

Active Directory Cybersecurity Homelab

Overview

Built a simulated enterprise Windows environment to practice identity management, endpoint administration, and Active Directory configuration using Hyper-V.

Step 1: Virtual Machine Deployment

Created a virtual enterprise environment using Hyper-V with three virtual machines:

- Windows Server — configured as the Domain Controller
- PC-01 — Windows client workstation
- PC-02 — Windows client workstation

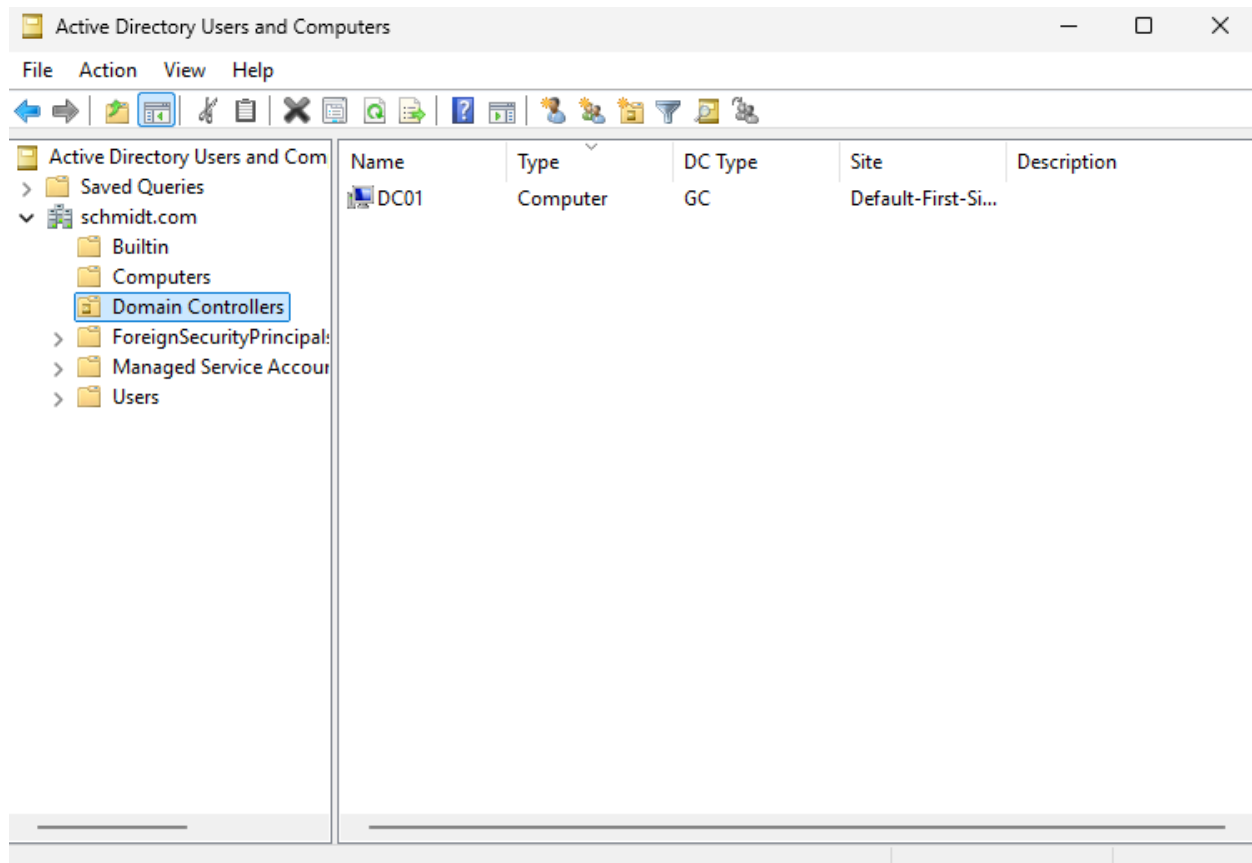
Configured the systems to communicate within a dedicated virtual network to simulate a corporate environment.

Virtual Machines				
Name	State	CPU Usage	Assigned Memory	Uptime
 Windows Server	Running	49%	3888 MB	00:19:30
 PC-02	Running	0%	1718 MB	00:16:23
 PC-01	Running	0%	1946 MB	00:06:19

Step 2: Domain Controller & DNS Configuration

Installed and configured Active Directory Domain Services (AD DS) by promoting the Windows Server machine to a Domain Controller.

Configured DNS services and established centralized authentication for the lab environment.

