Comment OpenDNS/Umbrella résout les enregistrements de ressources du cache

Table des matières

[Introduction](#)

[Aperçu](#)

[Quelles données sont mises en cache ?](#)

[Comment les données sont-elles ajoutées et supprimées du cache ?](#)

Introduction

Ce document décrit comment OpenDNS/Umbrella résout les enregistrements de ressources de cache.

Aperçu

Les résolveurs OpenDNS/Umbrella utilisent un programme appelé OpenDNSCache (ODC) pour résoudre les requêtes DNS. ODC met en cache les données qu'il reçoit afin de renvoyer plus rapidement et plus efficacement les résultats aux clients. Cet article se concentre sur la façon dont la mise en cache se produit et quand elle est utilisée.

Cet article s'adresse aux utilisateurs qui souhaitent en savoir plus sur les spécificités de la mise en cache ODC (généralement les administrateurs de serveurs de noms et de domaines), ou dans les cas où la résolution DNS ne fonctionne pas comme prévu.

Quelles données sont mises en cache ?

Conformément à la RFC 2181 (https://datatracker.ietf.org/doc/html/rfc2181), les réponses peuvent être renvoyées dans une réponse ou stockées dans un cache en fonction de la fiabilité des données. La RFC définit 7 niveaux de confiance dans la section 5.4.1 :

1. Données d'un fichier de zone principale, autres que les données de collage.
    - Cela ne s'applique qu'aux serveurs de noms faisant autorité, pas aux résolveurs OpenDNS
2. Données d'une zone de transfert, autres que la colle.
    - Cela ne s'applique qu'aux serveurs de noms faisant autorité, pas aux résolveurs OpenDNS
3. Données faisant autorité incluses dans la section de réponse d'une réponse faisant autorité.
    - Cela s'applique à OpenDNSCache
4. Données de la section autorité d'une réponse faisant autorité.
    - Cela s'applique à OpenDNSCache
5. Colle d'une zone principale ou colle d'un transfert de zone.

    - Cela ne s'applique qu'aux serveurs de noms faisant autorité, pas aux résolveurs OpenDNS
6. i) Données de la section de réponse d'une réponse ne faisant pas autorité, et ii) données ne faisant pas autorité de la section de réponse des réponses faisant autorité.
    - i) est un exemple de ce que nos résolveurs retournent. C'est-à-dire des données ne faisant pas autorité.
    - Pour ii), notez que la section de réponse d'une réponse faisant autorité ne contient normalement que des données faisant autorité. Toutefois, lorsque le nom demandé est un alias (voir la section 10.1.1), seul le dossier décrivant cet alias fait nécessairement autorité. Les clients peuvent supposer que d'autres enregistrements doivent provenir du cache du serveur. Lorsque des réponses faisant autorité sont requises, le client peut effectuer une nouvelle requête en utilisant le nom canonique associé à l'alias.
7. i) des informations complémentaires provenant d'une réponse faisant autorité ; ii) les données provenant de la section « autorité » d'une réponse ne faisant pas autorité ; iii) Informations supplémentaires provenant de réponses ne faisant pas autorité.
    - Tous ces éléments s'appliquent à OpenDNSCache
    - Les enregistrements reçus de l'une de ces sources ne doivent pas être mis en cache afin de renvoyer les résultats aux requêtes.

OpenDNSCache met en cache les données des réponses avec les niveaux de confiance 3, 4 et 6. Si nous recevons de nouvelles données avec un niveau de confiance supérieur ou égal, nous remplaçons l'ancienne entrée de cache.

L'exception ici concerne les enregistrements NS, pour lesquels nous ne remplaçons les données qu'avec un niveau de confiance supérieur.

Comment les données sont-elles ajoutées et supprimées du cache ?

Les données expirées ne sont pas supprimées du cache. C'est la base de la fonctionnalité SmartCache, qui permet de renvoyer les enregistrements de ressources expirés du cache si nous ne parvenons pas à joindre les autorités pour une raison quelconque.

Au lieu de cela, le cache sur chaque résolveur est de taille fixe et lorsqu'un nouveau RR est ajouté au cache, le RR le plus ancien est supprimé. Ceci peut être visualisé comme une file d'attente où de nouvelles entrées sont ajoutées à la file d'attente, repoussant les anciennes entrées hors de la file d'attente (pour les informaticiens là-bas, ceci est en fait implémenté comme une liste circulaire doublement liée).

Notez que, comme décrit ci-dessus, une réponse DNS peut contenir plusieurs RR qui ont des niveaux de confiance différents, et qui ne correspondent pas tous aux données initialement demandées. Ainsi, après réception d'une réponse, nous pourrions avoir plusieurs RR à ajouter au cache.

Comme indiqué ci-dessus, notez que les enregistrements NS sont exemptés de ce comportement,

car nous ne remplaçons les entrées des enregistrements NS dans le cache que si le niveau de confiance des données est supérieur à l'entrée existante. Ceci est fait pour s'assurer que nous pouvons détecter des changements aux autorités dans la colle parente si les anciennes autorités répondent encore et se réapproprient comme l'autorité.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.