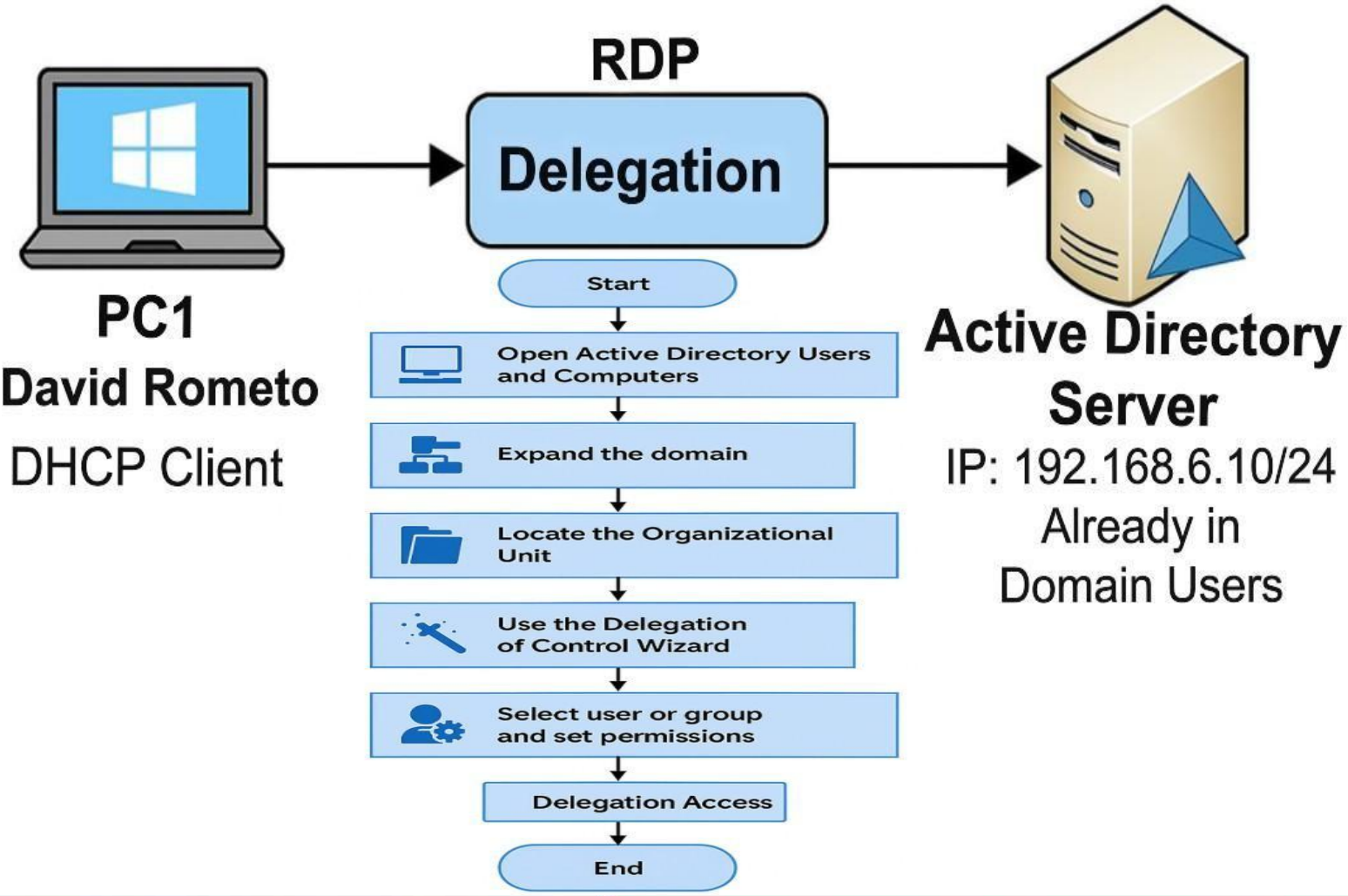
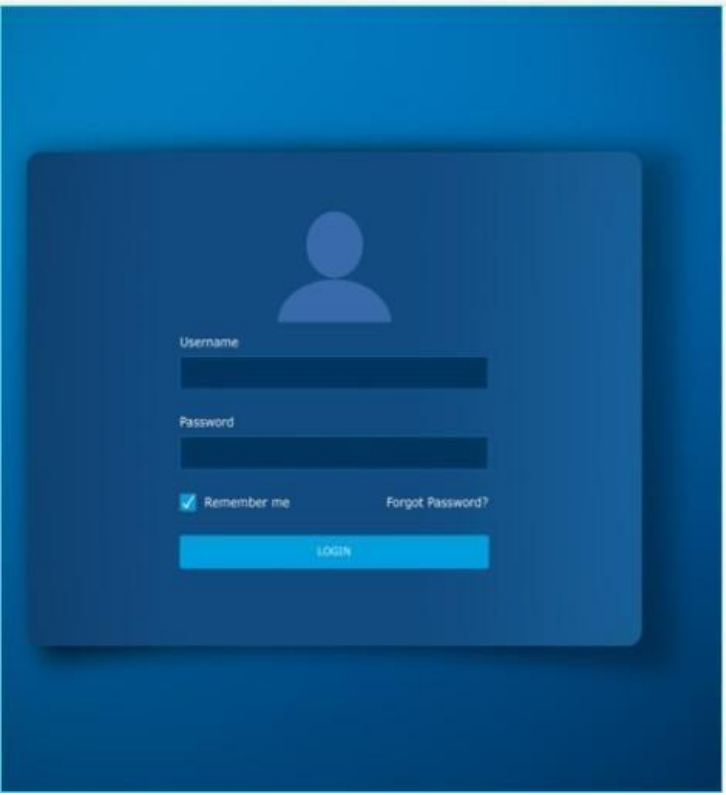
Delegate Access in Active Directory

Empowering IT Teams with Secure Role-Based Permissions





WHAT IS DELEGATION IN ACTIVE DIRECTORY?

Definition of Delegation

Delegation grants specific permissions without giving full Domain Admin rights to users or groups.

Tasks Enabled by Delegation

Delegated users can reset passwords, manage user accounts, and control groups within specific OUs.

Security and Efficiency Benefits

Delegation distributes administrative tasks securely and efficiently, maintaining domain security.

Use of Delegate Control Wizard

The Delegate Control Wizard simplifies assigning permissions for specific actions in Active Directory.

❖ Delegation in AD means giving specific permissions to someone for an OU without making them a Domain Admin. For example, you can allow IT staff to reset passwords or create users in the Employees OU.

➢ Open ADUC

Click Start → Administrative Tools → Active Directory Users and Computers.

