21 de octubre de 2013

Sistema de Datos de Zona Centralizado

Preguntas Frecuentes

Durante la reunión n.° 47 de la ICANN (Corporación para la Asignación de Nombres y Números en Internet) en Durban, el personal hizo una presentación sobre el Sistema de Datos de Zona Centralizado (entonces conocido como el CZDAP), la solución de la ICANN para la ampliación de la transferencia de datos de zona a medida que se añaden cientos de nuevos gTLD (Dominios Genéricos de Alto Nivel) a Internet. Durante la sesión, recibimos una buena cantidad de observaciones que no hemos podido abordar completamente por falta de tiempo. A continuación, encontrará respuestas a éstas y a una variedad de otras preguntas que hemos recibido acerca del CZDS. Puede acceder a otras preguntas y respuestas a través de las páginas de ayuda en: https://czds.icann.org/en/help

Usuario Final

Pregunta: ¿Podrá el usuario cambiar la dirección IP que utiliza para el acceso?

Respuesta: Sí, en la sección de perfil del usuario se puede identificar una o más direcciones IP a partir la cual Ud. puede acceder a los servidores de SFTP (Protocolo de Transferencia de Archivos SSH).

Pregunta: Si un usuario final puede acceder a múltiples TLD (Dominios de Alto Nivel), por ejemplo a 1400, ¿debe descargar cada archivo de datos en forma individual?

Respuesta: No, hemos creado el CZDS API que es un sistema basado en tokens de seguridad (dispositivo criptográfico/de autenticación), que permite la descarga masiva de credenciales de SFTP. El token de seguridad garantiza que el acceso pueda ser automatizado, lo cual permite a los individuos extraer nuevos datos de zona sin la necesidad de registrarse en forma manual. En los casos en que se detecta un abuso, la

caducidad del token de seguridad (establecida ya sea por el administrador del CZDS o por los usuarios del propio Operador de Registro) elimina la posibilidad de que determinada cadena de caracteres complete otras descargas hasta que se introduzca un nuevo token de seguridad válido del usuario en dicha cadena de caracteres.

Las herramientas para la descarga masiva de las credenciales SFTP ya han sido creadas. Toda la información referente a las herramientas puede encontrarse en el repositorio de código abierto: https://github.com/fourkitchens/CZDS-tools

Pregunta: Podría ser útil tener una página de descarga que muestre todos los archivos a los cuales tengo acceso en lugar de tener que acceder a cada página individual. Debería haber una página con una lista de todos los TLD a los cuales tengo acceso y la misma debería contar con algunos metadatos adjuntos. Por ejemplo: cuándo fue actualizado por última vez por parte del Registro y otras cosas que se verían en el FTP. Debería haber una cuenta de FTP donde se pudiese ver todo.

Respuesta: Por el momento esta característica no está disponible.

Pregunta: ¿Existe la posibilidad de contar con algún tipo de historial, por ejemplo, de la semana pasada o las últimas cuatro semanas?

Respuesta: El Sistema no ofrece esa funcionalidad.

Pregunta: ¿Hay alguna manera de cuestionar una denegación del Registro?

Respuesta: El Acuerdo de Registro exige al registro de gTLD ofrecer datos de zona, sin costo para el consumidor de datos. Si un usuario final considera que un registro está negando el acceso injustamente o no recibe respuesta por parte de un registro, puede presentar un reclamo ante el Departamento de Cumplimiento de la ICANN, quien se contactará con el registro e investigará.

Operadores de Registro

Pregunta: ¿Cuándo se exigirá a los Registros de nuevos gTLD que comiencen a ofrecer sus datos de zona: a la firma del contrato, al momento de la delegación técnica o aún no se ha decidido?

Respuesta: Los Registros de nuevos gTLD tienen la obligación de comenzar a brindar sus datos de zona al momento de la delegación.

Pregunta: ¿Cómo colocan los Registros sus datos de zona en el sistema CZDS: mediante carga por FTP o transferencia de la zona?

Respuesta: Existen dos opciones: el Operador de Registro bien puede mantener el control de sus datos sólo mediante la aprobación del acceso y la prestación de credenciales de acceso a los usuarios para su servidor SFTP (vía CZDS) o puede permitir que la ICANN haga transferencias de zona periódicas (AXFR) y configure los datos en su nombre, que luego estarán disponibles para que los usuarios descarguen directamente a través del sistema de CZDS.

