Active Directory and Domain Controller Deployment in a Simulated Banking Environment

Lab Project by: **DAVID OLADAYO AWE**

Role: SECURITY ENGINEER

Date: April, 2025.

1. Lab Overview

Objective of the Lab:
The objective of this lab was to design, deploy, and secure a Microsoft Active Directory (AD) environment in a simulated banking infrastructure. This setup mimics a small to medium-sized bank branch network, providing hands-on experience with user authentication, resource access controls, group policies, and administrative delegation, all critical to enterprise-level cybersecurity operations.

Summary of What Was Achieved:

- Deployed a **Windows Server** machine and promoted it to a **Domain Controller (DC)** for the domain davidabank.local.
- Joined **Windows 10** client machine to the domain for centralized authentication and policy enforcement.
- Created a structured **Organizational Unit (OU)** hierarchy representing different departments (e.g., Tellers, Managers, Auditors, IT Admins).
- Created **users** and **security groups** mapped to realistic banking job roles.
- Implemented and applied **Group Policy Objects (GPOs)** to enforce password policies, restrict user capabilities (like disabling Control Panel and Command Prompt for Tellers), and enhance security.
- Configured role-based access to shared folders using **NTFS (New Technology File System)** permissions and **AD** security groups.
- Delegated administrative rights to **IT Admins** for managing specific OUs using the **Delegation of Control Wizard.**
- Enabled **auditing** to track login attempts, account changes, and other key events via **Windows Event Viewer**.

Tools and Operating Systems Used:

- **Windows Server 2022**
- **Windows 10 Pro**
- **Active Directory Domain Services (AD DS)**
- **DNS Server**
- **Group Policy Management Console (GPMC)**
- **Event Viewer**

2. **Environmental setup**

VM Configurations

VM Name	Role	Operating System	RAM	IP Address	Domain
Windows Server 2022	Domain Controller	Windows Server 2022	4GB	192.168.10.30	Davidabank.local
Windows 10 Pro	Domain-Joined Client	Windows 10 Pro	2GB	192.168.10.40	Davidabank.local

Virtualization Platform:

- **Hypervisor:** VM Workstation

Network Setup:

- **Network Type:** Host-Only Adapter (Isolated from external internet access)
- **Gateway/DNS:** No external router; DNS service provided by Davidabank

Domain Naming Convention:

- **Domain Name: davidabank.local**
- **Hostnames:**
    - Domain Controller: Davidabank
    - Client Machine: Client
- **OU Naming:** Reflects real banking departments (e.g., Tellers, IT_Admins, BranchManagers)

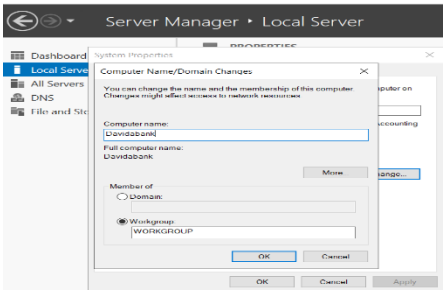
Notes:

- **Host-only network** ensures the lab simulates an enterprise LAN without real-world exposure.
- The **Windows Server** also functions as **DNS** for name resolution within the domain.

3. Domain Controller Installation – davidabank.local

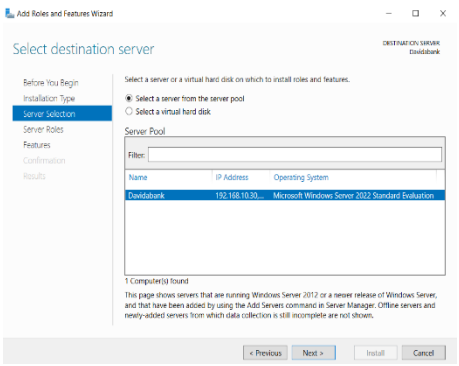
Step 1: Renamed the Server DavidaBank

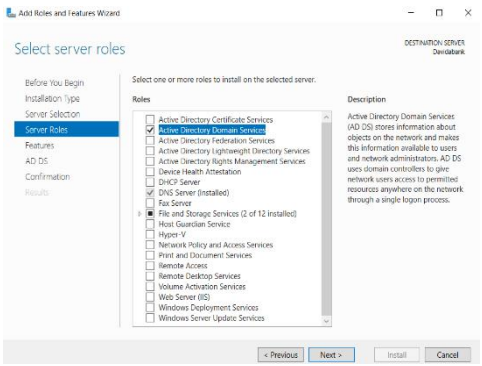
1. Opened **Server Manager** and navigated to **Local Server.**
2. Clicked on the existing **Computer Name** to access the **System Properties** window.
3. Entered the new name **DavidaBank**, and confirmed the change.
4. Restarted the server to apply the new computer name.



