

# **The Active Directory Series: Part 1**

By Miguel K.

---

## **Building My Own Active Directory Instance**

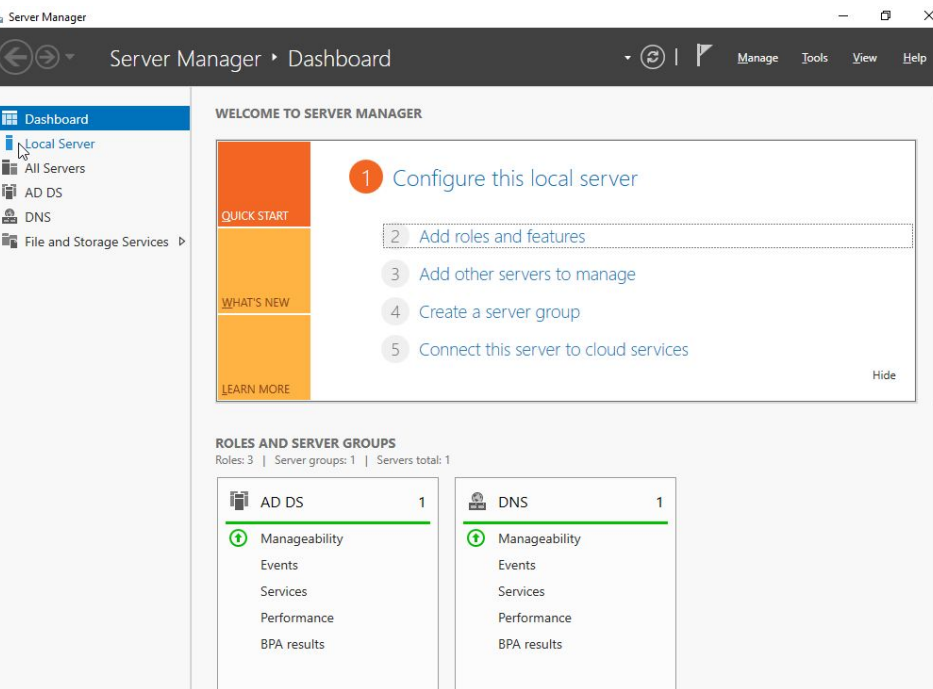
# Project Overview: Part 1 – Setting Up an Active Directory Network

In this first installment of the Active Directory series, I set up a Windows Server virtual machine (VM) and configure an Active Directory network. I begin by provisioning a Windows VM, joining it to the Active Directory domain, and creating organizational units (OUs) and user accounts within the domain.

Next, I demonstrate the functionality by signing into the Windows VM, which initially only has a local user account, using the credentials of a domain user created in Active Directory. This project highlights my ability to establish and configure an Active Directory instance and create a functional network environment.

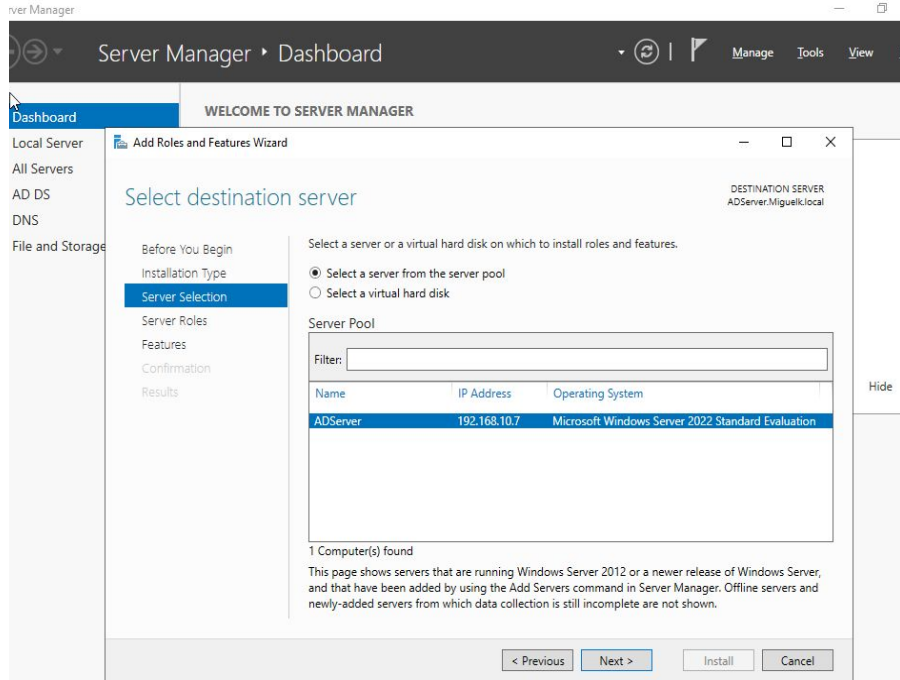
This foundational work sets the stage for subsequent projects in the series, which will include automating user creation with PowerShell scripts, implementing role-based access control (RBAC), and strengthening network security.