Pregunta: Si un Operador de Registro elige brindar el acceso de zona a través de sus propios sistemas, en lugar de hacerlo a través del método de descarga directa vía el Sistema de Datos de Zona Centralizado, ¿cómo sería ese proceso?

Respuesta: El Operador de Registro debe elegir "credenciales SFTP" como su método de descarga. Cuando un usuario final haga una solicitud, el Operador de Registro aprobará la solicitud y proporcionará al usuario final su nombre de servidor SFTP y las credenciales de inicio de sesión. El usuario final debe entonces recuperar los datos en el host especificado introduciendo el nombre de usuario y la contraseña proporcionados en el CZDS. Antes de almacenar las credenciales, el sitio web del CZDS las cifrará utilizando la clave pública de cada usuario individual.

Pregunta: ¿Cómo debe un Operador de Registro entregar su archivo de zona al CZDS? ¿Se deben enviar los archivos a través de una API, sin comprimir?

Respuesta: El Operador de Registro debe proporcionar su clave TSIG y dirección del servidor al Administrador del CZDS y/o permitir transferencias (AXFR) desde la lista de direcciones IP designadas por la ICANN. La ICANN llevará a cabo la transferencia y entregará los datos en el formato especificado para su descarga directa por parte del usuario final, a través del CZDS.

Pregunta: ¿Están obligados los registros de nuevos gTLD a suministrar los datos de zona para el sistema?

Respuesta: Sí. De conformidad con la Sección 2 de la Especificación 4 del Acuerdo de Registro de gTLD, un nuevo registro de gTLD está obligado a suministrar los datos de zona a los usuarios finales que así lo soliciten. También se exige a los registros de nuevos gTLD utilizar el CZDS. Pueden hacerlo, ya sea permitiendo que la ICANN realice la transferencia de datos de zona o pueden proporcionar su nombre del servidor SFTP con credenciales para que el usuario final pueda obtener los datos fuera del sistema.

Pregunta: Como un registro futuro, ¿puedo aprobar todas las solicitudes en forma automática?

Respuesta: Puede aprobar todas las solicitudes a la vez en forma masiva mediante la selección de todas las solicitudes y haciendo clic en aprobar, pero en este momento no se puede "preaprobar" todas las solicitudes de manera predeterminada. La ICANN explorará la adición de esta característica de autoaprobación para una versión futura.

Pregunta: ¿Cómo puede un Operador de Registro saber si hay una solicitud pendiente para aprobar o denegar?

Respuesta: El Operador de Registro tiene la capacidad de activar o desactivar la característica de notificaciones por correo electrónico. De modo que podrán ser notificados cada vez que haya una nueva solicitud; pero si comienzan a obtener un alto volumen, pueden desactivar dicha opción. En este caso, tendrán que ingresar periódicamente al sistema y comprobar si hay nuevas solicitudes.

Pregunta: Si un Operador de Registro debe publicar el archivo de zona antes de firmar el Acuerdo de Registro, ¿no sería mejor utilizar "aprobar" en forma predeterminada?

Respuesta: Para ser precisos, un nuevo Operador de Registro está obligado a suministrar sus datos de zona *luego de* firmar el Acuerdo de Registro, al momento de delegación, y no *antes* de firmar el Acuerdo de Registro. Actualmente no hay disponible una característica de preaprobación automática.

Pregunta: No deseo tener que ingresar todos los días y aprobar. Sería agradable poder preaprobar o autoaprobar todo.

Respuesta: Los Operadores de Registro no están obligados a iniciar sesión y aprobar todos los días, aunque son responsables por la validación de las solicitudes de los usuarios finales. La regla de 24 horas significa que los Operadores de Registro deben cargar su zona cada 24 horas, y este proceso se puede automatizar.

Pregunta: ¿Hay alguna expectativa acerca de la rapidez con que los registros deben responder a las solicitudes? Y, ¿el departamento de Cumplimiento de ICANN lo comprobará?

Respuesta: No hay tiempo de respuesta específico obligatorio, aunque se espera que los registros respondan en un plazo razonable. El departamento de Cumplimiento Contractual de la ICANN exigirá el cumplimiento de proporcionar acceso a los datos de zona.

