Enhancing Hybrid Cloud DNS Resolution with Azure Private DNS Resolver: Architecture, Benefits, and Implementation Strategies

Venkata Raman Immidisetti

Sr. Systems Engineer
Raleigh, North Carolina
vimmidisetti@gmail.com

Abstract

The Azure Private DNS Resolver is a managed service for DNS resolution in hybrid cloud environments, eliminating the need for conventional DNS forwarder VMs. In hybrid architectures, seamless name resolution between on-premises infrastructure and Azure is crucial for connectivity, security, and operational efficiency. Historically, organizations used DNS forwarders within Azure VNets to relay DNS queries, adding complexity, latency, and administrative overhead. The Azure Private DNS Resolver solves these issues by providing bidirectional DNS query resolution through inbound and outbound endpoints, enabling on-premises resources to resolve Azure private DNS zones and vice versa. This paper examines the architecture, advantages, and deployment considerations of Azure Private DNS Resolver, highlighting its role in simplifying hybrid DNS management, reducing operational costs, and enhancing security. Additionally, the paper explores best practices for deploying the resolver in hub-spoke network topologies, ensuring efficient, scalable, and secure DNS resolution across hybrid environments

Keywords: Azure Private DNS Resolver, Hybrid Cloud DNS, DNS Forwarding, On-Premises Name Resolution, Azure Networking, Private DNS Zones, Cloud Connectivity, Domain Name System, Bidirectional DNS Resolution, Secure Name Resolution

I. INTRODUCTION

In contemporary hybrid cloud architectures, seamless integration between on-premises infrastructure and cloud platforms, such as Microsoft Azure, is of paramount importance. A critical component of this integration is the Domain Name System (DNS), which translates human-readable domain names into IP addresses, thereby facilitating network communication. Traditionally, organizations have employed DNS forwarders, servers configured to direct DNS queries to specific external DNS servers, to enable name resolution across disparate networks. In hybrid environments, DNS forwarders are frequently deployed within Azure virtual networks (VNets) to relay queries from on-premise systems to Azure's DNS services., this configuration, however introduces complexities, such as the necessity for additional infrastructure management, potential latency issues, and challenges in maintaining high availability.

To address these challenges, Microsoft introduced Azure DNS Private Resolver, a fully managed service designed to streamline DNS resolution in hybrid scenarios. This service enables bidirectional DNS query resolution between on-premises networks and Azure without the requirement of deploying and managing custom DNS forwarders on virtual machines. By establishing inbound and outbound endpoints within an Azure VNet, the DNS Private Resolver facilitates seamless name resolution for resources in Azure Private

DNS zones and on-premises domains. This integration not only reduces operational overhead, but also enhances security and performance by eliminating the necessity of route queries through additional intermediaries.

The Azure DNS Private Resolver offers several advantages over traditional DNS forwarders:

- Simplified Management: As a fully managed service, it eliminates the necessity of providing, configuring, and maintaining virtual machines for DNS forwarding, thereby reducing administrative burden.
- Enhanced Performance: By residing within the Azure network, the service provides low-latency resolution for Azure resources, improving application responsiveness.
- Improved Security: Direct integration with Azure's networking infrastructure ensures that DNS queries remain within trusted boundaries, reducing exposure to potential threats.
- Scalability and High Availability: The service is designed to handle high query volumes and offers built-in redundancy, ensuring reliable name resolution, even during peak loads.

This paper presents a comprehensive analysis of the Azure DNS Private Resolver, exploring its architecture, deployment strategies, benefits, and potential challenges. By examining real-world scenarios and best practices, we aim to provide insights into how organizations can effectively leverage this service to achieve seamless and secure DNS integration in hybrid cloud environments.

