Windows Server 2012: Zonas DNS

©InterGrupo 2013

Tabla de Contenidos

©InterGrupo 2013

©InterGrupo 2013

Objetivos

- Explicar los distintos tipos de zona DNS.
- Explicar cómo crear zonas.
- Crear una zona de rutas internas.
- Explicar las transferencias de zonas DNS.

©InterGrupo 2013

©InterGrupo 2013

Zonas DNS

Las zonas DNS es un concepto importante en la infraestructura de DNS, ya que **permiten separar lógicamente la gestión de dominio DNS**.

¿Qué es una zona DNS?

Una zona DNS aloja la totalidad o una porción de un dominio y sus subdominios. Los subdominios pueden pertenecer a la zona con sus padres o se pueden delegar en otra zona.

Los datos de una zona se pueden replicar en más de un servidor. Esto añade **redundancia a una zona** porque la información necesaria para encontrar recursos en la zona se encuentra en dos o más servidores**. El nivel de redundancia que se necesita** es una razón para crear zonas. Si usted tiene una zona que aloja registros sobre recursos críticos del servidor, es probable que esta zona tendrá una mayor nivel de redundancia que una zona en la que no existan datos críticos.

Los datos de una zona se mantienen en un servidor DNS y se almacenan de una de estas dos maneras:

- En un archivo en la zona que contiene una relación de listas.
- Integrado en Active Directory.

Un servidor DNS es autoritativo para la zona **si es sede los registros de los recursos y de las direcciones de los clientes que solicitan el archivo**.

Tipos de zonas DNS

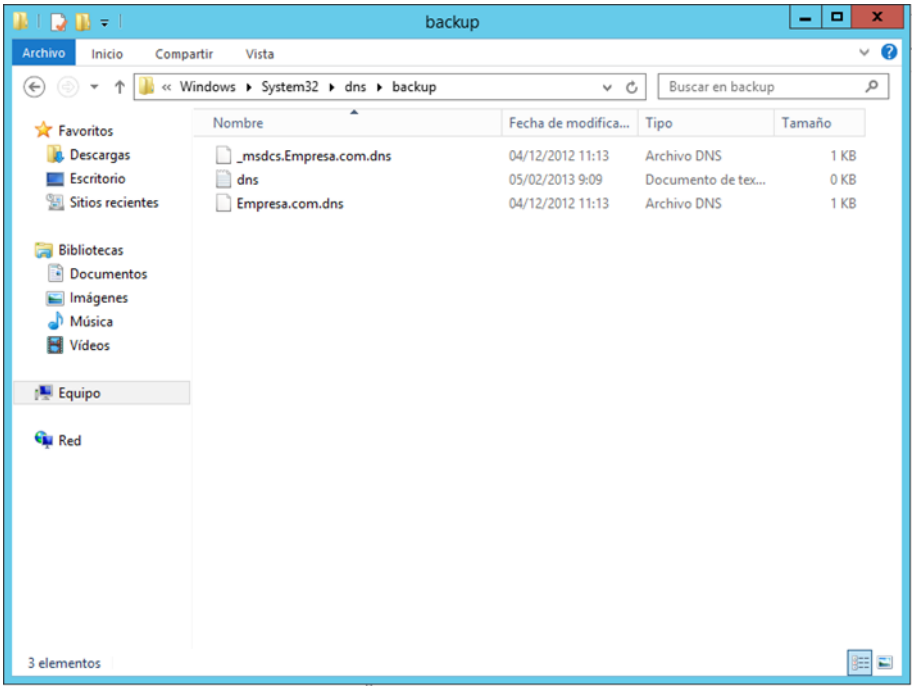
Existente cuatro **tipos de zonas DNS**:

- Principal.
- Secundaria.
- Rutas internas.
- Integrada con Active Directory.

©InterGrupo 2013

Zona principal

Cuando una zona es principal, **el servidor DNS es la fuente principal de información sobre esta zona,** y almacena la copia maestra de los datos de la zona en un archivo local o en Active Directory. Cuando el servidor DNS almacena la zona en un archivo, el archivo de la zona principal tiene de nombre predeterminado "**Nombre_zona.dns**" y se encuentra en la ruta "**Windows\System32\DNS\Backup**" en el servidor. Cuando la zona no se almacena en Active Directory, el servidor DNS que aloja la zona principal es el único servidor DNS que tiene una copia modificable del archivo de la zona.



