The Internet Corporation for Assigned Names and Numbers

Resumen del Impacto de la Escalabilidad de la Zona Raíz

Fecha de Publicación: Octubre de 2010

Resumen Ejecutivo

En el mes de febrero de 2009, la Junta Directiva de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) solicitó la realización de un estudio para examinar el impacto de la inclusión de una serie de nuevas tecnologías y la posible adición de una cantidad significativa de nuevos dominios de alto nivel a la raíz del Sistema de Nombres de Dominio (DNS). Si bien para ese momento algunas de estas tecnologías ya habían tenido algún tipo de implementación, en la comunidad se plantearon algunas inquietudes respecto a que la estabilidad del Sistema de Nombres de Dominio (DNS) pudiese estar en riesgo si los cambios y adiciones no se llevasen a cabo con prudencia. Como resultado de la solicitud de la Junta Directiva de la Corporación para la Asignación de Números y Nombres en Internet (ICANN), se realizaron dos estudios, uno que se enfocó sobre el impacto de las nuevas tecnologías y adiciones de Dominios de Alto Nivel (TLDs) en el servidor raíz, el otro se realizó con una visión más amplia y teniendo en cuenta todos los procesos asociados con la gestión del sistema raíz.

Las nuevas tecnologías de interés incluyen el protocolo IPv6 (tanto en términos de direcciones IPv6 asociadas a dominios de alto nivel y servidores raíz, así como el apoyo a las consultas de IPv6 enviadas a los servidores raíz), los Nombres de Dominio Internacionalizados (IDN) y mejoras de seguridad para el Sistema de Nombres de Dominio (DNSSEC). Sin embargo, desde —e incluso en algunos casos, antes de— la resolución de la Junta Directiva de la Corporación para la Asignación de Números y Nombres en Internet (ICANN), todas estas tecnologías se han implementado o aplicado en la raíz, por lo que existe cierta evidencia empírica que puede ser utilizada para comprender su impacto.

Hasta la fecha, el despliegue de IPv6, las Extensiones de Seguridad para el Sistema de Nombres de Dominio (DNSSEC) y los Nombres de Dominio Internacionalizados (IDN) en el sistema raíz no han tenido un impacto perjudicial significativo. Si bien el despliegue de estas nuevas tecnologías puede haber causado una degradación menor del servicio debido a la falta de una infraestructura de IPv6 robusta y/o del tamaño de respuesta más amplio (debido a la adición de registros IPv6 o a la firma de las Extensiones de Seguridad para el Sistema de Nombres de Dominio —DNSSSEC— en la raíz) causando que la respuesta decayese y dando como resultado tiempos de espera y retransmisiones, ninguno de los impactos ha sido lo suficientemente significativo como para haber generado una preocupación entre las comunidades relevantes.

Con mira al futuro y asumiendo como correcta la estimación de un límite de menos de 1000 nuevos Dominios Genéricos de Alto Nivel (gTLD) al año adicionándose a la zona raíz, y suponiendo que no se alteren substancialmente otros parámetros relacionados con la gestión de la raíz del Sistema de Nombres de Dominio (DNS), parece probable que el contar con ciclos operativos de actualización normales y con la asignación de recursos será suficiente para garantizar que la escalabilidad de la raíz —tanto en términos de nuevas tecnologías como de nuevo contenido—, no tendrá ningún impacto significativo sobre la estabilidad del sistema raíz.

Sin embargo, en el entendimiento de que la gestión de la raíz del Sistema de Nombres de Dominio (DNS) involucra a varias partes y en el interés de los más altos niveles de cuidado respecto a la estabilidad de la raíz del Sistema de Nombres de Dominio (DNS), debe mejorarse el monitoreo del sistema de gestión de la raíz sobre todo en las áreas más sensibles a los cambios en índice de crecimiento o en aquellas que requieran de un tiempo significativo desde el comienzo hasta la finalización del cambio a realizar. En forma adicional, la comunicación más clara y más frecuente entre los asociados que gestionan la raíz y otras partes interesadas —incluyendo comunicaciones formales entre el personal de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) y los operadores del servidor raíz en relación a la proyección de la cantidad de solicitudes aprobadas, las tecnologías adicionales que deben ser implementadas y en qué plazos, etc.—, probablemente mejorará la confianza en que los cambios realizados en el sistema raíz no afectarán negativamente a la estabilidad de ese sistema.

Introducción

Entre 2004 y 2010, la raíz del Sistema de Nombres de Dominio (DNS) ha experimentado cambios significativos, tanto en términos de contenido así como en su infraestructura de apoyo. Desde la incorporación de los Nombres de Dominio Internacionalizados (IDN) en la raíz hasta el despliegue de IPv6 y las Extensiones de Seguridad para el Sistema de Nombres de Dominio (DNSSEC), es seguro decir que en los últimos 5 ó 6 años se produjeron mayor cantidad de cambios que los que ocurrieron desde la implementación inicial del Sistema de Nombres de Dominio (DNS). Con la inminente aceptación de las solicitudes para nuevos Dominios Genéricos de Alto Nivel (gTLD), pueden esperarse más cambios substantivos en la raíz del Sistema de Nombres de Dominio (DNS).

En consonancia con la misión de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) de "garantizar el funcionamiento estable y seguro de los sistemas de identificación única de Internet" [1] la Junta Directiva de dicha Corporación solicitó un estudio a realizarse conjuntamente por el Comité Asesor del Sistema de Servidores Raíz (RSSAC) y el Comité Asesor de Seguridad y Estabilidad (SSAC), con el apoyo de personal principal de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) para investigar el impacto de las modificaciones propuestas al sistema raíz del Sistema de Nombres de Dominio (DNS). Sin embargo, tanto antes como durante la ejecución de este estudio, muchos de los cambios en el sistema raíz de interés para la Junta Directiva ya se habían implementado sin consecuencias negativas observables.