II. DNS FORWARDER VIRTUAL MACHINE

Prior to the implementation of the Azure DNS Private Resolver, organizations utilized DNS forwarder virtual machines (VMs) to enable on-premise servers to resolve Azure private DNS zone records. This methodology necessitated the deployment of a DNS forwarder VM within an Azure virtual network (VNet) to facilitate name resolution between on-premise environments and Azure-hosted services. The on-premises DNS server is configured with a conditional forwarder, directing DNS queries for Azure services to the DNS forwarder VM in Azure. Subsequently, the DNS forwarder relays these requests to the Azure internal recursive resolver (168.63.129.16) for processing. The response was then propagated back through the resolution path, ultimately enabling the on-premisesclient to establish a secure connection with Azure resources.

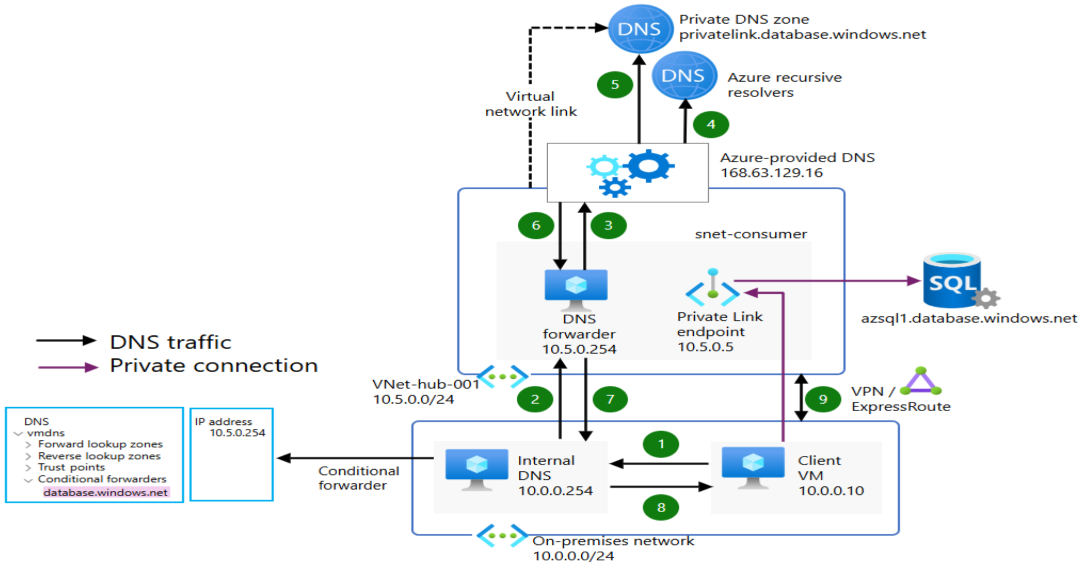

Figure 1: DNS resolution from on-premises using DNS forwarder VM in azure

Name Resolution Workflow

1. A client virtual machine (VM) initiates a name resolution request for an Azure service hostname (e.g., azsql1.database.windows.net). This request is transmitted to the on-premise DNS server.
2. The on-premises DNS server, configured with a conditional forwarder, redirects the query for the database.windows.net domain to the DNS forwarder VM situated in the Azure virtual network.
3. The DNS forwarder VM forwards the query to Azure's internal DNS resolver (168.63.129.16) in order to resolve the requested domain.
4. The Azure DNS service processes the request and queries Azure's recursive resolvers, returning a canonical name (CNAME) record that maps the requested domain (azsql1.database.windows.net) to its private endpoint alias (azsql1.privatelink.database.windows.net).
5. The Azure DNS resolver subsequently queries the Azure Private DNS Zone (privatelink.database.windows.net), which provides the associated private IP address (e.g., 10.5.0.5) for the requested service.
6. The resolved private IP address (10.5.0.5) is transmitted back through the DNS resolution chain, propagates first to the DNS forwarder VM, then to the on-premises DNS server, and finally reaches the client VM that originates the request.
7. The client VM establishes a private connection to the Azure private endpoint by utilizing the resolved private IP address (10.5.0.5), ensuring a secure, direct connection to the requested Azure database service.

