



IBM i

Redes

Sistema de nombres de dominio (DNS)

Versión 7.2





IBM i

Redes

Sistema de nombres de dominio (DNS)

Versión 7.2

Aviso

Antes de utilizar esta información y el producto al que hace referencia, lea la información que figura en el apartado “Avisos” en la página 53.

Esta edición se aplica a IBM i 7.2 (número de producto 5770-SS1) y a todos los releases y modificaciones subsiguientes hasta que se indique lo contrario en nuevas ediciones. Esta versión no se ejecuta en todos los modelos de sistema con conjunto reducido de instrucciones (RISC) ni tampoco se ejecutan en los modelos CISC.

Este documento puede contener referencias al código interno bajo licencia. El código interno bajo licencia es código de máquina cuya licencia se obtiene bajo los términos del Acuerdo de licencia de IBM para código de máquina.

© Copyright IBM Corporation 1998, 2014.

Contenido

Sistema de nombres de dominio (DNS)	1
Novedades de IBM i 7.2	1
Archivo PDF de Sistema de nombres de dominio (DNS)	2
Conceptos sobre el sistema de nombres de dominio (DNS)	2
Qué son las zonas	3
Qué son las consultas al sistema de nombres de dominio (DNS)	4
Configuración del dominio del sistema de nombres de dominio (DNS)	6
Actualizaciones dinámicas	6
Características de BIND 9	8
Registros de recursos del sistema de nombres de dominio (DNS)	10
Registros de correo y de intercambiador de correo (MX)	14
Introducción a las Extensiones de seguridad de DNS (DNSSEC)	15
Ejemplos: sistema de nombres de dominio (DNS)	16
Ejemplo: un único servidor de sistema de nombres de dominio (DNS) para una intranet	16
Ejemplo: un único servidor de sistema de nombres de dominio (DNS) con acceso a Internet	18
Ejemplo: un sistema de nombres de dominio (DNS) y el protocolo de configuración dinámica de hosts (DHCP) en el mismo IBM i	20
Ejemplo: dividir el DNS por el cortafuegos configurando dos servidores DNS en el mismo IBM i	22
Ejemplo: dividir el DNS a través de un cortafuegos, utilizando una vista	24
Elaborar un plan para el sistema de nombres de dominio (DNS)	26
Determinar las autorizaciones del sistema de nombres de dominio (DNS)	26
Determinar la estructura del dominio	27
Planificar medidas de seguridad	27
Requisitos del sistema de nombres de dominio (DNS)	28
Determinar si el sistema de nombres de dominio (DNS) está instalado	29
Instalar el sistema de nombres de dominio (DNS)	29
Configurar el sistema de nombres de dominio (DNS)	29
Acceder al sistema de nombres de dominio (DNS) en IBM Navigator for i	30
Configurar servidores de nombres	30
Crear una instancia del servidor de nombres	30
Editar las propiedades del servidor de sistema de nombres de dominio (DNS)	31
Configurar zonas en un servidor de nombres	31
Configurar vistas en un servidor de nombres	32
Configurar el sistema de nombres de dominio (DNS) para que reciba actualizaciones dinámicas	32
Configurar DNSSEC	33

Configurar claves de confianza/claves gestionadas	33
Configurar las opciones de DNSSEC	33
Firmar una zona primaria	34
Volver a firmar una zona primaria	34
Retirar la firma de una zona primaria	34
Configurar DNSSEC para una zona dinámica	34
Configurar la opción allow-update	35
Configurar la opción update-policy	35
Configurar la opción auto-dnssec	35
Importar archivos del sistema de nombres de dominio (DNS)	35
Validación de registros	36
Acceder a los datos de un sistema de nombres de dominio (DNS) externo	36
Gestionar el sistema de nombres de dominio (DNS)	37
Verificar el funcionamiento de la función del sistema de nombres de dominio (DNS)	37
Gestionar las claves de seguridad	38
Gestionar las claves del sistema de nombres de dominio (DNS)	38
Gestionar claves de actualización dinámica	38
Efectuar actualizaciones manuales en una zona dinámica	39
Gestionar DNSSEC	40
Verificar el funcionamiento de la función DNSSEC	40
Volver a firmar una zona	40
Consideración sobre la renovación de claves	41
Gestionar DNSSEC para una zona dinámica	41
Acceder a las estadísticas del servidor de sistema de nombres de dominio (DNS)	42
Acceder a las estadísticas del servidor	42
Acceder a una base de datos del servidor activo	43
Mantener los archivos de configuración del sistema de nombres de dominio (DNS)	43
Características avanzadas del sistema de nombres de dominio (DNS)	46
Iniciar o detener servidores de sistema de nombres de dominio (DNS)	47
Cambiar los valores de depuración	47
Resolución de problemas relacionados con el sistema de nombres de dominio (DNS)	47
Anotar mensajes del servidor de sistema de nombres de dominio (DNS)	48
Cambiar los valores de depuración del sistema de nombres de dominio (DNS)	50
Información relacionada con el sistema de nombres de dominio (DNS)	51

Avisos	53
Información de la interfaz de programación	55
Marcas registradas	55
Terms and conditions	55

Sistema de nombres de dominio (DNS)

Sistema de nombres de dominio (DNS) es un sistema de bases de datos distribuidas que permite gestionar los nombres de host y las direcciones de protocolo de Internet (IP) asociadas a ellos.

Con el DNS, la gente puede utilizar nombres simples (como `www.jkltoys.com`) para localizar un host, en lugar de tener que utilizar las direcciones IP (por ejemplo, `192.168.12.88` en IPv4, o `2001:D88::1` en IPv6). Un único servidor solo se puede encargar de conocer los nombres de host y las direcciones IP de una pequeña parte de una zona, pero los servidores DNS pueden colaborar entre sí para correlacionar todos los nombres de dominio con sus direcciones IP. Los servidores DNS que colaboran entre sí permiten que los sistemas se comuniquen por Internet.

En IBM® i 7.2, los servicios de DNS se basan en la implementación de DNS de estándar industrial, conocida como Berkeley Internet Name Domain (BIND) versión 9. En los releases anteriores de IBM i, los servicios de DNS se basaban en la versión anterior de BIND 9 o BIND 8. Para utilizar el nuevo servidor DNS de BIND versión 9 DNS en V7R2, debe tener instalados IBM i opción 31 (DNS) y opción 33 (Portable Application Solutions Environment (PASE)) y 5733-SC1 opción 1 (OpenSSH, OpenSSL, zlib) en IBM i. Por razones de seguridad, a partir de IBM i V6R1, BIND 4 y 8 se han sustituido por BIND 9. Por tanto, es necesaria la migración a BIND 9 para el servidor DNS.

Novedades de IBM i 7.2

Aquí encontrará la información nueva o la que ha cambiado sustancialmente en el temario Sistema de nombres de dominio (DNS).

DNS for i5/OS® da soporte a DNSSEC en este release. Se han añadido nuevos mandatos y opciones de configuración.

Nuevos mandatos de DNSSEC

Se han añadido los mandatos siguientes para la configuración y mantenimiento de DNSSEC.

Generar clave DNSSEC (GENDNSKEY)

El mandato Generar clave DNS (GENDNSKEY) genera claves para DNSSEC (DNS seguro) según lo definido en la RFC 2535 y la RFC 4034. También genera claves que se utilizan en TSIG (firmas de transacción) según lo definido en la RFC 2845, o TKEY (clave de transacción) según lo definido en la RFC 2930. De forma predeterminada, los archivos generados se almacenarán en el directorio /QIBM/UserData/OS400/DNS/_DYN.

Añadir firma DNSSEC (ADDDNSSIG)

El mandato Añadir firma DNS (ADDDNSSIG) firma una zona. Genera registros NSEC y RRSIG y produce una versión firmada de la zona. El estado de seguridad de las delegaciones de la zona firmada (es decir, si las zonas hijas son seguras o no) queda determinado por la presencia o ausencia de un archivo de conjunto de claves para cada zona hija.

Generar RR DS de DNSSEC (GENDNSDSRR)

El mandato Generar RR DS de DNSSEC (GENDNSDSRR) genera el registro de recurso (RR) de firmante de delegación (DS).

Establecer bit REVOKE de DNSSEC (SETDNSRVK)

El mandato Establecer bit REVOKE de DNSSEC (SETDNSRVK) lee un archivo de claves DNSSEC, establece el bit REVOKED en la clave y crea un nuevo par de archivos de claves que contiene la clave ahora revocada (now-revoked).

Mandatos de configuración nuevos

Se han añadido los mandatos siguientes para crear la configuración de DDNS e imprimir el contenido de un archivo de diario de zona.

Crear configuración DDNS (CRTDDNSCFG)

El mandato Crear configuración DDNS (**CRTDDNSCFG**) genera una clave utilizada por el mandato NSUPDATE y el servidor DNS dinámico (DDNS). Simplifica la configuración de zonas dinámicas generando una clave y suministrando el mandato NSUPDATE y la sintaxis de named.conf que será necesaria para utilizarlo, incluido un ejemplo de sentencia update-policy. Tenga en cuenta que el propio servidor DNS puede configurar una clave DDNS local para utilizarla con NSUPDATE LOCALHOST(*YES). Este mandato sólo es necesario cuando se requiere una configuración más elaborada: por ejemplo, si debe utilizarse NSUPDATE desde un sistema remoto.

Volver archivo de diario de DNS (DMPDNSJRN)

El mandato Volcar archivo de diario de DNS (**DMPDNSJRN**) vuelca el contenido de un archivo de diario de zona en un formato legible por el usuario.

Conceptos relacionados:

“Introducción a las Extensiones de seguridad de DNS (DNSSEC)” en la página 15
DNSSEC es un conjunto de especificaciones RFC IETF que añaden ampliaciones de seguridad a DNS.

Archivo PDF de Sistema de nombres de dominio (DNS)

Puede ver e imprimir un archivo PDF de esta información.


Para ver o descargar la versión PDF de este documento, seleccione Sistema de nombres de dominio (DNS) (alrededor de 625 KB).

Cómo guardar los archivos PDF

Si desea guardar un archivo PDF en su estación de trabajo para verlo o imprimirlo:

1. En el navegador, pulse el enlace del PDF con el botón derecho del ratón.
2. Pulse la opción destinada a guardar el PDF localmente.
3. Navegue hasta el directorio en el que desea guardar el archivo PDF.
4. Pulse **Guardar**.

Cómo descargar Adobe Reader

Para poder ver o imprimir estos archivos PDF, debe instalar Adobe en su sistema. Puede descargar una copia gratuita desde el sitio Web de Adobe (www.adobe.com/products/acrobat/readstep.html) .

Referencia relacionada:

“Información relacionada con el sistema de nombres de dominio (DNS)” en la página 51
Publicaciones IBM Redbooks, sitios Web y otros temarios de Information Center con información relacionada con el temario Sistema de nombres de dominio (DNS). Puede ver o imprimir cualquiera de los archivos PDF.

Conceptos sobre el sistema de nombres de dominio (DNS)

El sistema de nombres de dominio (DNS) es un sistema de bases de datos distribuidas que permite gestionar los nombres de host y las direcciones de protocolo de Internet (IP) asociadas a ellos. Con el DNS, puede utilizar nombres simples (como www.jkltoys.com) para localizar un host, en lugar de tener que utilizar las direcciones IP (por ejemplo, 192.168.12.88 en IPv4, o 2001:D88::1 en IPv6).

Un único servidor solo se puede encargar de conocer los nombres de host y las direcciones IP de una pequeña parte de una zona, pero los servidores DNS pueden colaborar entre sí para correlacionar todos los nombres de dominio con sus direcciones IP. Los servidores DNS que colaboran entre sí permiten que los sistemas se comuniquen por Internet.

Los datos de DNS se bifurcan en una jerarquía de dominios. Los servidores son responsables de conocer únicamente una parte pequeña de los datos, por ejemplo, un único subdominio. La parte de un dominio de la que el servidor es directamente responsable se denomina zona. Un servidor DNS que tenga la información y los datos de hosts completos de una zona tiene autoridad sobre la zona. Este tipo de servidor puede responder a las consultas sobre hosts de su zona mediante sus propios registros de recursos. El proceso de consulta depende de una serie de factores. En el tema Qué son las consultas DNS se explican los pasos que un cliente puede realizar para resolver una consulta.

Qué son las zonas

Los datos del sistema de nombres de dominio (DNS) se dividen en conjuntos gestionables de datos llamados *zonas*. Y cada uno de estos conjuntos corresponde a un tipo de zona concreto.

Las zonas contienen información sobre nombres y direcciones IP acerca de una o más partes de un dominio DNS. El servidor que contiene toda la información de una zona se considera el servidor autorizador del dominio, llamado *zona padre*. A veces conviene delegar la autorización para responder a las consultas de DNS de un subdominio determinado a otro servidor DNS, que se llama *zona hija*. En tal caso, el servidor DNS del dominio puede configurarse de tal forma que las consultas del subdominio se remitan al servidor apropiado.

Por cuestión de seguridad y redundancia, los datos de zona suelen almacenarse en servidores que no sean el servidor DNS autorizador. Estos otros servidores se denominan servidores secundarios, que cargan los datos de zona del servidor autorizador. Si se configuran servidores secundarios, podrá equilibrar la demanda de servidores, y proporciona también una copia de seguridad en caso de que el servidor primario no esté operativo. Los servidores secundarios obtienen los datos de zona mediante transferencias de zona desde el servidor autorizador. Cuando se inicializa un servidor secundario, este carga una copia completa de los datos de zona del servidor primario. El servidor secundario también vuelve a cargar los datos de zona del servidor primario o de otros servidores secundarios de ese dominio cuando los datos de zona se modifican.

Tipos de zonas DNS

Puede utilizar el DNS de IBM i para definir varios tipos de zonas que le ayuden a gestionar los datos del DNS:

Zona primaria

La zona primaria carga los datos de zona directamente a partir de un archivo de un host. Puede contener una subzona o zona hija. También puede contener registros de recursos, como los registros de host, de alias (CNAME), de dirección IPv4 (A), de dirección IPv6 (AAAA) o de puntero de correlación inversa (PTR).

Nota: Las zonas primarias se denominan en ocasiones *zonas maestras* en la documentación adicional sobre BIND.

Subzona

La subzona es una zona que se encuentra dentro de la zona primaria. Las subzonas permiten organizar los datos de zona en cantidades más manejables.

Zona hija

La zona hija es una subzona que delega la responsabilidad sobre los datos de la subzona a uno o más servidores de nombres.

Alias (CNAME)

El alias es un nombre alternativo para el nombre del dominio primario.

Host El objeto host correlaciona los registros A y PTR con un host. Puede haber registros de recursos adicionales asociados a un host.

Zona secundaria

La zona secundaria carga los datos de zona desde el servidor primario de una zona o desde otro servidor secundario. Mantiene una copia completa de la zona a la que pertenece.

Nota: Las zonas secundarias se denominan en ocasiones *zonas esclavas* en la documentación adicional sobre BIND.

Zona apéndice

La zona apéndice es similar a una zona secundaria, pero solo transfiere los registros del servidor de nombres (NS) de dicha zona.

Zona de reenvío

La zona de reenvío dirige todas las consultas de esa zona concreta a otros servidores.

Conceptos relacionados:

“Qué son las consultas al sistema de nombres de dominio (DNS)”

Los clientes del sistema de nombres de dominio (DNS) emplean servidores DNS para resolver consultas. Las consultas pueden proceder directamente del cliente o de una aplicación que se ejecute en el cliente.

Tareas relacionadas:

“Configurar zonas en un servidor de nombres” en la página 31

Después de configurar una instancia de servidor el sistema de nombres de dominio (DNS), debe configurar las zonas para el servidor de nombres.

Referencia relacionada:

“Ejemplo: un único servidor de sistema de nombres de dominio (DNS) para una intranet” en la página 16
Este ejemplo describe una subred simple con un servidor de sistema de nombres de dominio (DNS) para uso interno.

“Registros de recursos del sistema de nombres de dominio (DNS)” en la página 10

Los registros de recursos se utilizan para almacenar datos sobre nombres de dominio y direcciones IP. Puede utilizar la tabla de búsqueda de registros de recursos para buscar los registros de recursos soportados para el sistema operativo IBM i.

Qué son las consultas al sistema de nombres de dominio (DNS)

Los clientes del sistema de nombres de dominio (DNS) emplean servidores DNS para resolver consultas. Las consultas pueden proceder directamente del cliente o de una aplicación que se ejecute en el cliente.

El cliente envía un mensaje de consulta al servidor DNS que contiene un nombre de dominio totalmente calificado (FQDN), un tipo de consulta (por ejemplo, un registro de recurso concreto que el cliente necesite) y la clase del nombre del dominio, que suele ser la clase Internet (IN). En la figura siguiente se describe la red de muestra del caso de ejemplo Un único servidor DNS con acceso a Internet.

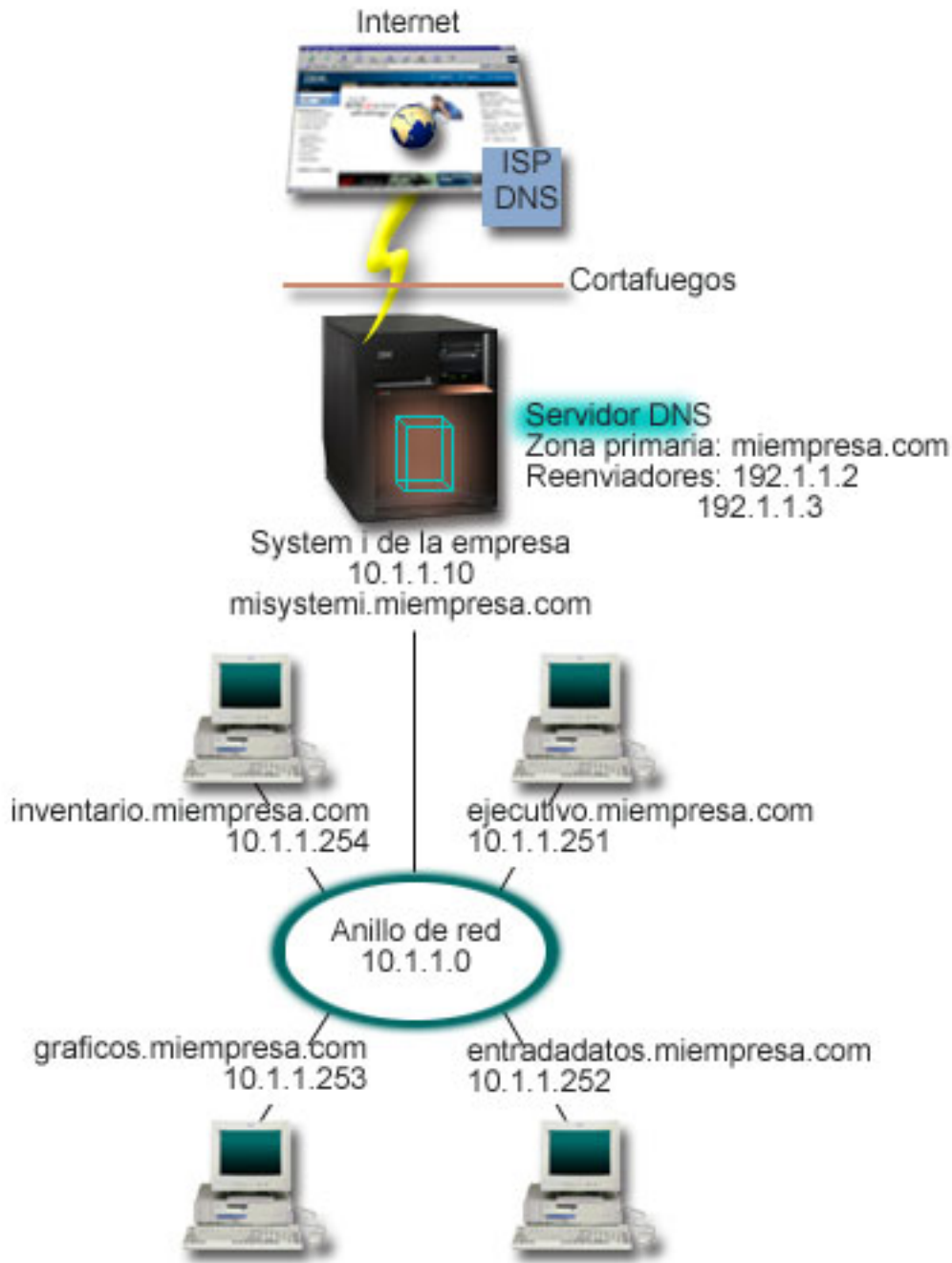


Figura 1. Un único servidor DNS con acceso a Internet

Supongamos que el host *entradadatos* consulta al servidor DNS el nombre *graficos.miempresa.com*. El servidor DNS utilizará sus propios datos de zona y responderá con la dirección IP 10.1.1.253.