Archivo de la zona principal

Zona secundaria

Cuando una zona es secundaria, **el servidor DNS es una fuente secundaria de información de la zona**. La zona en este servidor debe ser obtenida de otro servidor DNS remoto que también alberga esta zona. Este servidor DNS debe **tener acceso de red al servidor DNS remoto** para recibir la información actualizada de la zona. Debido a que una zona secundaria es una copia de una zona principal, **no se puede almacenar en Active Directory**. Las zonas secundarias pueden ser útiles si usted replica datos de zonas DNS que no se encuentren en Windows o estén ejecutando DNS en los servidores que no son controladores del dominio de Active Directory.

Zona de rutas internas

Windows Server 2003 introdujo las zonas de rutas, que r**esuelven varios problemas con grandes espacios de nombres DNS y bosques con varios árboles**. Un bosque de árboles múltiples es un bosque de Active Directory que contiene dos diferentes dominios de nivel superior.

©InterGrupo 2013

Active Directory integrada en las zonas

Si Active Directory almacena la zona, DNS puede tomar ventaja del modelo de replicación con múltiples maestros para reproducir la zona principal. Esto le permite editar los datos de zona en cualquier servidor DNS. Windows Server 2012 introdujo un nuevo concepto llamado controlador de dominio de solo lectura (**RODC**)**. Con Active Directory integrada en las zonas se puede replicar en los controladores de dominio**, **incluso si la función DNS no está instalada** en el controlador de dominio. Si el servidor es un controlador de dominio de sólo lectura, el proceso local no puede escribir los datos.

¿Qué son las zonas de búsqueda directa e inversa?

Hay dos tipos de zonas de búsquedas, conocidas **como búsqueda directa o hacia adelante**, y **búsqueda inversa o hacia atrás**.

Zonas de búsqueda directa

La zona de búsqueda directa **resuelve los nombres de host en direcciones IP y albergan los registros de recursos comunes**: A, CNAME, SRV, MX, SOA, TXT y NS.

Zonas de búsqueda inversa

La zona de búsqueda inversa **resuelve una dirección IP a un nombre de dominio, y albergan los registros:** SOA, NS y PTR.

Las funciones de la zona de búsqueda inversa son las mismas que la zona de búsqueda directa, pero la dirección IP es la parte de la consulta y el nombre de host es la información devuelta. **Las zonas de búsqueda inversa no siempre se configuran, pero es recomendable** que usted las configure para reducir las advertencias y mensajes de error. Muchos protocolos estándar de internet se basan en datos de la zona de búsqueda inversa para validar la información de la zona de búsqueda directa. Por ejemplo, si la búsqueda directa indica que Empresa.com se resuelve en 192.168.0.250, puede utilizar una búsqueda inversa para confirmar que la dirección 192.168.0.250 está asociada a Empresa.com.

Muchas puertas de enlace de seguridad de correo electrónico utilizan búsquedas inversas para validar que la dirección IP que está enviando mensajes se asocia a un dominio.

Descripción general de las zonas de rutas internas

Una zona de rutas internas es una copia replicada de una zona que sólo contiene los registros de recursos necesarios para identificar los servidores con autoridad de esa zona DNS. Una zona de rutas internas resuelve los nombres de espacios de nombres DNS. **Una zona de rutas consiste** en lo siguiente:

- La zona delegada del registro de recursos **SOA**, los registros **NS** y **los registros de recursos**.

©InterGrupo 2013

- **La dirección IP de uno o más servidores maestros** que se puedan utilizar para actualizar la zona de rutas internas.

Los servidores maestros de una zona de rutas internas son uno o más servidores DNS que tienen autoridad para la zona secundaria, normalmente el servidor DNS que aloja la zona principal para el nombre de dominio delegado.

Resolución de una zona de rutas internas

Cuando un servidor DNS realiza una operación de consulta recursiva a un servidor DNS que aloja una zona de rutas internas, **el servidor DNS utiliza los registros de recursos en la zona de rutas para resolver la consulta**. El servidor DNS envía una consulta iterativa a los servidores DNS autorizados.

El servidor DNS almacenará los registros de recursos que recibe de los servidores DNS autorizados de una zona de rutas internas en sus listas de cache, pero no va a almacenar estos registros de recurso en la zona de rutas internas en sí. Sólo el SOA, NS y los registros de los recursos devueltos en la respuesta de la consulta se almacenan en la zona de rutas internas.

Si la consulta es una consulta iterativa, **el servidor DNS devuelve una referencia que contiene los servidores de las zonas de rutas internas específicas**.