This legacy approach necessitated additional infrastructure, manual configuration, and ongoing maintenance, rendering it operationally complex and resource-intensive. Furthermore, it relied on Azure's internal DNS resolver, which could not be utilized to resolve on-premise domain names, further limiting its capabilities. The introduction of the Azure DNS Private Resolver eliminated these challenges by providing a fully managed, scalable, and integrated DNS resolution service that seamlessly enables bidirectional name resolution between on-premises and Azure workloads without the requirement for custom DNS forwarders.

III. AZURE PRIVATE DNS RESOLVER

The Azure DNS Private Resolver is a fully managed service that facilitates seamless Domain Name System (DNS) resolution between on-premises networks and Azure environments without the need to deploy and manage custom DNS forwarding solutions. This service enables bidirectional DNS query resolution, allowing on-premises resources to resolve names in Azure private DNS zones, and vice versa.

The Azure DNS Private Resolver operates within an Azure Virtual Network (VNet) and comprises two primary components:

- Inbound Endpoints: These endpoints receive DNS queries from on-premise networks or other private locations. When an on-premises DNS server requires the resolution of a domain hosted in Azure, it forwards the query to the IP address of the inbound endpoint within VNet.
- Outbound Endpoints: These endpoints handle DNS queries from Azure resources that require the resolution of names in on-premise or external domains. Queries are processed based on a configurable DNS forwarding rule set that determines the routing of specific domain queries to designated DNS servers.

Implementing the Azure DNS Private Resolver offers several advantages:

- Fully managed service: Eliminate the operational overhead associated with deploying and maintaining DNS forwarder virtual machines, providing built-in high availability and zone redundancy.
- Cost Reduction: Reduces operating expenses by obviating the need for infrastructure-as-a-service (IaaS) solutions traditionally utilized for DNS forwarding.
- Enhanced Security: Facilitates private access to Azure private DNS zones with conditional forwarding capabilities, ensuring that DNS queries remain within trusted network boundaries.
- Scalability: Delivers high-performance DNS resolution capable of handling substantial query volumes per endpoint.
- DevOps Integration: Supports infrastructure as code practices, allowing deployment and management through tools such as Terraform, Azure Resource Manager (ARM) templates, or Bicep.

By utilizing Azure DNS Private Resolver, the requirement for deploying a DNS forwarder virtual machine (VM) is eliminated, allowing Azure DNS to directly resolve on-premises domain names. This implementation follows a hub-spoke network topology aligned with the best practices recommended in the Azure landing zone design pattern. This architectural model facilitates efficient resource management and enhances security in hybrid cloud environments. A secure hybrid network connection is established through Azure ExpressRoute in conjunction with Azure Firewall, ensuring controlled and secure communication between the on-premises and Azure workloads. The DNS Private Resolver is strategically deployed within a spoke network, adhering to network segmentation principles to optimize the DNS resolution, security, and scalability within the hybrid cloud infrastructure.

