombres específicos como responsables del tráfico DNS basado en WAN.

Se pueden seleccionar servidores de nombres DNS específicos para ser reenviadores, en cuyo caso sus servidores resolverán consultas DNS en nombre de otros servidores DNS.

Proceso de los reenviadores DNS

En la ilustración, el servidor DNS local no ha conseguido resolver el nombre solicitado con sus archivos de zona y los datos almacenados en la caché, así que reenvía la consulta al reenviador. El reenviador empieza el proceso de enviar a otros servidores de nombres consultas iterativas.

Los reenviadores DNS utilizan el proceso siguiente:

1. El servidor DNS local recibe una consulta recursiva de un cliente DNS.

   Por ejemplo, el servidor DNS local recibe una consulta recursiva de Computer1.

2. El servidor DNS local reenvía la consulta al reenviador.

3. El reenviador envía una consulta iterativa al servidor raíz para obtener un nombre autorizado de un servidor de nombres autorizado.
4. El servidor raíz responde con una referencia a un servidor DNS cercano al nombre de dominio enviado.

   Por ejemplo, el servidor raíz responde con una referencia al servidor DNS para .com.
5. El reenviador realiza una consulta iterativa al servidor DNS que está más cerca del nombre de dominio enviado.

   Por ejemplo, el reenviador efectúa entonces una consulta iterativa al servidor DNS para .com.
6. El proceso continúa hasta que el reenviador recibe una respuesta autorizada.

   Por ejemplo, el servidor DNS para .com responde con una referencia al servidor DNS para nwtraders.com. Después, el reenviador envía una consulta iterativa al servidor DNS para que nwtraders.com obtenga un servidor de nombres autorizado. El reenviador recibe entonces una respuesta autorizada del servidor DNS para nwtraders.com.
7. El reenviador envía la respuesta al servidor DNS local, que envía entonces la respuesta al cliente DNS.

   Por ejemplo, el reenviador envía la respuesta al servidor DNS local, que envía entonces la respuesta a Computer1.

Comportamiento del reenviador

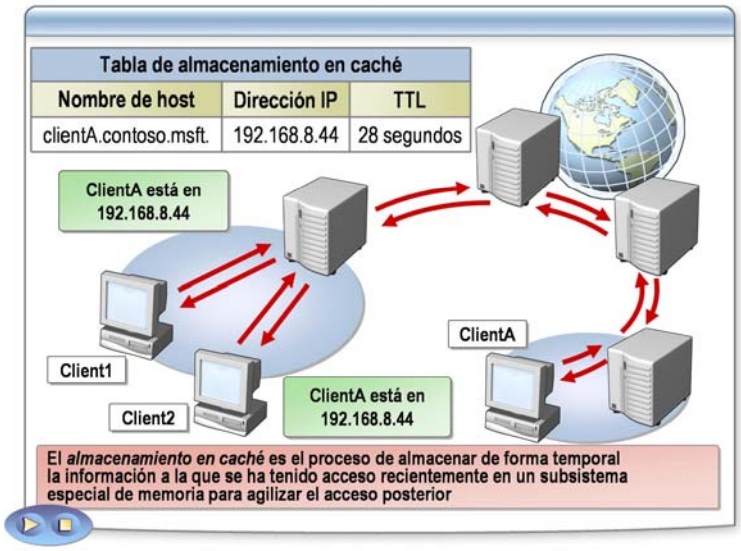
Los servidores de nombres que no son reenviadores pueden configurarse para utilizar reenviadores. Los servidores DNS pueden configurarse con la dirección de uno o varios reenviadores.

Un servidor de nombres puede utilizar un reenviador en modo exclusivo o no exclusivo:

- En *modo no exclusivo*, si el reenviador no puede resolver la consulta, el servidor de nombres que recibió la consulta original intenta resolver la consulta por sí mismo.
- En *modo exclusivo*, si el reenviador no puede resolver la consulta, el servidor de sólo reenvío devuelve un error de consulta al solicitante original. Los servidores de sólo envío no intentan resolver la solicitud por sí mismos si el reenviador no puede resolverla.

El *reenvío condicional* permite a un servidor DNS utilizar un reenviador cuando el servidor resuelve un conjunto de dominios seleccionado. Por ejemplo, el reenvío condicional permitiría a un servidor DNS reenviar solicitudes de resolución de direcciones IP para hosts en una organización asociada que tenga una infraestructura DNS privada para su servidor DNS, mientras que todas las demás solicitudes podrían resolverse normalmente.

Cómo funciona el almacenamiento en caché del servidor DNS



Definición

El *almacenamiento en caché* es el proceso de almacenar de forma temporal la información a la que se ha tenido acceso recientemente en un subsistema especial de memoria para agilizar el acceso posterior.

Finalidad del almacenamiento en caché del servidor DNS

El almacenamiento en caché proporciona respuestas más rápidas a las solicitudes y reduce el tráfico de red DNS. Mediante el almacenamiento en caché de las respuestas DNS, el servidor DNS puede resolver las solicitudes futuras para dicho registro desde la caché. De este modo se reduce enormemente el tiempo de respuesta y se elimina el tráfico de red que se genera al enviar la solicitud a otro servidor DNS.

Proceso de almacenamiento en caché del servidor DNS

Cuando un servidor está procesando una consulta recursiva, se le podría pedir que distribuya varias solicitudes para encontrar la respuesta definitiva. En el caso más desfavorable para resolver un nombre, el servidor de nombres local empieza en la parte superior del árbol DNS con uno de los servidores de nombres raíz y va bajando hasta encontrar los datos solicitados.

El servidor almacena en la caché toda la información que recibe durante este proceso durante un período especificado en los datos devueltos. Este intervalo de tiempo se denomina *período de vida* (TTL, *Time to Live*) y se especifica en segundos. El administrador del servidor para la zona principal que contiene los datos decide el TTL para los datos. Los valores de TTL menores ayudan a asegurar que la información acerca del dominio es más coherente en la red, en caso que estos datos cambien a menudo. No obstante, un período de vida menor incrementa la carga en los servidores de nombres que contienen el nombre y también incrementa el tráfico de Internet. Puesto que los datos se almacenan en la caché, los cambios efectuados en registros de recursos podrían no estar disponibles inmediatamente en todo Internet.

Una vez que un servidor DNS almacena los datos en la caché, el período de vida empieza a contar de manera que el servidor DNS sabrá cuándo borrarlos de su caché. Cuando el servidor DNS responde a una solicitud con sus datos almacenados en la caché, incluye el período de vida restante para los datos. El servicio de resolución almacena estos datos en la caché y utiliza el TTL que envía el servidor.

Almacenamiento en caché de referencias no encontradas

Además de almacenar en la caché las respuestas positivas a consultas (que contienen información de registro de recursos en la respuesta) de servidores DNS, el servicio Cliente DNS también almacena en caché las respuestas negativas a las consultas. Un respuesta negativa se genera cuando no existe un registro de recursos para el nombre consultado.

El almacenamiento en caché de referencias no encontradas (o de respuestas negativas) impide la repetición de solicitudes adicionales para nombres que no existen. Cualquier información de solicitud que se almacene en la caché e indique que la referencia no se ha encontrado se guarda durante un período más breve que las respuestas positivas a las solicitudes: de manera predeterminada, no más de cinco minutos. El valor de cinco minutos limita el almacenamiento en caché continuado de respuestas negativas con información antigua si los registros pasan a estar disponibles más tarde.

Servidores sólo obtener

Aunque todos los servidores de nombres DNS almacenan en la caché las consultas que han resuelto, los servidores sólo obtener son servidores de nombres DNS cuya única tarea es realizar consultas, almacenar las respuestas en la caché y devolver los resultados. No están autorizados para ningún dominio y sólo contienen información que han almacenado en la caché mientras resolvían solicitudes. Los servidores sólo obtener no tienen zonas principales o secundarias.

Un servidor DNS que ejecute Windows Server 2003 en su configuración de instalación inicial no tiene ninguna zona. Con la ayuda de sugerencias de raíz, se convierte en un servidor sólo obtener en su estado inicial.

Almacenamiento en la caché de resolución del cliente DNS

El solucionador de cliente DNS también almacena en caché la información de las asignaciones resueltas de hosts a direcciones IP. El cliente DNS revisa primero la caché local antes de entrar en contacto con el servidor DNS. Los clientes DNS también pueden realizar almacenamiento en caché de respuestas negativas o referencias no encontradas.

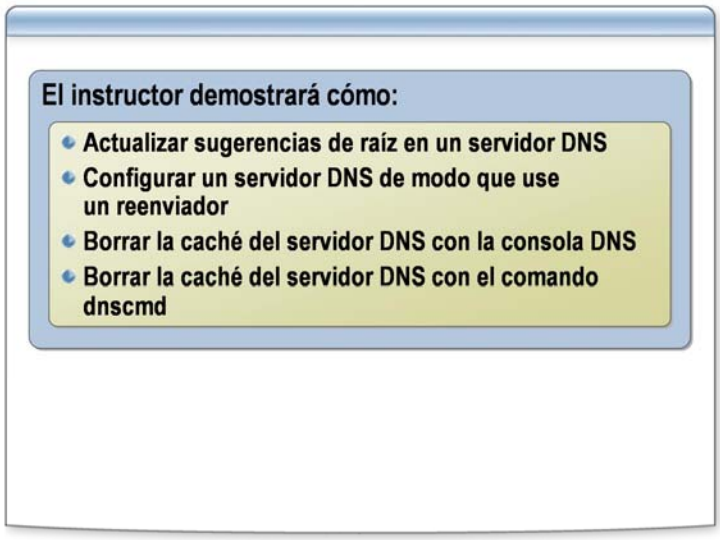
Nota Para obtener más información acerca del solucionador de cliente DNS, consulte el módulo 4, “Resolución de nombres”, en el curso 2184A, *Implementación, administración y mantenimiento de infraestructuras de redes en Microsoft Windows Server™ 2003: Servicios de red*.

Ejemplo

En la ilustración, se muestra que la primera vez que Client1 envía una solicitud para clientA.contoso.msft, el servidor DNS debe utilizar consultas iterativas para localizar el recurso. Cuando se envía la respuesta autorizada al servidor DNS local, éste almacena en la caché el recurso con el valor del período de vida. (El período de vida lo proporciona el servidor DNS autorizado que proporciona la respuesta.) El cliente DNS almacena también en la caché el registro de la caché de su solucionador DNS local mediante el período de vida que proporciona el servidor DNS.

Cuando Client2 emite una consulta a clientA.contoso.msft.com, el servidor DNS puede responder desde la respuesta almacenada en la caché para este recurso, siempre que los datos sigan estando allí. Esto quiere decir que el servidor DNS puede responder con más rapidez a la consulta, puesto que el servidor DNS no tiene que consultar servidores DNS fuera de la organización. De esta manera se elimina el tráfico de red que tendría que generarse para resolver la consulta si no hubiera estado en la caché.

Cómo configurar propiedades para el servicio Servidor DNS



Introducción

Para configurar propiedades para el servicio Servidor DNS, es necesario actualizar las sugerencias de raíz en un servidor DNS. Las sugerencias de raíz determinan si los servidores tienen acceso al servidor raíz a través de Internet o de un servidor raíz interno.

También se puede configurar un servidor DNS para utilizar un reenviador además de actualizar la caché de DNS.

Nota Es recomendable que inicie sesión con una cuenta que no tenga credenciales administrativas y que ejecute el comando **Ejecutar como** con una cuenta de usuario que disponga de las credenciales administrativas apropiadas para realizar esta tarea.

Procedimiento para actualizar sugerencias de raíz en un servidor DNS

Para actualizar sugerencias de raíz en un servidor DNS:

1. Abra la consola DNS.
2. En la consola DNS, seleccione el servidor correspondiente.
3. En el menú **Acción**, haga clic en **Propiedades**.
4. En la ficha **Sugerencias de raíz**, puede hacer clic en:
   - **Agregar** para agregar un servidor de nombres. Escriba el nombre de dominio completo y la dirección IP del servidor de nombres.
   - **Modificar** para modificar un servidor de nombres. Modifique el nombre de dominio completo o dirección IP del servidor de nombres.
   - **Quitar** para quitar un servidor de nombres.
   - **Copiar desde servidor** para copiar la lista de servidores de nombres desde un servidor DNS.
5. Haga clic en **Aceptar** para cerrar el cuadro de diálogo **Propiedades** y, a continuación, cierre la consola DNS.

Procedimiento para configurar un servidor DNS de modo que use un reenviador

Para configurar un servidor DNS de modo que utilice un reenviador:

1. Abra la consola DNS.
2. En la consola DNS, seleccione el servidor correspondiente.
3. En el menú **Acción**, haga clic en **Propiedades**.
4. En la ficha **Reenviadores**, haga clic en **Nuevo**.
5. En el cuadro de diálogo **Reenviador nuevo**, escriba el nombre del dominio DNS que al que el servidor DNS enviará las consultas y, después, haga clic en **Aceptar**.
6. En la ficha **Reenviadores**, en el campo **Lista de direcciones IP del reenviador del dominio seleccionado**, escriba la dirección IP del servidor DNS que actuará como reenviador para consultas del dominio DNS del servidor y, después, haga clic en **Agregar**.
7. En la ficha **Reenviadores**, en el cuadro **Segundos transcurridos hasta agotarse el tiempo de espera de envío de consultas**, escriba el valor en segundos.
8. Si es necesario, en la ficha **Reenviadores**, seleccione la opción **No usar recursividad para este dominio** y, después, haga clic en **Aceptar**.
9. Cierre la consola DNS.

Procedimiento para borrar la caché del servidor DNS con la consola DNS

Para borrar la caché del servidor DNS con la consola DNS:

1. Abra la consola DNS.
2. En la consola DNS, seleccione el servidor.
3. En el menú **Acción**, haga clic en **Borrar caché**.

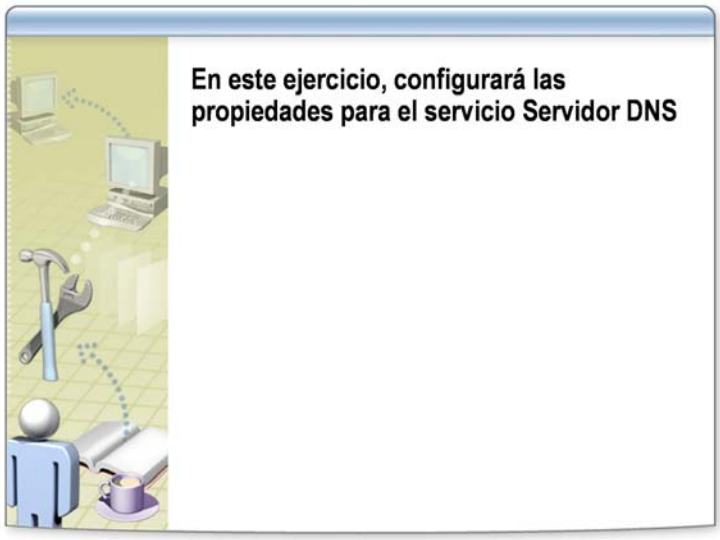
Procedimiento para borrar la caché del servidor DNS con la línea de comandos

Para borrar la caché del servidor DNS con el comando **dnscmd**:

1. En el servidor DNS, instale Herramientas de soporte técnico del CD de Windows 2003 Server.
2. En el servidor DNS, en el símbolo del sistema, escriba **dnscmd** *NombreDeServidor* **/clearcache** (donde *NombreDeServidor* es el nombre del servidor DNS).

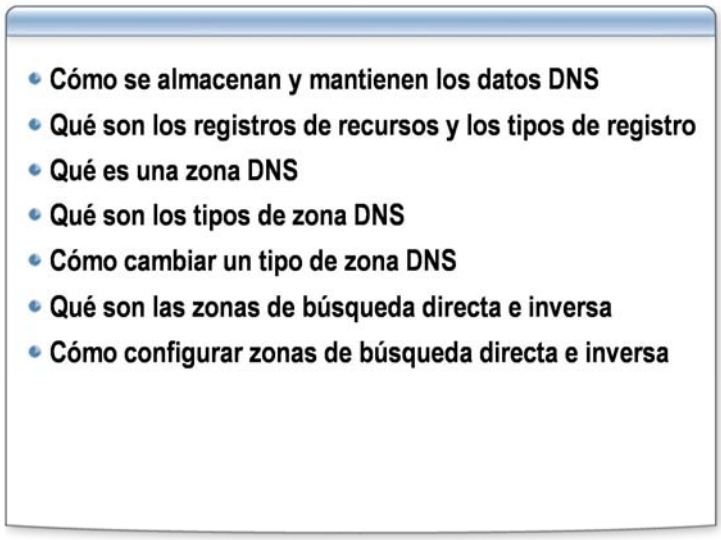
Nota El comando **dnscmd** se explicará en el módulo 6, “Administrar y supervisar el Sistema de nombres de dominio (DNS)”.

