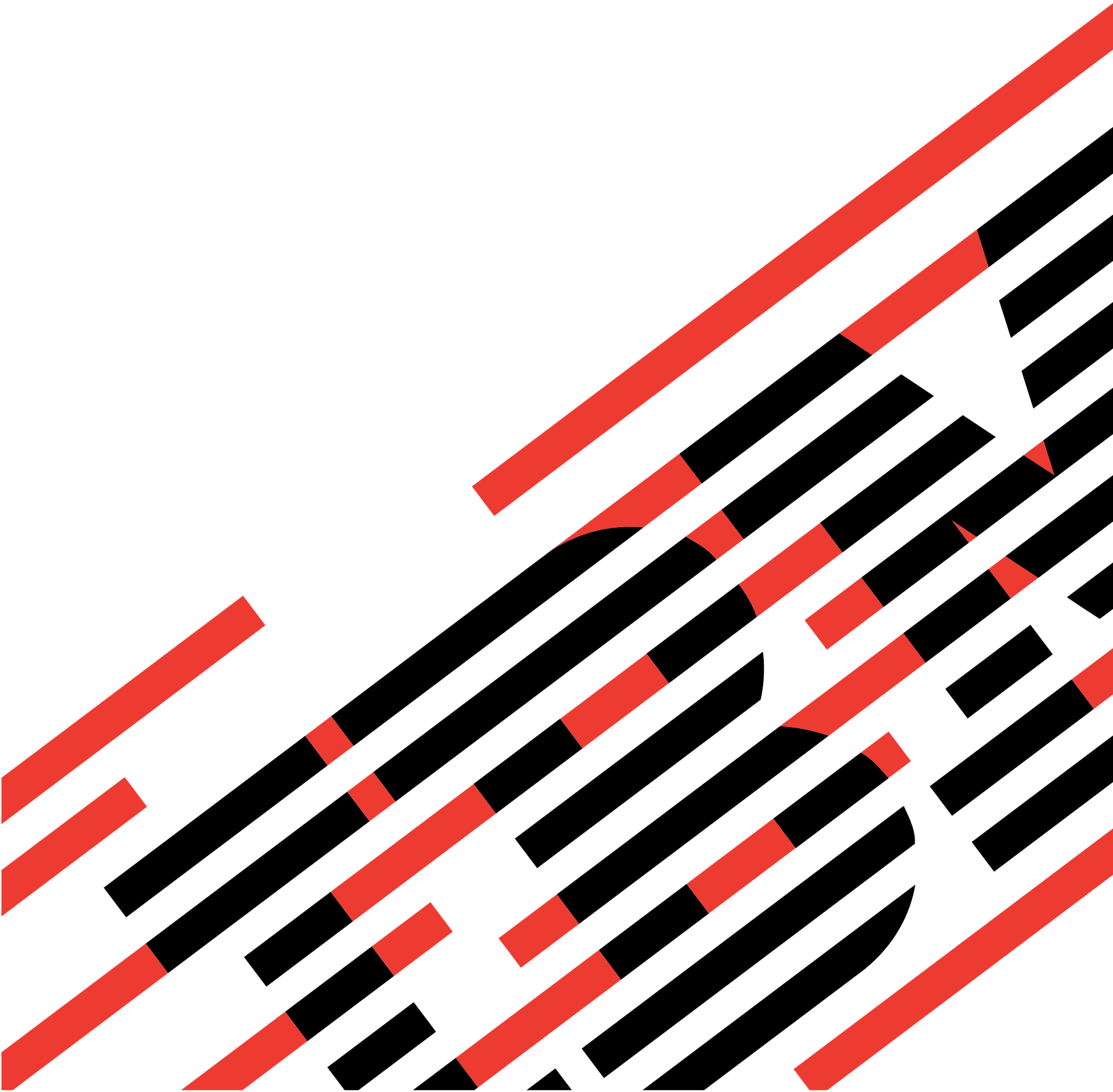
IBM Systems - iSeries

DNS (Sistema de nombres de dominio) en red

Versión 5 Release 4



IBM Systems - iSeries

DNS (Sistema de nombres de dominio) en red

Versión 5 Release 4

Nota

Antes de utilizar esta información y el producto al que da soporte, lea la información de la sección “Avisos”, en la página 41.

Sexta edición (febrero de 2006)

Esta edición se aplica a la versión 5, release 4, modificación 0 de IBM i5/OS (número de producto 5722-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.

Contenido

DNS (Sistema de nombres de dominio)

DNS (Sistema de nombres de dominio) es un sistema de bases de datos distribuidas que se utiliza para gestionar los nombres de los sistemas principales y sus direcciones IP (Protocolo de Internet) asociadas.

El uso de DNS implica que los usuarios pueden utilizar nombres sencillos, como por ejemplo www.jkltoys.com, para localizar un sistema principal, en lugar de emplear la dirección IP (xxx.xxx.xxx.xxx). Un único servidor sólo puede ser responsable de conocer los nombres de sistema principal y direcciones IP de un subconjunto pequeño 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 son los que permiten que los sistemas se comuniquen a través de Internet.

En IBM OS/400 Versión 5 Release 1 (V5R1), los servicios del DNS se basan en la implementación de DNS estándar de la industria, conocido como BIND (Berkeley Internet Name Domain) versión 8. Los servicios del DNS del IBM OS/400 se basaban en BIND versión 4.9.3. La opción 33 del i5/OS, PASE (Portable Application Solutions Environment), debe estar instalada en el servidor IBM eServer iSeries si desea utilizar el nuevo servidor DNS basado en BIND versión 8. Si no tiene instalada la opción PASE, puede ejecutar igualmente el mismo servidor DNS basado en BIND versión 4.9.3, disponible en las versiones anteriores. Sin embargo, la migración a BIND 8 proporciona una función mejorada e incorpora una mayor seguridad para el servidor DNS.

Nota: En este tema se explican las nuevas funciones basadas en BIND 8. Si no utiliza PASE para ejecutar DNS basado en BIND 8, consulte el tema DNS V4R5 del Information Center para obtener información relativa a DNS basado en BIND 4.9.3.

PDF imprimible

Este tema explica cómo ver e imprimir un PDF de esta información.

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

Guardar archivos PDF

Para guardar un PDF en la estación de trabajo con el fin de verlo o imprimirlo:

1. Pulse el botón derecho sobre el PDF en el navegador (pulse el botón derecho del ratón sobre el enlace anterior).
2. Pulse en la opción que guarda el PDF localmente.
3. Vaya al directorio donde desea guardar el PDF.
4. Pulse en **Guardar**.

Bajar Adobe Reader

Necesita tener instalado Adobe Reader en el sistema para ver o imprimir estos PDF. Puede bajar una copia gratuita del sitio Web de Adobe (www.adobe.com/products/acrobat/readstep.html)  .

Conceptos sobre DNS (Sistema de nombres de dominio)

Este tema explica qué es y cómo funciona DNS (Sistema de nombres de dominio). También muestra los diferentes tipos de zonas que pueden definirse en un servidor DNS.

DNS (Sistema de nombres de dominio) es un sistema de bases de datos distribuidas que se utiliza para gestionar los nombres de los sistemas principales y sus direcciones IP (Protocolo de Internet) asociadas. El uso de DNS implica que los usuarios pueden utilizar nombres sencillos, como por ejemplo www.jkltoys.com, para localizar un sistema principal, en lugar de emplear la dirección IP (xxx.xxx.xxx.xxx). Un único servidor sólo puede ser responsable de conocer los nombres de sistema principal y direcciones IP de un subconjunto pequeño 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 son los que permiten que los sistemas se comuniquen a través de 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 cuente con toda la información del sistema principal y con los datos de una zona tiene autoridad sobre la zona. Este tipo de servidor puede responder a las consultas sobre sistemas principales de su zona mediante sus propios registros de recursos. El proceso de consulta depende de una serie de factores. En el apartado Comprender las consultas de DNS se explican los pasos que un cliente debe realizar para resolver una consulta.

Comprender las zonas

Este tema explica las zonas DNS (Sistema de nombres de dominio) y los tipos de zonas.

Los datos de DNS se dividen en conjuntos gestionables de datos llamados *zonas*. Las zonas contienen información sobre nombres y direcciones IP acerca de una o más partes de un dominio DNS. Un servidor que contenga toda la información sobre una zona se considera el servidor que tiene autoridad sobre el dominio. En ocasiones conviene delegar la autorización para responder a las consultas de DNS de un subdominio determinado a otro servidor DNS. En tal caso, el servidor DNS del dominio puede configurarse de tal forma que las consultas del subdominio se remitan al servidor apropiado.

Para mantener copias de seguridad, los datos de zona suelen almacenarse en servidores que no sean el servidor DNS autorizado sobre dicha zona. Estos otros servidores se denominan servidores secundarios, que cargan los datos de zona del servidor autorizado. 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 autorizado. Cuando se inicializa un servidor secundario, éste 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 iSeries para definir diversos tipos de zonas que le ayudarán a gestionar los datos del DNS:

Zona primaria

Una zona primaria carga los datos de zona directamente a partir de un archivo de un sistema principal. Puede contener una subzona o zona hija. También puede contener registros de recursos, por ejemplo registros del sistema principal, alias (CNAME), dirección (A) o puntero de correlación inversa (PTR).

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

Subzona

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

Alias (CNAME)
Un alias es un nombre alternativo para el nombre del dominio primario.

Sistema principal
Un objeto de sistema principal correlaciona los registros A y PTR a un sistema principal. Puede haber registros de recursos adicionales asociados a un sistema principal.

Zona secundaria
Una 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.

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

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

Conceptos relacionados

"Comprender las consultas de DNS (Sistema de nombres de dominio)"
Este tema explica cómo DNS (Sistema de nombres de dominio) resuelve las consultas en nombre de los clientes.

"Configurar zonas en un servidor de nombres" en la página 25
Después de configurar una instancia de servidor DNS (Sistema de nombres de dominio), debe configurar las zonas para el servidor de nombres.

Referencia relacionada

"Ejemplo: un único servidor DNS (Sistema de nombres de dominio) para una intranet" en la página 14
Este ejemplo describe una subred simple con un servidor DNS (Sistema de nombres de dominio) para uso interno.

"Registros de recursos de DNS (Sistema de nombres de dominio)" en la página 8
Este tema explica cómo DNS (Sistema de nombres de dominio) utiliza los registros de recursos. Los registros de recursos se utilizan para almacenar datos sobre nombres de dominio y direcciones IP. En este tema encontrará una lista en la que podrá buscar los registros de recursos soportados en OS/400 V5R1.

Comprender las consultas de DNS (Sistema de nombres de dominio)

Este tema explica cómo DNS (Sistema de nombres de dominio) resuelve las consultas en nombre de los clientes.

Los clientes utilizan servidores DNS para buscar información. La petición puede provenir 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 calificado al completo (FQDN), un tipo de consulta, por ejemplo un registro de recurso concreto que el cliente necesita, y la clase del nombre del dominio, que suele ser la clase IN (Internet). En la figura siguiente se describe la red de muestra del caso de ejemplo Un único servidor DNS con acceso a Internet.

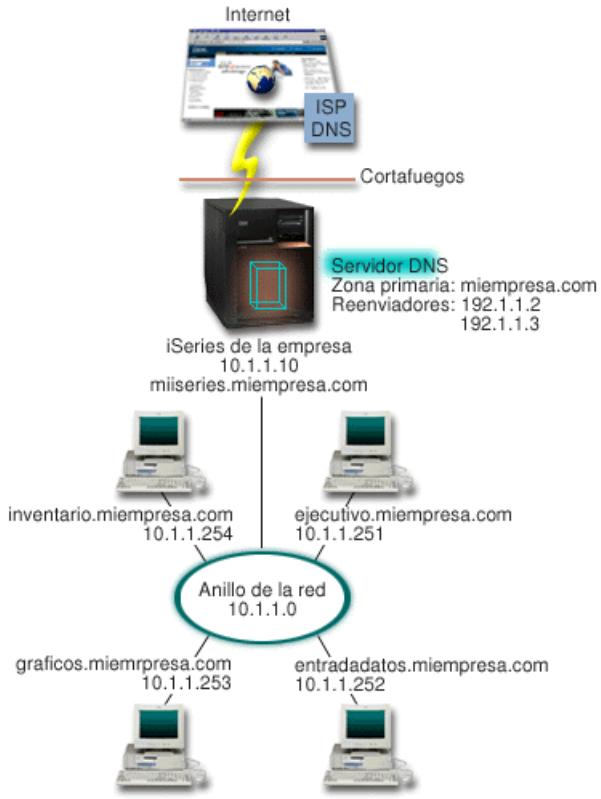


Figura 1. Un único servidor DNS con acceso a Internet

Supongamos que el sistema principal *entradadatos* realiza la consulta de gráficos.miempresa.com. al servidor DNS. 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 sistema principal no se encuentra en los datos de zona del servidor DNS. Existen ahora dos vías que pueden seguirse, repetición o iteración. Si el servidor DNS se ha definido para que utilice la repetición, el servidor puede consultar o contactar con otros servidores DNS de parte del cliente que realiza la solicitud con el objeto de resolver el nombre, y a continuación enviar la respuesta al cliente. Si el servidor DNS consulta a otro servidor DNS, el servidor que realiza la petición guardará la respuesta en su antememoria para poder utilizarla la próxima vez que reciba esa consulta. Un cliente puede tratar él mismo de contactar con otros servidores DNS para resolver un nombre. En este proceso, llamado *iteración*, el cliente utiliza consultas adicionales individuales basadas en respuestas de los servidores.

