ICANN79 | Foro de la comunidad – Cómo funciona - Sesión 2: operaciones de servidores raíz
Domingo, 3 de marzo de 2024 – 1:15 a 2:30 SJU

NICOLAS ANTONIELLO: Hola y bienvenidos a la sesión sobre la información del sistema de servidores raíz, mi nombre es Nicolas Antoniello y voy a ser el coordinador de la participación remota de esta sesión. Tengan en cuenta que esta sesión está siendo grabada y se rige por los estándares de comportamiento esperado de la ICANN, durante esta sesión las preguntas y comentarios se leerán si están presentados en el espacio de preguntas y respuestas correspondientes, por favor levanten la mano en Zoom si desean tomar la palabra y cuando se les autorice podrán tomar la palabra, los participantes presenciales podrán utilizar los micrófonos de la sala.

Esta sesión cuenta con interpretación simultánea en francés, árabe, español e inglés, por favor mencionen sus nombres para los registros y el idioma en el que se expresarán, si es uno distinto del inglés, y recuerden hablar a una velocidad razonable. Ahora sí voy a darle la palabra a Ken Renard.

KEN RENARD: Hola a todos, buenas tardes, somos miembros del RSSAC y vamos a contarles sobre los antecedentes técnicos y el contexto en que funciona el sistema de servidores raíz. Tenemos aquí a Jeff Osborn,

Wes y Liman de Netnod, tenemos seis de los doce operadores de sistema raíz en esta sala, así que, siéntanse libres de hacer preguntas, si quieren saber cómo funciona el sistema de servidores raíces y cuál es la función del RSSAC.

Aquí vemos la agenda y los detalles técnicos de cómo funciona el sistema de servidores raíz, vamos a hablar de Anycast, que es una capacidad importante dentro del sistema de servidores raíz, también vamos a hablar de la evolución de la gobernanza. Pasemos a la próxima diapositiva, por favor.

El identificador fundamental de internet son las direcciones de IP, esto es lo que permite a las computadoras hablar entre sí, entonces cada vez que hay una dirección numérica cuando uno se conecta a internet tiene una dirección IP, vemos aquí algunos ejemplos de direcciones de IPv4 e IPv6, probablemente ya estén familiarizados y lo hayan visto antes.

¿Por qué hacemos el DNS? En primer lugar, recordar estas direcciones de IP resulta difícil porque los números se pueden confundir y también cambian con frecuencia, vemos que las direcciones cambian si un servidor se mueve de una compañía a otra o está en una ubicación distinta y el problema más moderno es que la dirección IP se puede compartir, es decir, hay diferentes sitios webs que pueden compartir una misma dirección de IP.

Entonces el DNS nos ayuda, en realidad, a resolver estas cuestiones, nosotros como usuarios del sistema podemos tener una mejor comprensión de esta manera. El uso primario del DNS es este mapeo de un nombre, por ejemplo, www.ejemplo.org traducido a una dirección y cuando vemos el espacio de nombres vemos una jerarquía de nombres, está la raíz en la parte superior, luego los dominios de alto nivel como .UK, .ORG, .EDU y luego hay múltiples delegaciones debajo de ese nivel.

También hay otros muchos usos del DNS, por ejemplo, para encontrar servidores de correo para los correos electrónicos, hay muchas direcciones de IPv6, cuestiones o registros de seguridad, búsquedas reversas, pero generalmente se utiliza para el mapeo de todas estas direcciones de IPv4 a IPv6 y verán que debajo dice que es una base de datos dinámica, escalable, coherente y distribuida a nivel global, una de las bases de datos más grandes que existen y que funciona de una forma muy resiliente.

Vamos ahora a hablar sobre el proceso de resolución de nombres de dominios, es muy importante comprender donde está el sistema de servidores, este es un diagrama que da una presentación lógica de cómo trabaja en función al DNS, vemos un diagrama que verán en toda presentación, en todo manual técnico, pero luego les voy a contar un secreto al respecto.

Vamos a comenzar, el escenario empieza cuando tenemos un dispositivo móvil, una laptop, una heladera o algún otro dispositivo

que tiene que hacer la búsqueda de un nombre y esto se da con mucha frecuencia, entonces va a contactar lo que nosotros denominamos como un resolutor recursivo, esto es una máquina intermedia que es brindada por un ISP habitualmente o por una organización y la podrían tener en el sótano si ustedes lo desean, también puede ser un servicio de resolución abierto como el que brinda Google.

Entonces se hace la pregunta, ¿cuál es la dirección de www.ejemplo.com? El resolutor recursivo va a tomar esa pregunta y va a pasar al paso lógico, la primera parte lógica que tiene que saber es la ubicación de .COM, ¿dónde está el servidor de .COM? Y hace esa pregunta a la raíz, el siguiente paso será preguntar dónde está este servidor de .COM, ¿dónde está ejemplo.com? y luego sigue avanzando en la cadena.

El resolutor recursivo una vez que recibe las respuestas tiene memoria de todas las preguntas o consultas que se hacen, por supuesto, hay un límite en las entradas que van a permanecer en el caché. Entonces una vez que tiene todas las respuestas vuelve este resolutor al dispositivo móvil y le dice: “Bueno, puede contactar al sistema directamente”. Ahora les voy a contar un secreto, este diagrama realmente no muestra la frecuencia relativa con la cual se hacen estas preguntas a la raíz, por ejemplo, ejemplo.com.

Si pensamos en este caché, tenemos aquí el servidor raíz en la parte superior y la respuesta puede estar dando vueltas hasta por 48 horas, entonces imagínense todos los usuarios que existen y todas las

preguntas que se hacen; que pueden ser miles de millones, y solamente, en este caso, tiene que preguntar por .COM cada 48 horas porque realmente ya sabe la respuesta. Entonces la magia de todo esto y de la infraestructura del DNS son estos resolutores recursivos, que son los que hacen todo el trabajo, los que hablan con los usuarios y los que tienen la memoria, estos son sistemas autoritativos que tienen que estar allí, pero que no son tan utilizados como se cree.

