Importante: la versión original del siguiente contenido está publicada en icann.org y fue traducida del idioma inglés al español. La versión en idioma inglés de este contenido publicada en icann.org debe considerarse como la versión oficial.

Preguntas y Respuestas Frecuentes (FAQ) del RSSAC

Esta página contiene preguntas y respuestas referidas a muchas de las consultas que se efectúan con más frecuencia sobre el RSSAC. Se actualizará conforme las respuestas cambien, o cuando las nuevas preguntas se tornen frecuentes.

Si tiene alguna pregunta que no se enumera a continuación, o desea obtener más información o alguna aclaración, puede enviar un correo directamente a ask-rssac@icann.org. Si desea hacer referencia a una pregunta contenida en estas preguntas frecuentes, por favor, incluya el número y el título de la pregunta en su correo electrónico.

Lista de Temas

1. **Cantidad de Operadores**

1.1 ¿Por qué hay 13 identificadores de servidores raíz?

En 1985 había cuatro servidores raíz. Desde 1987 a 1991 hubieron siete, y todos se ubicaban en los EE. UU. Hacia1993 existían ocho. En este punto, se halló un problema. La RFC 1035estipula que "los mensajes [DNS] transportados mediante UDP están restringidos a 512 bytes". Agregar más servidores de nombres raíz daría como resultado una respuesta inicial que excedería los 512 bytes. La RFC 1035 no brinda un fundamento que avale el límite de 512 bytes, pero también vale la pena señalar que, en ese momento, había un requisito común de que los paquetes de IP en Internet se limitaran a 576 bytes.

Los operadores de servidores raíz advirtieron que sería posible agregar más servidores de nombres si podían aprovechar la compresión de nombres en el DNS. Por lo tanto, se propuso dar nombres a los servidores raíz en la zona root-servers.net. Hacia 1995, los nueve servidores raíz existentes habían cambiado de nombre a "a.root-servers.net", "b.root-servers.net", y así sucesivamente. En 1997, se agregaron cuatro más, lo que elevaba el número total de identificadores de servidores raíz (RSI) a 13.

Hasta 1998, el Dr. Jon Postel, como administrador de la IANA, había sido el encargado de designar a los operadores de los servidores raíz. Tras su muerte en 1998, el número de operadores no ha variado, aunque un pequeño número ha cambiado de manos a lo largo de los años.

Desde 1998, el panorama ha mutado de varias maneras. Cada servidor raíz ha agregado su propia dirección IPv6, y la ICANN firmó la zona con Extensiones de Seguridad del DNS (DNSSEC). Además, el tamaño de los mensajes transportados a través de UDP se ha ampliado mediante la utilización de la extensión del protocolo de Mecanismos de Extensión para DNS (EDNS). En forma conjunta, estos cambios han logrado que el límite UDP de 512 bytes y el límite de 13 RSI sean mucho menos importantes.

En 2002, el Internet Software Consortium (ISC, ahora Internet Systems Consortium) se convirtió en el primer operador de servidor raíz en implementar IP anycast, aunque el Proyecto WIDE había experimentado con la tecnología anteriormente. Con los años, los demás operadores de servidores raíz siguieron los pasos. Anycast permite a cada operador prestar el servicio desde múltiples instancias distintas. Si bien hoy quedan 13 RSI, en realidad, hay más de 1000 instancias anycast en funcionamiento en todo el mundo.

Para comprender mejor la historia del sistema de servidores raíz (RSS), véase RSSAC023: Historia del Sistema de Servidores Raíz. Si desea conocer más sobre la evolución continua del (RSS), véase RSSAC037: Modelo de Gobernanza Propuesto para el Sistema de Servidores Raíz del DNS.

1.2 ¿Cuál era la matemática detrás del límite de 13 identificadores para los servidores raíz?