Referencia relacionada

"Comprender las zonas" en la página 2
Este tema explica las zonas DNS (Sistema de nombres de dominio) y los tipos de zonas.

"Ejemplo: un único servidor DNS (Sistema de nombres de dominio) con acceso a Internet" en la página 15
Este ejemplo describe una subred simple con un servidor DNS (Sistema de nombres de dominio) conectado directamente a Internet.

Configuración del dominio DNS (Sistema de nombres de dominio)

Este tema proporciona una visión general del registro del dominio, que enlaza con otros sitios de referencia para configurar su propio espacio del dominio.

El DNS (Sistema de nombres de dominio) permite proporcionar nombres y direcciones en una intranet o red interna. También permite proporcionar 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 por usted. El Centro InterNIC (Internet Network Information Center) mantiene un directorio con todos los registradores de nombres de dominio que están autorizados por la organización ICANN (Internet Corporation for Assigned Names and Numbers).

Referencia relacionada

"Ejemplo: un único servidor DNS (Sistema de nombres de dominio) con acceso a Internet" en la página 15
Este ejemplo describe una subred simple con un servidor DNS (Sistema de nombres de dominio) conectado directamente a Internet.

Información relacionada

Internet Network Information Center (InterNIC)

Actualizaciones dinámicas

OS/400 DNS V5R1 basado en BIND 8 permite realizar actualizaciones dinámicas. De este modo, fuentes externas, como por ejemplo DHCP (Protocolo de configuración dinámica de sistemas principales), pueden enviar actualizaciones al servidor DNS (Sistema de nombres de dominio).

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 permite definir los parámetros de configuración del sistema principal de red en una ubicación central y automatizar la configuración de los sistemas principales. 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. Ahora, los servidores DNS que ejecutan BIND 8 pueden configurarse de forma que acepten las peticiones de otras fuentes para actualizar los datos de zona dinámicamente.

Puede configurar el servidor DHCP para enviar peticiones de actualización al servidor DNS cada vez que asigne una dirección nueva a un sistema principal. 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 sistemas principales 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 las consultas de los sistemas principales, incluso cuando sus direcciones IP hayan cambiado.

Puede configurar DHCP para que actualice los registros de correlación de direcciones (A), los registros de puntero de búsqueda inversa (PTR), o ambos, de parte del cliente. El registro A correlaciona el nombre del sistema principal de una máquina con su dirección IP. El registro PTR correlaciona la dirección IP de una máquina con su nombre de sistema principal. Cuando la dirección de un cliente cambia, DHCP puede enviar automáticamente una actualización al servidor DNS para que el resto de los sistemas

principales de la red puedan localizar al cliente en su nueva dirección IP a través de consultas DNS. 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 define que DHCP sólo debe actualizar registros PTR, deberá configurar DNS para que permita las actualizaciones de los clientes, de manera que cada cliente pueda actualizar su registro A. No todos los clientes DHCP dan soporte a la operación de realizar peticiones de actualización de su propio registro A. Consulte la documentación de su plataforma 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 *Firma 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.

Las actualizaciones dinámicas pueden efectuarse entre DNS y DHCP en un único servidor iSeries, entre servidores iSeries diferentes o entre un servidor iSeries y otros servidores capaces de realizar actualizaciones dinámicas.

Nota: La interfaz de programación de aplicaciones (API) de actualización dinámica QTOBUPT es indispensable para servidores que envían actualizaciones dinámicas al DNS. Se instala automáticamente con la opción 31 de i5/OS, DNS.

Conceptos relacionados

Protocolo de configuración dinámica de sistemas principales (DHCP)

Tareas relacionadas

“Configurar el DNS (Sistema de nombres de dominio) para recibir actualizaciones dinámicas” en la página 26
Los servidores DNS (Sistema de nombres de dominio) que ejecutan BIND 8 pueden configurarse de modo que acepten peticiones de otras fuentes para actualizar los datos de la zona de forma dinámica. Este tema ofrece instrucciones para configurar la opción allow-update para que el DNS pueda recibir actualizaciones dinámicas.

Configuración de DHCP para enviar actualizaciones dinámicas

Referencia relacionada

“Ejemplo: DNS (Sistema de nombres de dominio) y DHCP (Protocolo de configuración dinámica de sistemas principales) en el mismo servidor iSeries” en la página 17
Este ejemplo ilustra DNS (Sistema de nombres de dominio) y DHCP (Protocolo de configuración dinámica de sistemas principales) en el mismo servidor.

“Registros de recursos de DNS (Sistema de nombres de dominio)” en la página 8
Este tema explica cómo DNS (Sistema de nombres de dominio) utiliza los registros de recursos. Los registros de recursos se utilizan para almacenar datos sobre nombres de dominio y direcciones IP. En este tema encontrará una lista en la que podrá buscar los registros de recursos soportados en OS/400 V5R1.

QTOBUPT

“Funciones de BIND 8”
Además de las actualizaciones dinámicas, BIND 8 ofrece varias funciones para mejorar el rendimiento del servidor DNS (Sistema de nombres de dominio).

Funciones de BIND 8

Además de las actualizaciones dinámicas, BIND 8 ofrece varias funciones para mejorar el rendimiento del servidor DNS (Sistema de nombres de dominio).

DNS ha sido rediseñado para utilizar BIND 8 para OS/400 V5R1. Si no tiene instalada la opción PASE, puede seguir configurando y ejecutando el servidor DNS OS/400 de la versión anterior basado en BIND 4.9.3. En el tema Requisitos del sistema DNS se explica lo que necesita para ejecutar el DNS basado en BIND 8 en su servidor iSeries. Si utiliza el nuevo DNS disfrutará de las ventajas siguientes:

Varios servidores DNS que se ejecutan en un solo iSeries

En releases anteriores, sólo podía configurarse un servidor DNS. Ahora puede configurar varios servidores o instancias DNS. De esta forma podrá configurar una división lógica entre los servidores. Cuando cree varias instancias, deberá definir explícitamente las direcciones IP de interfaz de escucha para cada una de ellas. Dos instancias DNS no pueden escuchar la misma interfaz.

Una de las aplicaciones prácticas que implica tener varios servidores es la división del DNS, en que hay un servidor con un grado de autorización mayor en la red interna, y un segundo servidor que se utiliza para consultas externas.

Reenvío condicional

El reenvío condicional le permite configurar su servidor DNS para definir las preferencias sobre la función de reenvío. Puede configurar un servidor de manera que reenvíe todas las consultas sobre las que no conozca la respuesta. Puede definir la opción de reenvío a un nivel global y añadir excepciones a los dominios para los que desea forzar una resolución iterativa normal. O bien, puede definir la resolución iterativa normal a un nivel global y forzar la opción de reenvío en determinados dominios.

Actualizaciones dinámicas seguras

DHCP (Protocolo de configuración dinámica de sistemas principales) y otras fuentes autorizadas pueden enviar actualizaciones dinámicas de registros de recursos mediante firmas de transacción (TSIG) y/o mediante la autorización de la dirección IP de origen. De esta forma se reduce la necesidad de realizar actualizaciones manuales de los datos de zona a la vez que se garantiza que sólo se utilizarán fuentes autorizadas en las actualizaciones.

NOTIFY

Cuando se inicia NOTIFY, la función NOTIFY del DNS queda activada allí donde se actualicen los datos de zona del servidor primario. El servidor primario enviará a todos los servidores secundarios conocidos un mensaje que indica que los datos han cambiado. A continuación, los servidores secundarios pueden responder con una petición de transferencia de zona para los datos de zona actualizados. Así se contribuye a mejorar el soporte del servidor secundario, al mantener actualizados los datos de zona de seguridad.

Transferencias de zona (IXFR y AXFR)

Antiguamente, cuando los servidores secundarios tenían que volver a cargar los datos de zona, cargaban el conjunto de datos completo en una transferencia de zona Total (AXFR). BIND 8 admite un nuevo método de transferencia de zona: transferencia de zona incremental (IXFR). IXFR es un método por el que los servidores pueden transferir únicamente los datos modificados en lugar de la zona completa.

Cuando se activa en el servidor primario, a los datos modificados se les asigna un distintivo que indica que se ha efectuado algún cambio. Cuando un servidor secundario solicita una actualización de zona en un IXFR, el servidor primario sólo enviará los datos nuevos. IXFR resulta especialmente útil cuando la zona se actualiza dinámicamente. Esta transferencia reduce la carga de tráfico mediante el envío de pequeñas cantidades de datos.

Nota: Tanto el servidor primario como el servidor secundario deben habilitarse para IXFR para poder utilizar esta función.

Conceptos relacionados

"Requisitos de DNS (Sistema de nombres de dominio)" en la página 22
En este tema se describen los requisitos de software para ejecutar el DNS (Sistema de nombres de dominio) en el servidor iSeries.

"Actualizaciones dinámicas" en la página 5
OS/400 DNS V5R1 basado en BIND 8 permite realizar actualizaciones dinámicas. De este modo, fuentes externas, como por ejemplo DHCP (Protocolo de configuración dinámica de sistemas principales), pueden enviar actualizaciones al servidor DNS (Sistema de nombres de dominio).

Referencia relacionada

"Ejemplo: dividir DNS (Sistema de nombres de dominio) con un cortafuegos" en la página 19
Este ejemplo describe el funcionamiento del DNS (Sistema de nombres de dominio) con un cortafuegos para proteger los datos internos de Internet, a la vez que se permite que los usuarios internos accedan a los datos de Internet.

"Planificar medidas de seguridad" en la página 21
El DNS (Sistema de nombres de dominio) proporciona opciones de seguridad para limitar el acceso externo a su servidor.

Registros de recursos de DNS (Sistema de nombres de dominio)

Este tema explica cómo DNS (Sistema de nombres de dominio) utiliza los registros de recursos. Los registros de recursos se utilizan para almacenar datos sobre nombres de dominio y direcciones IP. En este tema encontrará una lista en la que podrá buscar los registros de recursos soportados en OS/400 V5R1.

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 del sistema principal con una dirección IP, y los registros de puntero de búsqueda inversa (PTR) correlacionan una dirección IP con un nombre de sistema principal. El servidor utiliza estos recursos para resolver las consultas de los sistemas principales de su zona. Si desea más información, utilice la tabla para ver los registros de recursos de DNS.

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 sistema principal. 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 AFSDB (Andrew File System Database)	AFSDB	El registro AFSDB especifica la dirección AFS o DCE del objeto. Los registros AFSDB se utilizan como los registros A para correlacionar un nombre de dominio con su dirección AFSDB 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 RFC 1183.

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

Registro de recurso	Abreviatura	Descripción
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 RFC 1035.
Registros de información de sistema principal	HINFO	El registro HINFO especifica información general acerca de una máquina de sistema principal. Los nombres de sistema operativo y CPU estándares se definen en los números asignados de RFC 1700. No obstante, la utilización de números estándares no es necesario. Este tipo de registro se define en RFC 1035.
Registros de Red Digital de Servicios Integrados	ISDN	El registro ISDN especifica la dirección de este objeto. Este registro correlaciona un nombre de sistema principal con la dirección ISDN. Solamente se utilizan en redes RDSI. Este tipo de registro se define en RFC 1183.
Registros de dirección IP Versión 6	AAAA	El registro AAAA especifica la dirección de 128 bits de un sistema principal. Los registros AAAA se utilizan como los registros A para correlacionar un nombre de sistema principal con su dirección IP. Utilice los registros AAAA para dar soporte a las direcciones IP versión 6, que no caben en el formato estándar de registro A. Este tipo de registro se define en 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 eficiencia de la red o para realizar correlaciones de red física. Este tipo de registro se define en RFC 1876.