Ahora supongamos que *entradadatos* solicita la dirección IP de *www.jkl.com*. Este host no se encuentra en los datos de zona del servidor DNS. Se pueden seguir dos procedimientos: *recursión* o *iteración*. Si se establece que un servidor DNS utilice la *recursión*, el servidor puede consultar (o contactar con) otros servidores DNS en nombre del cliente peticionario para que resuelva el nombre totalmente y luego envíe una respuesta de nuevo al cliente. Además, el servidor peticionario almacena la respuesta en su caché para poder utilizarla la próxima vez que el servidor reciba esa consulta. Si se establece que un servidor DNS utilice la *iteración*, el cliente puede intentar ponerse en contacto con otros servidores DNS por sí

mismo para resolver un nombre. En este proceso, el cliente emplea consultas separadas y adicionales en función de las respuestas al respecto que le envíen los servidores.

Referencia relacionada:

“Qué son las zonas” en la página 3

Los datos del sistema de nombres de dominio (DNS) se dividen en conjuntos gestionables de datos llamados *zonas*. Y cada uno de estos conjuntos corresponde a un tipo de zona concreto.

“Ejemplo: un único servidor de sistema de nombres de dominio (DNS) con acceso a Internet” en la página 18

Este ejemplo describe una subred simple con un servidor de sistema de nombres de dominio (DNS) conectado directamente a Internet.

Configuración del dominio del sistema de nombres de dominio (DNS)

Para configurar el dominio del sistema de nombres de dominio (DNS), hay que registrar el nombre de dominio para impedir que los demás lo utilicen.

El DNS le permite servir nombres y direcciones en una intranet, o red interna. También le permite servir nombres y direcciones al resto del mundo a través de Internet. Si desea configurar dominios en Internet, deberá registrar un nombre de dominio.

Si va a configurar una intranet, no es necesario que registre un nombre de dominio para uso interno. La decisión de registrar o no un nombre de intranet dependerá de si desea garantizar que nadie pueda utilizar ese nombre en Internet, independientemente del uso interno que haga del mismo. El hecho de registrar un nombre que vaya a utilizar internamente garantiza que nunca tendrá problemas si más adelante decide utilizar el nombre del dominio externamente.

El registro del dominio puede realizarse poniéndose en contacto directamente con un registrador autorizado de nombres de dominio o a través de un Proveedor de Servicios de Internet (ISP). Algunos ISP ofrecen el servicio de someter peticiones de registro de nombres de dominio en su nombre. Internet Network Information Center (InterNIC) mantiene un directorio con todos los registradores de nombres de dominio que estén autorizados por la Corporación de nombres y números asignados de Internet (ICANN).

Referencia relacionada:

“Ejemplo: un único servidor de sistema de nombres de dominio (DNS) con acceso a Internet” en la página 18

Este ejemplo describe una subred simple con un servidor de sistema de nombres de dominio (DNS) conectado directamente a Internet.

Información relacionada:

 [Internet Network Information Center \(InterNIC\)](#)

Actualizaciones dinámicas

El sistema de nombres de dominio (DNS) de IBM i que está basado en BIND 9 admite las actualizaciones dinámicas. Las fuentes externas, como el protocolo de configuración dinámica de hosts (DHCP), pueden enviar actualizaciones al servidor DNS. Además, también se pueden utilizar las herramientas de cliente DNS, como el programa de utilidad de actualización dinámica (NSUPDATE), para realizar actualizaciones dinámicas.

DHCP es un estándar de TCP/IP que utiliza un servidor central para gestionar las direcciones IP y otros datos de configuración de una red completa. Un servidor DHCP responde a las consultas de los clientes y les asigna propiedades dinámicamente. DHCP le permite definir los parámetros de configuración de host de red en una ubicación central, y automatizar la configuración de los hosts. Se utiliza a menudo para asignar direcciones IP temporales a los clientes de redes que contienen más clientes que direcciones IP disponibles.

Antiguamente, todos los datos DNS se almacenaban en bases de datos estáticas. Todos los registros de recursos de DNS los creaba y mantenía el administrador. Pero los servidores DNS basados en BIND 8 o posterior se pueden configurar para que acepten las peticiones de otras fuentes para actualizar los datos de zona dinámicamente.

Puede configurar el servidor DHCP para que envíe peticiones de actualización al servidor DNS cada vez que asigne una dirección nueva a un host. Este proceso automatizado reduce las tareas administrativas del servidor DNS en las redes TCP/IP de crecimiento o cambio constante, así como en las redes en las que los hosts cambian de ubicación con frecuencia. Cuando un cliente que utiliza DHCP recibe una dirección IP, los datos correspondientes se envían inmediatamente al servidor DNS. Mediante este método, el DNS puede seguir resolviendo satisfactoriamente consultas de hosts, incluso cuando sus direcciones IP hayan cambiado.

Puede configurar DHCP para que actualice los registros de correlación de direcciones (A en el caso de IPv4 o AAAA en el caso de IPv6) y/o los registros de puntero de búsqueda inversa (PTR) en nombre de un cliente. El registro de correlación de direcciones (A o AAAA) correlaciona el nombre de host de una máquina con su dirección IP. El registro PTR correlaciona la dirección IP de una máquina con su nombre de host. Cuando la dirección de un cliente cambia, DHCP puede enviar automáticamente una actualización al servidor DNS para que los demás hosts de la red puedan localizar el cliente por medio de consultas DNS en la nueva dirección IP del cliente. Por cada registro que se actualiza dinámicamente, se escribe un registro de texto (TXT) asociado para indicar que el registro lo ha escrito DHCP.

Nota: Si establece que DHCP solo debe actualizar los registros PTR, debe configurar el DNS con el fin de que permita las actualizaciones procedentes de los clientes, para que cada cliente pueda actualizar su registro A si el cliente emplea una dirección IPv4 o para que pueda actualizar su registro AAAA si el cliente emplea una dirección IPv6. No todos los clientes DHCP permiten que se realicen peticiones para actualizar su propio registro A o AAAA. Consulte la documentación de su plataforma de cliente antes de elegir este método.

Las zonas dinámicas quedan protegidas mediante la creación de una lista de fuentes autorizadas a las que se les permite enviar actualizaciones. Puede definir fuentes autorizadas utilizando direcciones IP individuales, subredes completas, paquetes que se hayan firmado mediante una clave secreta compartida (llamada *signatura de transacción* o TSIG), o cualquier combinación de estos métodos. El DNS verifica si los paquetes de petición de entrada provienen de una fuente autorizada antes de actualizar los registros de recursos.

Pueden realizarse actualización dinámica entre DNS y DHCP en una sola plataforma IBM i, entre diferentes plataformas IBM i o entre una plataforma IBM i y otros sistemas que tengan capacidad para las actualizaciones dinámicas.

Nota: Se necesita la API Actualización dinámica de DNS (QTOBUPDT) en los servidores que envían actualizaciones dinámicas al DNS. Se instala automáticamente junto con la opción 31 de IBM i, DNS. Sin embargo, en BIND 9, es preferible utilizar el mandato **NSUPDATE** para hacer las actualizaciones en la plataforma IBM i.

Conceptos relacionados:

Protocolo de configuración dinámica de hosts (DHCP)

Tareas relacionadas:

“Configurar el sistema de nombres de dominio (DNS) para que reciba actualizaciones dinámicas” en la página 32

Los servidores del sistema de nombres de dominio (DNS) que ejecutan BIND 9 se pueden configurar de modo que acepten peticiones de otras fuentes para actualizar dinámicamente los datos de la zona. Este tema ofrece instrucciones para configurar la opción allow-update para que el DNS pueda recibir actualizaciones dinámicas.

Configurar el protocolo DHCP para que envíe actualizaciones dinámicas a DNS

“Volver a firmar una zona” en la página 40

Para una zona primaria firmada, si se han realizado nuevos cambios en los registros de recurso de la zona, ésta debe volver a firmarse.

Referencia relacionada:

“Ejemplo: un sistema de nombres de dominio (DNS) y el protocolo de configuración dinámica de hosts (DHCP) en el mismo IBM i” en la página 20

Este ejemplo ilustra un sistema de nombres de dominio (DNS) y el protocolo de configuración dinámica de hosts (DHCP) en la misma plataforma IBM i.

“Registros de recursos del sistema de nombres de dominio (DNS)” en la página 10

Los registros de recursos se utilizan para almacenar datos sobre nombres de dominio y direcciones IP. Puede utilizar la tabla de búsqueda de registros de recursos para buscar los registros de recursos soportados para el sistema operativo IBM i.

QTOBUPT

“Características de BIND 9”

BIND 9 se parece a BIND 8, pero proporciona varias características para mejorar el rendimiento del servidor Sistema de nombres de dominio (DNS), como las vistas.

Características de BIND 9

BIND 9 se parece a BIND 8, pero proporciona varias características para mejorar el rendimiento del servidor Sistema de nombres de dominio (DNS), como las vistas.

Vistas en un solo servidor DNS de IBM i

La sentencia *view* (vista) permite que una sola instancia de DNS responda a una consulta de manera diferente en función del lugar del que procede la consulta, como puede ser de Internet o de una intranet.

Una aplicación práctica de la característica Vista es que divide las configuraciones de DNS sin tener que ejecutar múltiples servidores DNS. Por ejemplo, en un solo servidor DNS, puede definir una vista para responder a las consultas de una red interna y definir otra vista para responder a las consultas de una red externa.

Mandatos de cliente nuevos

Los siguientes mandatos de cliente mejoran la capacidad de gestión del servidor DNS:

Utilidad de actualización dinámica (NSUPDATE)

El mandato Utilidad de actualización dinámica (**NSUPDATE**) sirve para someter peticiones de actualización dinámica de DNS (tal como se definen en la petición de comentarios (RFC) 2136) a un servidor DNS. Esto permite que los registros de recursos se añadan o eliminen de una zona mientras el servidor DNS esté en ejecución. Por lo tanto, no hace falta que actualice los registros editando manualmente el archivo de zona. Una sola petición de actualización puede contener peticiones de añadir o eliminar múltiples registros de recursos, pero los registros de recursos que se añaden o eliminan dinámicamente con el mandato **NSUPDATE** deben estar en la misma zona.

Nota: No edite manualmente las zonas que estén bajo control dinámico utilizando el mandato **NSUPDATE** ni mediante un servidor DHCP. Las ediciones manuales pueden entrar en conflicto con las actualizaciones dinámicas y provocar una pérdida de datos.

Iniciar consulta DIG (DIG)

El sondeador de información de dominio (DIG) es una herramienta de consulta más potente, si se compara con el mandato Búsqueda de servidor de nombres (**NSLOOKUP**), que puede servir para recuperar información de un servidor DNS o para probar la respuesta de un servidor DNS. El mandato **NSLOOKUP** ha caído en desuso y solo se proporciona por cuestión de compatibilidad con las versiones anteriores. Puede utilizar DIG para verificar que hay un servidor DNS que responde

correctamente, antes de configurar su sistema para utilizarlo. Mediante DIG también puede recuperar información de DNS sobre hosts, dominios y otros servidores DNS.

Puede utilizar el mandato Arrancar consulta DIG (**STRDIGQRY**) o su alias DIG para iniciar la herramienta Sonda de información de dominio (DIG).

Arrancar consulta HOST (HOST)

El mandato Arrancar consulta HOST (**HOST**) se emplea para las búsquedas DNS. Puede utilizarlo para convertir nombres de dominio a direcciones IP (ya sea IPv4 o IPv6) y viceversa.

Control de daemon de nombres remoto (RNDC)

El mandato Control de daemon de nombres remoto (**RNDC**) es un potente programa de utilidad que permite a un administrador del sistema controlar el funcionamiento de un servidor de nombres. El mandato lee un archivo de configuración, que se llama `rndc.conf`, para determinar cómo establecer contacto con el servidor de nombres y para averiguar qué algoritmo y qué clave tiene que utilizar. Si no se encuentra ningún archivo `rndc.conf`, se emplea por defecto un archivo `rndc-key_KID` creado durante la instalación, que otorga automáticamente acceso mediante la interfaz de bucle de retorno.

Soporte IPv6

BIND 9 permite realizar búsquedas de nombre a dirección o de dirección a nombre en todos los formatos de IPv6 definidos actualmente. En el caso de las búsquedas directas, BIND 9 soporta ambas clases de registros, AAAA y A6, pero ahora los registros A6 han caído en desuso. En el caso de las búsquedas inversas de IPv6, BIND 9 admite el formato "nibble" tradicional empleado en el dominio `ip6.arpa`, así como en el dominio `ip6.int` más antiguo, ahora en desuso.

Archivos de diario

Los archivos de diario sirven para guardar las actualizaciones dinámicas de una zona. El archivo se crea automáticamente cuando se recibe la primera actualización dinámica de un cliente, y no desaparece. Es un archivo binario y no se debe editar.

Con el archivo de diario, el servidor, cuando se reinicia después de una conclusión o una caída del sistema, reproduce el archivo de diario para incorporar a la zona las actualizaciones que tuvieron lugar después del último vuelco de la zona. Los archivos de diario también sirven para almacenar las actualizaciones del método de transferencias de zona incrementales (IXFR).

Se ha rediseñado DNS para IBM i con el fin de que utilice BIND 9. Para ejecutar DNS de BIND 9 en el sistema, este debe cumplir determinados requisitos de software.

Conceptos relacionados:

"Requisitos del sistema de nombres de dominio (DNS)" en la página 28

Tenga en cuenta estos requisitos de software a la hora de ejecutar el sistema de nombres de dominio (DNS) en la plataforma IBM i.

"Actualizaciones dinámicas" en la página 6

El sistema de nombres de dominio (DNS) de IBM i que está basado en BIND 9 admite las actualizaciones dinámicas. Las fuentes externas, como el protocolo de configuración dinámica de hosts (DHCP), pueden enviar actualizaciones al servidor DNS. Además, también se pueden utilizar las herramientas de cliente DNS, como el programa de utilidad de actualización dinámica (NSUPDATE), para realizar actualizaciones dinámicas.

Referencia relacionada:

"Ejemplo: dividir el DNS por el cortafuegos configurando dos servidores DNS en el mismo IBM i" en la página 22

En este ejemplo se describe un servidor de sistema de nombres de dominio (DNS) que funciona a través de un cortafuegos para proteger los datos internos ante Internet, permitiendo a la vez que los usuarios internos accedan a los datos en Internet. Esta configuración implanta esta protección configurando dos

servidores DNS en la misma plataforma IBM i.

“Planificar medidas de seguridad” en la página 27

El sistema de nombres de dominio (DNS) proporciona opciones de seguridad para limitar el acceso externo al servidor.

Registros de recursos del sistema de nombres de dominio (DNS)

Los registros de recursos se utilizan para almacenar datos sobre nombres de dominio y direcciones IP. Puede utilizar la tabla de búsqueda de registros de recursos para buscar los registros de recursos soportados para el sistema operativo IBM i.

Una base de datos de zona de DNS está formada por una serie de registros de recursos. Cada registro de recurso especifica la información pertinente sobre un objeto determinado. Por ejemplo, los registros de correlación de direcciones (A) correlacionan un nombre de host con una dirección IP, y los registros de puntero de búsqueda inversa (PTR) correlacionan una dirección IP con un nombre de host. El servidor utiliza estos recursos para resolver las consultas de los hosts de su zona. Si desea más información, utilice la tabla para ver los registros de recursos de DNS.

Nota: Las entradas de la tabla de búsqueda de registros de recursos se podrían añadir o eliminar según el cambio del documento BIND. Además, esta no es una lista exhaustiva de todos los registros de recursos enumerados en BIND.

Tabla 1. Tabla de búsqueda de registros de recursos

Registro de recurso	Abreviatura	Descripción
Registros de correlación de direcciones	A	El registro A especifica la dirección IP de este host. Los registros A se utilizan para resolver una consulta de la dirección IP de un nombre de dominio determinado. Este tipo de registro se define en la petición de comentarios (RFC) 1035.
Registros AFSDDB (Andrew File System Database)	AFSDB	El registro AFSDDB especifica la dirección AFS o DCE del objeto. Los registros AFSDDB se utilizan como los registros A para correlacionar un nombre de dominio con su dirección AFSDDB o para correlacionar el nombre de dominio de una celda con los servidores de nombre autenticados de dicha celda. Este tipo de registro se define en la RFC 1183.
Registros de nombre canónico	CNAME	El registro CNAME especifica el nombre de dominio real de este objeto. Cuando DNS consulta un nombre de alias y encuentra un registro CNAME que apunta al nombre canónico, consultará dicho nombre de dominio canónico. Este tipo de registro se define en la RFC 1035.
Registro de validación anticipada DNSSEC	DLV	El registro DLV especifica anclas de confianza de DNSSEC externas a la cadena de delegación de DNS. Utiliza el mismo formato que el registro DS. Este tipo de registro se define en la RFC 4431.

Tabla 1. Tabla de búsqueda de registros de recursos (continuación)

Registro de recurso	Abreviatura	Descripción
Registro de claves DNS	DNSKEY	El registro DNSKEY especifica el registro de claves de DNSSEC. Una zona firma sus RRsets autorizados mediante una clave privada y almacena la clave pública correspondiente en un RR DNSKEY. Este tipo de registro se define en la RFC 4034.
Registro DS	Firmante de delegación	El registro DS especifica la clave de firma de DNSSEC de una zona delegada. Este tipo de registro se define en la RFC 4034.
Registros de información de host	HINFO	El registro HINFO especifica información general acerca de un host. Los nombres de sistema operativo y CPU estándar se definen en la RFC de números asignados, 1700. No obstante, la utilización de números estándar no es necesaria. Este tipo de registro se define en la RFC 1035.
Registros de Red Digital de Servicios Integrados	RDSI	El registro RDSI especifica la dirección de este objeto. Este registro correlaciona un nombre de host con la dirección RDSI. Solamente se utilizan en las redes RDSI. Este tipo de registro se define en la RFC 1183.
Registros de dirección IP Versión 6	AAAA	El registro AAAA especifica la dirección IPv6 de 128 bits de un host. Los registros AAAA, parecidos a los registros A, sirven para resolver consultas de la dirección IPv6 de un nombre de dominio específico. Este tipo de registro se define en la RFC 1886.
Registros de ubicación	LOC	El registro LOC especifica la ubicación física de los componentes de red. Las aplicaciones pueden utilizar estos registros para evaluar la eficacia de la red o para correlacionar la red física. Este tipo de registro se define en la RFC 1876.

Tabla 1. Tabla de búsqueda de registros de recursos (continuación)

Registro de recurso	Abreviatura	Descripción
Registros de intercambiador de correo (MX)	MX	Los registros MX definen un host intercambiador de correo para enviar correo a este dominio. El protocolo simple de transferencia de correo (SMTP) utiliza estos registros para localizar los hosts que procesan o reenvían el correo de este dominio, junto con los valores de preferencias de cada host intercambiador de correo. Cada host intercambiador de correo debe tener su correspondiente registro de dirección de host (A) en una zona válida. Este tipo de registro se define en la RFC 1035.
Registros de grupo de correo	MG	Los registros MG especifican el nombre de dominio del grupo de correo. Este tipo de registro se define en la RFC 1035.
Registros de buzón	MB	Los registros MB especifican el nombre de dominio de host que contiene el buzón de este objeto. El correo que se envía al dominio se dirige al host especificado en el registro MB. Este tipo de registro se define en la RFC 1035.
Registros de información de buzón	MINFO	Los registros MINFO especifican el buzón que debe recibir los mensajes o errores de este objeto. El registro MINFO se utiliza más habitualmente para enviar listas que para un solo buzón. Este tipo de registro se define en la RFC 1035.
Registros de red denominación de buzón	MR	Los registros MR especifican un nuevo nombre de dominio para un buzón. Puede utilizar el registro MR como una entrada de reenvío para un usuario que se ha trasladado a un buzón distinto. Este tipo de registro se define en la RFC 1035.
Registros de servidor de nombres	NS	El registro NS especifica un servidor de nombres autorizado para este host. Este tipo de registro se define en la RFC 1035.
Registro Next-Secure	NSEC	El registro NSEC especifica datos utilizados para probar que un nombre no existe. Este tipo de registro se define en la RFC 4034.
Registro NSEC versión 3	NSEC3	El registro NSEC3 especifica datos para la denegación autenticada de la existencia de conjuntos de registros de recurso de DNS. Este tipo de registro se define en la RFC 5155.

