	Compte Rendu de Travaux Pratiques

Compte Rendu - Travaux Pratiques En Cloud & Virtualisation

Filière : Réseaux Informatiques & Télécommunications
Niveau : 4ème Année

Sujet :

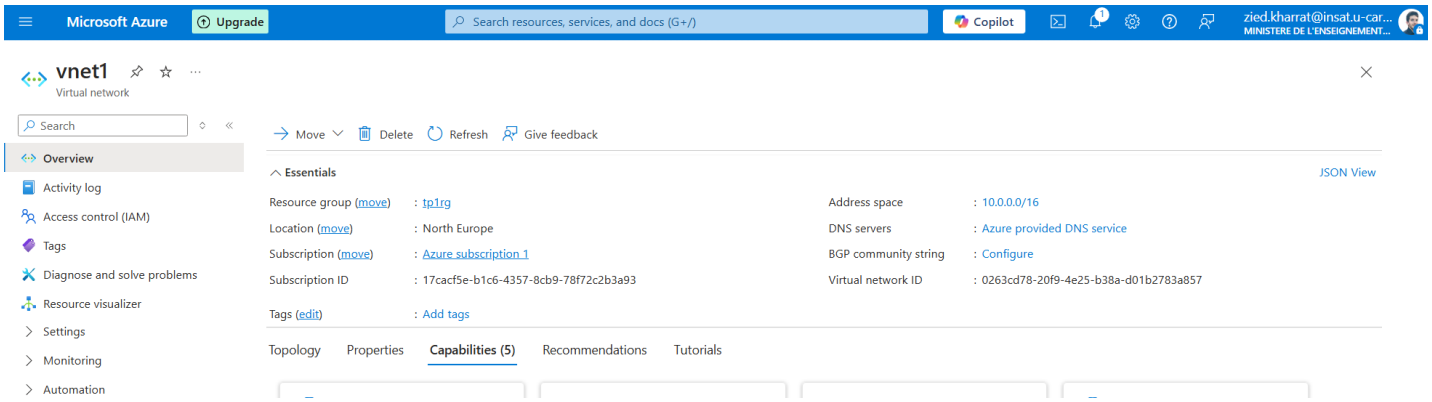
TP1 : Virtual Machines

Réalisé par :

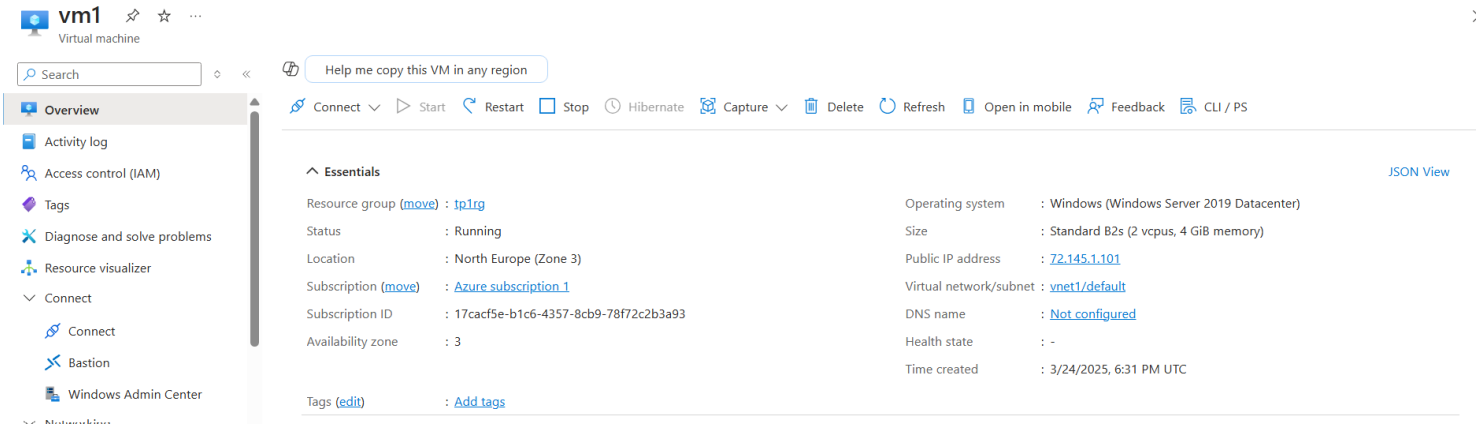
Zied KHARRAT
Nidhal JABNOUNI
Yassine BELARBI

Année Universitaire : 2024-25

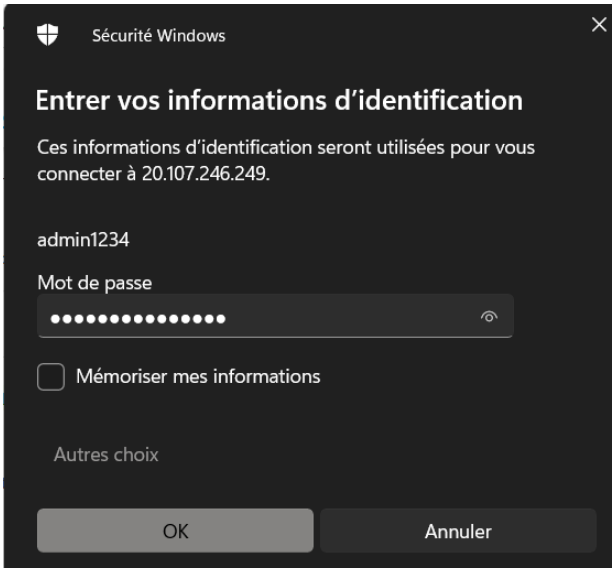
1. We have successfully deployed the Virtual Network vnet1 as part of resource group tp1rg in the North Europe Region.

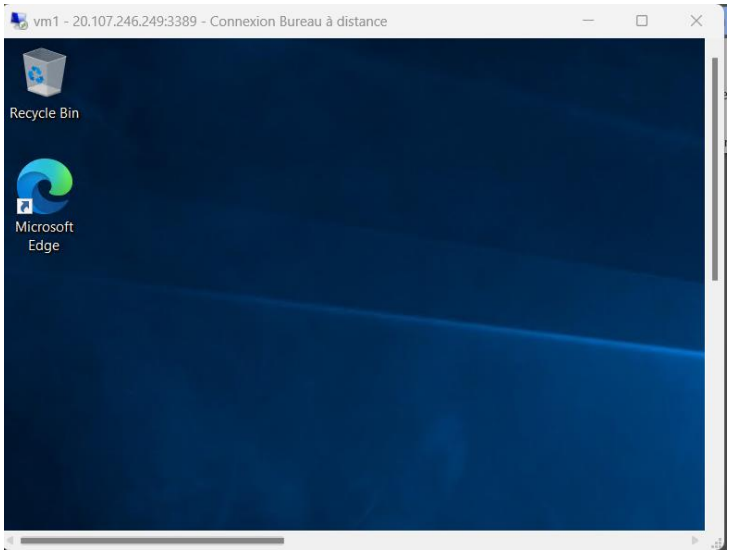


2. We successfully deployed the virtual machine vm1 as part of the newly created virtual network from task 1, with Windows Server 2019 as the image, in the North Europe region, and configured RDP access for remote login.