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

Registro de recurso	Abreviatura	Descripción
Registros Mail Exchanger (MX)	MX	Los registros MX definen un sistema principal intercambiador de correo para enviar correo a este dominio. SMTP (Protocolo simple de transferencia de correo) utiliza estos registros para localizar los sistemas principales que procesan o reenvían el correo de este dominio, junto con los valores de preferencias de cada sistema principal intercambiador de correo. Cada sistema principal intercambiador de correo debe tener su correspondiente registro de dirección de sistema principal (A) en una zona válida. Este tipo de registro se define en 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 RFC 1035.
Registros de buzón	MB	Los registros MB especifican el nombre de dominio de sistema principal que contiene el buzón de este objeto. El correo que se envía al dominio se dirige al sistema principal especificado en el registro MB. Este tipo de registro se define en 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 RFC 1035.
Registros de redenominación 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 RFC 1035.
Registros de servidor de nombres	NS	El registro NS especifica un servidor de nombres autorizado para este sistema principal. Este tipo de registro se define en RFC 1035.
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 RFC 1706.

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

Registro de recurso	Abreviatura	Descripción
Registros de clave pública	KEY	El registro KEY especifica una clave pública asociada a un nombre DNS. La clave puede ser para una zona, un usuario o un sistema principal. Este tipo de registro se define en 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 sistema principal. Este tipo de registro se define en RFC 1183.
Registros de puntero de búsqueda inversa	PTR	El registro PTR especifica el nombre de dominio de un sistema principal para el que desea tener un registro PTR definido. Los registros PTR permiten la búsqueda de nombres de sistema principal a partir de direcciones IP. Este tipo de registro se define en RFC 1035.
Registros de ruta a través	RT	El registro RT especifica un nombre de dominio de sistema principal que puede actuar como un reenviador de paquetes IP para este sistema principal. Este tipo de registro se define en RFC 1183.
Registros de inicio de autoridad	SOA	El registro SOA especifica que este servidor es autorizativo para esta zona. Un servidor autorizativo es la mejor fuente de 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 RFC 1035.
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 RFC 1035. Los registros TXT los utiliza iSeries en las actualizaciones dinámicas. El servidor DHCP escribe un registro TXT asociado para cada actualización de registro A y PTR que realiza el servidor DHCP. Los registros DHCP tienen un prefijo de AS400 DHCP.

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

Registro de recurso	Abreviatura	Descripción
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 RFC 1035.
Registros de correlación de direcciones X.400	PX	Los registros PX son un puntero a información de correlación X.400/RFC 822. Este tipo de registro se define en 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 sistema principal con la dirección PSDN. Solamente se utilizan en redes X25. Este tipo de registro se define en RFC 1183.

Conceptos relacionados

"Actualizaciones dinámicas" en la página 5
OS/400 DNS V5R1 basado en BIND 8 permite realizar actualizaciones dinámicas. De este modo, fuentes externas, como por ejemplo DHCP (Protocolo de configuración dinámica de sistemas principales), pueden enviar actualizaciones al servidor DNS (Sistema de nombres de dominio).

"Registros de correo y de intercambio de correo (MX)"
El DNS (Sistema de nombres de dominio) da soporte al direccionamiento avanzado de correo mediante el uso de registros de correo y de intercambio de correo (MX).

Referencia relacionada

"Ejemplo: un único servidor DNS (Sistema de nombres de dominio) para una intranet" en la página 14
Este ejemplo describe una subred simple con un servidor DNS (Sistema de nombres de dominio) para uso interno.

"Comprender las zonas" en la página 2
Este tema explica las zonas DNS (Sistema de nombres de dominio) y los tipos de zonas.

Registros de correo y de intercambio de correo (MX)

El DNS (Sistema de nombres de dominio) da soporte al direccionamiento avanzado de correo mediante el uso de registros de correo y de intercambio de correo (MX).

Los registros de correo y MX los utilizan programas de direccionamiento de correo, como por ejemplo SMTP (Protocolo simple de transferencia de correo). La tabla de búsqueda en los registros de recursos de DNS contiene los tipos de registros de correo que están soportados por iSeries DNS.

El DNS incluye información para enviar correo electrónico utilizando información de intercambio de correo. Si la red utiliza DNS, la aplicación SMTP no se encarga de entregar el correo con destino al sistema principal TEST.IBM.COM mediante la apertura de una conexión TCP a TEST.IBM.COM. SMTP primero solicita al servidor DNS que averigüe qué servidores del sistema principal pueden utilizarse 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 *intercambio de correo* (MX). Los registros MX correlacionan un nombre de dominio o de sistema principal con un valor de preferencia o un nombre de sistema principal. Los registros MX suelen utilizarse para indicar que un sistema principal se utilice para procesar correo para otro sistema principal. Los registros también se utilizan para indicar a otro sistema principal que entregue el correo en caso de que no se pueda alcanzar el primer sistema principal. En otras palabras, permiten que el correo destinado a un sistema principal se entregue a un sistema principal diferente.

Pueden existir varios registros de recursos MX para un mismo nombre de dominio o de sistema principal. Cuando hay varios registros MX para el mismo dominio o sistema principal, 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 sistema principal preferido, la aplicación de envío de correo intenta contactar con el siguiente sistema principal 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 sistema principal de destino.

Nota: No se recomienda utilizar un carácter comodín (ejemplo: `*.miempresa.com`) en los registros MX de un dominio.

Ejemplo: registro MX de un sistema principal

En el ejemplo siguiente, el sistema envía el correo de fsc5.test.ibm.com de forma prioritaria al propio sistema principal. Si no puede alcanzarse el sistema principal, 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 de DNS (Sistema de nombres de dominio)" en la página 8
Este tema explica cómo DNS (Sistema de nombres de dominio) utiliza los registros de recursos. Los registros de recursos se utilizan para almacenar datos sobre nombres de dominio y direcciones IP. En este tema encontrará una lista en la que podrá buscar los registros de recursos soportados en OS/400 V5R1.

Ejemplos de DNS (Sistema de nombres de dominio)

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

DNS es un sistema de bases de datos distribuidas que sirve para gestionar nombres de sistemas principales y sus direcciones IP asociadas. 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 DNS (Sistema de nombres de dominio) para una intranet

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

En la ilustración siguiente se describe la ejecución del DNS en un sistema iSeries de una red interna. Esta única instancia de servidor DNS está configurada para que atienda las consultas de todas las direcciones IP de la interfaz. El servidor es un servidor de nombres primario de la zona miempresa.com.

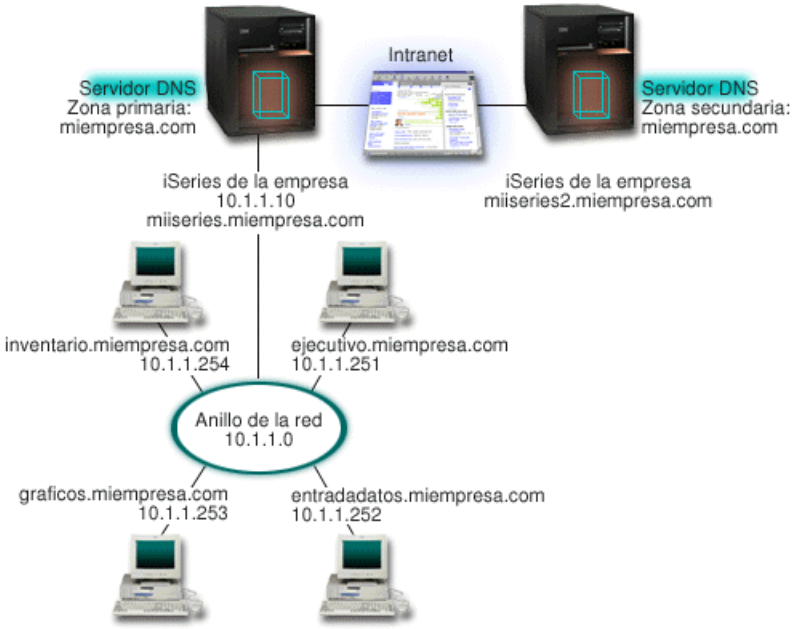


Figura 2. Un único servidor DNS para una intranet

Cada sistema principal de la zona tiene una dirección IP y un nombre de dominio. El administrador debe definir manualmente los sistemas principales de los datos de zona del DNS a través de la creación de registros de recursos. Los registros de correlación de direcciones (A) correlacionan el nombre de una máquina con su dirección IP asociada. De esta forma, el resto de los sistemas principales de la red pueden solicitar al servidor DNS que busquen la dirección IP que está asignada a un nombre de sistema principal particular. Los registros de puntero de búsqueda inversa (PTR) correlacionan la dirección IP de una máquina con su nombre asociado. De esta forma, el resto de los sistemas principales de la red pueden solicitar al servidor DNS que busquen el nombre del sistema principal que se corresponda con una dirección IP.

Además de los registros A y PTR, el DNS admite otros muchos registros de recursos que pueden ser necesarios 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 intercambio de correo (MX) para que SMTP pueda solicitar al DNS que busque cuáles son los sistemas que están ejecutando 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 autorizado. Los servidores secundarios obtienen los datos de zona mediante transferencias de zona desde el servidor autorizado. 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 haga una consulta al servidor de nombres primario y determine que los datos han cambiado. En la figura 2, el servidor miiseries forma parte de una intranet. Se ha configurado otro servidor iSeries, miiseries2, para que actúe como servidor DNS secundario de la zona miempresa.com. El servidor secundario puede utilizarse para equilibrar la demanda de servidores y también para proporcionar una copia de seguridad en caso de que el servidor primario no esté operativo. Conviene tener al menos un servidor secundario para cada zona.

Referencia relacionada

"Registros de recursos de DNS (Sistema de nombres de dominio)" en la página 8
Este tema explica cómo DNS (Sistema de nombres de dominio) utiliza los registros de recursos. Los registros de recursos se utilizan para almacenar datos sobre nombres de dominio y direcciones IP. En este tema encontrará una lista en la que podrá buscar los registros de recursos soportados en OS/400 V5R1.

"Comprender las zonas" en la página 2
Este tema explica las zonas DNS (Sistema de nombres de dominio) y los tipos de zonas.

"Ejemplo: un único servidor DNS (Sistema de nombres de dominio) con acceso a Internet"
Este ejemplo describe una subred simple con un servidor DNS (Sistema de nombres de dominio) conectado directamente a Internet.

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

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

En la ilustración siguiente se describe 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 en la red.

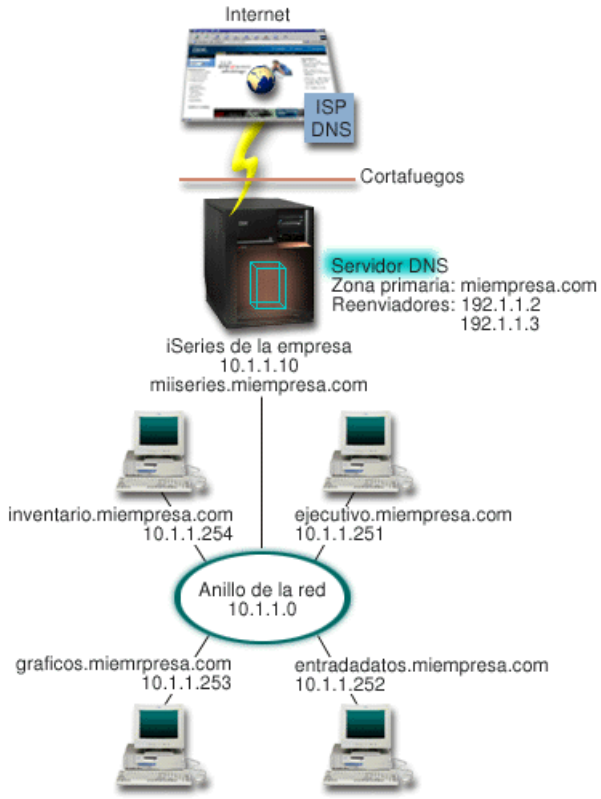


Figura 3. Un único servidor DNS con acceso a Internet

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 por omisión, pero posiblemente necesitará actualizar la lista. Estos servidores pueden ayudarle a resolver las direcciones fuera de su propia zona. Si desea ver las instrucciones sobre cómo obtener los servidores raíz de Internet actuales, consulte la sección "Acceso a los datos externos del DNS (Sistema de nombres de dominio)" en la página 28.
- Habilitar la función de reenvío

  Puede configurar la función de reenvío para pasar las consultas sobre zonas fuera de miempresa.com a los servidores DNS externos, por ejemplo los que ejecute su proveedor de servicios de Internet (ISP). Si desea habilitar una búsqueda por servidores de reenvío y servidores raíz, deberá establecer la opción `reenviar` con el valor **primero**. El servidor intenta realizar la consulta primero en el servidor de reenvío y luego en los servidores raíz siempre que el primero no pueda 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, se trata de direcciones restringidas y no pueden utilizarse fuera de una intranet. Se muestran a continuación sólo a título de ejemplo, pero es su ISP quien determine sus propias direcciones IP y otros factores de la red.
- Registrar el nombre de su dominio

  Si desea estar accesible en Internet y si aún no se ha registrado, debe registrar un nombre de dominio.
- Establecer un cortafuegos

  No se recomienda que permita que su servidor DNS se conecte directamente a Internet. Debe configurar un cortafuegos o tomar otras medidas de precaución para proteger su servidor iSeries.