Tabla 1. Tabla de búsqueda de registros de recursos (continuación)

Registro de recurso	Abreviatura	Descripción
Parámetros de NSEC3	NSEC3PARAM	NSEC3PARAM especifica parámetros que se utilizan con NSEC3. Este tipo de registro se define en la RFC 5155.
Registros de protocolo de acceso de servicios de red	NSAP	El registro NSAP especifica la dirección de un recurso NSAP. Los registros NSAP se utilizan para correlacionar nombres de dominio con direcciones NSAP. Este tipo de registro se define en la RFC 1706.
Registros de clave pública	KEY	El registro KEY especifica una clave pública asociada a un nombre DNS. La clave puede ser de una zona, un usuario o un host. Este tipo de registro se define en la RFC 2065.
Registros de persona responsable	RP	El registro RP especifica la dirección de correo internet y descripción de la persona responsable de esta zona o este host. Este tipo de registro se define en la RFC 1183.
Registros de puntero de búsqueda inversa	PTR	El registro PTR especifica el nombre de dominio de un host para el que desea tener un registro PTR definido. Los registros PTR permiten la búsqueda de nombres de host a partir de direcciones IP. Este tipo de registro se define en la RFC 1035.
Firma DNSSEC	RRSIG	El registro RRSIG especifica firmas digitales utilizadas en el proceso de autenticación de DNSSEC. Este tipo de registro se define en la RFC 4034.
Registros de ruta a través	RT	El registro RT especifica un nombre de dominio de host que puede actuar como un reenviador de paquetes IP para este host. Este tipo de registro se define en la RFC 1183.
Registros de servicios	SRV	El registro SRV especifica los hosts que soportan los servicios definidos en el registro. Este tipo de registro se define en la RFC 2782.
Registros de inicio de autorización	SOA	El registro SOA especifica que este servidor es autorizador para esta zona. Un servidor autorizador es la mejor fuente de los datos de una zona. El registro SOA contiene información general acerca de la zona y reglas de recarga para servidores secundarios. Solamente puede haber un registro SOA por zona. Este tipo de registro se define en la RFC 1035.

Tabla 1. Tabla de búsqueda de registros de recursos (continuación)

Registro de recurso	Abreviatura	Descripción
Registros de texto	TXT	El registro TXT especifica múltiples series de texto, con una longitud máxima de 255 caracteres cada una de ellas, que deben asociarse a un nombre de dominio. Los registros TXT se pueden utilizar junto con los registros de persona responsable (RP) para proporcionar información acerca del responsable de una zona. Este tipo de registro se define en la RFC 1035. los registros TXT se utilizan en el protocolo DHCP de IBM i para las actualizaciones dinámicas. El servidor DHCP escribe un registro TXT asociado para cada actualización de registro A y PTR que realice el servidor DHCP. Los registros DHCP llevan el prefijo AS400DHCP.
Registros de servicios bien conocidos	WKS	El registro WKS especifica los servicios bien conocidos que soporta el objeto. Con mucha frecuencia los registros WKS indican en esta dirección se soportan los protocolos tcp, udp o ambos. Este tipo de registro se define en la RFC 1035.
Registros de correlación de direcciones X.400	PX	Los registros PX son un puntero hacia la información de correlación X.400/RFC 822. Este tipo de registro se define en la RFC 1664.
Registros de correlación de direcciones X25	X25	El registro X25 especifica la dirección de un recurso X25. Este registro correlaciona un nombre de host con la dirección PSDN. Solamente se utilizan en las redes X25. Este tipo de registro se define en la RFC 1183.

Conceptos relacionados:

“Registros de correo y de intercambiador de correo (MX)”

El sistema de nombres de dominio (DNS) soporta el direccionamiento de correo avanzado mediante el uso de registros de correo y de intercambiador de correo (MX).

Referencia relacionada:

“Ejemplo: un único servidor de sistema de nombres de dominio (DNS) para una intranet” en la página 16 Este ejemplo describe una subred simple con un servidor de sistema de nombres de dominio (DNS) para uso interno.

“Qué son las zonas” en la página 3

Los datos del sistema de nombres de dominio (DNS) se dividen en conjuntos gestionables de datos llamados *zonas*. Y cada uno de estos conjuntos corresponde a un tipo de zona concreto.

Registros de correo y de intercambiador de correo (MX)

El sistema de nombres de dominio (DNS) soporta el direccionamiento de correo avanzado mediante el uso de registros de correo y de intercambiador de correo (MX).

Los registros de correo y MX se utilizan en los programas de direccionamiento de correo, como el protocolo simple de transferencia de correo (SMTP). La tabla de búsqueda de los registros de recursos DNS contiene los tipos de registros de correo soportados por el DNS de IBM i.

El DNS incluye información para enviar correo electrónico utilizando información de intercambio de correo. Si la red utiliza DNS, la aplicación SMTP no entrega el correo con destino al host TEST.IBM.COM abriendo una conexión TCP con TEST.IBM.COM. SMTP primero solicita al servidor DNS que averigüe qué servidores de host se pueden usar para entregar el mensaje.

Entregar correo a una dirección específica

Los servidores DNS utilizan registros de recursos que se conocen con el nombre de registros de *intercambiador de correo* (MX). Los registros MX correlacionan un nombre de dominio o de host con un valor de preferencia y un nombre de host. Los registros MX suelen utilizarse para indicar que un host se utilice para procesar correo para otro host. Los registros también se utilizan para indicar a otro host que entregue el correo en caso de que no se pueda acceder al primer host. En otras palabras, permiten que un correo destinado a un host se entregue a un host diferente.

Pueden existir múltiples registros de recursos MX para un mismo nombre de dominio o de host. Cuando hay múltiples registros MX para el mismo dominio o host, el valor de preferencia (o prioridad) de cada registro determina el orden en el que se procesan. El valor de preferencia más bajo corresponde al registro con mayor prioridad, que se procesará en primer lugar. Cuando no pueda alcanzarse el host preferido, la aplicación de envío de correo intenta contactar con el siguiente host MX, de prioridad menor. El administrador del dominio, o el creador del registro MX, es el que define el valor de preferencia.

Un servidor DNS puede responder con una lista vacía de registros de recursos MX cuando el nombre se encuentra autorizado en el servidor DNS pero no tiene ningún MX asignado. Si esto ocurre, la aplicación de envío de correo podría tratar de establecer una conexión directamente con el host de destino.

Nota: No conviene utilizar un comodín (por ejemplo: *.mycompany.com) en los registros MX para un dominio.

Ejemplo: registro MX de un host

En el ejemplo siguiente, el sistema envía el correo de fsc5.test.ibm.com de forma prioritaria al propio host. Si no puede alcanzarse el host, el correo puede entregarse a psfred.test.ibm.com o a mvs.test.ibm.com (si tampoco puede alcanzarse psfred.test.ibm.com). A continuación se muestra un ejemplo del aspecto que tendrán estos registros MX:

```
fsc5.test.ibm.com  IN MX 0 fsc5.test.ibm.com
                  IN MX 2 psfred.test.ibm.com
                  IN MX 4 mvs.test.ibm.com
```

Referencia relacionada:

“Registros de recursos del sistema de nombres de dominio (DNS)” en la página 10

Los registros de recursos se utilizan para almacenar datos sobre nombres de dominio y direcciones IP. Puede utilizar la tabla de búsqueda de registros de recursos para buscar los registros de recursos soportados para el sistema operativo IBM i.

Introducción a las Extensiones de seguridad de DNS (DNSSEC)

DNSSEC es un conjunto de especificaciones RFC IETF que añaden ampliaciones de seguridad a DNS.

El protocolo DNS original no da soporte a la seguridad. Puede producirse suplantación y corrupción de los datos DNS entre un servidor maestro y un programa de resolución debido a que DNS no proporciona una mecanismo para validar las respuestas. Esto hace que DNS sea vulnerable a estos tipos de ataques.

DNSSEC proporciona comunicaciones autenticadas entre servidores que dan soporte a TSIG/SIG0. Puede establecerse una cadena de confianza para verificar la autenticidad e integridad de los datos.

En una zona DNS, ZSK (claves de firma de zona) firmará los datos de la zona DNS, y KSK (clave de firma de clave) firmará la ZSK. Puede copiarse un registro de recurso (RR) de firmante de delegación (DS), derivado de KSK, en la zona padre para formar una cadena de confianza. Por tanto, los RRsets de una zona segura contendrán: RRs DNSKEY (ZSK y KSK), RRs RRSIG (firma de registro de recurso), RRs NSEC (próximo protegido) y (opcionalmente) RRs DS de la zona hija.

Cuando un programa de resolución de DNS con conocimiento de la seguridad reciba una respuesta de una consulta, intentará validar los RR RRSIG con el RR DNSKEY de la zona. A continuación, validará el RR DNSKEY con el RR DS que puede obtenerse de la zona padre, y así sucesivamente, hasta que el RR DNSKEY o el RR DS coincida con el ancla de confianza configurada en el programa de resolución.

Para obtener más información acerca de DNSSEC, consulte las RFC 4033, 4034 y 4035.

Conceptos relacionados:

“Novedades de IBM i 7.2” en la página 1

Aquí encontrará la información nueva o la que ha cambiado sustancialmente en el temario Sistema de nombres de dominio (DNS).

“Gestionar el sistema de nombres de dominio (DNS)” en la página 37

La tarea de gestionar el sistema de nombres de dominio (DNS) incluye verificar el funcionamiento de la función DNS, el mantenimiento de DNSSEC, supervisar el rendimiento, y mantener los datos y archivos del DNS.

“Gestionar DNSSEC” en la página 40

Este tema presenta el mantenimiento de DNSSEC en la plataforma IBM i.

Ejemplos: sistema de nombres de dominio (DNS)

Puede utilizar estos ejemplos para entender cómo se utiliza el sistema de nombres de dominio (DNS) en la red.

DNS es un sistema de bases de datos distribuidas que sirve para gestionar nombres de hosts y las direcciones IP asociadas a ellos. Los ejemplos siguientes contribuyen a explicar el funcionamiento de DNS, y cómo puede utilizarlo en la red. En los ejemplos se describe la configuración y las razones por las que se utilizará. También enlaza a una serie de conceptos relacionados que puede encontrar útiles para comprender las figuras.

Ejemplo: un único servidor de sistema de nombres de dominio (DNS) para una intranet

Este ejemplo describe una subred simple con un servidor de sistema de nombres de dominio (DNS) para uso interno.

En la siguiente figura se ve un DNS que se ejecuta en una plataforma IBM i para una red interna. Esta única instancia de servidor DNS está configurada para que esté a la escucha de las consultas en todas las direcciones IP de la interfaz. El sistema es un servidor de nombres primario de la zona miempresa.com.

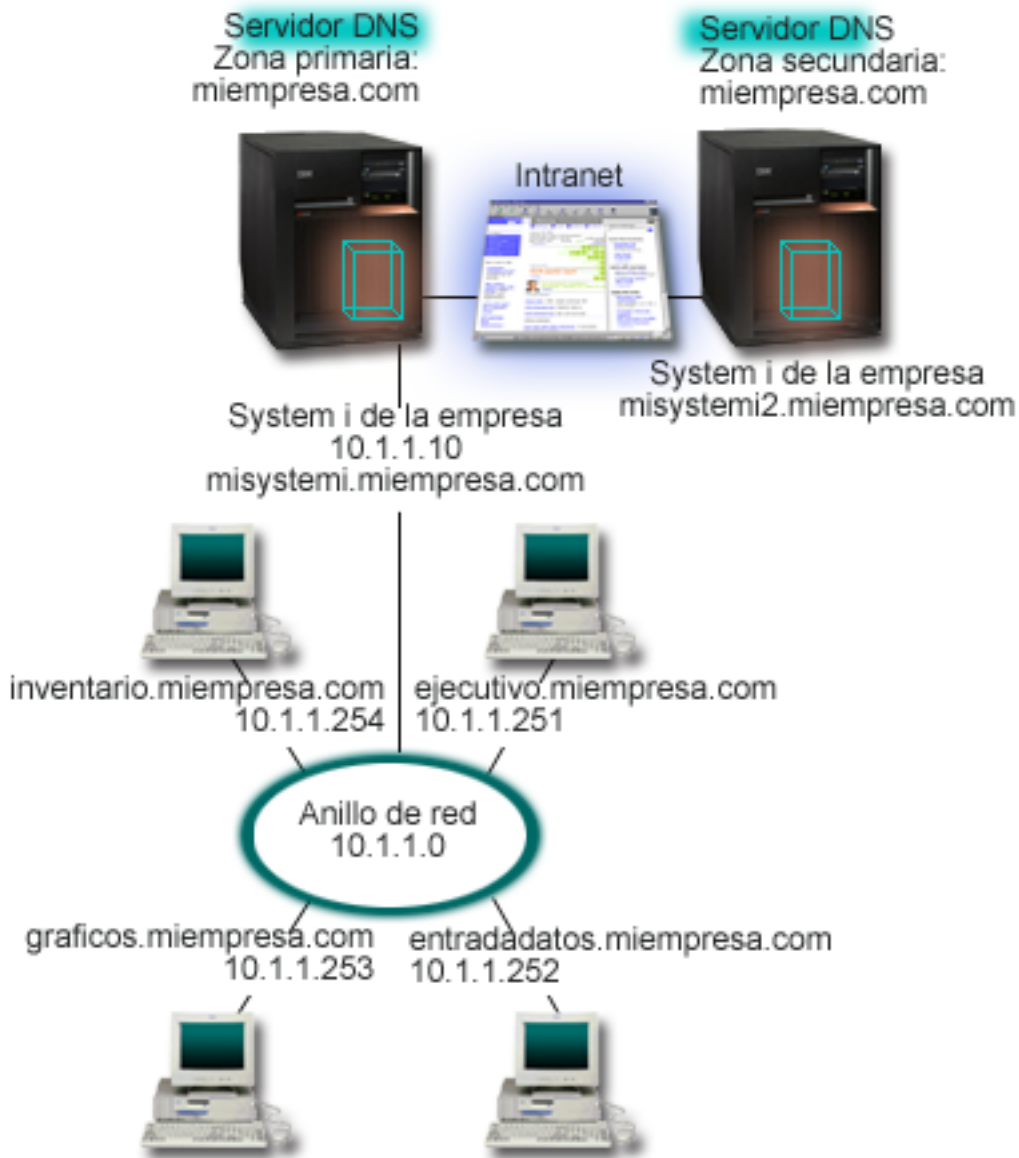


Figura 2. Un único servidor DNS para una intranet

Cada host de la zona tiene una dirección IP y un nombre de dominio. El administrador debe definir manualmente los hosts en los datos de zona del DNS, creando registros de recursos. Los registros de correlación de direcciones (A en el caso de IPv4 o AAAA en el caso de IPv6) correlacionan el nombre de una máquina con la dirección IP asociada a ella. De esta forma, los demás hosts de la red pueden consultar el servidor DNS para que localice la dirección IP asignada a un determinado nombre de host. Los registros de puntero de búsqueda inversa (PTR) correlacionan la dirección IP de una máquina con el nombre asociado a ella. De esta forma, los demás hosts de la red pueden consultar el servidor DNS para saber el nombre del host que se corresponde con una dirección IP.

Además de los registros A, AAAA y PTR, el DNS admite otros muchos registros de recursos que se podrían necesitar, en función de qué otras aplicaciones basadas en TCP/IP se ejecuten en la intranet. Por ejemplo, si ejecuta sistemas internos de correo electrónico, es posible que necesite añadir registros de intercambiador de correo (MX) para que SMTP pueda consultar el DNS para saber qué sistemas ejecutan los servidores de correo.

Si esta pequeña red formara parte de una intranet más extensa, podría ser necesario definir servidores raíz internos.

Servidores secundarios

Los servidores secundarios cargan los datos de zona del servidor autorizador. Los servidores secundarios obtienen los datos de zona mediante transferencias de zona desde el servidor autorizador. Cuando un servidor de nombres secundario se inicia, solicita todos los datos del dominio especificado del servidor de nombres primario. Un servidor de nombres secundario solicita datos actualizados del servidor primario ya sea porque reciba una notificación del servidor de nombres primario (si se utiliza la función NOTIFY) o porque consulte el servidor de nombres primario y determine que los datos han cambiado. En la figura anterior, el servidor misystemi forma parte de una intranet. Se ha configurado otro sistema, misystemi2, para que funcione como servidor DNS secundario de la zona miempresa.com. El servidor secundario puede utilizarse para equilibrar la demanda de servidores y también para hacer de reserva en el caso de que el servidor primario no esté operativo. Conviene tener al menos un servidor secundario para cada zona.

Referencia relacionada:

“Registros de recursos del sistema de nombres de dominio (DNS)” en la página 10

Los registros de recursos se utilizan para almacenar datos sobre nombres de dominio y direcciones IP. Puede utilizar la tabla de búsqueda de registros de recursos para buscar los registros de recursos soportados para el sistema operativo IBM i.

“Qué son las zonas” en la página 3

Los datos del sistema de nombres de dominio (DNS) se dividen en conjuntos gestionables de datos llamados *zonas*. Y cada uno de estos conjuntos corresponde a un tipo de zona concreto.

“Ejemplo: un único servidor de sistema de nombres de dominio (DNS) con acceso a Internet”

Este ejemplo describe una subred simple con un servidor de sistema de nombres de dominio (DNS) conectado directamente a Internet.

Ejemplo: un único servidor de sistema de nombres de dominio (DNS) con acceso a Internet

Este ejemplo describe una subred simple con un servidor de sistema de nombres de dominio (DNS) conectado directamente a Internet.

En la siguiente figura se ve la misma red que en el ejemplo Un único servidor DNS para una intranet, pero en este caso la empresa ha añadido una conexión a Internet. En este ejemplo, la empresa puede acceder a Internet, pero el cortafuegos está configurado para que bloquee el tráfico de Internet que entra en la red.

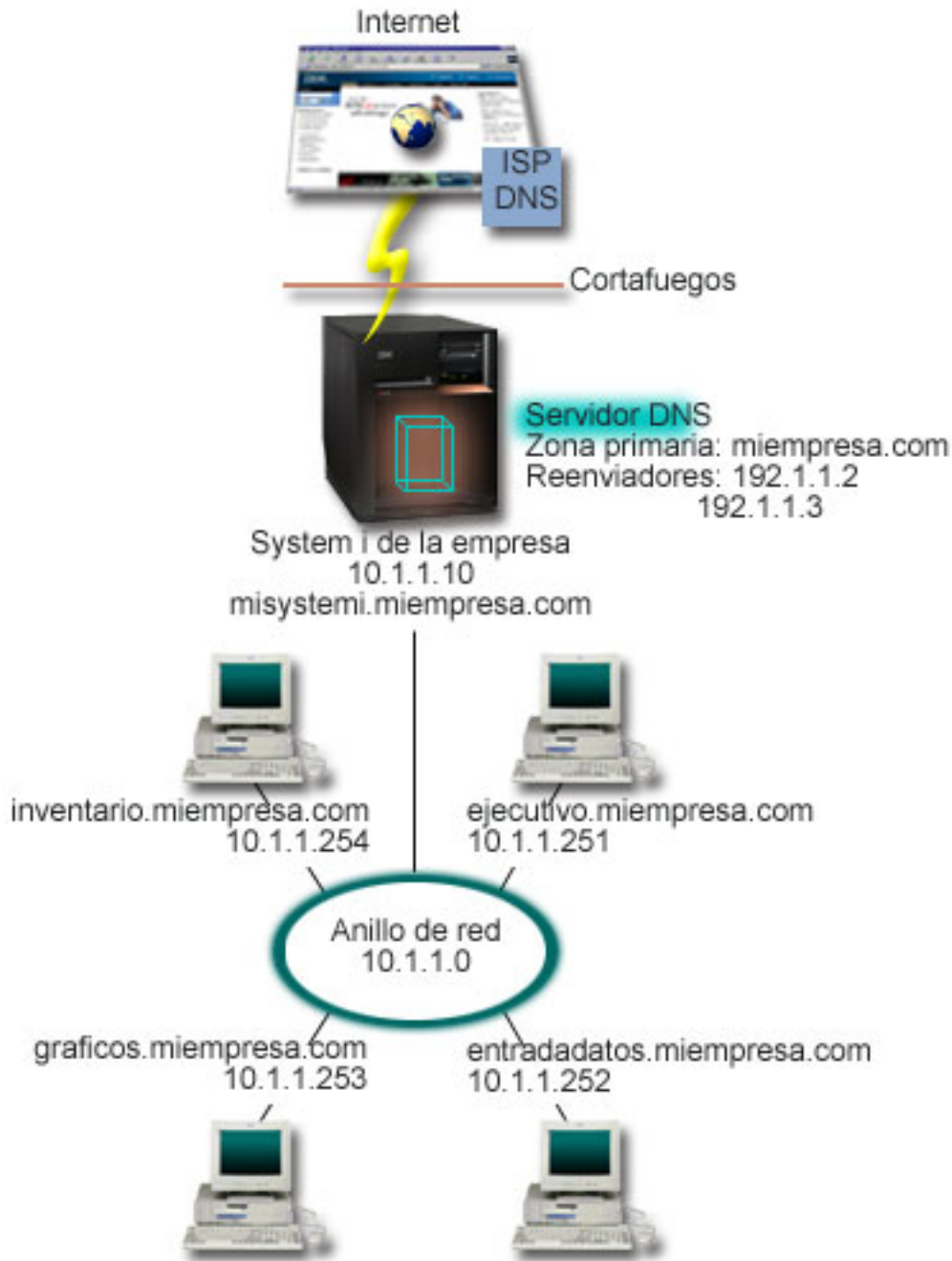


Figura 3. Un único servidor DNS con acceso a Internet

Para resolver las direcciones de Internet, debe realizar al menos una de las siguientes tareas:

- Definir servidores raíz de Internet

Puede cargar automáticamente los servidores raíz de Internet predeterminados, pero posiblemente necesitará actualizar la lista. Estos servidores pueden ayudarle a resolver las direcciones fuera de su propia zona. Las instrucciones para obtener los servidores raíz de Internet actuales están en: Acceder a los datos de un sistema de nombres de dominio (DNS) externo.