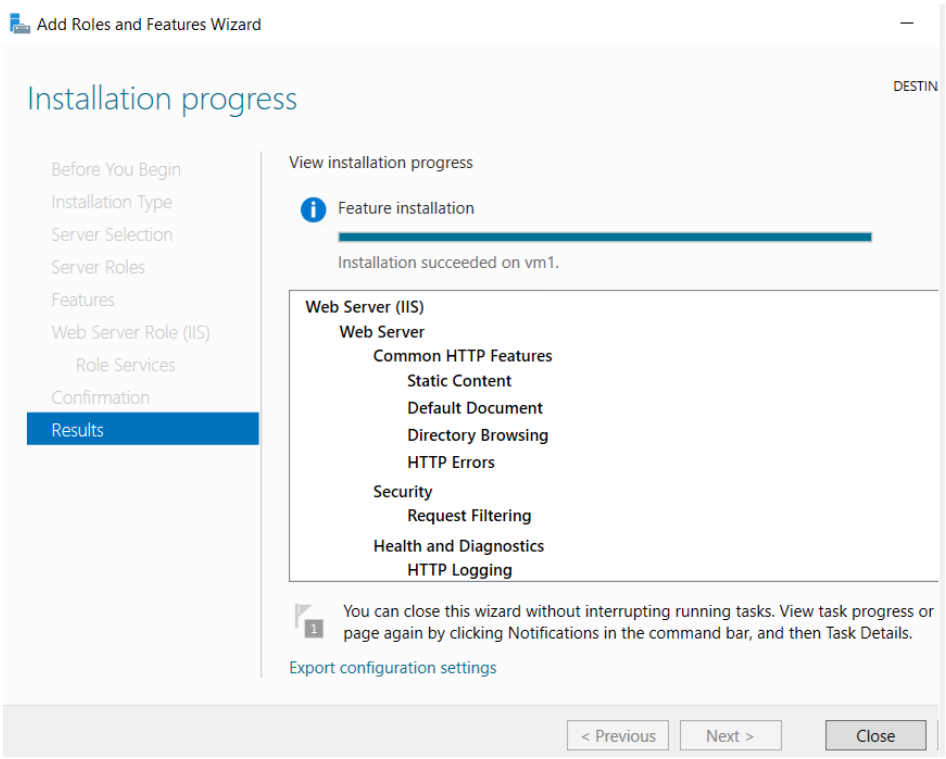


3. We successfully connected to the newly created virtual machine vm1 using RDP, logged in with the provided credentials, and installed the Internet Information Services (IIS) role through Server Manager to set up a web server on the machine.

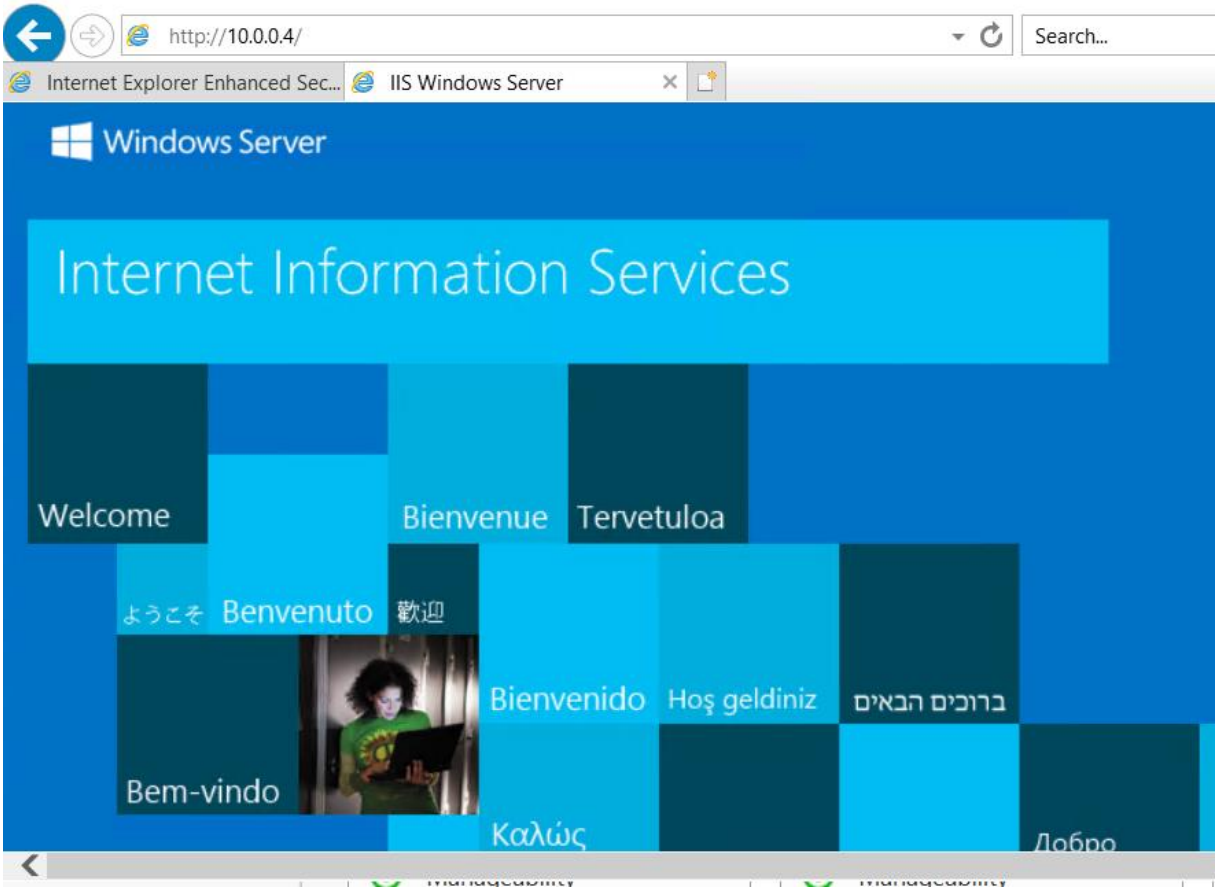




We have successfully installed IIS.