# Creating My Active Directory Instance



To create my Active Directory instance, I accessed the **Server Manager Dashboard** on my Windows Server VM and selected **Add Roles and Features** to begin the setup process.

# Selecting the Server for Active Directory Installation



After choosing the the role|feature based installation option, I selected a server from the server pool. For this installation, I chose my designated **AD Server**, which will host the Active Directory Domain Services.

## Promoting the Server to a Domain Controller

Filter: <input type="text"/>		
Name	IP Address	Operating System
ADServer.Miguelk.local	192.168.10.7	Microsoft Windows Server 2022 Standard Evaluation

Next, I promoted the server to a **Domain Controller**. I chose to create a new **forest** for my network and named the root domain **MiguelK.local**.

After completing the installation, my Active Directory network was successfully deployed and ready for use.

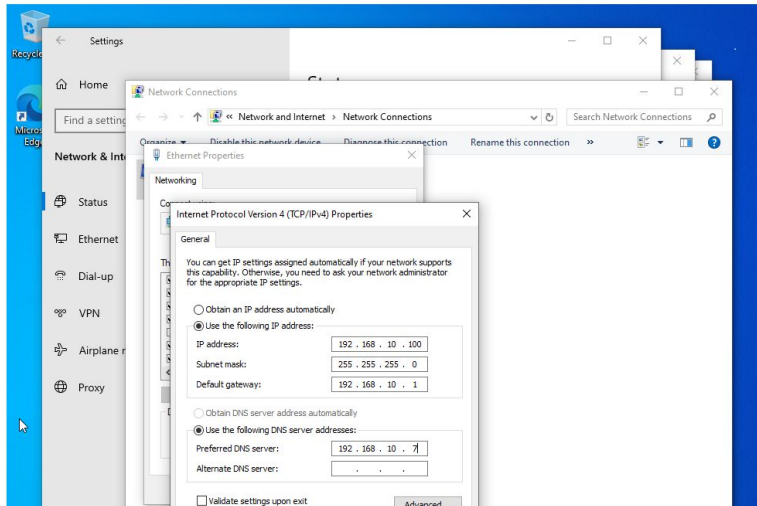
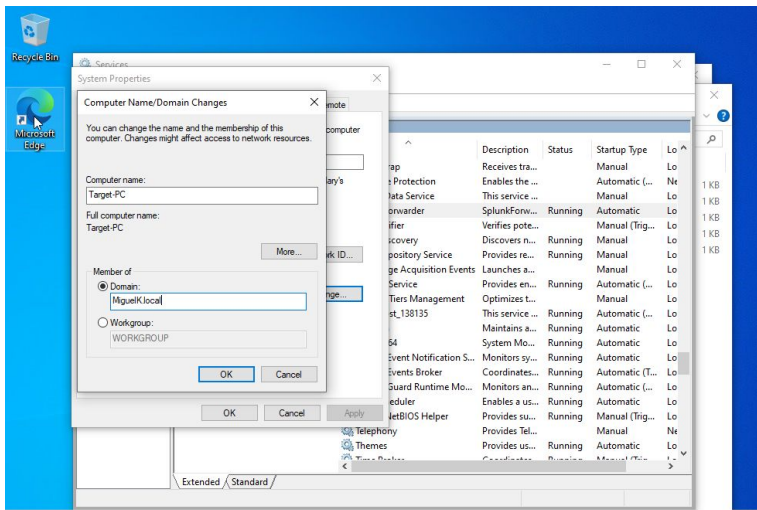
---