Este documento ofrece un resumen de los cambios que han ocurrido en la raíz del Sistema de Nombres de Dominio (DNS) y ofrece un análisis de esos cambios junto con estimaciones relacionadas con el impacto previsto de los cambios futuros, incluyendo la adición de nuevos dominios de alto nivel.

Antecedentes

El 3 de febrero de 2009, la Junta Directiva de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) resolvió por unanimidad en la resolución 2009-02-03-04[2] que se realizara un conjunto entre el Comité Asesor del Sistema de Servidores Raíz (RSSAC) y el Comité Asesor de Seguridad y Estabilidad (SSAC) para analizar "*el impacto sobre la seguridad y estabilidad dentro del sistema del servidor raíz del Sistema de Nombres de Dominio (DNS) a causa de [el protocolo IPv6, los Dominios de Alto Nivel de Nombres de Dominio Internacionalizados (IDN TLDs), las Extensiones de Seguridad para el Sistema de Nombres de Dominio (DNSSEC) y los nuevos Dominios Genéricos de Alto Nivel (gTLD)] las implementaciones propuestas*". La resolución estableció que el estudio conjunto debería:

- *"Abordar las implicancias de la implementación inicial de estos cambios al producirse durante un período de tiempo comprimido.*
- *"Abordar la capacidad y escalabilidad del sistema de servidores raíz para hacer frente a una gran serie de desafíos técnicos y exigencias operacionales que pudiesen surgir como parte de la implementación de los cambios propuestos."*

[1] Del "Artículo 1, Sección 1. Misión" de los Estatutos de la Corporación para la Asignación de Números y Nombres en Internet (ICANN), véase: http://www.icann.org/en/general/bylaws.htm

[2] Véase http://www.icann.org/en/minutes/prelim-report-03feb09.htm

- *"Desarrollar los términos de referencia para el Estudio y nombrar un comité de dirección para orientar el esfuerzo antes del 28 de febrero de 2009."*
- *"Involucrar la participación directa de personal técnico principal de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) involucrados en sus implementaciones planificadas para estas actividades y proporcionar el apoyo necesario para poner en práctica los aspectos de este estudio bajo los términos y con la aprobación definitiva de los comités asesores."*
- Garantizar que "*el proceso para el establecimiento de los términos, diseño e implementación del estudio se ocupará de las cuestiones técnicas y operativas en relación a la expansión de la zona raíz del Sistema de Nombres de Dominio (DNS) que se han expresado sobre este tema."*
- Proporcionar a la Junta Directiva de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) *"hallazgos/conclusiones y recomendaciones del estudio antes del 15 de mayo de 2009*."

Como resultado de esta resolución, se llevaron a cabo dos esfuerzos, un estudio enfocado sobre el impacto de la escalabilidad de la raíz en un servidor raíz (el servidor raíz "L" operado por la Corporación para la Asignación de Números y Nombres en Internet —ICANN—) y un estudio más general con el objetivo de modelar los procesos del sistema de gestión de la raíz y de analizar los resultados de la ampliación de capacidad del sistema. Para llevar a cabo este segundo estudio se estableció un equipo de estudio dedicado conocido como el " Equipo de Estudio del Servidor Raíz " (RSST) compuesto por miembros del Comité Asesor del Sistema de Servidores Raíz (RSSAC), Comité Asesor de Seguridad y Estabilidad (SSAC) y expertos externos.

El Estudio de la Raíz "L"

El Estudio de la Raíz "L" realizado por el Centro de Investigación y Análisis de Operaciones para el Sistema de Nombres de Dominio (DNS-OARC) bajo contrato con la Corporación para la Asignación de Números y Nombres en Internet (ICANN) se enfocó específicamente sobre el impacto de diferentes combinaciones de adición del protocolo IPv6, las Extensiones de Seguridad para el Sistema de Nombres de Dominio (DNSSEC) y los nuevos dominios de alto nivel (TLDs) en una simulación de laboratorio del Servidor Raíz "L". El informe final de este estudio, titulado "Ampliación de la Zona Raíz y Análisis de Impacto", fue publicado el día 17 de septiembre de 2009 y está disponible en http://www.icann.org/en/topics/ssr/root-zone-augementation-analysis-17sep09-en.pdf.

El Estudio del Equipo de Estudio del Servidor Raíz (RSST)

El Estudio del Equipo de Estudio del Servidor Raíz (RSST), el cual utilizó al Estudio de la Raíz "L" como parte de su información de entrada, tercerizó el desarrollo de una simulación de los procesos de gestión de la raíz y llevó a cabo entrevistas con los operadores del servidor raíz, el personal de la Autoridad de Números Asignados en Internet (IANA), VeriSign, la Administración Nacional de Telecomunicaciones e Información (NTIA) y otros, fue mucho más general y tuvo como objetivo no sólo ver el impacto en los servidores raíz, sino también en los sistemas de aprovisionamiento que conducen a la zona raíz siendo propagados a los servidores raíz. El informe final de este estudio, titulado "Ampliación de la raíz" con un sub-título de "Informe sobre el impacto del Aumento de Tamaño y Volatilidad de la Zona Raíz en el Sistema Raíz del Sistema de Nombres de Dominio (DNS)" se publicó el 31 de agosto 2009 y está disponible en http://www.icann.org/en/committees/dns-root/root-scaling-study-report-31aug09-en.pdf.

Eventos de Escalabilidad de la Raíz

Con anterioridad y desde que la Junta Directiva de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) solicitó a su personal principal, al Comité Asesor de Seguridad y Estabilidad (SSAC), Comité Asesor del Sistema de Servidores Raíz (RSSAC) realizar el estudio de las implicaciones de la escalabilidad de la raíz, muchos de los temas de estudio ya habían sido implementados. En la Tabla 1 a continuación se muestra el cronograma asociado con la introducción de las nuevas tecnologías.

