Azure

Azure DNS Private Resolver

Author

Ketan Valsangkar

Cloud Architect & Devops Engineer

Azure DNS Private Resolver it's PAAS service by Microsoft Azure, so no need to think about managing virtual machine and its scale

Features	Pre-requisites	Limitations
Scalability: High performance per endpoint.	Required virtual network in the same region.	A virtual network can't contain more than one DNS resolver.
Azure DNS private resolver allows to create multiple inbound end points and multiple outbound endpoints.	Dedicated 0.0.0.0/28,0.0.0.0/24 ,0.0.0.26, or larger subnets are required for Inbound endpoints and Outbound endpoints.	A virtual network can't be shared between multiple DNS resolvers
When you use Azure DNS Private Resolver, you don't need a DNS forwarder VM, and Azure DNS is able to resolve on-premises domain names.	Must have established connectivity between on-prem to Azure with Express route or VPN gateway.	DNS private resolver does not support Azure ExpressRoute Fast Path.
Azure DNS Private Resolver is a fully managed Microsoft service that can handle millions of requests. Use a subnet address space between /28 and /24. For most users, /26 works best.	An Azure private DNS zone that is linked to each virtual network.	A single DNS resolver can only reference a single virtual network.
Cost reduction: Reduce operating costs and run at a fraction of the price of traditional IaaS solutions.	Azure DNS Private Resolver is in one of the regions listed, you don't need to take any other action beyond provisioning the service.	single Azure Private Resolver is not able to sync with other one.
Private access to your Private DNS zones: Conditionally forward to and from on-premises.		Azure DNS Private Resolver can only resolve virtual networks that are within the same geographical region as the resolver.
Fully managed: Built-in high availability, zone redundancy		Assign a dedicated subnet to each inbound and outbound endpoint.

Overview

On-Prem Network

- Customer datacenters is connected to Azure via ExpressRoute or a site-to-site Azure VPN Gateway connection. Network components include one local DNS server and Infoblox anycast device.
- Local DNS server is uses the name resolution and Infoblox is having some features like scalability, HA, fault tolerance, single control for all local and hybrid environments Both are work as resolvers or forwarders for all computers inside the on-premises network.

Hub Network

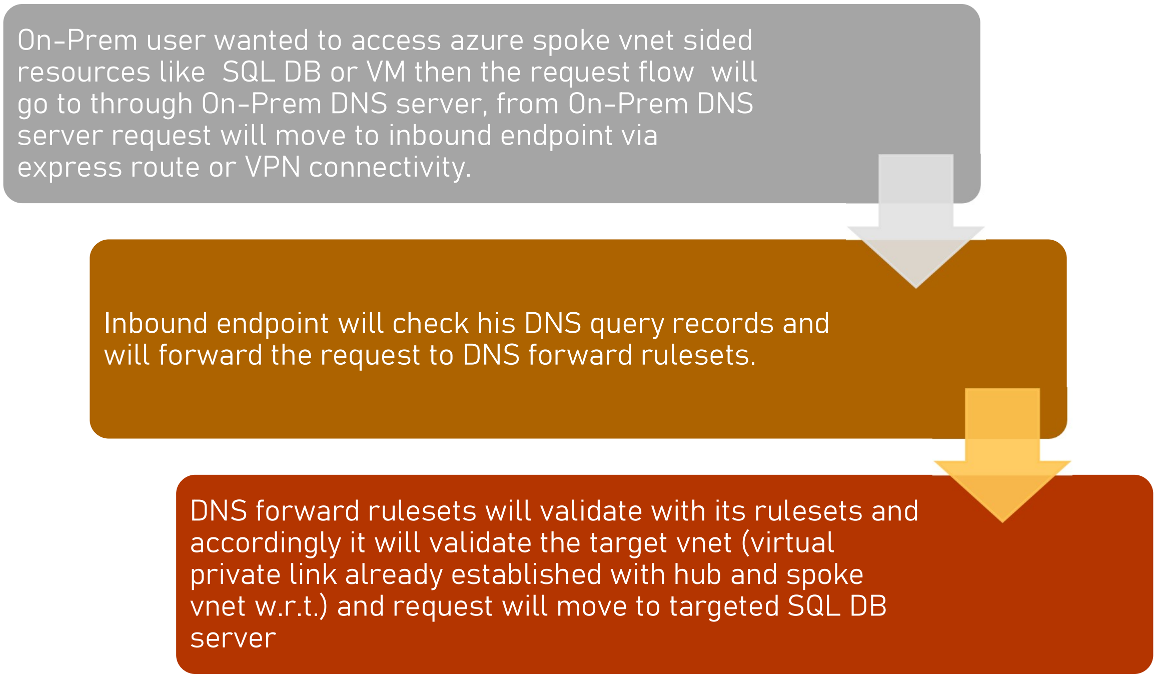
- VPN Gateway or an ExpressRoute connection is used for the hybrid connection to Azure.
- For App DNS names, the DNS forwarding rule set is configured. The hub virtual network is linked to the private DNS zones for Blob Storage and the API service.
- Azure DNS private resolver is configured in hub vnet and linked with Azure private DNS.
- The hub vnet is connected with spokes vnet through v-net peering. All network traffic came from On-prem that is in landed in hub network.
- The hub virtual network is linked to the private DNS zones for Blob Storage and the API service.