Comunicación entre los servidores DNS que alojan padre y las zonas hijo

Un servidor DNS que delega un dominio a una zona secundaria en otro servidor DNS está al tanto de los nuevos servidores DNS autorizados para la zona secundaria. Esto es un proceso manual que requiere de los administradores de los servidores para que **los servidores DNS se comuniquen**. Las zonas de ruta internas habilitan un servidor DNS que aloja una zona de rutas interna para uno de sus dominios delegados para obtener las actualizaciones de los servidores DNS autorizados. **La actualización se realiza desde el servidor DNS que aloja la zona de ruta internas** y el administrador del servidor DNS que aloja la zona hijo que tiene que ser contactada.

Contrastes zona de rutas internas y reenviadores condicionales

Puede haber cierta confusión acerca de **cuándo utilizar reenviadores condicionales en lugar de zonas de rutas internas**. Eso se debe a que dos características permiten responde a una preguntar. Sin embargo, **estos valores tienen propósitos diferentes:**

- **Un reenviador condicional** se configuraren el servidor DNS para reenviar una consulta que recibe, dependiendo del nombre DNS que contiene la consulta.
- **Una zona de rutas internas** mantiene el servidor DNS que aloja una zona principal al tanto de todos los servidores DNS que tienen autoridad para una zona secundaria.

©InterGrupo 2013

Cuando utilizar reenviadores condicionales

Si desea que los clientes DNS en redes separadas resuelvan los nombres de los demás sin tener que consultar servidores DNS de internet, debe **configurar los servidores DNS de la red para renviar las consultas de nombres en la red**. Los servidores DNS en una red enviarán los nombres de los clientes a un servidor DNS específico de otra red que construirá una caché de información general acerca de la otra red. Esto le permite **crear un punto de contacto directo entre las dos redes de servidores DNS**, lo que reduce la necesidad de recursividad.

Las zonas de rutas no proporcionan el mismo beneficio que el servidor – servidor. Esto se debe a que un servidor DNS que aloja una zona de rutas en una red, responde a las consultas de nombres en la otra red con una lista de todos los servidores DNS autorizados para la zona con ese nombre, en lugar de los servidores DNS específicos que haya designado para manejar este tráfico. Esta configuración complica la seguridad que desea establecer entre los servidores DNS.

Cuando utilizar zonas de rutas internas

Utilice las zonas de rutas internas cuando **desee que un servidor DNS permanezca al tanto de los servidores DNS autorizados para una zona exterior**.

Un reenviador condicional no es una forma eficaz de mantener un servidor DNS que aloja una zona principal **al tanto de lo servidores autorizados para una zona secundaria.** Esto se debe a que cada vez que aparece un servidor DNS autorizado, hay que configurar el reenviador condicional de manera manual en el servidor DNS que aloja la zona principal. En concreto, debe actualizar la dirección IP para cada nuevo servidor DNS autorizado para la zona infantil.

Delegación zona DNS

DNS es un sistema jerárquico, y la delegación de zonas DNS conecta niveles.

Al decidir si se debe dividir el espacio de nombres DNS para zonas adicionales, considere las siguientes **razones**:

- Es necesario **delegar la gestión de una parte del espacio de nombres DNS** a otro lugar de la organización o departamento.
- Es necesario **dividir una gran zona** en zonas más pequeñas para que pueda distribuir las cargas de tráfico entre varios servidores. Esto mejora la resolución de nombres DNS, y crea un entorno más tolerante a fallos.
- Es necesario **ampliar el espacio de nombres** al agregar numerosos subdominios inmediatamente para dar cabida a la apertura de una nueva sucursal o sitio.

©InterGrupo 2013

Creación de una zona de rutas de internas

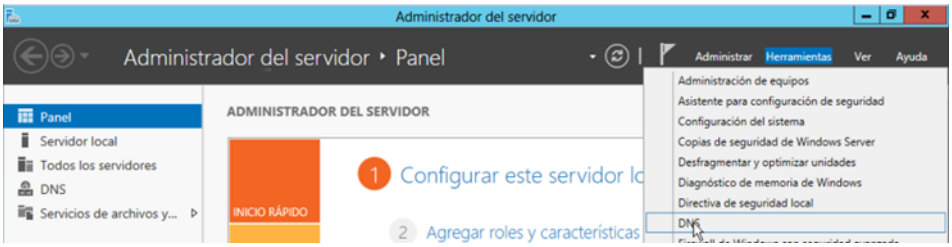
Se creará una **zona de rutas internas.** Para ellos se utilizará una máquina virtual con un **Windows Server 2012** instalado, denominado **Server2012P2**, que se encuentra en el dominio **Empresa.com**, y que tiene instalado el rol **Servicio DNS.**

Se replicará la zona de búsqueda directa **Empresa.com**, del Server2012, que durante todo este proceso debe estar **encendido y en funcionamiento**.

