

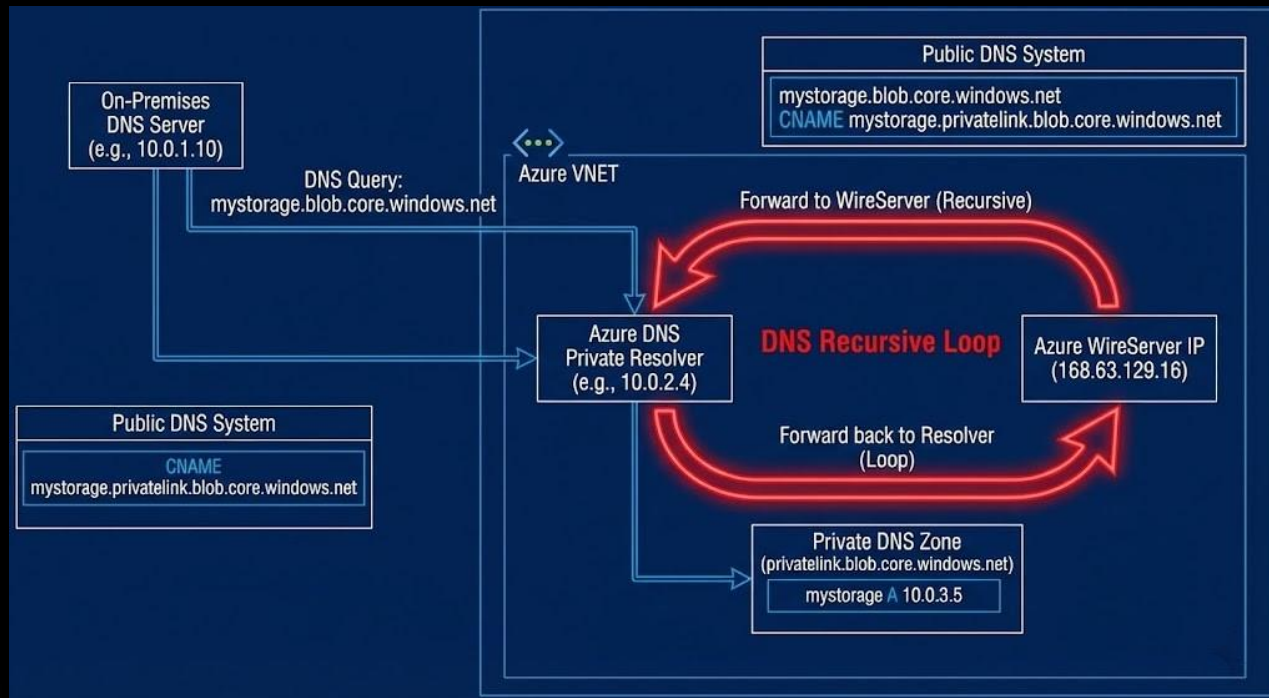
The Azure Private Endpoint Trap

Why DNS Loops and Subnet Exhaustion
are killing migrations before the 2026
outbound retirement.



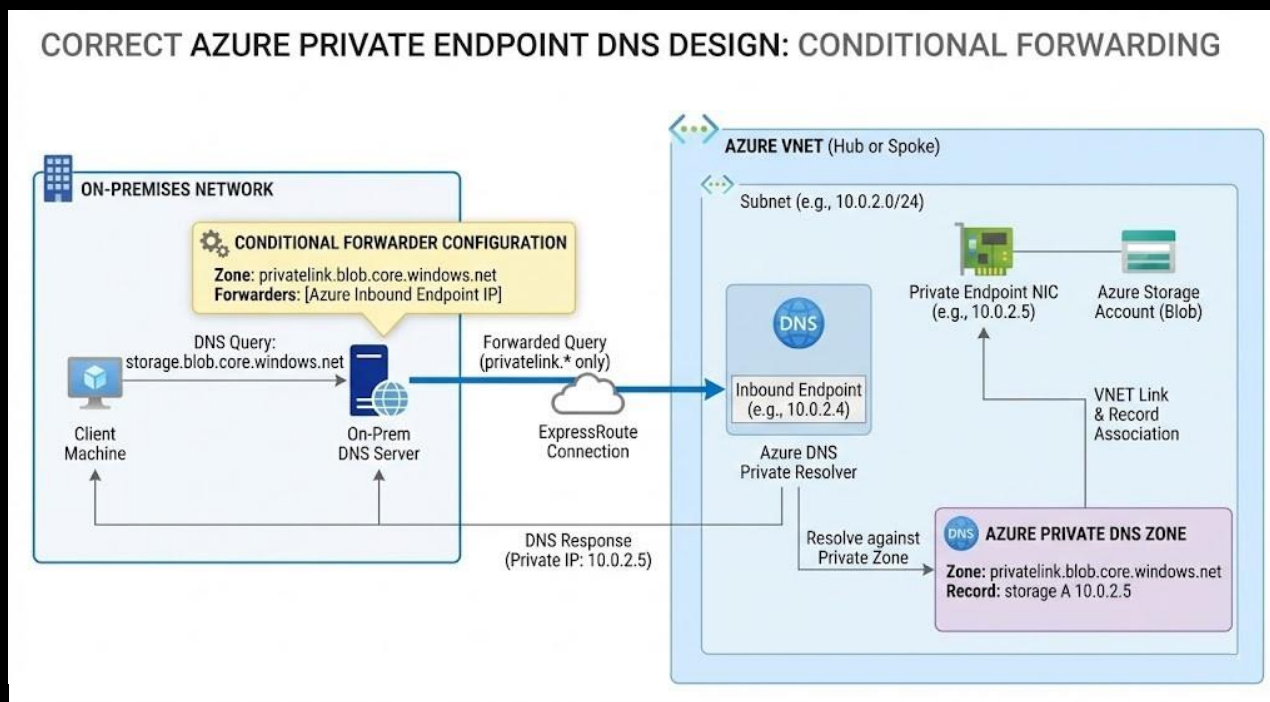
The "Broad Forwarder" Loop

- On-prem DNS forwards *.core.windows.net to Azure.
- Azure attempts public resolution and bounces it back.
- Result: High latency, random 404s, and timeouts.



