Assignment - 12

DNS Zone

Add Custom DNS server in virtual Network

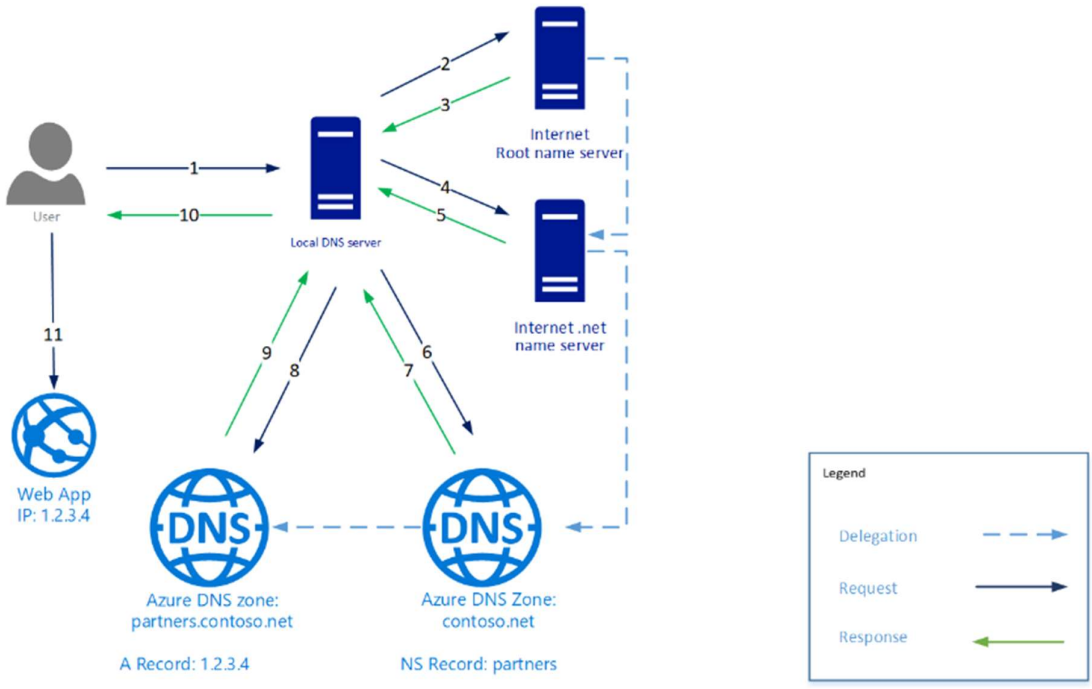
Ananya Srivastava
CLOUD INFRA

Table of Contents

Introduction

In the realm of cloud computing, efficient and reliable name resolution is paramount for seamless operations and communication between resources. Microsoft Azure, a leading cloud service provider, offers robust networking capabilities that include the configuration of Domain Name System (DNS) settings within virtual networks (VNets). By default, Azure provides internal DNS name resolution services for virtual machines (VMs) deployed in a VNet. However, certain scenarios necessitate the use of custom DNS servers, whether for enhanced control, compliance requirements, or integration with on-premises infrastructure.

This document aims to provide an in-depth understanding of how to add a custom DNS server to an Azure virtual network. We will explore the prerequisites, step-by-step procedures, and common scenarios where custom DNS servers prove beneficial. Additionally, we will discuss best practices for configuration and troubleshooting tips to ensure smooth DNS operations within your virtual network.



Custom DNS servers are particularly useful in hybrid cloud environments where on-premises DNS servers need to resolve names for resources in Azure, or vice versa. They also come in handy when there is a need for advanced DNS features such as DNSSEC, custom DNS records, or integration with existing DNS infrastructures that are not natively supported by Azure's internal DNS.

The process of configuring a custom DNS server involves creating a virtual network, specifying DNS server IP addresses, and validating the configuration to ensure proper name resolution. Throughout this document, we will guide you through these steps with detailed

instructions and screenshots, making it easy for you to implement and manage custom DNS settings in your Azure environment.