Step 2: Installed AD DS and DNS Roles

1. Opened **Server Manager**, clicked **Manage**, and selected **Add Roles and Features**.
2. Chose **Role-Based or Feature-Based Installation** and clicked **Next**.
3. Selected the local server (**Davidabank.local**) and continued by clicking **Next**.
4. Under **Server Roles**, I checked both **Active Directory Domain Services** and **DNS Server**.
5. Clicked **Next** through the **Features** and **Confirmation** sections, then clicked **Install** and waited for the installation to complete.

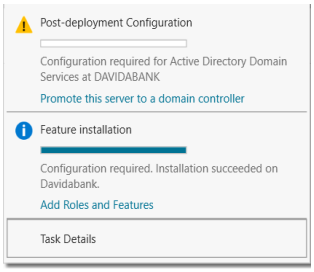


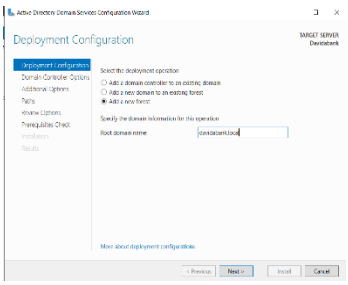


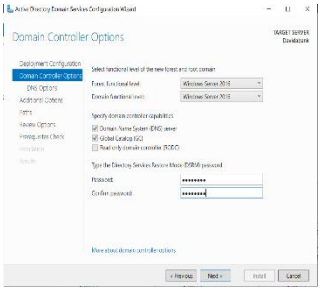
Step 3: Promoting the Server to a Domain Controller

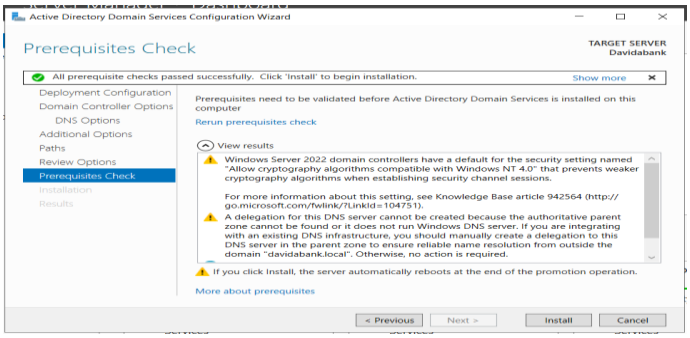
1. After the role installation, I clicked **"Promote this server to a domain controller"** from the yellow notification flag in **Server Manager**.

2. Selected **"Add a new forest"** and entered the root domain name as davidabank.local.
3. Set a **Directory Services Restore Mode (DSRM) password** and clicked **Next**.
4. Kept the **DNS** and **NetBIOS** settings at their default values, reviewed the selections, and clicked **Install**.
5. The server **automatically rebooted** after the promotion process completed.