Hablamos aquí un poco más del caché, cada registro del DNS tiene un TTL o tiempo de vida, este es el período durante el cual se mantiene en la memoria, es decir, es un límite antes de volver a hacer la pregunta porque hay cuestiones que pueden cambiar, entonces estos registros de DNS tienen este valor de TTL, que usualmente es de 48 horas. Los servidores raíz solo contienen información sobre cómo buscar TLD o dominios de alto nivel, es todo lo que pueden informar, no saben más que eso, no saben lo que está dentro de .COM, simplemente señala al .COM para encontrar la respuesta. Siguiente diapositiva.

Entonces hay algunas modificaciones o avances del DNS, comenzó por los 80’ y evolucionó muchísimo, una de las más importantes cuestiones son las extensiones de seguridad del DNS, las DNSSEC, son firmas criptográficas en los datos del DNS que permiten autenticar o verificar que la información no fue modificada desde la fuente original. La fuente original de estos datos no es el sistema de servidores, sino es la IANA, que es la que crea la zona raíz, los resolutores pueden utilizar métodos criptográficos para verificar la integridad de los datos que vuelven para garantizar que la respuesta que obtienen es correcta.

Entonces no hay que confiar de dónde se obtienen los datos, en realidad, hay que validar esas firmas desde el creador original del contenido. Otras mejoras tienen que ver con la privacidad, hay varias tecnologías que pueden dar especificaciones para el DNS, así que, es un tema muy importante. Hay algunas cuestiones, por ejemplo, DNS/TLD, DNS/HTTPS o minimización de nombres de consultas… Esto implica los dispositivos móviles, el resolutor recursivo y otra modificación, también es Anycast, esto permite escalar la instalación de estos servidores autoritativos de una manera mucho más sencilla.

Ahora le voy a dar la palabra a Liman para que nos cuente sobre las próximas diapositivas.

LARS-JOHAN LIMAN: Yo trabajo en Netnod en Suecia y operamos las identidades del servidor. Voy a utilizar algunos términos específicos y los vamos a ver, primero, para definir qué significan. La zona raíz es una parte del contenido de la base de datos del DNS, el DNS es una base de datos gigante distribuida en todo el internet y la zona raíz es una parte de ese rompecabeza, la zona raíz es la parte que contiene información sobre los dominios de alto nivel que existen, los gTLD y los ccTLD, la diferencia entre otros sistemas está en las políticas y procesos de registros, pero no en cuanto al sistema técnico.

Entonces la zona raíz es la lista de dominios de alto nivel y la información relacionada para poder llegar a la próxima capa en el

proceso de resolución. El sistema de servidores raíz son todos los servidores raíz, operado por todos los operadores de servidores raíz y todos los elementos que necesitamos para que esto funcione, el operador del servidor raíz es la entidad que opera una o varias de estas identidades, somos 12 los operadores, hay varios operadores aquí en la sala hoy.

Instancia Anycast del servidor raíz. Hay 13 identidades, direcciones de IPv4 y de IPv6 hacia donde se puede enviar la consulta de DNS para recibir una respuesta de la zona raíz, pero si se usa Anycast nosotros como operadores podemos operar muchas copias utilizando una misma dirección IP, en nuestro caso tenemos entre 80 y 90 equipos distribuidos por el mundo que utilizan la misma dirección IP y según donde uno esté como cliente o resolutor en la red, llegará a algunos de estos equipos y la red se asegurará de que lleguen al más cercano a ustedes.

El comité asesor del sistema de servidores raíz es un comité asesor en la ICANN, es uno de los primeros, data de 1998 y su rol es asesorar a la Junta Directiva y a la comunidad de la ICANN, incluso a la comunidad de internet, en general, sobre cuestiones relacionadas con el sistema de servidores raíz. Vamos a hablar más de esto después. Próxima diapositiva, por favor.

Entonces la zona raíz versus el sistema de servidores raíz, la zona es el punto de partida para las búsquedas cuando no tenemos nada en el caché, la zona raíz está ubicada en los servidores raíz, entonces

ponemos esta zona raíz en el servidor raíz, así que, se accede a estos datos a través del servidor raíz.

La zona raíz es gestionada por la IANA, la IANA es una afiliada de ICANN, es parte de la estructura de la ICANN, pero la IANA hace la función administrativa y la ICANN es el sistema político, desarrolla las políticas que instruyen a la IANA sobre cómo hacer su trabajo, la zona raíz es compilada y distribuida por la entidad encargada del mantenimiento de la zona raíz. La IANA indica los cambios necesarios a los operadores, estos hacen los cambios en la zona, los firman y los ponen a disposición de todos los operadores de zona raíz y a la población en general. Esto no es nada secreto.

Después nosotros descargamos esto y los ponemos en nuestros servidores de manera segura, luego los servidores raíz brindan esta información a todo el internet a través del protocolo de DNS. El sistema de servidores raíz responde con datos de la zona raíz, como dije, en este momento hay 13 direcciones IPv4 y 13 IPv6, alrededor de 1.733 instancias, hay diferentes servidores en internet que brindan este servicio.

Esto es una infraestructura totalmente técnica, la zona raíz es lo que recibimos de la entidad encargada del mantenimiento de la zona raíz, los datos que tienen los operadores son los mismos en todos los equipos y no hay ninguna forma en que el operador de la zona raíz pueda manipular el contenido de la zona raíz sin que alguien se dé cuenta, por el tema de las firmas del DNS, el operador de la zona raíz

no tiene acceso a la clave de firma que se usa para firmar el archivo de la zona, entonces si el operador hace un cambio todos los resolutores de validación del área se darían cuenta, así que, esto no es posible.