Conceptos relacionados

"Configuración del dominio DNS (Sistema de nombres de dominio)" en la página 4
Este tema proporciona una visión general del registro del dominio, que enlaza con otros sitios de referencia para configurar su propio espacio del dominio.

iSeries y la seguridad en Internet

"Comprender las consultas de DNS (Sistema de nombres de dominio)" en la página 3
Este tema explica cómo DNS (Sistema de nombres de dominio) resuelve las consultas en nombre de los clientes.

Referencia relacionada

"Ejemplo: un único servidor DNS (Sistema de nombres de dominio) para una intranet" en la página 14
Este ejemplo describe una subred simple con un servidor DNS (Sistema de nombres de dominio) para uso interno.

Ejemplo: DNS (Sistema de nombres de dominio) y DHCP (Protocolo de configuración dinámica de sistemas principales) en el mismo servidor iSeries

Este ejemplo ilustra DNS (Sistema de nombres de dominio) y DHCP (Protocolo de configuración dinámica de sistemas principales) en el mismo servidor.

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

En la figura siguiente se describe una pequeña subred con un servidor iSeries que actúa como 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. Mediante una unidad de red, conectan el servidor de archivos de gráficos al nombre del sistema principal correspondiente.

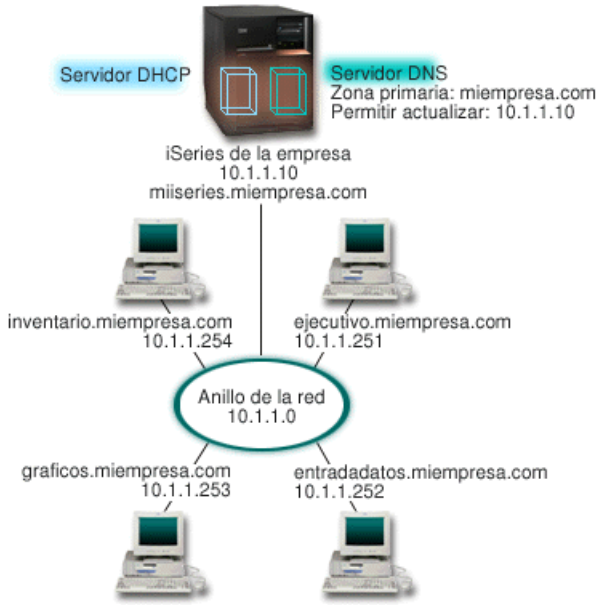


Figura 4. DNS y DHCP en el mismo servidor iSeries

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 un DHCP, los clientes que dependen de él no podrán correlacionar la unidad de red con su nombre de sistema principal porque los registros DNS contendrán la dirección IP anterior del servidor de archivos.

Con el servidor DNS de OS/400 V5R1 basado en BIND 8, puede configurar la zona DNS para que acepte actualizaciones dinámicas en los registros DNS además de otros cambios intermitentes de direcciones realizados a través de DHCP. Por ejemplo, cuando el servidor de archivos de gráficos renueva su vínculo temporal y el servidor DHCP le asigna la dirección IP 10.1.1.250, los registros DNS asociados se actualizarán dinámicamente. De esta forma, el resto de los clientes podrán solicitar al servidor DNS el servidor de archivos de gráficos por su nombre de sistema principal de forma ininterrumpida.

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.Consulte la sección “Determinar la estructura del dominio” en la página 21 si desea más información sobre cómo configurar las zonas para utilizar 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 incremental (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 5
OS/400 DNS V5R1 basado en BIND 8 permite realizar actualizaciones dinámicas. De este modo, fuentes externas, como por ejemplo DHCP (Protocolo de configuración dinámica de sistemas principales), pueden enviar actualizaciones al servidor DNS (Sistema de nombres de dominio).

“Determinar la estructura del dominio” en la página 21
Si está configurando por primera vez un dominio, planifique sus necesidades y el mantenimiento antes de crear zonas.

Tareas relacionadas

Configuración de DHCP para enviar actualizaciones dinámicas

Referencia relacionada

Ejemplo: DNS y DHCP en servidores iSeries diferentes

Ejemplo: dividir DNS (Sistema de nombres de dominio) con un cortafuegos

Este ejemplo describe el funcionamiento del DNS (Sistema de nombres de dominio) con un cortafuegos para proteger los datos internos de Internet, a la vez que se permite que los usuarios internos accedan a los datos de Internet.

En la ilustración siguiente se describe una subred simple que utiliza un cortafuegos de seguridad. El DNS de OS/400 V5R1 basado en BIND 8 le permite configurar varios servidores DNS en un solo sistema iSeries. 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 del sistema principal externo 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 desean que las personas externas encargadas de resolver nombres tengan acceso a la red interna.

Para conseguirlo, la empresa configura dos instancias de servidor DNS en el mismo servidor iSeries, uno para la intranet y el otro para todo lo demás de su dominio público. Esta situación se denomina *DNS dividido*.

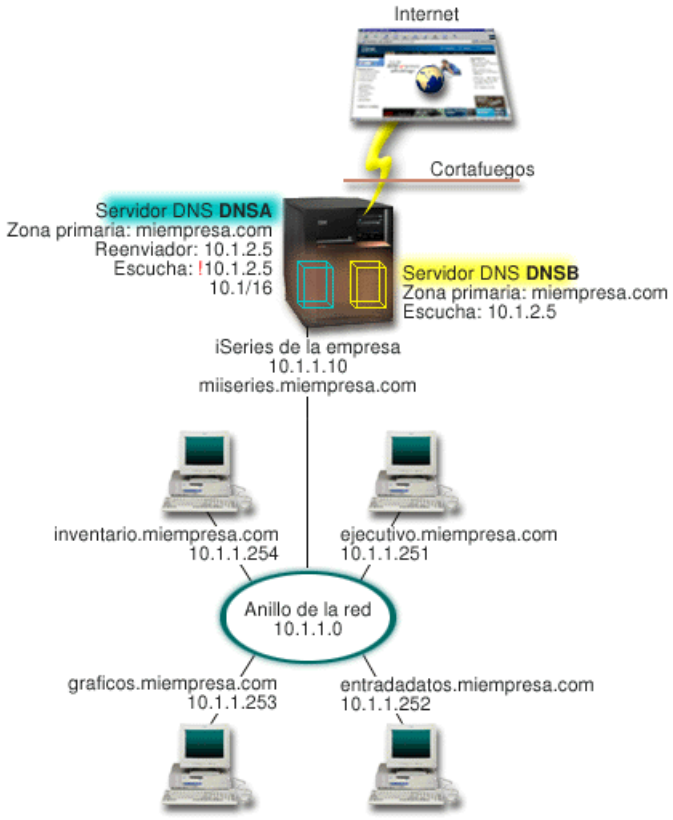


Figura 5. Dividir DNS con un cortafuegos

El servidor externo, DNSB, está configurado con una zona primaria llamada 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 una zona primaria miempresa.com, pero los datos de la zona definidos en DNSA contienen registros de recursos de la intranet. La opción de reenvío está definida como 10.1.2.5. Esto hace que 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 sólo admita consultas a la zona interna miempresa.com procedentes de sistemas principales internos. Para que todo esto funcione correctamente, los clientes internos necesitan estar configurados de forma que sólo se realicen consultas al servidor DNSA. Debe considerar los valores de configuración siguientes para configurar la división del DNS:

- Escucha (listen-on)

  En los ejemplos anteriores, sólo había un servidor DNS en un sistema iSeries. Estaba configurado para escuchar todas las direcciones IP de la interfaz. Siempre que tenga varios servidores DNS en un sistema iSeries, debe definir las direcciones IP de interfaz que escucha cada servidor. Dos servidores DNS no pueden escuchar la misma dirección. En este caso, supongamos que todas las consultas que proceden del cortafuegos se envían a la dirección 10.1.2.5. Estas consultas deben enviarse al servidor externo. Por lo tanto, DNSB se configura para que escuche la dirección 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* la 10.1.2.5. Para excluir esta dirección, ésta debe estar situada en la Lista de correlación de direcciones (AML) antes que el prefijo de la dirección que desea incluirse.
- Orden de los elementos de la Lista de correlación de direcciones (AML)

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

  Si los elementos están invertidos (10.1/16; !10.1.2.5), se permitirá el acceso a la dirección IP 10.1.2.5 porque el servidor la comparará con el primer elemento, que coincide, y la aceptará sin comprobar el resto de las normas.

Referencia relacionada

"Funciones de BIND 8" en la página 6
Además de las actualizaciones dinámicas, BIND 8 ofrece varias funciones para mejorar el rendimiento del servidor DNS (Sistema de nombres de dominio).

Elaborar un plan para DNS (Sistema de nombres de dominio)

DNS (Sistema de nombres de dominio) 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 antes de implementar el servidor DNS.

Determinar las autorizaciones de DNS (Sistema de nombres de dominio)

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

Al configurar el DNS, debe tomar una serie de precauciones 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 del iSeries pueda configurar y administrar el servidor DNS. Otorgar acceso a todos los objetos significa garantizar que el administrador pueda realizar las tareas administrativas del servidor DNS. Se recomienda otorgar a los usuarios que configuren el DNS acceso como responsables de seguridad con autorización para todos los objetos (*ALLOBJ). Utilice iSeries Navigator para autorizar a los usuarios. Si necesita más información, lea el tema Otorgar autorización al administrador de DNS en la ayuda en línea del servidor 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 de DNS (Sistema de nombres de dominio)" en la página 31
Este tema describe los archivos que utiliza DNS (Sistema de nombres de dominio), así como las directrices para hacer una copia de seguridad de los mismos y mantenerlos.

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 se divide el dominio o 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 tener información más detallada.

Si configura una zona DNS (Sistema de nombres de dominio) como zona dinámica, no podrá realizar cambios manuales en los datos de zona mientras el servidor esté ejecutándose. 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 envían a un servidor DNS detenido no pueden completarse. 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 por ejemplo dynamic.miempresa.com, para los clientes que se vayan a mantener de forma dinámica.

El DNS de iSeries proporciona una interfaz gráfica para configurar los servidores. En algunos casos, la interfaz utiliza terminología y conceptos que podrían representarse de forma diferente en otras fuentes. Si consulta otras fuentes de información cuando planifique la configuración del DNS, podría resultarle útil recordar lo siguiente:

- Todas las zonas y objetos definidos en el servidor están organizados en las carpetas **Zona de búsqueda directa** y **Zona de búsqueda inversa**. Las zonas de búsqueda directa se utilizan para correlacionar nombres de dominio con direcciones IP, como los registros A. Las zonas de búsqueda inversa se utilizan para correlacionar direcciones IP con nombres de dominio, como los registros PTR.
- En el DNS de iSeries se utilizan 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 sobre la que se ha delegado responsabilidad sobre uno o más servidores de nombres.

Referencia relacionada

"Ejemplo: DNS (Sistema de nombres de dominio) y DHCP (Protocolo de configuración dinámica de sistemas principales) en el mismo servidor iSeries" en la página 17
Este ejemplo ilustra DNS (Sistema de nombres de dominio) y DHCP (Protocolo de configuración dinámica de sistemas principales) en el mismo servidor.