➢ Expand Your Domain

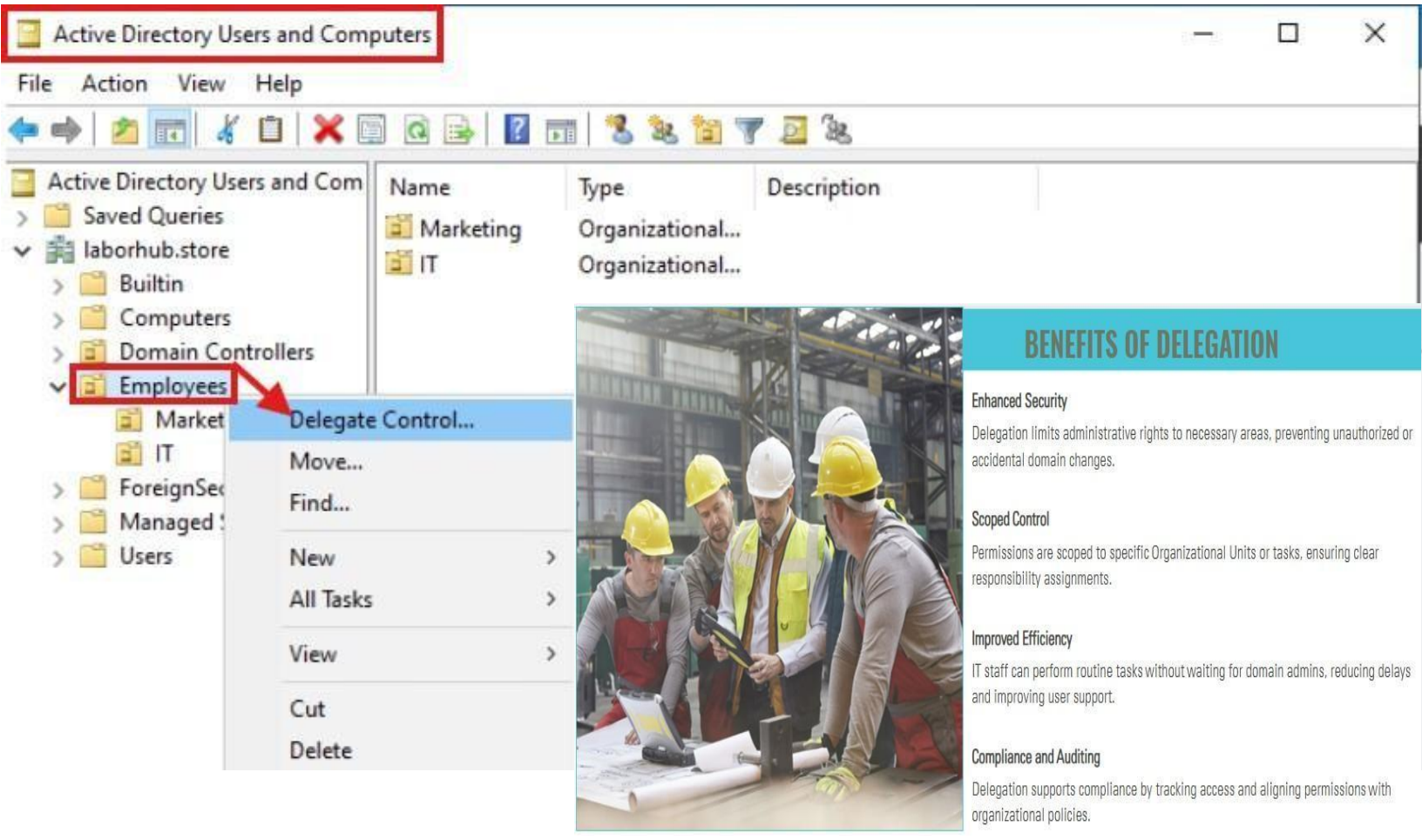
In the left pane, expand your domain (e.g., laborhub.store).

➢ Locate the OU

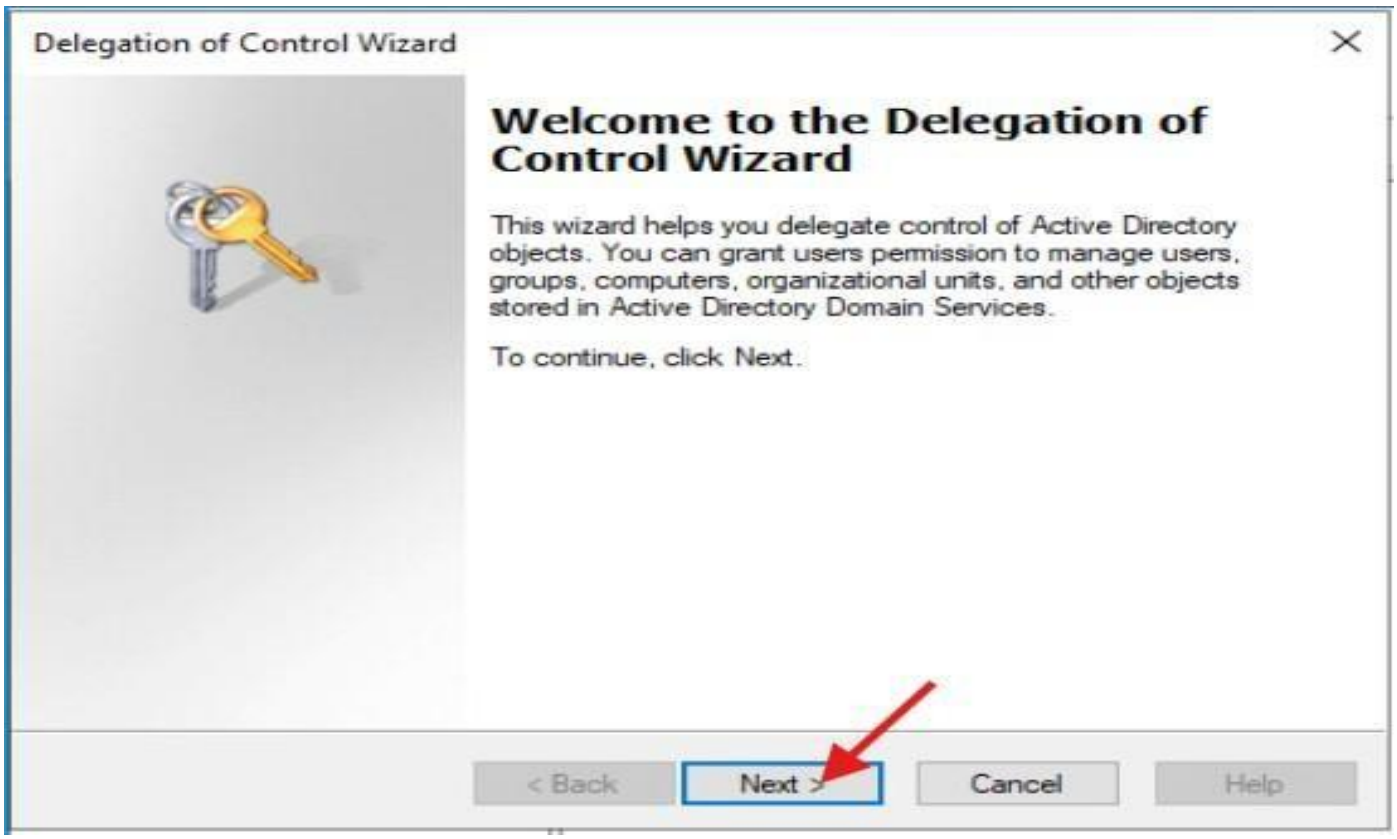
Find the OU you want to delegate permissions for (here, Employees).