En el **Server2012P2,** haga clic en el icono del "**Administrador del servidor**" que se encuentra en la barra de acceso rápido, en la parte inferior de la pantalla.

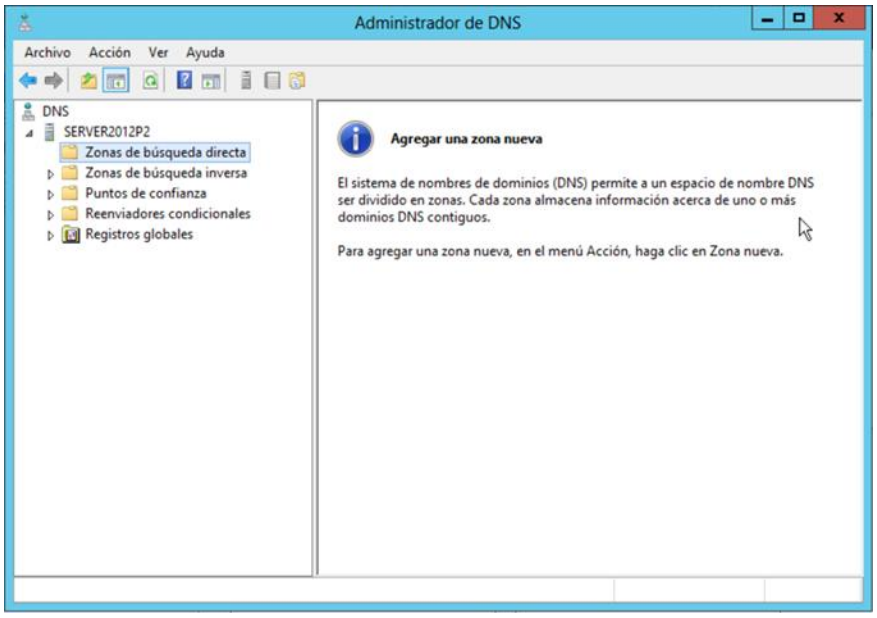
Icono del Administrador del servidor

Aparecerá la consola del "**Administrador del servidor**". Haga clic en el apartado "**Herramientas**", que se encuentra en la parte superior derecha de la consola. De la lista desplegable seleccione "**DNS**".



Administrador del servidor / DNS

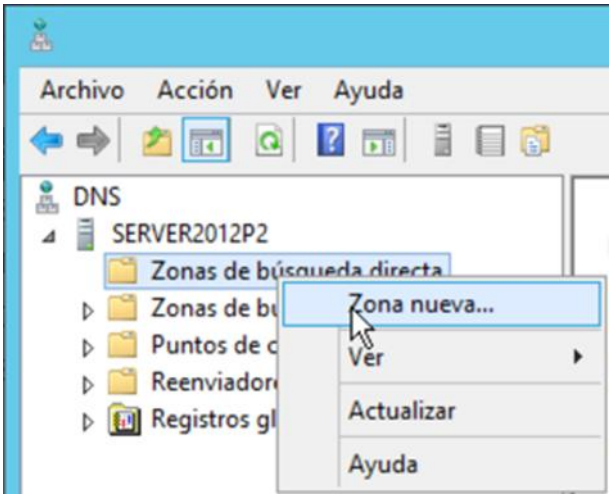
Aparecerá la consola del "**Administrador de DNS**".