Fecha	Tecnología	Evento
Julio 2004	IPv6	Primeras direcciones IPv6 adicionadas a la zona raíz para dominios de alto nivel (KR y JP).
Noviembre 2005	DNSSEC	Firma del primer dominio de alto nivel (.SE).
Junio 2007	DNSSEC	Disponibilidad del banco de prueba de la raíz de IANA firmada con DNSSEC.
Agosto 2007	IDNs	Prueba de adición de dominios de alto nivel de Nombres de Dominio Internacionalizados (IDN) a la raíz.
Febrero 2008	IPv6, gTLDs	Primeras direcciones IPv6 adicionadas para servidores raíz (A, F, J, K, L y M). Un límite de un máximo de menos de 1000 nuevos Dominios Genéricos de Alto Nivel (gTLDs) por año se derivó de estimaciones del cronograma de procesamiento de gTLDs.
Enero 2010	DNSSEC	Zona Raíz Deliberadamente Invalidadora (DURZ) publicada en primer servidor raíz ("L").
Mayo 2010	IDNs, DNSSEC	Primera producción de Nombres de Dominio Internacionalizados (IDNs) agregados a la raíz (para Egipto, Arabia Saudita y Emiratos Árabes Unidos). Zona Raíz Deliberadamente Invalidadora (DURZ) desplegada en todos los 13 servidores raíz.
Junio 2010	DNSSEC	Primeros registros Firmantes de Delegación (DS) son publicados en la zona raíz (para .UK y .BR).
Julio 2010	DNSSEC	La raíz es firmada con Extensiones de Seguridad para el Sistema de Nombres de Dominio (DNSSEC) y se publica el anclaje de confianza de la raíz.

Tabla 1 – Eventos de Escalabilidad de la Raíz

Impactos

Durante el período comprendido entre julio de 2004, cuando las primeras direcciones IPv6 fueron agregadas a la zona raíz de los servidores de nombres de Dominios de Alto Nivel (TLD), hasta que la raíz fue firmada con las Extensiones de Seguridad para el Sistema de Nombres de Dominio (DNSSEC) firmada y los registros Firmantes de Delegación (DS) fueron insertados en la raíz en el mes de julio de 2010, el servicio de raíz del Sistema de Nombres de Dominio (DNS) ha continuado su funcionamiento sin haberse informado o visto públicamente una degradación visible del servicio en relación con estos eventos. En esta sección se

examina el impacto de cada uno de los varios cambios realizados en la raíz del Sistema de Nombres de Dominio (DNS).

IPv6

La inclusión del protocolo IPv6 en la raíz del Sistema de Nombres de Dominio (DNS) tiene dos componentes: la adición de los "registros de pegado" —*glue records*— IPv6 en la zona raíz para los servidores de nombres de Dominios de Alto Nivel (TLD) autorizados y la adición de los "registros de pegado" IPv6 a los servidores raíz. Cada uno de estos impactos se examinará de manera independiente.

Dominios de Alto Nivel

En julio de 2004, los dominios .JP y .KR fueron los primeros Dominios de Alto Nivel (TLDs) en contar con la adición de "registros de pegado" IPv6. Al 6 de septiembre de 2010, hay 283 "registros de pegado" IPv6 en la zona raíz, que cubren 203 Dominios de Alto Nivel (TLDs). Un impacto del aumento del uso de los "registros de pegado" IPv6 ha sido un incremento en la cantidad de resoluciones que utilizan el transporte IPv6. Al 6 de septiembre de 2010, al menos un servidor de raíz (el Servidor Raíz "L") está encontrando que aproximadamente el 1.3% de las consultas del Sistema de Nombres de Dominio (DNS) re realiza a través de IPv6[3]. Debido a la infraestructura de red menos robusta de IPv6 dentro de la Internet de hoy en día, las consultas y/o respuestas IPv6 se pueden perder con más frecuencia que con IPv4, resultando en más tiempos de espera y retransmisiones que las que hubiesen ocurrido sin el soporte de IPv6 en los Dominios de Alto Nivel (TLD). No obstante, este impacto tiene consecuencias negativas mínimas y se espera que mejore a medida que continúa el despliegue de IPv6.

Servidores Raíz

Cuando algunos de los operadores de servidores raíz agregaron las direcciones IPv6 a sus registros del servidor de nombres raíz, el tamaño de la "consulta principal" aumentó de manera significativa. Tal como se analizó en el informe elaborado conjuntamente por el Comité Asesor del Sistema de Servidores Raíz (RSSAC) y el Comité Asesor de Seguridad y Estabilidad (SSAC) codificado como SAC018 y titulado "Acomodar los Registros de Recurso de la Versión 6 de IP para la Raíz del Sistema de Nombres de Dominio", existían preocupaciones debido al hecho de que se anticipaba que la respuesta preliminar crecería a más de la

[3] Comunicación privada con los operadores del servidor raíz "L". Los demás servidores raíz deberían ver un porcentaje de consultas similar.

“clásica” respuesta no truncada máxima del Sistema de Nombres de Dominio (DNS) de 512 bytes. Si la resolución que solicita la respuesta preliminar no proporcionó un mayor tamaño de búfer para respuesta a través de la extensión EDNS0, se temía que los servidores raíz pudiesen indicar una respuesta truncada causando que la resolución solicitante vuelva a transmitir la solicitud a través del Protocolo de Control de Transmisión (TCP). Dado que las consultas del Sistema de Nombres de Dominio (DNS) basadas en el Protocolo de Control de Transmisión (TCP) son significativamente más intensivas en relación a los recursos que aquellas consultas normales basadas en el Protocolo del Nivel de Transporte (UDP), había cierta preocupación de que los servidores raíz pudiesen sobrecargarse resultando en la degradación del servicio para todos los usuarios que consultasen los servidores raíz. Además, había cierta preocupación de que la respuesta más amplia de los servidores raíz fuese bloqueada o filtrada por los cortafuegos, Traductores de Dirección de Red (NATs) y otros dispositivos "intermedios" de control que "conociesen" (incorrectamente) que una respuesta del Sistema de Nombres de Dominio (DNS) nunca podría superar los 512 bytes. En tales casos, existía el riesgo de que los solicitantes no pudiesen recibir una respuesta y, por tanto, no pudiesen obtener las direcciones de los servidores raíz.