Moreover, we will delve into the benefits of using custom DNS servers, such as improved security, control over DNS records, and the ability to implement organization-specific DNS policies. We will also highlight best practices to follow when configuring custom DNS servers to avoid common pitfalls and ensure high availability and performance.

In summary, this document is designed to be a comprehensive guide for IT professionals, network administrators, and cloud architects who are responsible for managing DNS in Azure. By the end of this guide, you will have a clear understanding of how to add and manage custom DNS servers in an Azure virtual network, along with practical insights to optimize your DNS configuration for various use cases.

Prerequisites

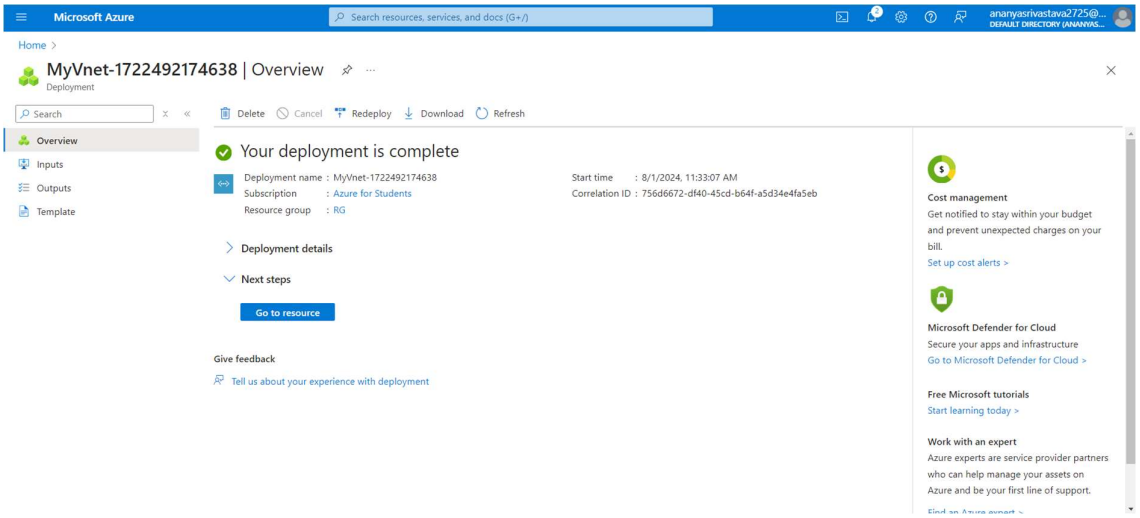
Before configuring a custom DNS server in an Azure virtual network, ensure that you have the following prerequisites:

1. An active Azure subscription.
2. Proper permissions to create and manage virtual networks.
3. A custom DNS server with a static IP address.
4. Basic understanding of Azure networking concepts.