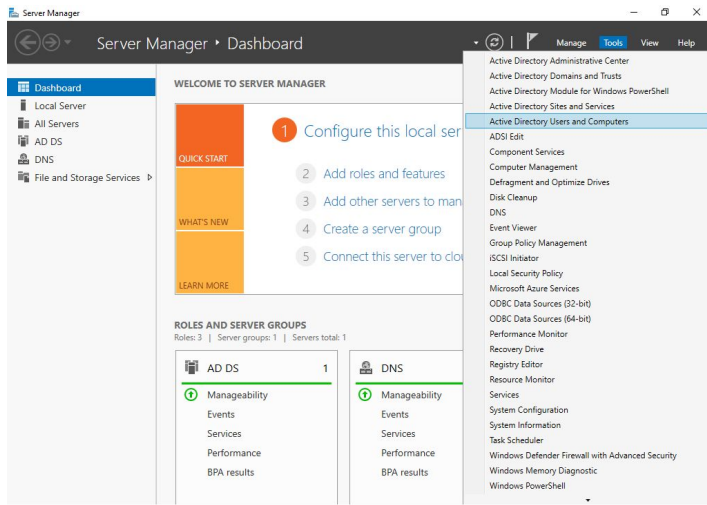
## Joining the Windows VM to the Domain

To join my Windows VM to the domain, I logged in and accessed **Advanced System Settings**. From there, I configured the **Domain** settings, entering the domain name **MiguelK.local**

Additionally, I ensured that the **Preferred DNS server** was set to the IP address of the Active Directory server, ensuring proper domain connectivity.

---

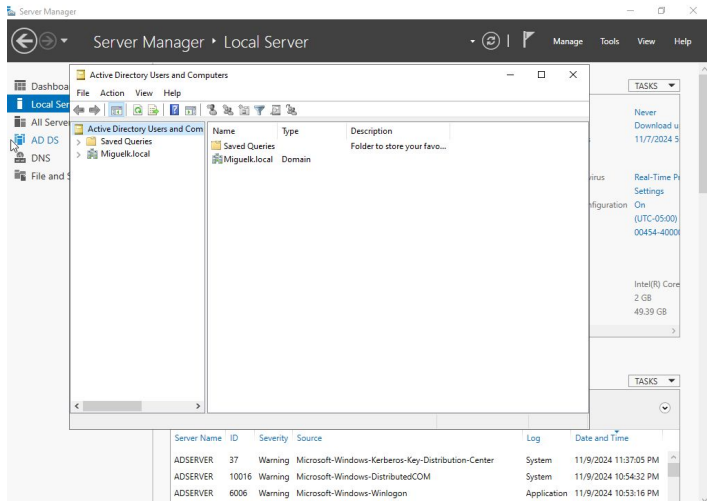


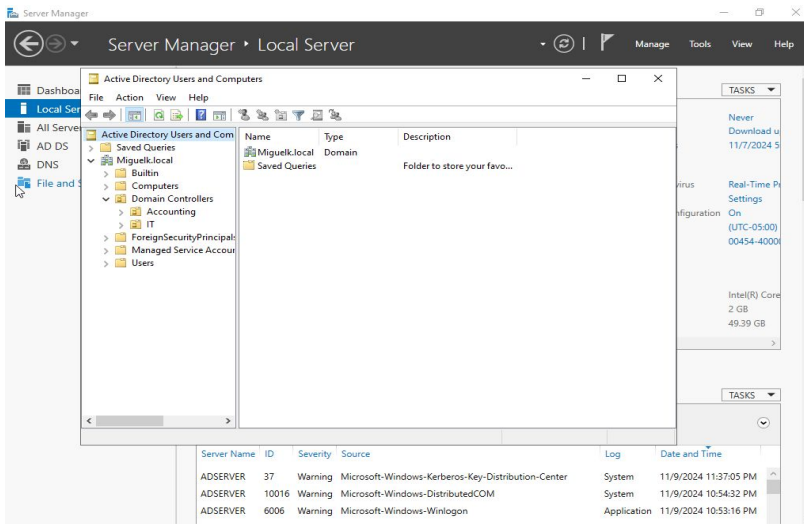


## Managing Active Directory

After successfully joining the Windows VM to the domain, I accessed **Active Directory Users and Computers**.

This tool allows me to manage and organize objects within the domain, such as creating new users, computers, organizational units (OUs), and controlling access permissions across the network.