4. We have successfully connected to the VM's private IP and got the IIS welcome page.

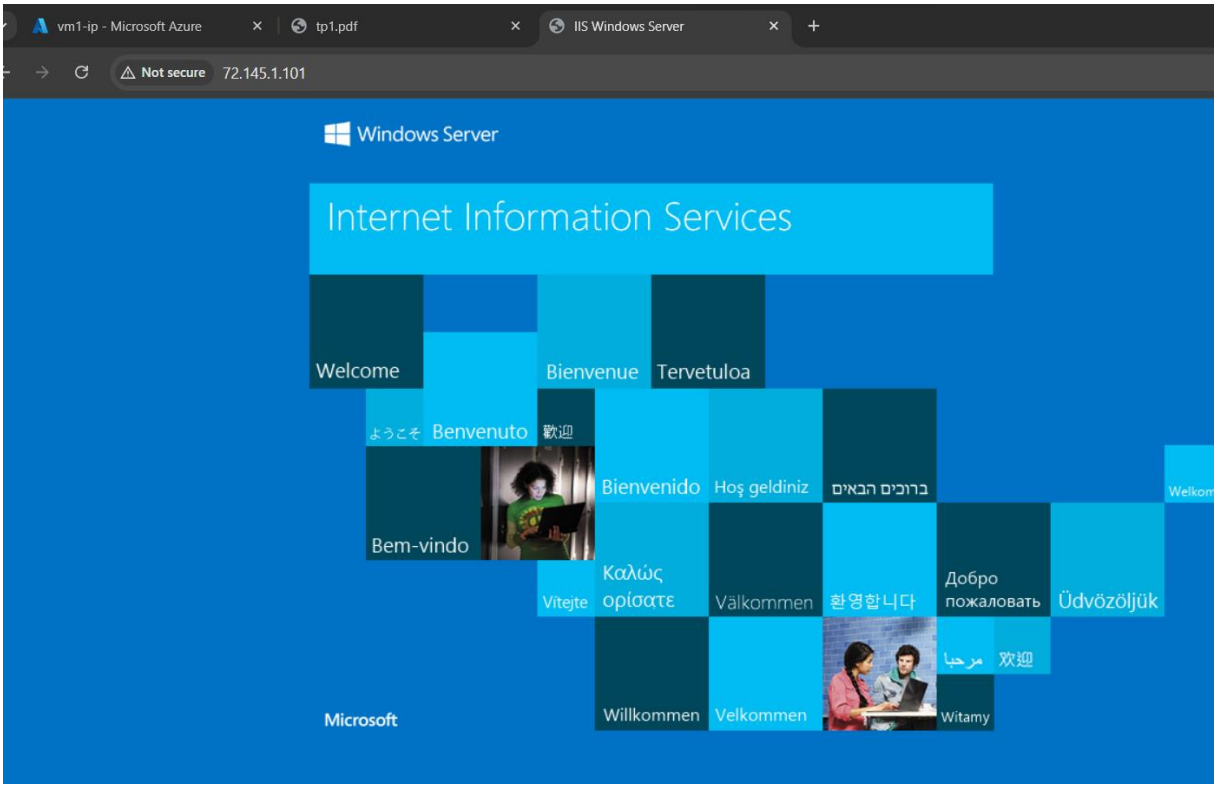


5. We successfully configured the Network Security Group (NSG) by adding an inbound port rule that allows HTTP traffic on port 80, enabling external access to the web server hosted on vm1.

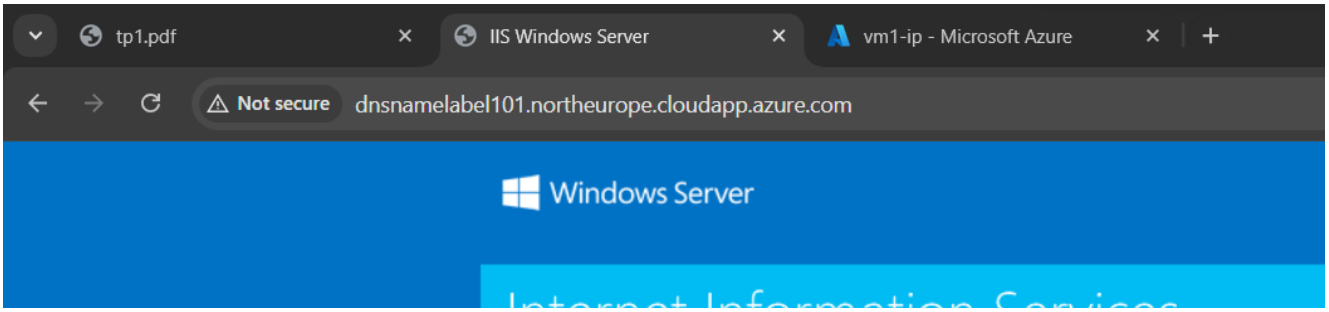
Search rules | Source == all | Destination == all | Protocol == all | Action == all

Priority ↑	Name	Port	Protocol	Source	Destination	Action
Inbound port rules (5)						
300	RDP	3389	TCP	Any	Any	Allow
310	AllowAnyHTTPInbound	80	TCP	Any	Any	Allow

6. We successfully accessed the homepage of our web server meaning our config works.



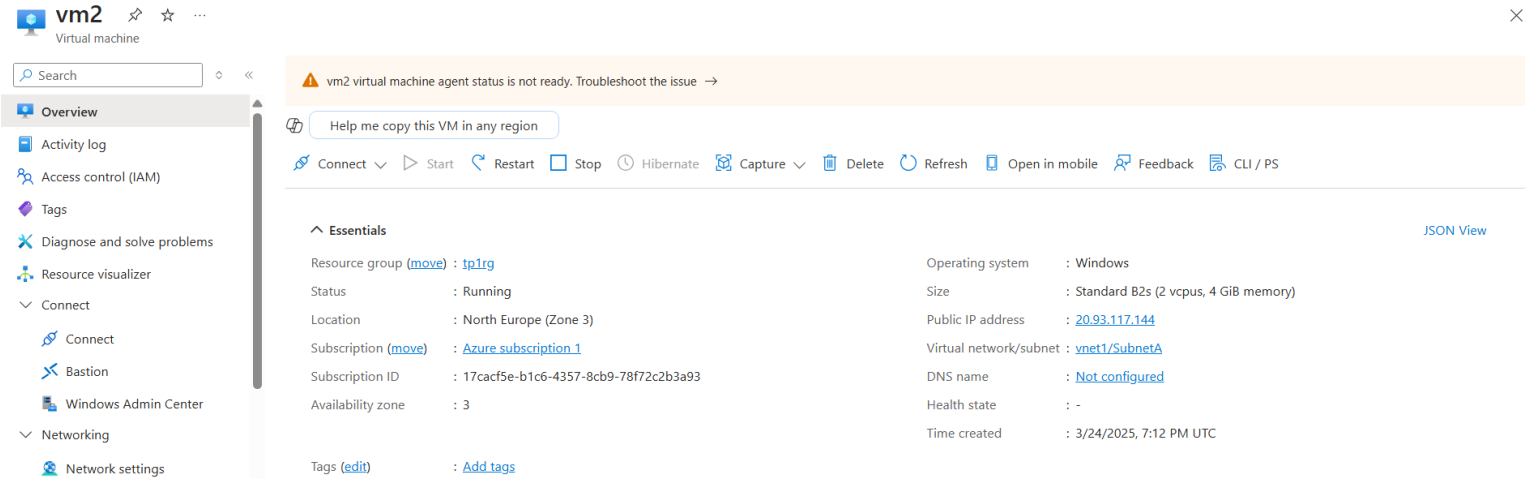
7. We successfully assigned a DNS name label to the virtual machine's public IP address (DNSlabel and dnslabel were not available names.) and verified that the web server is accessible by pasting the generated URL into a web browser.