Después de un importante estudio y pruebas significativas sobre este tema, las direcciones IPv6 se agregaron a la zona raíz en febrero de 2008. En la práctica, las implementaciones del servidor del Sistema de Nombres de Dominio (DNS) que se ejecutan en la raíz descartaron información no esencial ("Sección Adicional") en lugar de truncar las respuestas a las consultas que no especificaban un mayor tamaño de búfer para respuesta a través de la extensión EDNS0 (o no utilizaban EDNS0). Esto podría haber dado lugar a un leve aumento en la cantidad de consultas enviadas a los servidores raíz, en la medida que se requería que la resolución emita consultas adicionales para datos que previamente habían sido suministrados en la Sección Adicional; nos obstante si así hubiese sido, el incremento no ha sido notable.

Para aquellos solicitantes que suministraron un mayor tamaño de búfer para respuesta a través de la extensión EDNS0, puede haber habido un aumento en la cantidad de paquetes fragmentados que podrían haber resultado en la caída de las respuestas, ya sea debido a la pérdida de un fragmento o porque los dispositivos intermedios de control estuviesen configurados para descartar fragmentos. En forma adicional, algunas políticas de seguridad han sugerido (erróneamente) que el Sistema de Nombres de Dominio (DNS) basado en Protocolo de Control de Transmisión (TCP) debe ser bloqueado. En tales casos, una consulta principal sin la opción EDNS0 (o en la cual el almacenamiento ofrecido fuese menor que el tamaño de la respuesta) podría resultar en una

respuesta de que ha sido bloqueada. Sin embargo, en los más de dos años y medio desde que los primeros “registros de pegado” IPv6 para los servidores raíz fueron instalados en la raíz, no se han producido informes (si los hay) significativos acerca de consecuencias negativas.

En cuanto a la parte de procesamiento del sistema de gestión de la raíz, los procesos y sistema de gestión de la raíz de la Corporación para la Asignación de Números y Nombres en Internet (ICANN), así como los procesos y sistemas de VeriSign han requerido de algunas modificaciones para hacer frente a los registros de recursos IPv6 "AAAA" y para verificar la accesibilidad IPv6 en los "controles técnicos" realizados por ambas partes. Sin embargo, los impactos fueron mínimos tanto para la Corporación para la Asignación de Números y Nombres en Internet (ICANN) y como para VeriSign y los sistemas continúan hoy en día funcionando sin incidente alguno.

Nombres de Dominio Internacionalizados (IDNs)

Desde la perspectiva del Sistema de Nombres de Dominio (DNS), aparte de una longitud promedio de etiqueta un poco más larga, esencialmente los Nombres de Dominio Internacionalizados (IDN) son indistinguibles de cualquier otro nombre de dominio. Por tanto para el Sistema de Nombres de Dominio (DNS) la adición de los Nombres de Dominio Internacionalizados (IDN) a la raíz no fue diferente a la adición de cualquier otro Dominio de Alto Nivel (TLD) a la raíz. Por consiguiente, no se observó ningún impacto a nivel del Sistema de Nombres de Dominio (DNS).

Hubo, sin embargo, un cierto impacto en los procesos y sistemas de gestión de la raíz de la Corporación para la Asignación de Números y Nombres en Internet (ICANN). A fin de mostrar información útil de los Nombres de Dominio Internacionalizados (IDN), el personal de la Autoridad de Números Asignados en Internet (IANA) tuvo que revisar los procesos para solicitar etiquetas-U además de etiquetas-A y tuvo que modificar sistemas de la Autoridad de Números Asignados en Internet (IANA), tales como el servidor de Whois para que permita la visualización tanto de las etiquetas-A como de las etiquetas-U. En términos más generales, el apoyo de los Nombres de Dominio Internacionalizados (IDNs) en los sistemas secundarios o *back-end* —particularmente en la visualización de los datos de registración—, sigue siendo un tema de debate continuo en foros de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) (así como otros temas, por ejemplo relacionados a la seguridad). Se puede anticipar que en el futuro, la correcta visualización de la información de los

Nombres de Dominio Internacionalizados (IDNs) producirá un impacto no trivial entre (al menos) los registradores.

Extensiones de Seguridad para el Sistema de Nombres de Dominio (DNSSEC)

La adición de las Extensiones de Seguridad para el Sistema de Nombres de Dominio (DNSSEC) a la raíz tuvo un impacto significativo tanto en términos del tamaño de la zona de la raíz como en el tamaño de las respuestas a las consultas de la raíz, así como implicaciones que el despliegue de dichas Extensiones ha tenido para la Corporación para la Asignación de Números y Nombres en Internet (ICANN), VeriSign y la Administración Nacional de Telecomunicaciones e Información (NTIA), las partes involucradas en la gestión de la zona raíz. En cuanto todos los registros relacionados con las Extensiones de Seguridad para el Sistema de Nombres de Dominio (DNSSEC) —es decir, los registros de recursos DNSKEY, NSEC, DS y RRSIG— fueron despojados de esa zona, el tamaño de la zona resultante fue de 122.657 bytes. Sin embargo, sobre la base de datos del Estudio de la Raíz "L", se prevé que la carga de datos adicionales sobre cualquier servidor de nombres razonablemente configurado impuesta por las Extensiones de Seguridad para el Sistema de Nombres de Dominio (DNSSEC) sería intrascendente y en la práctica, esto se hizo realidad: no se informó ninguna dificultad experimentada por ninguno de los operadores de servidores raíz que cargaban y entregaban la zona firmada por las Extensiones de Seguridad para el Sistema de Nombres de Dominio (DNSSEC) durante la implementación de la Zona Raíz Deliberadamente Invalidadora (DURZ), el despliegue por etapas de las Extensiones de Seguridad para el Sistema de Nombres de Dominio (DNSSEC) en la raíz antes de la publicación del anclaje de confianza de la raíz.

