😊 Private DNS

Azure Private DNS Zone is a service provided by Microsoft Azure that allows you to create a private domain in Azure's DNS system. This domain can be used to provide name resolution for resources within a virtual network (VNet) or between peered VNets.

Key Features and Benefits:

1. **Private DNS Name Resolution:** Allows you to resolve the names of resources in your virtual network without the need for public internet DNS.
2. **Integration with Azure Resources:** Seamlessly integrates with Azure Virtual Networks (VNets), Virtual Machine Scale Sets, and other Azure resources.
3. **Custom DNS Names:** You can define custom domain names (e.g., contoso.local) and map them to Azure resources.
4. **Centralized DNS Management:** Provides a central location to manage DNS settings for Azure resources, reducing the overhead of managing multiple DNS configurations.
5. **DNS Traffic Routing:** Helps in routing DNS queries between virtual networks when they are peered together, ensuring consistent name resolution across interconnected VNets.
6. **Security and Isolation:** Keeps DNS traffic within the Azure backbone network, enhancing security by avoiding exposure to the public internet.

😄 Use Cases:

1. **Private Domains for Azure Resources:** Use private DNS zones to define custom domain names for Azure VMs, Azure SQL Databases, Azure Storage accounts, etc., within a VNet.
2. **Centralized DNS Management:** Simplify DNS management by consolidating DNS configurations for various Azure resources under a single private DNS zone.
3. **Cross-VNet Name Resolution:** Facilitate name resolution across peered VNets without exposing internal resource names to the public internet.

🤔 What are we doing in this lab?

In this lab, you're expanding the initial infrastructure by introducing additional components and configurations. Here's a summary of the key steps and objectives:

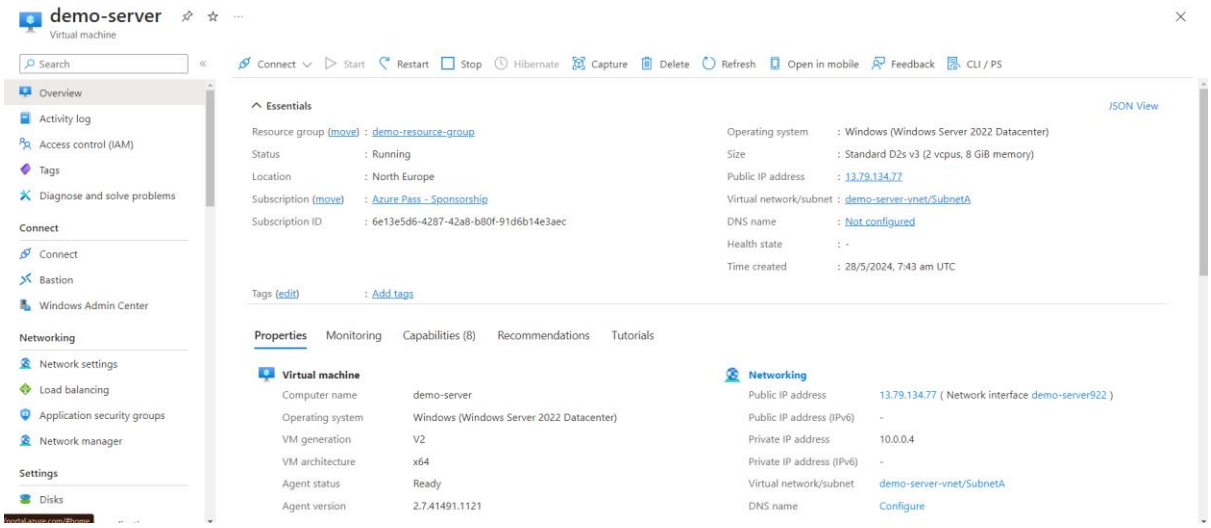
1. **VM Setup**:
    - **Demo Server VM**: A virtual machine with a public IP address, acting as the primary access point.
    - **Web Server VM**: A virtual machine without a public IP address, hosting IIS with a default HTML page. This setup can be done directly using a custom script extension or by manually installing IIS after temporarily assigning a public IP address.