- Habilitar el reenvío

Puede configurar el reenvío para pasar las consultas sobre zonas fuera de miempresa.com a los servidores DNS externos, como los que ejecute su proveedor de servicios de Internet (ISP). Si desea

habilitar la búsqueda por reenvío y por servidores raíz, debe establecer que la opción forward (reenviar) tenga el valor **first** (primero). El servidor intenta primero reenviar y luego consulta los servidores raíz, pero solo si el reenvío no puede resolver la consulta.

Es posible que también sean necesarios los cambios de configuración siguientes:

- Asignar direcciones IP sin restricción

En el ejemplo anterior se muestran las direcciones 10.x.x.x. Sin embargo, son direcciones restringidas y no pueden utilizarse fuera de una intranet. Se muestran a continuación solo a título de ejemplo, pero es su ISP quien determine sus propias direcciones IP y otros factores de la red.

- Registrar el nombre del dominio

Si desea ser visible en Internet y aún no se ha registrado, debe registrar un nombre de dominio.

- Establecer un cortafuegos

No conviene que permita que el DNS esté directamente conectado a Internet. Debe configurar un cortafuegos o tomar otras medidas de precaución para proteger la plataforma IBM i.

Conceptos relacionados:

“Configuración del dominio del sistema de nombres de dominio (DNS)” en la página 6

Para configurar el dominio del sistema de nombres de dominio (DNS), hay que registrar el nombre de dominio para impedir que los demás lo utilicen.

System i y la seguridad en Internet

“Qué son las consultas al sistema de nombres de dominio (DNS)” en la página 4

Los clientes del sistema de nombres de dominio (DNS) emplean servidores DNS para resolver consultas.

Las consultas pueden proceder directamente del cliente o de una aplicación que se ejecute en el cliente.

Referencia relacionada:

“Ejemplo: un único servidor de sistema de nombres de dominio (DNS) para una intranet” en la página 16
Este ejemplo describe una subred simple con un servidor de sistema de nombres de dominio (DNS) para uso interno.

Ejemplo: un sistema de nombres de dominio (DNS) y el protocolo de configuración dinámica de hosts (DHCP) en el mismo IBM i

Este ejemplo ilustra un sistema de nombres de dominio (DNS) y el protocolo de configuración dinámica de hosts (DHCP) en la misma plataforma IBM i.

La configuración puede utilizarse para actualizar dinámicamente los datos de zona DNS cuando DHCP asigna las direcciones IP a los hosts.

En la siguiente figura se ve una pequeña subred con una plataforma IBM i que funciona a modo de servidor DHCP y DNS para cuatro clientes. En este entorno de trabajo, supongamos que los clientes ejecutivos, de entrada de datos y de inventario crean documentos con gráficos a partir del servidor de archivos de gráficos. Se conectan al servidor de archivos de gráficos mediante una unidad de red con el correspondiente nombre de host.

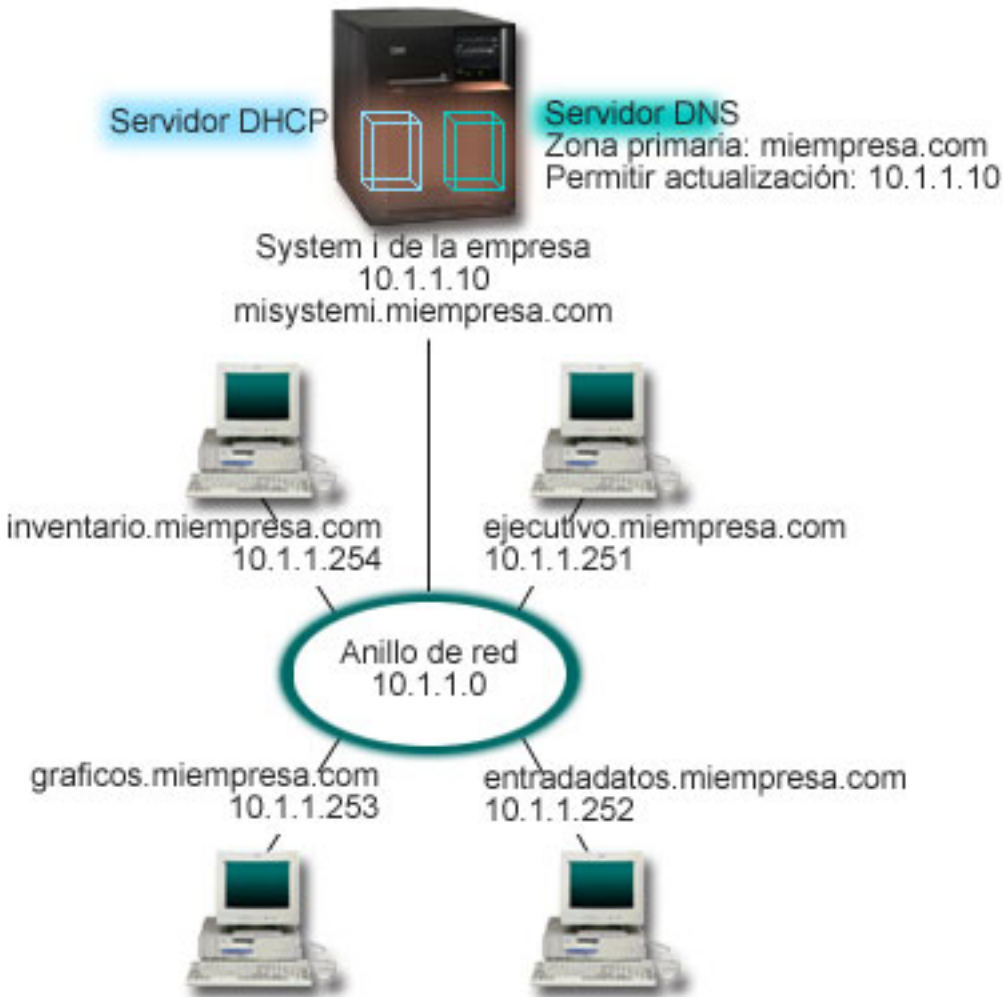


Figura 4. DNS y DHCP en la misma plataforma IBM i

Las versiones anteriores de DHCP y DNS eran independientes entre sí. Si DHCP asignaba una nueva dirección IP a un cliente, el administrador debía actualizar manualmente los registros DNS. En este ejemplo, si la dirección IP del servidor de archivos de gráficos cambia porque está asignada por DHCP, los clientes que dependen de él no podrán correlacionar la unidad de red con su nombre de host porque los registros de DNS contendrán la dirección IP anterior del servidor de archivos.

Con el servidor DNS de the IBM i basado en BIND 9, puede configurar la zona de DNS para que acepte actualizaciones dinámicas en los registros del DNS junto con cambios de dirección intermitentes mediante DHCP. Por ejemplo, cuando el servidor de archivos de gráficos renueva su cesión y el servidor DHCP le asigna la dirección IP 10.1.1.250, los registros de DNS asociados se actualizarán dinámicamente. De esta forma, los demás clientes podrán consultar el servidor DNS con respecto al servidor de archivos de gráficos mediante sus nombres de host sin interrupción.

Para configurar una zona DNS para que acepte actualizaciones dinámicas, realice estas tareas:

- Identificar la zona dinámica

No puede actualizar manualmente una zona dinámica mientras el servidor se esté ejecutando. Si lo hiciera, podría interferir en las actualizaciones dinámicas de entrada. Las actualizaciones manuales pueden hacerse cuando el servidor está detenido, pero perderá las actualizaciones dinámicas que se envíen mientras el servidor se encuentre inactivo. Por esta razón, es posible que desee configurar una

zona dinámica por separado para minimizar la necesidad de realizar actualizaciones manuales. En: Determinar la estructura del dominio hallará más información sobre cómo configurar las zonas para que utilicen la función de actualización dinámica.

- Configurar la opción allow-update

Las zonas que tengan configurada la opción allow-update se consideran zonas dinámicas. La opción allow-update se define por zonas. Para aceptar actualizaciones dinámicas, la opción allow-update debe estar habilitada para esta zona. En este ejemplo, la zona miempresa.com tiene la opción allow-update datos, pero otras zonas definidas en el servidor pueden estar configuradas como estáticas o dinámicas.

- Configurar DHCP para enviar actualizaciones dinámicas

Debe autorizar al servidor DHCP para actualizar los registros DNS correspondientes a las direcciones IP que ha distribuido.

- Configurar las preferencias de actualización del servidor secundario

Para que los servidores secundarios se mantengan actualizados, puede configurar DNS para que utilice NOTIFY para enviar un mensaje a los servidores secundarios de la zona miempresa.com cuando los datos de la zona presenten cambios. También debe configurar las transferencias de zona incrementales (IXFR), que permiten a los servidores secundarios habilitados para IXFR rastrear y cargar únicamente los datos de la zona actualizada y no de la zona completa.

Si ejecuta DNS y DHCP en servidores diferentes, existen algunos requisitos de configuración adicionales para el servidor DHCP.

Conceptos relacionados:

“Actualizaciones dinámicas” en la página 6

El sistema de nombres de dominio (DNS) de IBM i que está basado en BIND 9 admite las actualizaciones dinámicas. Las fuentes externas, como el protocolo de configuración dinámica de hosts (DHCP), pueden enviar actualizaciones al servidor DNS. Además, también se pueden utilizar las herramientas de cliente DNS, como el programa de utilidad de actualización dinámica (NSUPDATE), para realizar actualizaciones dinámicas.

Tareas relacionadas:

Configurar el protocolo DHCP para que envíe actualizaciones dinámicas a DNS

Referencia relacionada:

Ejemplo: DNS y DHCP en distintas plataformas System i

Ejemplo: dividir el DNS por el cortafuegos configurando dos servidores DNS en el mismo IBM i

En este ejemplo se describe un servidor de sistema de nombres de dominio (DNS) que funciona a través de un cortafuegos para proteger los datos internos ante Internet, permitiendo a la vez que los usuarios internos accedan a los datos en Internet. Esta configuración implanta esta protección configurando dos servidores DNS en la misma plataforma IBM i.

En la siguiente figura se ve una subred simple que utiliza un cortafuegos por cuestión de seguridad. Supongamos que la empresa tiene una red interna con un espacio IP reservado, así como una sección externa de una red disponible para el público. La empresa desea que sus clientes internos puedan resolver los nombres de host externos e intercambiar correo con los usuarios externos. La empresa también desea que los usuarios internos que se encargan de resolver nombres tengan acceso a determinadas zonas que son exclusivamente internas y que no están disponibles fuera de la red. Sin embargo, no quiere que las personas externas encargadas de resolver nombres tengan acceso a la red interna.

Con el DNS de IBM i basado en BIND 9, puede implantar esta solución de dos maneras. La primera consiste en que la empresa configura dos instancias de servidor DNS en la misma plataforma IBM i, una para la intranet y otra para todo lo que hay en el dominio público, que se describe en este ejemplo. Otra manera consiste en utilizar la función vista proporcionada en BIND 9, que se describe en el ejemplo de

cómo dividir el DNS a través de un cortafuegos utilizando una vista.

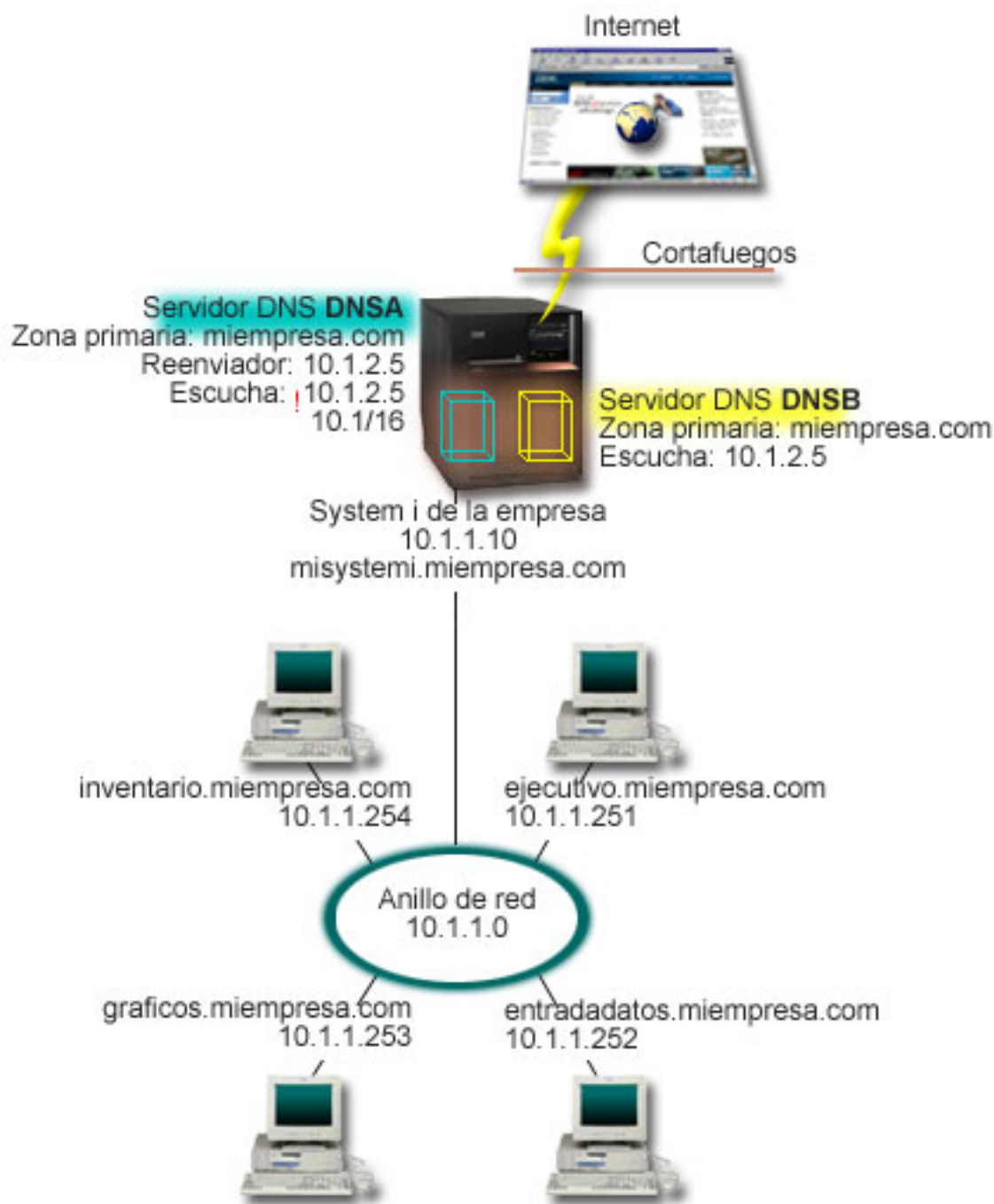


Figura 5. Dividir el DNS a través del cortafuegos, configurando dos servidores DNS en el mismo System i

El servidor externo, DNSB, está configurado con una zona primaria miempresa.com. Los datos de esta zona incluyen únicamente los registros de recursos que han de formar parte del dominio público. El servidor interno, DNSA, está configurado con la zona primaria miempresa.com, pero los datos de la zona definidos en el DNSA contienen registros de recursos de la intranet. La opción de reenviador está definida como 10.1.2.5. Esto obliga a que el DNSA reenvíe las consultas que no puede resolver al servidor DNSB.

Si le preocupa la integridad del cortafuegos u otros problemas de seguridad, puede optar por utilizar la opción de escucha para contribuir a proteger los datos internos. Para ello, puede configurar el servidor interno de manera que solo admita consultas a la zona interna miempresa.com procedentes de hosts internos. Para que todo esto funcione correctamente, los clientes internos deben estar configurados de forma que solo consulten el servidor DNSA. Debe tener en cuenta los siguientes valores de configuración para dividir el DNS:

- Escucha (listen-on)

En los otros ejemplos, solo hay un servidor DNS en una plataforma IBM i. Se ha establecido para que esté a la escucha en todas las direcciones IP de la interfaz. Siempre que tenga múltiples servidores DNS en una plataforma IBM i, debe definir las direcciones IP de interfaz en la que cada uno esté a la escucha. Dos servidores DNS no pueden estar a la escucha en la misma dirección. En este caso, supongamos que todas las consultas que entran a partir del cortafuegos se envían a 10.1.2.5. Estas consultas deben enviarse al servidor externo. Por lo tanto, el DNSB se ha configurado para estar a la escucha en 10.1.2.5. El servidor interno, DNSA, está configurado para que acepte las consultas procedentes de cualquier fuente en las direcciones IP de interfaz 10.1.x.x, excepto 10.1.2.5. Para excluirla eficazmente, esta dirección debe estar situada en la lista de coincidencia de direcciones (AML) antes que el prefijo de dirección incluido.

- Orden de la lista de coincidencia de direcciones

Se utiliza el primer elemento de una lista de coincidencia de direcciones con el que coincida una dirección dada. Por ejemplo, para permitir todas las direcciones de la red 10.1.x.x excepto 10.1.2.5, los elementos de la ACL deben estar en el orden (!10.1.2.5; 10.1/16). En este caso, la dirección 10.1.2.5 se compara con el primer elemento y se denegará inmediatamente.

Si los elementos están invertidos (10.1/16; !10.1.2.5), se permite el acceso a la dirección IP 10.1.2.5, porque el servidor la compara con el primer elemento, que coincide, y la aceptará sin comprobar las demás reglas.

Referencia relacionada:

“Características de BIND 9” en la página 8

BIND 9 se parece a BIND 8, pero proporciona varias características para mejorar el rendimiento del servidor Sistema de nombres de dominio (DNS), como las vistas.

“Ejemplo: dividir el DNS a través de un cortafuegos, utilizando una vista”

En este ejemplo se describe un servidor de sistema de nombres de dominio (DNS) que funciona a través de un cortafuegos para proteger los datos internos ante Internet, permitiendo a la vez que los usuarios internos accedan a los datos en Internet utilizando la característica *vista* proporcionada en BIND 9.

Ejemplo: dividir el DNS a través de un cortafuegos, utilizando una vista

En este ejemplo se describe un servidor de sistema de nombres de dominio (DNS) que funciona a través de un cortafuegos para proteger los datos internos ante Internet, permitiendo a la vez que los usuarios internos accedan a los datos en Internet utilizando la característica *vista* proporcionada en BIND 9.