Planificar medidas de seguridad

El DNS (Sistema de nombres de dominio) proporciona opciones de seguridad para limitar el acceso externo a su servidor.

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 iSeries se describen en diversas fuentes, que incluyen iSeries e Internet en el Information Center. El manual DNS and BIND también trata sobre la seguridad relacionada con el DNS.

Listas de correlación de direcciones

DNS utiliza listas de correlación 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 TSIG (Firma de transacción). Puede definir una lista de entidades a las que desee permitir o denegar el acceso e incluirlas en una lista de correlación de direcciones. Si desea poder

reutilizar la lista de correlación 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 de la lista de correlación de nombres

Se utiliza el primer elemento de una lista de correlación de direcciones con el que coincida una dirección determinada. Por ejemplo, para permitir el acceso a todas las direcciones de la red 10.1.1.x excepto 10.1.1.5, los elementos de la lista de correlación 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 su acceso será denegado 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 el resto de las normas.

Opciones de control de acceso

DNS le permite definir limitaciones 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 sistemas principales tienen permiso para realizar consultas a este servidor. Si no se especifica, el valor por omisión es permitir las consultas de todos los sistemas principales.

allow-transfer
Especifica qué sistemas principales tienen permiso para recibir transferencias de zona del servidor. Si no se especifica, el valor por omisión es permitir las transferencias de todos los sistemas principales.

allow-recursion
Especifica qué sistemas principales tienen permiso para realizar consultas repetidas a través de este servidor. Si no se especifica, el valor por omisión es permitir las consultas repetidas de todos los sistemas principales.

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 serán respondidas.

Conceptos relacionados

iSeries y la seguridad en Internet

Referencia relacionada

“Funciones de BIND 8” en la página 6
Además de las actualizaciones dinámicas, BIND 8 ofrece varias funciones para mejorar el rendimiento del servidor DNS (Sistema de nombres de dominio).

Requisitos de DNS (Sistema de nombres de dominio)

En este tema se describen los requisitos de software para ejecutar el DNS (Sistema de nombres de dominio) en el servidor iSeries.

La opción DNS (Opción 31) no se instala automáticamente con el sistema operativo base. Debe seleccionar DNS específicamente para que se instale. El nuevo servidor DNS añadido para OS/400 V5R1

se basa en la implementación del DNS estándar en la industria, conocido como BIND 8. Los servicios DNS del OS/400 se basaban en BIND 4.9.3, y siguen disponibles en OS/400 V5R1.

Después de que haya instalado el DNS, se configura por omisión un único servidor DNS que utiliza las funciones de servidor DNS basadas en BIND 4.9.3 y que estaban disponibles en las versiones anteriores. Si desea ejecutar uno o más servidores DNS mediante BIND 8, debe instalar PASE. PASE es la Opción 33 de SS1. Una vez instalada la opción PASE, iSeries Navigator maneja automáticamente la configuración de la implementación BIND correcta.

Si no utiliza PASE, no podrá beneficiarse de todas las funciones de BIND 8. Si no utiliza la opción PASE, puede seguir ejecutando el mismo servidor DNS basado en BIND 4.9.3 que estaba disponible en las versiones anteriores. Consulte el tema DNS V4R5 de Information Center para obtener información relativa a BIND 4.9.3.

Si desea configurar un servidor DHCP en un sistema iSeries diferente para enviar actualizaciones a este servidor DNS, la Opción 31 también debe instalarse en el DHCP de iSeries. El servidor DHCP (Protocolo de configuración dinámica de sistemas principales) utiliza las interfaces de programación que proporciona la Opción 31 para realizar actualizaciones dinámicas.

Conceptos relacionados

Portable Application Solutions Environment (PASE)

"Configurar el DNS (Sistema de nombres de dominio)" en la página 24
En este tema se explica cómo utilizar iSeries Navigator para configurar los servidores de nombres y para resolver las consultas realizadas fuera de su dominio.

Referencia relacionada

"Funciones de BIND 8" en la página 6
Además de las actualizaciones dinámicas, BIND 8 ofrece varias funciones para mejorar el rendimiento del servidor DNS (Sistema de nombres de dominio).

Información relacionada

Tema DNS V4R5 del Information Center

Determinar si DNS (Sistema de nombres de dominio) está instalado

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

1. En la línea de mandatos, escriba `GO LICPGM` y pulse Intro.
2. Escriba `10` (Ver los programas bajo licencia instalados) y pulse Intro.
3. Avance páginas hasta llegar a **5722SS1 Sistema de nombres de dominio** (SS1 Opción 31). Si el DNS se ha instalado correctamente, Estado instalación será `*compatible`, tal como se muestra a continuación:

```
LicPgm     Estado instalación     Descripción
5722SS1    *COMPATIBLE          Sistema de nombres de dominio
```

4. Pulse F3 para salir de la pantalla.

Instalar el DNS (Sistema de nombres de dominio)

Para instalar el DNS (Sistema de nombres de dominio), siga estos pasos:

1. En la línea de mandatos, escriba `GO 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.

Configurar el DNS (Sistema de nombres de dominio)

En este tema se explica cómo utilizar iSeries Navigator para configurar los servidores de nombres y para resolver las consultas realizadas fuera de su dominio.

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

Conceptos relacionados

"Requisitos de DNS (Sistema de nombres de dominio)" en la página 22
En este tema se describen los requisitos de software para ejecutar el DNS (Sistema de nombres de dominio) en el servidor iSeries.

Acceder al DNS (Sistema de nombres de dominio) en el iSeries Navigator

Este tema explica cómo acceder al DNS (Sistema de nombres de dominio) en el iSeries Navigator.

Las instrucciones siguientes le guiarán a lo largo de la interfaz de configuración de DNS en el iSeries Navigator. Si está utilizando la opción PASE, podrá configurar servidores DNS basados en BIND 8. Si no utiliza PASE, podrá ejecutar el mismo servidor DNS basado en BIND 4.9.3 que estaba disponible en los releases anteriores. Consulte el tema DNS V4R5 de Information Center para obtener información relativa a DNS basado en BIND 4.9.3.

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

1. En iSeries Navigator, expanda **su servidor iSeries** → **Red** → **Servidores** → **DNS**.
2. Pulse el botón secundario del ratón en **DNS** y seleccione **Configuración nueva**.

Conceptos relacionados

iSeries Navigator

Configurar servidores de nombres

DNS (Sistema de nombres de dominio) le permite crear varias instancias de servidor de nombres. Este tema proporciona las instrucciones para configurar un servidor de nombres.

iSeries DNS basado en BIND 8 admite el uso de varias instancias de un servidor de nombres. Las tareas siguientes le guiarán durante el proceso de crear una instancia de servidor de nombres, incluidas sus propiedades y zonas.

Si desea crear varias instancias, repita este 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 cree una instancia nueva, también se crean archivos de configuración individuales.

Referencia relacionada

"Mantener los archivos de configuración de DNS (Sistema de nombres de dominio)" en la página 31
Este tema describe los archivos que utiliza DNS (Sistema de nombres de dominio), así como las directrices para hacer una copia de seguridad de los mismos y mantenerlos.

Crear una instancia de servidor de nombres

Utilice el asistente Configuración de DNS (Sistema de nombres de dominio) nuevo para definir una instancia de servidor DNS.

Para iniciar el asistente **Configuración de DNS nuevo**, siga estos pasos:

1. En **iSeries Navigator**, expanda **su servidor iSeries** → **Red** → **Servidores** → **DNS**.

2. En el panel de la izquierda, pulse con el botón derecho del ratón sobre **DNS** y seleccione **Servidor de nombres nuevo...**
3. El asistente puede ayudarle durante el proceso de configuración.

El asistente necesita que introduzca la siguiente información:

Nombre de servidor DNS:
Escriba un nombre para el servidor DNS. Puede tener un máximo de 5 caracteres y debe empezar por un carácter alfabético. Si va a crear varios servidores, cada uno deberá tener un nombre exclusivo. En otras áreas del sistema, a este nombre se le denomina nombre de la ″instancia″ del servidor DNS.

Direcciones IP de escucha:
Dos servidores DNS no pueden escuchar la misma dirección IP. El valor por omisión es escuchar TODAS las direcciones IP. Si va a crear instancias de servidor adicionales, ninguna de ellas puede configurarse para que escuche TODAS las direcciones. Debe especificar la dirección IP que corresponde a cada servidor.

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

Nota: Sólo debe considerar la posibilidad de cargar los servidores raíz de Internet por omisión si se encuentra en Internet y espera que su DNS pueda resolver todos 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 DNS (Sistema de nombres de dominio)

Después de crear un servidor de nombres, puede editar sus propiedades, por ejemplo la opción allow-update y los niveles de depuración. Estas opciones sólo se aplican en la instancia del servidor que se modifica.

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

1. En **iSeries Navigator**, expanda **su servidor iSeries** → **Red** → **Servidores** → **DNS**.
2. En el panel de la derecha, pulse el botón secundario del ratón en **Nombre del servidor DNS** y seleccione **Configuración**.
3. Pulse el botón secundario del ratón en **Servidor DNS** y seleccione **Propiedades**.

Configurar zonas en un servidor de nombres

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

El servidor se visualiza en el panel de la derecha. Para configurar zonas en su servidor, pulse el botón secundario del ratón en el nombre del servidor y seleccione **Configuración**. Se visualiza la ventana Configuración de DNS.

Todas las zonas se configuran utilizando asistentes. Cree **Zonas de búsqueda directa** o **Zonas de búsqueda inversa** pulsando el botón secundario del ratón en la carpeta correspondiente. Se visualizarán las opciones de esa zona. Seleccione el tipo de zona que desea crear para iniciar el asistente.

Conceptos relacionados

"Acceso a los datos externos del DNS (Sistema de nombres de dominio)" en la página 28
Al crear datos de zona del DNS (Sistema de nombres de dominio), el servidor podrá resolver las consultas realizadas a dicha zona.

Tareas relacionadas

"Configurar el DNS (Sistema de nombres de dominio) para recibir actualizaciones dinámicas"
Los servidores DNS (Sistema de nombres de dominio) que ejecutan BIND 8 pueden configurarse de modo que acepten peticiones de otras fuentes para actualizar los datos de la zona de forma dinámica. Este tema ofrece instrucciones para configurar la opción allow-update para que el DNS pueda recibir actualizaciones dinámicas.

"Importar archivos de DNS (Sistema de nombres de dominio)" en la página 27
DNS (Sistema de nombres de dominio) 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

"Comprender las zonas" en la página 2
Este tema explica las zonas DNS (Sistema de nombres de dominio) y los tipos de zonas.

Configurar el DNS (Sistema de nombres de dominio) para recibir actualizaciones dinámicas

Los servidores DNS (Sistema de nombres de dominio) que ejecutan BIND 8 pueden configurarse de modo que acepten peticiones de otras fuentes para actualizar los datos de la zona de forma dinámica. 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 necesita realizar actualizaciones manuales en algunas partes del dominio, podría considerar la posibilidad de configurar zonas dinámicas y estáticas por separado. Si tiene que realizar actualizaciones manuales en una zona dinámica, detenga el servidor de la zona dinámica y reinícielo cuando haya completado las actualizaciones. Al detener el servidor, éste sincroniza todas las actualizaciones dinámicas que se hayan realizado desde que el servidor cargó los datos de zona de la base de datos de zona. Si no detiene el servidor, perderá todas las actualizaciones dinámicas que se han procesado desde que se inició. Sin embargo, al detener el servidor para realizar actualizaciones manuales podría perder las actualizaciones dinámicas que se envían mientras el servidor está inactivo.

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

1. En iSeries Navigator, expanda **su servidor iSeries** → **Red** → **Servidores** → **DNS**.
2. En el panel de la derecha, pulse el botón secundario del ratón en **Nombre del servidor DNS** y seleccione **Configuración**.
3. En la ventana Configuración de DNS, expanda **Zona de búsqueda directa** o **Zona de búsqueda inversa**.
4. Pulse el botón secundario del ratón en la zona primaria que desee editar y seleccione **Propiedades**.
5. En la página Propiedades de zona primaria, pulse en la pestaña **Opciones**.
6. En la página Opciones, expanda **Control de acceso** → **allow-update**.
7. DNS utiliza una lista de correlación de direcciones para verificar las actualizaciones autorizadas. Si desea añadir un objeto a la lista de correlación de direcciones, seleccione el tipo de elemento de dicha lista y pulse en **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 correlación de direcciones, pulse en **Aceptar** para cerrar la página Opciones.