En 1997, los servidores raíz también actuaban como servidores autoritativos para las zonas .COM, .NET y .ORG, y esta funcionalidad adicional impuso una restricción importante sobre la cantidad de RSI que podrían existir. Al igual que sucedía con la consulta inicial para la zona raíz, la consulta de NS RRSET para las zonas .COM, .NET y .ORG no podía exceder el límite de 512 bytes, y dado que los mismos servidores prestaban servicio a estas zonas, se aplicaba la misma limitación para todos de ellos.

Un paquete de respuesta del DNS también contiene la pregunta completa formulada en la sección Pregunta. Una respuesta a una consulta inicial en la raíz siempre usará 5 bytes para la sección Pregunta. El QNAME ocupa 1 byte, y el QTYPE y QCLASS ocupan 2 cada uno, lo que

hace un total de 5. Sin embargo, para una consulta inicial de .COM, la sección Pregunta podría ser considerablemente más grande.

Propósito	**Bytes**
Encabezado de DNS	12
Primer registro NS	31
12 registros NS comprimidos	(12 * 15) 180
13 registros A	(13 * 16) 208
Sección Pregunta QTYPE y QCLASS	4
Sección Pregunta QNAME	?
	=
	435

Tabla 1: Explicación de los bytes utilizados en la respuesta inicial de la raíz

Con 435 bytes en uso, quedaban 77 bytes disponibles para la sección Pregunta QNAME. En ese momento se determinó que serían suficientes 64 bytes para dar lugar a la mayoría de las consultas enviadas para .COM, .NET y .ORG. Agregar otro servidor requeriría 25 bytes, y dado que 435 + 64 + 25> 512, se decidió no agregar otro servidor.

2. Anycast

2.1 ¿Por qué algunos operadores tienen muchas instancias anycast mientras que otros operadores tienen solo unas pocas?

Los operadores de servidores raíz (RSO) son organizaciones independientes con diferentes mandatos, diferentes modelos operativos y diferentes fuentes de financiación. Estas diferencias pueden afectar el número de instancias anycast, así como otras opciones operativas. Los operadores de servidores raíz tienen un alto grado de independencia en la forma en que implementan su red; véase RSSAC042: Declaración del RSSAC sobre la Independencia de los Operadores de Servidores Raíz. Todos los RSO se comprometen a prestar un servicio de raíz del DNS de alta calidad.

2.2 ¿Cómo se garantiza de que la zona raíz se replique correctamente? ¿Existe alguna posibilidad de que los archivos de la zona raíz se corrompan debido a algún ataque o malware?

La transferencia del archivo de la zona raíz desde la Entidad Encargada del Mantenimiento de la Zona Raíz(RZM) a los RSO individuales se efectúa a través de los protocolos de

transferencia de la zona del DNS (AXFR en la RFC 5936 e IXFR en la RFC 1995). Estos mensajes de transferencia de zona están protegidos por el uso de registros de recursos TSIG como se describe en la RFC 2845. Este es un protocolo confiable y no se conoce la existencia de incidentes de corrupción de datos. Además, debido a que la zona raíz está firmada, los validadores de las DNSSEC pueden detectar respuestas incorrectas o falsificadas. El RSSAC fomenta el uso de la validación con DNSSEC siempre que sea posible

2.3 ¿La cantidad de nodos anycast es ilimitada, limitada o existe un cierto número?

La operación Anycast se define y describe en la RFC 4786"Funcionamiento de los Servicios Anycast" y la RFC 7094 "Consideraciones Arquitectónicas de IP Anycast". No hay un límite inherente en el número de nodos en un servicio anycast.

2.4 Los servidores raíz replican la zona raíz autoritativa y la vuelven a publicar, luego las instancias anycast vuelven a publicar sus datos. ¿Cuál es la diferencia entre estos dos tipos de nueva publicación?

Los RSO reciben los datos de la zona autoritativa de la Entidad Encargada del Mantenimiento de la Zona Raíz (RZM). Cada RSO luego usa su propio sistema interno de distribución para entregar la zona a todos sus sitios e instancias anycast.

2.5 Hospedamos una instancia anycast de un servidor raíz en una ciudad local. Observamos que está respondiendo consultas de todo el mundo. ¿Qué se debe hacer para que solo responda consultas del área local?