Esta es la información para llevar al encargado del mantenimiento de la zona raíz para la población o para el mundo en general, y el sistema de servidores raíz es operado por el operador correspondiente y aquí tratamos de mostrar cómo fluyen los datos por el sistema. A la izquierda tenemos una solicitud de cambio realizado por un operador, que puede ser un ccTLD o un gTLD, estamos hablando de operadores de alto nivel, se conectan de maneras levemente diferentes con la IANA, pero el proceso es muy parecido.

La función de la IANA, después de haber aprobado el cambio, es enviar la actualización al encargado del mantenimiento de la zona raíz, que sube un nuevo archivo que contiene estos datos modificados y los pone a disposición de los demás operadores de los servidores raíz de los otros 12 y después cada operador de la zona raíz tiene su propio conjunto de servidores, 80-90 en mi caso, otros operadores tienen más, otros menos, pero en mi caso nuestro rol es asegurarnos de que el archivo de zona se copie a todos estos servidores, lo tomamos del encargado de mantenimiento en la zona raíz y nos aseguramos de que nuestros servidores estén funcionando con los datos actualizados. También tenemos todas las instancias de servidores en la red que son mantenidos por los resolutores, esto es un proceso automático y nadie se da cuenta cuándo se hacen las cosas, de repente aparecen los datos actualizados y ya.

Esta es la historia del sistema de servidores raíz que ya existe desde hace 40 años, ha sido operado por voluntarios hasta ahora y pueden ver cómo creció esto a lo largo de los años y el último crecimiento se dio en el 98', entonces el sistema actual, en principio, ya tiene 25 años, no hubo mucho recambio entre los operadores y tratamos de que esto se mantenga muy estable, la estabilidad y la flexibilidad son importantes para los operadores.

Realmente preferimos utilizar alguna tecnología a veces más antigua, siempre que sea robusta y funcione, no queremos experimentar con nuestros equipos y máquinas. Entonces desde 2001 empezamos a aumentar el número de instancias y aquí realmente los números aumentaron muchísimo, prestamos atención a los cambios de tecnología, prestamos atención a DNSSEC, por supuesto, Anycast, IPv6 también lo agregamos y después hicimos debates cuidadosos, pruebas después de hacer experimentos en diferentes entornos colaborando y, finalmente, lo implementamos en nuestro sistema.

Hay un proceso de cambio, pero somos muy cuidadosos para que todo se mantenga estable, esta es una lista de los operadores de servidores raíz en este momento, versiones de IP, los nombres de los host, los servicios que se brindan y fíjense que hay una gran variedad de tipos de organizaciones, tenemos empresas comerciales, universidades, organizaciones sin fines de lucro, organismos gubernamentales… Y esto le da fortaleza al sistema, su diversidad, porque esto significa que si alguno de la organización; incluso todo un conjunto de

organizaciones, digamos, todas las empresas comerciales quiebran, seguirían funcionando aquellos sistemas manejados por un organismo gubernamental o por una ONG, etc.

Aquí vemos una imagen del sitio web donde vemos la colaboración entre los operadores del sistema de servidores raíz que cooperan mucho entre sí, abajo está la dirección de la página y pueden entrar en este mapa, acercarse y ver dónde están instaladas las instancias de servidores raíz para ver si hay alguna cercana a ustedes o en qué medida hay implementación de esto en su zona. También colaboramos mucho en cuanto a la forma de operar el servicio y desarrollamos 11 principios que usamos para operar, este es el punto de partida para el grupo de gobernanza del sistema de servidores raíz, después voy a hablar de esto, no voy a leer todos, pero voy a destacar algunos solamente.

Los principios dos y cuatro. El número dos creo que es el más importante de todos, nosotros utilizamos los mismos datos, todos acordamos que los datos que nos da la IANA a través de la entidad encargada de mantenimiento de la zona raíz son los datos que utilizamos, ningún operador de servidor raíz está en desacuerdo con esto y esto es muy importante, trabajamos con la misma información, además de la diversidad de las operaciones de los sistemas raíz; es una fortaleza del sistema, tratamos de que haya diversidad en todos los puntos, desde el hardware, los sistemas operativos, hasta el software que utiliza el DNS, los procedimientos operativos, los tipos de organizaciones, la legislación donde estamos operando donde las

empresas han sido constituidas. Tratamos de mantener la diversidad para que no haya un único punto de falla.

Otro principio muy importante es que debemos trabajar con las partes interesadas y relacionadas con ellas, no queremos estar sentados en una caja negra sin saber lo que pasa con el internet y la realidad de los usuarios, trabajamos con todos los grupos que utilizan nuestros servicios porque si no, no conoceremos sus expectativas ni sabremos cómo responder a las mismas, entonces participamos en conferencias de la IETF, en conferencias de estandarización y armonización, conferencias de la ICANN, en reuniones de RIPE, en otras reuniones que se ocupan del DNS… Los operadores de zona raíz van a estar en todas estas reuniones y lugares, nos gusta participar y relacionarnos con los demás.

Él número 10 también es una parte importante de la diversidad, los operadores de la zona raíz deben ser autónomos e independientes porque si no lo somos no podemos mantener la diversidad, es muy importante que podamos tomar nuestras decisiones sobre cómo operar el servicio. Hay una serie de mitos con respecto al sistema de servidores raíz que estamos tratando de eliminar, uno de ellos es que los servidores raíz controlan a dónde va el tráfico de internet y esto no es cierto, podemos decirles a los sistemas dónde está el punto de destino, pero no controlamos cómo el sistema se pone en contacto con el destinatario. Un GPS les puede dar la dirección en un mapa, por ejemplo, pero tiene que conducir su vehículo hasta allá.

La mayor parte de las consultas de DNS son manejadas por el servidor raíz y eso no es así, la memoria caché es muy importante, solo nos ponemos en contacto con los servidores raíz cuando es necesario. ¿La administración de la zona raíz y prestación de servicios son lo mismo? No, alguien escribe el libro, nosotros simplemente lo enviamos al que lee, no manejamos el contenido, simplemente lo desplazamos. ¿Los identificadores de los servidores raíz tienen un significado especial? No, son A, B, C, D… Son todos idénticos, ninguno tiene presidencia sobre los demás ni es más importante, ni más rápido, en realidad, todos ofrecemos exactamente los mismos datos.