➢ Right-Click the OU

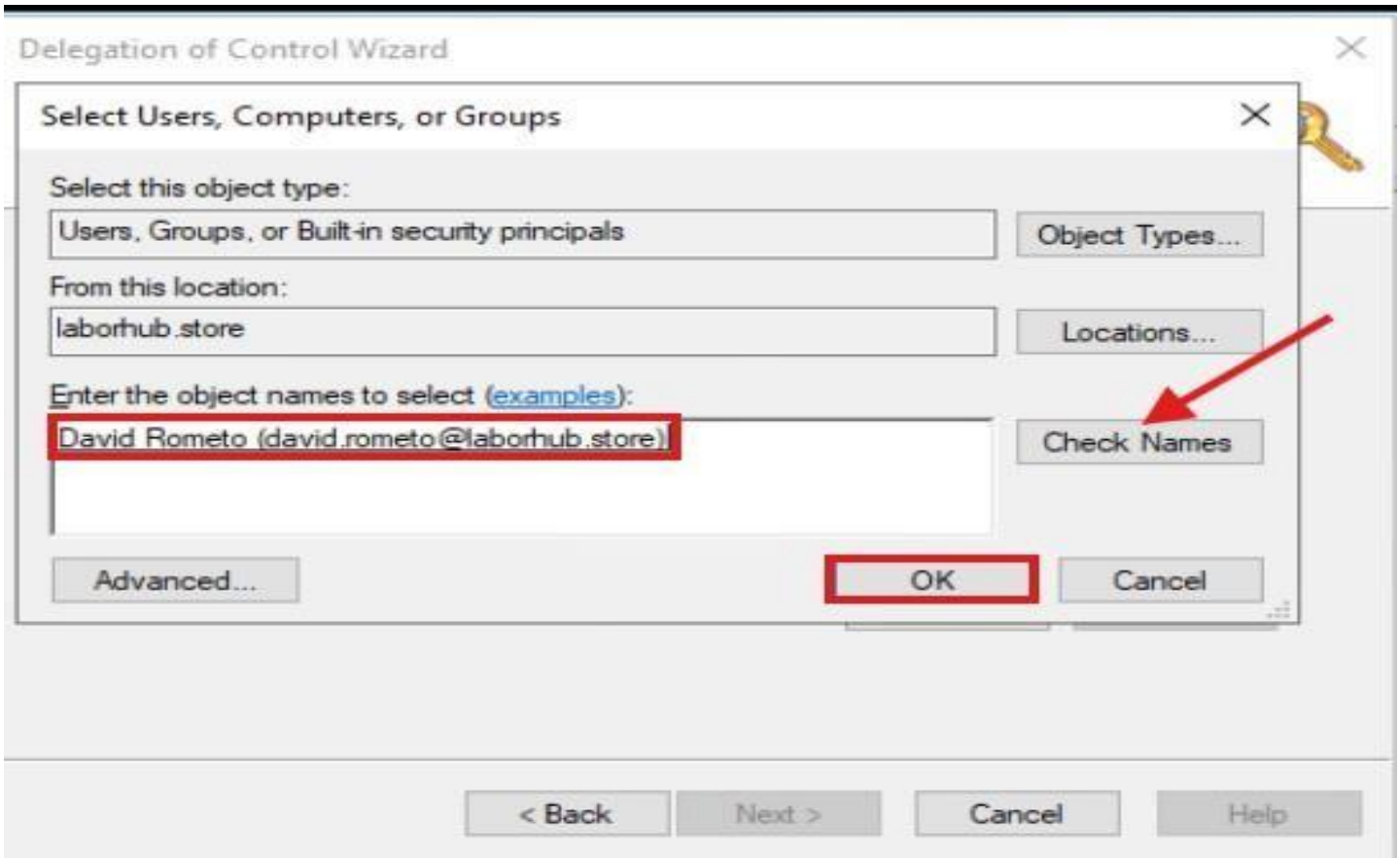
Select Delegate Control… from the context menu.



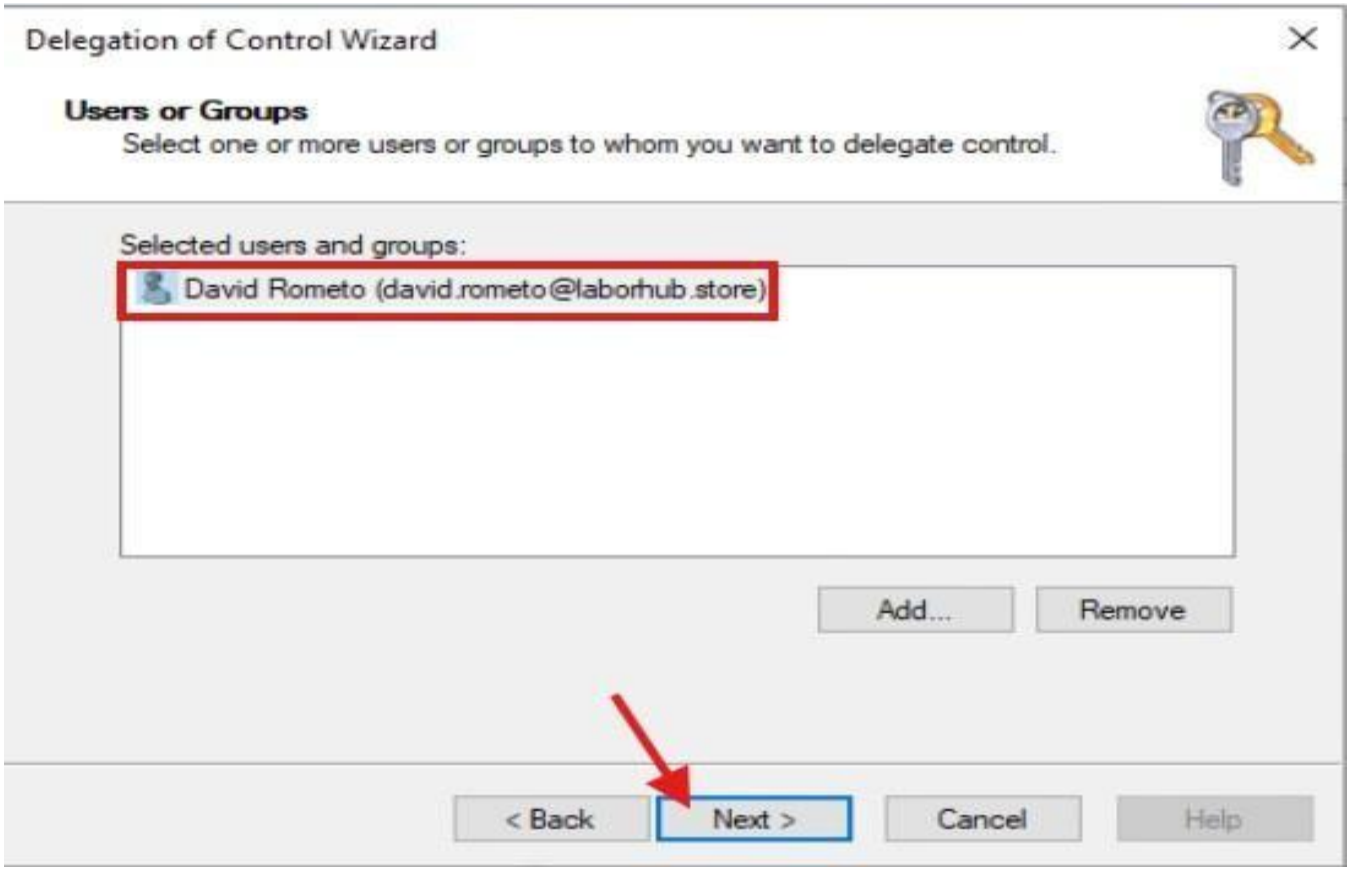
- This is the welcome screen of the Delegation of Control Wizard. Click Next to begin assigning permissions for an Active Directory Organizational Unit (OU).



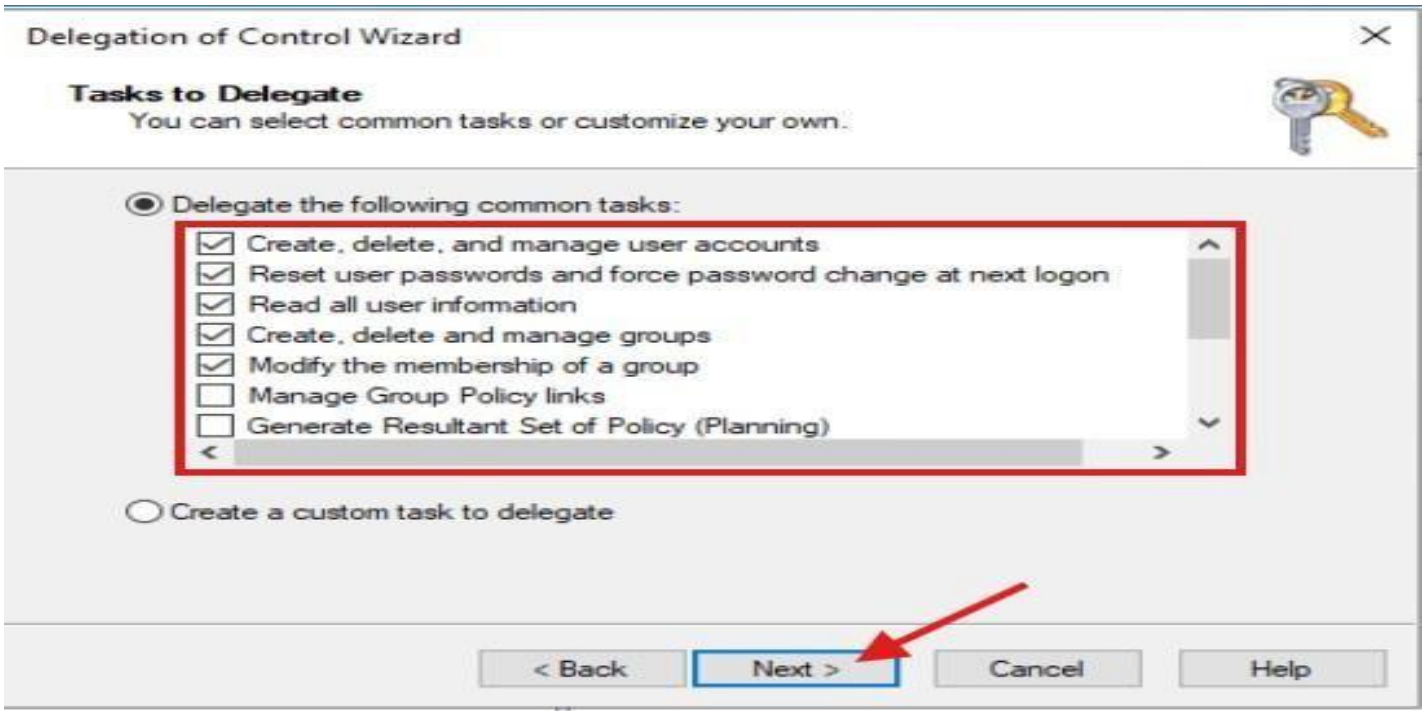
- Select the user or group (in this case, David Rometo) to delegate control, click Check Names to verify, and then click OK to proceed.