Pregunta: ¿Tiene el Operador de Registro que aprobar todas las solicitudes de los datos de zona? Por ejemplo, ¿puede .veryprivate, quien en realidad no está de acuerdo con el concepto de compartir estos datos por defecto, denegar todas las solicitudes?

Respuesta: El nuevo Acuerdo de Registro base de gTLD exige a los registros suministrar acceso a sus archivos de zona. Hay ciertas condiciones bajo las cuales las solicitudes pueden ser denegadas. Por favor, consulte el Acuerdo de Registro para ver las condiciones en las cuales un Operador de Registro puede denegar una solicitud de acceso a los archivos de zona.

Pregunta: Si un usuario final hace varias solicitudes de datos y el Operador de Registro ha revisado y aprobado al menos una de estas solicitudes, ¿podrá el Operador de Registro aprobar el proceso por lotes para todas las demás solicitudes de ese usuario?

Respuesta: El Operador de Registro debe aprobar cada solicitud de TLD individual presentada por parte de los usuarios. Cada aprobación es válida por al menos 90 días, o más tiempo si el Registro lo elige.

Pregunta: ¿Hay algún punitorio por *no* conceder autorizaciones para el acceso a los datos de zona?

Respuesta: Por favor refiérase a su Acuerdo de Registro para esta información.

Pregunta: Si un Operador de Registro gestiona múltiples TLD, cuántas cuentas —con conjuntos separados de credenciales de inicio de sesión— serán necesarias mantener con el fin de gestionar las solicitudes de acceso a datos de zona para todos sus TLD?

Respuesta: Hasta especificarse otra política, una cuenta en el CZDS debe representar exactamente a un individuo. Una cuenta individual puede operar múltiples TLD. El CZDS contiene una funcionalidad que permite a los usuarios del Operador de Registro y a los Súper Administradores conceder autoridad para ingresar en los términos y condiciones, en nombre de todos los TLD asociados con un Registro asignado. Los detalles específicos para cada "Súper Administrador" se basan en las decisiones comerciales de cada Registro. Por ejemplo, un Operador de Registro puede asignar uno o muchos usuarios del Operador de Registro para administrar el acceso a los datos de zona para múltiples TLD bajo su control, en función de su volumen.

Pregunta: ¿Puede haber más de un contacto del operador de registro?

Respuesta: Sí, la función del Súper Administrador permite a un Operador de Registro designar/añadir a otros usuarios del Operador del Registro para manejar su TLD. El Súper Administrador debe confirmar que todos los Operadores de Registro que designe tienen autoridad para ingresar en los términos y condiciones, en nombre del Registro.

Pregunta: Como una cartera de Registros, ¿podrá un Operador de Registro iniciar sesión y ver todo lo que está adjunto o habrá múltiples inicios de sesión?

Respuesta: Una vez que un usuario individual del Operador de Registro está asociado con un Registro, pueden ver todas las solicitudes de cualquier TLD que administren mediante un único inicio de sesión.

Pregunta: Si designo a alguien como Súper Administrador, ¿cómo puedo auditar lo que han hecho? Por ejemplo: ¿qué pasa si inicio sesión y tengo 5 registros y designo a mi administrador para tomar este rol para los 5 registros y presionan "aprobar todos" y luego dejan la empresa?

Respuesta: Si el usuario del Operador de Registro designado deja la empresa, el Súper Administrador puede deponerlo a un usuario final, en lugar de un usuario del Operador de Registro. No podrán aprobar más solicitudes, aunque todo lo que hayan aprobado en el pasado es válido hasta que los términos y condiciones expiren. Si no desea aprobar todas las solicitudes, usted puede revocar una o varias o todas las solicitudes de modo que los usuarios finales tendrían que iniciar sesión y volver a solicitar acceso.

Pregunta: ¿Hay planes para construir un entorno aislado (*sandbox*) - tanto en la versión SFTP, como en la versión de HTTP?

Respuesta: No hay planes para construir un entorno aislado. Los Registros pueden trabajar con el Administrador del CZDS para la configuración apropiada en el sistema y para comprobar sus transferencias de archivos de zona. La ICANN ayudará a asegurar que todo funciona correctamente antes de que el Operador de Registro comience a aprobar las solicitudes de los usuarios finales.

Pregunta: ¿Reemplazarán los términos y condiciones al acuerdo de acceso a archivos de zona?