En la siguiente figura se ve una subred simple que utiliza un cortafuegos por cuestión de seguridad. Supongamos que la empresa tiene una red interna con un espacio IP reservado, así como una sección externa de una red disponible para el público. La empresa desea que sus clientes internos puedan resolver los nombres de host externos e intercambiar correo con personas externas a la red. La empresa también desea que los usuarios internos que se encargan de resolver nombres tengan acceso a determinadas zonas que son exclusivamente internas y que no están disponibles fuera de la red interna. Sin embargo, la empresa no quiere que las personas externas encargadas de resolver nombres tengan acceso a la red interna.

Con el DNS de IBM i basado en BIND 9, puede implantar esta solución de dos maneras. La manera que se describe en este ejemplo consiste en que puede configurar el servidor DNS con dos vistas diferentes en las que estar a la escucha ante las diversas consultas, una para la intranet y otra para todo lo que

pertenezca al dominio público. Otra manera consiste en configurar dos instancias del servidor DNS en la misma plataforma IBM i, que se describe en el ejemplo sobre cómo dividir el DNS a través de un cortafuegos utilizando dos servidores DNS.

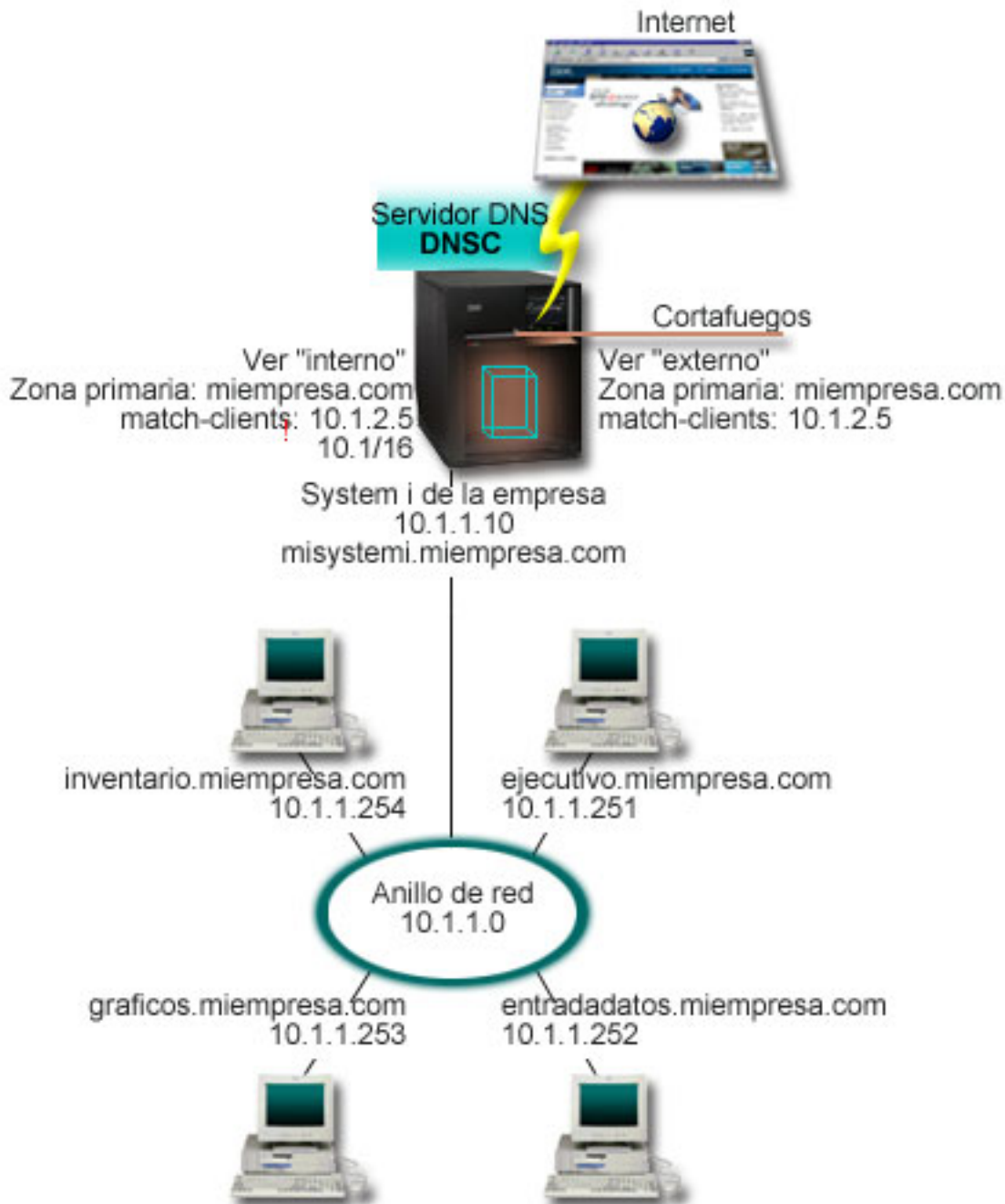


Figura 6. Dividir el DNS a través de un cortafuegos, utilizando una vista

El servidor DNS, DNSC, define dos vistas, llamadas *externa* e *interna*. La vista *externa* se configura con la zona primaria *miempresa.com*, que solo incluye los registros de recursos destinados a formar parte del dominio público, mientras que la vista *interna* se configura con la zona primaria *miempresa.com* que contiene los registros de recursos de la intranet.

Si le preocupa la integridad del cortafuegos u otros problemas de seguridad, puede optar por utilizar la subsentencia match-clients para contribuir a proteger los datos internos. Para ello, puede configurar la vista interna de manera que solo admita consultas a la zona interna miempresa.com procedentes de hosts internos. Debe tener en cuenta los siguientes valores de configuración para configurar la división de DNS:

- Match-clients

Match-clients en una sentencia de vista toma una lista de coincidencia de direcciones (AML) como argumento. Solo una dirección IP de la consulta que coincida con la lista de coincidencia de direcciones (AML) puede ver los valores de configuración definidos en la vista delimitadora. Si la dirección IP de una consulta coincide con múltiples entradas match-clients en diversas sentencias de vista (view), la primera sentencia de vista es la válida. En este caso, supongamos que todas las consultas que proceden del cortafuegos se envían a 10.1.2.5. Estas consultas las deben manejar los datos de la zona en la vista externa. Por lo tanto, se establece que 10.1.2.5 sea la dirección match-clients de la vista externa. La vista interna está configurada para que acepte las consultas procedentes de cualquier fuente en las direcciones IP de interfaz 10.1.x.x, excepto 10.1.2.5. Para excluirla eficazmente, esta dirección debe estar situada en la lista de coincidencia de direcciones (AML) antes que el prefijo de dirección incluido.

- Orden de la lista de coincidencia de direcciones

Se utiliza el primer elemento de una lista de coincidencia de direcciones con el que coincida una dirección dada. Por ejemplo, para permitir todas las direcciones de la red 10.1.x.x excepto 10.1.2.5, los elementos de la ACL deben estar en el orden (!10.1.2.5; 10.1/16). En este caso, la dirección 10.1.2.5 se compara con el primer elemento y se denegará inmediatamente.

Si los elementos están invertidos (10.1/16; !10.1.2.5), se permite el acceso a la dirección IP 10.1.2.5, porque el servidor la compara con el primer elemento, que coincide, y la aceptará sin comprobar las demás reglas.

Referencia relacionada:

“Ejemplo: dividir el DNS por el cortafuegos configurando dos servidores DNS en el mismo IBM i” en la página 22

En este ejemplo se describe un servidor de sistema de nombres de dominio (DNS) que funciona a través de un cortafuegos para proteger los datos internos ante Internet, permitiendo a la vez que los usuarios internos accedan a los datos en Internet. Esta configuración implanta esta protección configurando dos servidores DNS en la misma plataforma IBM i.

Elaborar un plan para el sistema de nombres de dominio (DNS)

El sistema de nombres de dominio (DNS) ofrece una serie de soluciones. Antes de configurar el DNS, conviene que planifique cómo funcionará en la red. Debe evaluar cuestiones como la estructura de la red, el rendimiento y la seguridad.

Determinar las autorizaciones del sistema de nombres de dominio (DNS)

Existen requisitos especiales de autorización para el administrador del sistema de nombres de dominio (DNS). Debe tener en cuenta también las implicaciones de seguridad de la autorización.

Al configurar el DNS, debe tomar medidas de precaución de seguridad para proteger su configuración. Debe establecer cuáles serán los usuarios autorizados para realizar cambios en la configuración.

Se necesita un nivel mínimo de autorización para permitir que el administrador pueda configurar y administrar el DNS. El hecho de otorgar acceso a todos los objetos garantiza que el administrador pueda realizar las tareas administrativas del DNS. Conviene otorgar a los usuarios que configuren el DNS acceso como responsables de seguridad con autorización sobre todos los objetos (*ALLOBJ). Utilice System i Navigator para autorizar a los usuarios. Si necesita más información, consulte el tema Otorgar autorización al administrador del DNS, en la ayuda en línea del DNS.

Nota: Si el perfil de un administrador no tiene plena autorización, debe otorgar acceso y autorización específicos a todos los directorios de DNS y archivos de configuración relacionados.

Referencia relacionada:

“Mantener los archivos de configuración del sistema de nombres de dominio (DNS)” en la página 43. Puede utilizar el DNS de IBM i para crear y gestionar instancias del servidor DNS en la plataforma IBM i. Los archivos de configuración del DNS se gestionan mediante IBM Navigator for i. NO debe editar manualmente los archivos. Utilice siempre IBM Navigator for i para crear, cambiar o suprimir los archivos de configuración del DNS.

Determinar la estructura del dominio

Si está configurando por primera vez un dominio, planifique sus necesidades y el mantenimiento antes de crear zonas.

Es importante determinar cómo va a dividir el dominio o los subdominios en zonas, cómo atender mejor a las demandas de la red, cómo acceder a Internet y cómo negociar los cortafuegos. Estos factores pueden resultar complejos y deben atenderse de uno en uno. Consulte otras fuentes autorizadas, como el manual O'Reilly DNS and BIND para obtener información más detallada.

Si configura una zona del sistema de nombres de dominio (DNS) como zona dinámica, no podrá realizar cambios manuales en los datos de la zona mientras el servidor esté en ejecución. Si lo hiciera, podría interferir en las actualizaciones dinámicas de entrada. Si es necesario realizar actualizaciones manuales, detenga el servidor, realice los cambios y luego reinicie el servidor. Las actualizaciones dinámicas que se envíen a un servidor DNS detenido nunca se llevarán a cabo. Por esta razón, es posible que desee configurar una zona dinámica y una zona estática por separado. Puede hacerlo creando zonas completamente separadas, o definiendo un subdominio nuevo (como `dynamic.miempresa.com`) para los clientes que se vayan a mantener de forma dinámica.

El DNS de IBM i proporciona una interfaz gráfica para configurar los sistemas. En algunos casos, la interfaz utiliza terminología y conceptos que podrían representarse de forma diferente en otras fuentes. Si consulta otras fuentes de información al planificar la configuración del DNS, le resultará útil recordar los siguientes puntos:

- Todas las zonas y objetos definidos en una plataforma IBM i están organizados en las carpetas Zonas de búsqueda directa y Zonas de búsqueda inversa. Las zonas de búsqueda directa se utilizan para correlacionar nombres de dominio con direcciones IP, como los registros A y AAAA. Las zonas de búsqueda inversa se utilizan para correlacionar direcciones IP con nombres de dominio, como los registros PTR.
- En el DNS de IBM i se emplean los términos *zonas primarias* y *zonas secundarias*.
- En la interfaz se utilizan *subzonas*, que en otras fuentes se denominan *subdominios*. Una zona hija es una subzona en la que se ha delegado la responsabilidad sobre uno o más servidores de nombres.

Planificar medidas de seguridad

El sistema de nombres de dominio (DNS) proporciona opciones de seguridad para limitar el acceso externo al servidor.

Listas de coincidencia de direcciones

El DNS utiliza listas de coincidencia de direcciones para permitir o denegar a entidades externas el acceso a determinadas funciones del DNS. Estas listas pueden incluir direcciones IP específicas, una subred (con un prefijo IP) o claves de signatura de transacciones (TSIG). Puede definir una lista de entidades a las que desee permitir o denegar el acceso e incluirlas en una lista de coincidencia de direcciones. Si desea poder reutilizar la lista de coincidencia de direcciones, puede guardarla como una lista de control de acceso (ACL). En adelante, siempre que necesite proporcionar la lista, puede llamar a la ACL para que se cargue la lista completa.

Orden de los elementos en la lista de coincidencia de direcciones

Se utiliza el primer elemento de una lista de coincidencia de direcciones con el que coincida una dirección dada. Por ejemplo, para permitir todas las direcciones de la red 10.1.1.x excepto la dirección 10.1.1.5, los elementos de la lista de coincidencia deben estar en este orden (!10.1.1.5; 10.1.1/24). En este caso, la dirección 10.1.1.5 se comparará con el primer elemento y se denegará inmediatamente.

Si los elementos están invertidos (10.1.1/24; !10.1.1.5), se permitirá el acceso a la dirección IP 10.1.1.5, porque el servidor la comparará con el primer elemento, que coincide, y la aceptará sin comprobar las demás reglas.

Opciones de control de acceso

El DNS le permite establecer limitaciones con respecto a quién puede enviar actualizaciones dinámicas al servidor, consultar datos y solicitar transferencias de zona. Puede utilizar listas de control de acceso (ACL) para restringir el acceso al servidor a las opciones siguientes:

allow-update

Para que el servidor DNS acepte las actualizaciones dinámicas de otras fuentes externas, debe habilitar la opción allow-update.

allow-query

Especifica qué hosts tienen permiso para consultar este servidor. Si no se especifica, el valor predeterminado es permitir las consultas procedentes de todos los hosts.

allow-transfer

Especifica qué hosts tienen permiso para recibir transferencias de zona del servidor. Si no se especifica, el valor predeterminado es permitir las transferencias procedentes de todos los hosts.

allow-recursion

Especifica qué hosts tienen permiso para realizar consultas recursivas mediante este servidor. Si no se especifica, el valor predeterminado es permitir consultas recursivas procedentes de todos los hosts.

blackhole

Especifica una lista de direcciones de las que el servidor no acepta consultas ni utiliza para resolver una consulta. Las consultas que proceden de estas direcciones no se responderán.

Es imprescindible proteger el servidor DNS. Además de las consideraciones sobre seguridad que se describen en este tema, la seguridad del DNS y la seguridad de IBM i se describen en una gran variedad de fuentes, incluida la plataforma IBM i y el temario de Internet. El manual *DNS and BIND* también describe la seguridad en relación con el DNS.

Conceptos relacionados:

System i y la seguridad en Internet

Referencia relacionada:

“Características de BIND 9” en la página 8

BIND 9 se parece a BIND 8, pero proporciona varias características para mejorar el rendimiento del servidor Sistema de nombres de dominio (DNS), como las vistas.

Requisitos del sistema de nombres de dominio (DNS)

Tenga en cuenta estos requisitos de software a la hora de ejecutar el sistema de nombres de dominio (DNS) en la plataforma IBM i.

La característica DNS, Opción 31, no se puede instalar automáticamente con el sistema operativo. Debe seleccionar el DNS específicamente para que se instale. El servidor DNS añadido para IBM i se basa en la implementación de DNS de estándar industrial conocida como BIND 9.

Una vez instalado el DNS, se le pedirá que migre y configure el servidor DNS de BIND 4 u 8 a BIND 9. También debe tener instalado IBM Navigator for i PASE (Opción 33 de i5/OS) y OpenSSH, OpenSSL, zlib(5733-SC1, opción 1). Una vez instalados estos dos programas de software, IBM Navigator for i maneja automáticamente la configuración de la implementación actual de BIND.

Si desea configurar el servidor del protocolo de configuración dinámica de hosts (DHCP) en una plataforma distinta para que envíe actualizaciones a este servidor DNS, también hay que instalar la opción 31 en ese servidor DHCP. El servidor DHCP emplea las interfaces de programación proporcionadas por la opción 31 para realizar actualizaciones dinámicas.

Conceptos relacionados:

i5/OS PASE

“Configurar el sistema de nombres de dominio (DNS)”

Puede utilizar IBM Navigator for i para configurar servidores de nombres y resolver consultas fuera de su dominio.

Referencia relacionada:

“Características de BIND 9” en la página 8

BIND 9 se parece a BIND 8, pero proporciona varias características para mejorar el rendimiento del servidor Sistema de nombres de dominio (DNS), como las vistas.

Determinar si el sistema de nombres de dominio (DNS) está instalado

Para determinar si el sistema de nombres de dominio (DNS) está instalado, siga estos pasos:

1. En la línea de mandatos, escriba G0 LICPGM y pulse Intro.
2. Escriba 10 (Ver los programas bajo licencia instalados) y pulse Intro.
3. Avance página hasta llegar a **5770SS1 Sistema de nombres de dominio** (Opción 31). Si el DNS se ha instalado satisfactoriamente, el estado de instalación será *COMPATIBLE, como se ve a continuación:

PgmLic	Estado instalación	Descripción
5770SS1	*COMPATIBLE	Sistema de nombres de dominio (DNS)

4. Pulse F3 para salir de la pantalla.

Instalar el sistema de nombres de dominio (DNS)

Para instalar el sistema de nombres de dominio (DNS), siga estos pasos.

1. En la línea de mandatos, escriba G0 LICPGM y pulse Intro.
2. Escriba 11 (Instalar programas bajo licencia) y pulse Intro.
3. Escriba 1 (Instalar) en el campo **Opción** junto a Sistema de nombres de dominio y pulse Intro.
4. Pulse Intro otra vez para confirmar la instalación.

Nota: El Sistema de nombres de dominio (DNS) también requiere las siguientes opciones de producción, que debe tener instaladas en el sistema.

- Portable App Solutions Environment(PASE) (5770-SS1, opción 33)
- OpenSSH, OpenSSL, zlib (5733-SC1, opción 1)

Configurar el sistema de nombres de dominio (DNS)

Puede utilizar IBM Navigator for i para configurar servidores de nombres y resolver consultas fuera de su dominio.

Antes de trabajar con la configuración del sistema de nombres de dominio (DNS), vea los requisitos del sistema de DNS para instalar los componentes del DNS necesarios.

Conceptos relacionados:

“Requisitos del sistema de nombres de dominio (DNS)” en la página 28

Tenga en cuenta estos requisitos de software a la hora de ejecutar el sistema de nombres de dominio (DNS) en la plataforma IBM i.

Acceder al sistema de nombres de dominio (DNS) en IBM Navigator for i

Estas instrucciones le orientarán en la interfaz de configuración de DNS en IBM Navigator for i.

Si se propone utilizar IBM i PASE, podrá configurar servidores DNS basados en BIND 9.

Si va a configurar el DNS por primera vez, siga estos pasos:

1. En IBM Navigator for i, expanda **Red > Servidores > Servidores DNS**.
2. Pulse la lista desplegable Acciones y seleccione el elemento de menú **Nuevo servidor de nombres**.

Conceptos relacionados:

Introducción a System i Navigator

Configurar servidores de nombres

El sistema de nombres de dominio (DNS) le permite crear múltiples instancias del servidor de nombres. Este tema proporciona las instrucciones para configurar un servidor de nombres.

El DNS de IBM i basado en BIND 9 admite múltiples instancias del servidor de nombres. Las tareas siguientes le guiarán durante el proceso de crear una instancia del servidor de nombres, incluidas sus propiedades y zonas.

Si desea crear múltiples instancias, repita estos procedimientos para cada una de las instancias que desee crear. En cada instancia del servidor de nombres puede especificar propiedades independientes, como los niveles de depuración y de inicio automático. Cuando crea una instancia nueva, se crean los distintos archivos de configuración.

Referencia relacionada:

“Mantener los archivos de configuración del sistema de nombres de dominio (DNS)” en la página 43
Puede utilizar el DNS de IBM i para crear y gestionar instancias del servidor DNS en la plataforma IBM i. Los archivos de configuración del DNS se gestionan mediante IBM Navigator for i. NO debe editar manualmente los archivos. Utilice siempre IBM Navigator for i para crear, cambiar o suprimir los archivos de configuración del DNS.

Crear una instancia del servidor de nombres

El asistente Nueva configuración de servidor de nombres DNS puede guiarle en el proceso de definir una instancia del servidor DNS.