El tamaño de la mayoría de las respuestas de los servidores raíz creció posiblemente en forma más significativa y en una cantidad no trivial, por ejemplo, una consulta para los servidores de nombres raíz pasó de 492 bytes a 829 bytes cuando se solicitó una respuesta firmada por las Extensiones de Seguridad para el Sistema de Nombres de Dominio (DNSSEC). A diferencia del tamaño de la zona de datos, la duplicación del tamaño de una respuesta del Sistema de Nombres de Dominio (DNS) fue preocupante debido al límite de 512 bytes previamente discutido en el contexto de IPv6. Las especificaciones de las Extensiones de Seguridad para el Sistema de Nombres de Dominio (DNSSEC) abordaron este límite requiriendo el uso de EDNS0 para señalar que la resolución fue equipada para manejar respuestas que incluyesen registros de recursos relacionados con las Extensiones de Seguridad para el Sistema de Nombres de Dominio (DNSSEC). Sin embargo, resultó que la mayoría de las resoluciones en

Internet —al menos aquellos que consultan a los servidores raíz— utilizan EDNS0 por defecto y configuran un dígito binario (bit) en las consultas del Sistema de Nombres de Dominio (DNS) (el bit "DNSSEC OK") para indicar que la resolución entiende que las respuestas incluyen registros de recursos relacionados con las Extensiones de Seguridad para el Sistema de Nombres de Dominio (DNSSEC) —independientemente de si la resolución va a hacer uso de los registros de recursos o no—. Como resultado, entre el 50% y el 80% de las consultas que llegan al servidor raíz antes de que la raíz sea firmada tenían el bit "DNSSEC OK" configurado y por lo tanto, cuando la raíz firmada era servida por todos los servidores raíz, esos servidores comenzaron a devolver inmediatamente un conjunto de al menos 50.000 registros de recursos relacionados con las Extensiones de Seguridad para el Sistema de Nombres de Dominio (DNSSEC), por segundo[4].

Antes de que la raíz sea firmada, existía una gran preocupación en relación al impacto de la devolución al cliente de respuestas más grandes firmadas con las Extensiones de Seguridad para el Sistema de Nombres de Dominio (DNSSEC) sin que las esperara. En particular, se temía que los dispositivos intermediarios pudiesen —como en el caso de IPv6 anteriormente mencionado—, descartar las respuestas de más de 512 bytes. Como resultado, la Corporación para la Asignación de Números y Nombres en Internet (ICANN), VeriSign y la Administración Nacional de Telecomunicaciones e Información (NTIA) acordaron un despliegue gradual de la firma de la zona raíz (la Zona Raíz Deliberadamente Invalidadora o "DURZ") que también incluyó la instrumentación substancial de los servidores raíz para observar cualquier cambio en los patrones de consulta. No obstante, después de implementar la firma de la zona raíz en los 13 servidores raíz en el transcurso de 6 meses, no se recibieron informes de consecuencias negativas de ninguna de las partes involucradas en la firma de la raíz.

En términos de cambios de proceso, el despliegue de las Extensiones de Seguridad para el Sistema de Nombres de Dominio (DNSSEC) en la raíz que resulta en la creación de elaborar nuevos procesos conjuntamente con nuevas instalaciones físicas que son necesarias para gestionar la clave para firma de la llave de la raíz en forma segura por parte de la Corporación para la Asignación de Números y Nombres en Internet y la clave para firma de la llave por parte de VeriSign. Los nuevos procesos también se establecieron a modo de permitir a los administradores de Dominios de Alto Nivel (TLDs) brindar información del

[4] Asumiendo la estimación de un promedio de 8000 consultas por segundo por clúster de servidor raíz sobre 13 clústeres de servidores raíz y con el bit “DNSSEC OK” configurado en la mitad de las consultas.

"Firmante de Delegación" (DS) a la Corporación para la Asignación de Números y Nombres en Internet (ICANN) en forma segura (y para permitir a dicha Corporación presentar la información de firmantes de delegación a VeriSigns para su inclusión en la zona raíz) a fin de permitir la creación de una "cadena de confianza" desde la raíz hasta las zonas menores firmadas. Al día de la fecha, estos nuevos procesos han operado sin incidente alguno.

Resumen

Resumiendo los impactos hasta la fecha de la adición del protocolo IPv6 al sistema raíz, los Dominios de Alto Nivel de Nombres de Dominio Internacionalizados (IDN TLDs) y el despliegue de las Extensiones de Seguridad para el Sistema de Nombres de Dominio (DNSSEC), no se han observado ni informado a la Corporación para la Asignación de Números y Nombres en Internet (ICANN) efectos perjudiciales significativos.

No obstante, habiendo dicho esto, un punto que se ha planteado en el contexto de los debates acerca de la escalabilidad de la raíz es la necesidad de mejorar las comunicaciones entre las partes interesadas involucradas en la gestión del sistema raíz. En algunos casos, la introducción de nuevas tecnologías podría haberse mejorado con una mayor comunicación formal de los requisitos de todas las partes que pudiesen verse afectadas, el debate de esos requisitos y efectos, planes documentados con cronogramas/plazos, etc. En este sentido, las comunicaciones, documentación y debates relacionados con el despliegue de la raíz firmada han sido sugeridas como ejemplos de pasos a seguir en la dirección correcta.