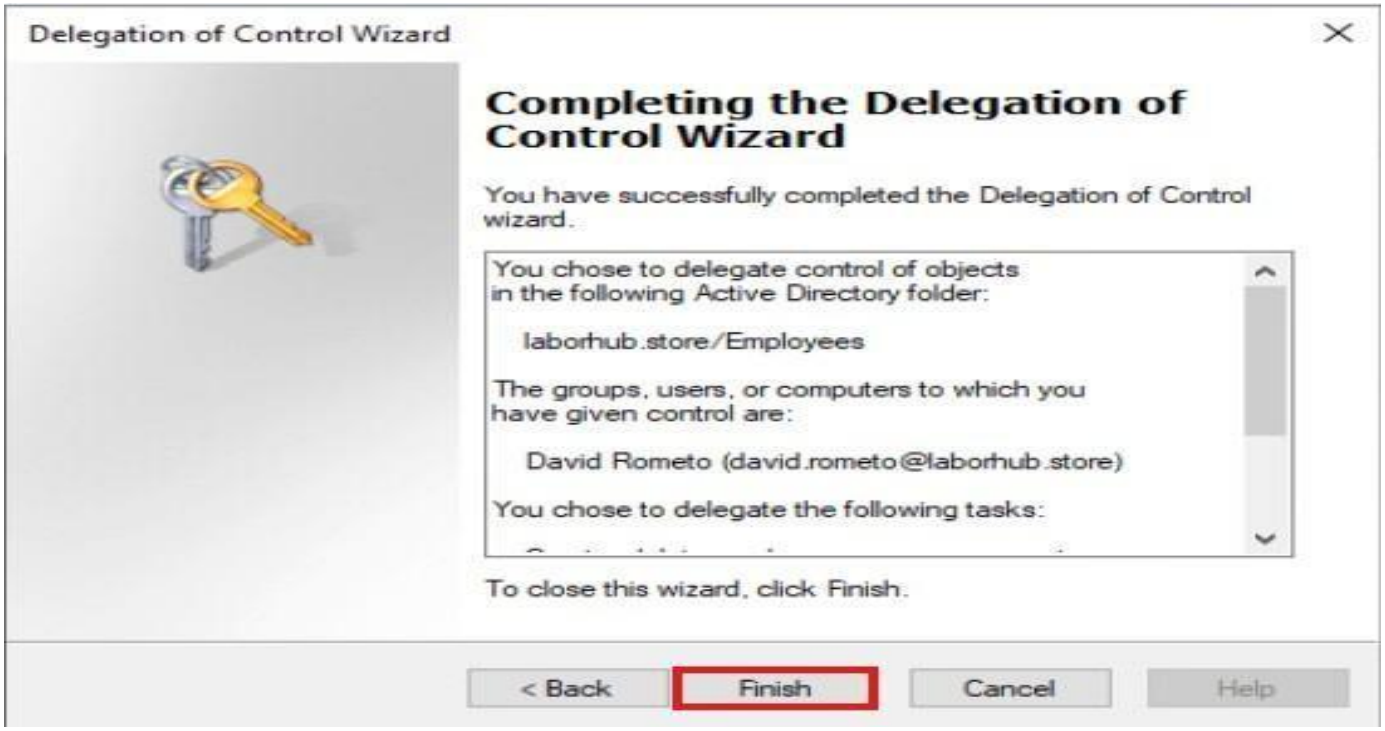
❖ Confirm the selected user or group for delegation (David Rometo) and click Next to proceed.



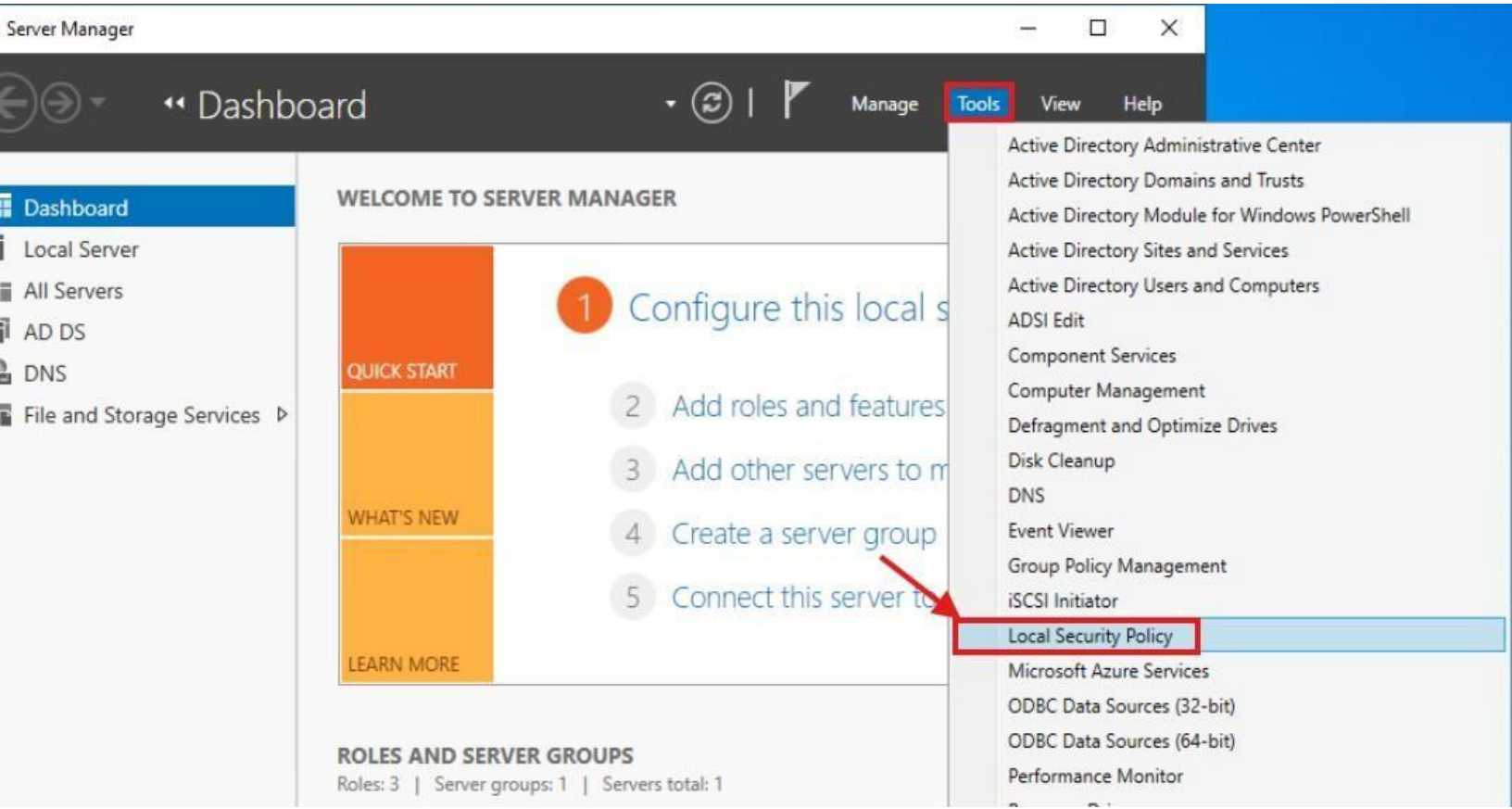
❖ "This step in the Delegation of Control Wizard allows you to assign specific tasks such as managing user accounts, resetting passwords, and handling groups without granting full Domain Admin rights. It's a secure way to delegate responsibilities while maintaining control.