Spoke Network

- VMs Apps and storage accounts are hosted in all spoke networks for testing and validating DNS Name resolution.
- All Azure spoke virtual networks use the default Azure DNS server at the IP address 168.63.129.16.
- All spoke networks are connected with hub vnet through hub vnet peering.
- The spoke virtual networks are linked to private DNS zones, which makes it possible to resolve the names of private endpoint link services.

How it works?

DNS query resolution from On-Prem user

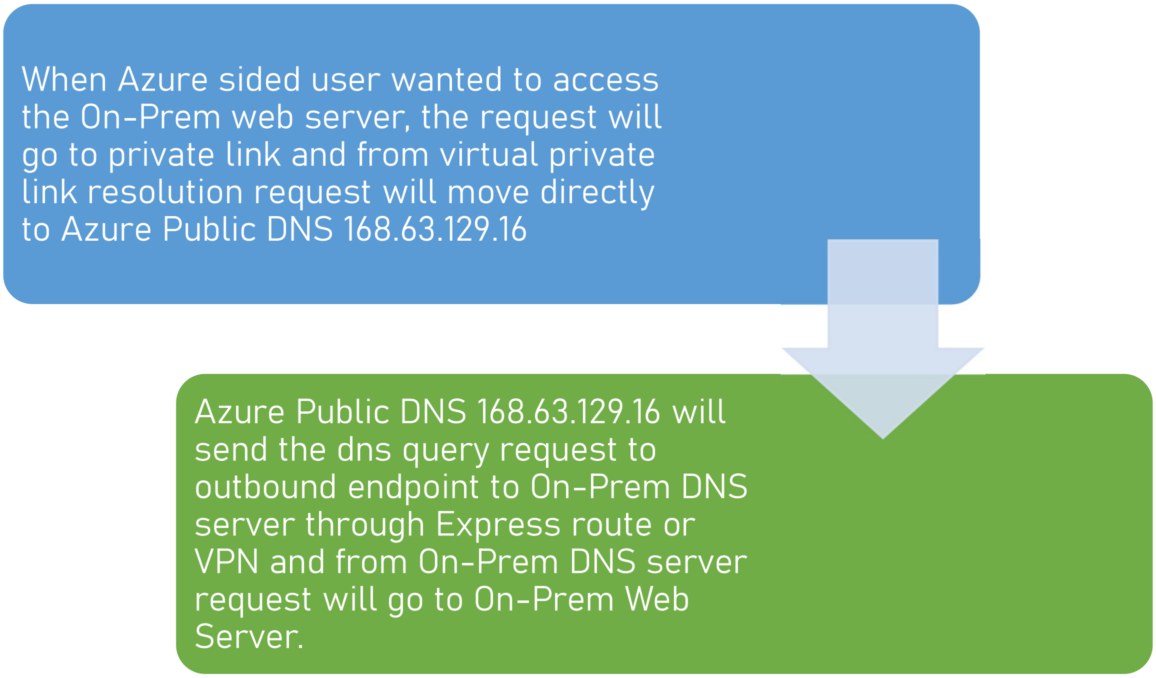


On-Prem user wanted to access azure spoke vnet sided resources like SQL DB or VM then the request flow will go to through On-Prem DNS server, from On-Prem DNS server request will move to inbound endpoint via express route or VPN connectivity.