2. **Private DNS Zone Configuration**:
    - Creation of a private DNS zone to manage internal domain name resolution within the virtual network.
    - Linking the virtual network to the DNS zone and auto-registering the demo and web servers, allowing internal access to the web server via a domain name (e.g., web-server.cloudservices.com).
3. **Peering and Additional VM**:
    - Deployment of a new VM (Test Server) in a separate virtual network with a public IP address.
    - Establishing a virtual network peering connection between the Test Server's network and the existing network, enabling communication between VMs across different networks.
4. **Testing and Validation**:
    - Validating access to the web page hosted on the web server via the private DNS name and private IP address from different VMs, including the newly added Test Server VM.

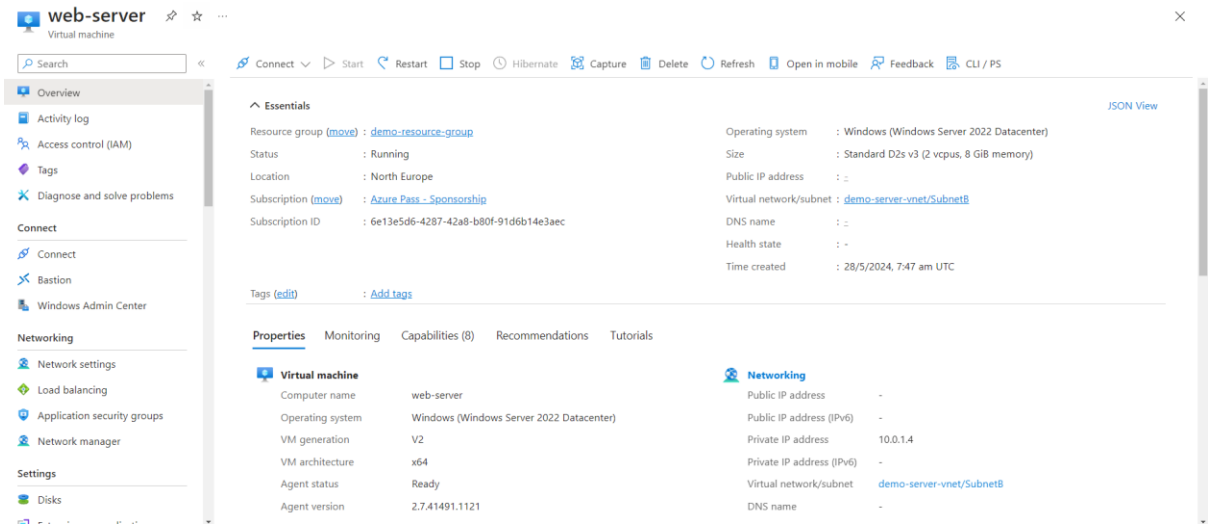
End Goal: The objective is to create a secure and internally accessible web service environment using private IP addresses and DNS, along with demonstrating inter-network communication through virtual network peering. The setup ensures that the web server is accessible only within the private network while still allowing administrative access and management via a public-facing demo server. The use of a private DNS zone enables easy access to internal resources using domain names rather than IP addresses.

😄 To begin with the Lab:

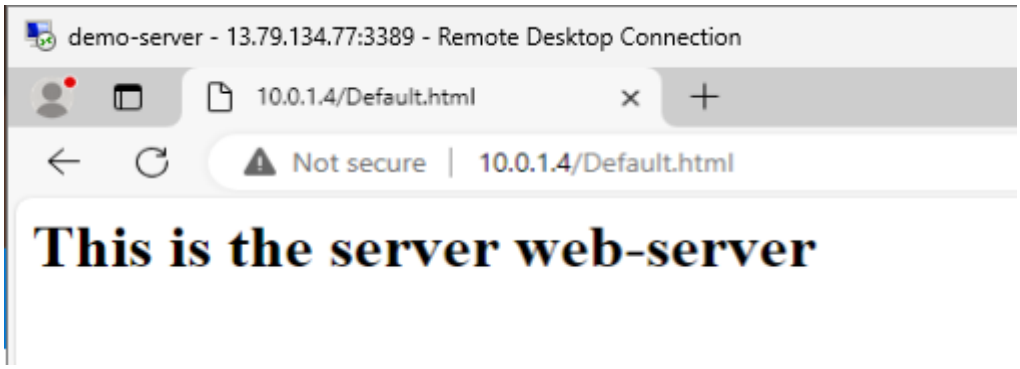
1. In this lab we have launched 2 VMs. One has the Public IP address in which we are going to log in. The second VM does not have any public IP address, it only has a Private IP address, but has IIS installed on it. All in a single Virtual Network.
2. So, you have to prepare all this before you begin. Also, you can use the Setup file to install IIS directly on your second VM or you can create it normally with a public IP address, login to the machine install IIS create a default HTML page, and then come back and delete the public IP address of your second VM. You can use any approach.
3. Below you can see that our one VM is called a demo server with a public IP address, but no IIS installed.



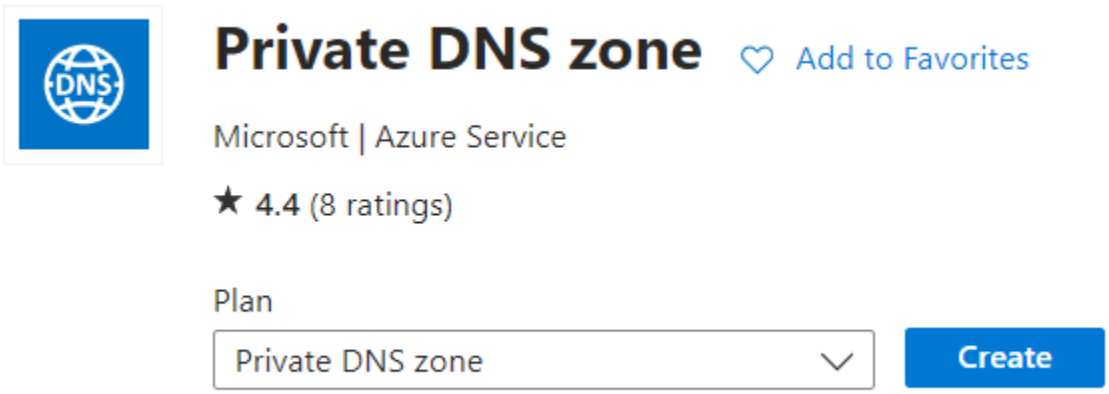
4. Here is your second VM web server. It does not have any public IP address, but IIS is installed on this machine.



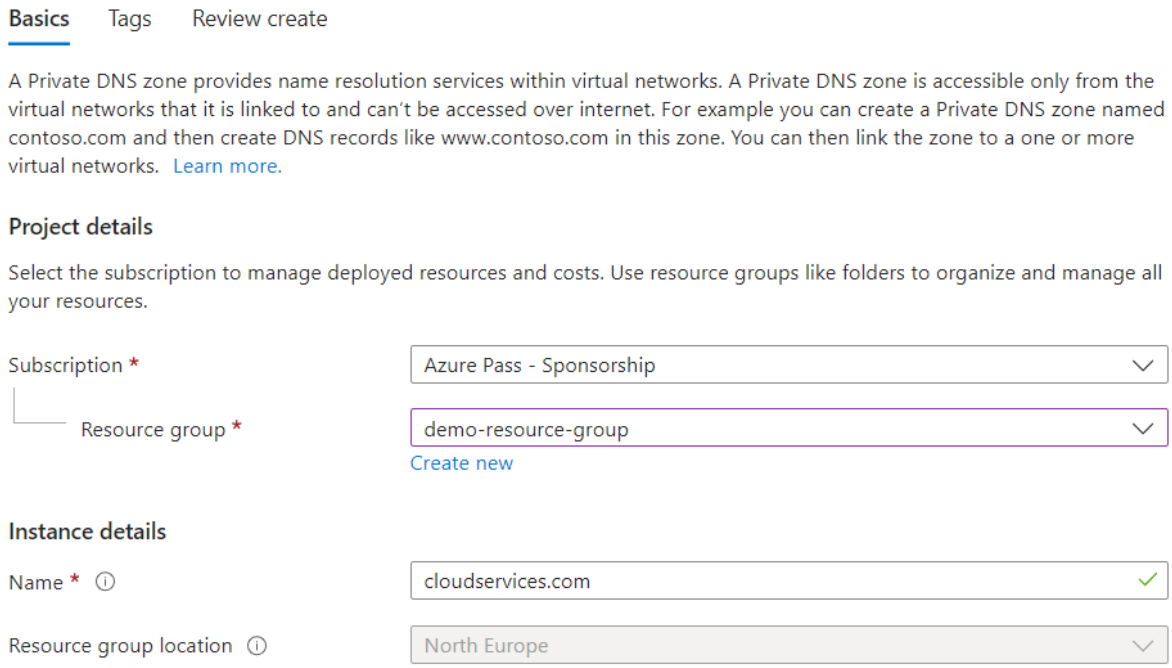
5. Now you need to log in to the demo server VM. Once you are in, if you open the Edge browser and paste the Private IP address of your web server VM then you can see the web page accordingly.