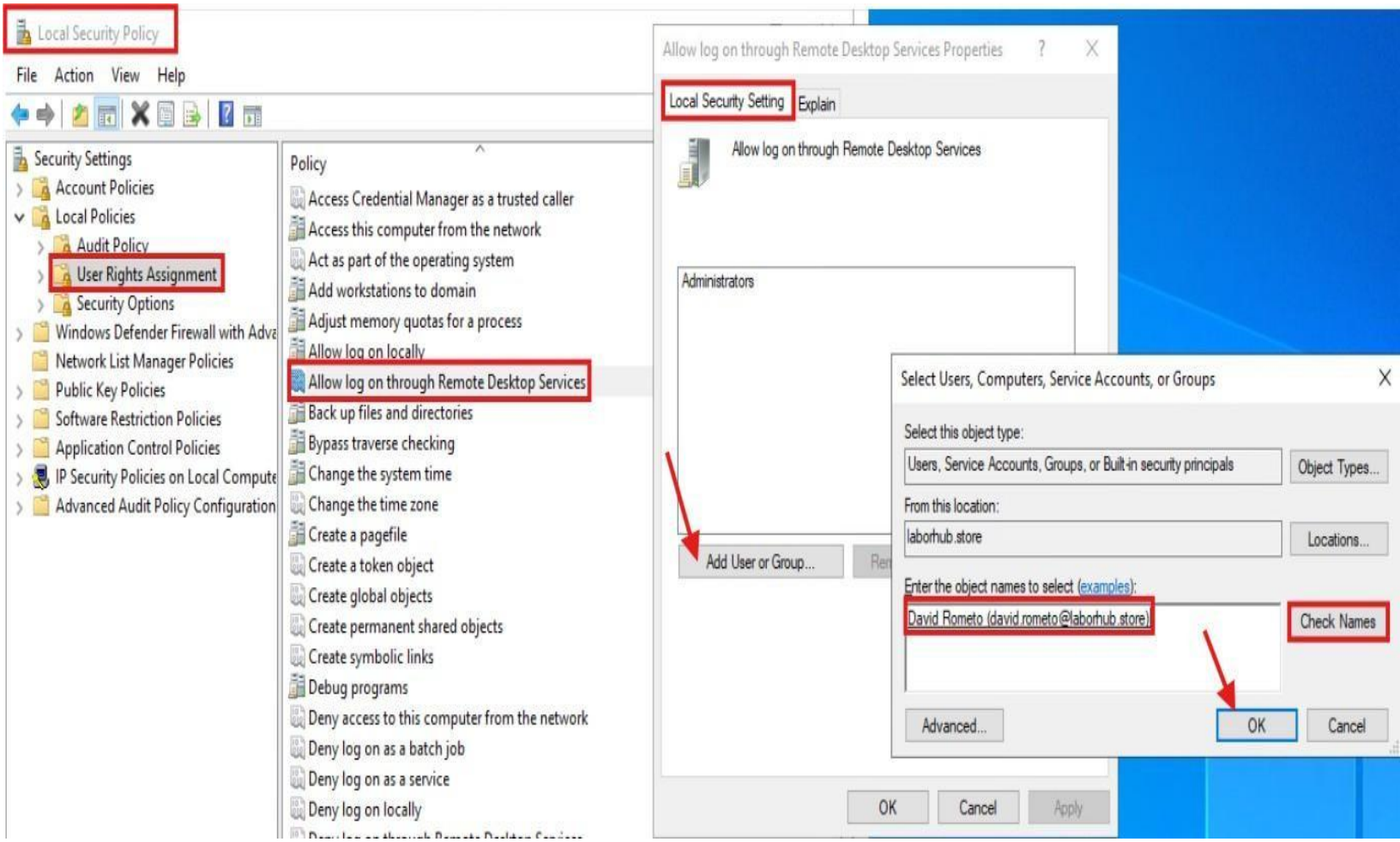
- Delegation completed: Control of the Employees OU is assigned to a specific user with selected permissions, ensuring secure administration without full Domain Admin rights.



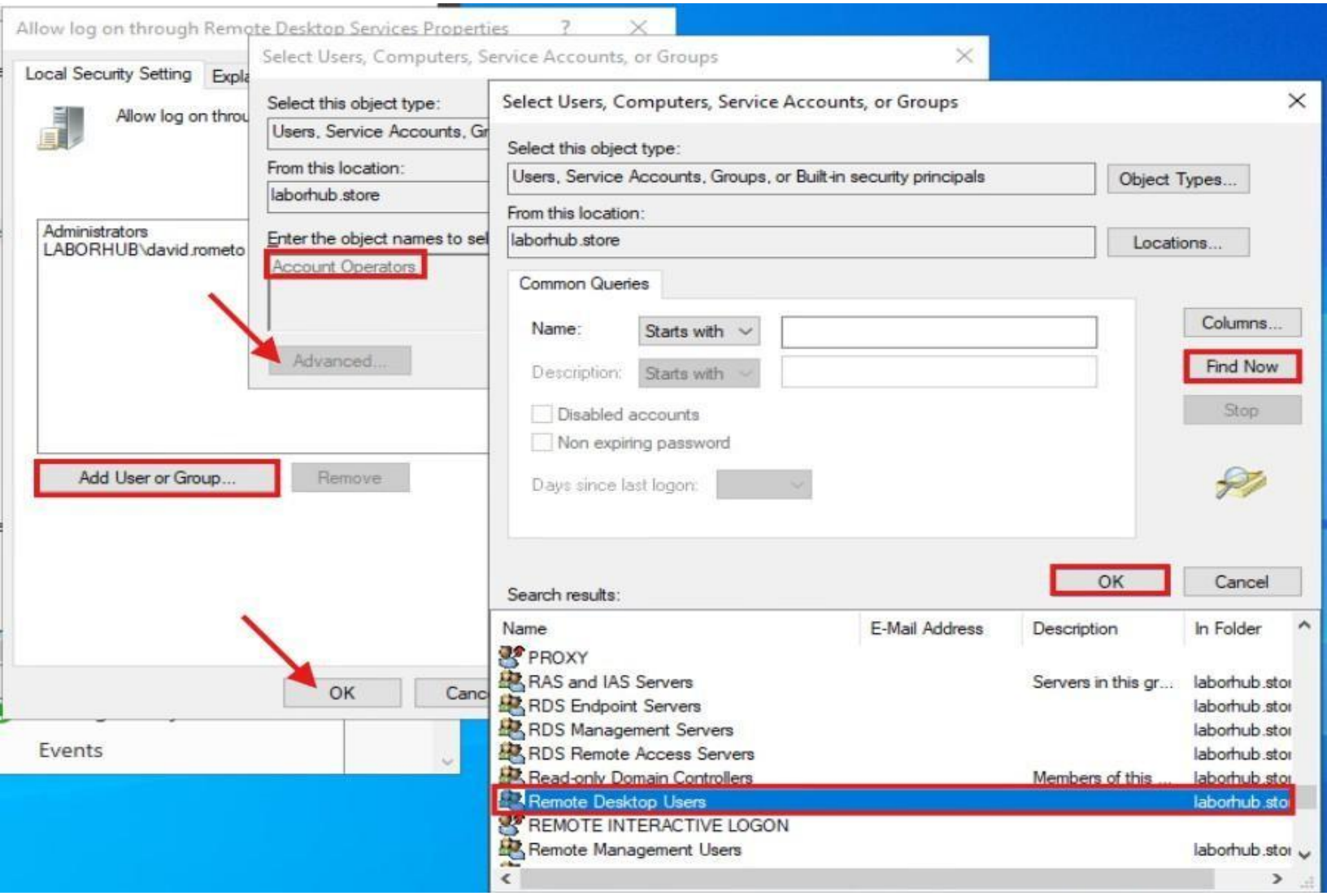
- Access Local Security Policy in Server Manager to configure security settings ensuring strong protection and compliance.
  - Server Manager → Tools → Local Security Policy