Steps to Add a Custom DNS Server

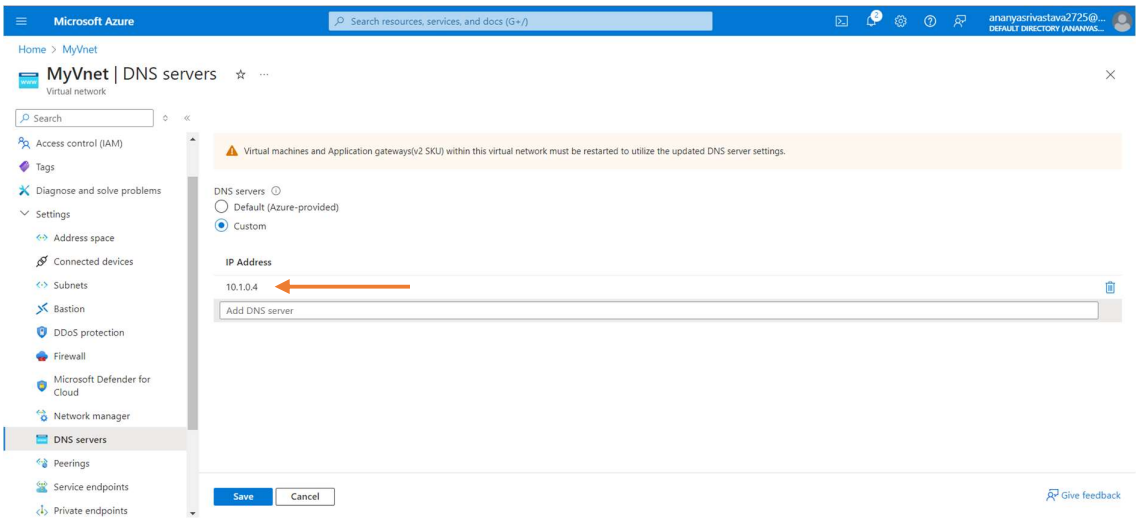
1. Create a Virtual Network

1.1 Navigate to the Azure portal.
1.2 In the left-hand menu, select "Create a resource".
1.3 Choose "Networking" and then select "Virtual Network".
1.4 Fill in the required fields (Name, Address space, Subnet, Resource group, Location) and click "Review + create".
1.5 Click "Create" to deploy the virtual network.