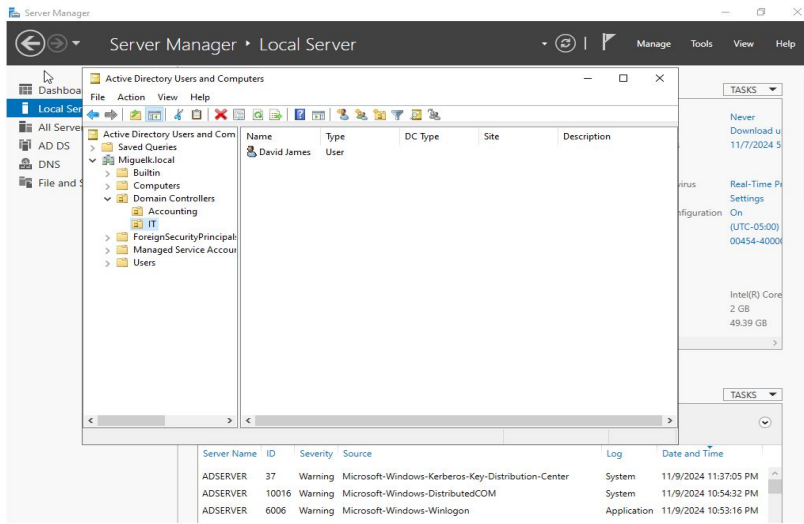




## Creating Organizational Units and Users

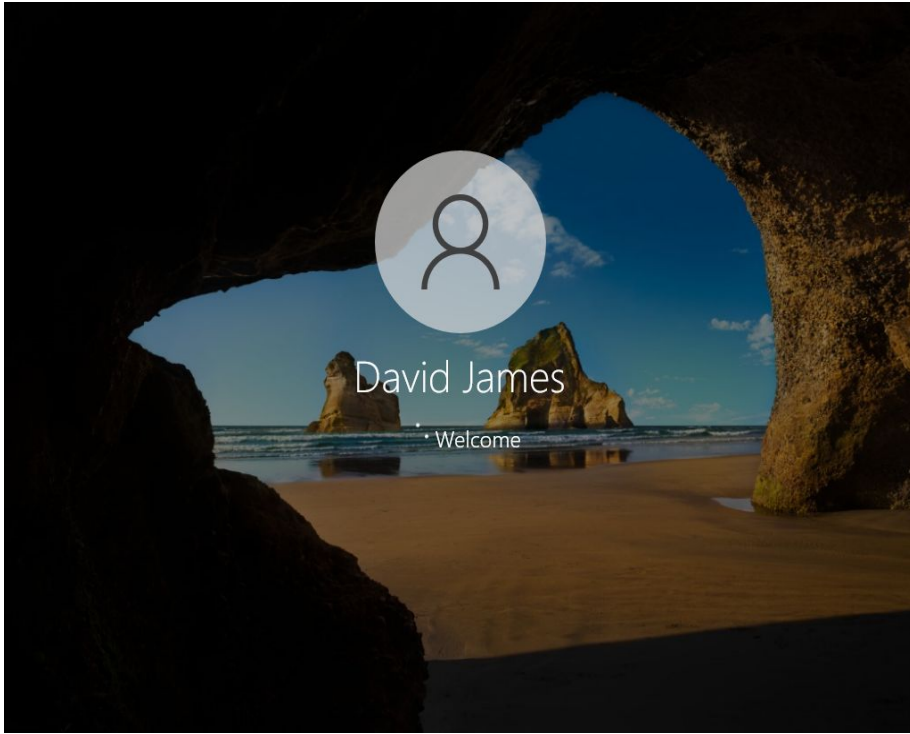
I created **two Organizational Units (OUs)** by right-clicking on the **Domain Controller**, selecting **New**, and then choosing **Organizational Unit**.

This sets the foundation for future projects in the Active Directory series. I then added a user, **David James**, to one of the OUs. In the next slide, we'll test if we can successfully sign into his account on the Windows VM.





## Successful Login and Project Conclusion



We successfully logged into the **Windows VM** using the credentials of a user created in **Active Directory**, confirming that the system is properly configured and functioning.

This marks the completion of Part 1 of the Active Directory series. The foundation has been laid, and we're now ready to build on it in future projects. Stay tuned for more as we continue to expand and enhance the Active Directory environment.

---