¿Los operadores de servicios de los servidores raíz realizan su operación de manera independiente? No, colaboramos y cooperamos muchos, nos reunimos varias veces por año y realizamos reuniones de conexión técnica para ver que los sistemas funcionen en paralelo, pero igualmente cada uno mantiene su propia independencia a fin de poder tomar sus propias decisiones para que el servicio se brinde con diversidad. ¿Las instancias de los servidores raíz reciben toda la consulta de DNS? Esto no siempre es verdad, a veces sí, a veces no, depende de quién envíe la consulta.

Hay formas modernas en las cuales el operador del servidor raíz solo manda parte de la consulta, que debe saber el servidor raíz, para poder enviar la respuesta correcta, si el resolutor utiliza esa tecnología o no, yo no lo sé, pero hay formas actuales de minimizar las consultas que llegan al servidor raíz para que no se vea el resto de la consulta, solo la parte imprescindible.

Si ustedes operan un resolutor hay algunas cosas que pueden considerar para brindar un buen servicio a los clientes o a los usuarios finales, asegúrense de tener servidores raíz cercanos, hay algunas instancias y hay muchos lugares en el mundo donde están estos servidores y ahora por un test de la red podemos ver a qué distancia están los servidores raíz, en general, debe haber tres o cuatro cerca de dónde estamos.

Utilizamos DNS, asegúrense de que el resolutor esté validando la respuesta y utilice estas firmas porque esa es la forma de asegurarse de que estén recibiendo los datos correctos. Participen en comunidades técnicas de DNS, en el sistema se dan cambios y siempre es bueno hablar con los demás, conversar para ver qué es lo que está sucediendo o si los nuevos avances pueden ser útiles para nuestras operaciones. Si están interesados en dar el hosting de una de estas instancias de Anycast acérquense a nosotros, continuamente estamos desplegando nuevas instancias en diferentes lugares y con mucho gusto podemos conversar de esto con ustedes, todos tenemos diferentes planes de implementación, así que, acérquense.

Este es un gráfico para ilustrar la cantidad de consultas que recibimos, como pueden ver, es muy alta, tenemos varios tipos de picos en esta curva, algunos hicieron que los operadores raíz de forma colectiva se preguntaran por qué tenían estos picos de consulta y lograron de esa manera mitigar el problema, hicieron una especie de mitigación a

modo de detectives. Ahora voy a darle la palabra a Wes, quien nos va a contar sobre Anycast.

WES HARDAKER: Anycast es una tecnología que fue desarrollada con el fin de permitir que un servidor responda. Aquí tenemos unicast versus Anycast, unicast es cuando hay una dirección o una consulta, envío esa consulta y la respuesta vuelve, todos los paquetes van al mismo destino. Con Anycast cuando se envía una solicitud a internet responde el que está más cerca, entonces, por un lado, tenemos una sola fuente y, por otro lado, varias fuentes, en realidad, se habla de una cercanía lógica y no física a la red.

Uno de los principales beneficios es que, en un sistema de unicast un ataque de DDoS va a una instancia única y en un ataque de DDoS en Anycast solamente afecta a una pequeña porción de un sistema mucho mayor. Aquí vemos un diagrama que ilustra un ejemplo de unicast, aquí pueden ver la fuente en verde, a la izquierda, hay una ruta que une tres puntos hasta llegar al destino que está en azul.

El beneficio de Anycast es que hay una serie de ubicaciones, entonces se toma la ruta más corta al destino más cerca y el que está en un punto recibe el tráfico más cerca. Entonces, como mencioné anteriormente, en caso de un ataque de DDoS si el atacante está, por ejemplo, a la izquierda, puede tratar de enviar todo el tráfico que pueda al sistema, pero solamente uno de esos nodos va a ser afectado y probablemente otros nodos ni siquiera tengan en cuenta o se

enteren de que existe un ataque. La tecnología de Anycast no solamente se utiliza en el sistema de DNS, sino en muchos otros sistemas a nivel mundial y funciona muy bien.

Vamos a tomar las preguntas al final, siéntanse libres de preguntar lo que deseen, pero ahora vamos a hablar del comité asesor que tiene relación con la ICANN, este es el RSAC y el Caucus o grupo de expertos. ¿Qué es el RSSAC? Este es el comité asesor del sistema de servidor raíz, tiene como objetivo asesorar a la comunidad y a la Junta Directiva sobre cuestiones relacionadas a la operación, administración, seguridad e integridad del sistema de servidores raíz de internet, solo nos concentramos en el sistema de servidores raíz, así que, nuestro enfoque y nuestra misión es muy acotada.

¿Qué es lo que hacemos entonces? Somos una comunidad que produce asesoramiento, que da asesoramiento, como dije anteriormente, y aunque nuestro nivel de asesoramiento es menor porque nuestro enfoque es mucho más acotado. Básicamente brindamos a la Junta Directiva este asesoramiento y también documentación a otros organismos de la ICANN y organizaciones que tienen que ver con el negocio del DNS.

Los operadores de los servidores raíz están representados dentro del RSSAC, el RSSAC en sí no se encarga de operaciones técnicas, el RSSAC es solo un comité asesor y hay un grupo aparte que tiene que ver con la comunicación de los detalles técnicos. El presidente actual está a mi izquierda, Jeff Osborn y el otro vicepresidente es Ken, son de dos

organizaciones distintas y son quienes representan el liderazgo del RSSAC. Pasemos, por favor, a la próxima diapositiva.

El RSSAC se compone de representantes de cada operador de servidor raíz, yo soy el representante de la Universidad del Sur de California, también tenemos representantes, por ejemplo, de otras partes o de otras instituciones. Y también tenemos coordinadores de enlaces entrantes con otros organismos, la vasta mayoría del asesoramiento que hacemos se hace a través del grupo de expertos del RSSAC, es un grupo reducido de expertos y esto pasa a este grupo de expertos.