Proyecciones

El sistema raíz continúa experimentando cambios, aunque ahora más en términos de despliegue continuado de tecnologías existentes que en cambios estructurales, tal como en el caso de la introducción de nuevas tecnologías. Esta sección examina algunas proyecciones de los posibles cambios, asumiendo que los parámetros tales como los tiempos de actualización de zona, los valores de Tiempo de vida (TTL) de archivos del Sistema de Nombres de Dominio (DNS), los índices de cambios de la zona raíz y la longitud y complejidad de los procesos administrativos no varían enorme ni inesperadamente respecto de los valores históricos.

IPv6

Es altamente probable que en el futuro, más dominios de alto nivel adicionen registros de direcciones IPv6 para sus servidores de nombres. Al 6 de septiembre de 2010, la zona raíz contiene 283 “registros de pegado” IPv6 correspondientes a 203 de los 294 dominios de nivel superior que tienen al menos un registro de direcciones IPv6 para sus servidores de nombres. A medida que el protocolo IPv6 sea más ampliamente implementado, es seguro asumir que más Dominios de Alto Nivel (TLDs) añadirán soporte para IPv6, cubriendo eventualmente a todos los Dominios de Alto nivel (TLDs) y que la cantidad promedio de servidores de nombres que respalden el protocolo IPv6 para esos Dominios de Alto Nivel (TLDs) aumentará. Hasta que la infraestructura IPv6 de Internet mejore a la par de la infraestructura IPv4, los usuarios finales pueden sufrir algunas consecuencias negativas en forma de retrasos derivados de consultas que se envían a los servidores de nombres IPv6 que están en tiempo de espera.

En el caso de la raíz, el documento SAC018 establece que el tamaño de la respuesta de consulta principal, cuando todos los servidores raíz hayan implementado IPv6 debería ser de 811 bytes. Mientras que los operadores de servidores raíz que aún no han desplegado IPv6 no han proporcionado fechas en las que planean habilitar IPv6 en sus servidores raíz, todos ellos han indicado que sí tienen la intención de hacerlo. Sin embargo, dado que ya se han encontrado respuestas mayores a 512 byte, es poco probable que los + de 100 bytes adicionales en una respuesta de consulta principal tengan un impacto notable.

Extensiones de Seguridad para el Sistema de Nombres de Dominio (DNSSEC)

Al 15 de julio de 2010, la zona raíz ha sido firmada y se está distribuyendo a todas las instancias de los 13 servidores raíz. De este modo, es probable que un mayor impacto a la zona raíz a partir de las Extensiones de Seguridad para el Sistema de Nombres de Dominio (DNSSEC) se limite a la adición, modificación y eliminación de los registros de recursos Firmantes de Delegación (DS), el potencial de cambios en los algoritmos de clave, las longitudes de clave o la cantidad de llaves y los eventos traspaso de clave.

Dado que los registros de recursos Firmantes de Delegación (DS) pueden variar de tamaño sobre la base del algoritmo de cálculo utilizado, el aumento exacto en el tamaño que tendrá la adición de registros Firmantes de Delegación (DS) en el futuro es difícil de predecir con exactitud. Sin embargo, dada la estructura de los registros de recursos Firmantes de Delegación (DS), se puede argumentar que

una estimación pesimista del tamaño del registro Firmante de Delegación (DS) podría ser de 64 bytes. Al 6 de septiembre de 2010, hay 49 registros Firmantes de Delegación (DS) para 29 Dominios de Alto Nivel (TLDs) (incluyendo la prueba de 11 Dominios de Alto Nivel de Nombres de Dominio Internacionalizados —IDN TLDs— todavía en la raíz). Suponiendo, como lo hace el Estudio de la Raíz "L", que el despliegue completo de los registros Firmantes de Delegación (DS) por los Dominios de Alto Nivel (TLDs) tendrá como resultado un total de 1440 Firmantes de Delegación (DS) RRs para 1000 zonas, la cantidad total de bytes que los registros Firmantes de Delegación (DS) añadirán sería menor a 100 Kbytes. Probablemente la cantidad real de bytes sea significativamente menor ya que está ligada al número de Dominios de Alto Nivel (TLDs) y, como se explica en la sección siguiente, se espera que este número sea significativamente inferior a los 1000 nuevos Dominios de Alto Nivel (TLDs) supuestos en el Estudio de la Raíz "L".

En cuanto a los cambios en los algoritmos de clave, las longitudes de clave y la cantidad de llaves, es posible que el cambio más significativo sea el de pasar a Criptografía de Curva Elíptica, lo cual resultará en claves significativamente menores con la misma fortaleza criptográfica.

Por último, aunque es más una cuestión operativa que una cuestión de escalabilidad de la raíz, los eventos de traspaso de clave ocurren con cierta regularidad con todas las zonas firmadas con Extensiones de Seguridad para el Sistema de Nombres de Dominio (DNSSEC). En el transcurso normal de los acontecimientos, los traspasos de clave de las Claves para Firma de la Llaves (KSK) requerirán de registros Firmantes de Delegación (DS) actualizados que deben facilitarse al administrador superior de la zona. En el caso de la zona raíz, el traspaso de la Clave para Firma de la Llaves (KSK) raíz requiere de la actualización del anclaje de confianza raíz en todas las resoluciones configuradas para su validación. Se espera que los mecanismos basados en RFC 5011 permitan que gran parte del traspaso de las Claves para Firma de la Llaves (KSK) sea automatizado, aunque se puede anticipar que ocurrirá alguna interrupción cuando la Clave para Firma de la Llaves (KSK) sea cambiada y por lo tanto, el traspaso de la Clave para Firma de la Llaves (KSK) raíz debe realizarse con cierto cuidado.