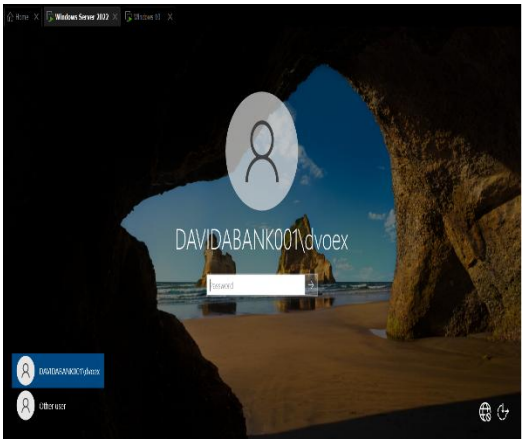


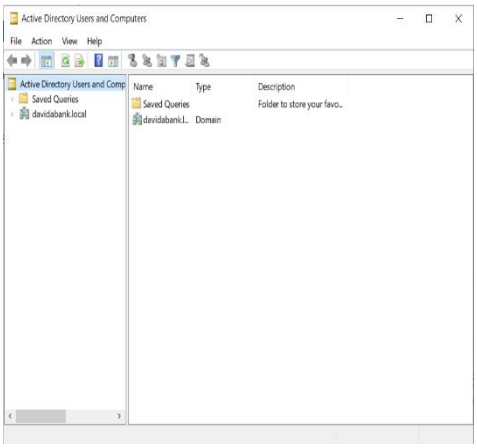


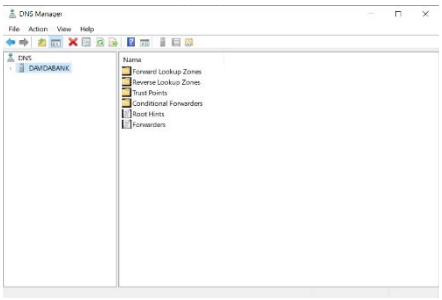


Step 4: Verifying Domain Controller Setup

1. After the server rebooted, I logged in as the **local administrator**.
2. Opened **Server Manager** and confirmed that both **Active Directory Domain Services (AD DS)** and **DNS** were listed as installed.
3. Opened **Active Directory Users and Computers (ADUC)** and verified that the domain **davidabank.local** was present.
4. Opened **DNS Manager** and confirmed that both the **forward** and **reverse lookup zones** had been successfully created.







Additional Notes:

- Static IP was configured prior to promoting to avoid DNS misconfiguration
- This server now acts as the **Primary Domain Controller (PDC)** and **DNS server** for the internal domain
- **ADUC** and **DNS Manager** are primary tools used post-installation for managing users, groups, and name resolution

4. Organizational Unit (OU) Structure

Davidabank.local

Steps Taken to Create OU Structire:

1. **Open Active Directory Users and Computers (ADUC)**
2. Right-click the domain root davidabank.local > **New > Organizational Unit**
3. Entered the name (e.g., "HeadOffice") and repeated for all departments and branches
4. Created sub-OUs under HeadOffice and BranchOffice to mirror real-world departments

Departments Created:

Under HeadOffice:

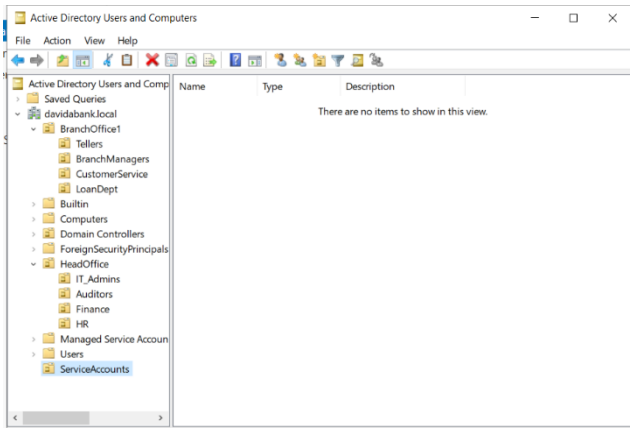
- IT_Admins
- Auditors
- Finance
- HR

Under BranchOffice1:

- Tellers
- BranchManagers
- CustomerService
- LoanDept

Top-Level OU:

- ServiceAccounts (for accounts used by backup systems, antivirus agents, and scheduled tasks)



Notes:

- This structure separates users by **location** and **job role,** improving administrative control
- Enables **GPO filtering** and **delegation** based on organizational responsibility.
- Follows least privilege principle by allowing GPOs to be scoped to only necessary OUs.
- OU names use PascalCase for consistency and readability.