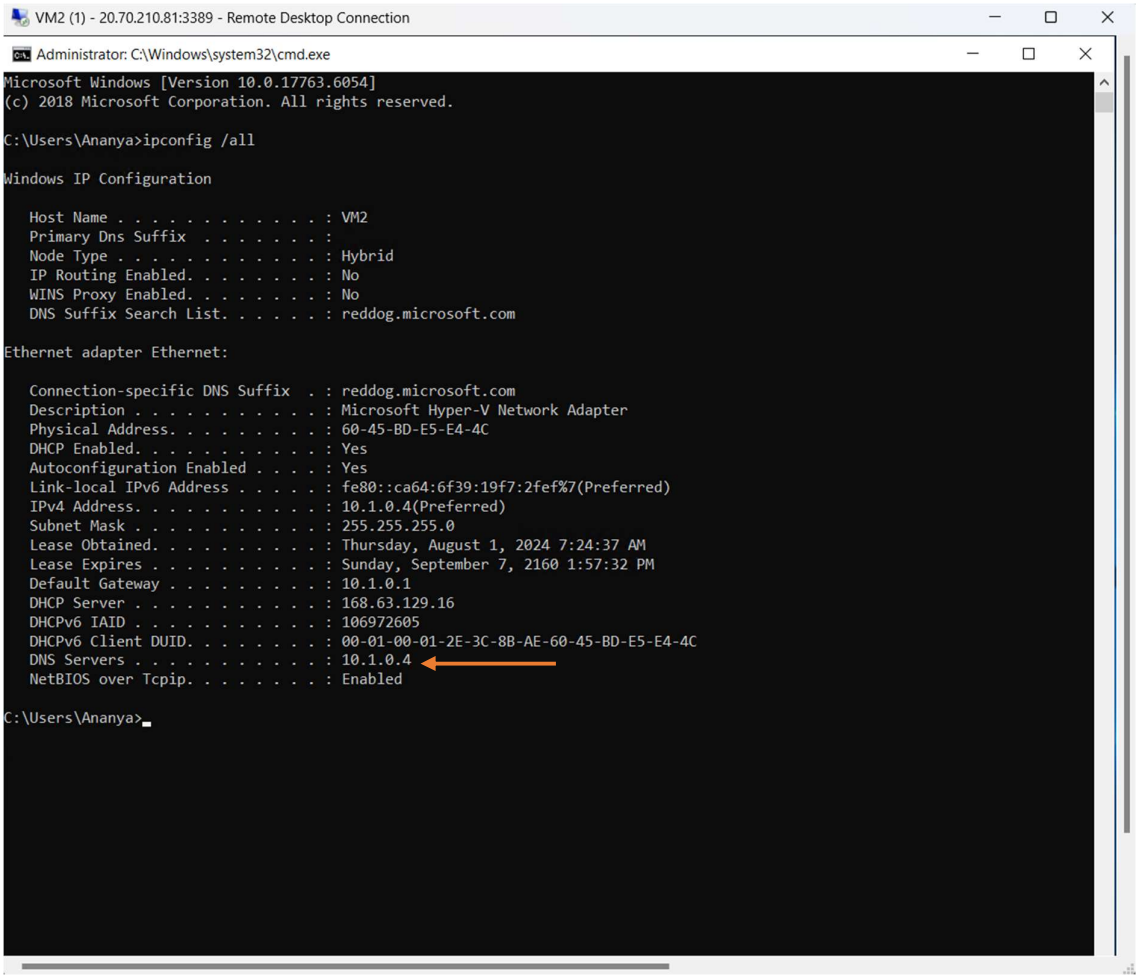
2. Configure DNS Settings

2.1 In the Azure portal, go to "Virtual networks".
2.2 Select the virtual network you created.
2.3 Under "Settings", select "DNS servers".
2.4 Choose "Custom" and enter the IP address of your custom DNS server.
2.5 Click "Save" to apply the changes.



3. Validate DNS Server Configuration

3.1 Deploy a virtual machine in the virtual network.
3.2 Connect to the VM and configure its DNS settings to use the custom DNS server.
3.3 Test name resolution using nslookup or a similar tool to ensure the custom DNS server is resolving names correctly.



Custom DNS server IP address **10.1.0.4** is listed in the output, the configuration is verified successfully.

Common Scenarios for Custom DNS Servers

- Hybrid cloud environments requiring integration with on-premises DNS.
- Organizations needing advanced DNS features not supported by Azure's internal DNS.
- Environments with specific compliance requirements for DNS configurations.

- Scenarios requiring DNS resolution across multiple cloud providers.

Benefits of Using Custom DNS Servers

- Enhanced control over DNS records and name resolution.
- Improved security through custom DNS policies and configurations.
- Integration with existing DNS infrastructure and services.
- Ability to implement DNS features such as DNSSEC.

Best Practices

- Use a high-availability DNS server setup to prevent single points of failure.
- Regularly update and patch your custom DNS servers.
- Monitor DNS server performance and logs for issues.
- Document DNS configurations and changes for future reference.

Troubleshooting

- Ensure the custom DNS server is reachable from the virtual network.
- Verify the DNS server IP address is correctly configured in the virtual network settings.
- Check firewall and network security group (NSG) rules to allow DNS traffic.
- Use diagnostic tools like nslookup to test name resolution.

Conclusion

Adding a custom DNS server to an Azure virtual network provides greater control and flexibility over DNS name resolution, especially in complex and hybrid environments. By following the steps outlined in this document, you can easily configure and validate a custom DNS server in your virtual network. Additionally, understanding the benefits, best practices, and troubleshooting tips will help you maintain a robust and reliable DNS infrastructure in Azure.

References

1. Microsoft Azure Documentation: Virtual Network DNS - https://learn.microsoft.com/en-us/azure/virtual-network/virtual-networks-name-resolution-for-vms-and-role-instances?tabs=redhat
2. Azure CLI Reference - https://learn.microsoft.com/en-us/azure/firewall/dns-settings?tabs=browser
3. Best Practices for DNS in Azure - https://learn.microsoft.com/en-us/azure/security/fundamentals/network-best-practices
4. nslookup Command Reference - https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/nslookup
5. Youtube - https://youtu.be/OSUhnt6GxIg?si=9dxkxV6FCA4Yi3ds