Identity and Access Management (IAM) Project
Active Directory (On-Premises) Deployment For CyberWelfare Solutions

Implementation of On-Premises Active Directory for Centralized Identity and Access Management
Organisation: CYBERWELFARE
Date: 25 SEPTEMBER 2025

Prepared By:JUNAID.ABDULRAHMAN.A
(Cybersecurity Analyst)

Before we proceed let see what Identity access management[IAM] and Active directory domain service are

What is Identity Access Management: [IAM] refers to a framework of policies,procedures and technologies designed to manage digital identities and regulate user access to systems,application or data in order to reduce risk to cyber attacks

What is Active Directory Domain Service:active directory domain service helps control all the computer we have on a network from one single point such that we can configure all the computers on a server by installing an active directory on the server then promote the active directory to a domain controller in other to configure and implement policy however and whenever

1. Project Overview

This project focused on deploying an **on-premises Active Directory Domain Controller to provide centralized Identity and Access Management (IAM)** for Cyberwelfare Solutions. The implementation included domain setup, client integration, creation of Organizational Units (OUs) aligned to regional offices, security group design, user provisioning, and enforcement of access control policies using Group Policy Objects (GPOs).

2. Company IT Structure

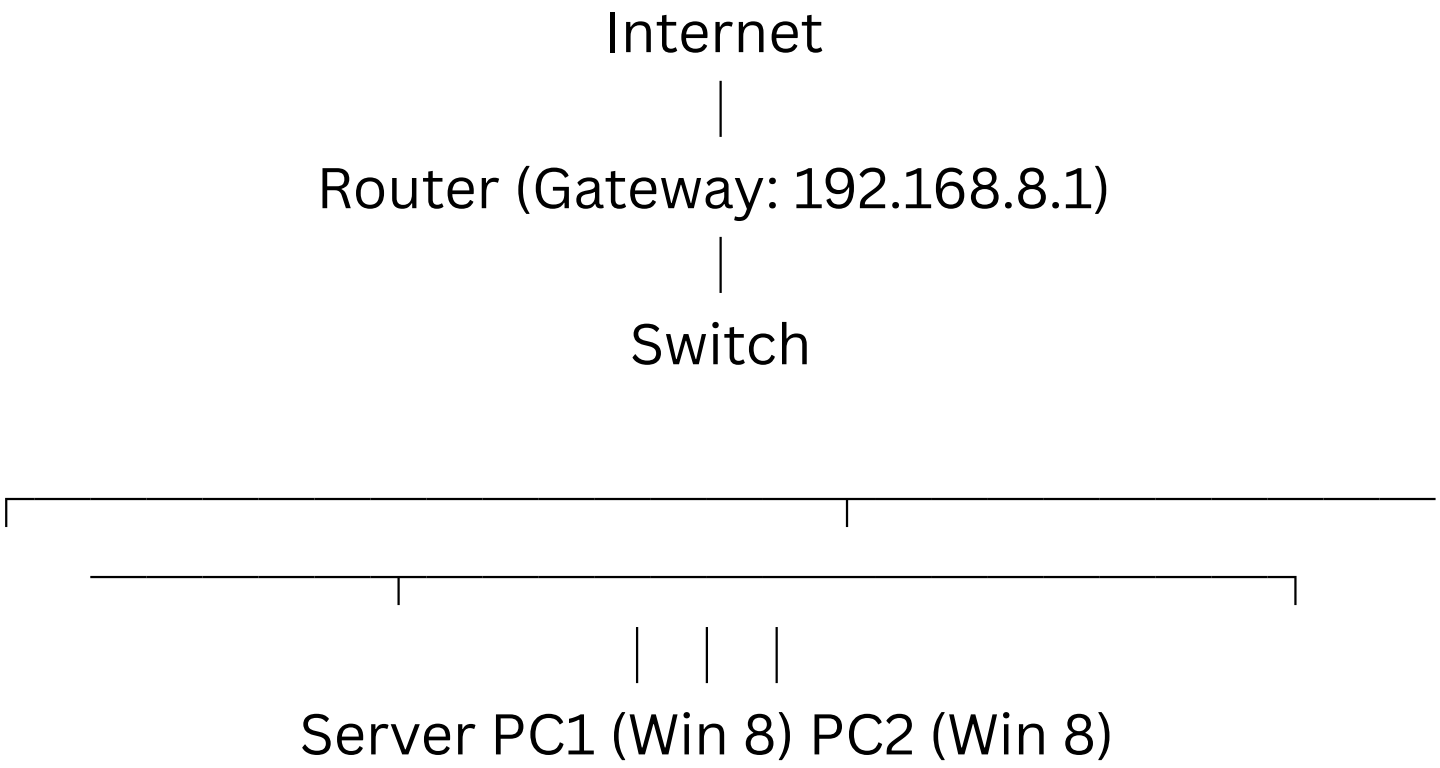
The simulated environment reflected a small IT services firm with distributed offices:

- 1 x Windows Server – Domain Controller (AD DS + DNS)
- 2 x Client PCs – Windows 8
- Two regional OUs – canada and uk
- Departmental Groups – Created within each OU to represent business functions

3. Project Objectives

- Deploy Active Directory Domain Services (AD DS) for centralized IAM.
- Configure regional Organizational Units (OUs) to mirror company structure.
- Provision security groups to manage access by department.
- Create user accounts and assign them to relevant groups.
- Apply Group Policies to enforce access restrictions.
- Demonstrate IAM governance in an on-premises enterprise setup.

4. Network Design



Device	IP Address	Role
Windows Server	10.0.2.4	AD Domain Controller (DC)
Windows 8 PC 1	DHCP	Client (UK OU – Cybersecurity)
Windows 8 PC 2	DHCP	Client (Canada OU – Developer)

5. Domain Configuration

- Domain Name: cyberwelfare.tech
- Server Name: CYBERWELFARE
- Static IP: 10.0.2.4
- Roles Installed:
  - Active Directory Domain Services (AD DS)
  - DNS Server

6. Organizational Units (OUs) and Groups

The directory structure was created as follows:

CyberWelfare.tech
├── OU: UK
│ ├── Group: Cybersecurity
│ └── Group: IT
│
├── OU: CANADA
│ ├── Group:DEVELOPER
│ └── Group:Ethical Hacker

7. Users and Group Memberships

Two test users were provisioned to demonstrate IAM principles:

Username	OU	Group Membership	Assigned Policy
Junaid Alabi	UK	Cybersecurity	Unable to shutdown
Sulaimon Tunji	CANADA	Developer	Hide settings tab