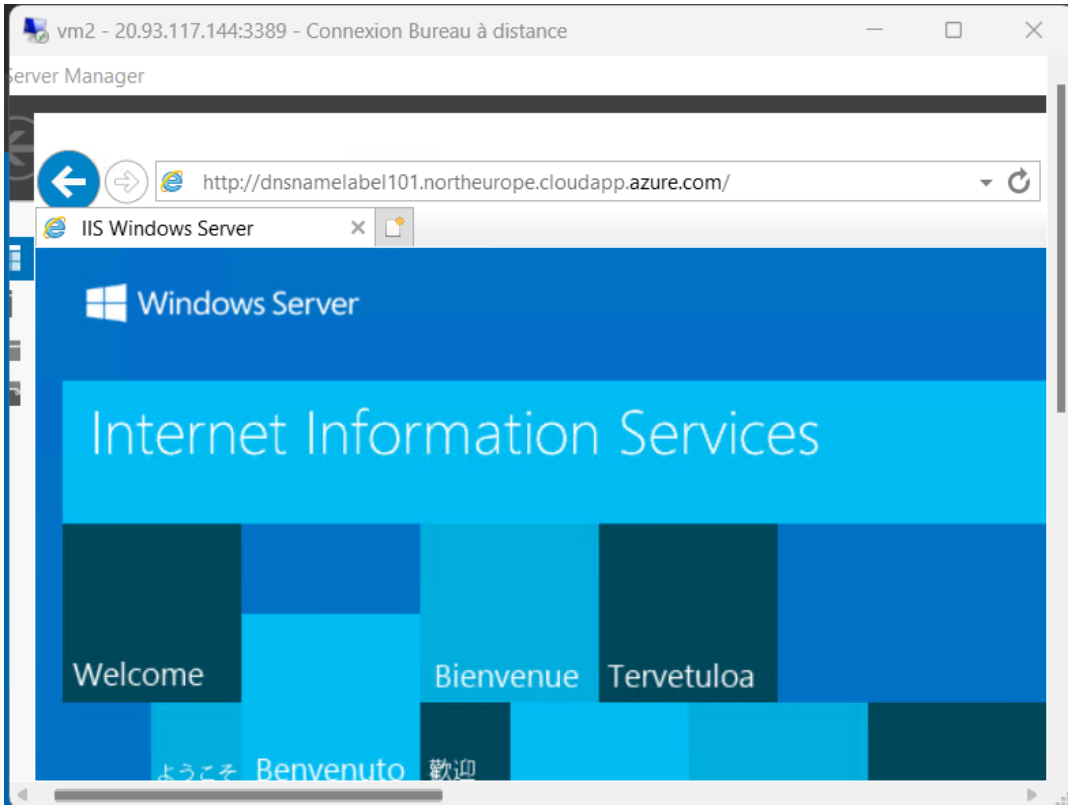
8. We deployed the subnet SubnetA of range 10.0.1.0/24

Name ↑	IPv4	IPv6	Available IPs	Delegated to	Security group	Route table
default	10.0.0.0/24	-	250	-	-	-
SubnetA	10.0.1.0/24	-	251	-	-	-

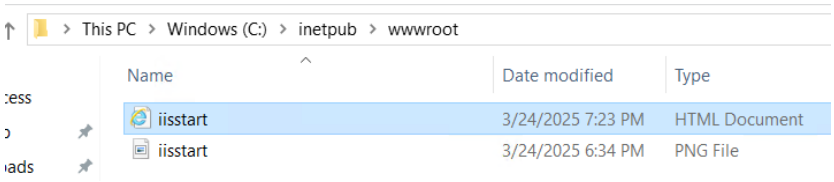
9. We deployed a new virtual machine, **vm2**, within **vnet1**, specifically using **SubnetA**, under the **tp1rg** resource group in the **North Europe** region. This ensures **vm2** is part of the same virtual network as **vm1**, allowing for internal communication between the two machines.

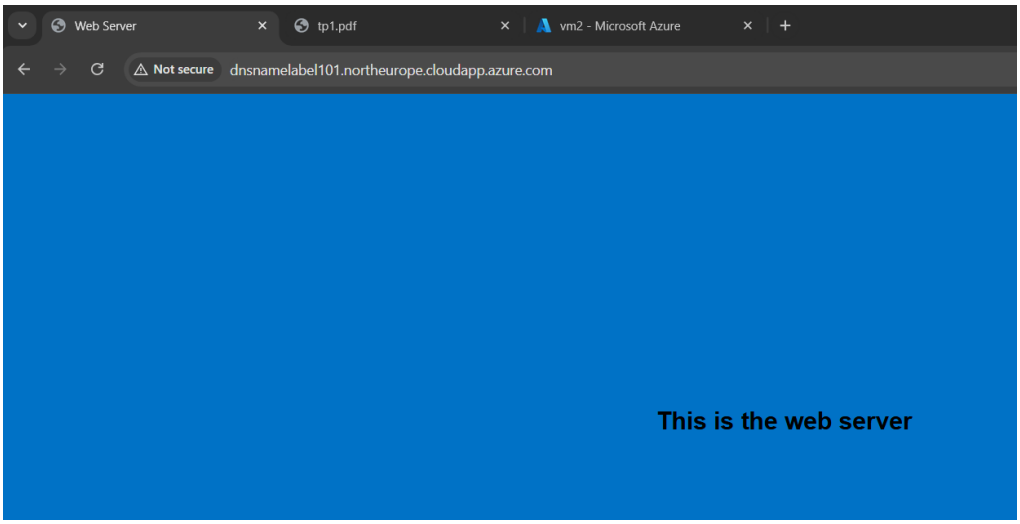


10. We successfully connected to **vm2**, opened Internet Explorer, and entered the private IP address of **vm1**. This allowed us to access the default homepage of Internet Information Services (IIS) on **vm1**. **Since both vm1 and vm2 are part of the same virtual network, they can communicate directly with each other without any external routing or firewall restrictions.**