5. **User and Group Configuration**

Users Created:

Head Office

IT_Admins – Femi S. Adebayo

Auditors – Blessing M. LAvia, Cynthia B. Chinemerem

Finance – Aishat G. Lawal, Funke J. Akindele

HR – Eniola K. Badmus, Odun A. Adekola

Branch Office

Tellers – Damola P. Akinwunmi, Neyo A. Ogun

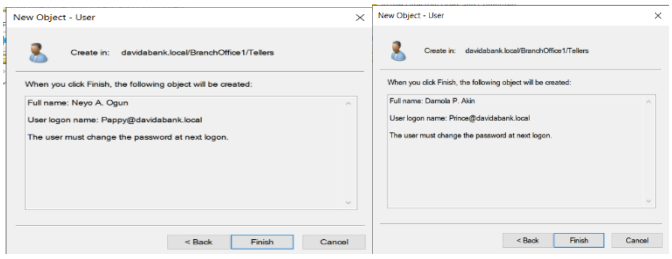
BranchManagers – Martin D. Badmus, Olamide F. Yekini

CustomerService - Dayo O. Fash, Olu D. Fash

LoanDept – Remi S. Ade, Seyi R. Ade

Steps to Create Users:

1. Open **Active Directory Users and Computers (ADUC)** and navigate to the appropriate OU (e.g., Tellers)
2. Right-click the OU > **New > User**
3. Enter details:
    - First name, Last name
    - User logon name (e.g., pappy@davidabank.local)
4. Set password (choose "Password never expires" or "User must change at next logon" as needed)
5. Repeat for all users



Steps to Create Groups and Assign Memberships:

1. In ADUC, navigate to the corresponding OU (e.g., Tellers)
2. Right-click the OU > **New > Group**

    - Name: e.g., Tellers
    - Scope: **Global**
    - Type: **Security**
3. Right-click the group > **Properties > Members > Add**
4. Type the username (e.g., pappy), click **Check Names,** and add
5. Repeat for each group and department

Group Type Used:

- **Global Security Groups:** For assigning permissions and targeting GPOs
- **Built-In Groups:**
  • Domain Admins (for tclark – IT Admin)

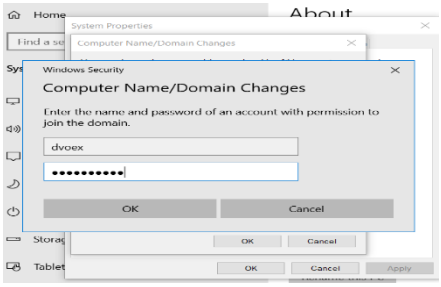
Notes:

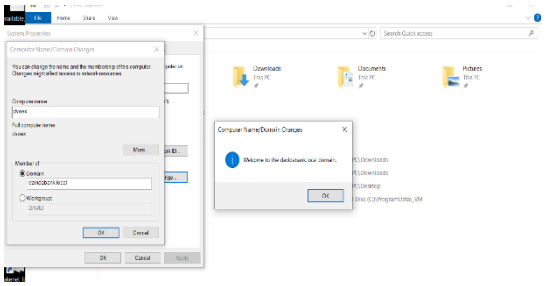
- Users were placed in OUs that reflect both **physical location** and **department function**
- Group memberships simplify the application of **GPOs** and **NFTS permissions** later in the lab
- Password policy was enforced as per domain settings

6. **Domain Join (Windows 10)**

Steps to Join Windows 10 to the Domain

1. **Verify Network Connectivity**
    - Ensure Client has the correct **static IP address** (e.g., 192.168.10.40)
    - DNS **must point to the Domain Controller** (Davidabank, IP: 192.168.10.30)
    - Test by pinging the domain controller:
      • ping Davidabank.local (from command prompt)
2. **Join the Domain**
    1. Right-click **This PC > Properties**
    2. Click **Rename this PC (Advanced) >** then click **Change**
    3. Under **Member of,** select Domain and enter davidabank.local
    4. When prompted, enter **domain credentials** (e.g., davidabank\dvoex)
    5. You will see a welcome message: "welcome to the davidabank.local domain"
    6. Click **OK and restart the system**

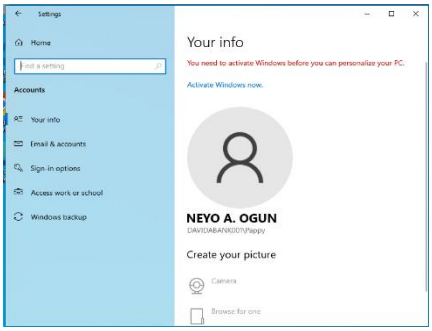




3. **Verify the Join Was Successful**
    - After reboot, login screen should show:
      • **Other User**
      • Sign in to: davidabank.com
    - Use a domain account (e.g., Pappy) to log in, and Windows will prepare a **new profile** for the domain user