Inbound endpoint will check his DNS query records and will forward the request to DNS forward rulesets.

DNS forward rulesets will validate with its rulesets and accordingly it will validate the target vnet (virtual private link already established with hub and spoke vnet w.r.t.) and request will move to targeted SQL DB server

DNS query resolution from Azure user

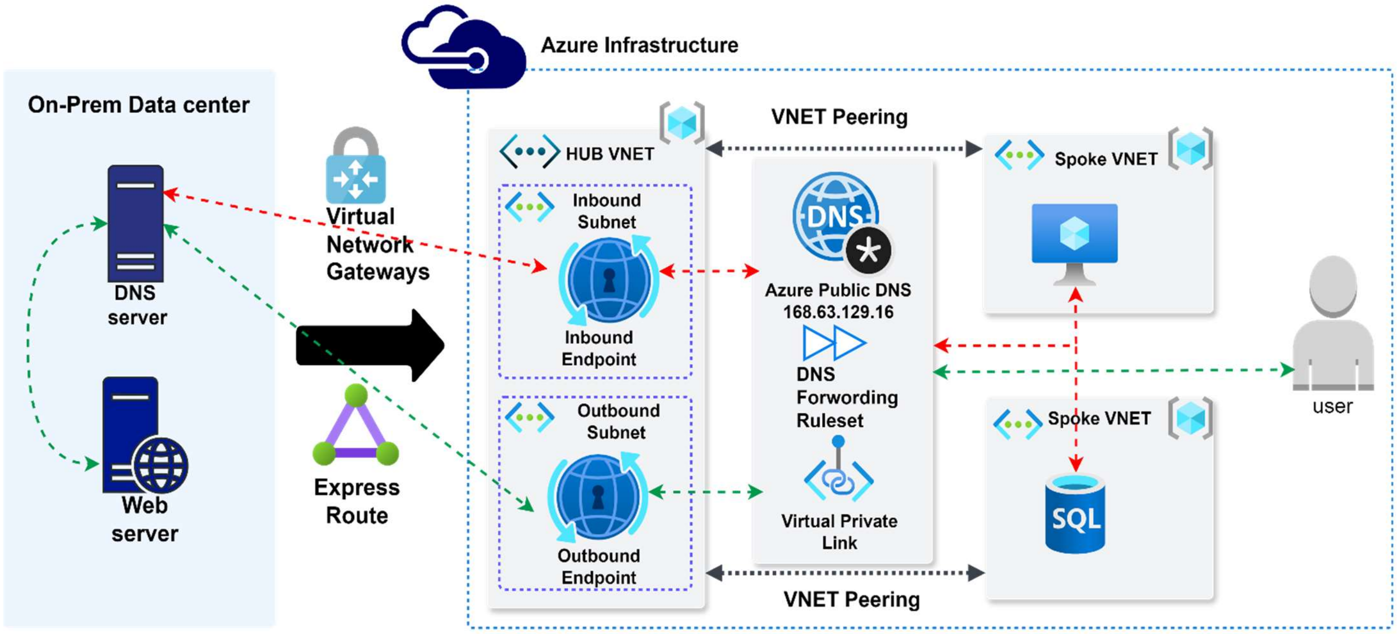


When Azure sided user wanted to access the On-Prem web server, the request will go to private link and from virtual private link resolution request will move directly to Azure Public DNS 168.63.129.16

Azure Public DNS 168.63.129.16 will send the dns query request to outbound endpoint to On-Prem DNS server through Express route or VPN and from On-Prem DNS server request will go to On-Prem Web Server.

Azure DNS Private Resolver

Workflow Design


Azure Infrastructure
On-Prem Data center
DNS server
Web server
Virtual Network Gateways
Express Route
VNET Peering
HUB VNET
Inbound Subnet
Inbound Endpoint
Outbound Subnet
Outbound Endpoint
Azure Public DNS 168.63.129.16
DNS Forwording Ruleset
Virtual Private Link
Spoke VNET
Spoke VNET
SQL
user
VNET Peering