Administrador de DNS

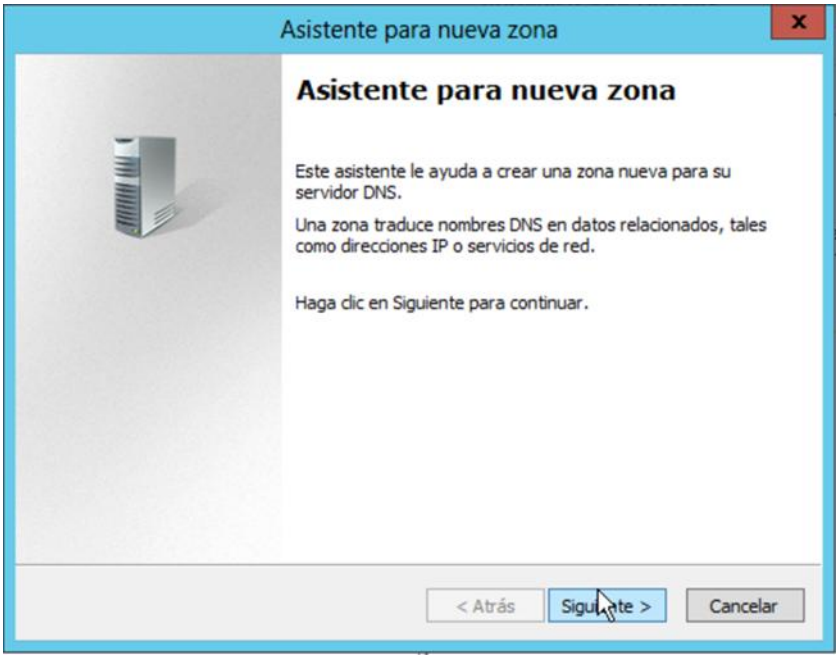
©InterGrupo 2013

Haga clic con el botón derecho sobre "**Zona nueva**" para agregar una zona que replicar.



Zona nueva

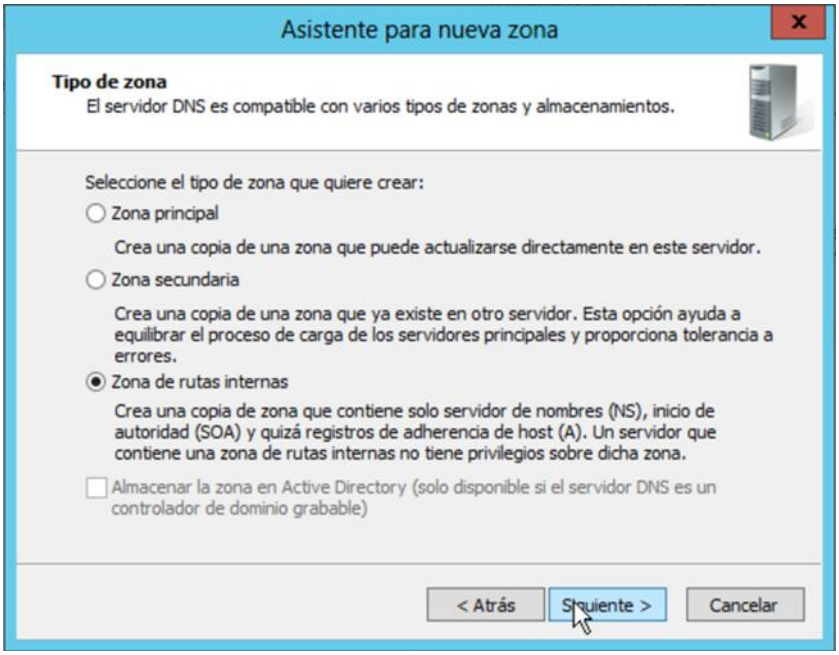
Aparecerá el "**Asistente para nueva zona**". En la página de bienvenida aparecerá información acerca las zonas. Haga clic en "**Siguiente**".