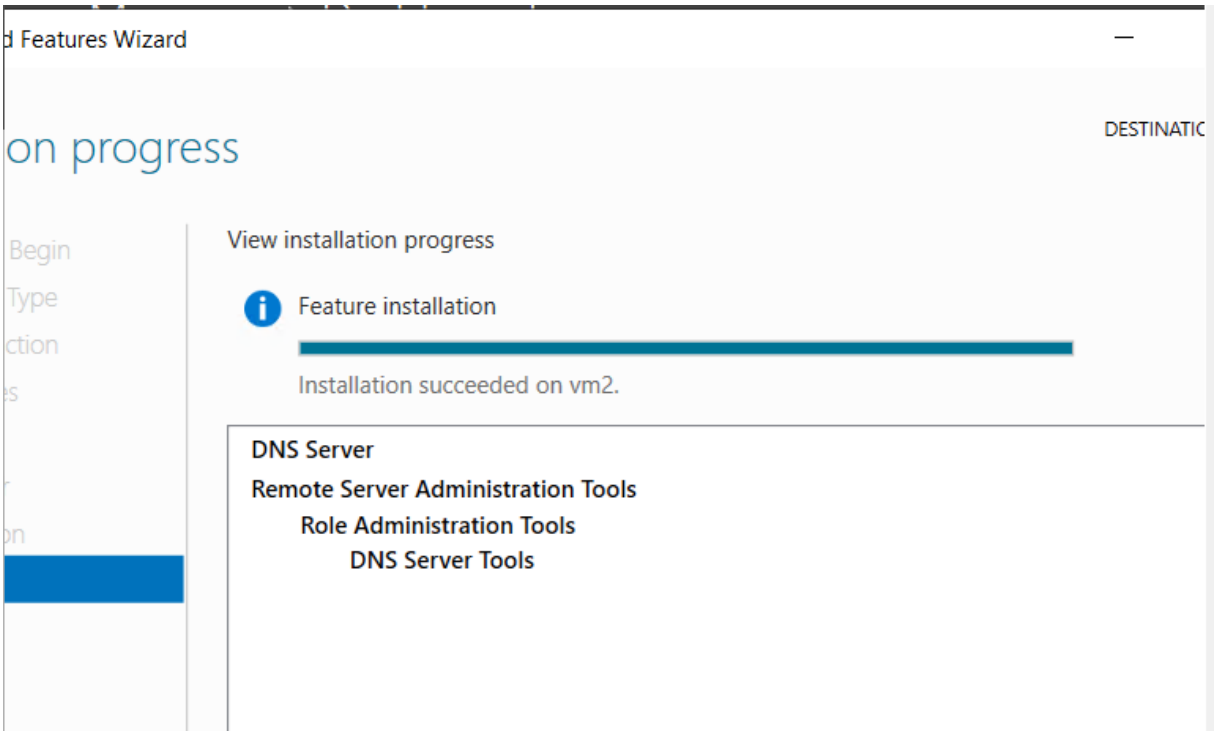


11. We edited the following HTML file to display “This is the web server”.

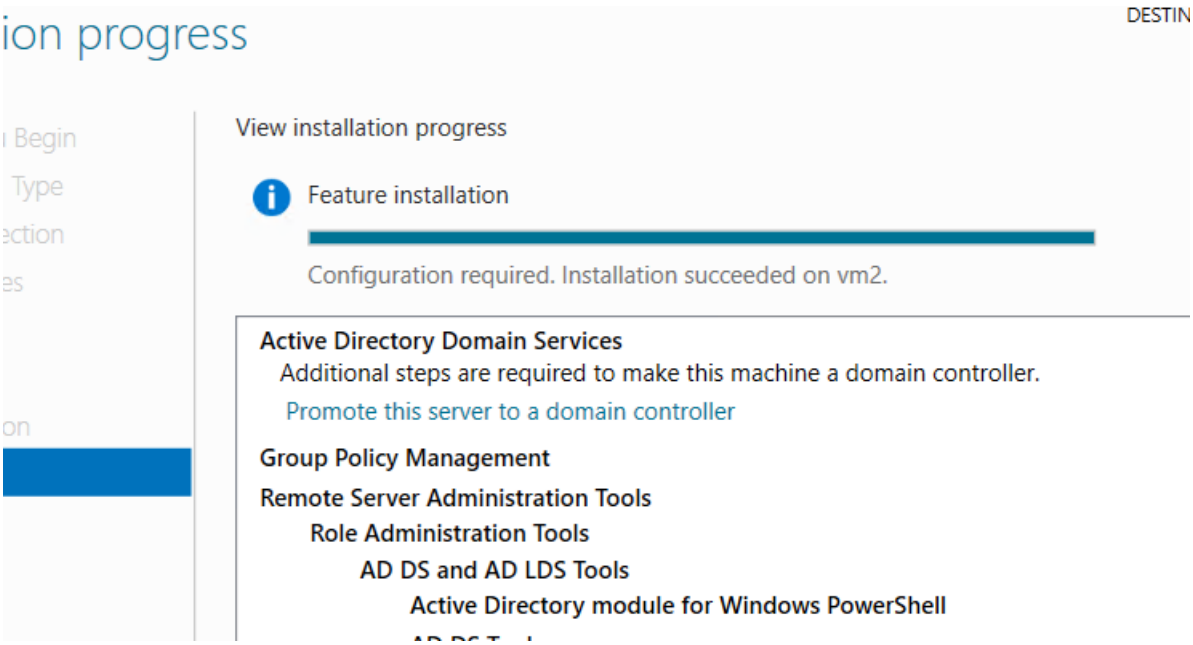


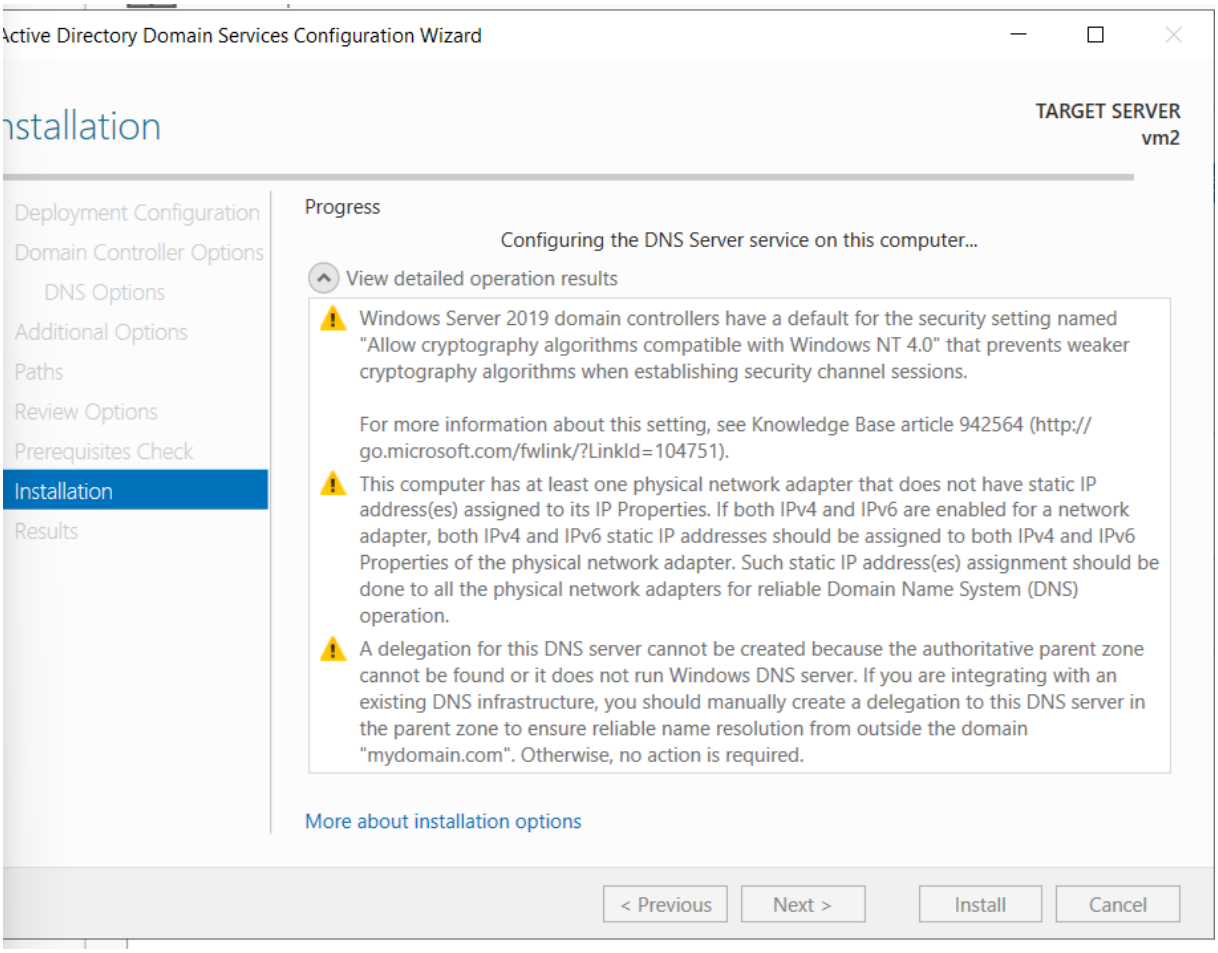


12. We successfully connected to the second virtual machine, **vm2**, and installed the DNS server by using the Server Manager. We added the **Active Directory Domain Services** role, which also installs the DNS software on the server.