Login Verification:

- Logged in successfully using Pappy (Teller) account
- Confirmed domain login by checking:
  • System Properties > Computer Name
- User Accounts info in **Start > Settings > Accounts**



Notes:

- Windows 10 must use the **domain controller as its DNS** server for successful join
- After login, a new user profile is created under C:\Users\jdoe
- Domain policies will be applied automatically if GPOs are configured
- This confirms that the domain controller is functioning and client communication is successful

7. Group Policy Objects (GPO)

GPO Name	Linked To	Purpose
SecurityBaseline	Davidabank.local (Domain Root)	Applies standard security settings across all domain computer
TellerRestrictions	BranchOffice1\Tellers	Restricts desktop access and user rights for Teller users
ITAdminPolicy	HeadOffice\IT_Admins	Enables tools and privileges required for IT admins
DisableUSB_HR	HeadOffice\HR	Blocks USB storage device access for HR users

Steps to Create and Link GPOs

1. Open **Group Policy Management Console (GPMC)**
   - Server Manager > **Tools > Group Policy Management**
2. Right-click the appropriate OU (e.g., Tellers) > **Create a GPO in this domain, and Link it here**
3. Name the GPO (e.g., TellerRestrictions) and click **OK**
4. Right-click the new GPO > **Edit** to open the Group Policy Management Editor

Key GPO Settings Applied:

1. **SecurityBaseline GPO**

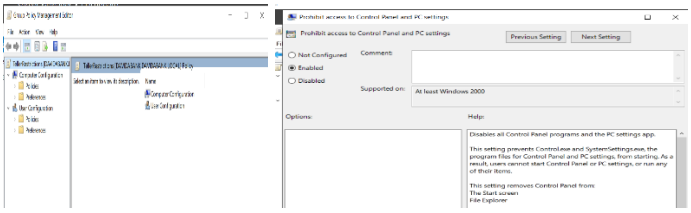
   Path: Computer Configuration > Policies > Windows Settings > Security Settings

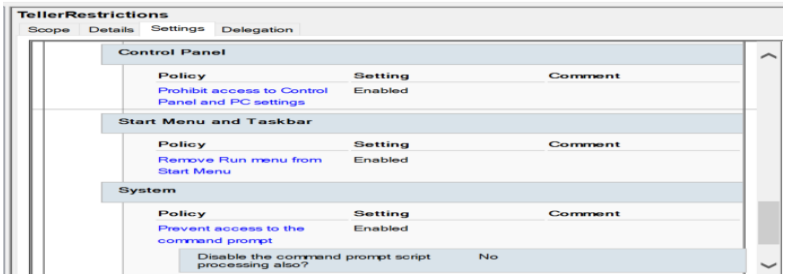
   - **Account Lockout Policy**: Lock after 3 failed attempts
   - **Minimum password length:** 16 characters
   - **Password complexity: Enabled**

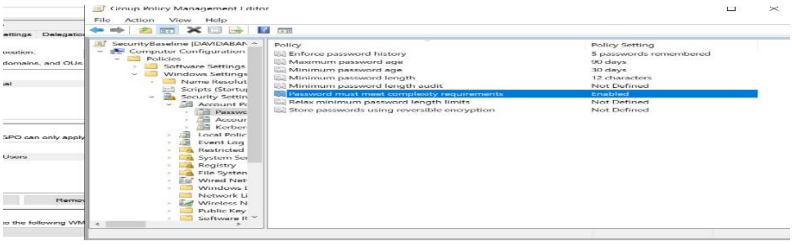
2. **TellerRestrictions GPO**
   Path: User Configuration > Policies > Adminstrative Templates
   - **Hide Control Panel and Settings:** Enabled
   - **Prevent access to command prompt:** Enabled
   - **Remove Run menu from Start Menu:** Enabled
   - **Disable Task Manager:** Enabled
3. **ITAdminPolicy GPO**
   Allows access to:
   - Powershell
   - Command Prompt
   - Device Manager
   - Control Panel
4. **DisableUSB_HR GPO**
   Path: Computer Configuration > Policis > Administrative Templates > System > Removable Storage Access
   - **All Removable Storage classes: Deny all access:** Enabled

Notes:

- GPOs were carefully scoped to **specific OUs** to prevent unnecessary restrictions across the entire domain
- Settings were tested on Client using domain accounts to confirm proper policy application
- This demonstrates ability to enforce **departmental security policies** in a realistic corporate environment







8. **Role-Based Access Control (RBAC)**

Access Matrix

Folder	Group Name	Permission Level	OU Location
\\fileserver\Tellers	Tellers	Read, Write	BranchOffice\Telllers
\\fileserver\HR	HR	Modify	HeadOffice\HR
\\fileserver\Finance	Finance	Modify	HeadOffice\Finance
\\fileserver\Audit	Auditors	Read-only	HeadOffice\Auditors
\\fileserver\IT	IT_Admins	Full Control	HeadOffice\IT_Admins

Steps to Implement RBAC:

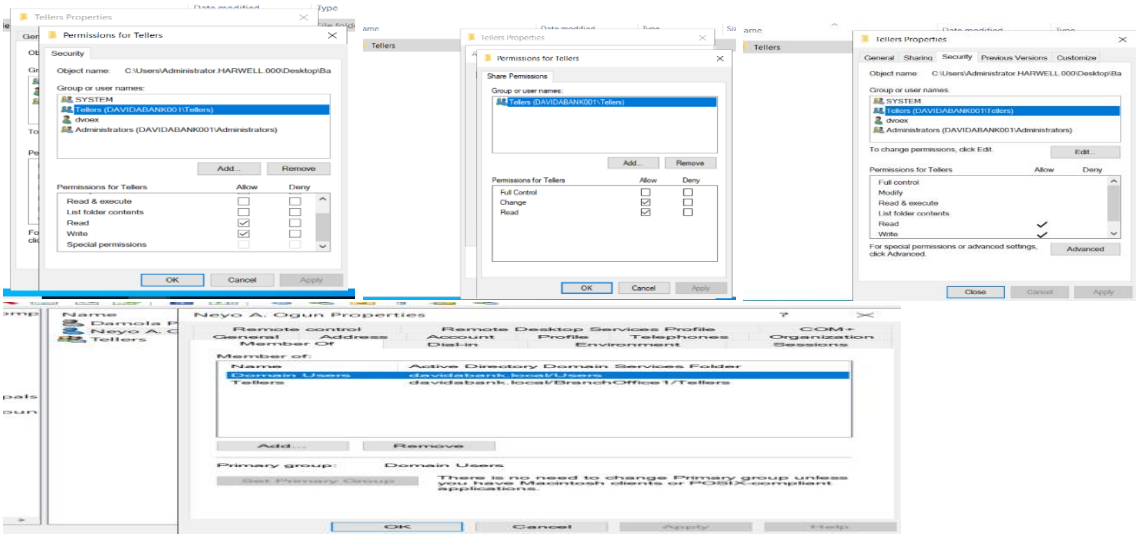
1. **Folder Creation on File Server**
   - On Windows Server (acting as File Server):
     • Create folders (e.g., C:\BankShares\Tellers)
     • Right-click folder > **Properties > Sharing**
       • Share as \\BankDC01\Tellers (or use a dedicated File Server)
       • Click **Permissions >** Remove "Everyone"
       • Add group (e.g., Tellers) and assign **Read/Write**
2. **Set NFTS Permissions**
   - Go to **Security** tab under folder properties:
     • Click **Edit >** Add group (e.g., Tellers)
     • Assign NTFS permissions:

- **Tellers:** Allow – Read & Write
- **Administrator:** Full Control
- Remove inheritance if stricter control is needed

3. **Add Users to Groups**
   - Use **ADUC:**
     - Navigate to each user's OU (e.g., Tellers)
     - Right-click user > **Properties > Member Of** > Add group (e.g., Tellers)

Notes:

- Security groups were used instead of individual users to allow acalable and manageable access control
- RBAC enforces strict boundaries between departments (e.g., Tellers can't access HR data)
- This structure is easily extensible to new branches or departments
- Proper permssions reduce risk of **data leaks, accidental modifications,** or **internal threats**



