

# Associez la résolution DNS à la stratégie et aux rapports de domaine d'enregistrement CNAME

## Table des matières

---

[Introduction](#)

[Problème](#)

[Solution](#)

[Motif](#)

[Additional Information](#)

---

## Introduction

Ce document décrit comment faire correspondre votre solution DNS à votre politique de domaine d'enregistrement CNAME et à vos rapports.

## Problème

Lorsque vous utilisez un serveur de mise en cache DNS (Domain Name System) tel que BIND (avec mise en cache activée) ou Infoblox, votre résolution DNS ne correspond pas à la stratégie et aux rapports attendus pour vos domaines d'enregistrement CNAME. Une demande d'enregistrement A autorisée est traitée par une référence CNAME à un autre enregistrement A sur un domaine bloqué différent.

Par exemple, domain.com est autorisé et blocked.com est bloqué, tandis que domain.com est un enregistrement CNAME pointant vers blocked.com, qui a un enregistrement A. Ce problème se présente comme un domaine autorisé bloqué sans aucun événement de ce type enregistré sur le tableau de bord.

## Solution

Il existe plusieurs méthodes pour résoudre ce problème :

- Désactivez la mise en cache DNS pour le transfert DNS vers Umbrella. Cela empêche ce problème de se produire.
- Autorisez le CNAME cible dans le tableau de bord Umbrella dès qu'il apparaît.
- Évitez de mettre en cache le type d'enregistrement CNAME ou de ne pas mettre en cache de manière réactive les domaines affectés.

## Motif

La cause principale de ce problème est la mise en cache DNS pour les enregistrements CNAME pointant vers un domaine différent, où le domaine cible est bloqué. Puisque le domaine est

autorisé, les résolveurs Umbrella marquent la requête entière comme autorisée, en poursuivant la chaîne CNAME. Cela entraîne l'exécution d'une requête autorisée.

Étant donné que les domaines varient en TTL et que les enregistrements de blocs Umbrella pour les catégories malveillantes ont une TTL de zéro, la mise en cache interfère.

Voici un scénario dans lequel domain.com est autorisé et blocked.com est bloqué et domain.com est un enregistrement CNAME pointant vers blocked.com qui a un enregistrement A.

Requête initiale :

Enregistrement A pour domain.com : Allow list, CNAME for blocked.com -> A-record query for blocked.com, provenant d'un CNAME, allow bit passé dans Umbrella - A-record for blocked.com retourné.

Analyse: Requêtes effectuées sur Umbrella : domain.com -> blocked.com. Résultat : Autorisé. Umbrella enregistre domain.com comme autorisé, blocked.com comme autorisé.

Requête suivante :

Enregistrement A pour domain.com : CACHED - il s'agit d'une requête CNAME pour blocked.com -> A-record pour blocked.com: CACHED - Un enregistrement A pour blocked.com a été renvoyé. Analyse: Requêtes effectuées sur Umbrella : Aucune. Pas de journaux Umbrella.

Requête future (déclenche le problème) :

Enregistrement A pour domain.com : CACHED - il s'agit d'une requête CNAME pour blocked.com -> A-record pour blocked.com (requête autonome - CNAME a été mis en cache) - bloqué. Analyse: Requêtes effectuées sur Umbrella : blocked.com. Résultat : Bloqué. Umbrella enregistre blocked.com comme bloqué.

## Additional Information

- [Documentation générale : Résolution DNS](#)

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.