Son expertos, como dije, en temas técnicos que pueden contribuir a nuestro trabajo, estos miembros son confirmados por el RSSAC sobre la base de las declaraciones de interés que presenten. En cuanto a los coordinadores de enlaces tenemos una serie de coordinadores entrantes, tenemos el coordinador de enlace a la entidad de la PTI, otro al mantenedor de la zona raíz, VeriSign, tenemos otro para la Junta de arquitectura de internet, en realidad, es mi colega y luego tenemos el comité asesor de estabilidad y seguridad o SSAC.

También tenemos un coordinador de enlace ante el SSAC y también tenemos coordinadores salientes, es decir, aquellos coordinadores de enlaces que se relacionan con otros organismos, por ejemplo, un coordinador de enlace ante la Junta Directiva, un coordinador de enlace ante el comité de nominaciones, otro ante el comité permanente de clientes y otros del comité revisor de la zona raíz, pero

en el grupo de expertos del RSSAC en donde se hace nuestra mayor cantidad de trabajo.

Son expertos que debaten diferentes temas, se compone actualmente de más de 100 expertos en materia de DNS, tienen una declaración de interés pública y trabajan en aspectos particulares. La autoría de los documentos del RSSAC no es el RSSAC en sí, sino el grupo de expertos, algunos documentos son muy técnicos, otros son documentos más bien generales y hay diferentes personas o expertos que se encargan de los diferentes documentos. El propósito de este grupo de expertos es reunir a estos expertos en materia del DNS para hacer diferentes publicaciones y contribuir a la transparencia del trabajo que hacen.

Y, en realidad, el propósito de este grupo de expertos es dar un marco para llevar adelante el trabajo. Entonces queremos también extender el alcance de este grupo de expertos para que todo el mundo pueda participar. Siguiente diapositiva.

Algo que tiene que ver con la evolución o que está más allá de la evolución y del grupo de expertos tiene que ver con la evolución de la gobernanza del sistema de servidores raíz, hoy por hoy no hay un proceso para agregar o eliminar RSO, quien hacía las asignaciones falleció en un momento y no hubo ningún plan de seguimiento para poder seguir, así que, en el 2018 el RSSAC publicó el documento RSSAC037, que era un enfoque propuesto a la gobernanza del sistema de servidores raíz, lo que incluía la posibilidad de agregar o remover RSO.

La idea es que estos documentos que producimos estén bien fundamentados porque es necesario continuar, es decir, hay que seguir estos principios fundamentales, la IANA es la única fuente de datos y este es el objetivo de los documentos. La Junta Directiva aprobó la creación de un grupo de trabajo de gobernanza del sistema de servidores raíz, ese es el RSS GWG, cuyo objetivo es desarrollar un modelo de gobernanza, preservar los principios guías; esto incluye la diversidad y la interdependencia, y esto implica muchísimo trabajo porque dedicamos mucho tiempo a buscar cuál es el mejor modelo de gobernanza para el sistema.

El modelo resultante va a estar abierto a comentario público para que todo el mundo pueda participar y expresarse, y las sesiones del grupo de trabajo son abiertas a los observadores en las reuniones de la ICANN. Tenemos esta semana varias sesiones, creo que 4 o 5 horas de trabajo, así que, es mucho trabajo el que tenemos por delante. Siguiente diapositiva.

Bien, en el RSSAC037; que habla del modelo de gobernanza, lo que queremos hacer es identificar las partes interesadas, es decir, quiénes necesitan que exista el RSS y, por supuesto, la respuesta es “todo internet”, pero nosotros sí encontramos o identificamos grupos particulares, uno es la comunidad de la ICANN, la comunidad depende del sistema del servidor raíz, pero también tenemos el IETF y la IAB, ellos son los responsables de la creación y gestión del sistema de nombres de dominios y los protocolos de internet, saben cómo

funciona y la comunidad de la ICANN es la que construye todo el sistema de nombres junto con los TLD.

Y, por supuesto, también los operadores de servidores raíz que son una parte interesada en este sistema. Con respecto a la composición de este grupo de trabajo de gobernanza hay un marco en el cual opera, se compone de miembros de diferentes organizaciones, particularmente las que mencioné anteriormente y la idea es incrementar la diversidad de opiniones, entonces tenemos gente del mantenedor del sistema raíz, del IETF, de la Junta de arquitectura de internet, tenemos también miembros de cada operador de servidor raíz, también miembros de la Junta Directiva, de la IANA.

La idea es garantizar que todas las perspectivas sean tenidas en cuenta. Siguiente. Bueno, eso sería todo con respecto a nuestra presentación, con gusto ahora vamos a recibir las preguntas que tengan. Cuando salgan de esta sesión verán que hay mucha documentación publicada en línea en la página de la ICANN, hay una parte de preguntas frecuentes que ustedes pueden consultar, es un documento muy interesante que pueden leer y también allí van a recibir o tener información detallada del sistema de servidores raíz.

También tenemos una lista de correo electrónico, que es Ask-RSSAC@icann.org y si quieren más información sobre el grupo de expertos también pueden explorar la página web, la lista del grupo de expertos y cómo postularse para participar. Como dije anteriormente, hay que crear una declaración de interés, enviarlo a la membresía del

RSSAC a través de la lista de correo electrónico y luego eso llega al RSSAC. El propósito de este grupo de expertos es reunir gente con conocimientos sólidos, no es un lugar para aprender, sino más bien es un lugar para arremangarse y comenzar a trabajar.

NICOLAS ANTONIELLO: Quisiera pedirle si puede hablar un poquito más lento.

WES HARDAKER: Les pido disculpas. Bueno, podría hacerlo si tuviéramos más tiempo. ¿Hay alguna pregunta o comentario sobre lo que hemos hablado sobre el sistema de servidores raíz? ¿Algo que ustedes quieran consultar?