Asistente para nueva zona

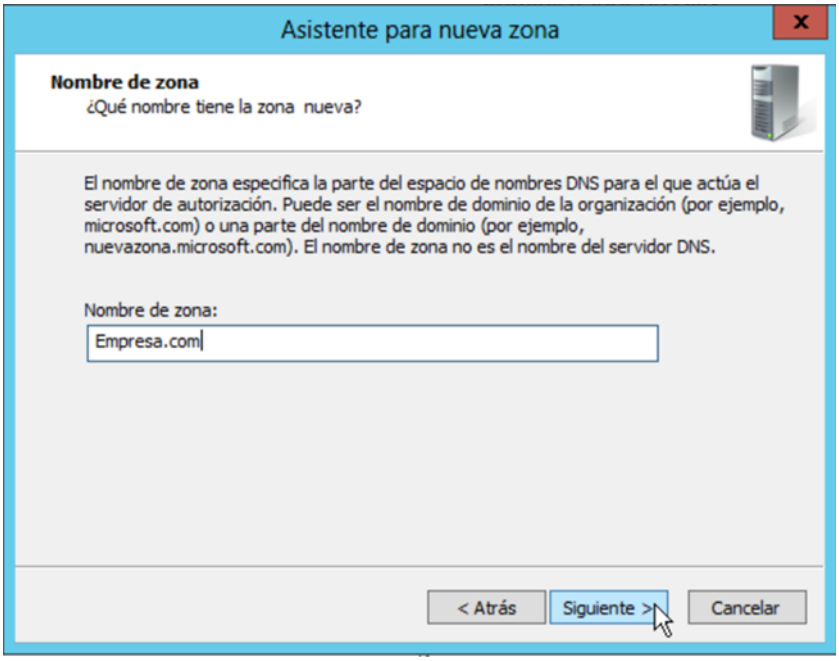
©InterGrupo 2013

Aparecerá la pantalla "**Asistente para nueva zona**". Debe seleccionar que tipo de zona va a crear. En este caso, seleccione "**Zonas de rutas internas**", para poder replicar los datos de la zona Empresa.com. Haga clic en "**Siguiente.**"



Tipo de zona

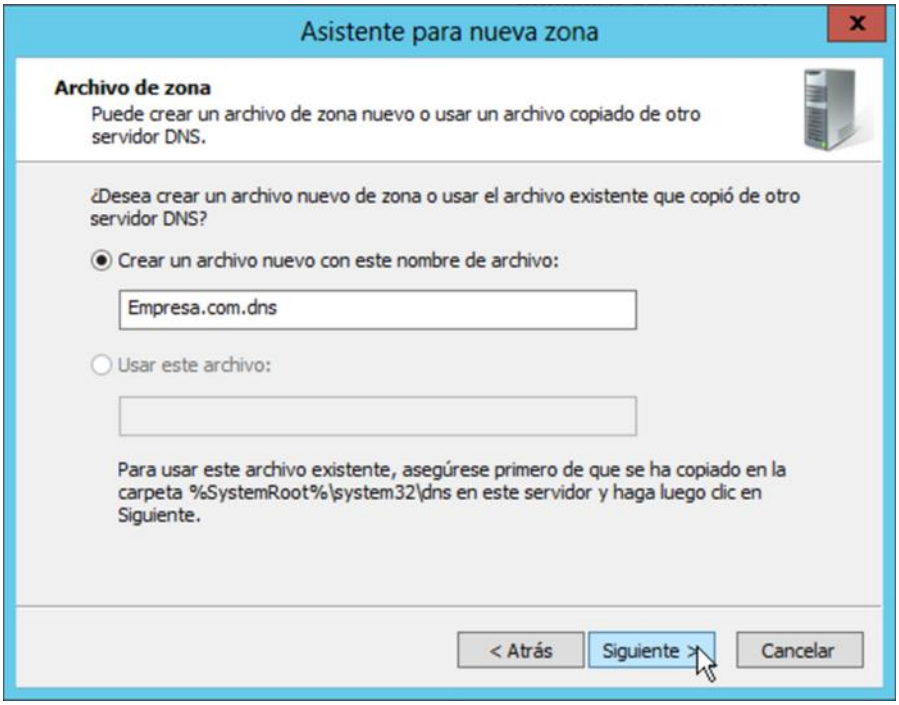
Aparecerá la pantalla "**Nombre de zona**". Introduzca "**Empresa.com**" en el cuadro de texto "**Nombre de zona**". Haga clic en "**Siguiente**".



