# Résoudre la pénalisation DNS dans MacOS et le problème d'accès avec les domaines internes

## Table des matières



## Introduction

Ce document décrit comment résoudre un problème avec des versions plus récentes de MacOS Big Sur qui affecte la résolution DNS.

## Informations générales

### Portée

- Module ou parapluie de sécurité d'itinérance AnyConnect sur le réseau (comme VA ou transfert)
  - Client d'itinérance autonome Umbrella non affecté. Un environnement de DNS unique est présent où tous les DNS sont écrasés par 127.0.0.1).
- Se produit dans les environnements comportant plusieurs interfaces réseau, mais une seule peut résoudre les adresses internes. Exemple :
  - VPN et hors VPN
  - Plusieurs cartes réseau : une pour l'entreprise et une pour les autres

### Symptômes

- Incapacité (ou capacité intermittente) d'accéder aux domaines locaux tout en conservant la capacité d'accéder aux domaines publics
  - nslookup n'est pas spécifiquement affecté et continue à fonctionner
    - ping, traceroute, etc. résout de manière incorrecte ou ne trouve pas le domaine interne

## Problème

Ce problème est causé par du code dans MacOS qui gère la façon dont les résolutions DNS sont gérées en présence de plusieurs serveurs DNS. Il peut s'agir de plusieurs résolveurs sur une seule carte réseau ou de plusieurs résolveurs sur différentes cartes réseau. Un serveur DNS qui répond par REFUSED est « pénalisé » pendant 60 secondes. Lorsque cela se produit, toutes les requêtes DNS supplémentaires qui se produisent pendant cette période sont essayées sur d'autres serveurs DNS qui ne sont pas pénalisés.

Par exemple, si DHCP annonce deux serveurs DNS pour un réseau, A et B, et A répond par REFUSED, alors B est privilégié par rapport à A pendant 60 secondes tant que B n'est pas pénalisé.

Si tous les serveurs DNS sont pénalisés, MacOS privilégie le serveur le moins récemment pénalisé. Par exemple, si B est pénalisé alors que A l'était déjà, MacOS privilégie A par rapport à B.

Ceci est aggravé par la façon dont MacOS 11 et les versions ultérieures tentent d'affirmer le DoH (DNS sur HTTPS). MacOS est programmé pour préférer un fournisseur DoH défini par l'utilisateur lorsque cela est possible. Cela contournerait la sécurité du DNS Umbrella, ce qui signifie que nous retournons une réponse REFUSED (selon RFC) quand MacOS lance une requête DoH. En raison de la pénalisation DNS, cela peut entraîner une résolution incorrecte des domaines internes. Pour plus d'informations sur ce problème, consultez cet article : Sélection du résolveur DNS dans iOS 14 et macOS 11.

# Solution

Nous ne savons pas encore si Apple prévoit de changer ce comportement ou si Umbrella est en mesure de changer leur comportement pour contourner ce problème. Pour l'instant, deux solutions de contournement sont possibles :

## Option 1

Activez le service DNS partagé dans la stratégie de groupe et ajoutez spécifiquement les domaines internes à la configuration du service DNS partagé afin qu'ils ne puissent être résolus que par tunnel. Cela garantit que ces domaines ne peuvent être résolus que sur le tunnel par le résolveur de système d'exploitation natif, alors que tous les autres domaines ne peuvent être résolus qu'en dehors du tunnel.

## Option 2

Activez tunnel-all-DNS dans la stratégie de groupe pour empêcher tout trafic DNS de sortir du tunnel.

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.