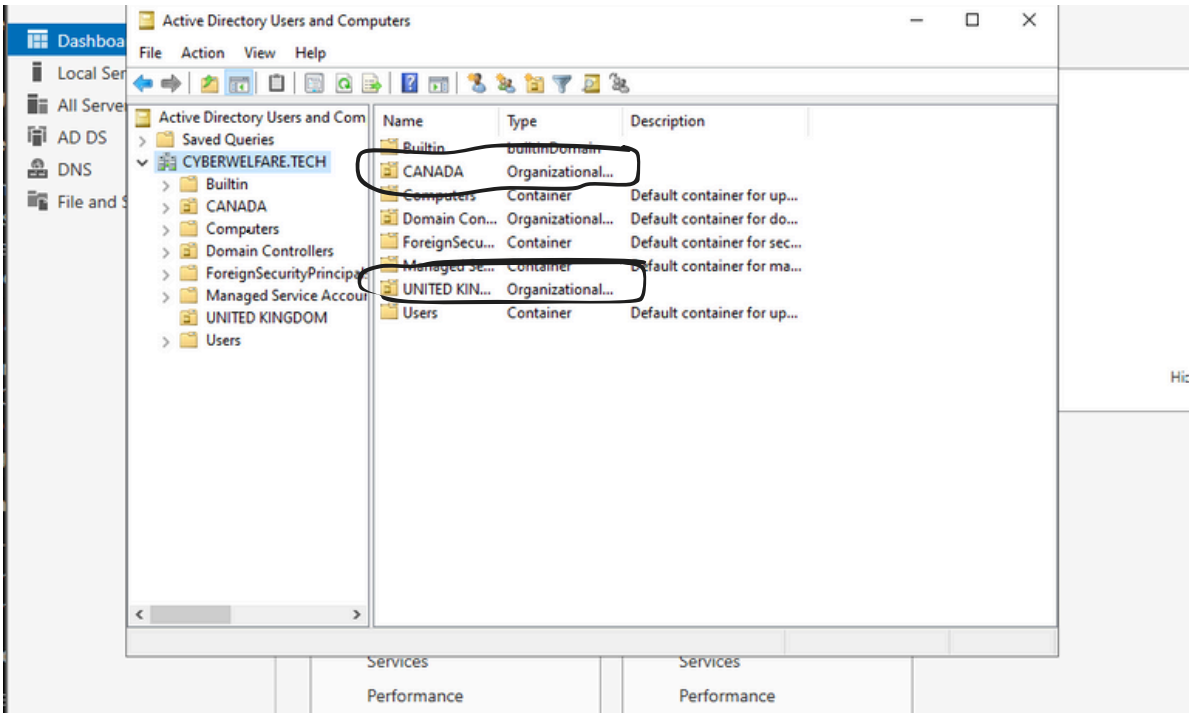
8. Group Policy (GPO) Implementation

Two GPOs were created and linked to specific users through security filtering:

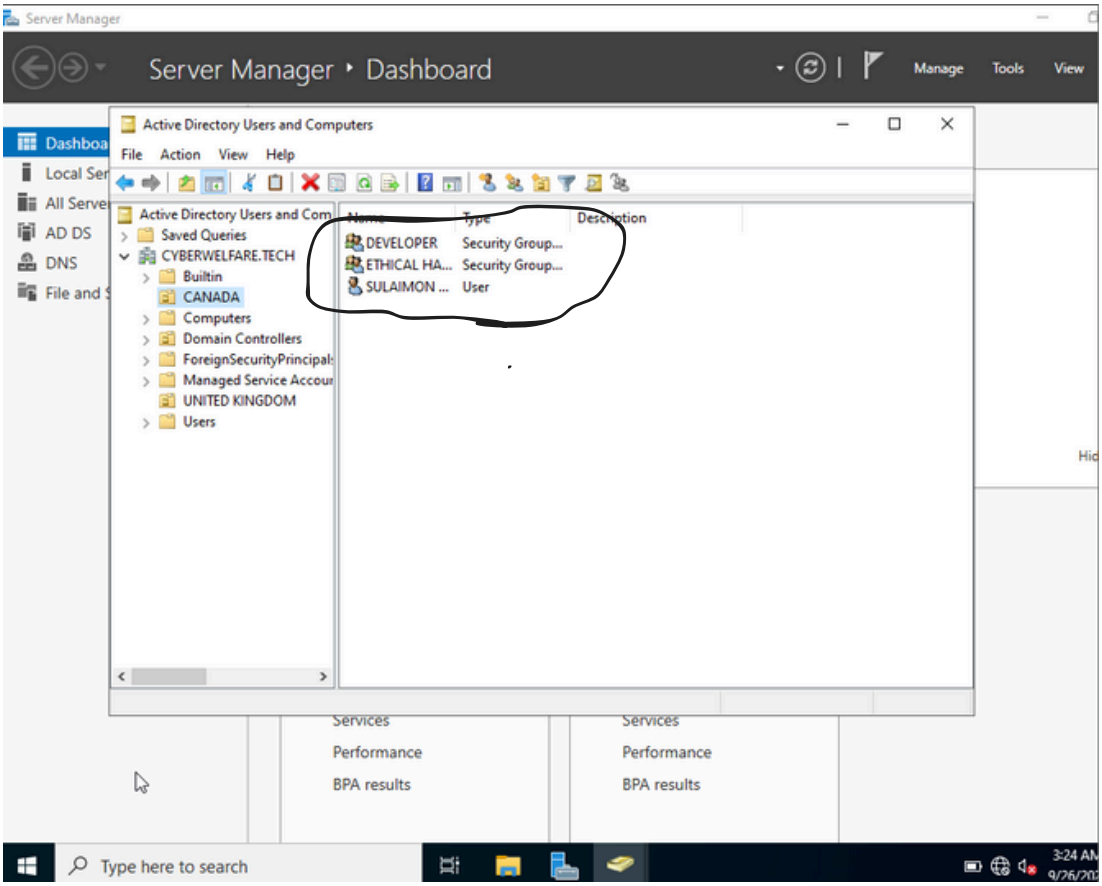
1. GPO Name: No Shutdown
    - Linked To: UK OU (Cybersecurity User – Junaid)
    - Policy:
    - User Configuration → Administrative Templates → Start Menu and Taskbar → Remove and prevent access to the Shut Down, Restart, Sleep, and Hibernate commands
    - Result: Junaid cannot shut down the assigned PC.
    -
2. GPO Name: No Settings Tab
    - Linked To: Canada OU (Developer User – Sulaimon)
    - Policy:
    - Computer Configuration → Administrative Templates → System → Control Panel → Display - Hide Settings Tab
    - Result: Sulaimon cannot use the setiing tab anymore.

