Beheben von DNS-Penalisierung in MacOS und Zugriffsproblemen mit internen Domänen

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie ein Problem mit neueren Versionen von MacOS Big Sur beheben, das sich auf die DNS-Auflösung auswirkt.

Hintergrundinformationen

Umfang

- AnyConnect Roaming Security-Modul oder Umbrella im Netzwerk (z. B. VA oder Forwarding)
  - Umbrella Standalone-Roaming-Client nicht betroffen. In einer Single-DNS-Umgebung wird der gesamte DNS mit 127.0.0.1 überschrieben.
- Tritt in Umgebungen mit mehreren Netzwerkschnittstellen auf, aber nur eine kann interne Adressen auflösen. Beispiele:
  - VPN und Off-VPN
  - Mehrere NICs - eine firmeneigene und eine nicht firmeneigene

Symptome

- Zugriff auf lokale Domänen ist nicht (oder nur zeitweilig) möglich, der Zugriff auf öffentliche Domänen bleibt jedoch erhalten.
  - nslookup ist nicht spezifisch betroffen und funktioniert weiterhin
    - ping, traceroute usw. nicht korrekt aufgelöst werden oder die interne Domäne nicht finden

Problem

Dieses Problem wird durch Code in MacOS verursacht, der die Verwaltung von DNS-Auflösungen bei Vorhandensein mehrerer DNS-Server übernimmt. Dabei kann es sich um mehrere Resolver auf einem einzelnen Netzwerkadapter oder um mehrere Resolver auf verschiedenen Netzwerkadaptern handeln. Ein DNS-Server, der mit REFUSED antwortet, wird für 60 Sekunden "bestraft". In diesem Fall werden alle weiteren DNS-Abfragen, die in diesem Zeitraum auftreten, auf alternativen DNS-Servern versucht, die nicht bestraft werden.

Wenn DHCP beispielsweise zwei DNS-Server für ein Netzwerk ankündigt, A und B, und A mit ABGELEHNT antwortet, wird B für 60 Sekunden gegenüber A bevorzugt, solange B nicht bestraft wird.

Wenn alle DNS-Server bestraft werden, bevorzugt MacOS den am wenigsten bestraften Server. Wenn B beispielsweise bestraft wird, während A bereits bestraft wurde, bevorzugt MacOS A gegenüber B.

Dies wird durch die Art und Weise, MacOS 11 und höher versuchen, DoH (DNS über HTTPS) zu behaupten verschlimmert. MacOS ist so programmiert, dass es einen DoH-Provider vorzieht, wenn dies möglich ist. Dies würde die Umbrella DNS-Sicherheit umgehen, was bedeutet, dass wir eine REFUSED-Antwort (gemäß RFC) zurückgeben, wenn MacOS eine DoH-Anfrage initiiert. Aufgrund von DNS Penalization kann dies dazu führen, dass interne Domänen nicht ordnungsgemäß aufgelöst werden. Weitere Informationen zu diesem Thema finden Sie in diesem Artikel: Auswahl des DNS-Resolvers in iOS 14 und macOS 11.

Lösung

Wir wissen noch nicht, ob Apple plant, dieses Verhalten zu ändern, oder ob Umbrella in der Lage ist, sein Verhalten zu ändern, um dieses Problem zu umgehen. Im Moment gibt es zwei Möglichkeiten, die als Lösung dienen:

Option 1

Aktivieren Sie Split-DNS in der Gruppenrichtlinie, und fügen Sie die internen Domänen der Split-DNS-Konfiguration hinzu, sodass sie nur über Tunnel aufgelöst werden können. Dadurch wird sichergestellt, dass diese Domänen nur über Tunnel vom nativen OS-Resolver aufgelöst werden können, während andere Domänen nur außerhalb des Tunnels aufgelöst werden können.

Option 2

Aktivieren Sie tunnel-all-DNS in der Gruppenrichtlinie, um zu verhindern, dass DNS-Datenverkehr außerhalb des Tunnels verläuft.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.