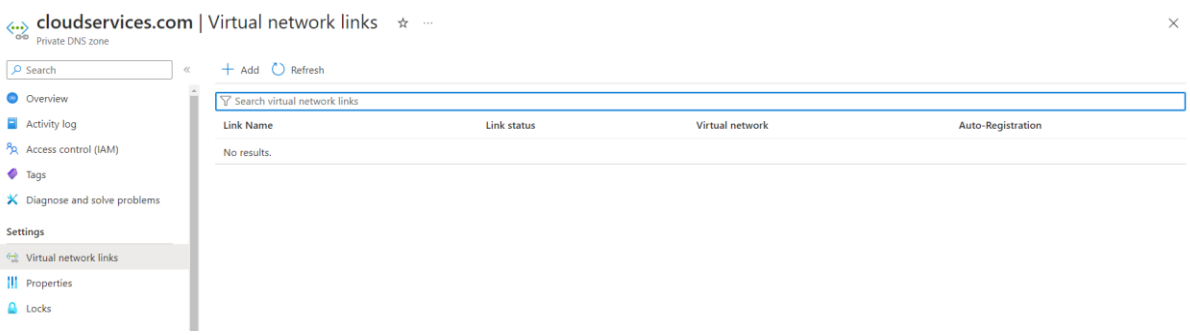
6. Now search the marketplace for a private DNS zone and choose the service accordingly.