Ejercicio: Configurar las propiedades del servicio Servidor DNS



Objetivo	En este ejercicio, configurará las propiedades para el servicio Servidor DNS.
Instrucciones	Para completar este ejercicio, consulte el documento *Valores del plan de implementación*, incluido en el apéndice al final del cuaderno de trabajo. Debe haber iniciado sesión con una cuenta que no tenga credenciales administrativas y ejecutar el comando **Ejecutar como** con una cuenta de usuario que disponga de las credenciales administrativas apropiadas para realizar la tarea.
Situación de ejemplo	La compañía está preocupada por la cantidad de tráfico DNS que se envía a través de Internet. Para reducir al mínimo el tráfico DNS, ha decidido limitar el número de servidores DNS que pueden enviar tráfico DNS fuera. Ha configurado un servidor DNS específico para enviar consultas DNS fuera a Internet. Para permitir que los servidores DNS restantes resuelvan consultas DNS de Internet, va a configurarlos de modo que usen este servidor DNS como reenviador. Configurará su servidor DNS para reenviar consultas DNS al servidor DNS que actúa como reenviador.
Ejercicio	**Configurar un servidor DNS para utilizar un reenviador** ■ Complete esta tarea desde los equipos de ambos alumnos ■ Nombre de usuario: **nwtraders***NombreDeEquipo***Admin** ■ Contraseña: **P@ssw0rd** ■ Dominio DNS: dejar valores predeterminados ■ Dirección IP del reenviador: **192.168.***x***.200** ■ No utilizar recursividad para este dominio: habilitar

Lección: Configurar zonas DNS



Introducción

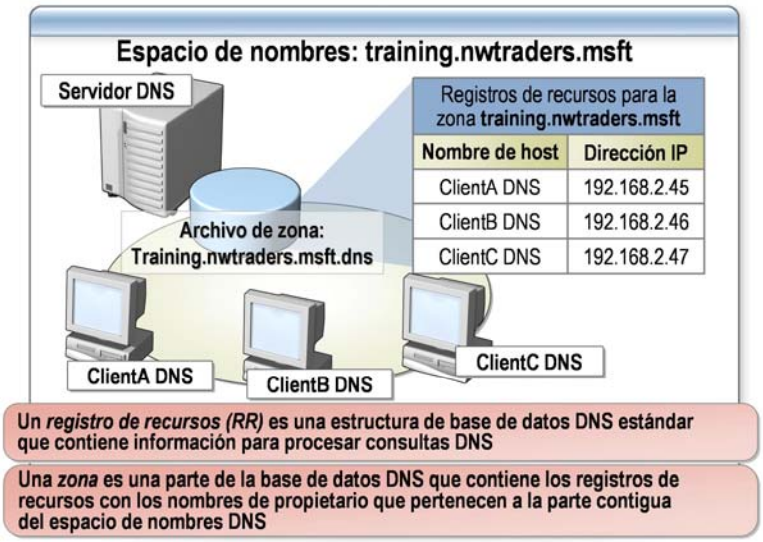
Una vez creadas las zonas DNS, y cuando contengan registros de recursos, el servicio DNS podrá permitir la resolución de nombres de host.

Objetivos de la lección

Después de finalizar esta lección, será capaz de:

- Describir cómo se almacenan y mantienen los datos DNS.
- Explicar qué son los registros de recursos y los tipos de registro.
- Explicar qué es una zona DNS.
- Explicar qué son los tipos de zona DNS.
- Cambiar un tipo de zona DNS.
- Explicar qué son las zonas de búsqueda directa e inversa.
- Configurar zonas de búsqueda directa e inversa.

Cómo se almacenan y mantienen los datos DNS



Definiciones

Un *registro de recursos (RR)* es una estructura de base de datos DNS estándar que contiene información para procesar consultas DNS.

Una *zona* es una parte de la base de datos DNS que contiene los registros de recursos con los nombres de propietario que pertenecen a la parte contigua del espacio de nombres DNS.

Un *archivo de zona* es el archivo del disco duro local del servidor DNS que contiene toda la información de configuración para una zona y los registros de recursos contenidos en ella.

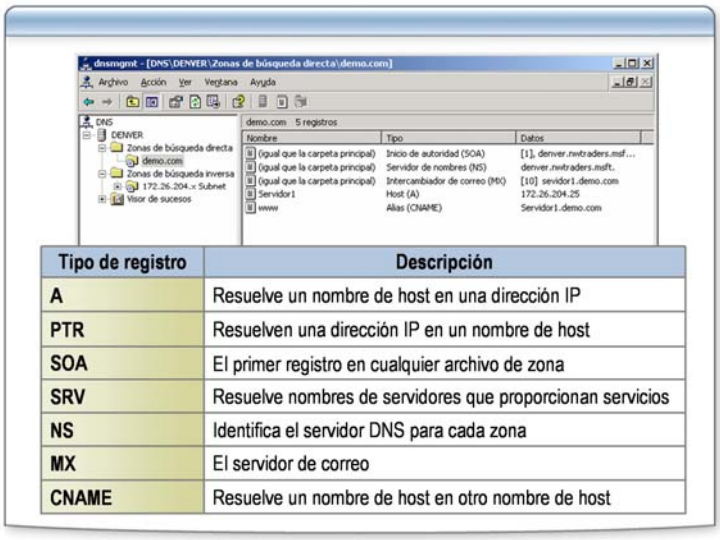
Proceso

Una vez instalado el servicio Servidor DNS y configuradas las propiedades del servicio DNS, ya se puede completar el servicio DNS mediante la adición de asignaciones entre nombres de host y direcciones IP. Estas asignaciones se denominan *registros de recursos* en DNS. Hay muchos tipos diferentes de registros de recursos. Los tipos de registros de recursos que se creen en DNS dependerán de las necesidades de DNS.

Para agregar registros de recursos, es necesario disponer de una estructura en DNS que pueda albergarlos. Estos contenedores lógicos se denominan *zonas* en DNS. Cuando se crea una zona, se crea un archivo de zona para almacenar las propiedades de zona y registros de recursos. Hay varias configuraciones diferentes de zonas en DNS y las zonas que se crearán vienen dictadas por las necesidades de DNS en el entorno.

Una vez creadas las zonas DNS y cuando contengan registros de recursos, el servicio DNS podrá realizar la resolución de nombres de host.

Qué son los registros de recursos y los tipos de registro



Tipo de registro	Descripción
A	Resuelve un nombre de host en una dirección IP
PTR	Resuelven una dirección IP en un nombre de host
SOA	El primer registro en cualquier archivo de zona
SRV	Resuelve nombres de servidores que proporcionan servicios
NS	Identifica el servidor DNS para cada zona
MX	El servidor de correo
CNAME	Resuelve un nombre de host en otro nombre de host

Finalidad de los registros de recursos

Los usuarios pueden tener acceso a registros de recursos DNS por sí mismos o bien pueden hacer que componentes de la red tengan acceso a los registros por ellos. Los siguientes son ejemplos de cuándo se utilizan registros de recursos DNS:

- Un usuario que busca un sitio Web envía una consulta de búsqueda directa a un servidor DNS.
- Cuando un usuario inicia sesión en un equipo de un dominio, el proceso de inicio de sesión localiza un controlador de dominio consultando a un servidor DNS.

Tipos de recurso

Diferentes tipos de registro representan diferentes tipos de datos almacenados dentro de la base de datos DNS. Las tablas siguientes muestran tipos de registro, junto con una descripción y un ejemplo para cada tipo.

Tipo de registro	Descripción	Ejemplo
Host (A)	• Un registro A representa un equipo o dispositivo en la red. • Los registros A son los más comunes y los registros DNS que se utilizan con más frecuencia. • Un registro A resuelve un nombre de host en una dirección IP.	Computer5.microsoft.com se resuelve como 10.1.1.5
Puntero (PTR)	• Un registro PTR se utiliza para buscar el nombre DNS que corresponde a una dirección IP. • El registro PTR se encuentra sólo en la zona de búsqueda inversa. • Los registros PTR resuelven una dirección IP en un nombre de host.	10.1.1.101 se resuelve como Computer1.microsoft.com

(*continuación*)

Tipo de registro	Descripción	Ejemplo
Inicio de autoridad (SOA)	• Un registro de recursos SOA es el primero en cualquier archivo de zona. • Identifica el servidor de nombres DNS principal de la zona. • Identifica la dirección de correo electrónico del administrador responsable de la zona. • Un registro de recursos SOA especifica la información necesaria para la replicación (como el número de serie, el intervalo de actualización, el intervalo de reintento y los valores de caducidad de la zona). • Un registro de recursos SOA resuelve un nombre de dominio (que es el mismo que la carpeta primaria) en un nombre de host.	microsoft.com se resuelve como NS1.microsoft.com
Registro de servicio (SRV)	• Un registro de recursos SRV indica un servicio de red que ofrece un host. • Un registro de recursos SRV resuelve un nombre de servicio en un nombre de host y puerto.	_TCP._LDAP.microsoft.com se resuelve como DC01.microsoft.com
Servidor de nombres (NS)	• Un registro NS facilita la delegación mediante la identificación de servidores DNS para cada zona. • Un registro NS aparece en todas las zonas de búsqueda directa e inversa. • Siempre que un servidor DNS necesite enviar una consulta a un dominio delegado, hace referencia al registro de recursos NS para servidores DNS en la zona de destino. • Un registro NS resuelve un nombre de dominio (que es el mismo que la carpeta primaria) en un nombre de host.	microsoft.com se resuelve como NS2.microsoft.com
Intercambiador de correo (MX)	• Un registro de recursos MX indica la presencia de un servidor de correo electrónico del Protocolo de transferencia de correo (SMTP). • Un registro de recursos MX resuelve un nombre como nombre de host.	Microsoft.com se resuelve como mail.microsoft.com
Alias (CNAME)	• Un registro de recursos CNAME es un nombre de host que hace referencia a otro nombre de host. • Un registro de recursos CNAME resuelve un nombre de host en otro nombre de host.	www.microsoft.com se resuelve como webserver12.microsoft.com

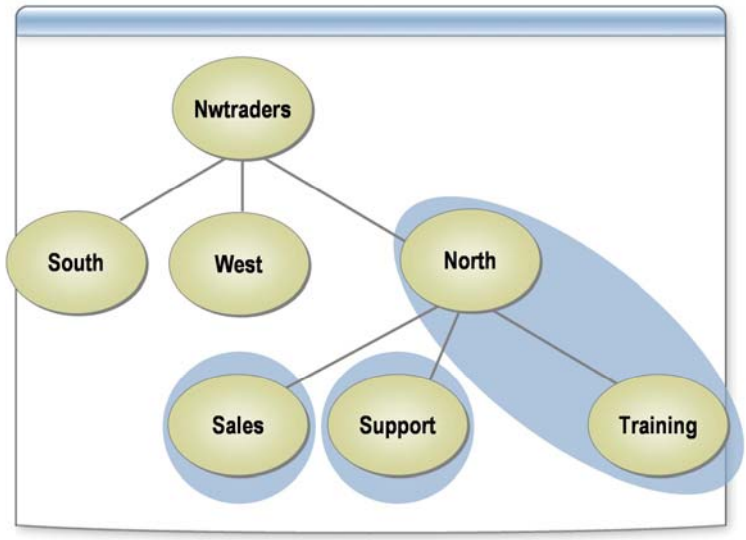
Ejemplos de registros de recursos y tipos de registro

La diapositiva muestra una vista del complemento Administrador de DNS en Microsoft Management Console (MMC), que muestra los registros de recursos y tipos de recursos de la zona Demo.com.

Ejemplo de un conjunto de registros de recursos

Por ejemplo, un cliente DNS podría consultar al servidor SMTP en nwtraders.msft. El conjunto de registros de recursos proporcionaría el registro MX que apunta a smtp.nwtraders.msft y el registro A, que asigna a smtp.nwtraders.msft la dirección IP 192.168.1.17.

Qué es una zona DNS



Finalidad de una zona DNS

Una zona puede albergar los registros de recursos para un dominio o los registros de recursos para varios dominios. Una zona puede alojar más de un dominio sólo si los dominios son contiguos; es decir, están conectados mediante una relación primario-secundario directa.

Una zona es también el representante físico de un dominio o dominios DNS. Por ejemplo, si tiene un espacio de nombres de dominio DNS de south.nwtraders.com, podría crear una zona en un servidor DNS denominado south.nwtraders.com y esta zona podría contener todos los registros de recursos encontrados en el dominio Training

Zona DNS

DNS permite que un espacio de nombres DNS se divida en zonas. Para cada nombre de dominio DNS incluido en una zona, la zona se convierte en la fuente autorizada de información acerca de dicho dominio.

Los archivos de zona se mantienen en servidores DNS. Un único servidor DNS se puede configurar para alojar ninguna, una o varias zonas. Cada zona puede estar autorizada para un dominio DNS o para más de uno siempre que sean contiguos en el árbol DNS. Las zonas pueden almacenarse en archivos de texto sin formato o en la base de datos de Active Directory.

Entre las características de una zona se incluyen las siguientes:

- Una zona es un conjunto de asignaciones entre nombres de host y direcciones IP para los hosts en una parte contigua del espacio de nombres DNS.
- Los datos de zona se mantienen en un servidor DNS y se almacenan de una de las dos maneras siguientes:
  - Como archivo de zona sin formato que contiene listas de asignaciones
  - En una base de datos de Active Directory
- Un servidor DNS está autorizado para una zona si aloja los registros de recursos para los nombres y las direcciones que los clientes solicitan en el archivo de zona.

Una zona DNS es:

- Un tipo de zona principal, secundaria o de código auxiliar.
- Una zona de búsqueda directa o inversa.

Nota Los tipos de zona y zonas de búsqueda se explican con detalle más adelante en esta lección.

Proteger una zona DNS

Para incrementar la seguridad, puede controlar quién administra zonas DNS si modifica la lista de control de acceso discrecional (DACL, *Discretionary Access Control List*) en las zonas DNS que están almacenadas en Active Directory. La DACL permite controlar los permisos para usuarios y grupos de Active Directory que puedan controlar las zonas DNS.

Nota Para obtener más información acerca de cómo proteger una zona DNS, consulte la sección acerca de cómo proteger zonas DNS en la documentación de Ayuda de Windows Server 2003.

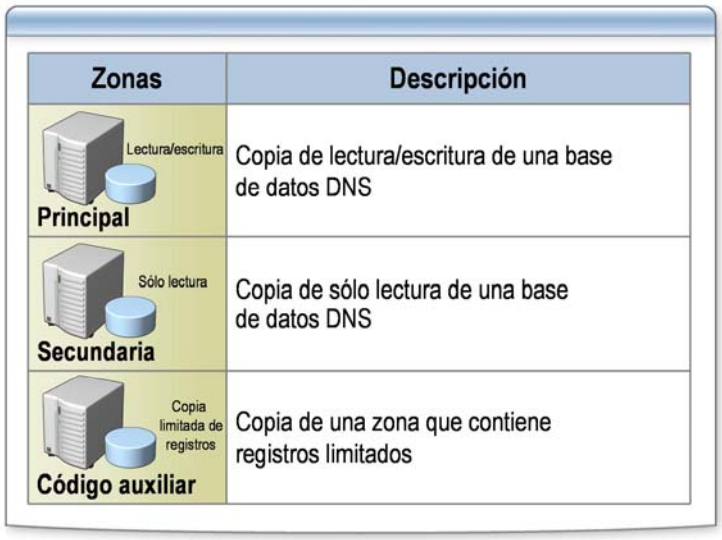
Ejemplo

En la ilustración hay tres zonas representadas:

- north.nwtraders.com
- sales.north.nwtraders.com
- support.north.nwtraders.com

La primera zona (north.nwtraders.com) está autorizada para dos dominios contiguos (north.nwtraders.com y training.north.nwtraders.com), mientras que cada una de las otras dos zonas (sales.north.nwtraders.com y support.north.nwtraders.com) representan un único dominio.

Qué son los tipos de zona DNS



Introducción

Al configurar un servidor DNS, puede configurarlo con varios tipos de zona o con ninguna, según el tipo de función que el servidor DNS desempeñe en la red.

Hay numerosas opciones para realizar la una configuración óptima del servidor DNS, basadas en decisiones tomadas según, por ejemplo, la topología de red y el tamaño del espacio de nombres. La operación normal del servidor DNS implica tres zonas:

- Zona principal
- Zona secundaria
- Zona de código auxiliar

Finalidad de los tipos de zona DNS

Mediante el uso de zonas diferentes, puede configurar la solución DNS para ajustarse mejor a sus necesidades. Por ejemplo, se recomienda configurar una zona principal y una zona secundaria en servidores DNS independientes, para proporcionar tolerancia a errores en caso de que un servidor falle. Si la zona se mantiene en un servidor DNS independiente, se puede configurar una zona de código auxiliar.