9. Screenshots (Evidence)

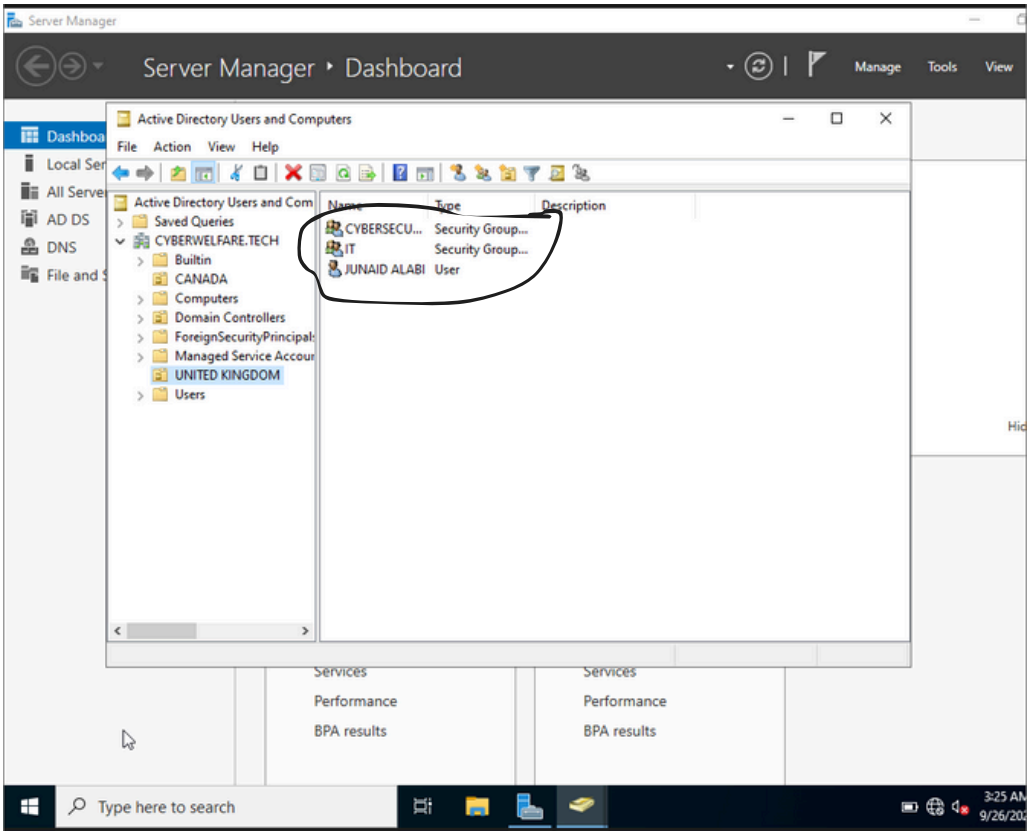
. The two organization unit created(Canada and United kingdom)