Nombre de zona

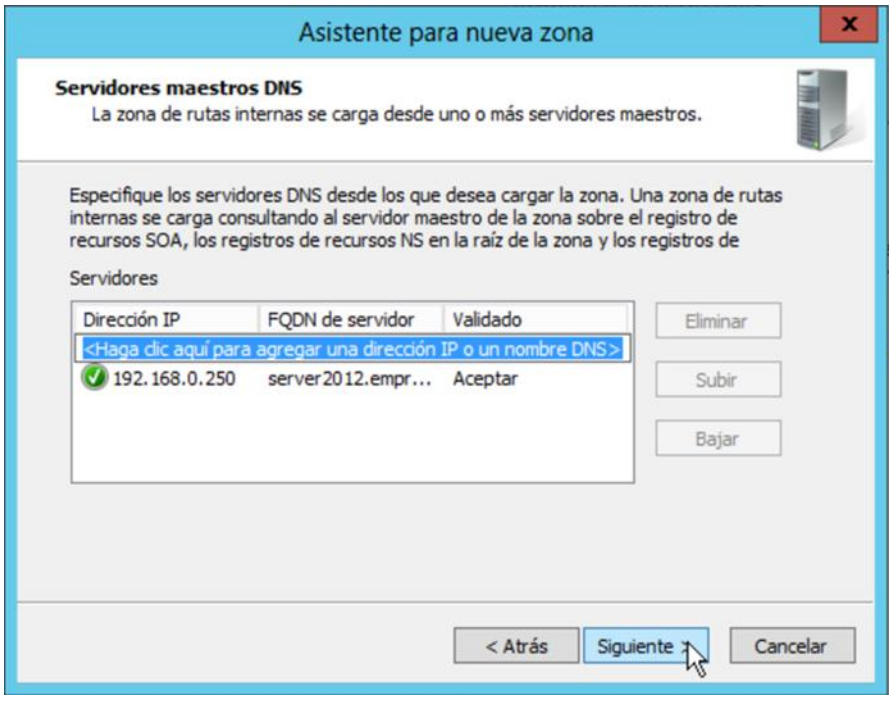
©InterGrupo 2013

Aparecerá la pantalla "**Archivo de zona**". Deje el valor predeterminado en el cuadro "**Crear un archivo nuevo con este nombre**" y haga clic en "**Siguiente**".



Archivo de zona

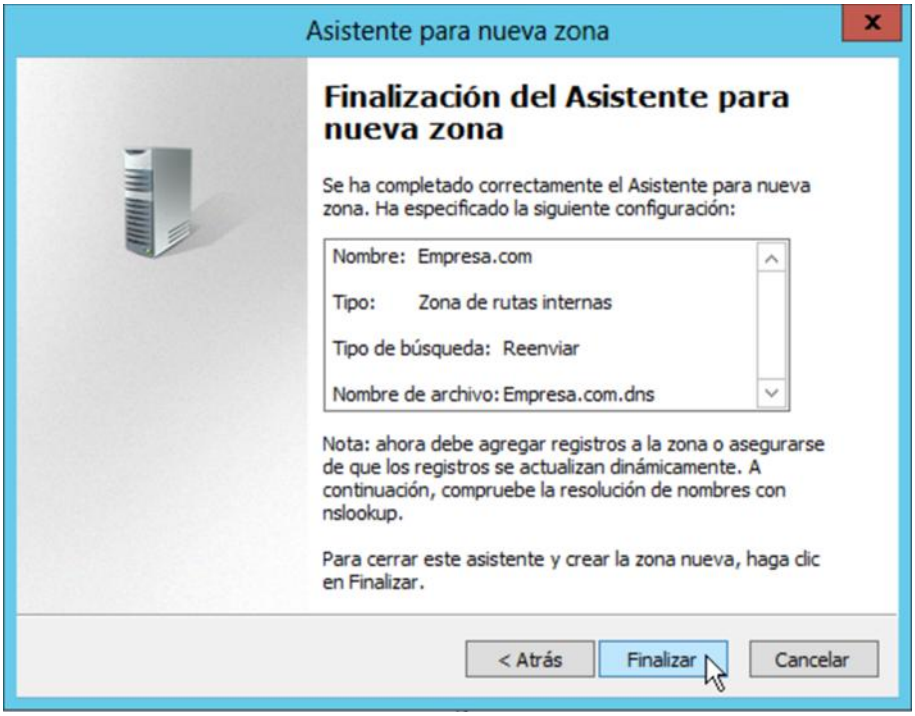
En la siguiente pantalla, "**Servidores maestros DNS**", debe introducir la IP del servidor DNS del que va a recoger los datos. En este caso, introduzca "**192.168.0.250**". Espere a que aparezca el **tic verde** para comprobar que la conexión esta correcta y haga clic en "**Siguiente**".