Zona principal

Una zona principal es la copia autorizada de la zona DNS, donde se crean y administran registros de recursos.

Al configurar servidores DNS con el fin de alojar zonas para un dominio, el servidor principal suele estar ubicado donde sea accesible para administrar el archivo de zona.

Zona secundaria

Una zona secundaria es una copia de la zona DNS que contiene la copia de sólo lectura de la zona DNS. Los registros de la zona secundaria no pueden modificarse; los administradores sólo pueden modificar registros de la zona DNS principal.

Normalmente, se configura al menos un servidor secundario con tolerancia a errores. No obstante, se podrían configurar varios servidores secundarios en otras ubicaciones para que los registros de la zona pudieran resolverse sin que la solicitud cruzara vínculos WAN.

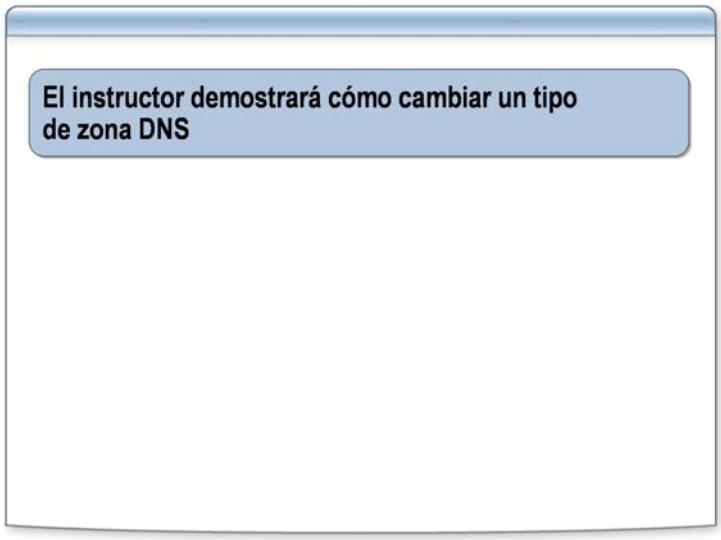
Zona de código auxiliar

Las zonas de código auxiliar son copias de una zona que contienen sólo los registros de recursos necesarios para identificar el servidor DNS autorizado para dicha zona. Una zona de código auxiliar contiene un subconjunto de datos de zona que consta de un registro SOA, NS y A, también conocido como registro de adherencia. Una zona de código auxiliar es como un marcador que simplemente apunta al servidor DNS que está autorizado para dicha zona.

Las zonas de código auxiliar pueden utilizarse donde las sugerencias de raíz apuntan a un servidor DNS interno, en lugar de a servidores raíz en Internet. Por razones de seguridad, el servidor DNS está diseñado sólo para resolver ciertas zonas.

Nota Los servidores sólo obtener no tienen zona.

Cómo cambiar un tipo de zona DNS



Introducción

Para configurar una zona DNS, puede ser necesario cambiar un tipo de zona DNS.

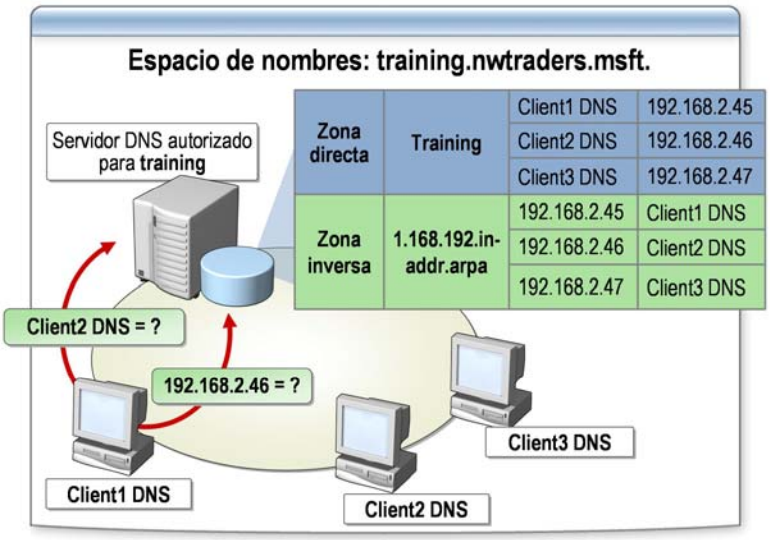
Nota Es recomendable que inicie sesión con una cuenta que no tenga credenciales administrativas y que ejecute el comando **Ejecutar como** con una cuenta de usuario que disponga de las credenciales administrativas apropiadas para realizar esta tarea.

Procedimiento

Para cambiar un tipo de zona DNS:

1. Abra la consola DNS.
2. En la consola **DNS**, seleccione la zona que desee cambiar.
3. En el menú **Acción**, haga clic en **Propiedades**.
4. En la ficha **General**, haga clic en **Cambiar**.
5. En el cuadro de diálogo **Cambiar tipo de zona**, seleccione una de las opciones siguientes y, después, haga clic en **Aceptar**:
   - **Zona principal**, si esta zona contendrá una copia de la zona que se puede actualizar directamente.
   - **Zona secundaria**, si esta zona almacena una copia de una zona existente.
   - **Zona de código auxiliar**, si esta zona almacena una copia de una zona que contiene sólo registros NS (servidor de nombres), SOA (inicio de autoridad) y, posiblemente, de adherencia.
6. En el cuadro de diálogo **Propiedades**, haga clic en **Aceptar**.

Qué son las zonas de búsqueda directa e inversa



Introducción

Una vez que haya decidido si la zona es de tipo principal, secundario o de código auxiliar, debe decidir en qué tipo de zona de búsqueda se almacenarán los registros de recursos, que pueden almacenarse en zonas de búsqueda directa o en zonas de búsqueda inversa.

Finalidad del reenviador DNS y zonas de búsqueda inversa

Una asignación puede almacenarse como una asignación entre un nombre de host y una dirección IP o a la inversa. Puede elegir el tipo de asignación necesario para una zona, en función de cómo desee que los clientes y servicios consulten registros de recursos.

Zona de búsqueda directa

En DNS, una *búsqueda directa* es un proceso de consulta en el que se busca el nombre para mostrar del dominio DNS de un equipo host para encontrar su dirección IP.

En el Administrador de DNS, las *zonas de búsqueda directa* se basan en los nombres de dominio DNS y suelen alojar registros de recursos de dirección de host (A).

Zona de búsqueda inversa

En DNS, una *búsqueda inversa* es un proceso de consulta mediante el cual se busca la dirección IP de un equipo host para encontrar su nombre para mostrar en el dominio DNS.

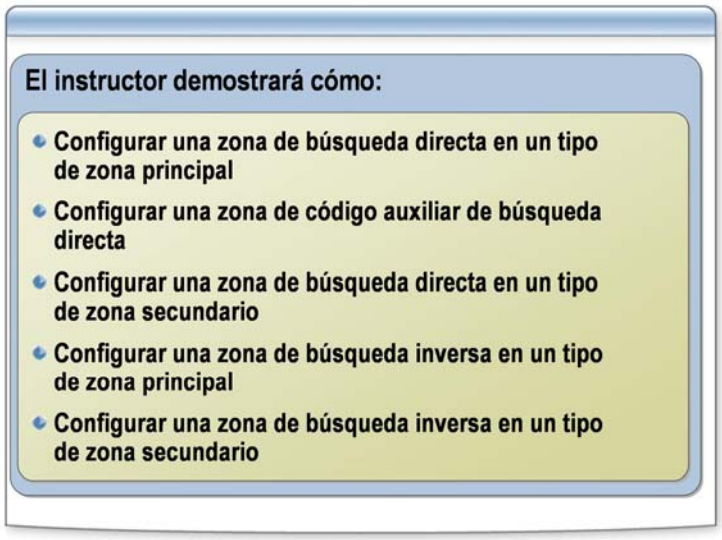
En el Administrador de DNS, las *zonas de búsqueda inversa* se basan en su nombre de dominio in-addr.arpa y suelen albergar registros de recursos de puntero (PTR).

Ejemplo

Client1 envía una consulta para la dirección IP del nombre client2.training.nwtraders.msft. El servidor DNS busca en su zona de búsqueda directa (training.nwtraders.msft) la dirección IP asociada con el nombre de host y devuelve la dirección IP a Client1.

Client1 envía una consulta para el nombre de host de la dirección IP 192.168.2.46. El servidor DNS busca en su zona de búsqueda inversa (1.168.192.in-addr.arpa) el nombre de host asociado con la dirección IP y lo devuelve a Client1.

Cómo configurar zonas de búsqueda directa e inversa



Introducción

Puede configurar una zona de búsqueda directa o una zona de búsqueda inversa en un tipo de zona principal o secundario. También puede configurar una zona de código auxiliar.

Procedimiento para configurar una zona de búsqueda directa en un tipo de zona principal

Para configurar una zona de búsqueda directa en un tipo de zona principal:

1. Abra la consola DNS.
2. En la consola DNS, haga clic con el botón secundario del *mouse* en el servidor DNS y, después, haga clic en **Zona nueva**.
3. En la página **Asistente para crear zona nueva**, haga clic en **Siguiente**.
4. En la página **Tipo de zona**, compruebe que la opción **Zona principal** está seleccionada y, a continuación, haga clic en **Siguiente**.
5. En la página **Zona de búsqueda directa o inversa**, compruebe que la opción **Zona de búsqueda directa** está seleccionada y, a continuación, haga clic en **Siguiente**.
6. En la página **Nombre de zona**, escriba el nombre DNS de la zona para la que este servidor estará autorizado y, después, haga clic en **Siguiente**.
7. En la página **Archivo de zona**, haga clic en **Siguiente** para aceptar los valores predeterminados.

8. En la página **Actualización dinámica**, seleccione una de las opciones siguientes y haga clic en **Siguiente**.
   a. **Permitir sólo actualizaciones dinámicas seguras (recomendado para Active Directory).** Esta opción está sólo disponible para zonas integradas en Active Directory.
   b. **Permitir todas las actualizaciones dinámicas (seguras y no seguras).** No se recomienda esta opción, puesto que se pueden aceptar actualizaciones que no sean de orígenes de confianza.
   c. **No admitir actualizaciones dinámicas.** Esta opción requiere que actualice manualmente los registros.
9. Una vez completada la página **Asistente para crear zona nueva**, haga clic en **Finalizar**.
10. Cierre la consola DNS.

Procedimiento para configurar una zona de código auxiliar de búsqueda directa

Para configurar una zona de código auxiliar de búsqueda directa:

1. Abra la consola DNS.
2. En la consola DNS, haga clic con el botón secundario del *mouse* en el servidor DNS y, después, haga clic en **Zona nueva**.
3. En la página **Asistente para crear zona nueva**, haga clic en **Siguiente**.
4. En la página **Tipo de zona**, seleccione **Zona de código auxiliar** y, a continuación, haga clic en **Siguiente**.
5. En la página **Zona de búsqueda directa o inversa**, seleccione **Zona de búsqueda directa** y, a continuación, haga clic en **Siguiente**.
6. En la página **Nombre de zona**, escriba el nombre DNS de la zona para la que este servidor estará autorizado y, después, haga clic en **Siguiente**.
7. En la página **Archivo de zona**, haga clic en **Siguiente** para aceptar los valores predeterminados.
8. En la página **Servidores maestros DNS**, en el campo **Dirección IP**, escriba la dirección IP del servidor DNS desde el que este servidor DNS copiará la zona. Haga clic en **Agregar** y, a continuación, en **Siguiente**.
9. En la página **Finalización del Asistente para crear zona nueva**, haga clic en **Finalizar**.
10. Cierre la consola DNS.

Procedimiento para configurar una zona de búsqueda directa en un tipo de zona secundario

Para configurar una zona de búsqueda directa en un tipo de zona secundario:

1. Abra la consola DNS.
2. En la consola DNS, haga clic con el botón secundario del *mouse* en el servidor DNS y, después, haga clic en **Zona nueva**.
3. En la página **Asistente para crear zona nueva**, haga clic en **Siguiente**.
4. En la página **Tipo de zona**, seleccione **Zona secundaria** y, a continuación, haga clic en **Siguiente**.
5. En la página **Zona de búsqueda directa o inversa**, compruebe que la opción **Zona de búsqueda directa** está seleccionada y, a continuación, haga clic en **Siguiente**.
6. En la página **Nombre de zona**, escriba el espacio de nombres DNS y haga clic en **Siguiente**.
7. En la página **Servidores maestros DNS**, en el campo **Dirección IP**, escriba la dirección IP del servidor DNS maestro, haga clic en **Agregar** y, después, haga clic en **Siguiente**.
8. En la página **Finalización del Asistente para crear zona nueva**, haga clic en **Finalizar**.
9. Cierre la consola DNS.

Procedimiento para configurar una zona de búsqueda inversa en un tipo de zona principal

Para configurar una zona de búsqueda inversa en un tipo de zona principal:

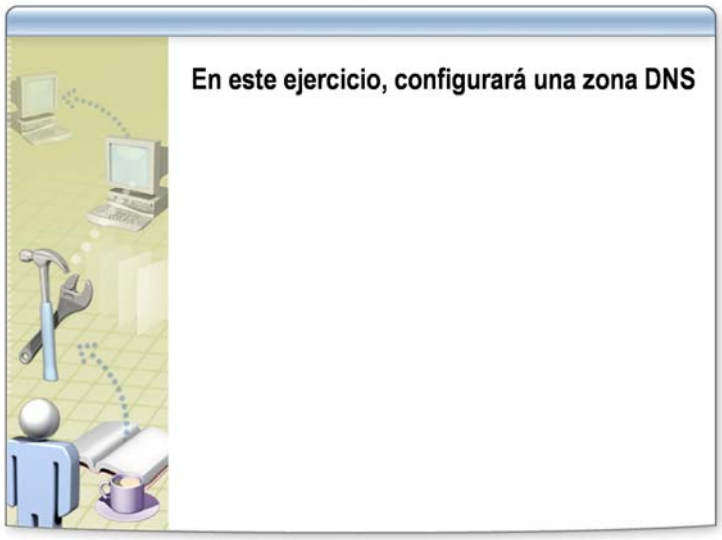
1. Abra la consola DNS.
2. En la consola DNS, haga clic con el botón secundario del *mouse* en el servidor DNS y, después, haga clic en **Zona nueva**.
3. En la página **Asistente para crear zona nueva**, haga clic en **Siguiente**.
4. En la página **Tipo de zona**, compruebe que la opción **Zona principal** está seleccionada y, a continuación, haga clic en **Siguiente**.
5. En la página **Zona de búsqueda directa o inversa**, seleccione **Zona de búsqueda inversa** y, a continuación, haga clic en **Siguiente**.
6. En la página **Nombre de la zona de búsqueda inversa**, en el campo **Id. de red**, escriba la parte del identificador de red de la dirección IP de la zona y, después, haga clic en **Siguiente**.
7. En la página **Archivo de zona**, haga clic en **Siguiente** para aceptar los valores predeterminados.
8. En la página **Actualización dinámica**, seleccione una de las opciones siguientes y haga clic en **Siguiente**.
   a. **Permitir sólo actualizaciones dinámicas seguras (recomendado para Active Directory).**
   b. **Permitir todas las actualizaciones dinámicas (seguras y no seguras).**
   c. **No admitir actualizaciones dinámicas.**
9. En la página **Finalización del Asistente para crear zona nueva**, haga clic en **Finalizar**.
10. Cierre la consola DNS.

Procedimiento para configurar una zona de búsqueda inversa en un tipo de zona secundario

Para configurar una zona de búsqueda inversa en un tipo de zona secundario:

1. Abra la consola DNS.
2. En la consola DNS, haga clic con el botón secundario del *mouse* en el servidor DNS y, después, haga clic en **Zona nueva**.
3. En la página **Asistente para crear zona nueva**, haga clic en **Siguiente**.
4. En la página **Tipo de zona**, seleccione **Zona secundaria** y, a continuación, haga clic en **Siguiente**.
5. En la página **Zona de búsqueda directa o inversa**, seleccione **Zona de búsqueda inversa** y, a continuación, haga clic en **Siguiente**.
6. En la página **Nombre de la zona de búsqueda inversa**, en el campo **Id. de red**, escriba la parte del identificador de red de la dirección IP de la zona y, después, haga clic en **Siguiente**.
7. En la página **Archivo de zona**, haga clic en **Siguiente** para aceptar los valores predeterminados.
8. En la página **Servidores maestros DNS**, en el campo **Dirección IP**, escriba la dirección IP del servidor DNS maestro, haga clic en **Agregar** y, después, haga clic en **Siguiente**.
9. En la página **Finalización del Asistente para crear zona nueva**, haga clic en **Finalizar**.
10. Cierre la consola DNS.