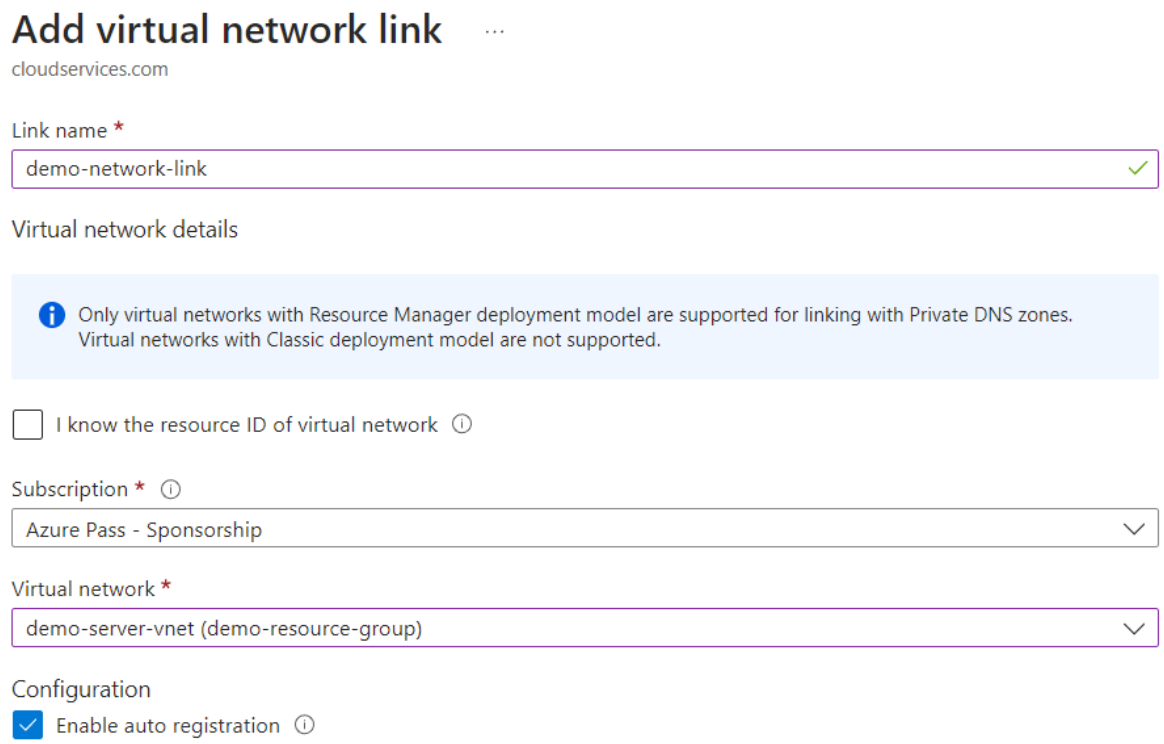
7. Then you need to choose your resource group and give the name of your domain. Also, you don't need to buy any domain name, it is a private DNS zone, and this will be private for our virtual network.



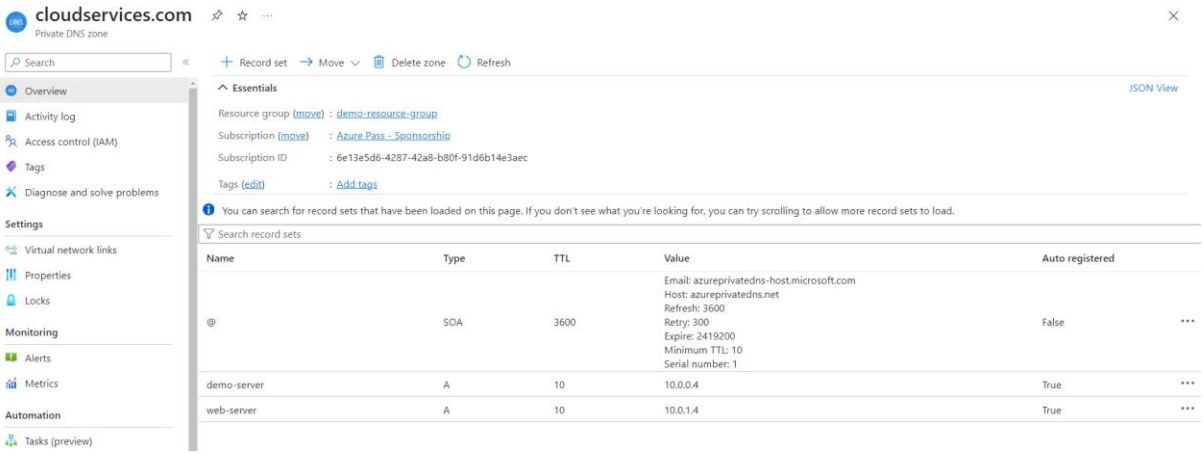
8. Once it is deployed open it and go to virtual network links and then link your network. For that click on add.