Para iniciar el asistente **Nueva configuración de DNS**, siga estos pasos:

1. En IBM Navigator for i, expanda **Red > Servidores > Servidores DNS**.
2. En el árbol de navegación de la izquierda, seleccione **Crear servidor DNS**.
3. Siga las instrucciones del asistente para llevar a cabo el proceso de configuración.

El asistente necesita los siguientes datos de entrada:

Nombre de servidor DNS:

Especifique un nombre para el servidor DNS. Puede tener un máximo de 5 caracteres y debe empezar por un carácter alfabético (de la A a la Z). Si va a crear varios servidores, cada uno deberá tener un nombre exclusivo. En otras áreas del sistema, este es el nombre de la instancia del servidor DNS.

Direcciones IP de escucha:

No puede haber dos servidores DNS a la escucha en la misma dirección IP. El valor predeterminado consiste en estar a la escucha en todas las direcciones IP. Si se propone crear instancias de servidor adicionales, ninguna de ellas se puede configurar para estar a la escucha en todas las direcciones IP. De lo contrario, no se podrían ejecutar al mismo tiempo. Debe especificar la dirección IP que corresponde a cada servidor.

Servidores raíz:

Puede cargar la lista predeterminada de servidores raíz de Internet o bien especificar sus propios servidores raíz, como los servidores raíz internos de una intranet.

Nota: Solo debe considerar la posibilidad de cargar los servidores raíz de Internet predeterminados si tiene acceso a Internet y espera que su DNS pueda resolver plenamente los nombres de Internet.

Inicio del servidor:

Puede especificar si desea que el servidor se inicie automáticamente cuando se inicie el protocolo TCP/IP. Si trabaja con varios servidores, puede iniciar instancias individuales y finalizarlas independientemente unas de otras.

Editar las propiedades del servidor de sistema de nombres de dominio (DNS)

Después de crear un servidor de nombres, puede editar sus propiedades, por ejemplo la opción allow-update y los niveles de depuración. Estas opciones solo atañen a la instancia del servidor que se cambie.

Para editar las propiedades de la instancia del servidor de sistema de nombres de dominio (DNS), siga estos pasos:

1. En IBM Navigator for i, expanda **Red > Servidores > Servidores DNS**.
2. En el panel de la derecha, pulse *Nombre del servidor DNS* con el botón derecho del ratón y seleccione **Configuración**.
3. En la página Configuración de DNS, seleccione **Servidor DNS** y seleccione **Archivo > Propiedades**.
4. Edite las correspondientes propiedades que desee.

Configurar zonas en un servidor de nombres

Después de configurar una instancia de servidor el sistema de nombres de dominio (DNS), debe configurar las zonas para el servidor de nombres.

Para configurar zonas en el servidor, siga estos pasos:

1. En IBM Navigator for i, expanda **Red > Servidores > Servidores DNS**.
2. En el panel de la derecha, pulse *su servidor DNS* con el botón derecho del ratón y seleccione **Configuración**.
3. En la página Configuración de DNS, seleccione el tipo de zona que desea crear, pulsando la carpeta **Zona de búsqueda directa** o **Zona de búsqueda inversa**.
4. Seleccione **Archivo > Nuevo > Zona primaria/secundaria/apéndice/reenvío**.
5. Siga las instrucciones del asistente para llevar a cabo el proceso de creación.

Conceptos relacionados:

“Acceder a los datos de un sistema de nombres de dominio (DNS) externo” en la página 36
Si usted crea datos de zona de un sistema de nombres de dominio (DNS), el servidor podrá resolver las consultas sobre esa zona.

Tareas relacionadas:

“Configurar el sistema de nombres de dominio (DNS) para que reciba actualizaciones dinámicas”
Los servidores del sistema de nombres de dominio (DNS) que ejecutan BIND 9 se pueden configurar de modo que acepten peticiones de otras fuentes para actualizar dinámicamente los datos de la zona. Este tema ofrece instrucciones para configurar la opción allow-update para que el DNS pueda recibir actualizaciones dinámicas.

“Importar archivos del sistema de nombres de dominio (DNS)” en la página 35

El sistema de nombres de dominio (DNS) puede importar archivos de datos de zona existentes. Siga estos rápidos procedimientos para crear una nueva zona a partir de un archivo de configuración existente.

Referencia relacionada:

“Qué son las zonas” en la página 3

Los datos del sistema de nombres de dominio (DNS) se dividen en conjuntos gestionables de datos llamados *zonas*. Y cada uno de estos conjuntos corresponde a un tipo de zona concreto.

Configurar vistas en un servidor de nombres

Una de las características que ofrece BIND 9 es la sentencia *view* (vista), que permite que una sola instancia del sistema de nombres de dominio (DNS) responda a una consulta de manera diferente en función del lugar del que procede la consulta, como puede ser de Internet o de una intranet. Una aplicación práctica de la vista es que divide las configuraciones de DNS sin tener que ejecutar múltiples servidores DNS.

Para configurar vistas en el servidor, siga estos pasos:

1. En IBM Navigator for i, expanda **Red** > **Servidores** > **Servidores DNS**.
2. En el panel de la derecha, pulse *su servidor DNS* con el botón derecho del ratón y seleccione **Configuración**.
3. En la página Configuración de DNS, pulse **Vistas** y seleccione **Archivo** > **Nuevo** > **Vista**.
4. Siga las instrucciones del asistente para llevar a cabo el proceso de creación.

Configurar el sistema de nombres de dominio (DNS) para que reciba actualizaciones dinámicas

Los servidores del sistema de nombres de dominio (DNS) que ejecutan BIND 9 se pueden configurar de modo que acepten peticiones de otras fuentes para actualizar dinámicamente los datos de la zona. Este tema ofrece instrucciones para configurar la opción allow-update para que el DNS pueda recibir actualizaciones dinámicas.

Al crear zonas dinámicas, debe tener en cuenta la estructura de la red. Si todavía necesita realizar actualizaciones manuales en algunas partes del dominio, podría considerar la posibilidad de configurar las zonas dinámicas y estáticas por separado. Si tiene que realizar actualizaciones manuales en una zona dinámica, debe detener el servidor de la zona dinámica y, cuando haya llevado a cabo las actualizaciones, volver a iniciarlo. Al detenerlo, el servidor está obligado a actualizar la base de datos de la zona con todas las actualizaciones dinámicas que se hayan realizado desde que el servidor cargó por primera vez los datos de zona procedentes de la base de datos de la zona. Si no detiene el servidor, se perderán las actualizaciones manuales que se hayan realizado en la base de datos de la zona, porque el servidor en ejecución las sobrescribirá. Sin embargo, al detener el servidor para realizar actualizaciones manuales podría perderse las actualizaciones dinámicas que se envíen mientras el servidor está inactivo.

El DNS indica que una zona es dinámica cuando hay objetos definidos en la sentencia allow-update. Para configurar la opción allow-update, siga estos pasos:

1. En IBM Navigator for i, expanda **Red** > **Servidores** > **Servidores DNS**.
2. En el panel de la derecha, pulse *su servidor DNS* con el botón derecho del ratón y seleccione **Configuración**.
3. En la página Configuración de DNS, expanda **Zona de búsqueda directa** o **Zona de búsqueda inversa**.

4. Pulse la zona primaria que desee editar y seleccione **Archivo > Propiedades**.
5. En la página Propiedades de zona primaria, pulse la pestaña **Opciones**.
6. En la página Opciones, expanda **Control de acceso > allow-update**.
7. El DNS utiliza una lista de coincidencia de direcciones para verificar las actualizaciones autorizadas. Si desea añadir un objeto a la lista de coincidencia de direcciones, seleccione un tipo de elemento de dicha lista y pulse **Añadir**. Puede añadir una dirección IP, un prefijo IP, una lista de control de acceso o una clave.
8. Cuando haya terminado de actualizar la lista de coincidencia de direcciones, pulse **Aceptar** para cerrar la página Opciones.

Tareas relacionadas:

“Configurar zonas en un servidor de nombres” en la página 31

Después de configurar una instancia de servidor el sistema de nombres de dominio (DNS), debe configurar las zonas para el servidor de nombres.

Configurar el protocolo DHCP para que envíe actualizaciones dinámicas a DNS

“Efectuar actualizaciones manuales en una zona dinámica” en la página 39

Debe prestarse una atención especial a las actualizaciones manuales en IBM Navigator for i (por ejemplo, la adición de registro de recurso) de una zona dinámica si la instancia del servidor DNS está en ejecución, ya que pueden producirse conflictos entre los cambios manuales y las actualizaciones dinámicas.

Configurar DNSSEC

El sistema de nombres de dominio (DNS) permite configurar DNSSEC para un servidor de dominio. Este tema proporciona las instrucciones para configurar DNSSEC.

El DNS de IBM i basado en BIND 9 da soporte a DNSSEC. Las tareas le guiarán en el proceso de configuración de DNSSEC para un servidor de dominio.

Configurar claves de confianza/claves gestionadas

Las instrucciones siguientes pueden servirle de guía en el proceso de configuración de claves de confianza/claves gestionadas.

Para configurar claves de confianza/claves gestionadas, siga estos pasos:

1. En IBM Navigator for i, expanda **Red > Servidores > Servidores DNS**.
2. Pulse el servidor DNS con el botón derecho del ratón y seleccione **Configuración**.
3. Pulse el nodo del servidor DNS en el árbol y seleccione **Archivo > Propiedades**.
4. Pulse la pestaña **Claves de confianza/claves gestionadas**, Añadir/Editar/Suprimir/Ver las claves.
5. Pulse Aceptar

Configurar las opciones de DNSSEC

Las instrucciones siguientes pueden servirle de guía en el proceso de configuración de opciones de DNSSEC.

Para habilitar las opciones de DNSSEC, siga estos pasos:

1. En IBM Navigator for i, expanda **Red > Servidores > Servidores DNS**.
2. Pulse el servidor DNS con el botón derecho del ratón y seleccione **Configuración**.
3. Pulse el nodo del servidor DNS en el árbol y seleccione **Archivo > Propiedades**.
4. Pulse la pestaña Opciones y expanda **Opciones > Opciones booleanas**.
5. Pulse la opción **dnssec-enable** y marque el recuadro de selección Habilitar para habilitarla.
6. Pulse la opción **dnssec-validation** y marque el recuadro de selección Habilitar para habilitarla.
7. Pulse Aceptar

Firmar una zona primaria

Las instrucciones siguientes pueden servirle de guía en el proceso de firmar una zona en un servidor DNS.

Para firmar una zona, siga estos pasos:

1. En IBM Navigator for i, expanda **Red > Servidores > Servidores DNS**.
2. Pulse el servidor DNS con el botón derecho del ratón y seleccione **Configuración**.
3. Expanda Servidor DNS > Zonas de búsqueda directa/Zonas de búsqueda inversa y seleccione la zona primaria que desee firmar.
4. Seleccione **Archivo > DNSSEC > Firmar**.
5. Siga las instrucciones del asistente para llevar a cabo el proceso de firma.

Nota: Una zona debe firmarse con claves ZSK y KSK. Cree las claves ZSK y KSK utilizadas para firmar con la opción "NEW".

Volver a firmar una zona primaria

Las instrucciones siguientes pueden servirle de guía en el proceso de volver a firmar una zona en un servidor DNS.

Para volver a firmar una zona, siga estos pasos:

1. En IBM Navigator for i, expanda **Red > Servidores > Servidores DNS**.
2. Pulse el servidor DNS con el botón derecho del ratón y seleccione **Configuración**.
3. Expanda Servidor DNS > Zonas de búsqueda directa/Zonas de búsqueda inversa y seleccione la zona primaria que desee volver a firmar.
4. Seleccione **Archivo > DNSSEC > Volver a firmar**.
5. Siga las instrucciones del asistente para llevar a cabo el proceso de volver a firmar.

Nota: Una zona puede volver a firmarse con nuevas claves ZSK o KSK. Cree las claves utilizadas para volver a firmar con la opción "NEW".

Tareas relacionadas:

"Volver a firmar una zona" en la página 40

Para una zona primaria firmada, si se han realizado nuevos cambios en los registros de recurso de la zona, ésta debe volver a firmarse.

Retirar la firma de una zona primaria

Las instrucciones siguientes pueden servirle de guía en el proceso de retirar la firma de una zona en un servidor DNS.

Para retirar la firma de una zona, siga estos pasos:

1. En IBM Navigator for i, expanda **Red > Servidores > Servidores DNS**.
2. Pulse el servidor DNS con el botón derecho del ratón y seleccione **Configuración**.
3. Expanda Servidor DNS > Zonas de búsqueda directa/Zonas de búsqueda inversa y seleccione la zona primaria cuya firma desea retirar.
4. Seleccione **Archivo > DNSSEC > Retirar firma**.
5. Siga las instrucciones del asistente para llevar a cabo el proceso de retirada de firma.

Configurar DNSSEC para una zona dinámica

Este tema proporciona instrucciones para configurar DNSSEC para una zona dinámica.

Para una zona segura (firmada), también puede configurar las opciones allow-update o update-policy para convertirla en una zona dinámica. Tenga en cuenta que las opciones allow-update y update-policy

tienen una función similar, por lo que es suficiente configurar una de ellas. También puede configurar la opción auto-dnssec para que la zona realice la firma de zona automática.

Configurar la opción allow-update:

Los servidores del sistema de nombres de dominio (DNS) que ejecutan BIND 9 se pueden configurar de modo que acepten peticiones de otras fuentes para actualizar dinámicamente los datos de la zona. Este tema ofrece instrucciones para configurar la opción allow-update para que el DNS pueda recibir actualizaciones dinámicas.

Consulte la sección “Configurar el sistema de nombres de dominio (DNS) para que reciba actualizaciones dinámicas” en la página 32.

Configurar la opción update-policy:

Las instrucciones siguientes pueden servirle de guía en el proceso de configuración de la opción update-policy.

Para configurar la opción update-policy, siga estos pasos:

1. En IBM Navigator for i, expanda **Red > Servidores > Servidores DNS**.
2. Pulse el servidor DNS con el botón derecho del ratón y seleccione **Configuración**.
3. Expanda Servidor DNS > Zonas de búsqueda directa/Zonas de búsqueda inversa y seleccione la zona primaria que desee configurar.
4. Seleccione **Archivo > Propiedades**.
5. Pulse la pestaña Opciones y expanda **Opciones > Opciones booleanas**.
6. Pulse la opción update-policy, especifique la utilización de las reglas de política de actualización local o pulse Añadir para añadir una.
7. Pulse Aceptar.

Configurar la opción auto-dnssec:

Las instrucciones siguientes pueden servirle de guía en el proceso de configuración de la opción auto-dnssec.

Para configurar la opción auto-dnssec, siga estos pasos:

1. En IBM Navigator for i, expanda **Red > Servidores > Servidores DNS**.
2. Pulse el servidor DNS con el botón derecho del ratón y seleccione **Configuración**.
3. Expanda Servidor DNS > Zonas de búsqueda directa/Zonas de búsqueda inversa y seleccione la zona primaria que desee configurar.
4. Seleccione **Archivo > Propiedades**.
5. Pulse la pestaña Opciones y expanda **Opciones > Otras**.
6. Pulse la opción auto-dnssec y seleccione Permitir/Mantener/Desactivar
7. Pulse Aceptar.

Importar archivos del sistema de nombres de dominio (DNS)

El sistema de nombres de dominio (DNS) puede importar archivos de datos de zona existentes. Siga estos rápidos procedimientos para crear una nueva zona a partir de un archivo de configuración existente.

Puede crear una zona primaria importando un archivo de datos de zona que sea un archivo de configuración de zona válido basado en la sintaxis de BIND. El archivo debe estar situado en un directorio del sistema de archivos integrado. Cuando se importa, el DNS verifica que es un archivo de datos de zona válido y lo añade al archivo named.conf de la instancia de servidor especificada.

Para importar un archivo de zona, siga estos pasos:

1. En IBM Navigator for i, expanda **Red > Servidores > Servidores DNS**.
2. En el panel de la derecha, pulse el servidor DNS con el botón derecho del ratón y seleccione **Configuración**.
3. En la página Configuración de DNS, seleccione **Archivo > Importar zona**.
4. Siga las instrucciones del asistente para importar la zona primaria.

Tareas relacionadas:

“Configurar zonas en un servidor de nombres” en la página 31

Después de configurar una instancia de servidor el sistema de nombres de dominio (DNS), debe configurar las zonas para el servidor de nombres.

Validación de registros

La función Importar datos de dominio lee y valida cada registro del archivo que se está importando.

Una vez que la función Importar datos de dominio haya terminado, los registros en los que se haya producido algún error podrán examinarse de forma individual en la página de propiedades Otros registros, de la zona importada.

Notas:

1. La importación de un dominio primario grande puede tardar varios minutos.
2. La función Importar datos de dominio no admite la instrucción \$include. El proceso que comprueba la validez de la función Importar datos de dominio identifica las líneas que contienen la instrucción \$include como líneas erróneas.

Acceder a los datos de un sistema de nombres de dominio (DNS) externo

Si usted crea datos de zona de un sistema de nombres de dominio (DNS), el servidor podrá resolver las consultas sobre esa zona.

Los servidores raíz son esenciales en el funcionamiento de un servidor DNS que esté directamente conectado a Internet o a una intranet extensa. Los servidores DNS deben utilizar servidores raíz para responder a las consultas sobre hosts que no sean los que se encuentran en sus propios archivos de dominio.

Para conseguir más información, un servidor DNS debe saber dónde buscar. En Internet, el primer lugar donde busca un servidor DNS son los servidores raíz. Los servidores raíz remiten un servidor DNS a otros servidores de la jerarquía hasta que se encuentra una respuesta, o bien se determina que no existe ninguna respuesta.

Lista predeterminada de servidores raíz de IBM Navigator for i

Solo debe utilizar los servidores raíz de Internet si tiene una conexión a Internet y desea resolver los nombres de Internet en caso de que no los resuelva el servidor DNS. En IBM Navigator for i se suministra una lista predeterminada de los servidores raíz de Internet. La lista está actualizada en el momento de la entrega de IBM Navigator for i. Puede verificar si la lista predeterminada está actualizada comparándola con la lista del sitio InterNIC. Restablezca la lista de servidores raíz de su configuración para mantenerla actualizada.

Obtener las direcciones de los servidores raíz de Internet

Las direcciones de los servidores raíz superiores cambian periódicamente, y mantenerlas actualizadas es responsabilidad del administrador de DNS. InterNIC mantiene una lista actualizada de las direcciones de los servidores raíz de Internet. Para conseguir la lista actualizada de dichos servidores, siga estos pasos:

1. Inicie sesión en el servidor InterNIC utilizando el protocolo de transferencia de archivos (FTP) en el método anonymity: FTP.INTERNIC.NET o RS.INTERNIC.NET
2. Baje este archivo: /domain/named.root
3. Almacene el archivo en la siguiente vía de acceso del directorio: /QOpenSys/QIBM/ProdData/OS400/DNS/ROOT.FILE

Es posible que un servidor DNS que se encuentre tras un cortafuegos no tenga definido ningún servidor raíz. En ese caso, el servidor DNS solo puede resolver las consultas que procedan de las entradas que existen en los archivos de su propia base de datos del dominio primario o en su caché. Podría reenviar consultas desde otro sitio al DNS cortafuegos. En ese caso, el servidor DNS cortafuegos actúa como remitente.

Servidores raíz de una intranet

Si su servidor DNS forma parte de una intranet extensa, es posible que tenga servidores raíz internos. Si su servidor DNS no va a acceder a Internet, no es necesario que cargue los servidores Internet predeterminados. Sin embargo, deberá añadir los servidores raíz internos para que el servidor DNS pueda resolver las direcciones internas fuera de su dominio.

Tareas relacionadas:

“Configurar zonas en un servidor de nombres” en la página 31

Después de configurar una instancia de servidor el sistema de nombres de dominio (DNS), debe configurar las zonas para el servidor de nombres.

Gestionar el sistema de nombres de dominio (DNS)

La tarea de gestionar el sistema de nombres de dominio (DNS) incluye verificar el funcionamiento de la función DNS, el mantenimiento de DNSSEC, supervisar el rendimiento, y mantener los datos y archivos del DNS.

Conceptos relacionados:

“Introducción a las Extensiones de seguridad de DNS (DNSSEC)” en la página 15

DNSSEC es un conjunto de especificaciones RFC IETF que añaden ampliaciones de seguridad a DNS.