NICOLAS ANTONIELLO: ¿Algún comentario de la participación remota o de los participantes en la sala? Si quieren pueden utilizar el pod de preguntas y respuestas, o bien levantar la mano y yo les voy a dar la palabra para que efectúen esa pregunta.

WES HARDAKER: No hay preguntas.

NICOLAS ANTONIELLO: Yo tengo algunas preguntas que he recabado a lo largo de nuestras instancias de relacionamiento, tenemos varios operadores, así que, seguramente queremos escuchar esto.

Una de las preguntas que habitualmente recibimos es la siguiente. Usted mencionó que, cada vez que un resolutor aprende algo nuevo de un resolutor autoritativo; más allá de dar la respuesta al dispositivo que hizo la consulta, lo almacena en la memoria caché durante un tiempo y luego de ese tiempo o ese período se olvida de la información, ¿quién decide el tiempo durante el cual esa información permanece en la memoria caché?

WES HARDAKER: Bueno, es una muy buena pregunta, pero generalmente se entiende de manera errónea. Cada registro tiene un tiempo de vida, un TTL; que es un tiempo de memorizar, eso no quiere decir que se deba mantener ese tiempo, es el tiempo máximo. Si uno no tiene demasiada memoria en el dispositivo puede ser que el período sea más corto, el IETF emitió un documento que dice que, si no pueden contactar a servidor, en realidad, pueden utilizar más tiempo, entonces ya no hay más un máximo, como se había establecido oportunamente.

Cada parte del sistema del DNS acepta sus propios valores, la zona raíz es la más extensa o una de las más extensas, pero dos días es el límite, el software va a recordar las respuestas durante dos días. Otros sitios web suelen hacer cambios con mayor frecuencia y pueden, por ejemplo, establecer ese tiempo en cinco minutos o incluso en un período mucho menor. Yo trabajo en una universidad y mis colegas en la universidad estudiaron esta cuestión, a mayor tiempo quiere decir que hay una mejor protección de ataques, entonces hay que encontrar

allí el equilibrio y generalmente se recomienda que sea una hora por día, etc., pero para el sistema de servidores raíz son dos días.

NICOLAS ANTONIELLO: Y a modo de seguimiento, ¿saben si hay algún trabajo en curso que le permita a un registratario, por ejemplo, o a quien es el titular del nombre, modificar el TTL?

WES HARDAKER. Es una muy buena pregunta. Hay dos lugares donde mencionan esa información, cuando se registra el TLD o se hace otro registro, entonces se establecen algunos de los TTL, pero esto se establece en los registros de www o en otros registros.

NICOLAS ANTONIELLO: Y tengo otra pregunta totalmente diferente. Cuando se explica la forma en que el archivo de la zona raíz se transmite de la IANA; que si no entendí mal es la única que puede modificarlo y la que preparó ese archivo, se envía al encargado del mantenimiento de la zona raíz y después a los operadores de la zona raíz, que son los que tienen los servidores, y ponen eso a disposición del internet en general.

Entonces supongamos que se dé algo muy improbable, que los operadores del servidor raíz pierdan contacto técnico con la entidad encargada del mantenimiento de la zona raíz, entonces no reciben las actualizaciones. En la práctica, ¿cuánto tiempo seguiría operando el sistema de servidores raíz? ¿Cuánto tiempo van a seguir brindando

servicios los operadores de la zona raíz? Antes de que alguien diga: "Bueno, no podemos seguir de esta manera", ¿sucede?

LARS-JOHAN LIMAN: Voy a intentar contestarla. El servidor final, una de estas instancias que mencioné, seguirá operando con los mismos datos hasta que se dé cuenta de que hubo un cambio en el archivo de zona y que necesita una nueva copia, y eso puede darse de dos maneras, o porque recibe una notificación que le dice: "Mire, hay una nueva versión, venga y retírela". O tiene un cronómetro interno que dice "cada dos horas" o lo que fuera, debo hablar con el servidor central para ver si hay una nueva copia de ese archivo. Y el mismo mecanismo se utiliza en todos los pasos del transporte.

Entonces si un operador de servidor raíz tiene un punto de distribución central para todas sus instancias, para todo su equipo armada de instancias, el problema que usted describió es si esta nave madre no puede comunicarse con la entidad encargada del mantenimiento de la zona raíz, si damos un paso atrás igual todavía sigue habiendo una relación entre las instancias y la nave insignia, digamos, siguen preguntando: "¿Pasó algo nuevo?" "¿Pasó algo nuevo?" La nave insignia no sabe qué paso algo y dice: "Sí, todo funciona igual, todo está bien", y en todas las instancias en el punto final siguen operando normalmente hasta que entre otra notificación u otro cronómetro y ya sabemos que la información está desactualizada, debemos recibirla.

WES HARDAKER: Mientras busca esto quiero decirles que, algo que no explicamos muy bien es la arquitectura de la entidad encargada del mantenimiento de la zona raíz, ellos utilizan Anycast, un sistema repetitivo… Duane, ¿quiere explicar usted cómo es su infraestructura? Bueno, le doy la palabra a usted.

DUANE WESSELS: Gracias. Soy Duane Wessels, soy enlace de las entidades encargadas del mantenimiento de la zona raíz con RSSAC. Cuando VeriSign publica la zona raíz se envía cientos de instancias de Anycast, entonces la probabilidad de que esa comunicación se pierda o interrumpa es muy baja, pero si queremos imaginar lo que pasaría, si eso se diera, la respuesta sería una semana. Hay un valor en el registro llamado campo vencido y el tiempo es una semana.

Las firmas DNSSEC también juegan un rol aquí, pero nos aseguramos de que las firmas tengan más duración que el tiempo de vencimiento.