9. Now you need to give it a name, choose your virtual network, enable auto registration then click on add.

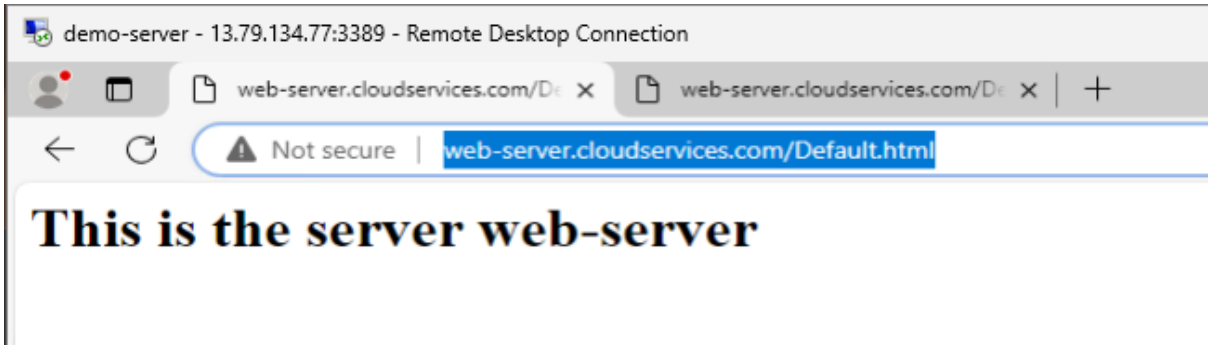


10. Now in your private DNS zone if you go to overview you will see that you have records for the demo server and web server.