Esto es realmente una cuestión de enrutamiento IP y de cómo el RSO opera su servicio anycast. Algunos RSO configuran sus enrutadores y sesiones de interconexión para que la instancia anycast solo reciba tráfico local. Otros los configuran para recibir tráfico global, y confían en que el sistema de enrutamiento elegirá la mejor ruta a través de la red. Si observa un comportamiento no deseado con un servidor alojado, el problema se debe abordar con el RSO que presta el servicio.

2.6 En 2016 se produjo un ataque importante contra Dyn. ¿Podría suceder lo mismo a todas las instancias anycast del servidor raíz?

Sí, al menos en teoría. Esa es una de las razones por las que el RSS tiene muchos operadores y muchas instancias de servidores raíz. El gran número de instancias anycast incrementa la capacidad del RSS y ciertamente ayuda en situaciones de ataque.

2.7 ¿Cómo solicito una instancia anycast de un servidor raíz para mi organización?

Comuníquese directamente con los operadores de los servidores raíz utilizando la información de contacto a continuación. Al igual que en la pregunta 3.4, también podría considerar ejecutar

una copia local de la zona raíz, como se describe en la RFC 7706, sin ser formalmente parte del sistema anycast del servidor raíz.

Cogent Communications	
Departamento de Defensa de los Estados Unidos (NIC)	
ICANN	https://www.dns.icann.org/imrs/host/
Internet Systems Consortium	https://www.isc.org/f-root/hosting-an-f-root-node/
NASA (Centro de Investigación Ames)	
Netnod	https://www.netnod.se/i-root/i.root-servers.net
RIPE NCC	https://www.ripe.net/analyse/dns/k-root/hosting-a-k-root-node
Universidad de Maryland	
Universidad del Sur de California Instituto de ciencias de la información	https://b.root-servers.org/
Ejército de los Estados Unidos (Laboratorio de Investigaciones)	
VeriSign, Inc.	https://www.verisign.com/rirs
Proyecto WIDE	

3. DNS y Redes

3.1 ¿Cómo eligen los servidores recursivos qué servidor raíz consultar y qué identificador del servidor raíz debería preferir mi servidor recursivo?

Esto se denomina “algoritmo de selección del servidor". El protocolo DNS no especifica cómo un servidor de nombres recursivo debe elegir entre un conjunto para una consulta en particular. Por lo tanto, cada proveedor de software recursivo determina su propio algoritmo de selección de servidor. Algunas implementaciones del resolutor se "bloquearán" en el servidor con menor latencia, o en uno de los servidores que tenga una latencia similar a la más rápida. Algunas implementaciones del resolutor eligen el servidor al azar en cada oportunidad y algunas distribuyen las consultas según fórmulas complejas. En un documento publicado en 2012, se describe el algoritmo de implementaciones más comunes en ese momento.

Probablemente resulte más confiable dejar que el software recursivo haga su trabajo según lo diseñado, en lugar de tratar de modificarlo para preferir o evitar servidores particulares.

3.2 Sabemos que el DNS funciona sobre UDP 53, ¿pueden explicar cuándo el DNS funciona sobre TCP 53?

Casi todos los clientes del DNS utilizan el transporte UDP por defecto para las consultas. Sin embargo, hay algunas situaciones en las que debe utilizarse TCP en reemplazo.

El uso más común de TCP ocurre cuando se trunca una respuesta UDP. Tal truncamiento sucede cuando la respuesta de un servidor es demasiado extensa para caber en un solo mensaje UDP. Esto depende del tamaño del búfer UDP anunciado por el cliente y de cualquier límite de tamaño de respuesta que el servidor pueda colocar sobre sí mismo. Cuando un cliente recibe una respuesta con el conjunto de bits truncado, el protocolo DNS dice que debe volver a intentar la consulta sobre TCP para obtener la respuesta completa.

Otro uso de TCP para DNS son las transferencias de zona. Como las zonas enteras son generalmente mucho más grandes de lo que cabría en un solo mensaje UDP, tiene sentido realizarlas a través de TCP.