LARS-JOHAN LIMAN: Si los números son correctos. En realidad, es un procedimiento de dos pasos que duplica el tiempo, o sea que hay dos semanas, nuestra nave insignia manda un aviso a una semana y después teneos una semana más, entonces yo diría que son dos semanas.

(Perdón, hablan varias personas en forma simultánea).

Tenemos dos semanas para resolver el problema, en cuanto se declare habrá docenas de ingenieros dedicando todo su tiempo a resolver este problema y si realmente no lo pueden resolver hay otra forma de transportar los datos de la zona, pero no utilizamos internet para transferir archivos de zona, se podría subir a un pendrive, subirse a un avión y volar a Suecia y entregárselo al operador de Suecia.

Eso se podría hacer, pero también se puede mandar por submarino o por paloma mensajera, pero bueno, no hace falta usar sí o sí internet para enviar esto, pero en cuanto nos damos cuenta de que hay un problema, de que algo no funciona y nos damos cuenta rápidamente tenemos un sistema de monitoreo con todos los operadores de zona raíz y hay muchísimas personas monitoreando nuestro sistema de forma externa, así que, sabemos cuándo hay un problema; si es que se da, pero tenemos por lo menos una semana para resolver el problema.

WES HARDAKER: Pero nunca pasó desde que se creó el sistema raíz, ni una vez.

[JEFF OSBORN]: Quiero decir algo. Tengo la suerte de trabajar con la Junta Directiva y que todos sumados tienen más de 200 años de experiencia en internet, hay muchísima experiencia. Yo presenté esta pregunta, piensen si llega a fallar el sistema de servidores raíz y uno de ellos me dijo: “Ah, entiendo, en el cuarto mes de una tormenta nuclear”, y yo dije: “¿Qué?” Es muy, muy difícil pensar en que el sistema puede fallar. Bueno, dos semanas es mucho tiempo cuando todo el mundo está

tratando de resolver algo, dos semanas es mucho tiempo para encontrar una respuesta, una solución y no tendríamos las nuevas direcciones, pero es un sistema muy flexible, resiliente, de todos modos.

ORADOR NO IDENTIFICADO: Todos somos ingenieros y pensamos todo el tiempo en esto, monitoreamos todo el tiempo el sistema, estos son escenarios de desastres que venimos debatiendo hace mucho tiempo y en los que venimos pensando desde hace mucho tiempo, no necesariamente la guerra nuclear, pero esto tiene que ver con la ingeniería del sistema, el sistema incluye seguridad, estabilidad y flexibilidad, desde el principio le prestamos atención todo el tiempo. Hay una pregunta allá en el fondo.

ORADOR NO IDENTIFICADO: Hola. Considerando la cantidad de ccTLD y gTLD que hay, que no ha aumentado muchísimo en los últimos años, en su experiencia, ¿creen ustedes que los resolutores…? Los que van a los servidores raíz, cuando hay un error en el navegador o cuando se busca, por ejemplo, un TLD que no existe o los resolutores simplemente lo filtran y no los llevan a la fuente.

ORADOR NO IDENTIFICADO: Voy a contestar esta pregunta yo. Vemos muchas consultas para lo que es .PDF, entonces sí se cometen errores. Duane, ¿cuántos son? 50% de las consultas que recibimos obviamente son de sistemas quebrados o

que no funcionan, eso está allí, es un volumen enorme, pero igual sigue mostrando una pequeña curva en nuestro radar, una pequeña punta en nuestro radar, pero el sistema sigue funcionando. A veces hay algún sistema que manda "basura" en forma de consultas, pero nosotros lo reconocimos porque pasó una vez, pero no afectó para nada la capacidad del sistema.

WES HARDAKER: Además, hay varias tecnologías que mejoran las resoluciones negativas, así que, cuando se manda una consulta para algo que no existe en la raíz pasan dos cosas, no quiero hablar de la criptografía, pero el caché negativo se ha utilizado cuando muchos resolutores globales sabrán que no hay nada entre manzana y zanahoria, o sea que no existe nada que esté en el medio, así que, ni mandan esa consulta. Esto está cada vez más implementado estos días y hay varias tecnologías para mantener una copia en la zona raíz, yo tengo un proyecto al respecto que nos ayuda a configurar el resolutor local para tener una copia.

Entonces no lo pueden usar para el resto del mundo, pero sí para su propia organización y hay un RFC086 que se ocupa de este tema, que ayuda con las respuestas negativas. ¿Hay alguna pregunta en línea?

NICOLAS ANTONIELLO: Hay una pregunta hecha por [Astrid Neges], la pregunta uno sería: ¿Nos pueden dar una descripción general de los requerimientos necesarios para administrar un servidor raíz? Nos quedan 10 minutos.

LARS-JOHAN LIMAN: Para operar un servidor raíz es necesario tener mucha experiencia en el DNS, antes hablamos de números compuestos, además de 200 años de servidores de DNS aquí reunidos en esta sala, y hay que ser reconocido en la comunidad de internet, todos deben saber quiénes somos y deben saber que podemos hacer esto, la organización debe tener estabilidad financiera.

Todo esto es muy costoso, estas operaciones son muy costosas, los operadores de servidores raíz brindan estos servicios en forma gratuita a la comunidad, no es gratuito para los operadores porque cuesta mucho dinero, así que, hay que lograr una manera de cubrir estos costos y es necesario tener la experiencia y conocimientos técnicos, hay que saber cómo gestionar servidores porque el tiempo de funcionamiento no es 99,9, sino 100,00. El sistema debe funcionar todo el tiempo.

Además, también se deben tener expertos en red porque Anycast no es algo sencillo, hay muchas consideraciones en cuanto a cómo fluye el tráfico de internet, cómo se envían las respuestas, a dónde sí o a dónde no, así que, hay que tener conocimientos en redes también. Y siempre es bueno conocer a la gente que maneja el software para que los podamos llamar a media noche y decir: “Mira, hay uno de los servidores que no está funcionando bien y el software tiene un problema, por favor resuélvalo”, “sí, 15 minutos estaría bien”.