Ejercicio: Configurar zonas DNS



Objetivo	En este ejercicio, configurará una zona DNS.
Instrucciones	Para completar este ejercicio, consulte el documento *Valores del plan de implementación*, incluido en el apéndice al final del cuaderno de trabajo. Debe haber iniciado sesión con una cuenta que no tenga credenciales administrativas y ejecutar el comando **Ejecutar como** con una cuenta de usuario que disponga de las credenciales administrativas apropiadas para realizar la tarea.
Situación de ejemplo	El espacio de nombres de dominio nwtraders.msft ha crecido demasiado. El ingeniero de sistemas ha planeado que cada servidor DNS del departamento de laboratorio mantenga una zona de búsqueda directa y una zona de búsqueda inversa. Tendrá que crear una zona de búsqueda directa principal y una zona de búsqueda inversa principal en el equipo DNS.
Ejercicio	**Configurar una zona de búsqueda directa en un tipo de zona secundario** ■ Complete esta tarea desde los equipos de ambos alumnos ■ Nombre de zona: **nwtraders.msft** ■ Dirección IP del servidor DNS maestro: **192.168.*x*.200** ■ Una vez finalizada la tarea, seleccione esta zona de búsqueda directa secundaria DNS y, en el panel de detalles, examine los registros DNS para comprobar que la zona se ha cargado desde el servidor DNS maestro

Configurar una zona de búsqueda inversa en un tipo de zona secundario

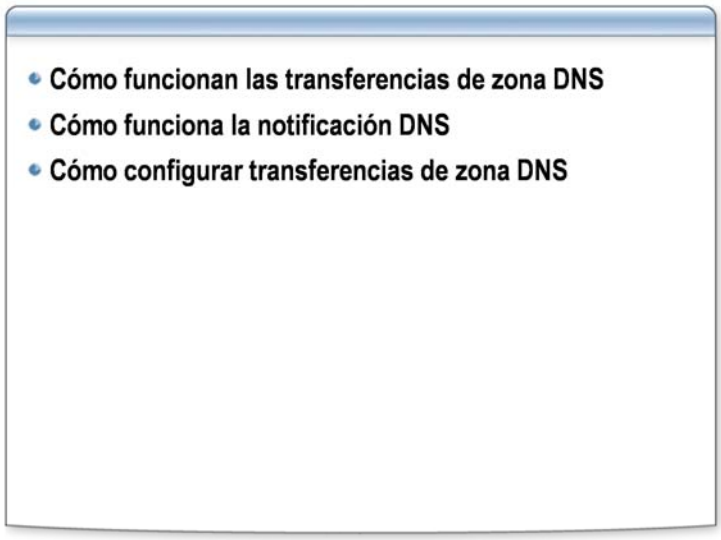
- Complete esta tarea desde los equipos de ambos alumnos
- Nombre de zona: **192.168.***x*
- Dirección IP del servidor DNS maestro: **192.168.***x***.200**
- Una vez finalizada la tarea, seleccione esta zona de búsqueda directa secundaria DNS y, en el panel de detalles, examine los registros DNS para comprobar que la zona se ha cargado desde el servidor DNS maestro.

Configurar una zona de búsqueda directa en un tipo de zona principal

- Complete esta tarea desde los equipos de ambos alumnos
- Nombre de zona: *srv***.nwtraders.msft** (donde *srv* es la etiqueta de tres letras del nombre del equipo)
- Actualización dinámica: **Permitir todas las actualizaciones dinámicas (seguras y seguras)**

Nota A modo de demostración, configurará Actualización dinámica para permitir actualizaciones dinámicas no seguras y seguras. Ésta no es una configuración que se suela recomendar.

Lección: Configurar las transferencias de zona DNS



Introducción

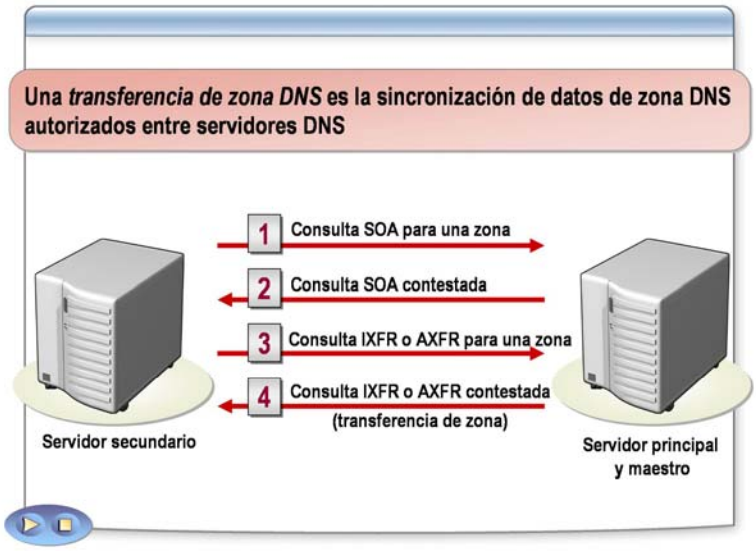
Las transferencias de zona son la transferencia parcial o completa de todos los datos de una zona desde el servidor DNS principal que aloja la zona hasta un servidor DNS secundario que aloja una copia de la zona. Al efectuar cambios en la zona en un servidor DNS principal, éste notifica a los servidores DNS secundarios que estos cambios se han producido y que se replican a todos los servidores DNS secundarios de dicha zona mediante transferencias de zona.

Objetivos de la lección

Después de finalizar esta lección, será capaz de:

- Describir cómo funcionan las transferencias de zona DNS.
- Describir cómo funciona la notificación DNS.
- Configurar transferencias de zona DNS.

Cómo funcionan las transferencias de zona DNS



Introducción

Hay dos tipos de transferencia de zona DNS: una transferencia de zona completa y una transferencia de zona incremental.

Definiciones

Un *servidor DNS principal* es la ubicación administrativa y la copia maestra de una zona. El servidor DNS principal contiene la copia de lectura-escritura de la base de datos de la zona y controla los cambios efectuados a la zona.

Un *servidor secundario* es aquél que mantiene una copia de una zona DNS existente.

Un *servidor maestro* es un servidor DNS que transfiere los cambios de zona a otro servidor DNS. Un servidor maestro puede ser un servidor DNS principal o un servidor DNS secundario, en función de cómo obtenga el servidor sus datos de zona.

Una *transferencia de zona DNS* es la sincronización de datos DNS autorizados entre servidores DNS. Un servidor DNS configurado con una zona secundaria solicita periódicamente a servidores maestros DNS que sincronicen sus datos de zona.

Una *transferencia de zona completa* es el tipo de consulta estándar que todos los servidores DNS admiten para actualizar y sincronizar datos de zona cuando se haya cambiado la zona. Cuando se efectúa una consulta DNS mediante AXFR como tipo de consulta especificado, la zona completa se transfiere como respuesta.

Una *consulta AXFR* es una solicitud para una transferencia de zona completa.

Una *transferencia de zona incremental* es un tipo de consulta alternativa que algunos servidores DNS utilizan para actualizar y sincronizar datos de zona cuando se cambia una zona desde la última actualización. Cuando dos servidores DNS permiten la transferencia de zona incremental, sólo pueden hacer un seguimiento y transferir aquellos cambios de registros de recursos incrementales entre cada versión de la zona.

Una *consulta IXFR* es una solicitud para una transferencia de zona incremental.

Finalidad de una transferencia de zona DNS

La finalidad de la transferencia de zona es asegurar que ambos servidores DNS que alojan la misma zona tienen la misma información de zona. Sin transferencias de zona, los datos del servidor principal serían actuales, pero el servidor DNS secundario no dispondría de información de zona actualizada y, por tanto, no podría realizar la resolución de nombres para dicha zona.

Proceso de transferencia de zona

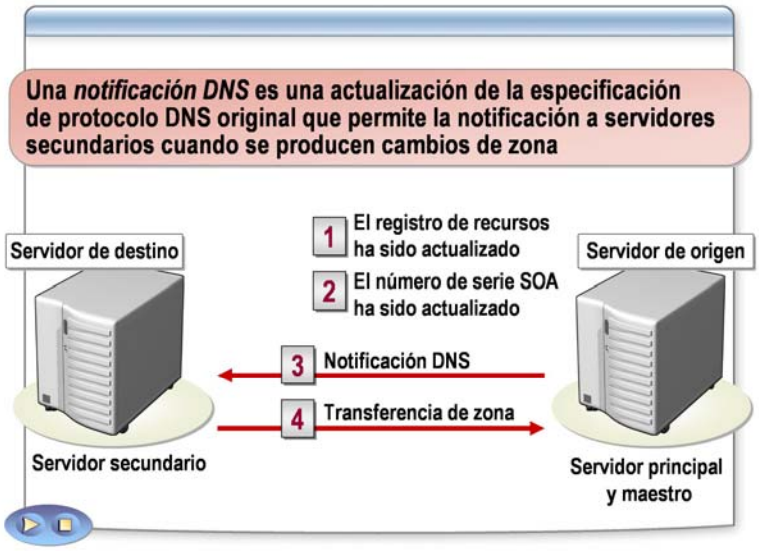
El proceso siguiente indica los pasos para realizar una transferencia de zona completa o incremental.

1. El servidor secundario para la zona espera cierto período (especificado en el campo **Actualizar** del registro de recursos SOA que el servidor secundario consiguió del servidor maestro). A continuación, el servidor secundario solicita al servidor maestro su SOA.
2. El servidor maestro de la zona responde con el registro de recursos SOA.
3. El servidor secundario de la zona compara el número de serie devuelto con su propio número de serie. Si el número de serie que el servidor maestro envía para la zona es superior al suyo propio, su base de datos de zonas no está actualizada. El servidor maestro envía entonces una consulta AXFR para solicitar una transferencia de zona completa. Si el servidor DNS admite transferencias de zona incrementales (como en Windows Server 2003 y Windows 2000), envía una IXFR para solicitar una transferencia de zona incremental, que transfiere registros de recursos que hayan sido modificados desde la última transferencia.
4. Para realizar una transferencia de zona completa, el servidor maestro de la zona envía la base de datos de zonas al servidor secundario; para realizar una transferencia de zonas incremental, sólo envía los datos de zona que hayan cambiado.

Nota Al crear una zona secundaria, el servidor DNS realiza una transferencia de zona completa para llenar la base de datos inicialmente.

Importante De manera predeterminada, el servicio Servidor DNS sólo permite transferir información de zona a servidores que aparezcan en la lista de registros de recursos de servidor de nombres (NS) de una zona. Ésta es una configuración segura. No obstante, para mejorar la seguridad, seleccione la opción para permitir transferencias de zona sólo a direcciones IP especificadas. Si se permiten las transferencias de zona a cualquier servidor podría exponer sus datos DNS a un intruso que intentara ocupar su red.

Cómo funciona la notificación DNS



Definiciones

Una *notificación DNS* es una actualización de la especificación de protocolo DNS original que permite la notificación a servidores secundarios cuando se producen cambios de zona.

Una *lista de notificación* es una lista para la zona de otros servidores DNS a los que debería notificarse cuando se producen cambios de zona. La lista de notificación que el servidor maestro mantiene está formada por direcciones IP para servidores DNS que están configurados como servidores secundarios para la zona. Cuando se notifica a los servidores mostrados un cambio en la zona, éstos iniciarán una transferencia de zona con otro servidor DNS y actualizarán la zona.

Finalidad de la notificación de DNS

Los servidores a los que se les notifica pueden iniciar una transferencia de zona para obtener los cambios de zona de sus servidores maestros y actualizar sus replicados locales de la zona.

Esto es una mejora acerca de los intervalos de tiempo que se establecen en la copia del servidor DNS secundario de la zona. Al utilizar la notificación de DNS, las copias de la zona DNS se actualizan cuando se producen cambios no programados.

La notificación de DNS puede ayudar a mejorar la coherencia de los datos de zona entre servidores secundarios. Por ejemplo, si las transferencias de zona DNS se producen sólo en ciertos momentos, se pueden dar dos situaciones dentro de un período:

- Pueden no haberse producido cambios en una zona DNS.
- Pueden haber pasado varios minutos antes de iniciar una transferencia de zona. La zona puede haber tenido muchos cambios de zona y estos cambios aún no han sido transferidos al servidor DNS secundario.

Con la notificación de DNS, se producen actualizaciones cada vez que se producen cambios.

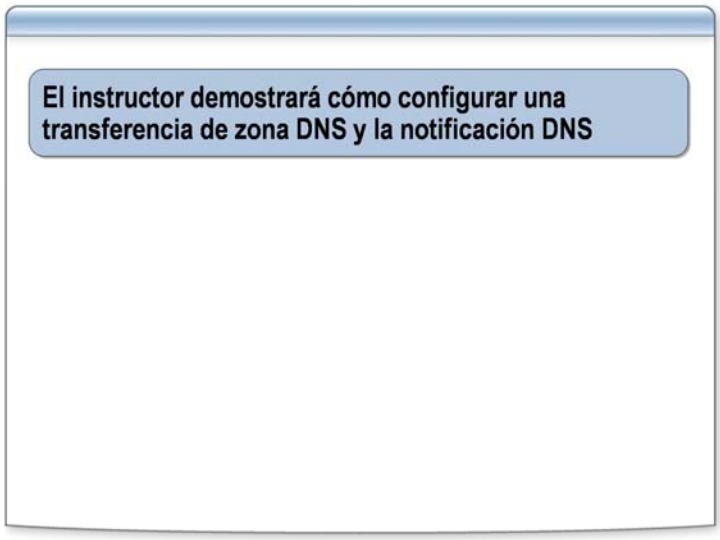
Además, los servidores DNS que ejecutan Windows Server 2003 o Windows 2000 admiten transferencias incrementales, de manera que sólo los datos que se hayan cambiado en el servidor DNS maestro se transfieren al servidor DNS secundario.

Proceso de notificación de DNS

Con la ayuda de la ilustración, los pasos siguientes indican el proceso de notificación de DNS:

1. La zona local de un servidor DNS principal se actualiza.
2. El campo **Número de serie** del registro SOA se actualiza para indicar que una nueva versión de la zona se ha escrito en un disco.
3. El servidor principal envía un mensaje de notificación a todos los demás servidores que forman parte de su lista de notificación.
4. Todos los servidores secundarios de la zona que reciben el mensaje de notificación responden con la iniciación de una consulta tipo SOA al servidor principal de notificación. Esta consulta inicia el proceso de transferencia de zona DNS.

Cómo configurar transferencias de zona DNS



Introducción

Para sincronizar los datos DNS autorizados entre los servidores DNS y actualizar los datos de zona DNS cuando se produzcan cambios no programados, puede configurar una transferencia de zona DNS y una notificación DNS.

Nota Es recomendable que inicie sesión con una cuenta que no tenga credenciales administrativas y que ejecute el comando **Ejecutar como** con una cuenta de usuario que disponga de las credenciales administrativas apropiadas para realizar esta tarea.

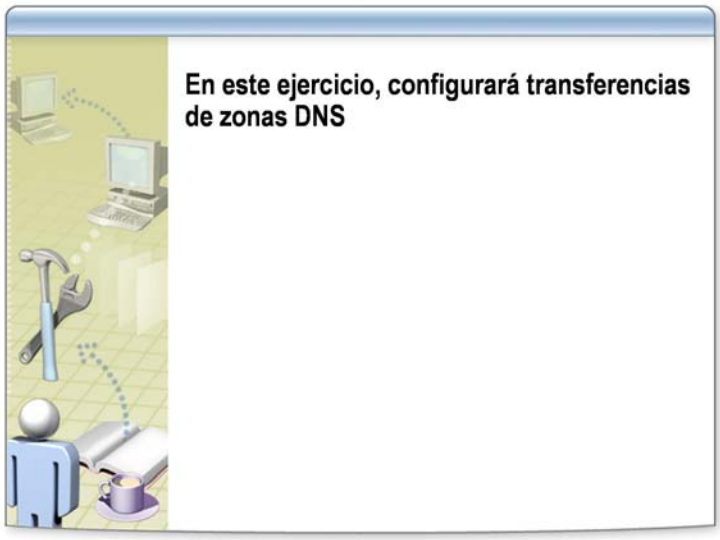
Procedimiento

Para configurar una transferencia de zona DNS y la notificación DNS:

1. Abra la consola DNS.
2. Expanda el servidor correspondiente y, a continuación, expanda **Zonas de búsqueda directa** o **Zonas de búsqueda inversa**.
3. Seleccione la zona DNS apropiada.
4. En el menú **Acción**, haga clic en **Propiedades**.
5. En el cuadro de diálogo **Propiedades** para la zona DNS, en la ficha **Transferencias de zona**, compruebe que está seleccionada la opción **Permitir transferencias de zona**.
6. Seleccione **Sólo a los siguientes servidores**.
7. En el campo **Dirección IP**, escriba la dirección IP del servidor DNS al que se transferirán los datos de zona y haga clic en **Agregar**.

