Dealing with Amazon AWS DNS limits

In a client configuration I noticed he was using 127.0.0.1 as DNS in /etc/resolv.conf and asked about an explaination. This is his answer:

The 127.0.0.1 loopback configuration is intentional. We were experiencing intermittent issues because Asterisk relies so heavily on DNS. AWS enforces a strict, unmodifiable hard limit of 1,024 Packets Per Second (PPS) per network interface to their default VPC resolver (172.31.0.2). Because of Asterisk's high query volume and the internal search paths, we were constantly exceeding this threshold.

When this limit is breached, AWS silently drops the packets at the hypervisor level. Before making the change, I checked the internal network interface statistics, and the linklocal_allowance_exceeded counter had already reached 62,661 dropped packets.

To resolve this permanently and prevent these drops, I did the following:

Installed DnsMasq: It now acts as a local DNS cache on 127.0.0.1, absorbing repetitive queries so they don't count toward the AWS network limit.

Configured Upstream Servers: For cache misses, DnsMasq safely forwards requests to a mix of the local VPC resolver, Cloudflare, and Google (172.31.0.2, 1.1.1.1, and 8.8.8.8).

Locked NetworkManager: Configured dns=none so NetworkManager doesn't overwrite /etc/resolv.conf on reboot.

Revision #1
Created 2026-06-28 08:26:42 UTC by Admin
Updated 2026-06-28 08:28:20 UTC by Admin