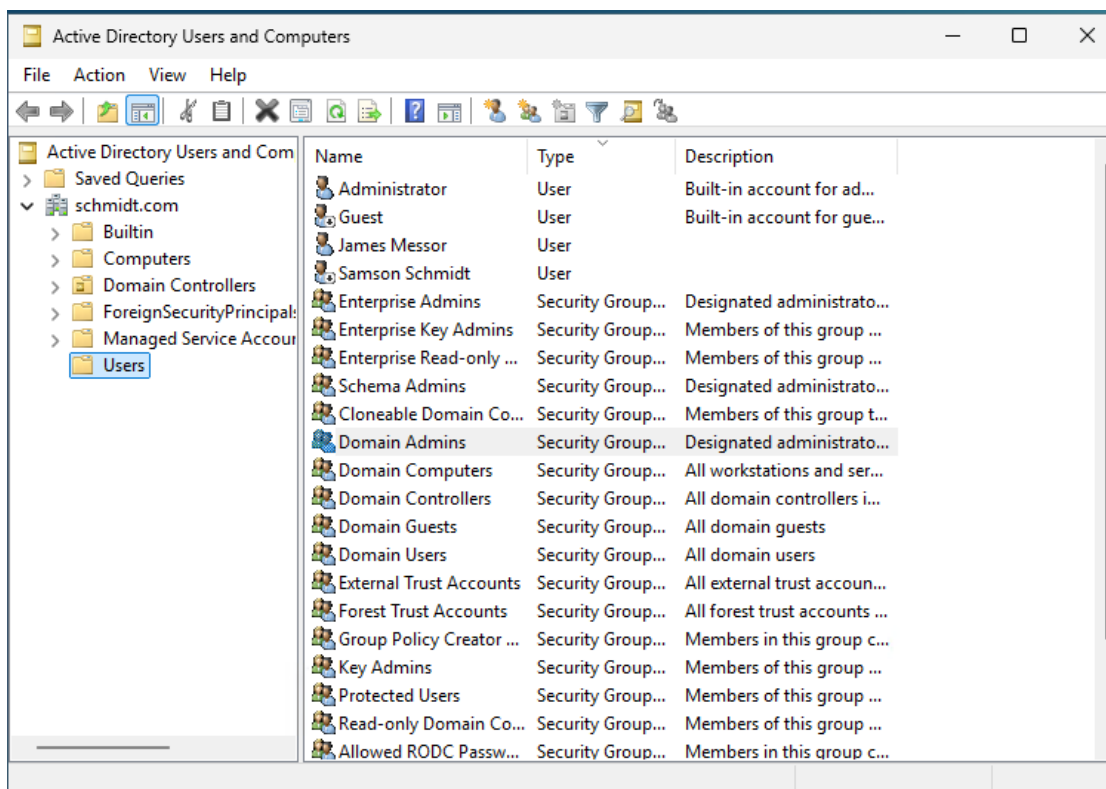


Step 3: Active Directory Configuration

Configured Active Directory by creating and managing:

- User accounts
- Computer accounts
- Domain authentication

Tested account creation and centralized user management within the domain environment.

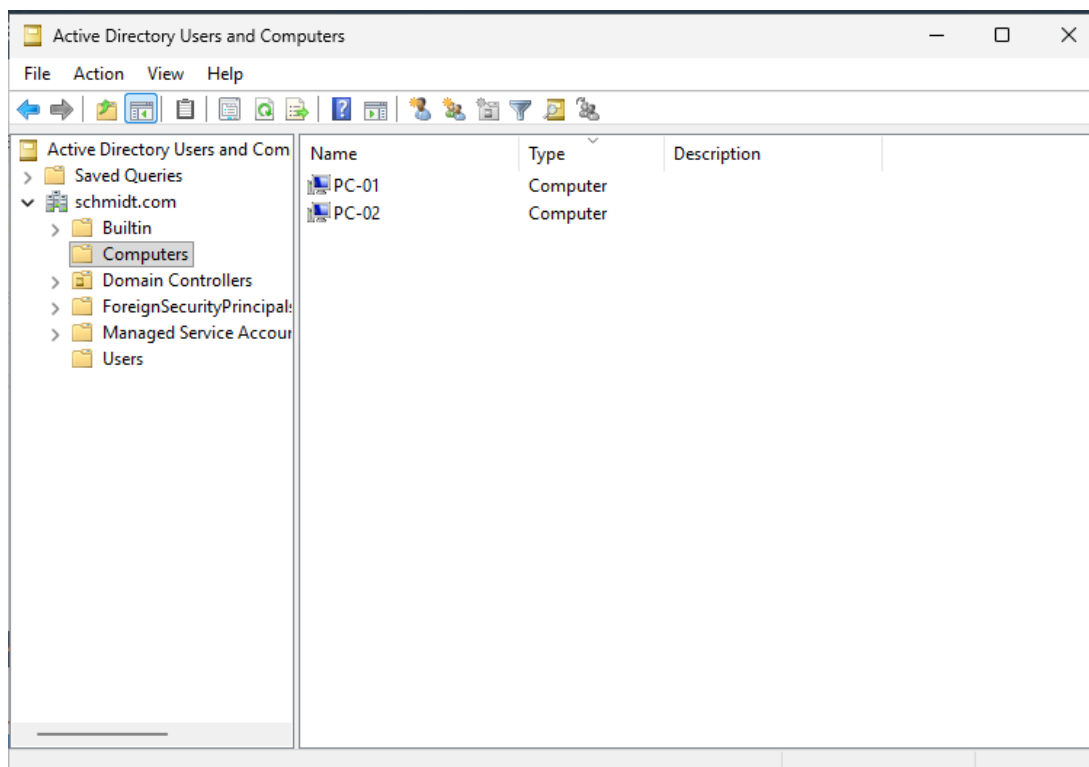


Step 4: Domain Workstation Integration

Joined Windows client machines to the Active Directory domain.

Verified:

- Domain connectivity
- User authentication
- Centralized account access
- Communication between domain systems



Project Outcome

Successfully built a functional Active Directory environment that simulates a small enterprise network. This project provided hands-on experience with Active Directory, Windows Server administration, domain authentication, and foundational identity and access management concepts.