8. En el cuadro de diálogo **Propiedades** para la zona DNS, en la ficha **Transferencias de zona**, haga clic en **Notificar**.
9. En el cuadro de diálogo **Notificar**, haga clic en la opción **Los siguientes servidores**.
10. En el campo **Dirección IP**, escriba la dirección IP del servidor DNS que recibirá la notificación automática y haga clic en **Aceptar**.
11. En la ficha **Propiedades de zona**, haga clic en **Aceptar**.
12. Cierre la consola DNS.

Ejercicio: Configurar las transferencias de zona DNS



Objetivo

En este ejercicio, configurará transferencias de zonas DNS.

Instrucciones

Para completar este ejercicio, consulte el documento *Valores del plan de implementación*, incluido en el apéndice al final del cuaderno de trabajo.

Debe haber iniciado sesión con una cuenta que no tenga credenciales administrativas y ejecutar el comando **Ejecutar como** con una cuenta de usuario que disponga de las credenciales administrativas apropiadas para realizar la tarea.

Situación de ejemplo

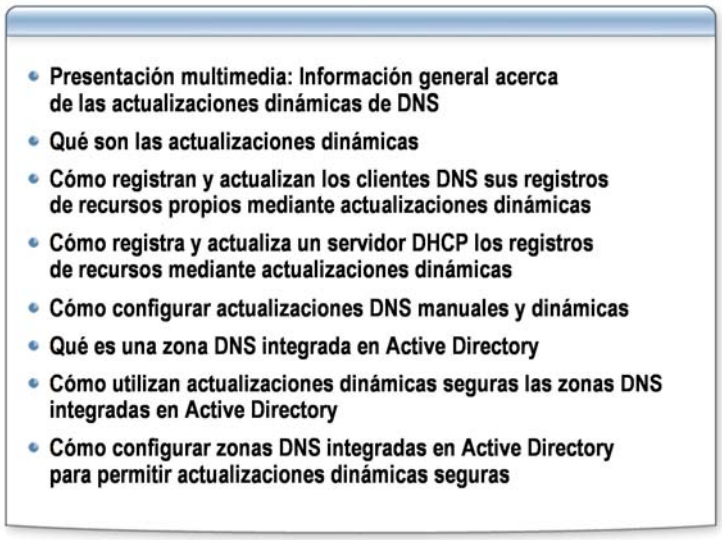
Se ha configurado un nuevo servidor DNS como servidor secundario para el servidor DNS de la práctica. Realizará la configuración de transferencia de zona en la zona DNS de su servidor DNS. A continuación, comprobará que dicha transferencia de zona ha finalizado.

Ejercicio

Configurar la transferencia de zona DNS y la notificación DNS en una zona de búsqueda directa principal

- Complete esta tarea desde los equipos de ambos alumnos
- Zona de búsqueda directa principal: *srv*.**nwtraders.msft** (donde *srv* es la etiqueta de tres letras del nombre del equipo)
- Dirección IP del servidor que solicita la transferencia de zona: **192.168.***x*.**200**
- Dirección IP del servidor al que hay que notificar: **192.168.***x*.**200**

Lección: Configurar las actualizaciones dinámicas DNS



Introducción

Puesto que DNS se utiliza para tener acceso a recursos, es imprescindible que los recursos de DNS estén actualizados. Cuando los registros de recursos DNS no están actualizados se pueden producir errores.

Si un registro de recursos DNS se crea manualmente en DNS, el administrador DNS debe actualizar manualmente el registro de recursos DNS para reflejar los cambios en el recurso cuando la dirección IP del mismo cambie.

Debido al volumen de registros de recursos en DNS, la actualización manual de registros sobrecarga rápidamente las tareas de mantenimiento del administrador DNS. La solución a este problema es crear un método para permitir a los clientes DNS actualizar y mantener sus propios registros de recursos en DNS. Las actualizaciones dinámicas permiten a los clientes DNS actualizar y mantener sus propios registros de recursos en DNS.

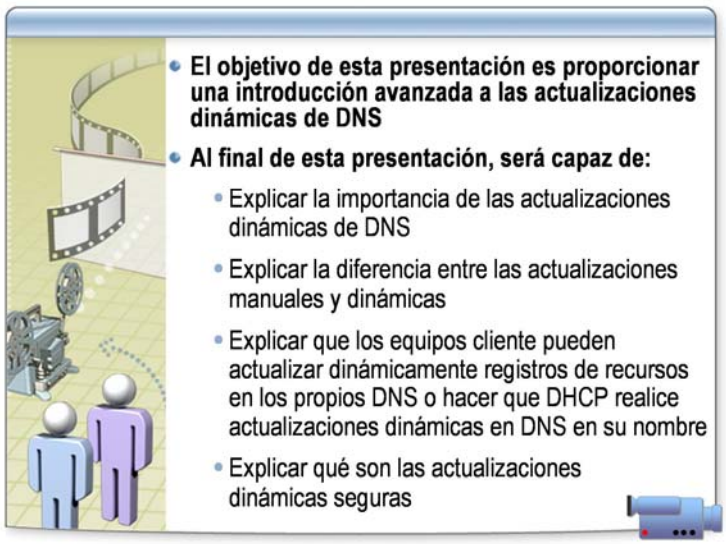
Para permitir que las actualizaciones de DNS se produzcan automáticamente, sin interacción por parte del administrador de DNS, éste debe configurar la zona DNS para permitir actualizaciones dinámicas. Además, los administradores deben configurar los clientes DNS para actualizar registros DNS en DNS o bien configurar el servidor DHCP que usan los clientes DNS para actualizar los registros DNS en su nombre.

Objetivos de la lección

Después de finalizar esta lección, será capaz de:

- Describir cómo funcionan las actualizaciones dinámicas de DNS.
- Explicar qué son las actualizaciones dinámicas.
- Describir cómo registran y actualizan los clientes DNS sus propios registros de recursos mediante la actualización dinámica.
- Describir cómo registra y actualiza un servidor DHCP los registros de recursos mediante la actualización dinámica.
- Configurar actualizaciones dinámicas y manuales DNS.
- Explicar qué es una zona DNS integrada en Active Directory.
- Describir el modo en que las zonas DNS integradas en Active Directory utilizan actualizaciones dinámicas seguras.
- Configurar zonas DNS integradas en Active Directory para utilizar actualizaciones dinámicas seguras.

Presentación multimedia: Información general acerca de las actualizaciones dinámicas de DNS



Ubicación de los archivos

Para iniciar la presentación *Información general acerca de las actualizaciones dinámicas DNS*, abra el archivo media30_2.htm que se puede encontrar dentro del fichero media30.zip.

Objetivos

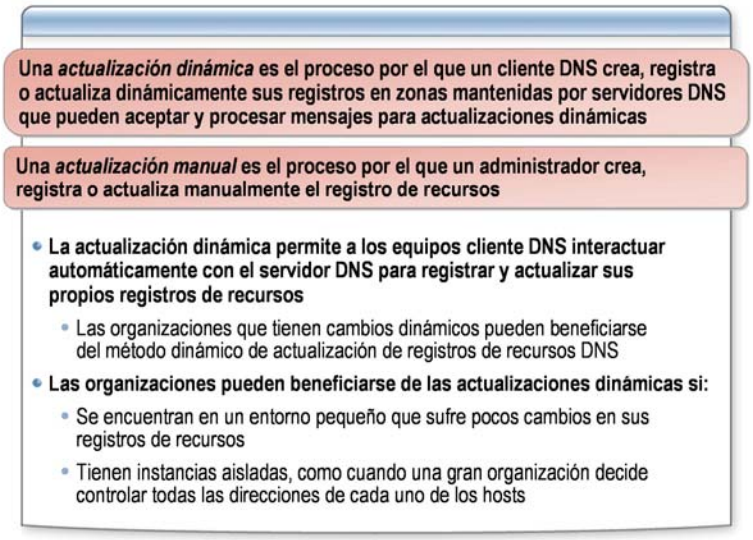
Al final de esta presentación, será capaz de:

- Explicar la importancia de las actualizaciones dinámicas de DNS.
- Explicar la diferencia entre las actualizaciones manuales y dinámicas.
- Explicar que los equipos cliente pueden:
  - Actualizar dinámicamente registros de recursos en los propios DNS.
  - Hacer que DHCP realice actualizaciones dinámicas en DNS en su nombre.
- Explicar qué son las actualizaciones dinámicas seguras.

Puntos clave

- Para que los usuarios tengan acceso a los recursos DNS correctamente, es fundamental que los registros de recursos DNS reflejen la configuración TCP/IP actual tanto en los equipos servidor como en los equipos cliente.
- Los registros de recursos DNS pueden actualizarlos los propios clientes DNS o DHCP en nombre de los clientes.
- Varios tipos de registros de recursos DNS, como registros de host (A) y registros de puntero (PTR), proporcionan a los clientes DNS diversos tipos de información.
- Puede utilizar un proceso de actualización manual para agregar y actualizar registros de recursos DNS, o bien puede habilitar los equipos cliente para actualizar y mantener dinámicamente sus propios registros de recursos en DNS.
- Una manera segura de actualizar los registros de recursos DNS es mediante las actualizaciones dinámicas seguras.

Qué son las actualizaciones dinámicas



Introducción

Hay dos maneras de crear, registrar y actualizar registros de recursos DNS en la base de datos DNS: dinámica y manualmente.

Al crear, registrar o actualizar registros de recursos, éstos se almacenan en el archivo de zona DNS.

Definiciones

Una *actualización dinámica* es el proceso por el que un cliente DNS crea, registra o actualiza dinámicamente sus registros en zonas mantenidas por servidores DNS que pueden aceptar y procesar mensajes para actualizaciones dinámicas.

Una *actualización manual* es el proceso por el que un administrador crea, registra o actualiza manualmente el registro de recursos.

Finalidad de las actualizaciones dinámicas

El proceso de actualizar manualmente registros de recursos de cliente no escala bien en una gran organización que soporte cambios continuos de registros de recursos DNS. Una gran organización que sufra cambios dinámicos debe confiar en el método dinámico de actualizar los registros de recursos DNS.

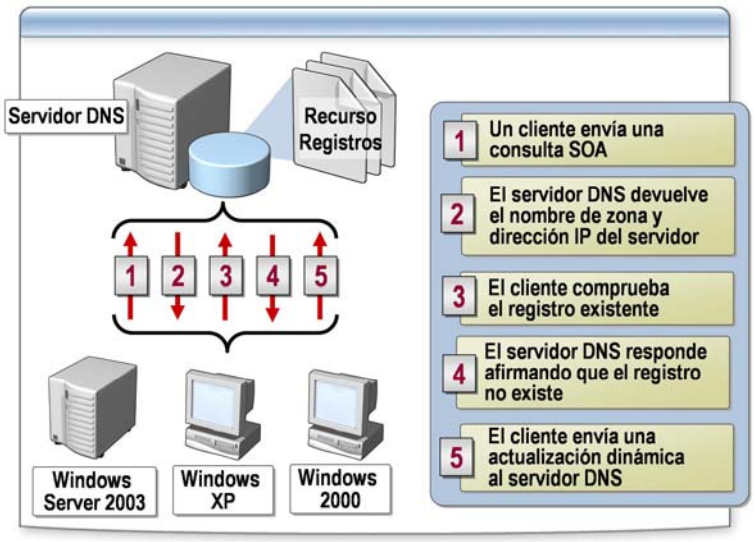
El registro y la actualización dinámicos permiten a los equipos cliente DNS interactuar automáticamente con el servidor DNS para registrar y actualizar sus propios registros de recursos. En una implementación de DNS que utilice un servidor DNS en el que se ejecute Microsoft Windows NT® 4.0 y versiones de BIND anteriores, el administrador tiene que modificar el archivo de zona correspondiente manualmente si debe cambiarse la información autorizada de un registro de recursos. A medida que el número de registros DNS de una zona aumenta y el administrador tiene dificultades para mantenerlo manualmente, la actualización dinámica se convierte en fundamental.

Circunstancias para configurar actualizaciones dinámicas manualmente

El administrador DNS puede beneficiarse del registro o la actualización manual de registros de recursos si la organización dispone de lo siguiente:

- Un entorno más pequeño con pocos cambios en los registros de recursos.
- Instancias aisladas, como cuando una gran organización decide controlar todas las direcciones de cada uno de los hosts.

Cómo registran y actualizan los clientes DNS sus registros de recursos propios mediante actualizaciones dinámicas



Tipos de clientes DNS que pueden registrar y actualizar dinámicamente registros de recursos

Los clientes DNS que ejecutan Windows Server 2003, Windows 2000 y Windows XP se configuran de manera predeterminada para registrar y actualizar dinámicamente sus nombres de host y direcciones IP en DNS.

Independientemente de que a un cliente DNS se le asigne una dirección IP mediante DHCP o de manera estática, un cliente DNS puede registrar y actualizar dinámicamente su nombre de host y dirección IP en DNS.

El componente que registra el registro de recursos DNS para un cliente DNS es el servicio Cliente DHCP. Incluso en clientes configurados con datos para una dirección IP estática, el servicio Cliente DHCP debe estar ejecutándose para que el cliente estático registre sus registros de recursos en DNS.

Proceso

El proceso siguiente indica los pasos para actualizar dinámicamente los clientes DNS:

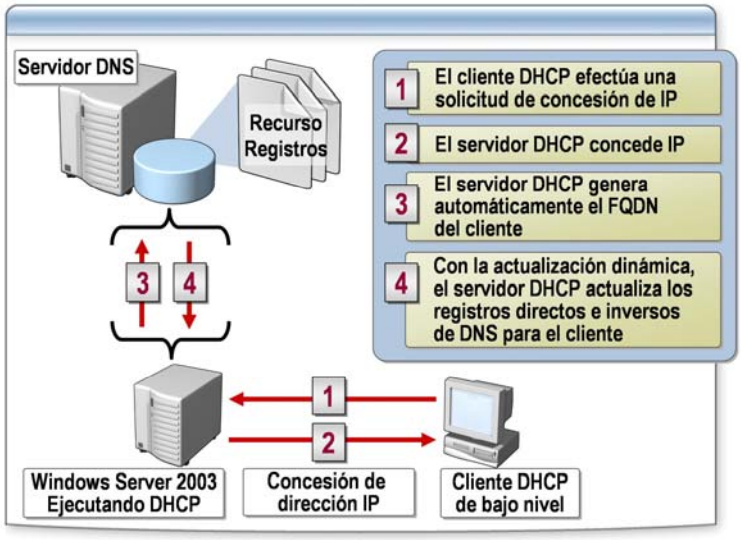
1. El cliente DNS envía una consulta SOA al servidor DNS que está autorizado para el registro de recursos con el que el cliente DNS se desea registrar.
2. El servidor DNS devuelve el nombre de zona y dirección IP del servidor DNS que está autorizado para la zona que el cliente DNS desea registrar en el servidor DNS.
3. El cliente DNS envía al servidor DNS autorizado de la zona una actualización de aserción para comprobar que no existe ningún registro en la zona.
4. El servidor DNS responde al cliente DNS.
5. Si no existe ningún registro en la zona DNS, el cliente DNS envía un paquete de actualización dinámica para registrar el registro de recursos.

Si el cliente DNS no consigue actualizar su registro de recursos en la base de datos de DNS tal como se describe en el proceso anterior, el cliente continúa intentando actualizar su registro de recursos en DNS.

1. El cliente DNS intenta registrar el registro con otros servidores principales en la zona. Varios servidores principales serán sólo una opción con una zona integrada en Active Directory.
2. Si todos los intentos fallan, el cliente intenta volver a registrar el registro después de cinco minutos y, después, de nuevo tras diez minutos.
3. Los errores dan como resultado un patrón repetido de intentos 50 minutos después del último intento.

Nota Un cliente de acceso remoto funciona de la misma manera que un cliente configurado con datos de configuración para una dirección IP estática. Por ejemplo, no se produce ninguna interacción entre el cliente y el servidor DHCP. Cuando el cliente de acceso remoto se conecta a la red, es responsable de actualizar dinámicamente los registros de recursos A y PTR en DNS. El cliente de acceso remoto intenta eliminar ambos registros antes de cerrar la conexión, pero los registros no se actualizan (lo que significa que no son actuales o válidos) si la actualización falló, como cuando un servidor DNS no funciona. Los registros tampoco se actualizan si la conexión falla de manera inesperada. En estos casos, un servidor de acceso remoto intenta la anulación de registro (lo que significa que el servidor de acceso remoto intenta eliminar el registro antiguo) del registro PTR correspondiente.

