Diagnose IPv6 connectivity without changing the network

A service can work over IPv4 while failing over IPv6. A published AAAA record may then cause intermittent-looking failures for clients that prefer IPv6. This guide collects evidence on Debian or Ubuntu without changing addresses, routes or firewall rules. Use your existing management connection and keep console access available.

Confirm that IPv6 is assigned

```
date -Is
ip -6 address show
ip -6 route show
getent ahosts server.example.com
```

Replace the hostname with the affected service. Compare global addresses with the allocation shown in your service information. A link-local address beginning with fe80 does not establish public IPv6 connectivity. Tentative or duplicate-address flags need investigation before the address can be considered usable.

Do not invent a gateway from another server or copy an address from a forum. Provider routing designs differ. The presence of an address alone does not prove that a return route exists. If no public IPv6 allocation was supplied, ask support about availability before publishing a DNS record.

Check the application listener

```
sudo ss -ltnp
sudo ss -lunp
```

Find the actual protocol and port. An application listening only on an IPv4 address may not accept IPv6. A wildcard display also requires interpretation of the application's socket settings and operating-system configuration. Container port publishing adds another layer, so inspect its deployment definition when applicable.

Test the real endpoint from a client with known working IPv6. For an HTTPS service you own, a bounded request such as `curl -6 --connect-timeout 5 --max-time 15 -I https://server.example.com/` checks one path without disabling certificate verification. Some applications reject HEAD requests, so interpret the HTTP response separately from transport success.

Separate DNS from routing

Compare the public AAAA record with the intended assigned address. Caches and split DNS can return different answers on different clients. A correct A record says nothing about the AAAA record. Note the resolver and time when capturing a mismatch.

Where authorized, use a small number of IPv6 ping or traceroute probes to the service. ICMP filtering can make those probes inconclusive, so do not infer an application outage from ping alone. Likewise, a responding gateway does not prove the full path to a remote client. Essential ICMPv6 traffic has network functions beyond simple echo requests; blocking it indiscriminately can break connectivity.

Preserve evidence and access

Collect the assigned prefix, relevant address and route lines, listener, public DNS answer and the exact failing client request. Redact unrelated addresses from public posts. Ask support to compare the same interval with upstream routing when local evidence looks correct.

No networking restart or firewall flush is needed for these checks. If a correction is required, write a separate change plan with console access, saved configuration and a tested rollback. Keep IPv4 management working while resolving IPv6. Remove or change a published record only through the normal DNS workflow after understanding which clients and services rely on it.

Related instructions

Diagnose network timeouts. Configure a domain and HTTPS.

Reference: Official documentation. Check the documentation installed on your own operating-system release when an option differs.

Revision #1
Created 2026-11-09 10:42:42 UTC by CloudExa Hosting Admin
Updated 2026-11-09 10:42:42 UTC by CloudExa Hosting Admin