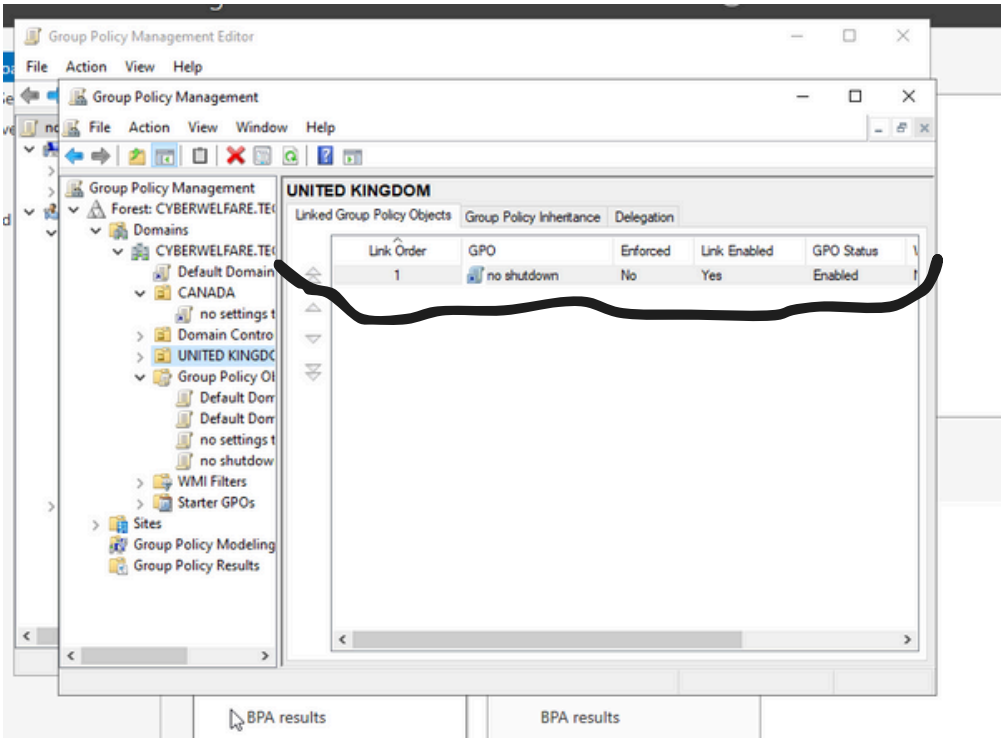
- Groups and Users created for Canada



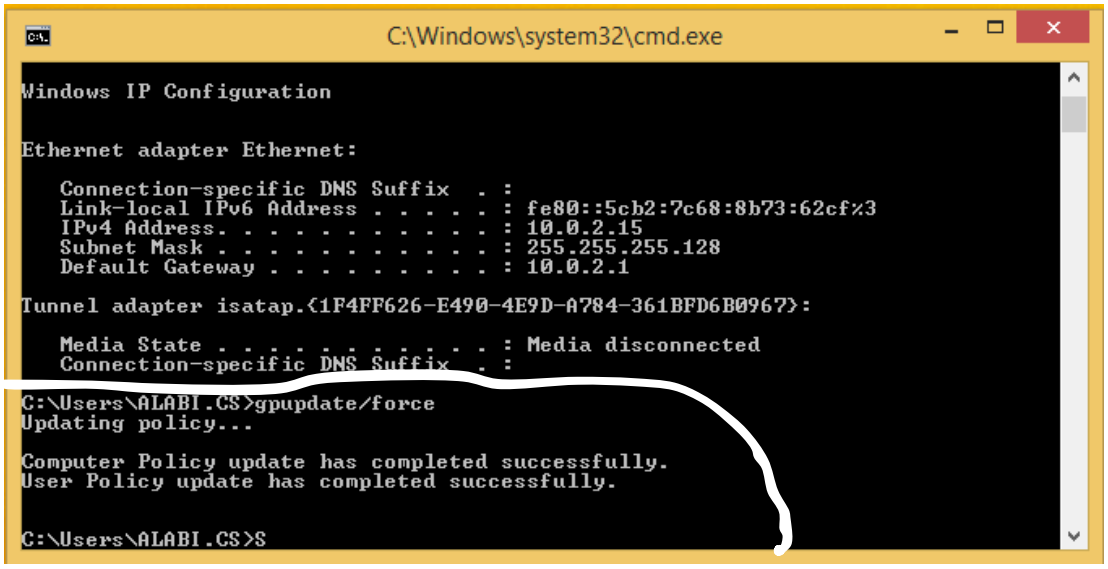