Cómo registra y actualiza un servidor DHCP los registros de recursos mediante actualizaciones dinámicas



Definición

Un *cliente de bajo nivel* es un cliente DHCP que ejecuta Windows NT 4.0 o una versión anterior. Los clientes de bajo nivel no pueden registrar ni actualizar sus registros de recursos en DNS por sí mismos.

Finalidad de las actualizaciones DNS dinámicas con un servidor DHCP

Puesto que los clientes de bajo nivel no pueden registrar ni actualizar sus propios registros de recursos, Microsoft diseñó su implementación del servidor DHCP con la capacidad de registrar registros de recursos de cliente DNS en nombre de los clientes DHCP.

Tipos de clientes DHCP que pueden registrar y actualizar dinámicamente registros de recursos

En un servidor DHCP que ejecuta Windows Server 2003 o Windows 2000, se puede configurar el servidor DHCP para actualizar dinámicamente los registros de recursos en DNS en nombre de clientes DHCP de la red. Los clientes que ejecutan Windows NT 4.0 y versiones anteriores pueden hacer que se introduzcan sus registros de recursos en la base de datos DNS si DHCP se configura para actualizar dinámicamente los registros DNS en su nombre.

Los administradores pueden configurar servidores DHCP que ejecuten Windows Server 2003 y Windows 2000 para actualizar registros de recursos de cliente DNS para los siguientes tipos de cliente:

- Cualquier cliente DHCP de nivel inferior que no solicite actualizaciones dinámicas.
- Cualquier cliente DHCP, incluidos aquéllos que ejecuten Windows XP y Windows 2000, independientemente de que soliciten una actualización dinámica.

Proceso de realización de actualizaciones dinámicas para un cliente de bajo nivel

En la ilustración, el servidor DHCP que ejecuta Windows Server 2003 realiza actualizaciones dinámicas para un cliente de bajo nivel.

1. El cliente DHCP efectúa una solicitud de concesión de IP.
2. El servidor DHCP concede una dirección IP.
3. El servidor DHCP genera automáticamente el nombre de dominio completo del cliente agregando el nombre de dominio definido para el ámbito DHCP al nombre del cliente. El nombre del cliente se obtiene del mensaje DHCPREQUEST que envía el cliente.
4. Con el protocolo de actualización dinámica, el servidor DHCP actualiza el:
   a. Nombre (A) directo de DNS para el cliente.
   b. Nombre (PTR) inverso de DNS para el cliente.

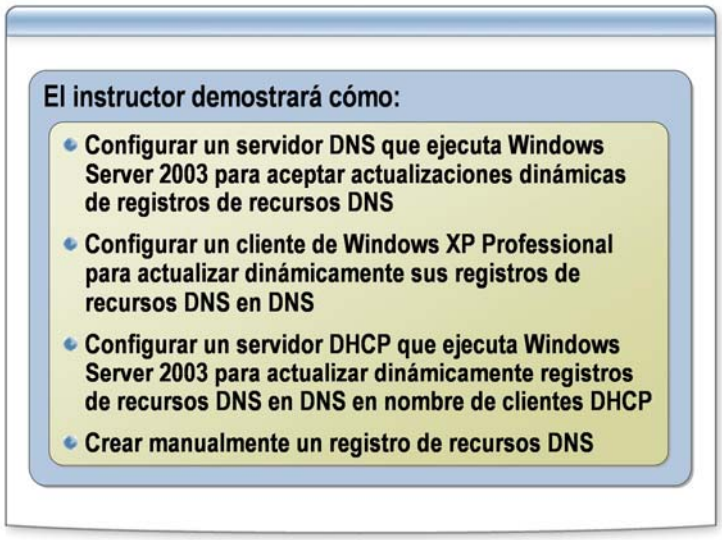
La capacidad de registrar tipos de registro A y PTR permite al servidor DHCP ejecutar Windows Server 2003 con el fin de actuar como proxy en clientes de bajo nivel para el registro DNS.

Proceso de realización de actualizaciones dinámicas para un cliente de Windows XP

Los pasos siguientes reflejan el proceso en el que un servidor DHCP que ejecuta Windows Server 2003 con la configuración predeterminada realiza actualizaciones dinámicas DNS para un cliente de Windows XP:

1. El cliente DHCP efectúa una solicitud de concesión de IP que incluye el nombre de dominio completo del cliente en la opción 81 de la solicitud DHCP.
2. El servidor DHCP concede una dirección IP.
3. El cliente conecta con el servidor DNS para actualizar el registro A para sí mismo.
4. El servidor DHCP actualiza el nombre (PTR) inverso de DNS para el cliente mediante el protocolo de actualización dinámica.

Cómo configurar actualizaciones DNS manuales y dinámicas



Introducción

Para configurar actualizaciones dinámicas como solución, es necesario elegir y configurar una o ambas de las opciones siguientes. Las actualizaciones dinámicas se admiten en zonas DNS principales.

Para utilizar un cliente DNS para actualizaciones dinámicas, configure:

1. El servidor DNS para aceptar actualizaciones dinámicas.
2. Los clientes DNS para crear actualizaciones dinámicas para sí mismos.

Con el fin de utilizar un servidor DHCP para actualizaciones dinámicas, configure:

1. El servidor DNS para aceptar actualizaciones dinámicas.
2. El servidor DHCP para crear actualizaciones dinámicas en nombre de los clientes DHCP.

Para crear manualmente un registro de recursos DNS, debe agregar un registro de recursos de host (A) a una zona de búsqueda directa.

Nota Es recomendable que inicie sesión con una cuenta que no tenga credenciales administrativas y que ejecute el comando **Ejecutar como** con una cuenta de usuario que disponga de las credenciales administrativas apropiadas para realizar esta tarea.

Procedimiento para configurar un servidor DNS para aceptar actualizaciones dinámicas

Para configurar un servidor DNS que ejecuta Windows Server 2003 para aceptar actualizaciones dinámicas de registros de recursos DNS:

1. Abra la consola DNS.
2. En el árbol de la consola, haga clic con el botón secundario del *mouse* en la zona aplicable y, a continuación, haga clic en **Propiedades**.
3. En la ficha **General**, en la lista desplegable **Actualizaciones dinámicas**, haga clic en **Sin seguridad y con seguridad**.
4. Haga clic en **Aceptar** para cerrar el cuadro de diálogo **Propiedades** de la zona DNS y, a continuación, cierre la consola **DNS**.

Procedimiento para configurar clientes DNS que ejecutan Windows XP Professional para actualización dinámica

Para configurar un cliente de Windows XP Professional de modo que actualice dinámicamente sus registros de recursos DNS en DNS:

1. En el Panel de control, abra el cuadro de diálogo **Propiedades** de la interfaz de red apropiada.
2. En el cuadro de diálogo **Propiedades**, seleccione **Protocolo de Internet (TCP/IP)** y, a continuación, haga clic en **Propiedades**.
3. En el cuadro de diálogo **Propiedades de protocolo de Internet (TCP/IP)**, haga clic en **Opciones avanzadas**.
4. En la ficha **DNS** del cuadro de diálogo **Configuración avanzada de TCP/IP**, seleccione **Registrar estas direcciones de conexiones en DNS**.
5. En la ficha **DNS** del cuadro de diálogo **Configuración avanzada de TCP/IP**, seleccione **Utilizar este sufijo DNS de conexión para registro DNS**, si es necesario.
6. En el cuadro de diálogo **Propiedades avanzadas de TCP/IP**, haga clic en **Aceptar**.
7. En el cuadro de diálogo **Propiedades de Protocolo de Internet (TCP/IP)**, haga clic en **Aceptar**.
8. En el cuadro de diálogo **Propiedades de Conexión de red**, haga clic en **Cerrar**.

Procedimiento para configurar un servidor DHCP de modo que actualice dinámicamente registros de recursos DNS en nombre de clientes DHCP

Para configurar un servidor DHCP que ejecuta Windows Server 2003 de modo que actualice dinámicamente registros de recursos DNS en DNS en nombre de clientes DHCP:

1. Abra la consola DHCP.
2. En la consola **DHCP**, seleccione el servidor DHCP correspondiente.
3. En el menú **Acción**, haga clic en **Propiedades**.
4. En la ficha **DNS**, compruebe que la opción **Habilitar actualizaciones DNS dinámicas de acuerdo con la siguiente configuración** está seleccionada y, a continuación, seleccione una de estas dos opciones:
   - **Actualizar dinámicamente registros DNS A y PTR sólo si los clientes DHCP lo solicitan.**
   - **Actualizar siempre dinámicamente los registros DNS A y PTR.**

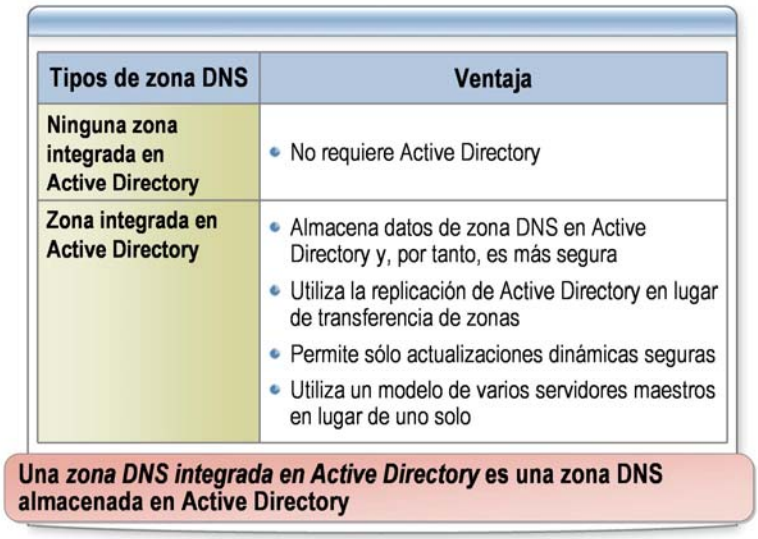
5. En la ficha **DNS**, compruebe que la opción **Descartar registros A y PTR cuando la concesión se suprima** está seleccionada.
6. En la ficha **DNS**, si es necesario, seleccione la opción **Actualizar dinámicamente registros DNS A y PTR para clientes DHCP que no soliciten actualizaciones** y, a continuación, haga clic en **Aceptar**.
7. Cierre la consola DHCP.

Procedimiento para crear manualmente registros de recursos DNS

Para crear manualmente un registro de recursos DNS:

1. Abra la consola DNS.
2. En el árbol de la consola, haga clic con el botón secundario del *mouse* en la zona de búsqueda directa correspondiente y, a continuación, haga clic en **Host nuevo (A)**.
3. En el cuadro de diálogo **Host nuevo**, en el campo **Nombre**, escriba el nombre de equipo DNS para el nuevo host.
4. En el cuadro de diálogo **Host nuevo**, en el campo **Dirección IP**, escriba la dirección IP para el nuevo host.
5. Como opción, seleccione **Crear registro del puntero (PTR) asociado** para crear un registro de puntero adicional en una zona inversa para este host, en función de la información especificada en los cuadros **Nombre** y **Dirección IP**.
6. En el cuadro de diálogo **Host nuevo**, haga clic en **Agregar host** para agregar el nuevo registro de host a la zona.
7. En el cuadro de mensaje **DNS**, haga clic en **Aceptar**.
8. En el cuadro de diálogo **Host nuevo**, haga clic en **Realizado**.
9. Cierre la consola DNS.

Qué es una zona DNS integrada en Active Directory



Definición

Una *zona DNS integrada en Active Directory* es una zona DNS almacenada en Active Directory.

Finalidad de las zonas DNS integradas en Active Directory

Al configurar un controlador de dominio, Active Directory requiere que DNS esté instalado. Las zonas, que se crean en un servidor DNS que es un controlador de dominio de Active Directory, pueden ser zonas DNS integradas en Active Directory.

Este tipo de zonas tiene muchas ventajas con respecto a las zonas DNS que no están integradas en Active Directory. Las zonas DNS integradas en Active Directory pueden utilizar Active Directory:

- Almacenar datos de configuración de zona en Active Directory, en lugar de almacenar datos de configuración de zona en un archivo de zona.
- Utilizar la replicación de Active Directory en lugar de transferencias de zonas.
- Permitir sólo actualizaciones dinámicas seguras (en lugar de actualizaciones seguras y no seguras en una zona DNS no integrada en Active Directory).

Zonas DNS integradas en Active Directory

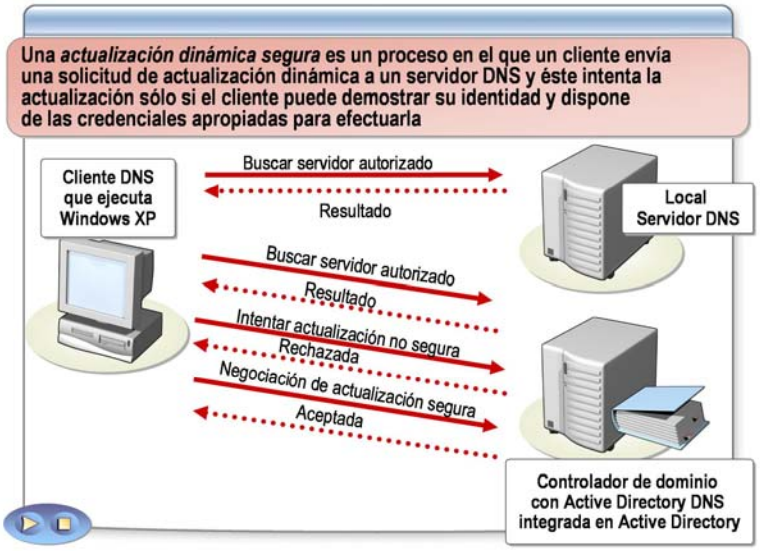
En una zona DNS no integrada en Active Directory, existe una única copia maestra de la zona DNS (principal) y puede existir cualquier número de copias adicionales de la zona DNS (secundaria).

En una zona DNS integrada en Active Directory, los datos de la zona están almacenados en Active Directory, por lo que puede seguirse un modelo con varios servidores maestros. Cada controlador de dominio puede administrar los cambios en la zona DNS.

El modelo con varios servidores maestros significa que si un controlador de dominio tiene una zona integrada en Active Directory, cualquier controlador de dominio que contenga dicha información de zona DNS puede actuar como servidor principal y puede efectuar cambios en la zona DNS.

Nota El modo de aplicación de Active Directory no admite el alojamiento de DNS integrado en Active Directory.

Cómo utilizan actualizaciones dinámicas seguras las zonas DNS integradas en Active Directory



Definición

Una *actualización dinámica segura* es un proceso en el que un cliente envía una solicitud de actualización dinámica a un servidor DNS y éste intenta la actualización sólo si el cliente puede demostrar su identidad y dispone de las credenciales apropiadas para efectuarla. Las actualizaciones dinámicas están disponibles únicamente en zonas integradas en Active Directory.

El mejor método en un controlador de dominio configurado con una zona DNS es permitir sólo las actualizaciones dinámicas seguras.

El otro método es configurar una zona que se encuentre en un servidor DNS no integrado en Active Directory, para permitir actualizaciones dinámicas seguras y no seguras.

Finalidad de las actualizaciones dinámicas seguras

DNS en Windows Server 2003 admite la actualización dinámica segura. Este tipo de actualización proporciona diversos beneficios, como son:

- La protección de zonas y registros de recursos frente a la modificación por parte de usuarios que no tienen autorización.
- Permitir al administrador especificar exactamente qué usuarios y grupos pueden modificar zonas y registros de recursos.

Al permitir actualizaciones dinámicas en una zona DNS, no es necesario crear y mantener manualmente todos los registros de recursos. No obstante, no se puede controlar qué clientes DNS pueden actualizar dinámicamente. Si se utiliza un servidor DNS independiente que no esté integrado en Active Directory, no se puede controlar quién lo actualiza dinámicamente. Por ejemplo, si un consultor externo trae a la organización un equipo portátil que no forma parte del dominio y si el equipo portátil se actualiza dinámicamente en DNS, se podría tener un problema de seguridad.

No obstante, si un servidor DNS aloja la zona DNS en una zona integrada en Active Directory, se puede configurar la zona DNS para permitir sólo actualizaciones seguras. Esto significa que si el mismo equipo portátil, que no es miembro del dominio, se intenta actualizar dinámicamente en la zona DNS, no se permitirá. Al utilizar la seguridad de dominio, puede controlar las actualizaciones dinámicas permitiendo actualizar sus registros dinámicamente sólo a los miembros del dominio.