9. **Delegation and Access Control**

Steps to Delegate Control

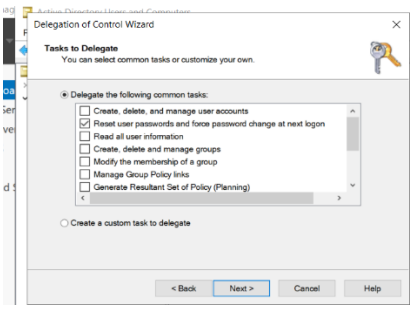
1. **Open ADUC** and navigate to BranchOffice1 > Tellers
2. Right-click on the Tellers OU > **Delegate Control**
3. Click **Next** on the welcome screen
4. **Add the delegated user or group** (e.g., Teller)
5. Select **"Delegate the following common tasks"**
   - Choose:
     - **Reset user passwords and force password change at next logon**

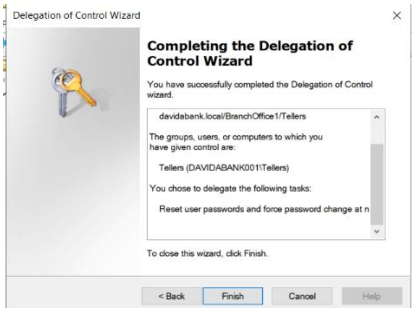
6. Click **Next > Finish**

Group Name	Purpose	Scope
Teller	Delegated rights over Tellers OU only	Global Security

Notes:

- Delegation ensures **least privilege** access for junior support staff
- Admin control was restricted to only the **Tellers OU,** enforcing **OU-based management boundaries**
- This prevents accidental or malicious changes in unrelated departments
- The **Delegation Wizard** is a powerful tool that avoids giving full-blown administrative rights unnecessarily





10. Logging and Monitoring

Audit Policy Configuration

1. Open **Group Policy Management Console (GPMC)**
2. Edit the **SecurityBaseline** GPO (created earlier)
3. Navigate to:
   Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Audit Policy
4. Enable the following settings:
   - **Audit account logon events –** Success, Failure
   - **Audit logon events –** Success, Failure
   - **Audit account management –** Success, Failure
5. Close and apply the GPO. Run gpupdate /force on clients

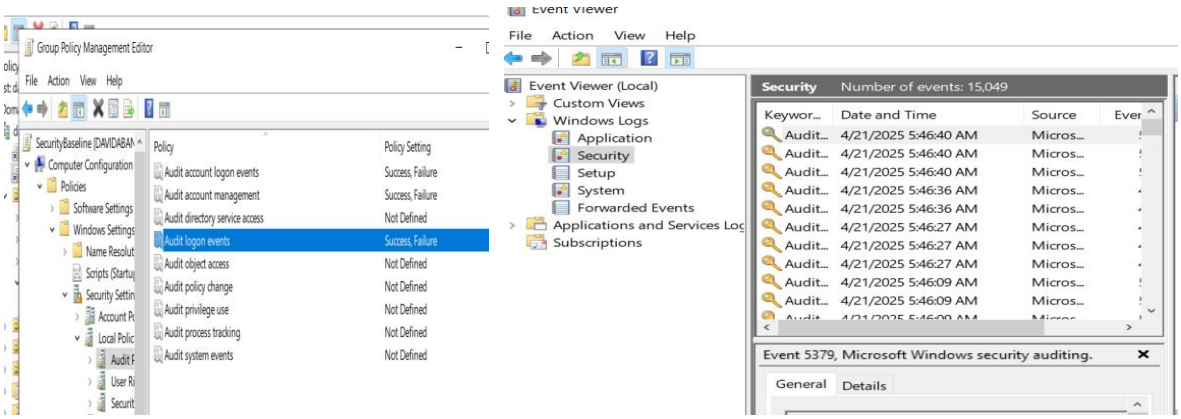
Event Viewer Usage

1. Log in to Windows Server (BankDC01)
2. Open **Event Viewer** (Start > Event Viewer)

3. Expand: Windows Logs > Security
4. Look for relevant **Event IDs:**

Notes:

- These audit logs provide **detailed forensic trail** for user and administrator actions
- In a production banking environment, logs should be forwarded to a **SIEM** like **Security Onion** or **Splunk**
- This configuration ensures that **compliance and investigation needs** can be met
- Use ”**Filter Cureent Logs”** in Event Viewer to quickly isolate relevant activities.



11. Challenges faced and resolution

12. Security engineer Insights

13. Conclusion