- Groups and Users created for United Kingdom



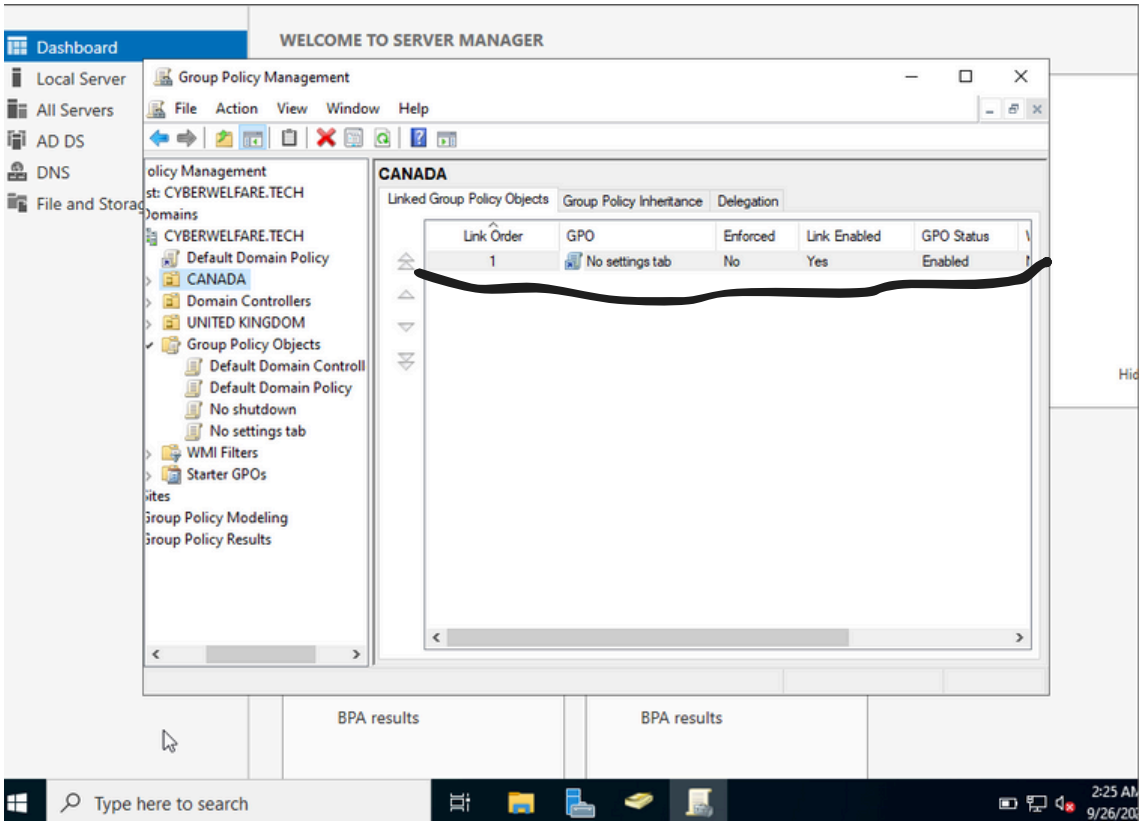
. No shutdown GPO enabled and linked to United Kingdom OU