Así que, es necesario formar parte de la comunidad y también uno debe estar en condiciones de cumplir con todos estos 11 principios básicos que mencioné para poder ser neutral, imparcial frente a todos los clientes que envían las consultas, así que, una organización que quiera operar un servidor raíz necesita muchas cosas.

[JEFF OSBORN]: Además, ¿qué es necesario para operar un servidor raíz? Se está hablando en este momento sobre cómo puede crearse un nuevo operador de servidor raíz, la pregunta es, ¿hace falta realmente un nuevo operador de servidores raíz? Esto se está debatiendo en el grupo de trabajo de gobernanza para ver cuál es el número correcto de operadores, no sabemos, ¿13 está bien? ¿100 estaría bien? ¿Uno estaría bien? Entones estos aspectos habría que considerarlos, el tema de agregar o reducir el número de operadores, esto se está debatiendo y está ahora abierto a comentarios públicos.

NICOLAS ANTONIELLO: La siguiente pregunta dice: “El tiempo de propagación…” Perdón, me corrijo. Hay otra pregunta antes, “¿cuánto creen ustedes que es la latencia que se da cuando no hay un servidor raíz cerca del lugar donde uno está?”

WES HARDAKER: No es muy alto, uno no se daría cuenta. Si ustedes fueran la persona desafortunada que pide por primera vez un sitio web y nadie más cerca de ustedes lo pidió desde hace más de una hora o desde hace dos días,

por ejemplo, si ustedes son la primera persona en dos días que pide información sobre .COM bueno, llevará 15 milisegundos o 100 milisegundos en el peor de los casos, ni se darían cuenta de la demora.

[JEFF OSBORN]: Quiero decir algo, una sorpresa que encontré investigando y leyendo un informe, que ya compartí con ustedes, hay más de 10.000 consultas que tienen que ir a un servidor específico, la mayor parte de las consultas son respondidas desde la memoria caché y muchas de las demás van a otros servidores autoritativos antes de ir a los servidores raíz, es un número que me sorprendió. Y si hablamos de 15 a 100 milisegundos en una búsqueda nadie se da cuenta, yo no me daría cuenta, es algo donde no nos daríamos cuenta, 100 milisegundos es muy poco.

LARS-JOHAN LIMAN: Lo importante es la distancia entre ustedes, la laptop y el resolutor, no entre el resolutor y el servidor raíz, pero, como dije antes, estamos hablando de milisegundos.

NICOLAS ANTONIELLO: Hay otra pregunta, la voy a leer… Hay una pregunta aquí.

EUGENIO PINTO: Yo soy Eugenio Pinto del registro .PT. Mi pregunta es sobre el avance de Blockchain, ¿pueden ustedes pensar en un mundo en el cual la

información de la raíz se publique en Blockchain, en lugar de la forma actual?

WES HARDAKER: En realidad, yo he leído varios documentos sobre Blockchain, el tema con la raíz del DNS es que no importa porque está firmado, son datos firmados, si yo les doy una copia en papel bueno, funcionaría, pero el método de distribución de los datos no importa en realidad y probablemente sea un Blockchain con datos de la raíz en alguna parte porque se colocan en diferentes… Es una excelente tecnología que se utiliza para diferentes propósitos.

Ahora bien, si esto va a ir por sobre el mecanismo de distribución bueno, es algo que hay que determinar, por otro lado, todo el mundo lo usa, entonces habría que preguntarse por qué está la necesidad de estar en Blockchain, por qué se debe hacer esto, entonces es otro mecanismo de transporte. Muy buena pregunta.

NICOLAS ANTONIELLO: Hay otra pregunta, dice: "¿El tiempo de propagación utilizado por un registrador o un registro de un nombre de dominio es afectado por cuán lejos está el servidor raíz?"

LARS-JOHAN LIMAN: No porque estamos solamente hablando del tiempo de propagación de una registración de un dominio de alto nivel, así el servidor raíz podría evolucionar, pero es un proceso deliberado y lento, y es bueno

si es lento porque puede también rastrear todo lo que se está haciendo y también rastrear todo lo que se hace en esa parte.

NICOLAS ANTONIELLO: Muy Bien, no hay más preguntas en el pod de preguntas y respuestas…. Ah, ¿hay una en el pod? Una más. Voy a pedir que reformulen la pregunta porque no logré entender correctamente la pregunta, hasta el momento no está reformulada, la voy a leer de todas formas para ver si pueden comprenderla, pero dice lo siguiente: "Considerando el potencial de la inteligencia artificial para procesar eficientemente grandes volúmenes de datos, ¿sería posible explorar una colaboración entre la inteligencia artificial y los servidores raíz? Particularmente mantenida por organizaciones como, por ejemplo, la NASA, con el fin de mejorar la recolección y análisis de datos meteorológicos.

JEFF OSBORN: No.

WES HARDAKER: Gracias, Jeff. A ver, una vez más. Siempre recibimos la pregunta de por qué, yo me hago siempre esa pregunta, ¿por qué? ¿Cuál es el beneficio? La inteligencia artificial es una herramienta maravillosa, a mí me encanta, pero a menos que haya un objetivo no es una entidad de inteligencia que pueda lograr una tecnología, no está el punto de hacer invenciones todavía, no logra hacer invenciones, entonces cuando hablamos de la zona raíz la respuesta va a ser "no".

JEFF OSBORN: Bueno, disculpen, pero la respuesta para mí es no.

NICOLAS ANTONIELLO: Parece que no hay más preguntas en el pod de preguntas y respuestas, y si no hay preguntas en la audiencia quiero agradecer a todos por esta excelente presentación, ha sido un placer tenerlos aquí y poder hacerles las preguntas pertinentes, así que, muchísimas gracias a todos. Ahora vamos a detener la grabación y, nuevamente, gracias a todos, damos por finalizada la sesión.

[FIN DE LA TRANSCRIPCIÓN]