Dominios de Alto Nivel

En el análisis realizado en el documento preliminar "Escenarios del Índice de Delegación de los nuevos Dominios Genéricos de Alto Nivel (gTLD)"[5], el personal

[5] Véase http://www.icann.org/en/topics/new-gtlds/anticipated-delegation-rate-model-25feb10-en.pdf

de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) estima que el índice esperado de ingreso de nuevos Dominios de Alto Nivel (TLD) a la raíz será del orden de 200 a 300, incluso con índices de solicitud más altos que los previstos. El mismo documento infiere que, independientemente de la cantidad de solicitudes, habrá un límite impuesto por el proceso en la adición de nuevos Dominios de Alto Nivel (TLDs) menor a un máximo de 1.000 nuevos Dominios Genéricos de Alto Nivel (gTLD) por año[6]. A los efectos de este análisis, se supondrá una cantidad fija de 1.000 nuevos Dominios de Alto Nivel (TLDs) adicionales por año.

Basado en el trabajo realizado en el Estudio de la Raíz "L", el tamaño anticipado de la zona raíz firmada con las Extensiones de Seguridad para el Sistema de Nombres de Dominio (DNSSEC), con IPv6, con un despliegue completo de Firmantes de Delegación (DS) y con 1.000 nuevos Dominios de Alto Nivel (TLDs) es de 624.791 bytes. Sobre la base de los aportes recibidos de los operadores de servidores raíz, es poco probable que esta cantidad de datos de la zona tensione a alguno de los servidores raíz. En forma adicional, esta zona raíz debe ser distribuida a cada instancia de los 13 servidores raíz. Por el propósito de este análisis y asumiendo que el ancho de banda mínimo efectivo (teniendo en cuenta el ruido de línea, comunicaciones interrumpidas, etc.) para la peor instancia de conexión de todos los servidores raíz es de 300 bits por segundo, el transferir toda la zona tomaría aproximadamente 4 horas y media, lo cual estaría bien dentro del plazo del actual período de regeneración de la zona raíz de 12 horas[7].

Mirando 10 años hacia el futuro y aún suponiendo un máximo de 1.000 nuevos Dominios de Alto Nivel (TLDs) por año, el Estudio de la Raíz "L" proyecta que la zona raíz habrá crecido a 7.471.784 bytes. Una vez más, sobre la base de los aportes de los operadores de servidores raíz, es poco probable que esta cantidad de datos de la zona tensione a alguno de los servidores raíz. En cuanto a ancho de banda, el mínimo de ancho de banda necesario para transferir la zona de este tamaño en un lapso de 12 horas sería de aproximadamente 1.400 bits por segundo.

Otro posible impacto futuro de la adición de nuevos Dominios de Alto Nivel (TLDs) se relaciona con la “separación” de la consulta. Es decir, que la dispersión de las consultas a través de una cantidad incrementada de Dominios de Alto Nivel

[6] 924 nuevos Dominios de Alto Nivel (TLDs) por año, para ser específicos.

[7] 300 bits por Segundo es, por supuesto un número irrealísticamente bajo; sin embargo, un número más realista permitirá que la zona sea transferida más rápidamente y por lo tanto se utiliza 300 bits por segundo en consideración del peor escenario.

(TLDs) puede tener algún impacto sobre el funcionamiento de los servidores caché individuales. Si bien no es seguro que una mayor cantidad de Dominios de Alto Nivel (TLDs) se traducirá en una mayor cantidad de consultas o que los patrones de consulta van a cambiar drásticamente, llevado al extremo, si una resolución envía una consulta para cada Dominio de Alto Nivel (TLD) en la raíz, la memoria caché de esa resolución terminará sosteniendo los registros NS para cada Dominio de Alto Nivel (TLD) (conjuntamente con los registros de pegado IPv4 e IPv6 y los registros relacionados con las Extensiones de Seguridad para el Sistema de Nombres de Dominio —DNSSEC—, si las hubiese) durante el transcurso del tiempo de vida (TTL) de los registros. En comparación con la limitada cantidad de Dominios de Alto Nivel (TLDs) de hoy en día, esto aumentaría la cantidad de memoria consumida por el servidor de nombres caché y, dependiendo de las técnicas de gestión de memoria del servidor de nombres caché, podría aumentar la probabilidad de que el servidor de nombres caché pueda quedarse sin memoria. Sin embargo, los servidores de nombre caché ya deben hacer frente a este tipo de retos de gestión de memoria, debido a que ya existen suficientes nombres de dominio que se puede consultar (en todos los niveles) como para desbordar a casi cualquier configuración de memoria si las consultas se realizaran con la suficiente rapidez (es decir, dentro del tiempo de vida de los registros de tal manera que se agreguen más nuevos registros que los que caducan). De este modo, el impacto asociado con un mayor grado de "separación" dentro de la zona raíz no se espera que cause efectos significativos en los servidores de caché.

Tal como se comentó en el informe del Equipo de Estudio del Servidor Raíz (RSST), la adición de nuevos dominios de alto nivel probablemente tendrá impactos relacionados con los procesos y sistemas secundarios o back-end que utiliza la Corporación para la Asignación de Números y Nombres en Internet (ICANN) (en el ejercicio de la función de Autoridad de Números Asignados en Internet —IANA—), VeriSign y la Administración Nacional de Telecomunicaciones e Información (NTIA). Por ejemplo, es probable que las cantidades de datos mantenidos en la base de datos utilizada para mantener la información de contacto de los administradores de Dominios de Alto Nivel (TLDs) aumenten de manera significativa y que los procesos utilizados para examinar las solicitudes en cada una de las organizaciones involucradas en la gestión de la raíz probablemente tendrá que cambiar para hacer frente al aumento de la carga asociada con las modificaciones diarias de la zona raíz. Sin embargo, todas las organizaciones implicadas en la gestión de la raíz han indicado que van a ajustar sus recursos para satisfacer la demanda. Por tanto la consideración primaria se convierte así en la detección del aumento de las cargas antes de que se

conviertan en un problema y en facilitar el ajuste de los recursos. De esta manera, dos ámbitos dentro de los cuales se requieren esfuerzos adicionales son: el monitoreo de los sistemas de gestión de la raíz en los puntos donde puedan surgir puntos de embotellamiento del sistema y la definición de umbrales que señalen las áreas de preocupación.