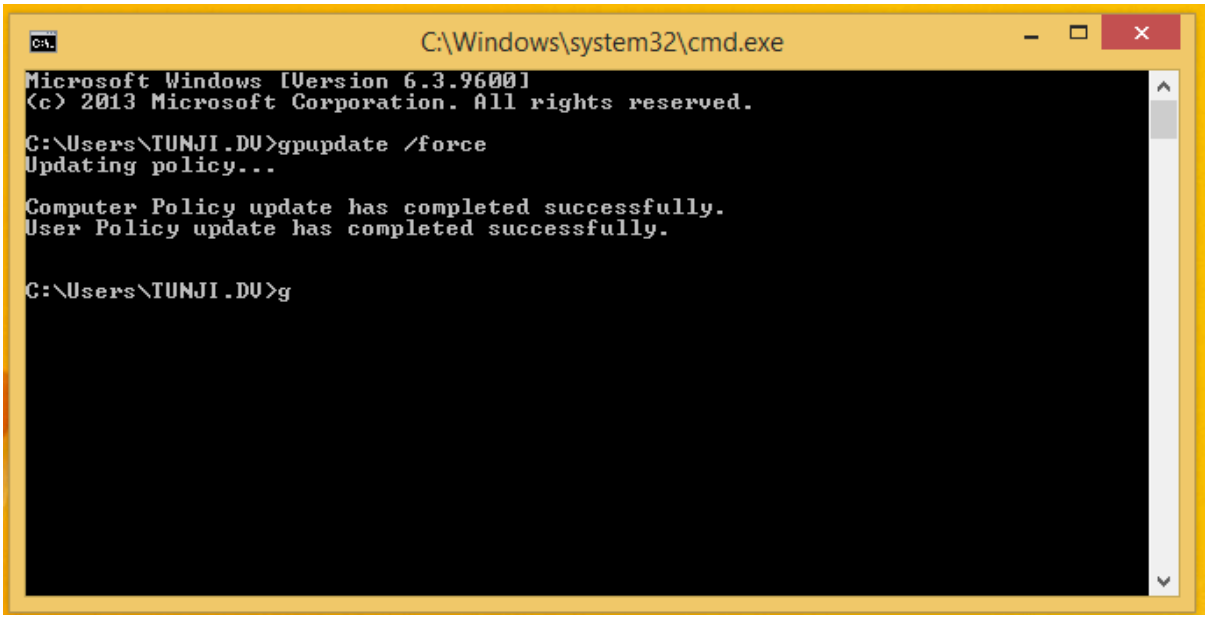
. No shutdown GPO enforced for the user(Junaid Alabi) in UK OU



. No settings tab GPO created and linked to Canada OU



. No settings tab GPO enforced for the user(Sulaimon Tunji) in Canada OU



10. Key Takeaways

- Successfully implemented an IAM framework on Active Directory.
- Mapped business structure (regions and departments) into OUs and groups.
- Demonstrated access control enforcement using Group Policy Objects (GPOs).
- Learned how to provision and manage users, groups, and security policies.
- Applied identity governance principles in a real-world simulated enterprise environment.