Verificar el funcionamiento de la función del sistema de nombres de dominio (DNS)

La herramienta Sonda de información de dominio (DIG) le ayudará a recoger información procedente de un servidor de sistema de nombres de dominio (DNS) y a someter a prueba su respuesta. Puede utilizar DIG para verificar si un servidor DNS funciona correctamente.

Solicite el nombre de host que está asociado a la dirección IP de bucle de retorno (127.0.0.1). Debería responder con el nombre de host (local). También puede solicitar nombres específicos que estén definidos en la instancia de servidor que está intentando verificar. De esta forma se confirma que la instancia de servidor específica que está sometiendo a prueba funciona correctamente.

Para verificar la función del DNS con DIG, siga estos pasos:

1. En la línea de mandatos, teclee `DIG HOSTNAME('127.0.0.1') REVERSE(*YES)`.

Debe aparecer esta información, incluido el nombre de host de bucle de retorno:

```
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id:865
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL:1

;; QUESTION SECTION:
;1.0.0.127.in-addr.arpa.      IN      PTR
```

```
;; ANSWER SECTION:
1.0.0.127.in-addr.arpa. 86400 IN PTR localhost.

;; AUTHORITY SECTION:
0.0.127.in-addr.arpa. 86400 IN NS ISA2LP05.RCHLAND.IBM.COM.

;; ADDITIONAL SECTION:
ISA2LP05.RCHLAND.IBM.COM. 38694 IN A 9.5.176.194

;; Query time: 552 msec
;; SERVER: 9.5.176.194#53(9.5.176.194)
;; WHEN: Thu May 31 21:38:12 2007
;; MSG SIZE rcvd: 117
```

El servidor DNS responde correctamente si devuelve el nombre de host de bucle de retorno **localhost**.

2. Pulse Intro para salir de la sesión.

Nota: Si necesita ayuda para utilizar DIG, teclee ?DIG y pulse Intro.

Gestionar las claves de seguridad

Las claves de seguridad le permiten limitar el acceso a los datos del sistema de nombres de dominio (DNS).

Existen dos tipos de claves relacionadas con el DNS, que son las claves DNS y las claves de actualización dinámica. Cada una desempeña un papel diferente en la protección de la configuración del DNS. En las descripciones siguientes se explica la forma en que cada una de ellas está relacionada con su servidor DNS.

Gestionar las claves del sistema de nombres de dominio (DNS)

Las claves del sistema de nombres de dominio (DNS) son claves que están definidas para BIND y que el servidor DNS utiliza como parte de la verificación de una actualización entrante.

Las claves pueden configurarse y se les puede asignar un nombre. A continuación, cuando desee proteger un objeto de DNS (como una zona dinámica), puede especificar la clave en la lista de coincidencia de direcciones (AML).

Para gestionar las claves de DNS siga estos pasos:

1. En IBM Navigator for i, expanda **Red > Servidores > Servidores DNS**.
2. En el panel de la derecha, pulse con el botón derecho del ratón la instancia de servidor DNS que desea gestionar y seleccione **Configuración**.
3. En la página Configuración de DNS, seleccione **Archivo > Gestionar claves**.

En la página Gestionar claves, puede realizar las correspondientes tareas de gestión.

Gestionar claves de actualización dinámica

Las claves de actualización dinámica se utilizan con el objeto de proteger las actualizaciones dinámicas que realiza el servidor del protocolo de configuración dinámica de hosts (DHCP).

Estas claves deben estar presentes cuando el sistema de nombres de dominio (DNS) y DHCP están en la misma plataforma de IBM i. Si DHCP está en una plataforma IBM i distinta, debe distribuir los mismos archivos de claves de actualización dinámica a cada plataforma IBM i que los necesite para enviar actualizaciones dinámicas a los servidores autorizados. Puede distribuirlas por FTP, correo electrónico, etcétera.

Para gestionar las claves de actualización dinámica, siga estos pasos:

1. En IBM Navigator for i, expanda **Red > Servidores > Servidores DNS**.
2. Seleccione **Gestionar claves de actualización dinámica DNS**.

A continuación puede realizar las tareas de gestión que corresponda en la página Gestionar claves de actualización dinámica.

Efectuar actualizaciones manuales en una zona dinámica

Debe prestarse una atención especial a las actualizaciones manuales en IBM Navigator for i (por ejemplo, la adición de registro de recurso) de una zona dinámica si la instancia del servidor DNS está en ejecución, ya que pueden producirse conflictos entre los cambios manuales y las actualizaciones dinámicas.

Si necesita añadir, editar o suprimir un registro de recurso para una zona dinámica, es aconsejable utilizar el mandato RUNDNSUPD o NSUPDATE en la interfaz basada en caracteres para enviar solicitudes de actualización dinámica al servidor DNS. Por ejemplo, los mandatos siguientes añaden un registro A con la dirección IP 192.168.1.100 para myhost.mycompany.com.

```
RUNDNSUPD BCHFILE(*NONE)
> update add myhost.mycompany.com 86400 A 192.168.1.100
> send
> quit
```

Nota: las líneas que empiezan por '>' son mandatos interactivos emitidos después de ejecutar RUNDNSUPD.

Si debe realizar cambios manuales en IBM Navigator for i, puede utilizar el mandato RNDC en la interfaz basada en caracteres para sincronizar el archivo de zona antes de realizar los cambios. Tenga en cuenta que puede perder actualizaciones dinámicas enviadas durante los cambios manuales.

Para realizar cambios manuales, siga estos pasos (se presupone que el servidor DNS está en ejecución):

1. Cierre todas las páginas de configuración de DNS abiertas en IBM Navigator for i.
2. En la interfaz basada en caracteres, especifique el mandato RNDC RNDCCMD(freeze nombre_zona) en la línea de mandatos, donde nombre_zona es el nombre de la zona dinámica. Este mandato provoca el bloqueo de la zona y la sincronización de las actualizaciones dinámicas (almacenadas en el archivo de diario) en el archivo de zona. En una zona bloqueada, las actualizaciones dinámicas dejarán de aceptarse. Tenga en cuenta que el archivo de diario de la zona se eliminará después de ejecutar este mandato.
3. Detenga la instancia del servidor en IBM Navigator for i; o bien, en la interfaz basada en caracteres, especifique el mandato RNDC RNDCCMD(stop) en la línea de mandatos.
4. Realice los cambios manuales en la zona en IBM Navigator for i., por ejemplo, la adición de registros de recurso.
5. Reinicie la instancia de servidor en IBM Navigator for i; o bien, especifique STRTCPSVR SERVER(*DNS) DNSSVR(nombre_instancia) en la línea de mandatos para reiniciar el servidor, donde nombre_instancia es el nombre de la instancia de servidor.
6. En la interfaz basada en caracteres, especifique el mandato RNDC RNDCCMD(thaw nombre_zona) en la línea de mandatos, donde nombre_zona es el nombre de la zona dinámica. Este mandato hace que la zona vuelva a cargarse y que vuelvan a aceptarse las actualizaciones dinámicas de la zona.

Tareas relacionadas:

“Configurar el sistema de nombres de dominio (DNS) para que reciba actualizaciones dinámicas” en la página 32

Los servidores del sistema de nombres de dominio (DNS) que ejecutan BIND 9 se pueden configurar de modo que acepten peticiones de otras fuentes para actualizar dinámicamente los datos de la zona. Este tema ofrece instrucciones para configurar la opción allow-update para que el DNS pueda recibir actualizaciones dinámicas.

Gestionar DNSSEC

Este tema presenta el mantenimiento de DNSSEC en la plataforma IBM i.

Conceptos relacionados:

“Introducción a las Extensiones de seguridad de DNS (DNSSEC)” en la página 15

DNSSEC es un conjunto de especificaciones RFC IETF que añaden ampliaciones de seguridad a DNS.

Verificar el funcionamiento de la función DNSSEC

Puede utilizar la herramienta DIG (Rastreador de información de dominio) para comprobar si la función DNSSEC funciona correctamente.

Supongamos que tiene una zona firmada denominada example.com en el servidor DNS y, dentro de dicha zona, existe un registro A 192.168.1.101 para host1.example.com.

Para comprobar la función DNSSEC con DIG, siga estos pasos:

1. En la línea de mandatos, especifique DIG HOSTNAME(host1.example.com) DMNNSVR('127.0.0.1') DNSSEC(*YES).

El servidor DNS está respondiendo correctamente si el código de estado es NOERROR y existen registros A y RRSIG en la sección ANSWER como los siguientes:

```
;; global options:  +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 64408
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 2, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;host1.example.com.          IN      A

;; ANSWER SECTION:
host1.example.com.          172800  IN      A          192.168.1.101
host1.example.com.          172800  IN      RRSIG      A 5 3 172800 20131116055306 20131017055306 11643
example.com. i4xLG5Zic+ifzvdUe91jjPlys2tjM3f1KFSa6H/iDnQfcUNWAS6aEDPY Tpr5ir6xs72mqJYepK5uaWarxDZAZ
a86yf7QjRI+9ab7t360+0g9DRGT q$3G/8JfyZIFeck1QSYT6Hm3JCdaWMWPEfT+l/sYfS3H1YDdN9RxrXMN 5I0=

;; AUTHORITY SECTION:
example.com.                172800  IN      NS          ...
example.com.                172800  IN      RRSIG      NS ...
...
```

2. Pulse Intro para salir de la sesión.

Volver a firmar una zona

Para una zona primaria firmada, si se han realizado nuevos cambios en los registros de recurso de la zona, ésta debe volver a firmarse.

Considere los casos siguientes:

- Se añaden nuevos registros de recurso (registros de recurso A, MX, etc.) a una zona firmada o se cambian registros existentes
- Se cambian claves ZSK/KSK o van a caducar
- Se reciben solicitudes de actualización dinámica para una zona dinámica

Para una zona estática, si se cambian claves ZKS/KSK u otros registros de recurso, deberá volver a firmar la zona manualmente. Para una zona dinámica, la instancia de servidor volverá a firmar automáticamente la zona una vez recibidas las actualizaciones dinámicas, por lo que no es necesario volver a firmarla manualmente.

Conceptos relacionados:

“Actualizaciones dinámicas” en la página 6

El sistema de nombres de dominio (DNS) de IBM i que está basado en BIND 9 admite las actualizaciones dinámicas. Las fuentes externas, como el protocolo de configuración dinámica de hosts (DHCP), pueden enviar actualizaciones al servidor DNS. Además, también se pueden utilizar las herramientas de cliente DNS, como el programa de utilidad de actualización dinámica (NSUPDATE), para realizar actualizaciones dinámicas.

Tareas relacionadas:

“Volver a firmar una zona primaria” en la página 34

Las instrucciones siguientes pueden servirle de guía en el proceso de volver a firmar una zona en un servidor DNS.

Consideración sobre la renovación de claves

Por razones de seguridad las claves KSK/ZSK deben renovarse periódicamente.

Es aconsejable sustituir las claves KSK cada 12 meses y las claves ZSK mensual o trimestralmente.

Gestionar DNSSEC para una zona dinámica

Este tema presenta el mantenimiento de DNSSEC para una zona dinámica.

DNSSEC y actualizaciones dinámicas

Si una zona dinámica despliega DNSSEC, el servidor DNS volverá a firmar periódicamente la zona para asegurarse de que también se firmen los registros sin firmar debidos a actualizaciones dinámicas.

Nota: el servidor DNS necesita conocer la ubicación de las claves privadas ZSK/KSK para firmar la zona, por lo que es necesario configurar una opción key-directory para una zona dinámica que utilice DNSSEC.

Mantener DNSSEC mediante el mandato NSUPDATE

Puede utilizar el mandato NSUPDATE para realizar operaciones relacionadas con DNSSEC para una zona dinámica. Por ejemplo, puede utilizarlo para añadir claves ZSK/KSK a una zona dinámica para firmar la zona o realizar la renovación de claves.

A continuación se indican los pasos necesarios para firmar una zona dinámica añadiendo claves ZSK/KSK a dicha zona:

1. Prepare el archivo de proceso por lotes (batch.file) que debe ejecutarse. El contenido del archivo de proceso por lotes puede ser parecido al siguiente. Tenga en cuenta que hay una línea en blanco al final del archivo.

```
ttl 3600
update add domainname DNSKEY 256 3 7 AwEAA...
update add domainname DNSKEY 257 3 7 AwEAA...
send
```

2. En la interfaz basada en caracteres, especifique el mandato NSUPDATE BCHFILE(batch.file) en la línea de mandatos y pulse Intro.

Firma de zona automática/renovación de claves automática para una zona dinámica

Configurando la opción auto-dnssec como “maintain”, puede hacer que la zona dinámica se firma automáticamente y que las claves ZSK/KSK se renueven automáticamente. Simplemente debe suministrar las claves ZSK/KSK correspondientes para el mantenimiento de zona. Siga estos pasos para preparar las claves:

1. Prepare las claves ZSK/KSK adecuadas utilizadas para firmar la zona. Estas claves pueden generarse utilizando el mandato GENDNSKEY en la interfaz basada en caracteres.
2. Otorgue al usuario QTCP el privilegio de acceso a las claves ZSK/KSK y a los archivos de zona.

En la interfaz basada en caracteres, para cada clave pública, especifique el mandato CHGAUT OBJ('/QIBM/UserData/OS400/DNS/_DYN/K<id-clave-n>.+aaa+nnnnn.key') USER(QTCP) DTAAUT(*RWX) OBJAUT(*ALL); para cada clave privada, especifique el mandato CHGAUT OBJ('/QIBM/UserData/OS400/DNS/_DYN/K<id-clave-n>.+aaa+nnnnn.private') USER(QTCP) DTAAUT(*RWX) OBJAUT(*ALL); para el archivo de zona utilizado, especifique el mandato CHGAUT OBJ('/QIBM/UserData/OS400/DNS/<instancia>/zonefile') USER(QTCP) DTAAUT(*RWX) OBJAUT(*ALL)

Nota: Puede consultar la sección “Configurar DNSSEC para una zona dinámica” en la página 34 para conocer los pasos de configuración de la opción auto-dnssec.

Acceder a las estadísticas del servidor de sistema de nombres de dominio (DNS)

Las herramientas de estadísticas y vuelco de la base de datos le ayudarán a revisar y gestionar el rendimiento del servidor.

El sistema de nombres de dominio (DNS) proporciona varias herramientas de diagnóstico. Pueden utilizarse para supervisar el rendimiento del servidor.

Referencia relacionada:

“Mantener los archivos de configuración del sistema de nombres de dominio (DNS)” en la página 43
Puede utilizar el DNS de IBM i para crear y gestionar instancias del servidor DNS en la plataforma IBM i. Los archivos de configuración del DNS se gestionan mediante IBM Navigator for i. NO debe editar manualmente los archivos. Utilice siempre IBM Navigator for i para crear, cambiar o suprimir los archivos de configuración del DNS.

Acceder a las estadísticas del servidor

Las estadísticas del servidor resumen el número de consultas y respuestas que el servidor ha recibido desde la última vez que reinició y recargó su base de datos.

El sistema de nombres de dominio (DNS) le permite ver las estadísticas de una instancia del servidor. La información se va agregando a este archivo de forma constante hasta que lo suprima. Esta información puede resultar útil para evaluar la cantidad de tráfico que recibe el servidor y para detectar los posibles problemas. Hay más información disponible sobre las estadísticas del servidor en el tema Qué son las estadísticas del servidor DNS, en la ayuda en línea del DNS.

Para acceder a las estadísticas del servidor, siga estos pasos:

1. En IBM Navigator for i, expanda **Red > Servidores > Servidores DNS**.
2. En el panel de la derecha, pulse *su servidor DNS* con el botón derecho del ratón y seleccione **Configuración**.
3. En la página Configuración de DNS, seleccione **Ver > Estadísticas del servidor**.

También puede utilizar el mandato Control de daemon de nombres remoto (**RNDC**) para visualizar la información de estadísticas del servidor en el archivo named.stats. El correspondiente mandato es como se indica a continuación.

```
RNDC RNDCCMD('stats')
```

Acceder a una base de datos del servidor activo

La base de datos del servidor activo contiene información de zona y de host, que incluye algunas propiedades de zona, como información sobre el inicio de autorización (SOA), y las propiedades entre los hosts, como información sobre el intercambiador de correo (MX), que puede ser útil para detectar posibles problemas.

El sistema de nombres de dominio (DNS) le permite ver un vuelco de los datos autorizados, los datos de la caché y otros datos para una instancia de servidor. El vuelco incluye la información que procede de las zonas primaria y secundaria del servidor (zonas de correlación directa e inversa), así como la información que el servidor ha obtenido a partir de las consultas.

Puede ver el vuelco de la base de datos del servidor activo utilizando IBM Navigator for i. Si tiene que guardar una copia de los archivos, el nombre de archivo del vuelco de la base de datos es `named_dump.db` y está en la vía de acceso del directorio de IBM i: `/QIBM/UserData/OS400/DNS/<instancia de servidor>/`, siendo `<instancia de servidor>` el nombre de la instancia del servidor DNS. Hallará más información sobre la base de datos del servidor activo en la ayuda en línea del DNS, en el tema `Qué es el vuelco de la base de datos del servidor DNS`.

Para acceder al vuelco de la base de datos del servidor activo siga estos pasos:

1. En IBM Navigator for i, expanda **Red > Servidores > Servidores DNS**.
2. En el panel de la derecha, pulse *Nombre del servidor DNS* con el botón derecho del ratón y seleccione **Configuración**.
3. En la página Configuración de DNS, seleccione **Ver > Base de datos del servidor activo**.

También puede utilizar el mandato Control de daemon de nombres remoto (**RNDC**) para visualizar la información de base de datos del servidor activo en el archivo `named_dump.db` file. El correspondiente mandato es como se indica a continuación.



```
RNDC RNDCCMD('dumpdb -a11')
```

Mantener los archivos de configuración del sistema de nombres de dominio (DNS)











Puede utilizar el DNS de IBM i para crear y gestionar instancias del servidor DNS en la plataforma IBM i. Los archivos de configuración del DNS se gestionan mediante IBM Navigator for i. NO debe editar manualmente los archivos. Utilice siempre IBM Navigator for i para crear, cambiar o suprimir los archivos de configuración del DNS.








Los archivos de configuración del DNS se almacenan en las vías de acceso del sistema de archivos integrado que figuran a continuación.





Nota: Esta estructura de archivos atañe a un DNS que se ejecute en BIND 9.

En la tabla siguiente, los archivos se enumeran con la jerarquía de vías de acceso que se muestra. Hay que hacer copia de seguridad de los archivos que presenten un icono de guardar  , para proteger los datos. Los archivos que presentan un icono de suprimir  se deben suprimir con regularidad.

Nombre	Icono	Descripción
<code>/QIBM/UserData/OS400/DNS/</code>		Directorio de partida de DNS.
<code>/QIBM/UserData/OS400/DNS/<instancia-n>/</code>		Directorio de partida de una instancia de DNS.

Nombre	Icono	Descripción
ATTRIBUTES		El DNS utiliza este archivo para determinar la versión de BIND que se está utilizando.
BOOT.AS400BIND4		Archivo de configuración y de políticas del servidor BIND 4.9.3 que se convierte al archivo named.conf de BIND 8 para esta instancia. Este archivo se crea si migra un servidor BIND 4.9.3 a BIND 9. Hace las veces de copia de seguridad para la migración, y se puede suprimir cuando el servidor BIND 9 ya funcione correctamente.
named.ca		Lista de servidores raíz para esta instancia del servidor.
named.conf		Este archivo contiene los datos de configuración. Indicar al servidor qué zonas específicas está gestionando, dónde están los archivos de zona, qué zonas se pueden actualizar dinámicamente, dónde están los servidores de reenvío, además de otras opciones.
named_dump.db		Vuelco de datos de servidor que se crea para la base de datos del servidor activo.
named.memstats		Estadísticas de memoria de servidor (si se han configurado en named.conf).
named.pid		Mantiene el ID de proceso del servidor en ejecución. Este archivo se crea cada vez que se inicia el servidor DNS. Se utiliza para las funciones Base de datos, Estadísticas y Actualizar del servidor. No debe suprimir ni modificar este archivo.
named.random		Archivo de entropía generado por el servidor.
named.recursing		Consultas de servidores que son recursivas (si IBM Navigator for i las solicita).
named.run		Archivo de anotaciones de depuración predeterminado (si se solicita). El archivo se puede relevar tomando los nombres named.run.0, named.run.1, y así sucesivamente.
named.stats		Estadísticas del servidor.
<zona-primaria-n>.db		Archivo de zona primaria de un determinado dominio en este servidor. El archivo contiene todos los registros de recursos de esta zona. Cada zona tiene un archivo .db aparte.