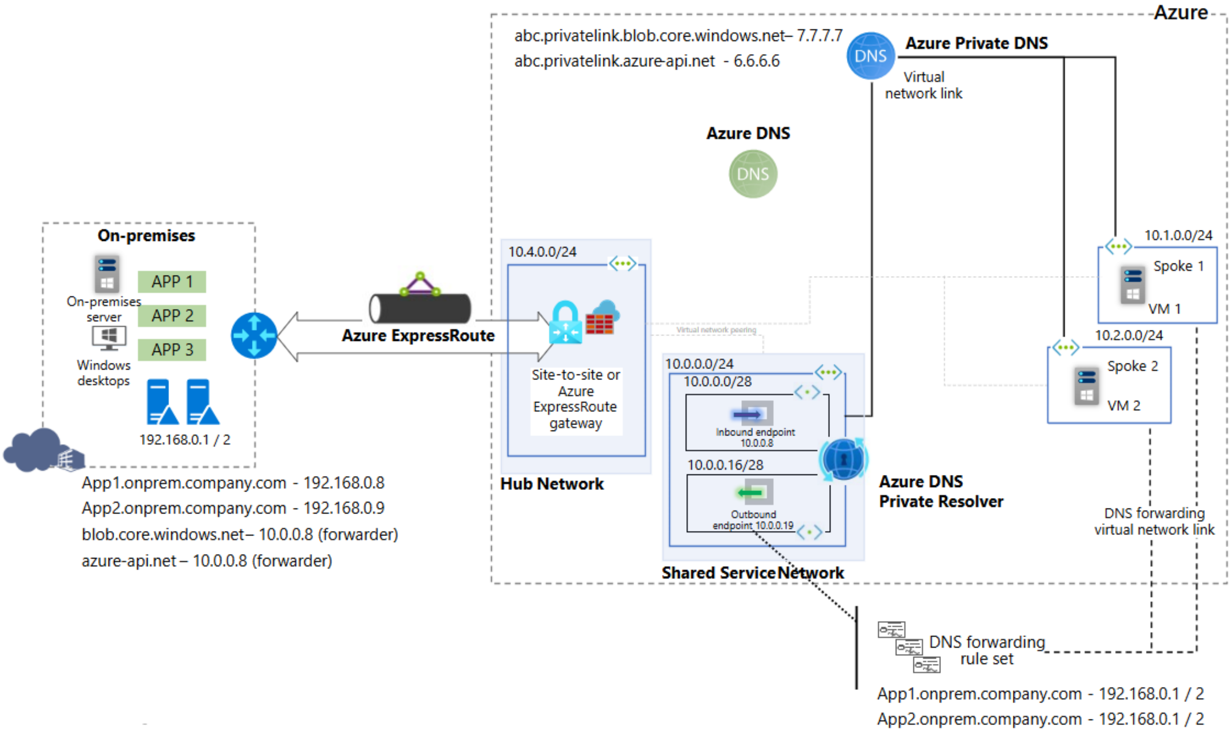
Azure
abc.privatelink.blob.core.windows.net– 7.7.7.7
abc.privatelink.azure-api.net - 6.6.6.6
DNS
Azure Private DNS
Virtual network link
Azure DNS
DNS
On-premises
On-premises server
APP 1
APP 2
APP 3
Windows desktops
192.168.0.1 / 2
App1.onprem.company.com - 192.168.0.8
App2.onprem.company.com - 192.168.0.9
blob.core.windows.net– 10.0.0.8 (forwarder)
azure-api.net – 10.0.0.8 (forwarder)
Azure ExpressRoute
10.4.0.0/24
Site-to-site or Azure ExpressRoute gateway
Hub Network
Virtual network peering
10.0.0.0/24
10.0.0.0/28
Inbound endpoint 10.0.0.8
10.0.0.16/28
Outbound endpoint 10.0.0.19
Shared Service Network
Azure DNS Private Resolver
10.1.0.0/24
Spoke 1
VM 1
10.2.0.0/24
Spoke 2
VM 2
DNS forwarding virtual network link
DNS forwarding rule set
App1.onprem.company.com - 192.168.0.1 / 2
App2.onprem.company.com - 192.168.0.1 / 2

Figure 2: Architecture of a private DNS resolver deployed in spoke network

Flow of on-premises DNS query using private DNS resolver:

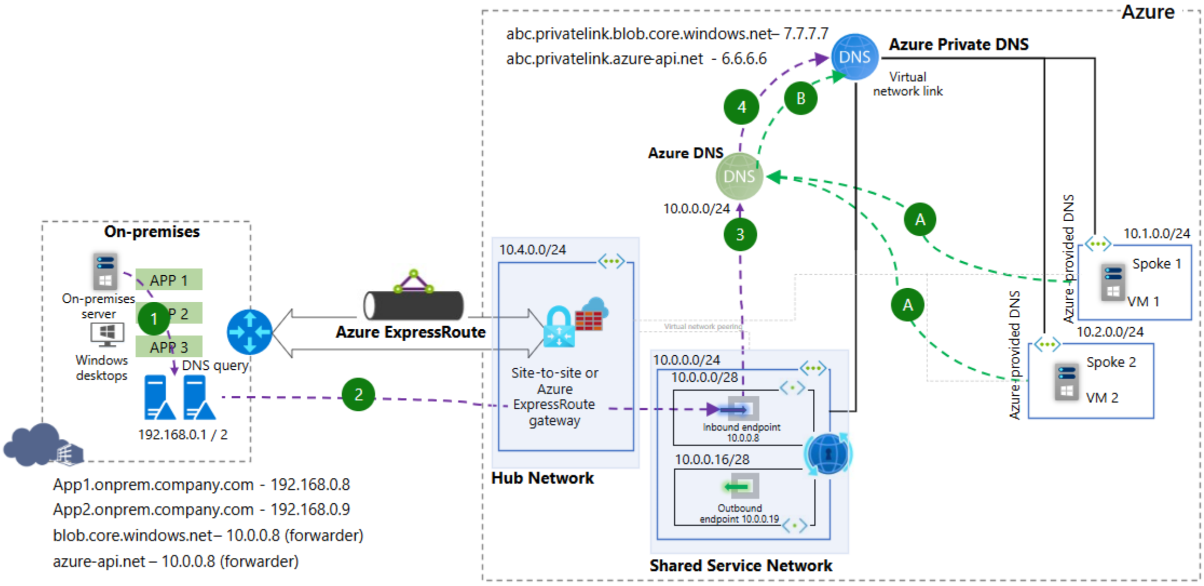

Figure 3: Flow of on-premises DNS query

- An on-premises server initiates a DNS query to resolve a private Azure DNS service record such as blob.core.windows.net. The request is first directed to the local DNS server configured at IP addresses 192.168.0.1 or 192.168.0.2, which serves as the primary DNS resolution point for all on-premises systems.
- A conditional forwarder is configured on the local DNS server to handle queries for blob.core.windows.net, ensuring that such requests are forwarded to the Azure DNS Private Resolver at IP address 10.0.0.8.
- The DNS Private Resolver then queries the Azure DNS and retrieves information regarding the associated Azure Private DNS Zone and its virtual network link.
- The Azure Private DNS service processes and resolves the query by interfacing with Azure Public DNS, directing the request through the inbound endpoint of the DNS Private Resolver, thereby enabling a seamless private name resolution for hybrid network environments.

The following sequence illustrates the traffic flow when Virtual Machine (VM) 1 initiates a DNS query through an Azure DNS Private Resolver inbound endpoint. In this scenario, the request originates from the Spoke 1 virtual network, which is configured to use a Private DNS Resolver for name resolution. Upon receiving the query, the Private DNS Resolver processes the request based on defined forwarding rules and resolution policies within the hybrid cloud environment. This ensures that DNS queries are handled appropriately, whether they require resolution within Azure Private DNS zones or need to be forwarded to an external DNS server based on predefined conditional forwarding rules.