Respuesta: Sí, de hecho, la redacción de los términos y condiciones fue tomada directamente a partir de los acuerdos de archivo de zona vigentes.

Pregunta: ¿Tenemos que crear nuestros propios términos y condiciones como Registros y, de ser así, podemos crear diferentes versiones para cada uno de nuestros TLD?

Respuesta: La Sección 2.1.1 de la Especificación 4 del nuevo acuerdo de registro de gTLD establece que el acuerdo de acceso a archivos de zona "será estandarizado, facilitado y administrado por un Proveedor del Sistema de Datos de Zona Centralizado."

Pregunta: Si un registro detecta un abuso por parte de un usuario, ¿cuál es el proceso de notificar a la ICANN?

Respuesta: El Operador de Registro puede revocar el acceso de un usuario por incumplimiento del acuerdo de acceso entre el usuario y el Operador de Registro. Cualquier consulta o informes sobre el CZDS debe ser enviada a CZDS@icann.org.

Seguridad

Pregunta: "¿Cómo es el cifrado de clave pública utilizado por el CZDS?" ¿Qué hace la tecla de descarga inicial? Los datos son ASCII y legibles, ¿por qué estos datos deben estar descifrados? ¿Por qué no utilizar HTTPS por ejemplo?

Respuesta: El HTTPS protege la confidencialidad de la información, en este caso las credenciales de acceso a los servidores de archivos de zona desde el servidor al cliente, es decir, entre dos partes. Sin embargo, el CZDS involucra a tres partes: el operador de registro, el usuario del archivo de zona y el operador del CZDS, quien actúa como intermediario. El uso de HTTPS únicamente protegería la información de una parte a la otra, pero no a toda la cadena de comunicación entre dos partes a través del intermediario. Mediante el uso del cifrado de clave pública podemos garantizar la privacidad del operador de registro al usuario del archivo de zona. El operador del CZDS (el intermediario) no tendrá acceso a las credenciales.

El sitio web del CZDS genera un par de claves RSA de 2048 bits (no PGP). Ambas

claves privada y pública se generan en el servidor web del CZDS. La clave privada es luego enviada a través de HTTPS para que el usuario puede descargarla, y después es destruida y nunca se escribe en el disco, la sesión del navegador o a través de ningún mecanismo que pudiese almacenar los datos. La clave pública se almacena con otros datos del perfil del usuario en el sitio web del CZDS. Este par de claves (la clave privada almacenada por cada usuario y su clave pública almacenada en el CZDS) son requeridas para descifrar las credenciales SFTP. El HTTPS no se utiliza con el fin de proteger a las credenciales de quedar expuestas a la tercera parte, el CZDS que el par de claves pública/privada.

La clave *pública* permanece en el servidor (igual que como una clave SSH pública permanece en un servidor), y mientras que no tenemos la intención de revelar esta clave públicamente, si esta clave pública se filtrase en el mundo de alguna manera, ello implicaría un evento de seguridad no crítica. Así que la almacenamos en la base de datos. Mientras tanto, después de la creación del par de claves, la clave *privada* se envía al usuario durante una operación de una sola vez (se transmite junto con la página web que contiene instrucciones para descargar la clave). El usuario debe descargar la clave privada y garantizar su seguridad. Tenemos un mensaje muy importante asesorando a los usuarios mantener la clave a salvo cuando acceden a la página que contiene la clave.

Si el usuario navega fuera de la página que contiene su clave privada sin descargarla, pierde la posibilidad efectiva de descifrar las credenciales y tendrá que generar un nuevo par de claves privada/pública, lo cual es fácil de hacer dentro de la interfaz del CZDS. En los casos en que el usuario intenta generar una nueva clave teniendo una clave pública ya almacenada en su cuenta, la interfaz emite una advertencia antes de sobrescribir su clave pública existente (para no sobrescribir accidentalmente una clave válida).

Para el descifrado, el usuario proporciona su clave *privada* a la página web que contiene las credenciales cifradas, que entonces son descifradas utilizando JavaScript, el lenguaje de programación de todos los navegadores web del lado del cliente. Durante esta operación, la clave privada NO se envía al servidor. El descifrado sucede

en la computadora de cada usuario.