Nombre	Icono	Descripción
<zona-primaria-n>.jnl		Archivos de diario que contienen las actualizaciones dinámicas de una zona. Se crea la primera cuando se recibe la primera actualización dinámica. El servidor, cuando se reinicia después de una conclusión o una caída del sistema, reproduce el archivo de diario para incorporar a la zona las actualizaciones que tuvieron lugar después del último vuelco de la zona. Este archivo también se utiliza para las transferencias de zona incrementales (IXFR). Estos archivos de anotaciones no desaparecen. Es un archivo binario y no se debe editar.
<zona-primaria-n>.db+<AAAAMDDHHMSS>.signature		Es la versión firmada del archivo de zona primaria de un determinado dominio. También contiene registros de recurso utilizados para DNSSEC (registro de recurso RRSIG, etc.).
db.<zona-secundaria-n>		Archivo de zona secundaria de un determinado dominio en este servidor. Contiene todos los registros de recursos de esta zona. El archivo se emplea para cargar inicialmente el servidor secundario en el momento del inicio, si el servidor primario resulta inaccesible. Cada zona tiene un archivo .db aparte.
/QIBM/UserData/OS400/DNS/_DYN/		Directorio que contiene los archivos necesarios para las actualizaciones dinámicas.
<id_clave-n>._KEY		.Symlink a la clave DNSSEC con la clave <id_clave-n>. Siempre señala hacia la última clave K<id_clave-n>.+aaa+nnnnn.key creada.
<id_clave-x>._DUK. <zona-a>		Clave de actualización dinámica que se necesita para iniciar una petición de actualización dinámica en <zona-a> utilizando la clave <id_clave-x>.
<id_clave-x>._KID		Archivo que contiene una sentencia key para el id_clave llamado <id_clave-x>
<id_clave-y>._DUK. <zona-a>		Clave de actualización dinámica que se necesita para iniciar una petición de actualización dinámica en <zona-a> utilizando la clave <id_clave-y>.
<id_clave-y>._DUK. <zona-b>		Clave de actualización dinámica que se necesita para iniciar una petición de actualización dinámica en <zona-b> utilizando la clave <id_clave-y>.

Nombre	Icono	Descripción
<id_clave-y>._KID		Archivo que contiene una sentencia key para el id_clave llamado <id_clave-y>
k<id_clave-n>.+aaa+nnnnn.key k<id_clave-n>.+aaa+nnnnn.private		Par de claves pública/privada de DNSSEC, utilizando el <id_clave-n>: K{name}.+{algorithm}.+{identifier}.key K{name}.+{algorithm}.+{identifier}.private Si el par de claves de este <id_clave-n> ya existe, se crea un par de claves con una parte de identificador diferente.
dsset-zona-primaria-n.		El archivo se utiliza para suministrar a los administradores de la zona padre los registros DS correspondientes.
keyset-zona-primaria-n.		El archivo se utiliza para suministrar a los administradores de la zona padre los DNSKEY.
rndc-confgen.random.nnnnnn dnssec-keygen.random.nnnnn dnssec-signzone.random.nnnnn		Archivos de entropía para diversos mandatos que los necesitan. El componente nnnnn es el número del trabajo que creó el archivo. Solo se conservan si se cancela el mandato por alguna razón y no se hace limpieza.
<instancia-n>/session.key		Se genera cuando se inicia el servidor y se utiliza para la actualización dinámica desde el host local. No debe suprimir ni modificar este archivo.

Conceptos relacionados:

“Determinar las autorizaciones del sistema de nombres de dominio (DNS)” en la página 26
Existen requisitos especiales de autorización para el administrador del sistema de nombres de dominio (DNS). Debe tener en cuenta también las implicaciones de seguridad de la autorización.

“Acceder a las estadísticas del servidor de sistema de nombres de dominio (DNS)” en la página 42
Las herramientas de estadísticas y vuelco de la base de datos le ayudarán a revisar y gestionar el rendimiento del servidor.

Tareas relacionadas:

“Configurar servidores de nombres” en la página 30

El sistema de nombres de dominio (DNS) le permite crear múltiples instancias del servidor de nombres. Este tema proporciona las instrucciones para configurar un servidor de nombres.

Características avanzadas del sistema de nombres de dominio (DNS)

Este tema explica cómo los administradores con experiencia pueden utilizar las características avanzadas del sistema de nombres de dominio (DNS) para gestionar un servidor DNS con mayor facilidad.

El DNS de IBM Navigator for i proporciona una interfaz con características avanzadas que permiten configurar y gestionar el servidor DNS. Para los administradores familiarizados con la interfaz gráfica de IBM i, se proporcionan las siguientes tareas a modo de atajos. Ofrecen métodos rápidos para cambiar el estado y los atributos del servidor simultáneamente en múltiples instancias.

Tareas relacionadas:

“Cambiar los valores de depuración del sistema de nombres de dominio (DNS)” en la página 50
La función de depuración del sistema de nombres de dominio (DNS) puede proporcionar información que le ayudará a determinar y corregir los problemas del servidor DNS.

Iniciar o detener servidores de sistema de nombres de dominio (DNS)

Si el sistema de nombres de dominio (DNS) de la interfaz de IBM Navigator for i interface no le permite iniciar ni detener simultáneamente múltiples instancias de servidor, puede utilizar la interfaz basada en caracteres para cambiar estos valores simultáneamente para múltiples instancias.

Si desea utilizar la interfaz basada en caracteres para iniciar de una sola vez todas las instancias del servidor DNS, escriba STRTCPSVR SERVER(*DNS) DNSSVR(*ALL) en la línea de mandatos. Para detener a la vez todos los servidores DNS, escriba ENDTCPSPV SERVER(*DNS) DNSSVR(*ALL) en la línea de mandatos.

Cambiar los valores de depuración

Resulta útil cambiar el nivel de depuración para los administradores que tienen zonas de gran tamaño y no quieren que se recoja una cantidad de datos de depuración tan grande cuando el servidor se inicia por primera vez y carga todos los datos de la zona.

En la interfaz de IBM Navigator for i, el sistema de nombres de dominio (DNS) no le permite cambiar el nivel de depuración mientras el servidor está en ejecución. Sin embargo, puede utilizar la interfaz basada en caracteres para cambiar el nivel de depuración mientras el servidor esté en ejecución. Para cambiar el nivel de depuración mediante la interfaz basada en caracteres, siga estos pasos, pero donde pone *nnnnnn* en el mandato, escriba el nombre de la instancia del servidor:

1. En la línea de mandatos, escriba ADDLIBBLE QDNS y pulse Intro.
2. Cambie el nivel de depuración:
 - Para activar la depuración o para aumentar el nivel de depuración en una unidad, teclee RNDCCMD('trace') y pulse Intro.
 - Para desactivar la depuración, teclee RNDCCMD('notrace') y pulse Intro.

Resolución de problemas relacionados con el sistema de nombres de dominio (DNS)

Los valores de depuración y anotaciones del sistema de nombres de dominio (DNS) le ayudarán a resolver los problemas relacionados con el servidor DNS.

El funcionamiento del DNS es muy similar al de otras funciones y aplicaciones de TCP/IP. Al igual de las aplicaciones SMTP o FTP, los trabajos de DNS se ejecutan en el subsistema QSYSWRK y generan anotaciones de trabajo con el perfil de usuario QTCP que contiene la información asociada al trabajo DNS. Si un trabajo DNS finaliza, puede utilizar las anotaciones de trabajo para determinar la causa. Si el servidor DNS no devuelve las respuestas que se esperan, es posible que las anotaciones de trabajo contengan la información que le ayude a analizar el problema.

La configuración de DNS consta de diversos archivos con diferentes tipos de registros en cada uno. Los problemas en el servidor DNS suelen ser el resultado de entradas incorrectas en los archivos de configuración DNS. Cuando se produce un problema, debe verificar que los archivos de configuración de DNS contienen las entradas previstas.

Identificar los trabajos

Si observa las anotaciones de trabajo para comprobar la funcionalidad del servidor DNS (utilizando WRKACTJOB, por ejemplo), tenga en cuenta las siguientes directrices sobre asignación de nombres:

- Si ejecuta servidores basados en BIND 9, habrá un trabajo aparte por cada instancia de servidor que ejecute. El nombre del trabajo tiene cinco caracteres fijos (QTOBD) seguidos del nombre de la instancia. Por ejemplo, si tiene dos instancias, INST1 e INST2, los nombres de los trabajos serán QTOBDINST1 y QTOBDINST2.

Anotar mensajes del servidor de sistema de nombres de dominio (DNS)

El sistema de nombres de dominio (DNS) proporciona numerosas opciones de anotaciones que se pueden ajustar cuando usted intente encontrar el origen de un problema. Las anotaciones proporcionan una gran flexibilidad, ya que ofrecen diversos niveles de gravedad, categorías de mensajes y archivos de salida para que, con un sistema de anotaciones más perfecto, le resulte fácil localizar los problemas.

BIND 9 ofrece varias opciones de anotaciones. Puede especificar qué tipos de mensajes se anotan, a dónde se envía cada tipo de mensaje y qué nivel de gravedad hay que anotar para cada tipo de mensaje. En general, son adecuados los valores predeterminados de las anotaciones, pero si desea cambiarlos, le sugerimos que consulte otras fuentes de documentación de BIND 9 para obtener información sobre las anotaciones.

Canales de anotaciones

El servidor DNS puede anotar mensajes en diferentes canales de salida. Los canales especifican el lugar al que se envían los datos de las anotaciones. Puede seleccionar los tipos de canales siguientes:

- **Canales de archivo**

Los mensajes anotados en los canales de archivo se envían a un archivo. Los canales de archivo predeterminados son `i5os_debug` e `i5os_QPRINT`. Por defecto, los mensajes de depuración se anotan en el canal `i5os_debug`, que es el archivo `named.run`, pero también puede especificar que se envíen otras categorías de mensajes a este archivo. Las categorías de mensajes anotadas en `i5os_QPRINT` se envían a un archivo en `spool QPRINT` para el perfil de usuario `QTCP`. Puede crear sus propios canales de archivo además de los canales que se proporcionan por defecto.

- **Canales syslog**

Los mensajes anotados en este canal se envían a las anotaciones de trabajo del servidor. El canal `syslog` predeterminado es `i5os_joblog`. Los mensajes anotados que se hayan dirigido a este canal se envían a las anotaciones de trabajo de la instancia del servidor DNS.

- **Canales nulos**

Todos los mensajes anotados en el canal nulo se descartan. El canal nulo predeterminado es `i5os_null`. Puede dirigir categorías al canal nulo si no quiere que los mensajes aparezcan en ningún archivo de anotaciones.

Categorías de mensajes

Los mensajes se agrupan en categorías. Puede especificar qué categorías de mensajes deben anotarse en cada canal. Las categorías son:

client Proceso de las peticiones de los clientes.

config Análisis y proceso del archivo de configuración.

database

Mensajes relacionados con las bases de datos que el servidor DNS utiliza internamente para almacenar datos de zona y de caché.

default

Definiciones de las opciones de anotaciones para aquellas categorías en las que no se ha definido una configuración específica.

delegation-only

Solo delegación. Se anotan las consultas que se han forzado en NXDOMAIN como resultado de una zona solo de delegación o una declaración solo de delegación en una zona de apéndice o en una sugerencia.

dispatch

Despachar paquetes entrantes a los módulos de servidor en los que se procesarán.

dnssec

Proceso del protocolo de extensiones de seguridad DNS (DNSSEC) y de signatura de transacciones (TSIG).

general

Categoría general en la que cabe todo lo que no está clasificado en las otras categorías.

lame-servers

Servidores incapacitados por culpa de una mala configuración en los servidores remotos, descubiertos por BIND 9 al intentar consultarlos durante la resolución.

network

Operaciones de red.

notify Protocolo NOTIFY.

resolver

Resolución DNS (como en las búsquedas recursivas) que se realiza en nombre de los clientes mediante un servidor de nombres en caché.

security

Aprobación y denegación de las peticiones.

xfer-in Transferencias de zona que recibe el servidor.

xfer-out

Transferencias de zona que envía el servidor.

unmatched

Mensajes que no han podido determinar la clase de una vista coincidente o para los que no había ninguna vista coincidente. También se anota un resumen de una sola línea en la categoría client. Esta categoría se envía preferiblemente a un archivo o a la salida de errores estándar. Por defecto, se envía al canal nulo.

update

Actualizaciones dinámicas.

update-security

Aprobación y denegación de las peticiones de actualización. Las consultas especifican dónde se deben anotar las consultas. En el momento del inicio, al especificar las consultas de categorías, se habilitan las anotaciones de consultas, a menos que se especifique la opción querylogd.

La entrada de anotaciones de consulta notifica la dirección IP y el número de puerto del cliente, el nombre de la consulta, su clase y su tipo. También notifica si se ha establecido el distintivo de recursión deseada (+ si se ha establecido, - si no se ha establecido), se estaba utilizando EDNS (E) o si la consulta iba firmada (S).

Los archivos de anotaciones pueden adquirir gran tamaño y hay que suprimirlos con regularidad. Todo el contenido del archivo de anotaciones de DNS se borra cuando el servidor DNS se detiene y se inicia.

Gravedad del mensaje

Los canales le permiten filtrar los mensajes según su gravedad. En cada canal se puede especificar el nivel de gravedad para el que se anotan los mensajes. A continuación figuran los niveles de gravedad que están disponibles:

- Muy grave
- Error
- Aviso
- Atención
- Info
- Depuración (especifique un nivel de depuración de 0 a 11)
- Dinámico (hereda el nivel de depuración de arranque del servidor)

Quedarán anotados todos los mensajes de la gravedad que seleccione más los mensajes cuyo nivel de gravedad sea superior al especificado. Por ejemplo, si selecciona Aviso, el canal anotará los mensajes con gravedad Aviso, Error y Muy grave. Si selecciona el nivel Depuración, puede especificar un valor de 0 a 11, que corresponderá a los mensajes de depuración que desea que queden anotados.

Cambiar los valores de las anotaciones

Para acceder a las opciones de las anotaciones, siga estos pasos:

1. En IBM Navigator for i, expanda **Red** > **Servidores** > **Servidores DNS**.
2. En el panel de la derecha, pulse *su servidor DNS* con el botón derecho del ratón y seleccione **Configuración**.
3. En la página Configuración de DNS, pulse **Servidor DNS** con el botón derecho del ratón y seleccione **Propiedades**.
4. En la página Propiedades del servidor, seleccione la pestaña **Canales** para crear nuevos canales de archivos o propiedades de un canal, como la gravedad de los mensajes anotados en cada canal.
5. En la página Propiedades del servidor, seleccione la pestaña **Anotaciones** para especificar qué categorías de mensajes deben anotarse en cada canal.

Consejo de resolución de problemas sobre el nivel de gravedad

El nivel de gravedad predeterminado del canal i5os_joblog es Error. Este valor se utiliza para reducir la cantidad de mensajes informativos y de aviso, que pueden disminuir el rendimiento. Si surgen problemas pero las anotaciones de trabajo no indican el origen del problema, es posible que tenga que cambiar el nivel de gravedad. Siga el procedimiento descrito más arriba para acceder a la página Canales, y cambie el nivel de gravedad del canal i5os_joblog por el de Aviso, Atención o Info, para poder ver así más datos de las anotaciones. Cuando haya resuelto el problema, restablezca el nivel de gravedad a Error para reducir el número de mensajes de las anotaciones de trabajo.

Cambiar los valores de depuración del sistema de nombres de dominio (DNS)

La función de depuración del sistema de nombres de dominio (DNS) puede proporcionar información que le ayudará a determinar y corregir los problemas del servidor DNS.

DNS ofrece 12 niveles de control de depuración. Las anotaciones suelen facilitar un método más sencillo para localizar los problemas, pero en algunos casos puede ser necesario utilizar la depuración. En condiciones normales, la depuración está desactivada (valor = 0). Le recomendamos que utilice primero las anotaciones para tratar de corregir los problemas.

Los niveles de depuración válidos son del 0 al 11. El representante de servicio de IBM puede ayudarle a determinar el valor de depuración apropiado para diagnosticar el problema del DNS. Los valores 1 y superiores hacen que se escriba información de depuración en el archivo named.run de la vía de acceso del directorio IBM i: /QIBM/UserData/OS400/DNS/<instancia de servidor>, siendo <instancia de servidor> el nombre de la instancia del servidor DNS. El archivo named.run va creciendo paulatinamente siempre que el nivel de depuración sea 1 o un valor superior, y si el servidor DNS sigue en ejecución. También

puede utilizar la página Propiedades del servidor - Canales para especificar las preferencias de tamaño máximo y de número de versiones del archivo named.run.

Para cambiar el valor de depuración de la instancia del servidor DNS, siga estos pasos:

1. En IBM Navigator for i, expanda **Red** > **Servidores** > **Servidores DNS**.
2. En el panel de la derecha, pulse *su servidor DNS* con el botón derecho del ratón y seleccione **Configuración**.
3. En la página Configuración de DNS, pulse el servidor DNS con el botón derecho del ratón y seleccione **Propiedades**.
4. En la página Propiedades del servidor - General, especifique el nivel de depuración de arranque del servidor.
5. Si el servidor se está ejecutando, deténgalo y reinícielo.

Nota: Los cambios que efectúe en el nivel de depuración no surtirán efecto mientras el servidor se esté ejecutando. El nivel de depuración definido aquí se utilizará la próxima vez que se reinicie por completo el servidor. Si necesita cambiar el nivel de depuración mientras el servidor se esté ejecutando, vea: Características avanzadas del DNS.

Conceptos relacionados:

“Características avanzadas del sistema de nombres de dominio (DNS)” en la página 46

Este tema explica cómo los administradores con experiencia pueden utilizar las características avanzadas del sistema de nombres de dominio (DNS) para gestionar un servidor DNS con mayor facilidad.

Información relacionada con el sistema de nombres de dominio (DNS)






Publicaciones IBM Redbooks, sitios Web y otros temarios de Information Center con información relacionada con el temario Sistema de nombres de dominio (DNS). Puede ver o imprimir cualquiera de los archivos PDF.

IBM Redbooks

AS/400 TCP/IP Autoconfiguration: DNS and DHCP Support  (5181 KB)

Esta publicación Redbooks describe el soporte de servidor del sistema de nombres de dominio (DNS) y del protocolo de configuración dinámica de hosts (DHCP) incluidos en IBM i. Este libro rojo le ayudará a instalar, adaptar, configurar y solucionar los problemas del soporte de DNS y DHCP mediante ejemplos.

Sitios Web

- *DNS and BIND*, quinta edición. Paul Albitz y Cricket Liu. Publicado por O'Reilly and Associates, Inc.  Sebastopol, California, 2006. Número ISBN: 0-59610-057-4.
- El manual de consulta del administrador de BIND (en versión PDF) del sitio Web de Internet System Consortium (ISC) .
- El sitio Web de Internet Software Consortium  contiene noticias, enlaces y otros recursos relacionados con BIND. También proporciona un listado de peticiones de comentarios (RFC) relacionadas con el DNS .
- El sitio InterNIC  mantiene un directorio con todos los registradores de nombres de dominio que estén autorizados por la Corporación de nombres y números asignados de Internet (ICANN).

Referencia relacionada:

“Archivo PDF de Sistema de nombres de dominio (DNS)” en la página 2
Puede ver e imprimir un archivo PDF de esta información.

Avisos

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
1623-14, Shimotsuruma, Yamato-shi
Kanagawa 242-8502 Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
Software Interoperability Coordinator, Department YBWA
3605 Highway 52 N
Rochester, MN 55901
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

© (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs.

Información de la interfaz de programación

Esta publicación Sistema de nombres de dominio facilita información sobre las interfaces de programación previstas que permiten al cliente escribir programas para obtener los servicios de IBM i.

Marcas registradas

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at “Copyright and trademark information” at www.ibm.com/legal/copytrade.shtml.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

Other product and service names might be trademarks of IBM or other companies.

Terms and conditions

Permissions for the use of these publications is granted subject to the following terms and conditions.

Personal Use: You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative works of these publications, or any portion thereof, without the express consent of IBM.

Commercial Use: You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.



Número de Programa: 5770-SS1

Impreso en España