Resumen

Se sabe que el predecir el futuro puede resultar un tanto desafiante; sin embargo, en el caso de proyectar el impacto de la escalabilidad de la raíz, parece probable que asumiendo que los patrones históricos no cambiarán de manera imprevista, el crecimiento anticipado se encuentra dentro de la capacidad del sistema para adaptarse a dicho crecimiento.

En el caso de IPv6, cerca del 70% de los dominios de alto nivel ya han desplegado IPv6, como lo han hecho 8 de los 13 servidores raíz. Es poco probable que al pasar al 100% de ambos se encuentren consecuencias negativas (más que posibles retrasos a los usuarios finales como resultado de los tiempos de espera debido a que la infraestructura IPv6 aún no esté a la par de la infraestructura IPv4).

En cuanto a las Extensiones de Seguridad para el Sistema de Nombres de Dominio (DNSSEC), mientras que no haya adiciones de nuevos registros Firmantes de Delegación (DS) a medida que más Dominios de Alto Nivel (TLDs) firmen sus zonas, es poco probable que esto cause algún cambio notable en la raíz además del crecimiento de la zona raíz a un índice que estará (como máximo) vinculado a la cantidad de nuevos Dominios de Alto Nivel (TLDs).

Por último, la adición de nuevos Dominios de Alto Nivel (TLDs) tiene el potencial de causar el mayor impacto; no obstante ello, dado el límite previsto de menos de 1000 nuevos Dominios de Alto Nivel (TLDs) al año, es poco probable que el impacto de este crecimiento cause alguna interrupción, siempre y cuando los sistemas y procesos sean adaptados como parte de las actualizaciones normales de funcionamiento.

Conclusión

A medida que el Sistema de Nombres de Dominio (DNS) continúa creciendo y evolucionando para satisfacer nuevos requisitos, resulta de vital importancia garantizar que los cambios no impacten negativamente la estabilidad del Sistema de Dominios (DNS). Como resultado de la resolución 2009-02-03-04 de la Junta Directiva de la Corporación para la Asignación de Números y Nombres en

Internet (ICANN), se llevaron a cabo dos estudios para analizar el impacto de la adición del protocolo IPv6, las Extensiones de Seguridad para el Sistema de Nombres de Dominio (DNSSEC), los Nombres de Dominio Internacionalizados (IDNs) y los nuevos Dominios Genéricos de Alto Nivel (gTLD) a la raíz del Sistema de Nombres de Dominio (DNS). En el Estudio de la Raíz "L" se demostró que al menos un servidor raíz podía manejar fácilmente tanto el despliegue de las nuevas tecnologías como un incremento en varios órdenes de la magnitud de nuevos Dominios de Alto Nivel (TLDs) previstos como posibles para ser procesados por la Corporación para la Asignación de Números y Nombres en Internet (ICANN) en un futuro previsible. El estudio del Equipo de Estudio del Servidor Raíz (RSST) sugirió que los números absolutos no eran particularmente relevantes, sino que lo importante fue el índice de cambio y la manera en que los diversos procesos de gestión de la raíz y de los sistemas secundarios o back-end son modificados para hacer frente a los cambios.

No obstante, en el tiempo transcurrido desde que se emitió la resolución 2009-02-03-04 y hoy en día, el despliegue de nuevas tecnologías ha continuado, por lo tanto los datos empíricos pueden utilizarse para validar las observaciones de ambos estudios. El despliegue de IPv6 en la raíz, que se inició en 2004, no ha causado efectos perjudiciales significativos. La inserción en la raíz de los Nombres de Dominio Internacionalizados (IDN), de manera similar que en el 2007 no fue un evento desde la perspectiva de la estabilidad del Sistema de Nombres de Dominio (DNS) y la implementación de las Extensiones de Seguridad para el Sistema de Nombres de Dominio (DNSSEC) en la raíz, que comenzó en el mes de enero de 2010 no ha dado a ninguna consecuencia negativa observable o informada.

Con mira al futuro, es poco probable que las futuras adiciones de IPv6, Extensiones de Seguridad para el Sistema de Nombres de Dominio (DNSSEC) y Nombres de Dominio Internacionalizados (IDN) tengan un impacto negativo sobre la estabilidad del Sistema de Nombres de Dominio (DNS), si bien el traspaso de la Clave para Firma de la Llave (KSK) tendrá que ser manejado con cuidado a fin de asegurar que las resoluciones de validación cuentan con la nueva configuración de anclaje de confianza de la raíz antes de que el viejo anclaje de confianza pierda validez. El único comodín que resta está relacionado con la cantidad de nuevos Dominios de Alto Nivel (TLDs) insertados en la raíz.

Una observación clara de los estudios llevados a cabo en respuesta a la Resolución 2009-02-03-04 de la Junta Directiva de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) y de los debates relacionados con esos estudios es que debe mejorarse tanto el monitoreo de los sistemas de gestión de la raíz como las comunicaciones entre las distintas partes interesadas que participan en la gestión de la raíz. Si bien hasta la fecha las modificaciones a la raíz no han resultado en efectos negativos notables, se puede argumentar que sin un monitoreo adicional y mejora en las comunicaciones, la ampliación de la raíz podría pasar un umbral crítico sin previo aviso, resultando en problemas de escalabilidad que podrían afectar a la estabilidad del Sistema de Nombres de Dominio (DNS) en su conjunto. Bajo el supuesto de que se adicionarán menos de 1000 nuevos Dominios de Alto Nivel (TLDs) al año y que mejorará el seguimiento/monitoreo y la comunicación entre las partes interesadas, parece claro que el sistema raíz debería permanecer estable a medida que cambia para satisfacer las nuevas demandas.