



HALOMD

Search



Updated Jul 21



Edit

Share



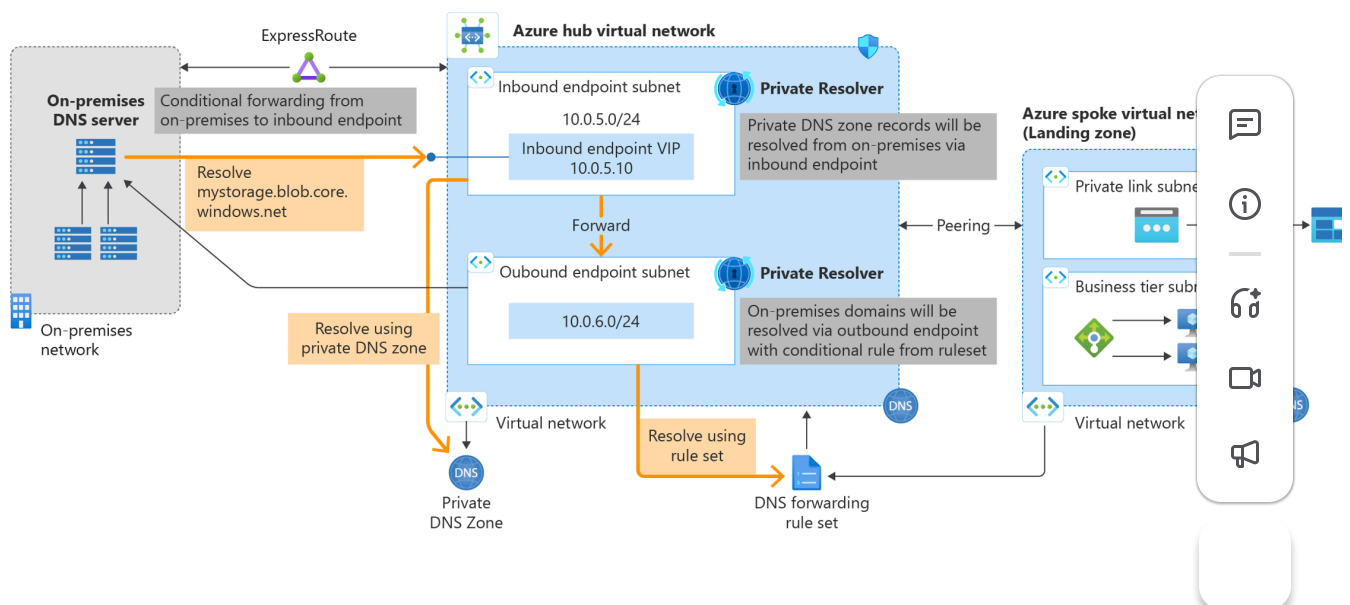
Private DNS Resolver

By Krishna Bhattarai 2 min 4 Add a reaction

One of the most important components of HaloMD's network Architecture is our Private DNS Resolver.

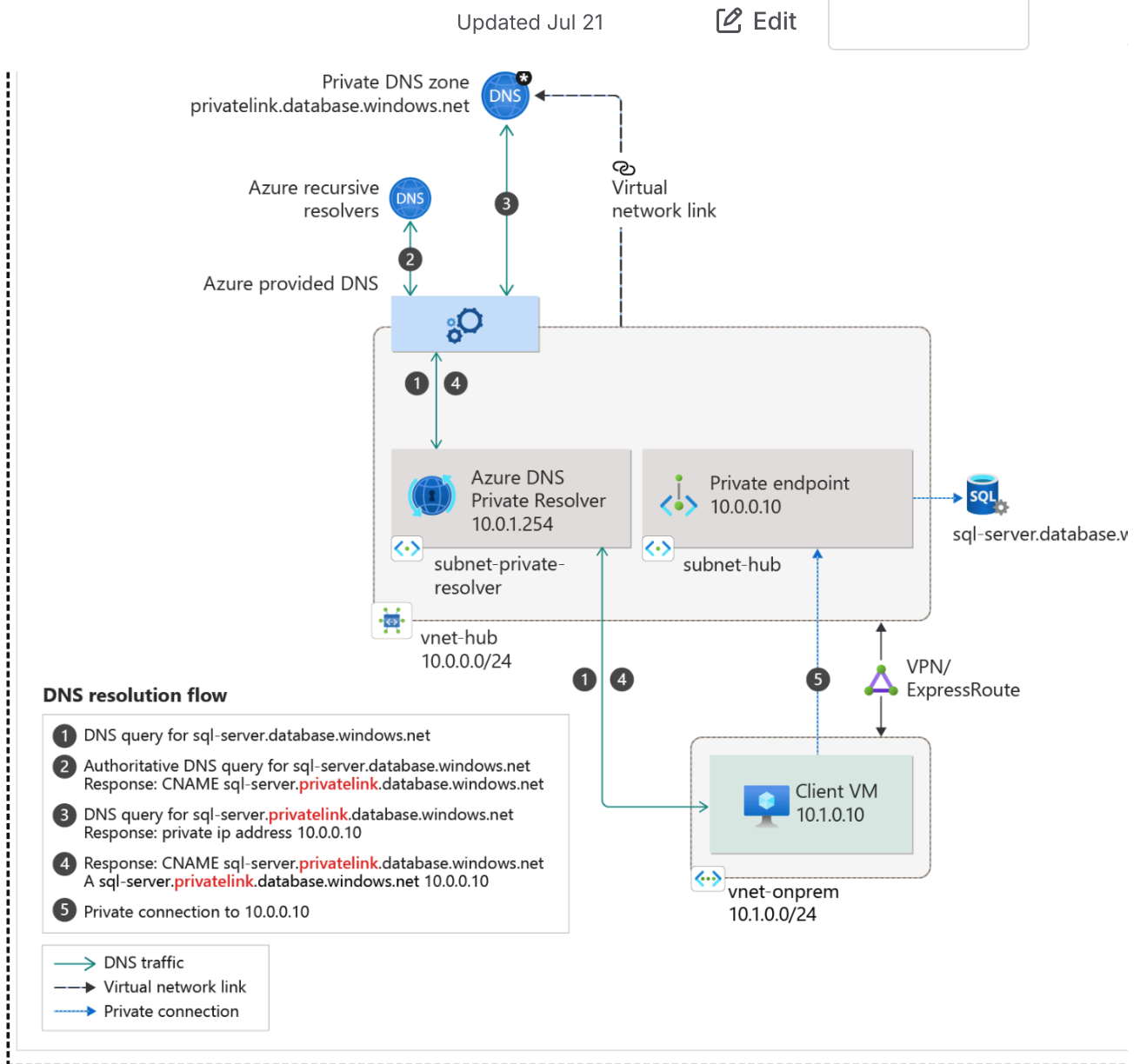
In this article, I will demystify, clarify, and document how Private DNS Resolver works.