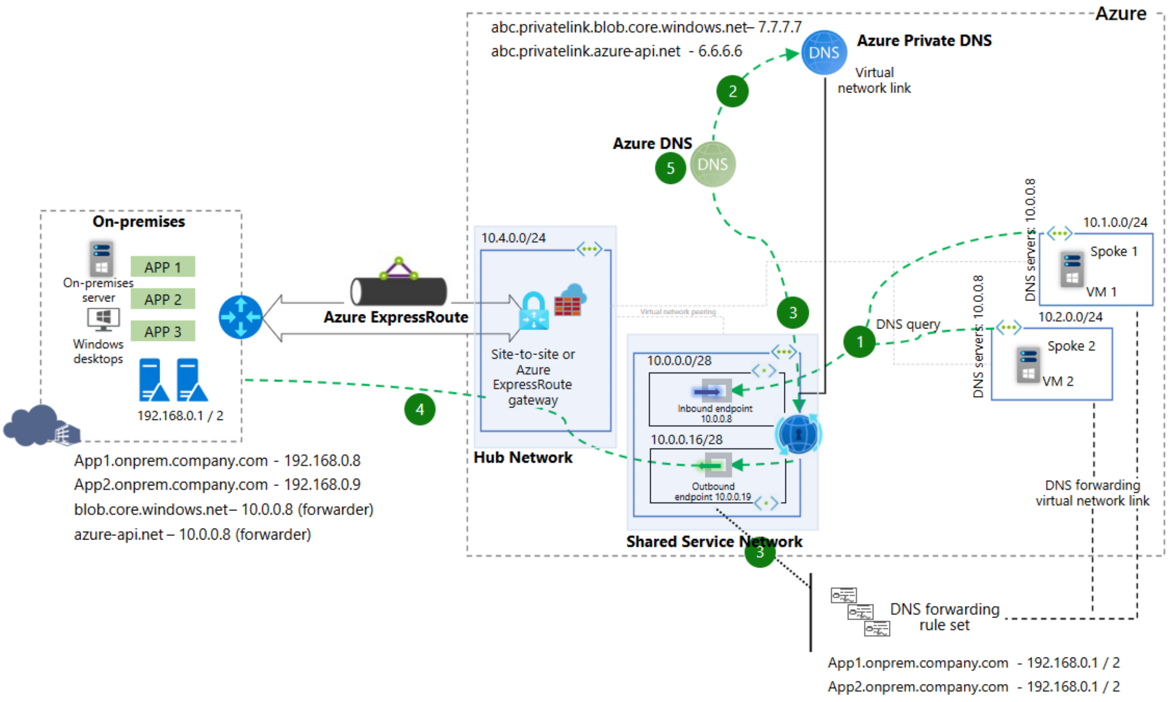
Azure
abc.privatelink.blob.core.windows.net– 7.7.7.7
abc.privatelink.azure-api.net - 6.6.6.6
DNS
Azure Private DNS
Virtual network link
2
Azure DNS
5
DNS
On-premises
On-premises server
APP 1
APP 2
APP 3
Windows desktops
192.168.0.1 / 2
Azure ExpressRoute
10.4.0.0/24
Site-to-site or Azure ExpressRoute gateway
Hub Network
Virtual network peering
3
1
DNS query
4
10.0.0.0/28
Inbound endpoint 10.0.0.8
10.0.0.16/28
Outbound endpoint 10.0.0.19
Shared Service Network
3
DNS servers: 10.0.0.8
10.1.0.0/24
Spoke 1
VM 1
DNS servers: 10.0.0.8
10.2.0.0/24
Spoke 2
VM 2
DNS forwarding virtual network link
DNS forwarding rule set
App1.onprem.company.com - 192.168.0.1 / 2
App2.onprem.company.com - 192.168.0.1 / 2
App1.onprem.company.com - 192.168.0.8
App2.onprem.company.com - 192.168.0.9
blob.core.windows.net– 10.0.0.8 (forwarder)
azure-api.net – 10.0.0.8 (forwarder)

Figure 4: Flow of a virtual machine DNS query via DNS resolver outbound endpoint

- When Virtual Machine (VM) 1 initiates a DNS query within a spoke virtual network, the request is directed to the Azure DNS Private Resolver, which has been designated as the primary name resolution service at IP address 10.0.0.8. The Azure Private DNS Resolver then processes the query through a structured resolution workflow to determine the appropriate response.
- If the requested domain name corresponds to a private DNS record, the Azure Private DNS Service is contacted to retrieve the necessary resolution information. However, if the queried domain does not match any private DNS zones linked to the virtual network, Azure DNS automatically forwards the request to the DNS Private Resolver. Because Spoke 1 has an established virtual network link, the resolver examines any associated DNS forwarding rule sets to determine whether a forwarding rule applies to the domain being queried.
- If the DNS forwarding rule set contains a matching entry, then the query is relayed to the outbound endpoint and forwarded to the target DNS server defined in the rule set. The forwarding rule configuration includes specific domain names, destination IP addresses, and designated ports, thereby ensuring conditional DNS query redirection to the appropriate external DNS infrastructure.
- If no match is found within the private DNS service or DNS Private Resolver, the query is ultimately resolved by Azure DNS, which serves as the fallback resolution mechanism.