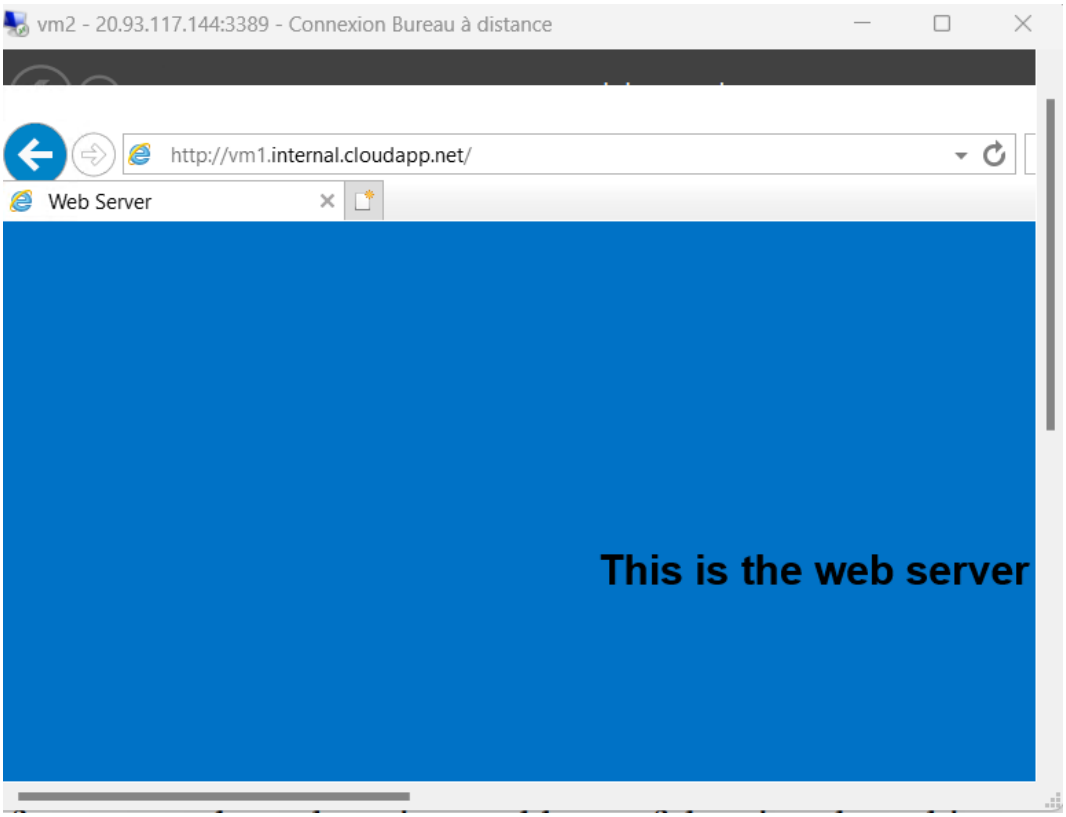


We successfully promoted **vm2** to a domain controller by configuring Active Directory Domain Services to manage the network's domain. This step is necessary to establish a central directory for authenticating users and computers, enabling centralized management of network resources, and **ensuring secure communication within the domain**.



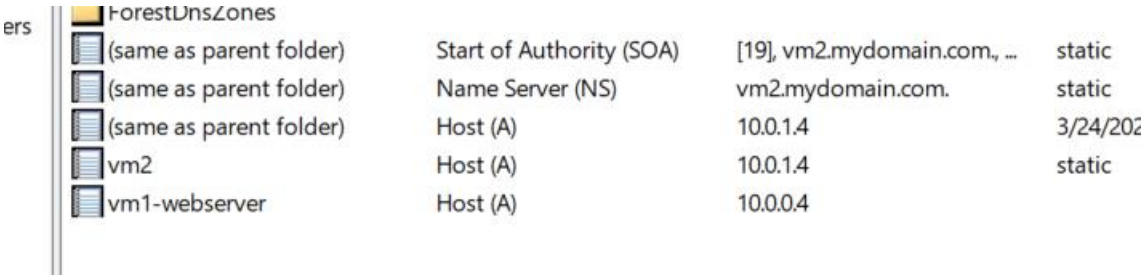


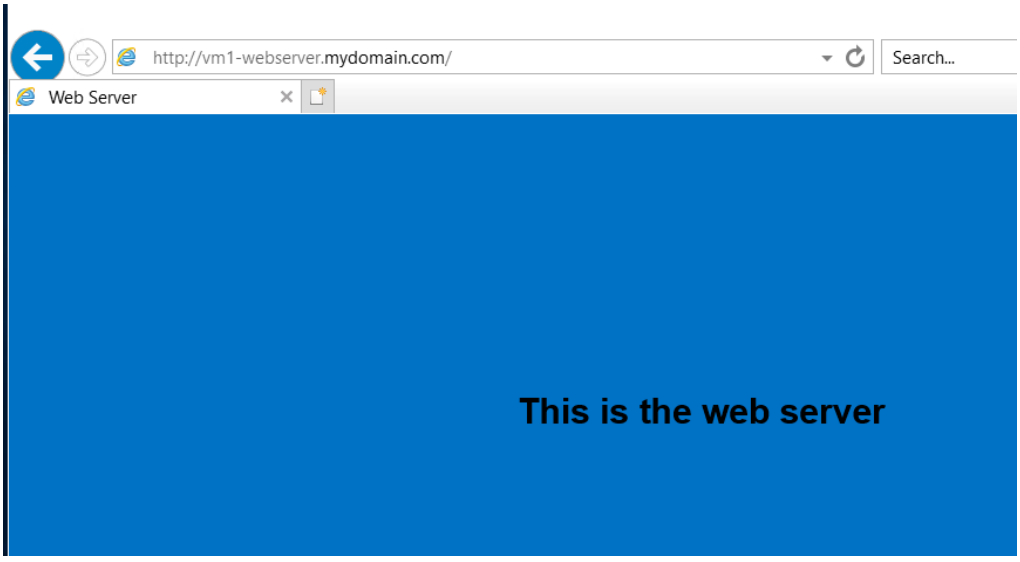
14. We successfully tested the DNS resolution on **vm2** by using the Azure-provided DNS name **vm1.internal.cloudapp.net**. This confirms that the DNS server is functioning properly and that **vm2** can resolve the internal address of **vm1**, allowing for seamless communication between the two virtual machines using friendly DNS names.



15. We successfully configured the custom DNS server for the virtual network by setting it to the private IP address of **vm2**, where the DNS service is running. This ensures that the virtual machines in the network will use **vm2**'s DNS service for name resolution, and restarting the VMs will apply the changes, enabling them to resolve domain names within the private network.

16. We successfully configured a DNS record on **vm2** (the DNS server) to map a name (e.g., **vm1-webserver**) to the private IP address of **vm1**. By creating an **A record** in the DNS forward lookup zone for **mydomain.com**, we can now access the web server on **vm1** using the fully qualified domain name (FQDN) **vm1-webserver.mydomain.com**. When entered in Internet Explorer, it displays the "This is the web server" message, confirming that the DNS configuration is working as expected.