Conceptos relacionados

"Actualizaciones dinámicas" en la página 5
OS/400 DNS V5R1 basado en BIND 8 permite realizar actualizaciones dinámicas. De este modo, fuentes externas, como por ejemplo DHCP (Protocolo de configuración dinámica de sistemas principales), pueden enviar actualizaciones al servidor DNS (Sistema de nombres de dominio).

"Configurar zonas en un servidor de nombres" en la página 25
Después de configurar una instancia de servidor DNS (Sistema de nombres de dominio), debe configurar las zonas para el servidor de nombres.

Tareas relacionadas

Configurar DHCP para enviar actualizaciones dinámicas

Importar archivos de DNS (Sistema de nombres de dominio)

DNS (Sistema de nombres de dominio) 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 mediante la importación de un archivo de datos de zona, o mediante la conversión de tablas del sistema principal existentes. Consulte el apartado Conversión de tablas de sistemas principales para crear datos de zona a partir de una tabla de sistemas principales.

Puede importar cualquier archivo que sea un archivo de configuración de zona válido basado en la sintaxis de BIND. El archivo debe residir en un directorio IFS. Cuando se importa, el DNS verifica si se trata de un archivo de datos de zona válido y lo añade al archivo NAMED.CONF de esta instancia de servidor.

Para importar un archivo de zona, siga estos pasos:

1. En iSeries Navigator, expanda **su servidor iSeries** → **Red** → **Servidores** → **DNS**.
2. En el panel de la derecha, pulse el botón secundario del ratón en la instancia del servidor DNS a la que desea importar la zona.
3. En el panel de la izquierda, pulse el botón secundario del ratón en **Servidor DNS** y seleccione **Importar zona**.
4. Siga las instrucciones del asistente para importar la zona primaria.

Conceptos relacionados

"Configurar zonas en un servidor de nombres" en la página 25
Después de configurar una instancia de servidor DNS (Sistema de nombres de dominio), debe configurar las zonas para el servidor de nombres.

Validación del registro

La función Importar datos de dominio interpreta 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 interpreta las líneas que contienen la instrucción $include como líneas erróneas.

Acceso a los datos externos del DNS (Sistema de nombres de dominio)

Al crear datos de zona del DNS (Sistema de nombres de dominio), el servidor podrá resolver las consultas realizadas a dicha 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 sistemas principales 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 de servidores raíz por omisión del iSeries Navigator

Utilice los servidores raíz de Internet únicamente si tiene una conexión a Internet y desea resolver los nombres de Internet en caso de que no los resuelva el servidor DNS. En el iSeries Navigator encontrará una lista por omisión de los servidores raíz de Internet. La lista se actualiza cuando se libera el iSeries Navigator. Puede verificar si la lista por omisión está actualizada comparándola con la lista del sitio InterNIC. Restablezca la lista de servidores raíz de su configuración para mantenerla actualizada.

Dónde conseguir 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. Ejecute FTP de forma anónima en el servidor InterNIC: `FTP.RS.INTERNIC.NET`
2. Baje este archivo: `/domain/named.root`
3. Guarde el archivo en la vía de acceso siguiente: `Integrated File System/Root/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 sólo 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 antememoria. 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 por omisión de Internet. Sin embargo, deberá añadir los servidores raíz internos para que el servidor DNS pueda resolver las direcciones internas fuera de su dominio.

Conceptos relacionados

"Configurar zonas en un servidor de nombres" en la página 25
Después de configurar una instancia de servidor DNS (Sistema de nombres de dominio), debe configurar las zonas para el servidor de nombres.

Gestionar el DNS (Sistema de nombres de dominio)

Este tema trata sobre el método para verificar la funcionalidad del DNS (Sistema de nombres de dominio), supervisar el rendimiento y mantener los datos y archivos del servidor DNS.

Verificar el funcionamiento de DNS (Sistema de nombres de dominio) con NSLookup (Búsqueda del servidor de nombres)

Puede utilizar NSLookup (Búsqueda de servidor de nombres) para verificar el funcionamiento de DNS (Sistema de nombres de dominio).

Utilice NSLookup para solicitar al servidor DNS una dirección IP. De esta forma se comprueba si el servidor DNS está respondiendo a las consultas. Solicite el nombre del sistema principal que está asociado a la dirección IP del bucle de retorno (127.0.0.1). Debería responder con el nombre del sistema principal (local). También debe solicitar nombres específicos que están definidos en la instancia del servidor que está comprobando. De esta forma se confirmará que la instancia del servidor específico que está comprobando funciona correctamente.

Para verificar el funcionamiento del DNS con NSLookup, siga estos pasos:

1. En la línea de mandatos escriba `NSLOOKUP DMNNAMSVR(n.n.n.n)`, donde n.n.n.n es la dirección que el usuario ha configurado como la que la instancia del servidor que está comprobando debe escuchar.
2. En la línea de mandatos, escriba `NSLOOKUP` y pulse Intro. Así se inicia una sesión de consulta de NSLookup.
3. Escriba `server` seguido del nombre de servidor y pulse Intro. Por ejemplo: `server miiseries.miempresa.com`. Se muestra esta información:

   ```
       Servidor:  miiseries.miempresa.com
     Dirección: n.n.n.n
   ```

   Donde `n.n.n.n` representa la dirección IP de su servidor DNS.
4. Teclee `127.0.0.1` en la línea de mandatos y pulse Intro.

   Debe mostrarse esta información, incluido el nombre del sistema principal del bucle de retorno:

   ```
   > 127.0.0.1
    Servidor:  miiseries.miempresa.com
    Dirección: n.n.n.n


   Nombre:    sistprallocal
       Dirección:  127.0.0.1
   ```

   El servidor DNS responde correctamente si devuelve el nombre de sistema principal del bucle de retorno **sistprallocal**.
5. Escriba `exit` y pulse Intro para salir de la sesión de terminal NSLOOKUP.

Nota: Si necesita ayuda para utilizar NSLookup, escriba `?` y pulse Intro.

Gestionar las claves de seguridad

Las claves de seguridad le permiten limitar el acceso a sus datos DNS (Sistema de nombres de dominio).

Existen dos tipos de claves relacionadas con el DNS. 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 claves de DNS (Sistema de nombres de dominio)

Las claves de DNS (Sistema de nombres de dominio) 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, por ejemplo una zona dinámica, puede especificar la clave en la lista de correlación de direcciones.

Para gestionar las claves de DNS siga estos pasos:

1. En iSeries Navigator, expanda **su servidor iSeries** → **Red** → **Servidores** → **DNS**.
2. En el panel de la derecha, pulse el botón secundario del ratón en la instancia del servidor DNS que desee para abrir y seleccionar **Configuración**.
3. En la ventana Configuración de DNS, seleccione **Archivo** → **Gestionar claves.**

Gestionar claves de actualización dinámica

Las claves para la actualización dinámica se utilizan con el objeto de proteger las actualizaciones dinámicas que realiza el servidor DHCP (Protocolo de configuración dinámica de sistemas principales).

Estas claves deben estar presentes cuando DNS (Sistema de nombres de dominio) y DHCP se encuentran en el mismo iSeries. Si el DHCP está en un iSeries diferente, deberá crear la misma clave de actualización dinámica en cada uno de los servidores iSeries para que puedan llevarse a cabo unas actualizaciones dinámicas seguras.

Para gestionar las claves de actualización dinámica siga estos pasos:

1. En iSeries Navigator, expanda **su servidor iSeries** → **Red** → **Servidores** → **DNS**.
2. Pulse con el botón derecho del ratón en **DNS** y seleccione **Gestionar claves de actualización dinámica**.

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

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

DNS (Sistema de nombres de dominio) proporciona diversas herramientas de diagnóstico. Pueden utilizarse para supervisar el rendimiento del servidor.

Referencia relacionada

"Mantener los archivos de configuración de DNS (Sistema de nombres de dominio)" en la página 31
Este tema describe los archivos que utiliza DNS (Sistema de nombres de dominio), así como las directrices para hacer una copia de seguridad de los mismos y mantenerlos.

Estadísticas del servidor

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

DNS (Sistema de nombres de dominio) le permite ver las estadísticas de la instancia de un 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 de ayuda en línea de DNS Comprender las estadísticas del servidor DNS.

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

1. En iSeries Navigator, expanda **su servidor iSeries** → **Red** → **Servidores** → **DNS**.
2. En el panel de la derecha, pulse el botón secundario del ratón en **Nombre del servidor DNS** y seleccione **Configuración**.
3. En la ventana Configuración de DNS, seleccione **Ver** → **Estadísticas del servidor**.

Base de datos activa del servidor

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

DNS (Sistema de nombres de dominio) le permite ver un vuelco de los datos autorizados, los datos de la antememoria 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.

Utilice el iSeries Navigator si desea ver el vuelco de la base de datos activa del servidor. Si tiene que guardar una copia de los archivos, el nombre de archivo del vuelco de la base de datos es NAMED_DUMP.DB en la vía de acceso del directorio de iSeries: **Integrated File System/Root/QIBM/UserData/OS400/DNS/<instancia servidor>**, donde "<instancia servidor>" es el nombre de la instancia del servidor DNS. Hay más información disponible sobre la base de datos activa del servidor en el tema de ayuda en línea de DNS **Comprender el vuelco de la base de datos del servidor DNS**.

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

1. En iSeries Navigator, expanda **su servidor iSeries** → **Red** → **Servidores** → **DNS**.
2. En el panel de la derecha, pulse el botón secundario del ratón en **Nombre del servidor DNS** y seleccione **Configuración**.
3. En la ventana Configuración de DNS, seleccione **Ver** → **Base de datos del servidor activo**.

Mantener los archivos de configuración de DNS (Sistema de nombres de dominio)

Este tema describe los archivos que utiliza DNS (Sistema de nombres de dominio), así como las directrices para hacer una copia de seguridad de los mismos y mantenerlos.

Puede utilizar i5/OS DNS para crear y gestionar instancias del servidor DNS en el iSeries. iSeries Navigator gestiona los archivos de configuración del DNS. No debe modificar los archivos manualmente. Utilice siempre iSeries Navigator 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 integrados que figuran a continuación.

Nota: La estructura de archivos que se muestra a continuación se aplica al DNS que se ejecuta en BIND 8. Si utiliza un DNS basado en BIND 4.9.3, consulte la sección Copia de seguridad de los archivos de configuración DNS y mantenimiento de los archivos de anotaciones en el tema DNS V4R5 de Information Center.

En la tabla siguiente, los archivos se enumeran con la jerarquía de vías de acceso que se muestra. Debe hacerse una copia de seguridad de los archivos que tienen un icono de guardar  para proteger los datos. Los archivos que tienen un icono del tipo  deben suprimirse periódicamente.

Nombre	Icono	Descripción
QIBM/UserData/OS400/DNS/		Directorio de partida de DNS.
ATTRIBUTES		DNS utiliza este archivo para determinar la versión de BIND que está utilizando.
QIBM/UserData/OS400/DNS/<*instancia-n*>/		Directorio de partida de una instancia de DNS.

Nombre	Icono	Descripción
ATTRIBUTES		Atributos de configuración que utiliza iSeries DNS.
NAMED.CONF		Este archivo contiene los datos de configuración. Se utiliza para indicar al servidor qué zonas específicas está gestionando, dónde se encuentran los archivos de zona, qué zonas pueden actualizarse de forma dinámica, dónde se encuentran los servidores de reenvío y otras opciones.
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 realiza una migración del servidor BIND 4.9.3 a BIND 8. Hace las veces de copia de seguridad durante la migración, y puede suprimirse cuando el servidor BIND 8 ya funciona correctamente.
NAMED.CA		Lista de servidores raíz para esta instancia del servidor.
NAMED_DUMP.DB		Vuelco de datos del servidor que se crea para la base de datos activa del servidor.
NAMED.STATS		Estadísticas del servidor.
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.
QUERYLOG		Las anotaciones cronológicas del servidor DNS de las consultas recibidas. Este archivo se crea cuando las anotaciones cronológicas del servidor DNS están activas. En ese caso, el tamaño del archivo aumenta y debe suprimirse periódicamente.
<*nombre-zona-a*>.DB		Archivo de zona de un dominio determinado que proporciona este servidor. Contiene todos los registros de recursos de esta zona.
<*nombre-zona-b*>.DB		Archivo de zona de un dominio determinado que proporciona este servidor. Contiene todos los registros de recursos de esta zona. Cada zona tiene un archivo .DB individual.