Traditionally, achieving DNS resolution between on-premises networks and Azure requires deploying DNS forwarder virtual machines within Azure VNets. These VMs act as intermediaries, forwarding queries between on-premises DNS servers and Azure's DNS infrastructure. This setup introduces additional complexity, potential points of failure, and increased maintenance efforts.

The Azure DNS Private Resolver streamlines this architecture by providing a native, fully managed solution that replaces the need for DNS forwarder VMs. By integrating directly with Azure VNets and supporting conditional forwarding rules, it ensures efficient and secure DNS resolution across hybrid environments without the associated overhead of managing the additional infrastructure.

IV. CONCLUSION

The Azure DNS Private Resolver represents a significant advancement in hybrid cloud networking, addressing the complexities associated with traditional DNS forwarder virtual machines (VMs). By eliminating the necessity for custom DNS forwarding infrastructure, this fully managed service enhances scalability, security, and operational efficiency. The capability to establish bidirectional DNS resolution between on-premises networks and Azure ensures seamless name resolution, while reducing latency and administrative overhead. The integration of inbound and outbound endpoints within an Azure Virtual Network (VNet) facilitates DNS query management, ensuring that Azure resources can resolve on-premises domain names and vice versa. Furthermore, the hub-spoke topology recommended for Azure landing zone architectures reinforces network segmentation, security, and scalability, rendering the Azure DNS Private Resolver a preferred solution for enterprise hybrid cloud deployments. The cost-effectiveness of removing DNS forwarder VMs, coupled with built-in redundancy and performance optimization, further solidifies its role as a strategic component in hybrid cloud architectures. This paper provides a comprehensive analysis of Azure DNS Private Resolver's architecture, benefits, deployment strategies, and security implications, demonstrating its viability as an optimal solution for hybrid DNS resolution. Future research could explore the impact of AI-driven automation in DNS query optimization, assess performance improvements in large-scale hybrid environments, and investigate the best practices for multi-cloud DNS resolution. As enterprises continue to adopt cloud-centric infrastructure, solutions such as Azure DNS Private Resolver will remain critical in ensuring efficient, secure, and scalable DNS resolution across hybrid cloud environments.

References

[1] Soh, J., Copeland, M., Puca, A., Harris, M. (2020). Overview of Azure Platform as a Service. In: Microsoft Azure. Apress, Berkeley, CA. https://doi.org/10.1007/978-1-4842-5958-0_3
[2] Copeland, M., Soh, J., Puca, A., Manning, M., Gollob, D. (2015). Extending Your Network with Azure. In: Microsoft Azure. Apress, Berkeley, CA. https://doi.org/10.1007/978-1-4842-1043-7_8
[3] Mazumdar, P., Agarwal, S., Banerjee, A. (2016). Microsoft Azure Networking. In: Pro SQL Server on Microsoft Azure . Apress, Berkeley, CA. https://doi.org/10.1007/978-1-4842-2083-2_4
[4] Toroman, Mustafa. *Azure Networking Cookbook: Practical recipes to manage network traffic in Azure, optimize performance, and secure Azure resources*. Packt Publishing Ltd, 2019.https://books.google.com/books?id=sc6PDwAAQBAJ&lpg=PP1&ots=6yLLy6hclx&dq=azure%20DNS&lr&pg=PP2#v=snippet&q=azure%20DNS&f=false
[5] Wali, Mohamed. *Hands-On Networking with Azure: Build large-scale, real-world apps using Azure networking solutions*. Packt Publishing Ltd, 2018 https://books.google.com/books?id=L5RRDwAAQBAJ
[6] Copeland, Marshall, Matthew Jacobs, Marshall Copeland, and Matthew Jacobs. "Azure Network Security Configuration." *Cyber Security on Azure: An IT Professional's Guide to Microsoft Azure Security* (2021): 37-81 https://doi.org/10.1007/978-1-4842-6531-4
[7] https://learn.microsoft.com/en-us/azure/architecture/networking/architecture/azure-dns-private-resolver