El protocolo TCP también puede utilizarse cuando un servidor se encuentra bajo ataque. El servidor puede enviar a los clientes respuestas truncadas como forma de determinar si las fuentes son falsificadas o no. Los clientes que establecen conexiones TCP se pueden incluir en la lista blanca como fuentes no falsificadas. Además, la técnica conocida como límite de velocidad de respuesta (RRL) ocasionalmente enviará respuestas truncadas para que los clientes legítimos tengan la oportunidad de recibir respuestas a través de TCP, mientras que el tráfico que proviene del ataque no volverá a intentarlo.

DNS sobre TCP es obligatorio para implementar en el software del DNS. Para más información, véase la RFC 7766.

3.3 ¿Cómo puedo disminuir la latencia entre el servidor recursivo que administro y un servidor raíz?

Primero, debe analizar detalladamente si acercarse a (más) servidores raíz reporta algún beneficio concreto. Analice el tráfico que sale de su servidor de nombres recursivo en busca de consultas que se envían a los servidores de nombres raíz. Si observa más tráfico del esperado, es posible que pueda corregir sus aplicaciones o configuraciones de red para que no sea necesario que consulten la raíz con tanta frecuencia. Utilice programas como el comando "dig" para medir las latencias reales. Si al menos dos servidores raíz están dentro de los 100 milisegundos, por lo general debería ser suficiente.

Utilice herramientas como "traceroute" para explorar la ruta de red entre su servidor recursivo y los servidores raíz que utiliza su servidor de nombres recursivo. Si encuentra algo que no tiene sentido (como el enrutamiento a través de ubicaciones lejanas), consulte con su ISP para determinar si es posible ajustar el enrutamiento.

Si desea obtener más información sobre las mediciones de calidad de servicio de DNS, el proyecto Atlas de Réseaux IP Européens (RIPE) supervisa la calidad de servicio del servicio raíz con su proyecto DNSMON. La latencia de la mayoría de los servidores, medida por cientos de anclajes de RIPE Atlas, es inferior a 60 ms.

Si no hay servidores raíz que se encuentren razonablemente cerca, puede intentar identificar un punto de intercambio o centro de datos cercano donde pueda ubicarse un servidor raíz. Consulte con uno o más de los operadores de los servidores raíz para saber si estarían dispuestos a colocar un servidor allí. No obstante, tenga en cuenta que si una ubicación ya tiene un servidor raíz, los operadores por lo general no querrán ubicar otro allí. La información de contacto del operador se puede encontrar en http://www.root-servers.org, y al ubicar los botones de "Correo electrónico de contacto" en la sección Servidores raíz en la parte inferior de la página.

3.4 ¿Puede configurar un servidor raíz usted mismo descargando el archivo de la zona raíz y validando la firma usted mismo?

La RFC 7706 describe los pasos para realizar esto, además de enumerar muchas advertencias sobre posibles inconvenientes. Tenga en cuenta que se requiere la validación DNSSEC. Véase también el Proyecto LocalRoot .

3.5 ¿Cuánto tiempo permanecerá la información de caché de un servidor recursivo?

El operador de la zona asigna a cada registro DNS un valor de tiempo de vida útil (TTL). Esto determina el tiempo durante el cual un servidor de nombres recursivo u otro cliente deben almacenar en caché los datos para reutilizarlos. Después de este tiempo, se espera que el servidor de nombres recursivo se contacte nuevamente con un servidor autoritativo para obtener datos nuevos.

En el caso de la zona raíz, algunos registros se brindan con un TTL de 24 horas y otros con un TTL de 48 horas. Algunos resolutores tienen un tiempo de vida útil de caché máximo, generalmente de 24 horas.

3.6 Debido a que el almacenamiento en caché brindará información incorrecta en algún momento, ¿cómo se puede actualizar un resolutor con la información de DNS correcta?

Si sospecha que los datos en el caché de un servidor de nombres recursivo están obsoletos, es posible vaciar su caché o reiniciar el proceso del servidor.

3.7 ¿Qué son las consultas y respuestas iniciales de DNS?