Nota Puesto que la zona DNS está integrada en Active Directory, puede configurar la lista de control de acceso (ACL) en registros de recursos paraproteger DNS aún más. Para obtener más información, consulte en la documentación de Ayuda de Windows Server 2003 cómo proteger DNS mediante ACL.

Actualizaciones dinámicas no seguras frente a las seguras

Si una zona está integrada en Active Directory, puede configurarse como Sólo segura. Una zona configurada como Sólo segura autentica el equipo que intenta efectuar la actualización y sólo permite la actualización si los permisos del registro lo permiten. Las zonas alojadas en Active Directory, además de las que no lo están, pueden configurarse para permitir actualizaciones no seguras, las cuales permitirían registros y modificaciones de DNS sin autenticar el equipo cliente.

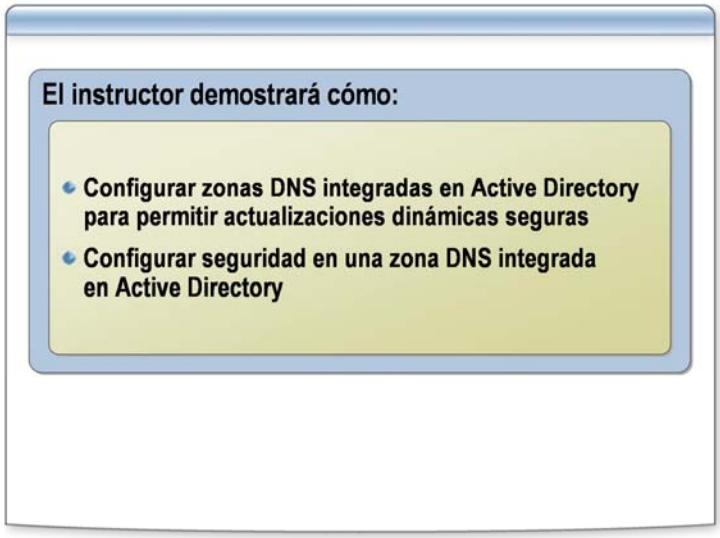
Proceso

En la ilustración, el procedimiento siguiente proporciona la secuencia de eventos del proceso de actualización dinámica segura:

1. El cliente consulta el servidor de nombres local para saber qué servidor está autorizado para el nombre que el cliente intenta actualizar y el servidor de nombres local responde con la referencia al servidor autorizado.
2. El cliente consulta al servidor autorizado para comprobar que el servidor DNS está autorizado para el nombre que el cliente intenta actualizar y el servidor confirma la consulta.
3. El cliente intenta una actualización no segura y el servidor rechaza la actualización no segura. Si el servidor se ha configurado para actualización dinámica no segura en la zona apropiada, en lugar de para actualización dinámica segura, el servidor habría intentado efectuar la actualización.
4. El cliente intenta entonces una actualización segura. Si la actualización tiene las credenciales apropiadas, el servidor DNS autorizado acepta la actualización y responde al cliente DNS.

Nota Si un servidor DHCP realiza la primera actualización dinámica segura en un registro de recursos DNS, dicho servidor DHCP se convierte en el propietario de dicho registro y sólo él puede actualizarlo. Esto puede causar problemas en algunos casos. Por ejemplo, supongamos que el servidor DHCP (DHCP1) creó un registro para el nombre nt4host1.nwtraders.msft y después dejó de responder, y que el servidor DHCP (DHCP2) intentó actualizar el nombre. DHCP2 no puede actualizar el nombre, puesto que DHCP2 no es el propietario del mismo. Por tanto, si se habilita actualización dinámica segura, todos los servidores DHCP deberían estar ubicados en un grupo de seguridad especial denominado DNSUpdateProxy. Los objetos creados por miembros del grupo DNSUpdateProxy no tienen seguridad; por tanto, cualquier usuario autenticado puede asumir la propiedad de los objetos. Para obtener más información acerca de DNSUpdateProxy o acerca de las actualizaciones dinámicas seguras, consulte la documentación de Ayuda de Windows Server 2003.

Cómo configurar zonas DNS integradas en Active Directory para permitir actualizaciones dinámicas seguras



Introducción

Tanto las zonas DNS integradas en Active Directory como las que no lo están pueden configurarse para permitir la actualización dinámica segura. También puede configurar la seguridad en zonas DNS integradas en Active Directory.

Nota Es recomendable que inicie sesión con una cuenta que no tenga credenciales administrativas y que ejecute el comando **Ejecutar como** con una cuenta de usuario que disponga de las credenciales administrativas apropiadas para realizar esta tarea.

Procedimiento para configurar zonas DNS integradas en Active Directory para permitir actualizaciones dinámicas seguras

Para configurar zonas DNS integradas en Active Directory para permitir actualizaciones dinámicas seguras:

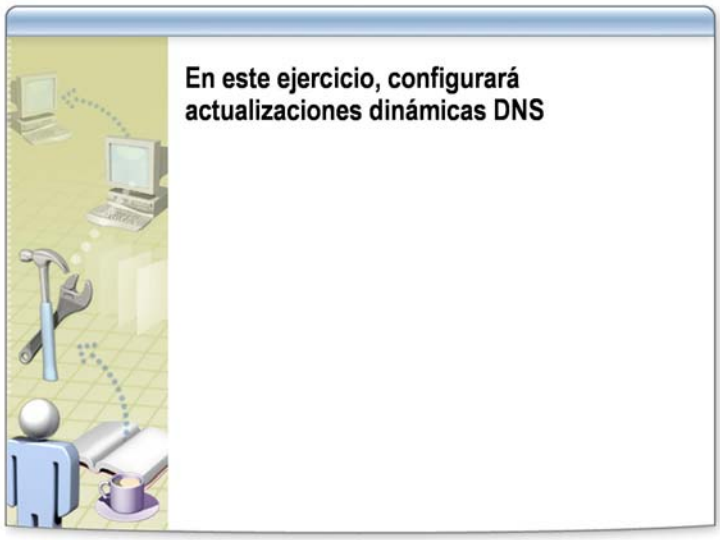
1. Abra la consola DNS.
2. En el árbol de la consola, haga clic con el botón secundario del *mouse* en la zona aplicable y, a continuación, haga clic en **Propiedades**.
3. En la ficha **General**, compruebe que el **Tipo** es **Integrada en Active Directory**.
4. En la lista desplegable **Actualizaciones dinámicas**, seleccione **Sólo con seguridad**.
5. Haga clic en **Aceptar** para cerrar el cuadro de diálogo **Propiedades** de la zona DNS y, a continuación, cierre la consola DNS.

Procedimiento para configurar seguridad en una zona DNS integrada en Active Directory

Para configurar seguridad en una zona DNS integrada en Active Directory:

1. Abra la consola DNS.
2. En el árbol de la consola, haga clic con el botón secundario del *mouse* en la zona aplicable y, a continuación, haga clic en **Propiedades**.
3. En la ficha **Seguridad**, configure los permisos de manera apropiada para su red.
4. Haga clic en **Aceptar** para cerrar el cuadro de diálogo **Propiedades** de la zona DNS y, a continuación, cierre la consola DNS.

Ejercicio: Configurar las actualizaciones dinámicas DNS



Objetivo

En este ejercicio, configurará actualizaciones dinámicas DNS.

Instrucciones

Para completar este ejercicio, consulte el documento *Valores del plan de implementación*, incluido en el apéndice al final del cuaderno de trabajo.

Debe haber iniciado sesión con una cuenta que no tenga credenciales administrativas y ejecutar el comando **Ejecutar como** con una cuenta de usuario que disponga de las credenciales administrativas apropiadas para realizar la tarea.

Situación de ejemplo

El número de equipos de la subred de desarrollo ha aumentado. Como resultado, se ha producido un incremento en el número de registros de recursos DNS que hay que crear manualmente. El servidor DHCP se configurará para crear automáticamente los registros de recursos en DNS en nombre de los clientes DHCP.

Ejercicio

Configurar un servidor DNS de modo que acepte actualizaciones dinámicas para una zona de búsqueda directa

- Complete esta tarea desde los equipos de ambos alumnos
- Zona de búsqueda directa principal: *srv*.**nwtraders.msft** (donde *srv* es la etiqueta de tres letras del nombre del equipo)
- Actualizaciones dinámicas: **Sin seguridad y con seguridad**

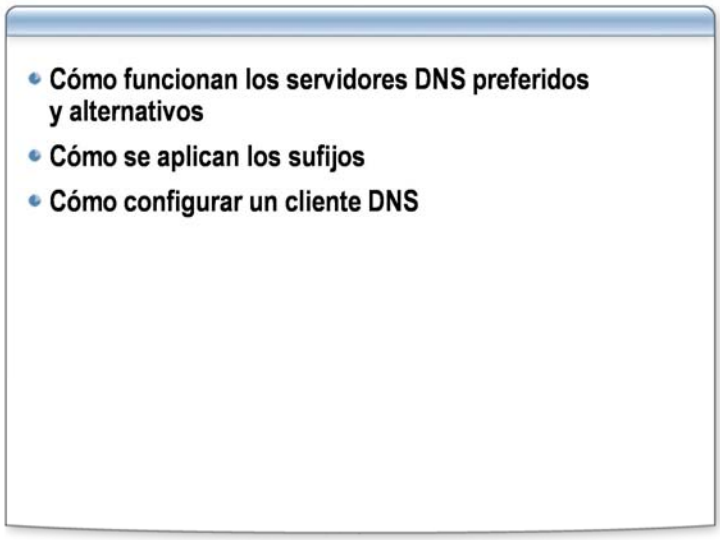
Configurar un servidor DHCP para actualizar dinámicamente registros de recursos DNS en nombre de clientes DHCP

- Complete esta tarea desde los equipos de ambos alumnos
- Servidor DHCP: su servidor DHCP
- Seleccione **Actualizar siempre dinámicamente registros DNS A y PTR**

Crear manualmente un registro de recursos de host DNS

- Complete esta tarea desde los equipos de ambos alumnos
- Zona de búsqueda directa principal: *srv***.nwtraders.msft** (donde *srv* es la etiqueta de tres letras del nombre del equipo)
- Nombre de host: *NombreDeEquipo***2** (donde *NombreDeEquipo* es el nombre del equipo de su compañero)
- Dirección IP: *Conexión de red del asociado* (donde *Conexión de red del asociado* es la dirección IP correspondiente a su compañero)

Lección: Configurar un cliente DNS



Introducción

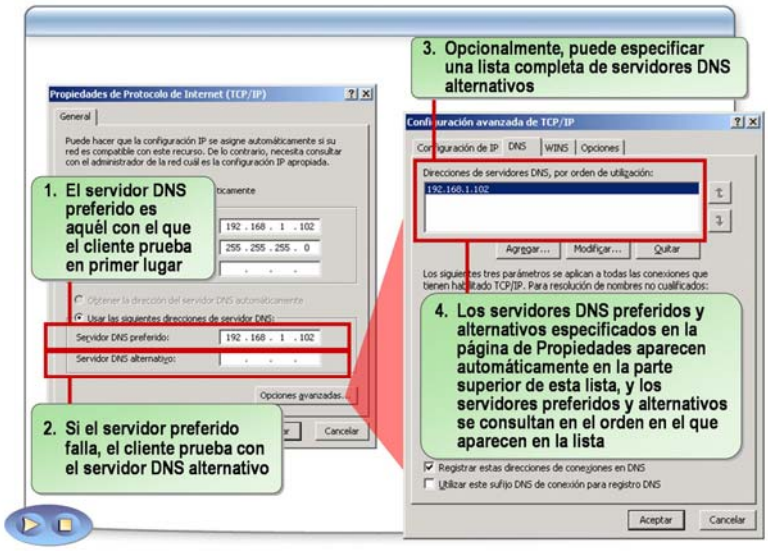
Se han instalado y configurado las propiedades del servidor DNS y se han creado las zonas apropiadas en el servidor DNS. Ahora es necesario asegurar que los clientes puedan registrar o crear sus registros de recursos en DNS y utilizar DNS para resolver consultas.

Objetivos de la lección

Después de finalizar esta lección, será capaz de:

- Describir cómo funcionan los servidores DNS preferidos y alternativos.
- Describir cómo se aplican los sufijos.
- Configurar un cliente DNS.

Cómo funcionan los servidores DNS preferidos y alternativos



Definiciones

Un *servidor DNS preferido* es aquél que es el destinatario de las consultas DNS que el cliente DNS envía. También es el servidor en el que el cliente DNS actualiza sus registros de recursos.

Un *servidor DNS alternativo* es aquél que se utiliza si el servidor DNS preferido no se puede utilizar o no puede resolver consultas DNS de un cliente DNS particular porque el servicio DNS ha fallado. El servidor alternativo no es necesario si la consulta de un nombre no puede resolverse.

Finalidad de los servidores DNS preferido y alternativo

Sin un servidor DNS preferido, el cliente DNS no puede consultar un servidor DNS.

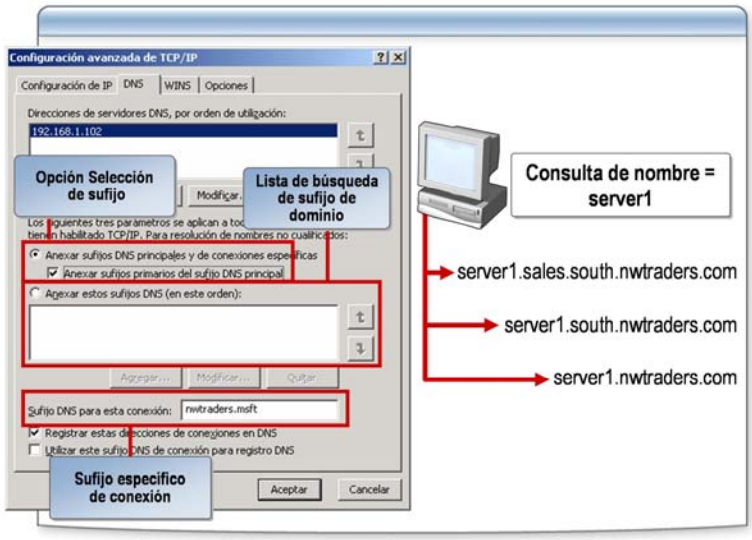
Sin un DNS alternativo, las consultas no se resolverán si el servidor DNS preferido falla. Se puede tener más de un servidor DNS alternativo.

Proceso

Los pasos siguientes indican el proceso para entrar en contacto con servidores DNS preferidos y alternativos:

1. El servidor DNS preferido responde primero a una consulta DNS o a una actualización DNS.
2. Si el servidor DNS preferido no responde a una consulta DNS o a una actualización DNS, la consulta o actualización se redirige al servidor DNS alternativo.
3. Si el servidor DNS alternativo no responde y el cliente DNS está configurado con las direcciones IP adicionales de servidores DNS, el cliente DNS envía la consulta o actualización al siguiente servidor DNS de la lista.
4. Si alguno de los servidores DNS (un servidor preferido, un servidor alternativo o cualquier otro de la lista) no responde, dicho servidor se quita temporalmente de la lista.
5. Si ninguno de los servidores DNS responden, la consulta o actualización del cliente DNS no se realiza.

Cómo se aplican los sufijos



Finalidad de la configuración de sufijos

Si no tiene un sufijo DNS configurado en el cliente, la resolución de nombres y la actualización pueden no funcionar correctamente. Mediante la correcta configuración de sufijos DNS en el cliente, se asegura que la resolución de nombres sea correcta.

Opción Selección de sufijo

La opción Selección de sufijo especifica que las resoluciones para nombres no calificados en este equipo se limiten a los sufijos de dominio del sufijo DNS principal hasta el dominio de segundo nivel.

Por ejemplo, si el sufijo DNS principal es nwtraders.msft y se intenta entrar en contacto con Server1, el equipo consulta a Server1.nwtraders.msft, además de cualquier sufijo configurado en los sufijos específicos de la conexión.

La opción Anexar sufijos primarios especifica que las resoluciones para nombres no calificados en este equipo están limitadas a los sufijos de dominio del sufijo primario y el sufijo específico de la conexión.

Por ejemplo, si el sufijo DNS primario es sales.south.nwtraders.msft e intenta entrar en contacto con Server1, el equipo consulta a server1.sales.south.nwtraders.msft. Si la consulta no se resuelve, el equipo consulta a server1.south.nwtraders.msft. Si la consulta sigue sin resolverse, el equipo consulta a server1.nwtraders.msft.

Sufijo específico de conexión

El Sufijo específico de conexión proporciona un espacio para configurar un sufijo DNS para esta conexión específica. Si un servidor DHCP configura esta conexión, y si no especifica un sufijo DNS, el servidor DHCP asigna un sufijo DNS si el servidor está configurado para hacerlo.