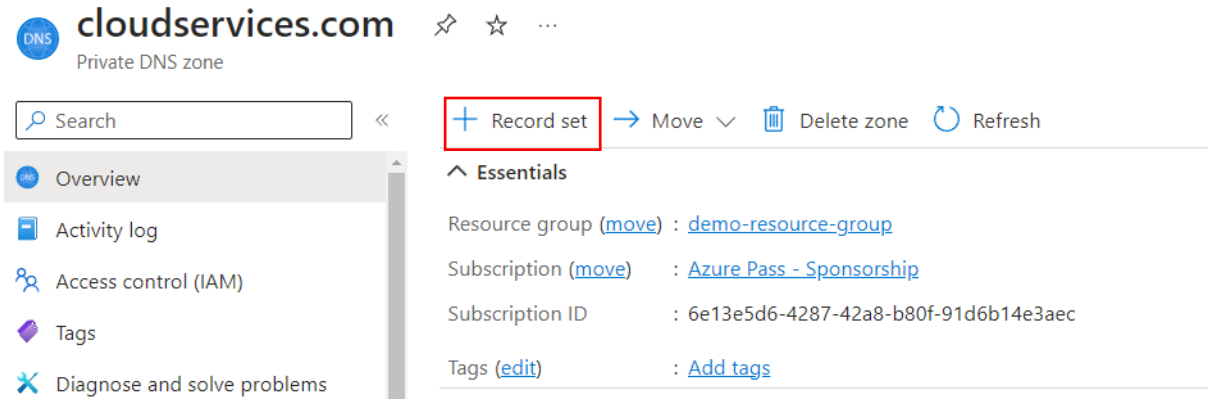


11. Now in your VM if you go and use your domain name to access the web page then you can do that and get the results.

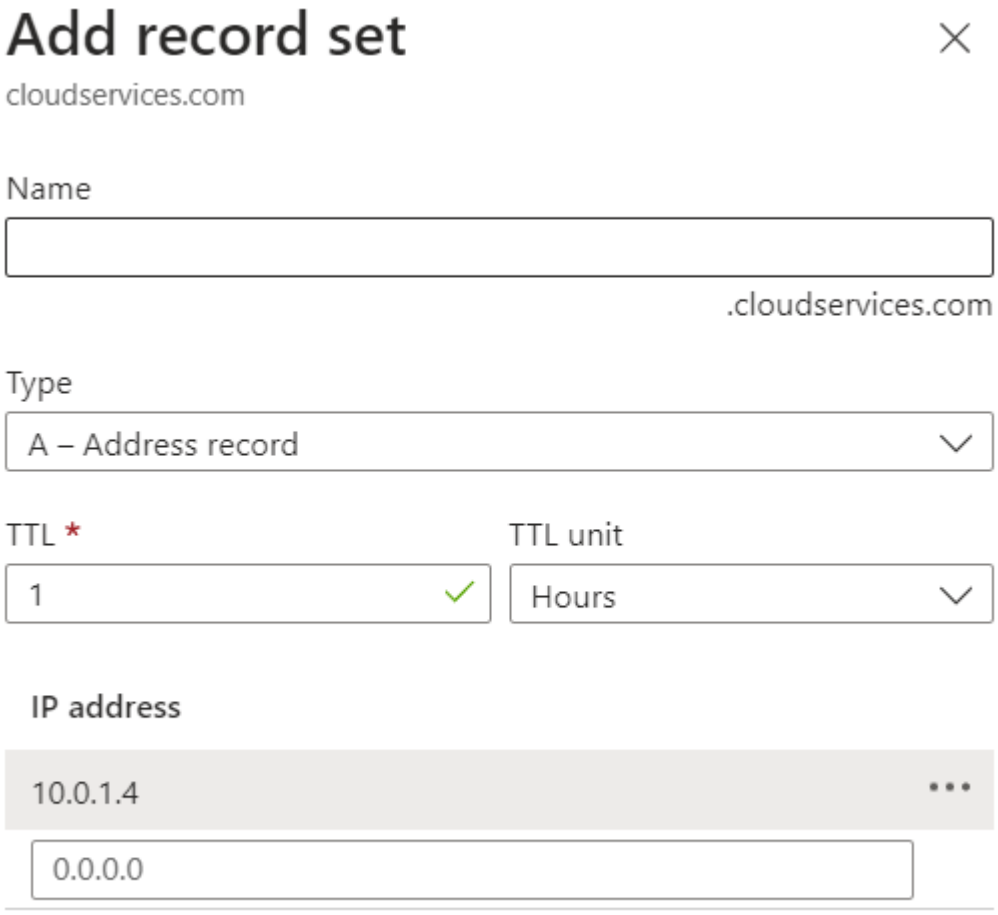
web-server.cloudservices.com/Default.html



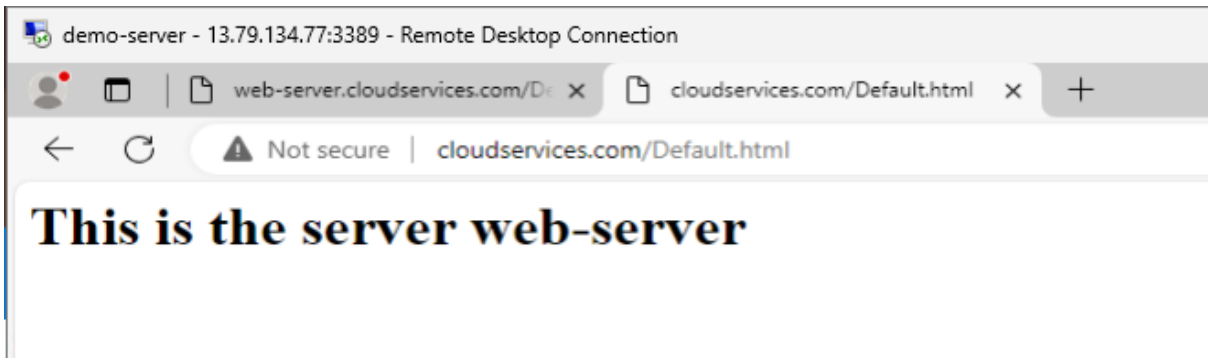
12. Now if you want to have just the domain name to access your web page then go to the overview of private DNS zone and click on add record set.