Los resolutores recursivos de DNS deben preparar sus cachés con datos específicos de la zona raíz antes de comenzar a responder consultas regulares. La RFC 8109 describe qué consultas envían los resolutores recursivos y las respuestas que esperan de los servidores raíz.

4. DNSSEC

4.1 ¿Pueden las DNSSEC brindar protección contra ataques fast flux?

No realmente. Las DNSSEC están diseñadas para brindar protección contra la manipulación de datos, pero no contra los ataques fast flux.

4.2 ¿Las DNSSEC dificultan servir una copia de la zona raíz localmente?

No, servir una copia local de la zona raíz simplemente significa servir copias actualizadas de la zona raíz sin cambios. La zona raíz proviene de la Entidad encargada del mantenimiento de la Zona Raíz (RZM) con todas las firmas de DNSSEC necesarias implementadas.

Para obtener más información sobre cómo servir la zona raíz localmente, consulte la pregunta 3.4 y RFC 7706.

4.3 Al parece DNS sobre UDP tiene un límite de 512 bytes, y DNS sobre TCP tiene un límite de 4096 bytes. Si firmo mi zona, tal vez el tamaño supere la MTU. ¿Entonces es posible que un firewall lo deje sin funcionar?

El DNS sobre UDP ya no se limita a 512 bytes. Los Mecanismos de Extensión para DNS (EDNS), descritos en la RFC 2671 y posteriormente actualizados por laRFC 6891, definen cómo los clientes y servidores pueden dar soporte para mensajes de más de 512 bytes.

TCP nunca se ha limitado a 4096 bytes. Está diseñado para entregar datos de un tamaño arbitrario.

Existen algunas inquietudes justificadas sobre el tamaño de las respuestas firmadas. Cuando una respuesta DNS sobre UDP supera el tamaño de MTU de la red, se fragmentará. Esto se ha identificado como un riesgo de seguridad que podría dar lugar a un envenenamiento del caché. Algunos firewalls bloquearán estos fragmentos. Por esta razón, los resolutores recursivos modernos están diseñados para usar tamaños de búfer EDNS menores y para volver a intentar consultas con tamaños de búfer más pequeños. Cuando el tamaño del búfer se vuelve lo suficientemente pequeño, el servidor de nombres recursivo recibirá una respuesta no fragmentada o una respuesta con el conjunto de bits truncado, lo que indica que debe volver a intentarlo a través de TCP.

5. RSSAC

5.1 ¿Cuál es la relación entre el RSSAC y el RZERC? ¿Es el RZERC un subgrupo del RSSAC?

El Comité Asesor del Sistema de Servidores Raíz (RSSAC) y el Comité de Revisión de la Evolución de la Zona Raíz (RZERC) son comités independientes dentro de la ICANN, aunque cada uno cuenta con coordinadores de enlace ante el otro y las personas pueden desempeñarse en ambos comités.

La carta orgánica del RSSAC estipula que:
"... asesora a la comunidad y a la Junta Directiva de la ICANN respecto de cuestiones relativas al funcionamiento, la administración, la seguridad y la integridad del Sistema de Servidores Raíz. Para obtener más información sobre el rol del RSSAC, véase el documento RSSAC033: Declaración del RSSAC sobre la diferencia entre el RSSAC y Root-Ops.

La carta orgánica del RZERC estipula que:
"... se espera que efectúe la revisión de los cambios en la arquitectura del contenido de la Zona Raíz del DNS, los sistemas (elementos de hardware y software) utilizados en la ejecución de cambios a la Zona Raíz del DNS y los mecanismos implementados para la distribución de la Zona Raíz del DNS.

El siguiente gráfico ayuda a explicar los roles de cada grupo.
< VER GRÁFICO AQUÍ: https://www.icann.org/groups/rssac/faq>

5.2 ¿Existe un cronograma que determine cuándo se conocerá la cantidad de servidores raíz que el RSSAC desea tener? ¿Cuándo se llevará a cabo la evaluación para determinar la cantidad de letras?