Here is a General Architectural Diagram of a Private DNS Resolver. Note that the subnets shown in the diagram are not specific to HaloMD, this is a generic diagram from Azure:



Here is another diagram from Azure that shows DNS resolution Flow:

The following diagram illustrates the DNS resolution sequence from an on-premises network. The configuration uses a Private Resolver deployed in Azure. The resolution is made by a private DNS zone



So what is a Private DNS Resolver?

In general terms, it is a fully managed, cloud-native service that enables DNS resolution between Azure virtual networks and on-premise environments without having to deploy custom DNS servers.

So architecturally where does this live?

Updated Jul 21

 Edit

central point of DNS resolution. In our case, it exists here:

<https://portal.azure.com/#@az.halomd.com/resource/subscriptions/54b02500-d420-4838-a98a-00d0854b5592/resourceGroups/hub-eus2-vnet-rg-1/providers/Microsoft.Network/dnsResolvers/hub-eus2-pDNS-1/resourceOverviewId>

It has a notion of these main components:

- inbound endpoint
- outbound endpoint
- virtual network links

Inbound Endpoint: This is the endpoint that accepts DNS Queries from peered-VNets or from on-premises environments if so configured. For us, this endpoint has a specific IP address that is **10.62.0.68**

As an example, when someone does a nslookup using the **HaloMD VPN**, they will and should see this:

```
1 nslookup briefbuilder.halomd.com
2 Server:      10.62.0.68
3 Address:     10.62.0.68#53
4
5 Non-authoritative answer:
6 Name:   briefbuilder.halomd.com
7 Address: 10.60.8.17
8
```

Notice how the server is 10.62.0.68? That is our Private DNS Resolver's endpoint.

Outbound Endpoint: So the purpose of this outbound endpoint is so that it can send DNS queries to other components like conditional forwarders, on premises DNS servers etc. This endpoint requires a dedicated subnet in the VNet where it is provisioned, with no other service running in the subnet, and

can only be delegated to **Microsoft.Network/dnsResolvers**. DNS Queries sent to the outbound endpoint will egress from Azure.

Updated Jul 21

 Edit

Our forwarder:

<https://portal.azure.com/#@az.halomd.com/resource/subscriptions/54b02500-d420-4838-a98a-00d0854b5592/resourceGroups/hub-eus2-vnet-rg-1/providers/Microsoft.Network/dnsForwardingRulesets/mpw-to-hub-ruleset/rules>


For example, we currently have an outbound endpoint named **hub-eus2-pDNS-outbound-1** and this component has what are called “**rulesets**“, and those rulesets are essentially **DNS forwarding rulesets**. So these rulesets have “rules”. For example, we have a ruleset where we forward specific DNS queries to the DNS controllers on the Mpower Tenant.

For example, we have a rule called “**MPW_SA_TRUST_DNS_SVR**“ that says if we get a request for a domain name stxn.local. we forward those requests to these specific IPs

- 1 10.10.0.8:53
- 2 10.100.48.4:53
- 3 10.100.48.5:53
- 4 10.10.0.5:53

Virtual Network Links: Virtual network links are an important component of how all of this works. So these links help with the name resolution for virtual networks that are linked to an outbound endpoint with a DNS forwarding ruleset.

Other Relevant Articles

More information can be found in this Azure Article:  [What is Azure DNS Private Resolver?](#) It goes in depth on what other restrictions exist.

Another very useful article is here: [Azure DNS Private Resolver - Azure Architecture Center](#)

Updated Jul 21

[Edit](#)

setups and how DNS traffic flows.


Another useful article is : [Azure Private Endpoint DNS Integration Scenarios](#)
This article is extremely important to read and understand!!

Another one: [Private resolver architecture - Azure DNS Private Resolver architecture guidance](#)


Another architectural diagram is here: [Azure DNS Private Resolver Template](#)


Related content




 [Hub Network](#)
[Technology Platform](#)


 More like this

 [Binding a subdomain wildcard certificate to azure web app](#)
[Technology Platform](#)

 More like this


 [Adding azurewebsites.net Addresses](#)
[Technology Platform](#)

 More like this


 [Development Network](#)
[Technology Platform](#)


 Read with this

Updated Jul 21

 Edit

 More like this

 Building a Managed Instance DWSQL SQL Server
Technology Platform

 More like this

 Add a comment

DEVOPS

USER-STORIES

 Add a reaction