13. While adding the resource set you don't need to give a name just give the private IP of the web server VM.

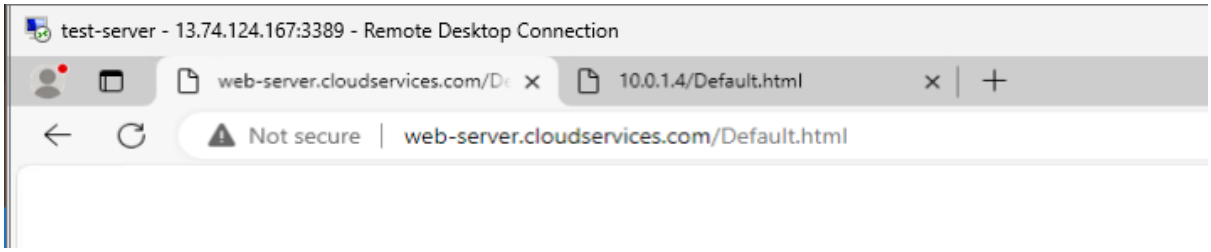


14. Below you can see that you have the results as expected.



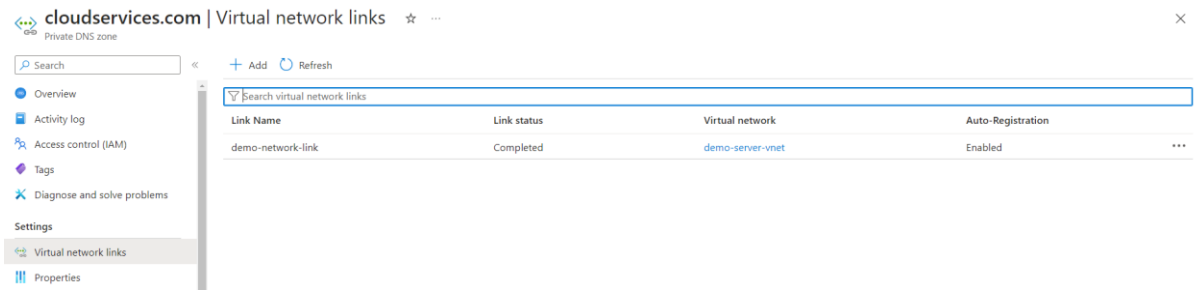
😄 Peered Networks

1. Now we are going to launch another VM **test server** and this VM will have a **new Virtual Network** with a **Public IP address**. Once it is launched then you need to establish a peering connection between the **test server VM** and the **demo server VM**.
2. Once it is all done then log in to the test server VM. In your VM open Edge browser and run this link you will see that the page is going blank.



3. But if use the Private IP address of your web server VM then you will get the result as expected.

4. So, now come to the private DNS zone, go to virtual network links, and click on add to create another.



5. Now give it a name then choose your virtual network as Test server VN. Then enable auto registration.

Add virtual network link

cloudservices.com

Link name *

test-server-link

Virtual network details

Only virtual networks with Resource Manager deployment model are supported for linking with Private DNS zones. Virtual networks with Classic deployment model are not supported.

I know the resource ID of virtual network

Subscription *

Azure Pass - Sponsorship

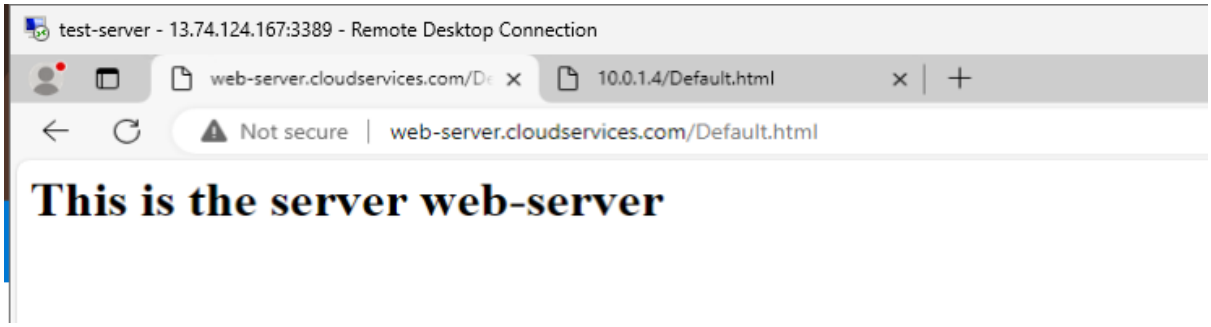
Virtual network *

test-VN (demo-resource-group)

Configuration

Enable auto registration

6. Once it gets added now you need to come back to test VM and refresh the page. You will the results accordingly.



7. Also, on the overview page you can see a record set for test server VM.