Nombre	Icono	Descripción
.ixfr.		Archivos IXFR (transferencia de zona incremental). Estos archivos los utilizan servidores secundarios para cargar únicamente los datos modificados desde la última transferencia de zona realizada. A medida que se efectúan las actualizaciones, el número de archivos IXFR se incrementa. Debe suprimir los archivos IXFR antiguos periódicamente. Si conserva los archivos que se crearon uno o dos días atrás, la mayoría de servidores secundarios seguirán cargando los IXFR. Si suprime todos los archivos, el servidor secundario solicitará una transferencia completa (AXFR).
TMP		Directorio que la instancia del servidor utiliza para crear archivos de trabajo temporal.
QIBM/UserData/OS400/DNS/TMP		Directorio temporal que utiliza el programa QTOBH2N para crear archivos intermedios volcados de la tabla del sistema principal para importarlos posteriormente mediante el iSeries Navigator.
QIBM/UserData/OS400/DNS/_DYN/		Directorio que contiene los archivos necesarios para realizar las actualizaciones dinámicas.
<*id_clave-nombre-x*>._KID		Archivo que contiene una sentencia clave BIND 8 para el id_clave denominado <*id_clave-nombre-x*>.
<*id_clave-nombre-x*>._DUK.<*nombre-zona-a*>		Clave de actualización dinámica necesaria para iniciar una petición de actualización dinámica en <*nombre-zona-a*> utilizando la clave <*id_clave-nombre-x*>.
<*id_clave-nombre-y*>._KID		Archivo que contiene una sentencia clave BIND 8 para el id_clave denominado <*id_clave-nombre-y*>.
<*id_clave-nombre-y*>._DUK.<*nombre-zona-a*>		Clave de actualización dinámica necesaria para iniciar una petición de actualización dinámica en <*nombre-zona-a*> utilizando la clave <*id_clave-nombre-y*>.
<*id_clave-nombre-y*>._DUK.<*nombre-zona-b*>		Clave de actualización dinámica necesaria para iniciar una petición de actualización dinámica en <*nombre-zona-b*> utilizando la clave <*id_clave-nombre-y*>.

Conceptos relacionados

"Determinar las autorizaciones de DNS (Sistema de nombres de dominio)" en la página 20
Existen requisitos especiales de autorización para el administrador de DNS (Sistema de nombres de dominio). Debe tener en cuenta también las implicaciones de seguridad de la autorización.

"Acceder a las estadísticas del servidor DNS (Sistema de nombres de dominio)" en la página 30
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 24
DNS (Sistema de nombres de dominio) le permite crear varias instancias de servidor de nombres. Este tema proporciona las instrucciones para configurar un servidor de nombres.

Características avanzadas de DNS (Sistema de nombres de dominio)

Este tema explica cómo los administradores con experiencia pueden utilizar las características avanzadas de DNS (Sistema de nombres de dominio) para gestionar más fácilmente un servidor DNS.

El DNS de iSeries Navigator proporciona una interfaz para configurar y gestionar el servidor DNS. Las tareas siguientes están disponibles como atajos para los administradores que están familiarizados con la interfaz gráfica de iSeries. Ofrecen una serie de métodos rápidos para cambiar el estado y los atributos del servidor en varias instancias a la vez.

Tareas relacionadas

"Cambiar los valores de depuración de DNS (Sistema de nombres de dominio)" en la página 37
La función de depuración de DNS (Sistema de nombres de dominio) puede proporcionar información que le ayudará a determinar y corregir los problemas del servidor DNS.

Cambiar los atributos de DNS (Sistema de nombres de dominio)

Puede cambiar los valores de DNS (Sistema de nombres de dominio) si la interfaz del DNS no le permite cambiar todos los niveles de autoinicio y de depuración de la instancia del servidor a la vez.

Puede utilizar la interfaz basada en caracteres para cambiar estos valores en instancias individuales del servidor DNS, o en todas las instancias a la vez. Para utilizar CHGDNSA siga estos pasos:

1. En la línea de mandatos, escriba `CHGDNSA` y pulse F4.
2. En la página Cambiar los atributos del servidor DNS (CHGDNSA), escriba el nombre de una sola instancia del servidor, o bien teclee `*ALL`, y pulse Intro.

   Se mostrarán las opciones disponibles de los atributos del servidor:

   ```
   Iniciar servidor automáticamente . . . . . *SAME *YES, *NO, *SAME
   Nivel de depuración . . . . . *SAME 0-11, *SAME, *DFT
   ```

3. **Inicio automático** Para especificar que los servidores DNS seleccionados se inicien automáticamente cuando se inicia TCP/IP, teclee `*YES`. Si no desea que el servidor se inicie cuando lo hace TCP/IP, teclee `*NO`. Para mantener los valores actuales del atributo, teclee `*SAME`.

   Nivel de depuración Para cambiar el nivel de depuración que deben utilizar los servidores DNS seleccionados, escriba un valor entre 0 y 11. Para especificar que el nivel de depuración herede el valor de depuración de inicio del servidor, teclee `*DFT`. Para mantener los valores actuales del atributo, teclee `*SAME`.

   Cuando haya especificado todas sus preferencias, pulse Intro para establecer los atributos del DNS.

Iniciar o detener servidor DNS (Sistema de nombres de dominio)

Puede cambiar los valores si la interfaz del DNS (Sistema de nombres de dominio) no le permite iniciar ni detener varias instancias del servidor a la vez.

Puede utilizar la interfaz basada en caracteres para cambiar estos valores en todas las instancias a la vez. Para utilizar la interfaz basada en caracteres para iniciar a la 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 `ENDTCPSVR SERVER(*DNS) DNSSVR(*ALL)` en la línea de mandatos.

Cambiar los valores de depuración

Puede cambiar el nivel de depuración, lo que resulta útil a los administradores que están al cargo de zonas extensas y cuando no desean la gran cantidad de datos de depuración que reciben al iniciar por primera vez el servidor y cargar todos los datos de la zona.

El DNS (Sistema de nombres de dominio) en la interfaz del iSeries Navigator no le permite cambiar el nivel de depuración mientras el servidor se esté ejecutando. Sin embargo, puede utilizar dicha interfaz para hacerlo. Para cambiar el nivel de depuración mediante la interfaz basada en caracteres, siga estos pasos sustituyendo <instancia> por el nombre de la instancia del servidor:

1. En la línea de mandatos, escriba `ADDLIBLE QDNS` y pulse Intro.
2. Cambie el nivel de depuración:
   - Para activar la depuración o para aumentar el nivel de depuración en incrementos de 1, escriba `CALL QTOBDRVS ('BUMP' '<instancia>')` y pulse Intro.
   - Para desactivar la depuración, escriba `CALL QTOBDRVS ('OFF' '<instance>')` y pulse Intro.

Resolución de problemas de DNS (Sistema de nombres de dominio)

Este tema trata sobre los valores de las anotaciones cronológicas y depuración del DNS (Sistema de nombres de dominio) que le ayudarán a resolver los problemas que puedan presentarse en 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 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 utiliza BIND 4.9.3, el nombre del trabajo del servidor será QTOBDNS. Hallará más información acerca de la depuración de DNS 4.9.3 en la sección *Resolución de problemas de los servidores DNS*.
- Si ejecuta servidores basados en BIND 8, habrá un trabajo individual por cada instancia de servidor que ejecute. El nombre del trabajo tiene 5 caracteres fijos (QTOBD) seguido del nombre de la instancia. Por ejemplo, si tiene dos instancias, INST1 e INST2, sus nombres de trabajo serán QTOBDINST1 y QTOBDINST2.

Conceptos relacionados

"Anotar mensajes del servidor DNS (Sistema de nombres de dominio)" en la página 36
DNS (Sistema de nombres de dominio) proporciona varias opciones de anotaciones cronológicas que pueden ajustarse cuando trata de encontrar el origen de un problema. Las anotaciones cronológicas proporcionan gran flexibilidad, ya que ofrecen diversos niveles de gravedad y archivos de salida para que se puedan generar anotaciones cronológicas más precisas, y ayudarle así a localizar los problemas.

Tareas relacionadas

"Cambiar los valores de depuración de DNS (Sistema de nombres de dominio)" en la página 37
La función de depuración de DNS (Sistema de nombres de dominio) puede proporcionar información que le ayudará a determinar y corregir los problemas del servidor DNS.

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

DNS (Sistema de nombres de dominio) proporciona varias opciones de anotaciones cronológicas que pueden ajustarse cuando trata de encontrar el origen de un problema. Las anotaciones cronológicas proporcionan gran flexibilidad, ya que ofrecen diversos niveles de gravedad y archivos de salida para que se puedan generar anotaciones cronológicas más precisas, y ayudarle así a localizar los problemas.

BIND 8 ofrece varias opciones nuevas para las anotaciones cronológicas. Puede especificar qué tipos de mensajes se anotan cronológicamente, dónde se envía cada tipo de mensaje y qué nivel de gravedad de cada tipo de mensaje debe anotarse. En general, los valores por omisión de las anotaciones cronológicas son los adecuados, pero si desea cambiarlos, se recomienda que consulte otras fuentes de documentación de BIND 8 para obtener información sobre las anotaciones cronológicas.

Canales de anotaciones cronológicas

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

- **Canales de archivos**

  Los mensajes anotados cronológicamente en los canales de archivos se envían a un archivo. Los canales de archivos por omisión son as400_debug y as400_QPRINT. Los mensajes de depuración se anotan cronológicamente por omisión en el canal as400_debug, que es el archivo NAMED.RUN, pero también puede especificar que se envíen otras categorías de mensaje a este archivo. Las categorías de mensaje anotadas cronológicamente en as400_QPRINT se envían al archivo de cola de impresión QPRINT para el perfil de usuario QTCP. Puede crear sus propios canales de archivos además de los canales que se proporcionan por omisión.
- **Canales de Syslog**

  Los mensajes anotados cronológicamente en este canal se envían a las anotaciones de trabajo de los servidores. El canal syslog por omisión es as400_joblog. Los mensajes anotados cronológicamente que se hayan direccionado a este canal se envían a las anotaciones de trabajo de la instancia del servidor DNS.
- **Canales nulos**

  Todos los mensajes anotados cronológicamente en el canal nulo serán descartados. El canal nulo por omisión es as400_null. Puede direccionar las categorías al canal nulo si no desea que los mensajes aparezcan en ningún archivo de anotaciones cronológicas.

Categorías de mensajes

Los mensajes se agrupan en categorías. Puede especificar qué categorías de mensajes deben anotarse cronológicamente en cada canal. Existen muchas categorías, entre las que se incluyen:

- config: proceso del archivo de configuración
- db: operaciones de la base de datos
- queries: genera un mensaje corto de registro para cada consulta que recibe el servidor
- lame-servers: detecta las delegaciones incorrectas
- update: actualizaciones dinámicas
- xfer-in: transferencia de zona que recibe el servidor
- xfer-out: transferencia de zona que envía el servidor

Los archivos de anotaciones cronológicas pueden llegar a ser enormes y deben suprimirse periódicamente. Todo el contenido del archivo de anotaciones cronológicas del servidor 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 por el que se anotan cronológicamente los mensajes. A continuación figuran los niveles de gravedad que están disponibles:

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

Quedarán anotados cronológicamente 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 Crítico. 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 valores de anotaciones cronológicas

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

1. En iSeries Navigator, expanda **su servidor iSeries** → **Red** → **Servidores** → **DNS**.
2. En el panel de la derecha, pulse el botón secundario del ratón en **Nombre del servidor DNS** y seleccione **Configuración**.
3. En la ventana Configuración de DNS, pulse el botón secundario del ratón en **Servidor DNS** y seleccione **Propiedades**.
4. En la ventana 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 ventana Propiedades del servidor, seleccione la pestaña **Anotaciones** para especificar qué categorías de mensajes deben anotarse en cada canal.

Consejo sobre resolución de problemas

El valor del nivel de gravedad por omisión del canal as400_joblog está establecido en 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 arriba para acceder a la página Canales y cambie el nivel de gravedad del canal as400_joblog por el de Aviso, Notificación o Info y poder ver así más datos sobre las anotaciones cronológicas. Una vez que haya resuelto el problema, restablezca el nivel de gravedad a Error para reducir el número de mensajes de las anotaciones de trabajo.

Tareas relacionadas

"Resolución de problemas de DNS (Sistema de nombres de dominio)" en la página 35
Este tema trata sobre los valores de las anotaciones cronológicas y depuración del DNS (Sistema de nombres de dominio) que le ayudarán a resolver los problemas que puedan presentarse en el servidor DNS.