El RSSAC no tiene ninguna idea preconcebida sobre el número de servidores raíz o el número de RSO que debería haber. El límite actual en la cantidad de operadores es técnico, no administrativo.

6. Grupo de Expertos del RSSAC

6.1 ¿Existe un límite en la cantidad de miembros del Grupo de Expertos del RSSAC?

No.

6.2 ¿Cuáles son los requisitos de tiempo de los miembros del Grupo de Expertos del RSSAC?

Se espera que los miembros del Grupo de Expertos del RSSAC participen en grupos de trabajo y formen parte de la lista de correo electrónico del Grupo de Expertos del RSSAC. Algunos miembros podrán dedicar más tiempo que otros, y ciertos grupos de trabajo y revisiones de

documentos requieren más tiempo que otros. Sin embargo, el RSSAC generalmente desea que los miembros dediquen, al menos, 4 horas mensuales a las actividades del Grupo de Expertos.

7. Errores Comunes

Para tener una introducción sobre cómo funciona el DNS, véase el documento El Sistema de Nombres de Dominio de Internet explicado para Quienes no son Expertos. elaborado por Daniel Karrenberg.

7.1 ¿Los servidores raíz controlan el destino del tráfico de Internet?

No, los enrutadores y el protocolo BGP determinan la ruta que toman los paquetes a través de la red en su camino desde el origen hasta el destino. El DNS proporciona un mapeo de los nombres orientados a personas a las direcciones IP, y son estas direcciones IP las que los enrutadores utilizan en última instancia para determinar el destino de los paquetes.

7.2 ¿La mayoría de las consultas al DNS son gestionadas por un servidor raíz?

No, la mayoría son gestionadas por los resolutores recursivos sin ninguna interacción con un servidor raíz a partir de los datos que ya tienen en sus cachés. Un resolutor recursivo solo interactúa con un servidor raíz si no tiene información que no haya expirado sobre dominios de alto nivel o sobre las raíces mismas en su caché. Casi todas las consultas recibidas por los servidores raíz dan como resultado una respuesta de referencia que indica al servidor de nombres recursivo dónde hacer su consulta.

7.3 ¿Alguno de los identificadores de los servidores raíz tiene un significado especial?

Ninguno de los identificadores de los servidores raíz es especial.

7.4 ¿Hay solo 13 servidores raíz?

Hay más de 1000 servidores a nivel mundial, pero solo 13 identificadores de servidores raíz (RSI), cada uno de los cuales utiliza una dirección IPv4 y una dirección IPv6 y enrutamiento anycast.

7.5 ¿Los operadores de los servidores raíz realizan operaciones de forma independiente?

Los RSO operan independientemente, pero también tienen una estrecha coordinación entre sí a través del RSSAC y otros foros. Para obtener más información, véase el documento RSSAC042: Declaración del RSSAC sobre la Independencia de los Operadores de Servidores Raíz.

7.6 ¿Los servidores raíz solo reciben la parte del TLD de la consulta al DNS?

Actualmente, los servidores raíz (y de hecho todos los servidores DNS) generalmente reciben el nombre completo de la consulta en la solicitud DNS. Sin embargo, se está realizando un nuevo esfuerzo para enviar solo la parte del TLD del nombre de dominio a los servidores raíz cuando sea necesario.

En 2016, el IETF publicó la RFC 7816 que describe cómo los servidores DNS recursivos pueden enviar solo la parte más pequeña necesaria del nombre de la consulta. Esto se llama minimización de nombre de consulta o minimización de QNAME. La minimización de QNAME funciona al hacer que los servidores DNS recursivos solo envíen las partes necesarias de un nombre de dominio a los servidores que consultan. Los servidores DNS recursivos que utilizan minimización de QNAME solo deben enviar la parte del TLD de la consulta de los servidores raíz. Esto minimiza la cantidad de información en el cable y, por lo tanto, proporciona una mayor privacidad para los usuarios que consultan el DNS. Al 2020, la minimización de QNAME es relativamente nueva y aún no se ha implementado en su totalidad.