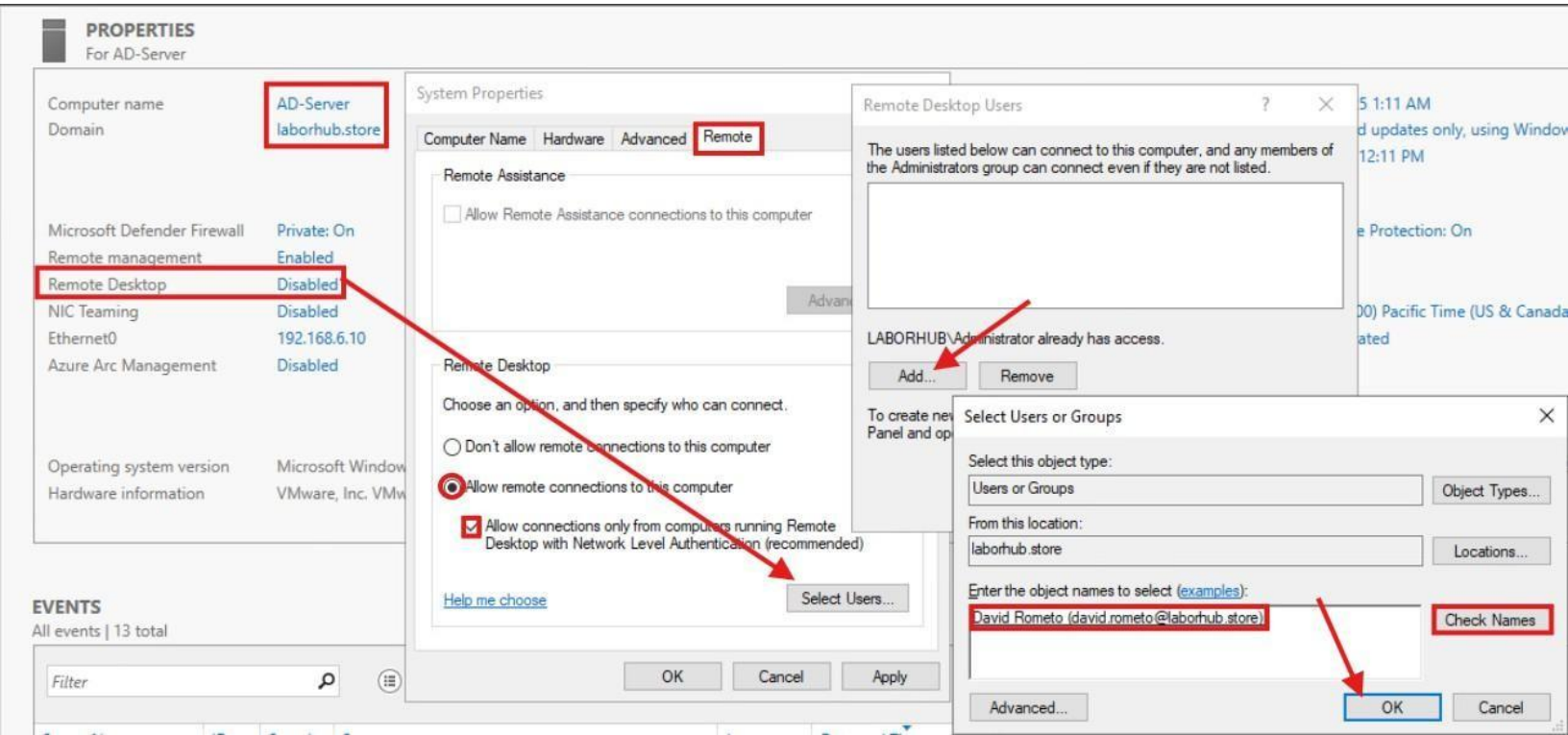
- Configuring Local Security Policy to allow Remote Desktop access: Navigate to User Rights Assignment, select 'Allow log on through Remote Desktop Services,' and add the required user. This ensures secure and controlled RDP access.



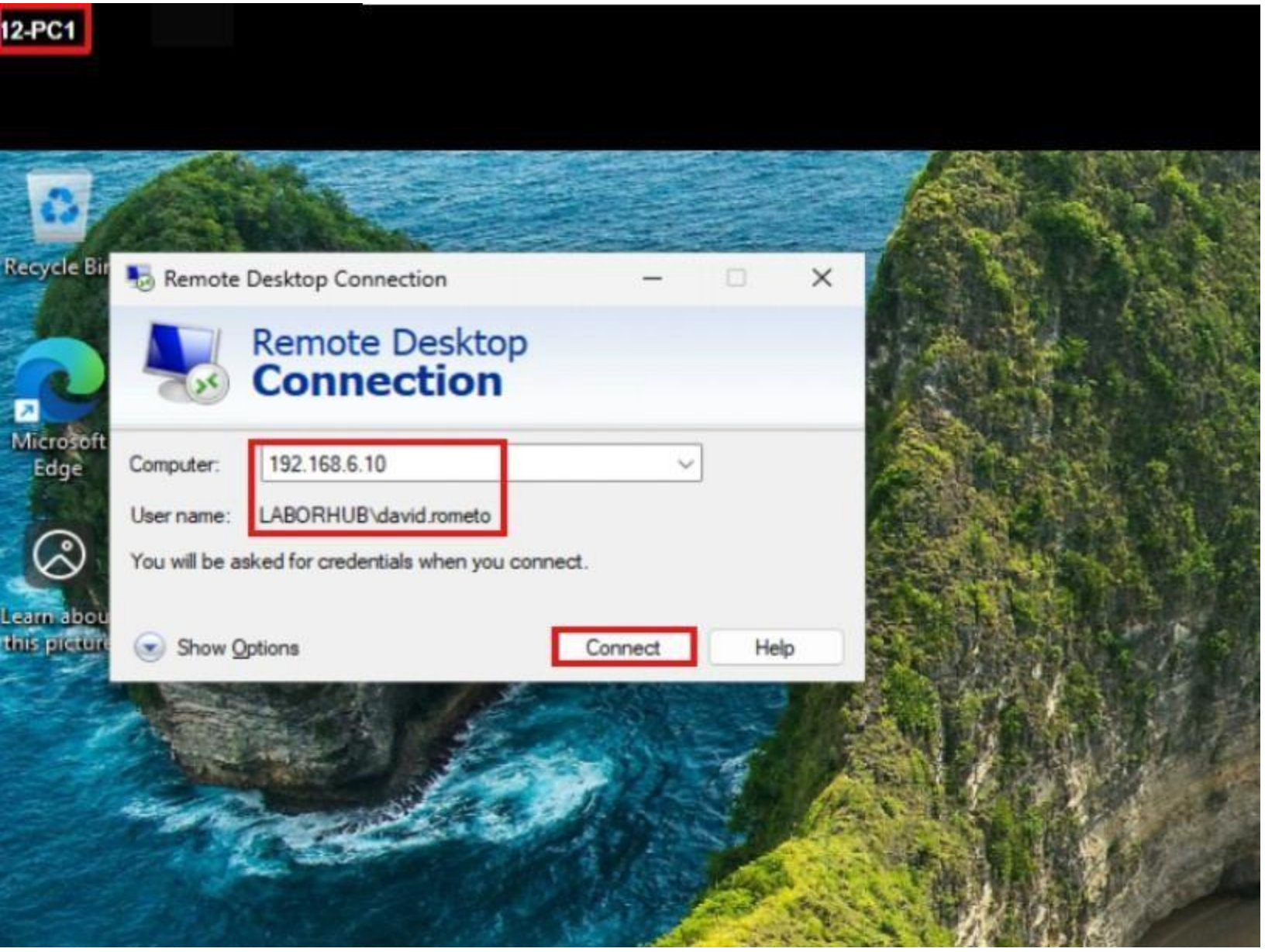
- Granting Remote Desktop access via Local Security Policy: Add the 'Remote Desktop Users' group under the policy 'Allow log on through Remote Desktop Services.' This ensures secure and role-based RDP permissions.