Hay un token de seguridad SEPARADO (para acceso API) que es *completamente ajeno* a las claves de cifrado/descifrado. El token de seguridad API permite al usuario descargar credenciales SFTP en forma masiva, y no tiene absolutamente ningún papel en el proceso de descifrado. El token de seguridad API es una característica opcional del CZDS y algunos usuarios podrían optar por ni siquiera crear uno.

Pregunta: "Si la clave privada RSA es utilizada para descifrar las credenciales SFTP y esta clave API brinda acceso masivo a estas credenciales SFTP, ¿el sistema API elude el cifrado RSA de las credenciales o las mismas (credenciales) deben ser descifradas fuera de banda? "

No. La API no elude el descifrado. Ninguna pieza del sistema puede eludir el descifrado porque las credenciales nunca se almacenan en texto plano, y la clave privada requerida para el descifrado nunca se almacena en el servidor.

Otros

Pregunta: Si hay un cambio en los términos y condiciones, ¿qué mecanismo estará disponible para notificar al usuario final? ¿Habrá una consecuencia para el usuario final por no conocer el cambio en los términos, tal como una negación de los datos?

Respuesta: Siempre que los términos y condiciones se cambien o actualicen, el Operador de Registro podrá optar por revocar el acceso para todos sus usuarios vigentes; de modo que deban ingresar y volver a solicitar el acceso a los archivos de zona, de conformidad con los nuevos términos. De lo contrario, el usuario final continuará regido por las obligaciones de los términos y condiciones que acordó para cada TLD individual. Es importante señalar que la revocación del acceso dentro del sistema CZDS no negará automáticamente el acceso a un usuario final que está accediendo a los datos de zona a través de SFTP. El cambiar las credenciales para los usuarios que han sido revocados o que han caducado en el sistema, está bajo control

del Operador de Registro fuera del CZDS.

Pregunta: ¿Qué elementos de datos están brindando?

Respuesta: Los archivos de zona TLD contienen la lista de los nombres de dominio registrados y activos para un registro dado. También contiene otros registros del DNS (Sistema de Nombres de Dominio) utilizados por los registros, en función de los servicios de registro que ofrecen. El formato de un archivo de zona se define en el documento RFC 1035 y las Solicitudes de Comentarios (RFC) posteriores. El formato requerido de los archivos de zona distribuidos por el CZDS es en realidad un subconjunto de estas RFC, conforme lo definido por el Grupo Asesor sobre Acceso a los Archivos de Zona en la página 9 de la sección 5.1.7 de su Propuesta Estratégica e incluido en la Especificación 4 del Acuerdo de Registro.

Pregunta: ¿A las direcciones IP de quién acceden ustedes y las pasan a través del sistema del DNS? ¿Cómo se muestra y cómo lo hacen y cómo mapea?

Respuesta: La dirección IP del usuario final es proporcionada por el usuario al crear su perfil de usuario y se pasa al Operador de Registro.

Pregunta: Si un usuario descarga datos para un Registro, ¿obtiene el Registro un historial de las personas que lo usan?

Respuesta: El Operador de Registro tiene un historial de solicitudes por usuario, pero no un historial de descargas por realizadas por el usuario. Puede ser posible registrar las descargas directas en el CZDS, pero en este momento no es una función que el sistema tenga.

Pregunta: La aprobación, ¿es por descarga o por acceso para el TLD?

Respuesta: Por TLD. El acceso se concede una vez para obtener los datos de zona para el TLD, por la duración de los términos y condiciones: un mínimo de 90 días o tanto como el Registro elija. Al vencimiento de los términos y condiciones, el usuario debe solicitar el acceso nuevamente.

Pregunta: Necesitamos expertos en la materia para conseguir la automatización completa para conseguir esto a escala. ¿Qué pasa con el juego y qué frecuentemente puedo descargarlo? Sería muy bueno contar con un botón de acceso.

Respuesta: En los términos y condiciones hay un requisito que limita la cantidad de veces que un usuario final puede acceder a los archivos de zona: una vez en un periodo de 24 horas. Los archivos se cargan una vez cada 24 horas, de modo que si un usuario final llegara a descargarlos más de una vez por día, no recibiría ninguna información nueva. Además, no se permite a un usuario realizar una descarga directa en el CZDS más de tres veces por TLD cada 24 horas. Si intentan hacerlo, recibirán un mensaje de error.