Servidores maestros DNS

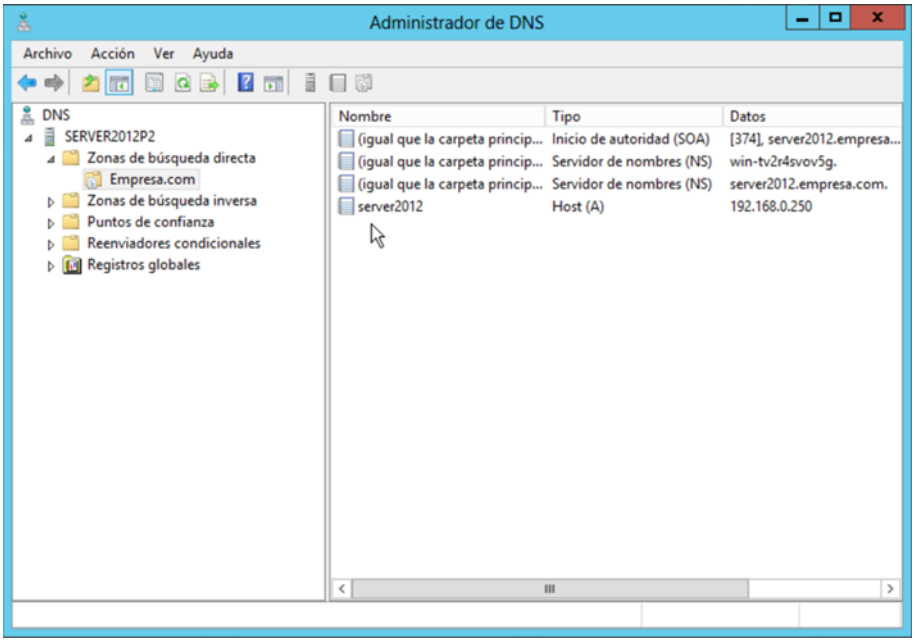
©InterGrupo 2013

Por último, aparecerá la página de "**Finalización del Asistente para nueva zona**". Compruebe que todo está correcto y haga clic en "**Finalizar**". La nueva zona de rutas internas estará creada.



Finalización del asistente

Compruebe que la zona se ha replicado correctamente.



Administrador de DNS / Zona replicada

©InterGrupo 2013

Configuración de transferencias de zona DNS

Las transferencias de zona DNS determinan cómo la infraestructura DNS se mueve de un servidor a otro. Sin las transferencias de zona, los servidores en su organización tendrían copias diferentes de los de la zona. Usted debe considerar que la zona contiene datos sensibles, y es importante **asegurar las transferencias de la zona**.

¿Qué es una transferencia de zona DNS?

Una transferencia de zona se produce **cuando se duplica la zona DNS que se encuentra en un servidor, a otro servidor DNS**.

Las transferencias de zona sincronizan las zonas DNS primaria y secundaria del servidor. Así es como DNS construye su resistencia en internet. Es importante que las zonas DNS se mantengan actualizadas. Las discrepancias en las zonas primaria y secundaria pueden causar interrupciones del servicio y provocar que los nombres de host se resuelvan incorrectamente.

Las transferencias de zona pueden ser de tres maneras:

- **Transferencia de zona completa**: Una transferencia de zona completa se produce cuando se copia toda la zona de un servidor DNS a otro. Una transferencia de zona completa se conoce como una transferencia de toda la zona (**AXFR**).
- **Transferencia de zona incremental**: Una transferencia de zona incremental se produce cuando hay una actualización del servidor DNS y sólo los registros de recursos que se han modificado se replican en el servidor. Se trata de una transferencia de zona incremental (**IXFR**).
- **Transferencia rápida**: Una transferencia rápida es un tipo de transferencia de zona que utiliza la compresión y envía varios registros de recursos en cada transmisión.

No todas las implementaciones del servidor DNS admiten transferencias de zonas incremental y rápida. Cuando se integra un servidor DNS de Windows Server 2012 con un dominio BIND del servidor DNS, debe asegurarse de que las características que usted necesita son compatibles con la versión BIND que está instalando.

Las zonas integradas en Active Directory replican mediante el uso de varios maestros de replicación de Active Directory, en lugar de utilizar el proceso de transferencia de zona. Esto significa que cualquier controlador de dominio estándar que tenga la función de DNS, puede actualizar la información de zona DNS, que luego se replica en todos los servidores DNS que alojan la zona.

©InterGrupo 2013

Notificación DNS

Un servidor maestro utiliza la notificación DNS para alertar a sus servidores secundarios que las actualizaciones de la zona están disponibles. Los servidores secundarios piden a su maestro las actualizaciones**. Es muy útil en un entorno sensible al tiempo**, donde la precisión de los datos es importante.

Configuración de seguridad de la zona de transferencia

Una zona proporciona datos sobre la organización, por lo que se debe tomar precauciones para **asegurarse de que está protegida** contra el acceso de usuarios malintencionados, y que no se puede sobrescribir con datos erróneos, que se conoce como **envenenamiento DNS**. Una forma de proteger la infraestructura de DNS es **garantizar las transferencias de zona.**

En la ventana "**Propiedades**" de la zona, en la pestaña "**Transferencias de zona**", puede especificar la lista de servidores DNS autorizados. Por defecto, las transferencias de zona están deshabilitadas.

©InterGrupo 2013

Resumen

- Se ha explicado los distintos tipos de zona DNS.
- Se ha explicado cómo crear zonas.
- Se ha creado una zona de rutas internas.
- Se ha explicado las transferencias de zonas DNS.

©InterGrupo 2013