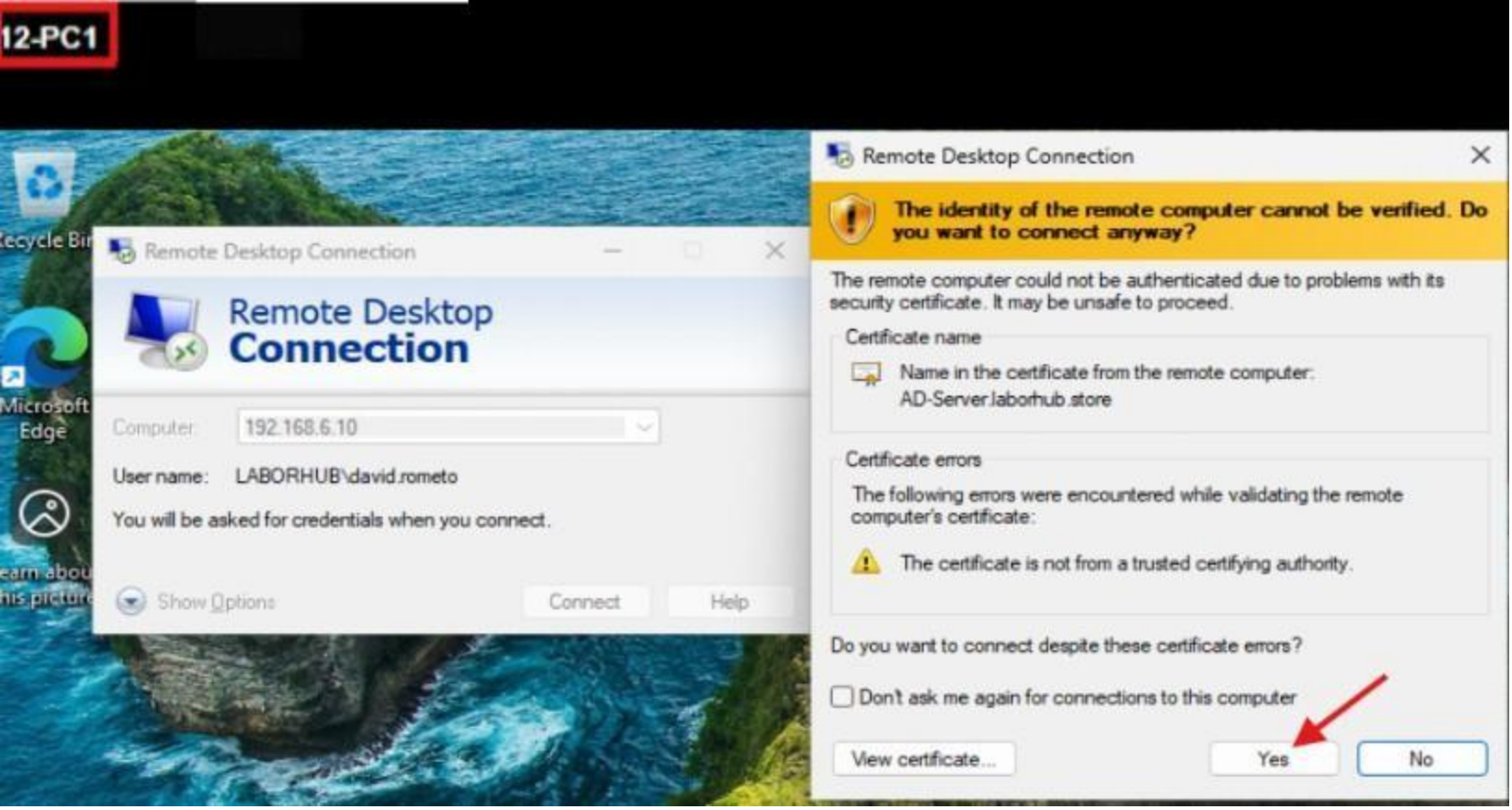
Enable Remote Desktop with Network Level Authentication and add authorized users for secure, controlled access.



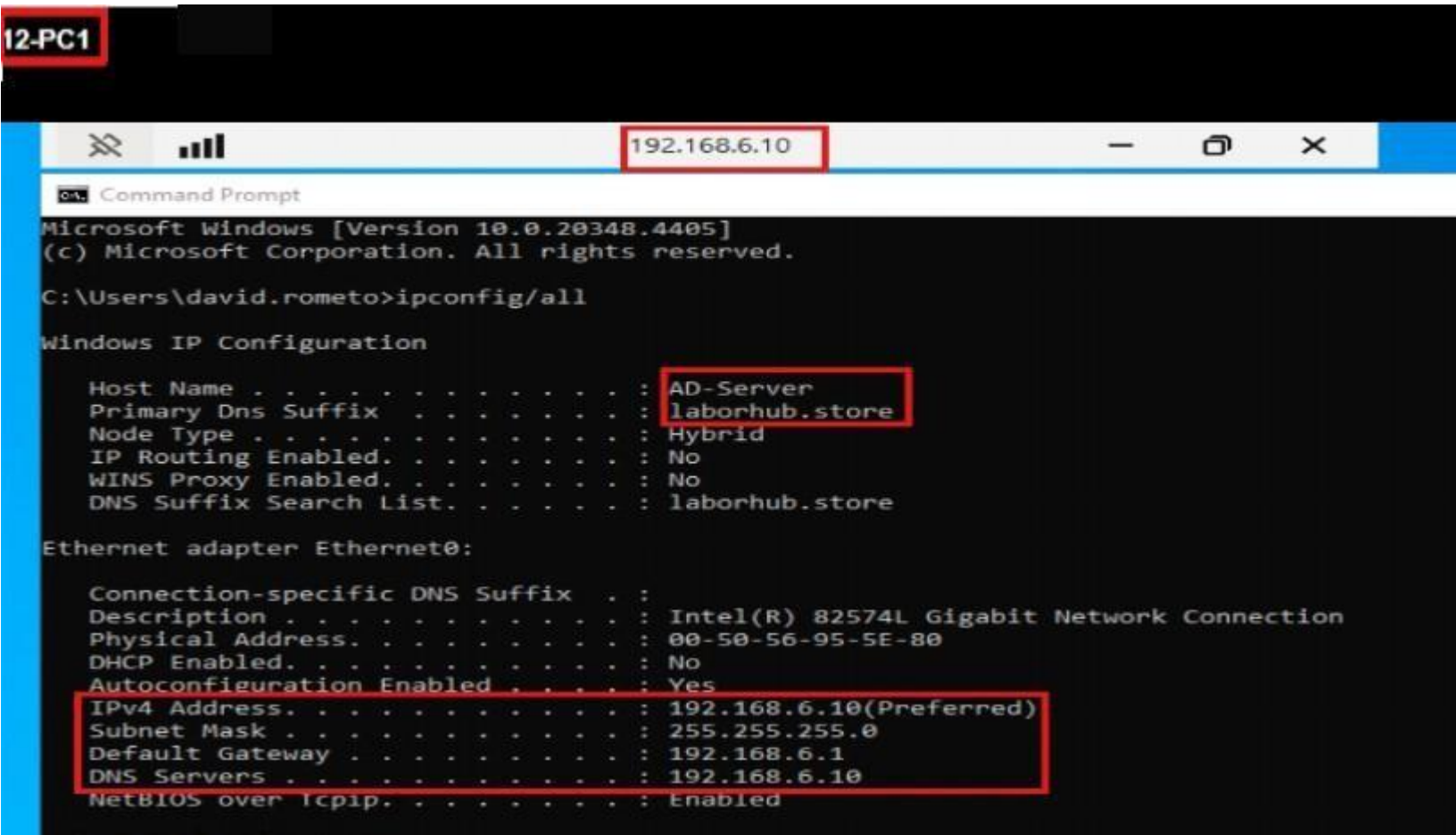
- Connecting to an Active Directory Server via Remote Desktop: Enter the AD server IP (192.168.6.10) and use the same delegated user credentials, then click Connect for secure remote access.