Cambiar los valores de depuración de DNS (Sistema de nombres de dominio)

La función de depuración de DNS (Sistema de nombres de dominio) 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 cronológicas 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). Se recomienda que utilice primero las anotaciones cronológicas 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 que tenga en su servidor DNS. Con un valor 1 o superior, la información de depuración se graba en el archivo NAMED.RUN, situado en la vía de acceso de iSeries: **Integrated File System/Root/QIBM/UserData/OS400/DNS/<instancia del servidor>**, donde "<instancia del servidor>" corresponde al 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 ejecutándose. Se recomienda suprimir el archivo de vez en cuando para que no ocupe mucho espacio en disco. 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 iSeries Navigator, expanda **su servidor iSeries** → **Red** → **Servidores** → **DNS**.
2. En el panel de la derecha, pulse el botón secundario del ratón en **Nombre del servidor DNS** y seleccione **Configuración**.
3. En la ventana Configuración de DNS, pulse el botón secundario del ratón en el servidor DNS 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, consulte la sección Características avanzadas de DNS.

Conceptos relacionados

"Características avanzadas de DNS (Sistema de nombres de dominio)" en la página 34
Este tema explica cómo los administradores con experiencia pueden utilizar las características avanzadas de DNS (Sistema de nombres de dominio) para gestionar más fácilmente un servidor DNS.

Tareas relacionadas

"Resolución de problemas de DNS (Sistema de nombres de dominio)" en la página 35
Este tema trata sobre los valores de las anotaciones cronológicas y depuración del DNS (Sistema de nombres de dominio) que le ayudarán a resolver los problemas que puedan presentarse en el servidor DNS.

Información relacionada para DNS (Sistema de nombres de dominio)

A continuación se listan los libros rojos IBM Redbooks (en formato PDF) y los sitios Web relacionados con el tema DNS (Sistema de nombres de dominio). Puede ver o imprimir cualquiera de los PDF.

IBM Redbooks

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

En este libro rojo se describe el soporte del servidor DNS (Sistema de nombres de dominio) y del servidor DHCP (Protocolo de configuración dinámica de sistemas principales) que se incluyen en el i5/OS. La información de este libro rojo le ayudará a instalar, adaptar, configurar y solucionar los problemas del soporte de DNS y DHCP a través de ejemplos.

Sitios Web

- *DNS and BIND*, tercera edición. Paul Albitz and Cricket Liu. Publicado por O'Reilly and Associates,Inc. Sebastopol, California, 1998. Número ISBN: 1-56592-512-2. Es la fuente de información con la máxima autoridad sobre DNS.
- El sitio Web Internet Software Consortium contiene noticias, enlaces y otros recursos para BIND.
- El sitio InterNIC mantiene un directorio con todos los registradores de nombres de dominio que ha autorizado ICANN (Internet Corporation for Assigned Names and Numbers).
- El Directorio de recursos de DNS proporciona material de referencia sobre DNS y enlaces a otros muchos recursos de DNS, incluidos foros de debate. También proporciona un listado de RFC relacionados con DNS .

Guardar archivos PDF

Para guardar un PDF en la estación de trabajo con el fin de verlo o imprimirlo:

1. Pulse el botón derecho sobre el PDF en el navegador (pulse el botón derecho del ratón sobre el enlace anterior).
2. Pulse en la opción que guarda el PDF localmente.
3. Vaya al directorio donde desea guardar el PDF.
4. Pulse en **Guardar**.

Bajar Adobe Reader

Necesita tener instalado Adobe Reader en el sistema para ver o imprimir estos PDF. Puede bajar una copia gratuita del sitio Web de Adobe (www.adobe.com/products/acrobat/readstep.html) .

Apéndice. Avisos

Esta información se ha escrito para productos y servicios ofrecidos en los EE.UU.

Es posible que en otros países IBM no ofrezca los productos, los servicios o las características que se describen en este documento. Consulte al representante de IBM local acerca de los productos y servicios disponibles actualmente en su zona. Las referencias a productos, programas o servicios IBM no pretender afirmar ni implican que únicamente puedan utilizarse dichos productos, programas o servicios IBM. En su lugar, puede utilizarse cualquier producto, programa o servicio funcionalmente equivalente que no vulnere ninguno de los derechos de propiedad intelectual de IBM. No obstante, es responsabilidad del usuario evaluar y verificar el funcionamiento de cualquier producto, programa o servicio que no sea de IBM.

IBM puede tener patentes o solicitudes de patente pendientes de aprobación que cubran los temas descritos en este documento. La entrega de este documento no le otorga ninguna licencia sobre dichas patentes. Puede enviar las consultas sobre licencias, por escrito, a la siguiente dirección:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
Estados Unidos

Para consultas sobre licencias relativas a la información de doble byte (DBCS), póngase en contacto con el departamento de propiedad intelectual de IBM en su país o envíe las consultas, por escrito, a:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokio 106-0032, Japón

El párrafo siguiente no se aplica al Reino Unido ni a ningún otro país en que dichas disposiciones entren en contradicción con las leyes locales: INTERNATIONAL BUSINESS MACHINES CORPORATION PROPORCIONA ESTA PUBLICACIÓN “TAL CUAL” SIN GARANTÍA DE NINGÚN TIPO, NI EXPLÍCITA NI IMPLÍCITA, INCLUYENDO, PERO NO LIMITÁNDOSE, A LAS GARANTÍAS IMPLÍCITAS DE NO VULNERABILIDAD, COMERCIALIZACIÓN O ADECUACIÓN A UN PROPÓSITO DETERMINADO. Algunas legislaciones no contemplan la declaración de limitación de responsabilidad, ni implícitas ni explícitas, en determinadas transacciones, por lo que cabe la posibilidad de que esta declaración no se aplique en su caso.

Esta información puede contener imprecisiones técnicas o errores tipográficos. Periódicamente se efectúan cambios en la información incluida en este documento; estos cambios se incorporarán en nuevas ediciones de la publicación. IBM puede efectuar mejoras y/o cambios en el producto(s) y/o el programa(s) descritos en esta publicación en cualquier momento y sin previo aviso.

Cualquier referencia hecha en esta información a sitios Web no de IBM se proporciona únicamente para su comodidad y no debe considerarse en modo alguno como promoción de esos sitios Web. Los materiales de estos sitios Web no forman parte de los materiales de IBM para este producto y el uso que se haga de estos sitios Web es de la entera responsabilidad del usuario.

IBM puede utilizar o distribuir la información que usted le suministre del modo que IBM considere conveniente sin incurrir por ello en ninguna obligación para con usted.

Los licenciatarios de este programa que deseen obtener información acerca del mismo con el fin de: (i) intercambiar la información entre programas creados independientemente y otros programas (incluyendo éste) y (ii) utilizar mutuamente la información que se ha intercambiado, deben ponerse en contacto con:

IBM Corporation
Software Interoperability Coordinator, Department YBWA
3605 Highway 52 N
Rochester, MN 55901
Estados Unidos

Esta información puede estar disponible, sujeta a los términos y condiciones adecuados, incluyendo en algunos casos el pago de una tarifa.

El programa bajo licencia descrito en esta información y todo el material bajo licencia a su disposición los proporciona IBM bajo los términos de los acuerdos IBM Customer Agreement, IBM International Program License Agreement, IBM License Agreement for Machine Code o de cualquier acuerdo equivalente entre nosotros.

Los datos de rendimiento contenidos en esta documentación se han determinado en un entorno controlado. Por tanto, los resultados obtenidos en otros entornos operativos pueden variar significativamente. Algunas de las mediciones pueden haberse efectuado en sistemas a nivel de desarrollo, y no existe garantía alguna de que dichas mediciones sean las mismas en sistemas disponibles a nivel general. Además, algunas mediciones pueden haberse estimado por extrapolación. Los resultados reales pueden variar. Los usuarios de este documento deben verificar los datos aplicables a su entorno específico.

La información concerniente a productos no IBM se ha obtenido de los proveedores de dichos productos, de sus anuncios publicados o de otras fuentes disponibles públicamente. IBM no ha probado estos productos y no puede confirmar la exactitud del rendimiento, de la compatibilidad ni de ninguna otra afirmación relacionada con productos no IBM. Las cuestiones relativas a las capacidades de productos no IBM deben dirigirse a los proveedores de dichos productos.

Todas las declaraciones relativas a la dirección o intención futura de IBM están sujetas a cambios o anulación sin previo aviso y representan únicamente metas y objetivos.

Esta información contiene ejemplos de datos e informes utilizados en operaciones comerciales diarias. Para ilustrarlos de la forma más completa posible, los ejemplos incluyen nombres de personas, empresas, marcas y productos. Todos estos nombres son ficticios y cualquier parecido con los nombres y direcciones utilizados por una empresa real es mera coincidencia.

LICENCIA DE COPYRIGHT:

Esta información contiene programas de aplicación de muestra en el lenguaje fuente, que ilustran técnicas de programación en varias plataformas operativas. Puede copiar, modificar y distribuir estos programas de ejemplo de cualquier forma sin pagar nada a IBM, bajo el propósito de desarrollo, uso, márketing o distribución de programas de aplicación de acuerdo con la interfaz de programación de la aplicación para la plataforma operativa para la cual se han escrito los programas de ejemplo. Estos ejemplos no se han verificado a fondo bajo todas las condiciones. IBM, por lo tanto, no puede garantizar ni dar por supuesta la fiabilidad, la posibilidad de servicio, ni el funcionamiento de estos programas.

Cada copia o cada parte de los programas de ejemplo o de los trabajos que se deriven de ellos debe incluir un aviso de copyright como se indica a continuación:

© (nombre de empresa) (año). Parte de este código se ha derivado de IBM Corp. Sample Programs. © Copyright IBM Corp. _especifique el año o los años_. Reservados todos los derechos.

Si está visualizando esta copia software de información, es posible que las fotografías y las ilustraciones en color no aparezcan.

Información de interfaces de programación

Esta publicación de DNS facilita información sobre las interfaces de programación previstas que permiten al cliente escribir programas para obtener los servicios de IBM i5/OS.

Marcas registradas

Los términos siguientes son marcas registradas de International Business Machines Corporation en los Estados Unidos y/o en otros países:

| AFS
| AS/400 e(logo)server
| eServer
| i5/OS
| IBM IBM (logotipo)
| iSeriesOS/400 Redbooks

Los demás nombres de compañías, productos y servicios pueden ser marcas registradas o de servicio de otras empresas.

Términos y condiciones

Los permisos para utilizar estas publicaciones están sujetos a los siguientes términos y condiciones.

Uso personal: puede reproducir estas publicaciones para uso personal (no comercial) siempre y cuando incluya una copia de todos los avisos de derechos de autor. No puede distribuir ni visualizar estas publicaciones ni ninguna de sus partes, como tampoco elaborar trabajos que se deriven de ellas, sin el consentimiento explícito de IBM.

Uso comercial: puede reproducir, distribuir y visualizar estas publicaciones únicamente dentro de su empresa, siempre y cuando incluya una copia de todos los avisos de derechos de autor. No puede elaborar trabajos que se deriven de estas publicaciones, ni tampoco reproducir, distribuir ni visualizar estas publicaciones ni ninguna de sus partes fuera de su empresa, sin el consentimiento explícito de IBM.

Aparte de la autorización que se concede explícitamente en este permiso, no se otorga ningún otro permiso, licencia ni derecho, ya sea explícito o implícito, sobre las publicaciones, la información, los datos, el software o cualquier otra propiedad intelectual contenida en ellas.

IBM se reserva el derecho de retirar los permisos aquí concedidos siempre que, según el parecer del fabricante, se utilicen las publicaciones en detrimento de sus intereses o cuando, también según el parecer del fabricante, no se sigan debidamente las instrucciones anteriores.

No puede bajar, exportar ni reexportar esta información si no lo hace en plena conformidad con la legislación y normativa vigente, incluidas todas las leyes y normas de exportación de Estados Unidos.

IBM NO PROPORCIONA NINGUNA GARANTÍA SOBRE EL CONTENIDO DE ESTAS PUBLICACIONES. LAS PUBLICACIONES SE PROPORCIONAN "TAL CUAL", SIN GARANTÍA DE NINGUNA CLASE, YA SEA EXPLÍCITA O IMPLÍCITA, INCLUIDAS, PERO SIN LIMITARSE A ELLAS, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN, NO VULNERACIÓN E IDONEIDAD PARA UN FIN DETERMINADO.

Impreso en España