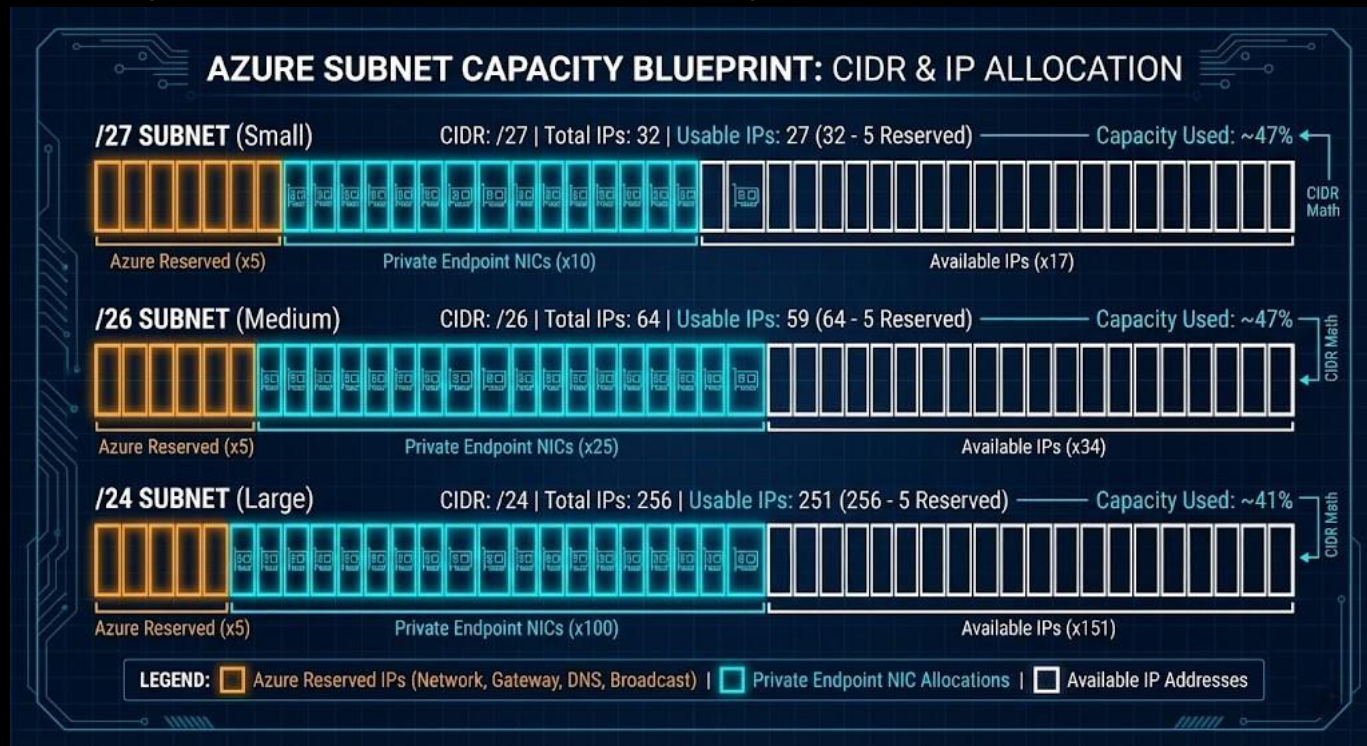
Surgical privatelink Forwarding

- The Azure WireServer IP (168.63.129.16) is invisible over VPN/ExpressRoute.
- Deploy Azure DNS Private Resolver.
- Only forward the exact privatelink suffix.



Subnet Math is Non-Negotiable

- Private Endpoints are NIC-backed.
- They do not share IPs. They cannot be moved.
- Azure reserves 5 IPs per subnet.
- A /27 safely holds ~20 Private Endpoints.



Stop Guessing. Validate Your Architecture.

- Run your environment through our stateless Azure PE Checker to instantly detect DNS loops and IP headroom.

 **RACK2CLOUD**
AZURE PE SANITY CHECKER

v0.1 Alpha

Stateless utility for auditing Azure Private Networking logic. Checks for CIDR exhaustion and recursive DNS loops locally.

1

Subnet Capacity Auditor

?

Subnet Mask

Planned Endpoints

/28 (16 Total)

5

☐ Include Private Link Service? (+1 NAT IP)

2

DNS Recursive Loop Sniper

?

On-Prem/Local Forwarder IP

e.g. 10.0.1.4

Azure Private Resolver Inbound IP

e.g. 10.20.0.4

Forwarding Zone Name

e.g. database.windows.net

RUN ANALYSIS

Found a configuration mess? Our architects catch what automated tools miss.

Book Architecture Audit



RACK2CLOUD

Think Like An Architect.
Build Like An Engineer.

Think Like An Architect. Build Like An Engineer.

Run the Audit:

www.Rack2Cloud.com