- When connecting to an AD server via Remote Desktop, you may see a certificate warning. This occurs if the server's certificate isn't trusted. Click 'Yes' to proceed if you trust the connection, or install a valid certificate for secure authentication.



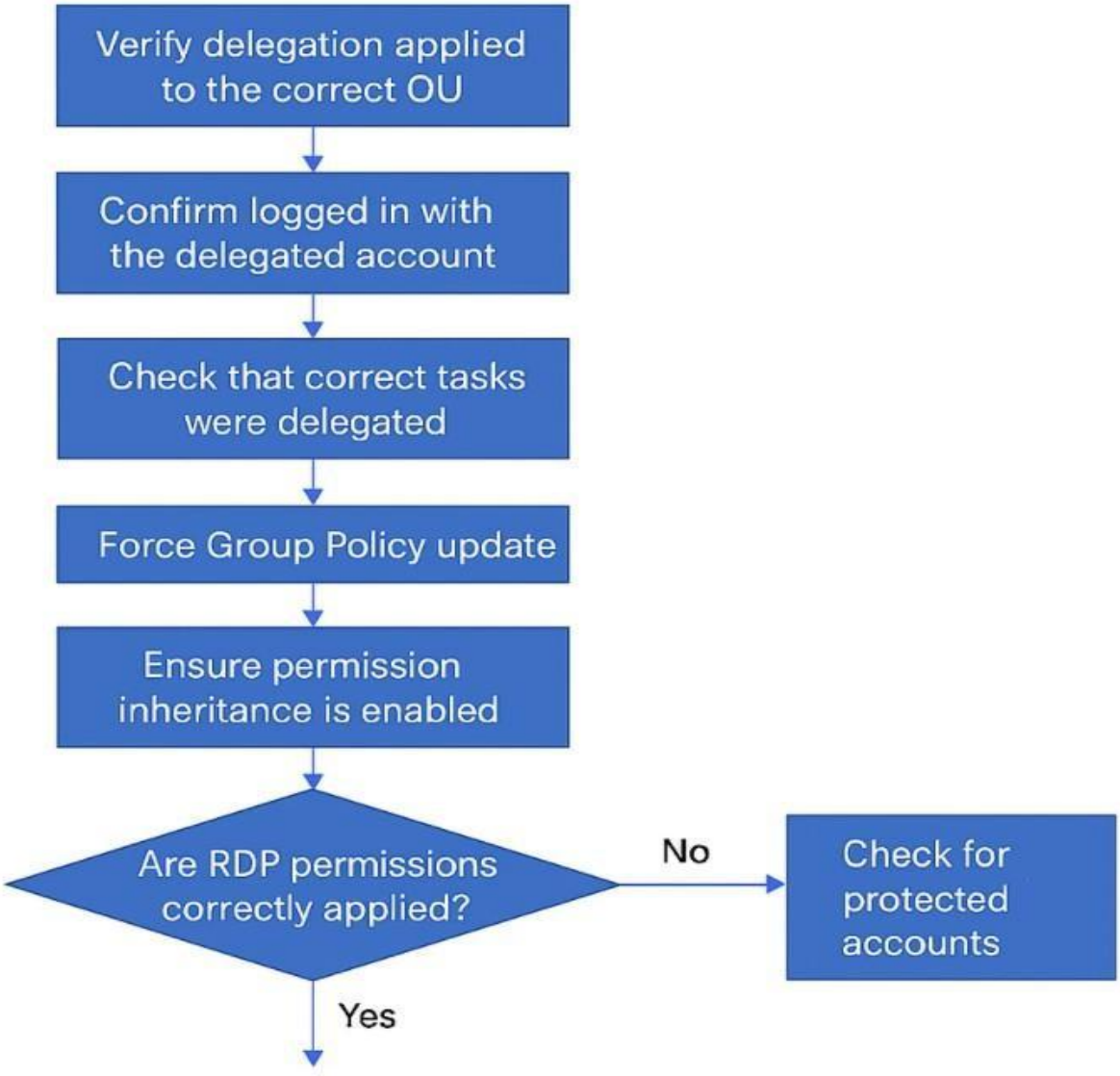
- Verifying AD Server connectivity: The server (192.168.6.10) is properly configured as IP and DNS for laborhub.store. Delegated user connects via Remote Desktop from PC1 to ensure secure access and functionality.



Troubleshooting Delegation in Active Directory

RESOLVING PERMISSION ISSUES WITHIN DIRECTORY SERVICES

Troubleshooting Delegation in Active Directory



Basic Troubleshooting for Delegation Access in Active Directory

1. Check Delegation on the Correct OU

Path:

Start → Administrative Tools → Active Directory Users and Computers → Domain (laborhub.store) → OU → Right-click OU → Properties → Security → Advanced

Purpose:

Verify the delegated user or group has permissions on the correct OU.

2. Confirm Logged-In Delegated Account

Path:

Start → Command Prompt → `whoami`

Purpose:

Ensure you are logged in using the correct delegated domain account.

3. Verify Delegated Tasks

Path:

Active Directory Users and Computers → Right-click OU → Delegate Control... → Delegation of Control Wizard → Tasks Selection

Purpose:

Confirm required tasks (reset passwords, create/delete users, manage groups) were selected.

4. Force Group Policy Update

Path:

Start → Command Prompt → Run as Administrator → `gpupdate /force`

Purpose:

Apply delegation and permission changes immediately.

5. Check Permission Inheritance

Path:

Active Directory Users and Computers → Right-click OU → Properties → Security → Advanced → Enable Inheritance

Purpose:

Ensure delegated permissions are inherited correctly.

6. Verify Remote Desktop Access (If Using RDP)

➢ Allow RDP Logon:

Path:

Server Manager → Tools → Local Security Policy → Local Policies → User Rights Assignment → Allow log on through Remote Desktop Services

➢ Check Group Membership

Path:

Computer Management → Local Users and Groups → Groups → Remote Desktop Users

Purpose:

Confirm the delegated user is allowed to access the server via RDP.

7. Check for Protected Accounts

Path:

Active Directory Users and Computers → User Account → Properties → Member Of

Purpose:

Verify the user you are managing is not part of protected groups like Domain Admins or Enterprise Admins.

8. Test Delegation from Delegated User

Path:

Login as Delegated User → Active Directory Users and Computers → Attempt Task (Reset Password / Create User)

Purpose:

Confirm delegation is working as expected.

Summary and Best Practices

Systematic Troubleshooting Steps

Follow a structured process verifying permissions, user identity, and delegated tasks to resolve issues efficiently.

Maintaining Secure Access Control

Validate inheritance and refresh policies to ensure secure and efficient access control in Active Directory environments.

Principle of Least Privilege

Uphold least privilege by accounting for protected accounts and ensuring proper delegation to enhance enterprise security.

❖ Short Summary about Trouble Shooting:

Delegation troubleshooting in Active Directory involves checking OU permissions, verifying delegated tasks, confirming user login, refreshing Group Policy, validating inheritance, ensuring RDP access, and avoiding protected accounts.

❖ Conclusion:

In this project, I implemented secure, least-privilege delegation in Active Directory by granting OU-level permissions for common tasks (like user creation and password resets) without elevating users to Domain Admins. I validated access end-to-end-configuring Local Security Policy for safe RDP sign-in, confirming effective permissions and inheritance, and testing with a non-admin account-so delegated actions work exactly as intended. I also documented practical troubleshooting paths (OU scope, identity checks, delegated task selection, policy refresh, RDP rights, and protected accounts), which turn this from a setup guide into a real operations playbook. The result is a configuration that reduces risk, improves administrative efficiency, and aligns with enterprise security best practices through role-based access control and clear verification steps.