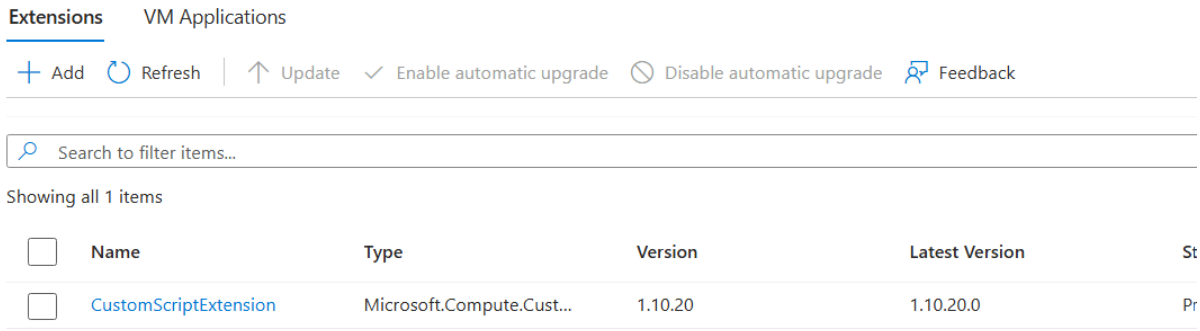




17. We successfully reverted the DNS server configuration on the virtual network blade to **Azure-provided DNS**. After saving the changes, we restarted the virtual machines to ensure they use the default Azure DNS servers instead of the custom internal DNS server. **This step ensures that the VMs will resolve external**

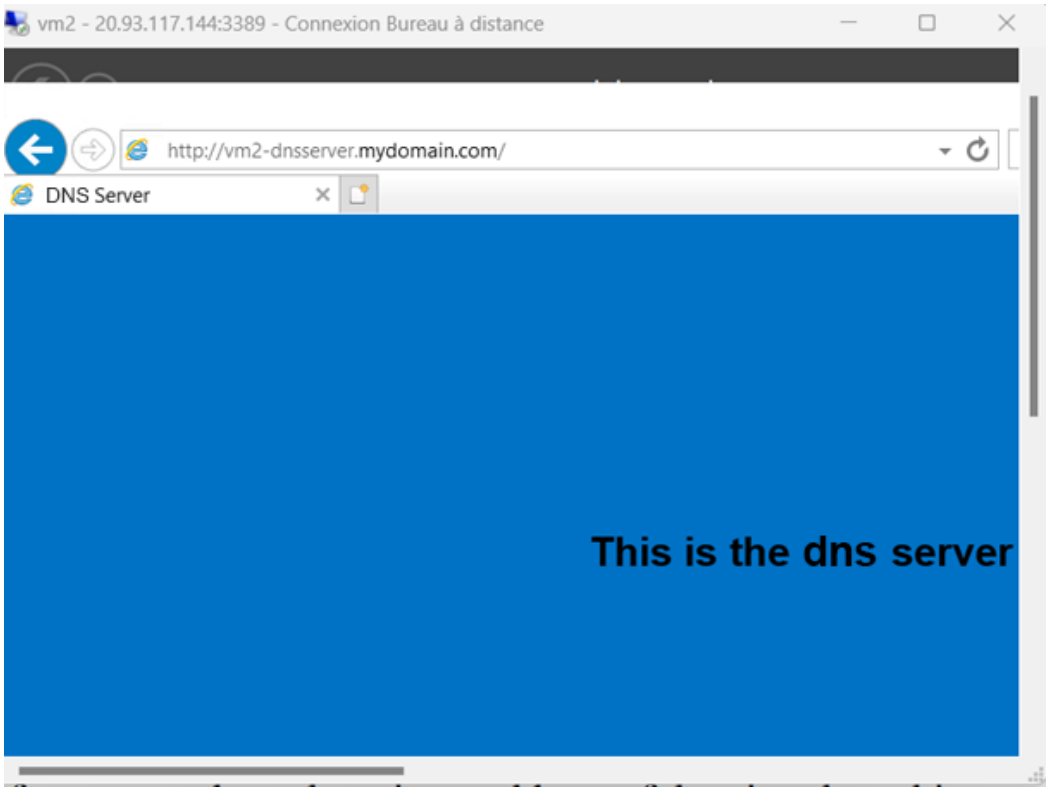
domain names using Azure's built-in DNS service, while still allowing internal names to be resolved via the internal DNS if needed.

18. We successfully added the **Custom Script Extension** to **vm2** and uploaded the **install_IIS.ps1** script to a storage account. This script installs IIS, removes the default start page, and replaces it with the VM's computer name. After executing the script, IIS is installed and configured on **vm2**.



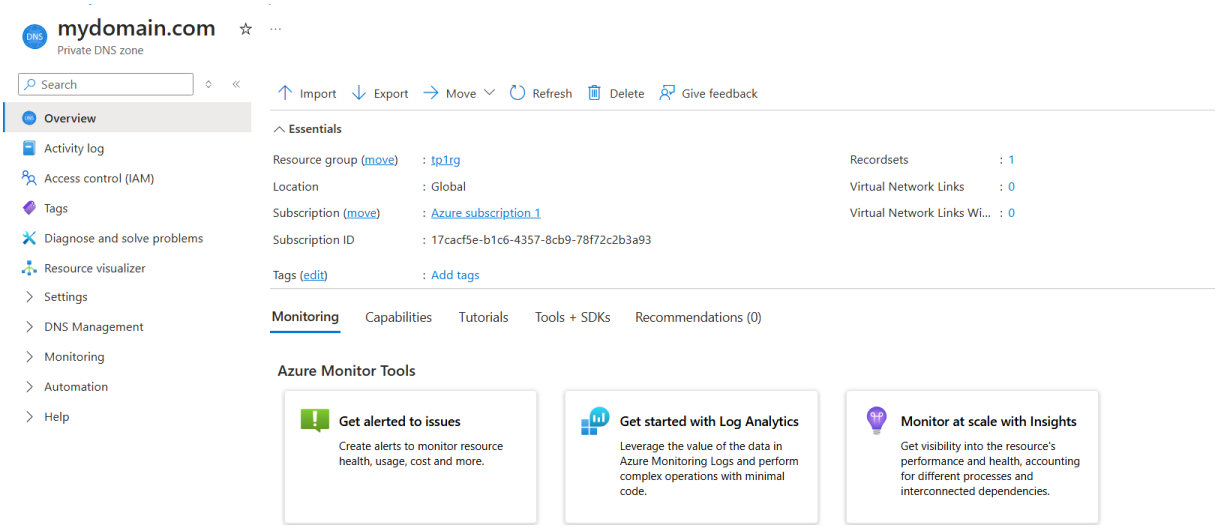
19. We edited the index.html, as done previously with the web server.

20. We successfully created a new **A record** in the DNS server on **vm2**, mapping the name **vm2-dnsserver** to its private IP address. After configuring the record, we used the fully qualified domain name (FQDN) in Internet Explorer and confirmed that the "This is the DNS server" message appears, indicating the DNS server is correctly set up.