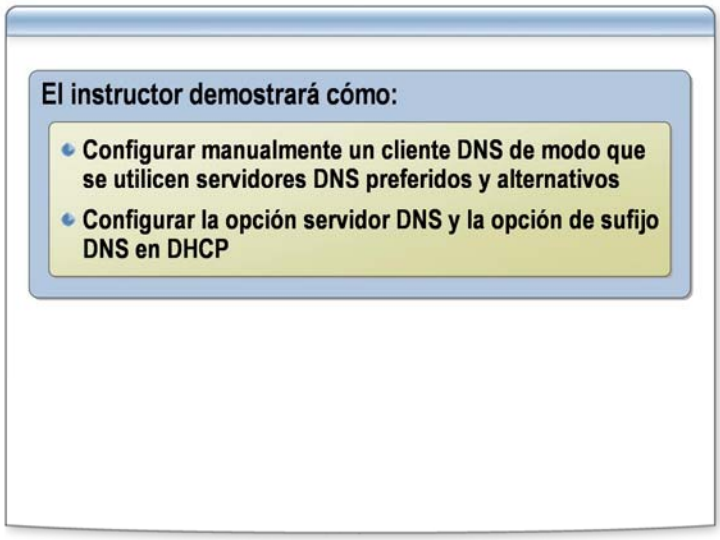
Cómo se aplican los sufijos

Cuando un usuario especifica un nombre de dominio completo (FQDN), el solucionador DNS consulta DNS con dicho nombre, de la forma siguiente:

1. El solucionador del cliente DNS envía la consulta al servidor DNS principal con el sufijo DNS principal.
2. Si la resolución no tiene éxito, el solucionador del cliente DNS anexa cada sufijo DNS específico de la conexión.
3. Si la resolución sigue sin realizarse correctamente, el solucionador DNS devuelve el nombre de dominio completo anexando el sufijo principal del nombre del sufijo DNS principal y el elemento primario de dicho sufijo, y así sucesivamente hasta que sólo queden dos etiquetas.

   Por ejemplo, server1.sales.south.nwtraders.com devuelve server1.south.nwtraders.com, que a continuación devuelve server1.nwtraders.com.
4. No obstante, si el usuario ha especificado una lista de búsqueda de sufijos de dominios, se pasan por alto tanto el sufijo DNS principal como el nombre del dominio específico de la conexión. Ni el sufijo DNS principal ni el nombre de dominio específico de la conexión se anexan al nombre de host antes de que el FQDN se envíe al DNS. En cambio, el solucionador DNS anexa cada sufijo de la lista de búsqueda de dominio en orden y lo envía al servidor DNS hasta que encuentra una correspondencia o se alcanza el final de la lista.

Cómo configurar un cliente DNS



Introducción

Es necesario configurar un cliente DNS de manera que el cliente pueda utilizar servidores DNS con el fin de resolver y actualizar información para la configuración de direcciones IP.

Un cliente DNS puede recibir datos de configuración de direcciones IP de dos maneras: manualmente o mediante DHCP.

Importante En esta situación de ejemplo, es necesario haber iniciado sesión como administrador o como miembro del grupo Administradores para completar el primer procedimiento. Inicie sesión como *NombreDeEquipo*Admin para realizar el primer procedimiento. Una vez completado, inicie sesión como *NombreDeEquipo*User (donde *NombreDeEquipo* es el nombre de su equipo).

Procedimiento para configurar manualmente un cliente DNS de modo que se utilicen servidores DNS preferidos y alternativos

Para configurar manualmente un cliente DNS de modo que se usen servidores DNS preferidos y alternativos:

1. En Conexiones de red, abra el cuadro de diálogo **Propiedades** para la Interfaz de red en la que desee configurar DNS.
2. En la ficha **General**, haga clic en **Protocolo de Internet (TCP/IP)** y, después, en **Propiedades**.
3. En el cuadro de diálogo **Propiedades de protocolo de Internet (TCP/IP)**, seleccione **Usar las siguientes direcciones de servidor DNS**.
4. En el campo **Servidor DNS preferido**, escriba la dirección IP del servidor DNS preferido.
5. En el campo **Servidor DNS alternativo**, escriba la dirección IP del servidor DNS alternativo y, a continuación, haga clic en **Opciones avanzadas**.

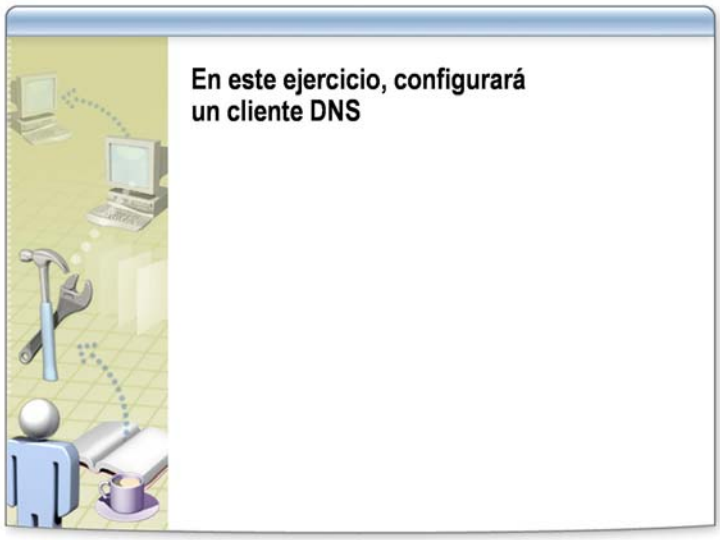
6. En el cuadro de diálogo **Configuración avanzada de TCP/IP**, en la ficha **DNS**, en el campo **Sufijo DNS para esta conexión**, escriba el sufijo DNS que se anexará al nombre de host del equipo y haga clic en **Aceptar**.
7. En el cuadro de diálogo **Propiedades de protocolo de Internet (TCP/IP)**, haga clic en **Aceptar**.
8. Cierre todas las ventanas abiertas.

Procedimiento para configurar la opción de servidor DNS y la opción de sufijo DNS en DHCP

Para configurar la opción de servidor DNS y la opción de sufijo DNS en DHCP:

1. Abra la consola DHCP.
2. En el ámbito apropiado, haga clic en **Opciones de ámbito** y, a continuación, en el menú **Acción**, haga clic en **Configurar opciones**.
3. En el cuadro de diálogo **Opciones de ámbito**, seleccione **006 Servidores DNS**.
4. En el campo **Dirección IP**, escriba la dirección IP del servidor DNS y, a continuación, haga clic en **Agregar**.
5. En el cuadro de diálogo **Opciones de ámbito**, seleccione **015 Nombre de dominio DNS**.
6. En el campo **Valor de la cadena**, escriba el sufijo de dominio DNS y haga clic en **Aceptar**.
7. Cierre la consola DHCP.
8. Mediante el comando **ipconfig**, asegúrese de que los clientes DHCP renuevan sus concesiones para actualizar sus datos de configuración IP con estas nuevas opciones de ámbito.

Ejercicio: Configurar un cliente DNS



Objetivo

En este ejercicio, configurará un cliente DNS para utilizar un servidor DNS preferido, un servidor DNS alternativo y un sufijo DNS.

Instrucciones

Para completar este ejercicio, consulte el documento *Valores del plan de implementación*, incluido en el apéndice al final del cuaderno de trabajo.

En este ejercicio, es necesario haber iniciado sesión como administrador o miembro del grupo Administradores para completar partes de este procedimiento. Inicie sesión como *NombreDeEquipo***Admin** para todo el ejercicio. Una vez completado el ejercicio, inicie sesión como *NombreDeEquipo***User**.

Situación de ejemplo

Se han agregado dos servidores DNS a su subred de *desarrollo*. Hay que configurar los equipos del laboratorio en su subred para utilizar un servidor DNS preferido y uno alternativo. Configurará su cliente DNS con las opciones DNS apropiadas.

Ejercicio

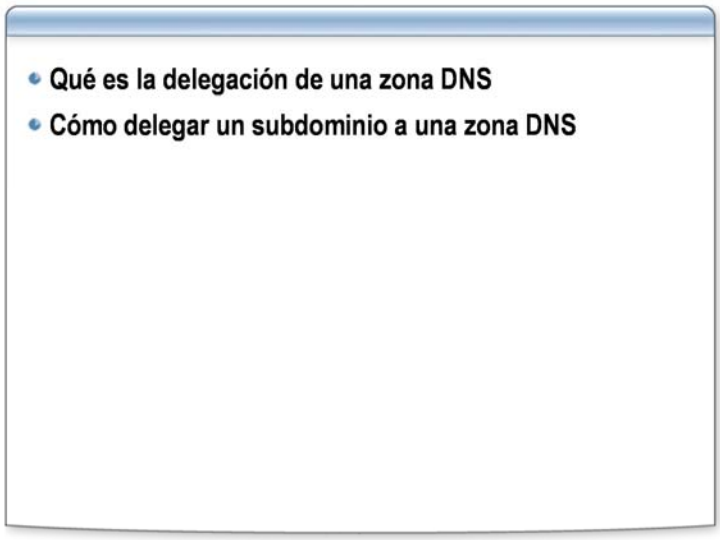
Configurar un cliente DNS

- Complete esta tarea desde los equipos de ambos alumnos
- Nombre de usuario: *NombreDeEquipo***Admin**
- Contraseña: **P@ssw0rd**
- Dominio: **nwtraders**
- Interfaz: **Conexión de red del aula**
- Dirección IP del servidor DNS preferido: *Conexión de red del aula* (la dirección IP de la conexión de red de su equipo)
- Dirección IP del servidor DNS alternativo: **192.168.*x*.200**
- Sufijo DNS: **nwtraders.msft**

Ver la configuración del cliente DNS mediante ipconfig

- Complete esta tarea desde los equipos de ambos alumnos
- Nombre de usuario: *NombreDeEquipo***User**
- Contraseña: **P@ssw0rd**
- Dominio: **nwtraders**
- Interfaz: **Conexión de red del aula**

Lección: Delegar la autoridad en las zonas



Introducción

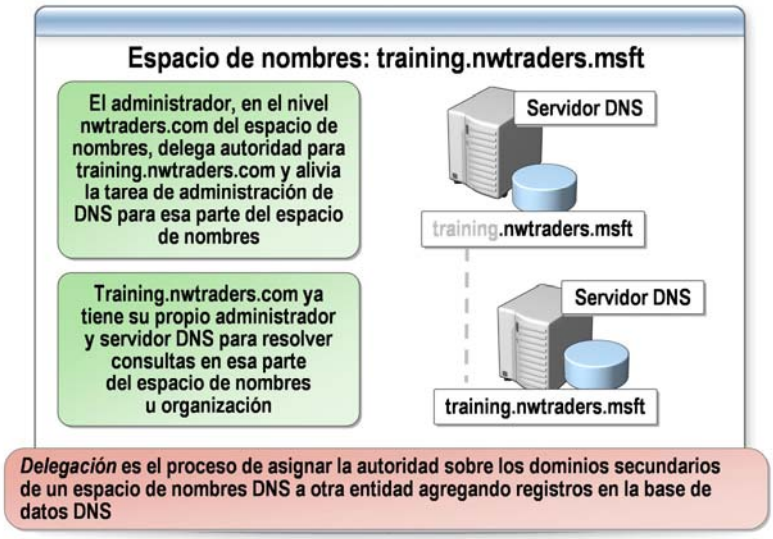
Una vez que la solución DNS funcione, puede ser necesario modificar el espacio de nombres DNS. El proceso mediante el cual se realizan estos cambios en el espacio de nombres DNS en el servidor DNS se denomina *delegación*.

Objetivos de la lección

Después de finalizar esta lección, será capaz de:

- Explicar qué es la delegación de una zona DNS.
- Delegar un subdominio a una zona DNS.

Qué es la delegación de una zona DNS



Definición

En términos técnicos, *delegación* es el proceso de asignar la autoridad sobre los dominios secundarios de un espacio de nombres DNS a otra entidad agregando registros en la base de datos DNS.

Finalidad de la delegación

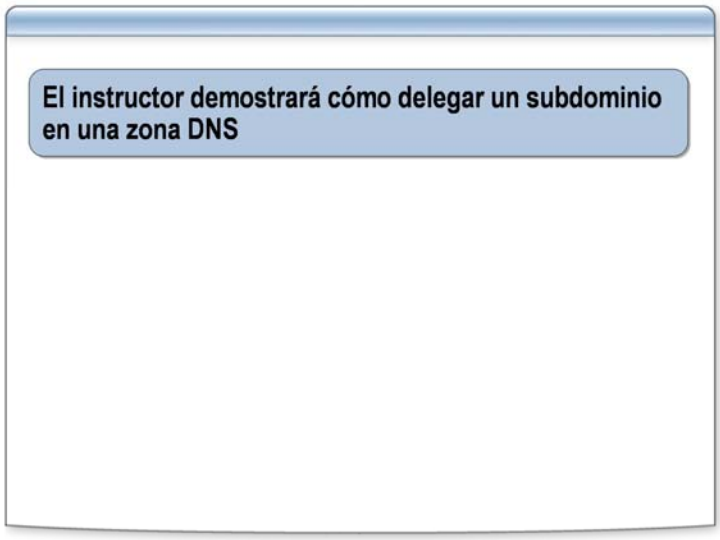
Como administrador de un dominio DNS, DNS proporciona la opción de crear dominios secundarios y sus respectivas zonas, que después pueden almacenarse, distribuirse y replicarse en otros servidores DNS. Estas zonas adicionales pueden delegarse a otros administradores para que las administren. Al decidir si se dividirá o no el espacio de nombres DNS para delegar zonas, debe tener en cuenta los siguientes motivos:

- La necesidad de delegar la administración de parte del espacio de nombres DNS a otra ubicación o departamento dentro de la organización.
- La necesidad de dividir una zona de gran tamaño en zonas más pequeñas para distribuir cargas de tráfico entre varios servidores, mejorar el rendimiento de la resolución de nombres DNS o crear un entorno DNS más tolerante a errores.
- La necesidad de ampliar el espacio de nombres mediante la adición de subdominios (por ejemplo, para acomodar la apertura de una nueva sucursal o sitio).

Ejemplo

En la ilustración, el administrador del nivel nwtraders.com del espacio de nombres delega autoridad para training.nwtraders.com y alivia la carga de trabajo de administración de DNS para esa parte del espacio de nombres. Training.nwtraders.com ya tiene su propia administración y servidor DNS para resolver consultas en esa parte del espacio de nombres. De este modo también se reduce la carga de trabajo para el administrador y el servidor DNS en el nivel nwtraders.com.

Cómo delegar un subdominio a una zona DNS



Introducción

Para asignar autoridad de partes del espacio de nombres DNS a otra entidad, puede delegar un subdominio en una zona DNS.

Directrices

Al delegar zonas dentro del espacio de nombres, hay que tener en cuenta que para cada nueva zona que se cree, se necesitarán registros de delegación, en otras zonas, que apunten a los servidores DNS autorizados para la nueva zona. Esto es necesario para transferir la autoridad y para proporcionar referencias correctas a otros servidores y clientes DNS de los nuevos servidores que se estén autorizando para la nueva zona.

Nota Es recomendable que inicie sesión con una cuenta que no tenga credenciales administrativas y que ejecute el comando **Ejecutar como** con una cuenta de usuario que disponga de las credenciales administrativas apropiadas para realizar esta tarea.

Procedimiento

Para delegar un subdominio en una zona DNS:

1. Abra la consola DNS.
2. Expanda el servidor DNS correspondiente, expanda **Zonas de búsqueda directa** o **Zonas de búsqueda inversa** y, a continuación, seleccione la zona apropiada que va a delegar.
3. En el menú **Acción**, haga clic en **Delegación nueva**.
4. En la página **Asistente para nueva delegación**, haga clic en **Siguiente**.
5. En la página **Nombre de dominio delegado**, en el campo **Dominio delegado**, escriba el nombre de dominio delegado y haga clic en **Siguiente**.

6. En la página **Servidores de nombres**, haga clic en **Agregar**.
7. En el cuadro de diálogo **Nuevo registro de recursos**, en el campo **Nombre de dominio completo**, escriba el FQDN correspondiente al servidor DNS al que delegar el dominio y, a continuación, haga clic en **Resolver**.
8. En el cuadro de diálogo **Nuevo registro de recursos**, en el campo **Dirección IP**, compruebe que se muestra la dirección IP correcta para el servidor que se resolvió y haga clic en **Aceptar**.
9. En la página **Servidores de nombres**, haga clic en **Siguiente**.
10. En la página **Finalización del Asistente para nueva delegación**, haga clic en **Finalizar**.
11. Cierre la consola DNS.