Cómo OpenDNS/Umbrella resuelve los registros de recursos de caché

Contenido

Introducción

Este documento describe cómo OpenDNS/Umbrella resuelve los registros de recursos de caché.

Overview

Los resolvers OpenDNS/Umbrella utilizan un programa conocido como OpenDNSCache (ODC) para resolver consultas DNS. ODC almacena en caché los datos que recibe para devolver los resultados a los clientes de forma más rápida y eficaz. Este artículo se centra en cómo se produce el almacenamiento en caché y cuándo se utiliza.

Este artículo está dirigido a los usuarios que desean obtener más información sobre los aspectos específicos del almacenamiento en caché de ODC (normalmente administradores de dominio y servidores de nombres) o para los casos en los que la resolución de DNS podría no funcionar como se esperaba.

¿Qué datos se almacenan en caché?

Según RFC 2181 (https://datatracker.ietf.org/doc/html/rfc2181), las respuestas se pueden devolver en una respuesta o almacenarse en una caché en función de la fiabilidad de los datos. RFC define 7 niveles de confianza en la sección 5.4.1:

1. Datos de un archivo de zona principal, que no sean datos de pegado.
    - Esto sólo se aplica a los servidores de nombres autorizados, no a los resolvers OpenDNS
2. Datos de una transferencia de zona, que no sean pegamento.
    - Esto sólo se aplica a los servidores de nombres autorizados, no a los resolvers OpenDNS
3. Los datos autorizados incluidos en la sección de respuesta de una respuesta autorizada.
    - Esto se aplica a OpenDNSCache
4. Datos de la sección de autoridad de una respuesta autorizada.
    - Esto se aplica a OpenDNSCache
5. Pegar desde una zona principal o pegar desde una transferencia de zona.

    - Esto sólo se aplica a los servidores de nombres autorizados, no a los resolvers OpenDNS
6. i) Datos de la sección de respuestas de una respuesta no autoritativa, y ii) datos no autoritativos de la sección de respuestas autorizadas.
    - i) es un ejemplo de lo que nuestros resolvers devuelven. Es decir, datos no autorizados.
    - Para ii), tenga en cuenta que la sección de respuesta de una respuesta autorizada normalmente contiene sólo datos autorizados. Sin embargo, cuando el nombre buscado es un alias (véase la sección 10.1.1), sólo el registro que describe ese alias tiene necesariamente autoridad. Los clientes pueden suponer que otros registros deben proceder de la caché del servidor. Cuando se requieren respuestas autorizadas, el cliente puede realizar una nueva consulta, utilizando el nombre canónico asociado con el alias.
7. i) Información adicional de una respuesta autorizada; ii) Datos de la sección de autoridad de una respuesta no autorizada; iii) Información adicional procedente de respuestas no autorizadas.
    - Todo esto se aplica a OpenDNSCache
    - Los registros recibidos de cualquiera de estos orígenes no deben almacenarse en caché para devolver los resultados a las consultas.

OpenDNSCache almacena en caché los datos de las respuestas con los niveles de confianza 3, 4 y 6. Si recibimos datos nuevos que tienen un nivel de confianza mejor o igual, reemplazamos la entrada de caché anterior.

La excepción aquí es para los registros NS, para los cuales solo reemplazamos los datos con un mejor nivel de confianza.

¿Cómo se agregan y eliminan datos de la caché?

Los datos caducados no se eliminan de la caché. Esta es la base de la función SmartCache, por la cual devolvemos los registros de recursos (RR) caducados de la memoria caché si no podemos ponernos en contacto con las autoridades por algún motivo.

En su lugar, la memoria caché de cada resolución tiene un tamaño fijo y, cuando se agrega un nuevo RR a la memoria caché, se quita el RR más antiguo. Esto se puede visualizar como una cola donde las nuevas entradas se agregan a la cola, desplazando las entradas antiguas de la cola (para los informáticos, esto se implementa realmente como una lista circular doblemente vinculada).

Tenga en cuenta que, como se ha descrito anteriormente, una respuesta DNS puede contener varios RR que tienen niveles de confianza diferentes, no todos los cuales eran los datos solicitados originalmente. Por lo tanto, después de recibir una respuesta, es posible que tengamos varios RR para agregar a la memoria caché.

Como se indicó anteriormente, tenga en cuenta que los registros NS están exentos de este comportamiento, ya que solo reemplazamos las entradas para los registros NS en la caché si el nivel de confianza de los datos es superior a la entrada existente. Esto se hace para garantizar

que podamos detectar cambios en las autoridades en el pegamento de los padres si las autoridades anteriores siguen respondiendo y regresando como la autoridad.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).