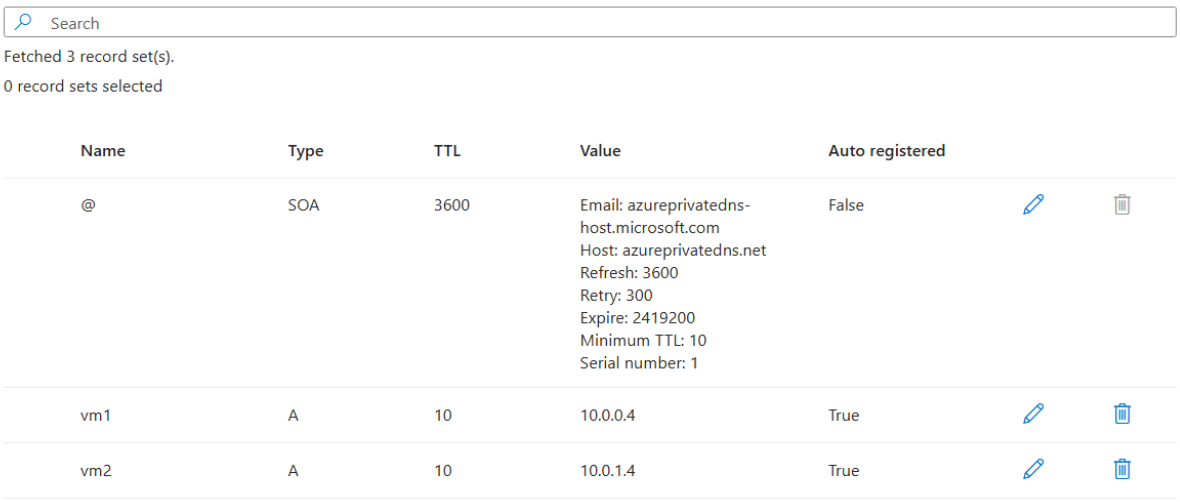


21. We attempted to connect to the DNS server from **vm1** using its fully qualified domain name (FQDN), but we couldn't reach the page. This happened because the web server doesn't have the necessary DNS resolution to access the DNS server. To fix this, we need to implement **Azure Private DNS** to enable proper name resolution within the virtual network.

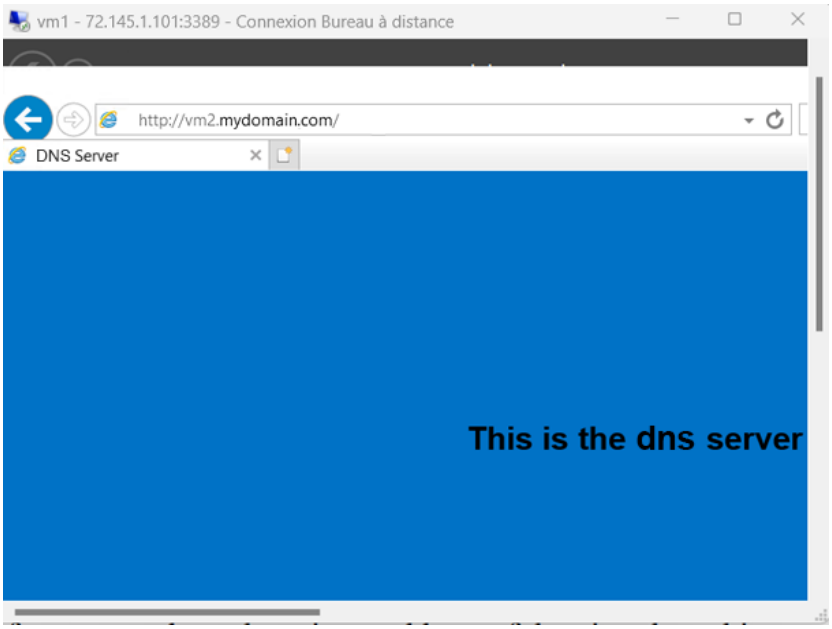
22. We successfully created a **Private DNS Zone** named **mydomain.com** in the same resource group, leaving the default values for other settings. This will allow us to manage DNS records for the domain within the private network.



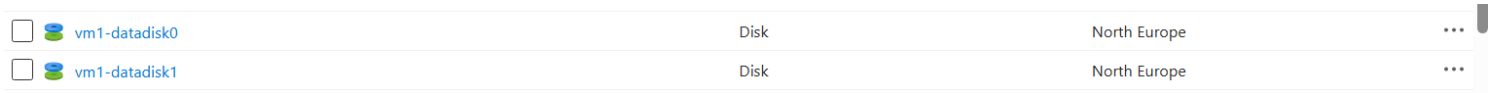
23. By enabling auto-registration, any virtual machines in vnet1 will automatically register with the DNS zone. After creating the link, we confirmed the presence of A records for vm1 and vm2 in the DNS zone. We also added the A record for vm2-dnsserver as per task 20, ensuring proper DNS resolution within the network.



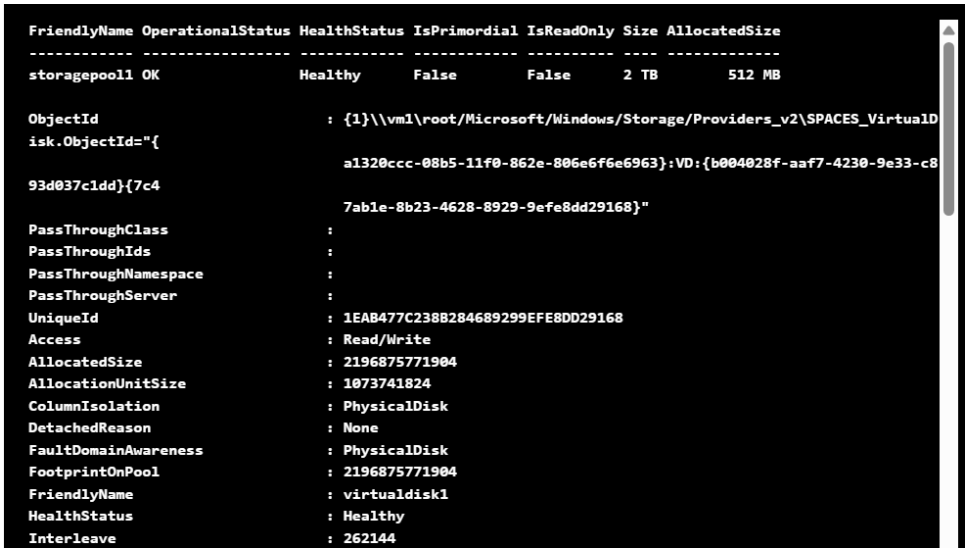
24. We successfully connected to the first virtual machine (**vm1**, the web server machine) and accessed the **fully qualified domain name (FQDN)** of the DNS server. As a result, we were able to see the "This is the DNS server" message, confirming that the web server could now resolve the DNS server's FQDN.



25. We successfully scaled the storage of **vm1** by attaching and configuring data disks. In the **vm1 blade**, we navigated to the **Automation section**, clicked **Export Template**, then **Deploy**, and edited the template. We replaced the "dataDisks": [ ] line with the provided code to define two new data disks of 1024 GB each, with **ReadOnly** caching and the **Empty** create option. After saving and creating the template, the new data disks were successfully attached to **vm1**.



26. We executed the provided PowerShell script to create a new **Z:** drive. The script performed several steps: it created a **storage pool** (storagepool1) using available physical disks, then created a **virtual disk** (virtualdisk1) with a simple resiliency setting and fixed provisioning. The disk was initialized, and a **new partition** was created on the disk with the maximum available size, and it was assigned the drive letter **Z**. This successfully set up a new drive, expanding the storage capacity on **vm1**.



27. We cleaned up by deleting our resource group tp1rg.

Conclusion:

During this lab, we learned how to **create and configure Azure virtual networks and virtual machines, set up web servers using Internet Information Services (IIS), implement DNS services, and manage network configurations**. We explored practical skills such as **connecting virtual machines via RDP, configuring network security groups, creating subnets, establishing domain controllers, and setting up private DNS zones**. Additionally, we gained experience with storage management by attaching and configuring data disks, demonstrating the comprehensive process of deploying and managing cloud infrastructure in the Azure environment.

Interpretation: The hands-on experience with storage management illustrates the importance of effectively handling data in the cloud, which is crucial for scaling applications. This also demonstrates a holistic understanding of managing not just compute resources but also storage solutions in a cloud ecosystem.