

Helpdesk Team Setup / System Administrator

Scenario: Goodcorp's IT department has grown, and a new Helpdesk team is being formed to assist with user management tasks. As the system administrator, you have been tasked with creating a secure and functional Helpdesk setup that adheres to the principle of least privilege. The team should be able to reset user passwords and create new user accounts, but they should not have full Domain Admin privileges.

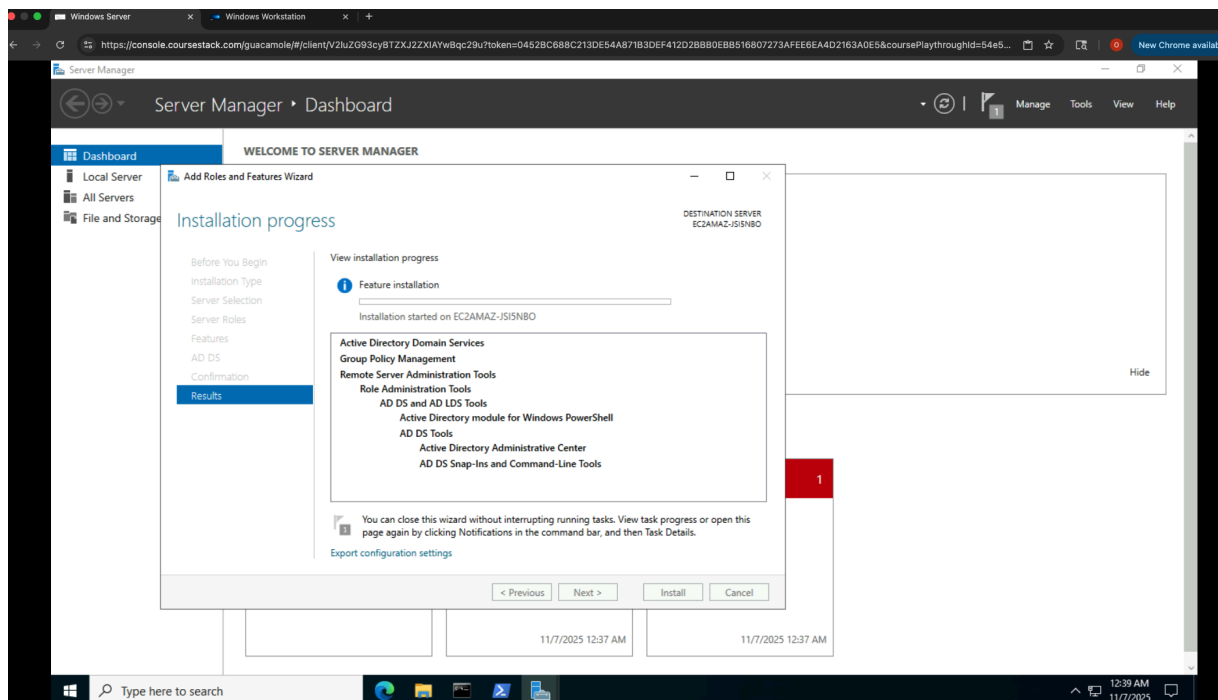
Objectives:

- Create a Helpdesk Security Group
- Create Two Helpdesk accounts for the helpdesk technicians
- Delegate limited control (Reset Passwords, Create New Users) on the UserAccount OU
- Verify that Helpdesk users cannot modify administrator accounts or make domain-wide changes

Steps Taken:

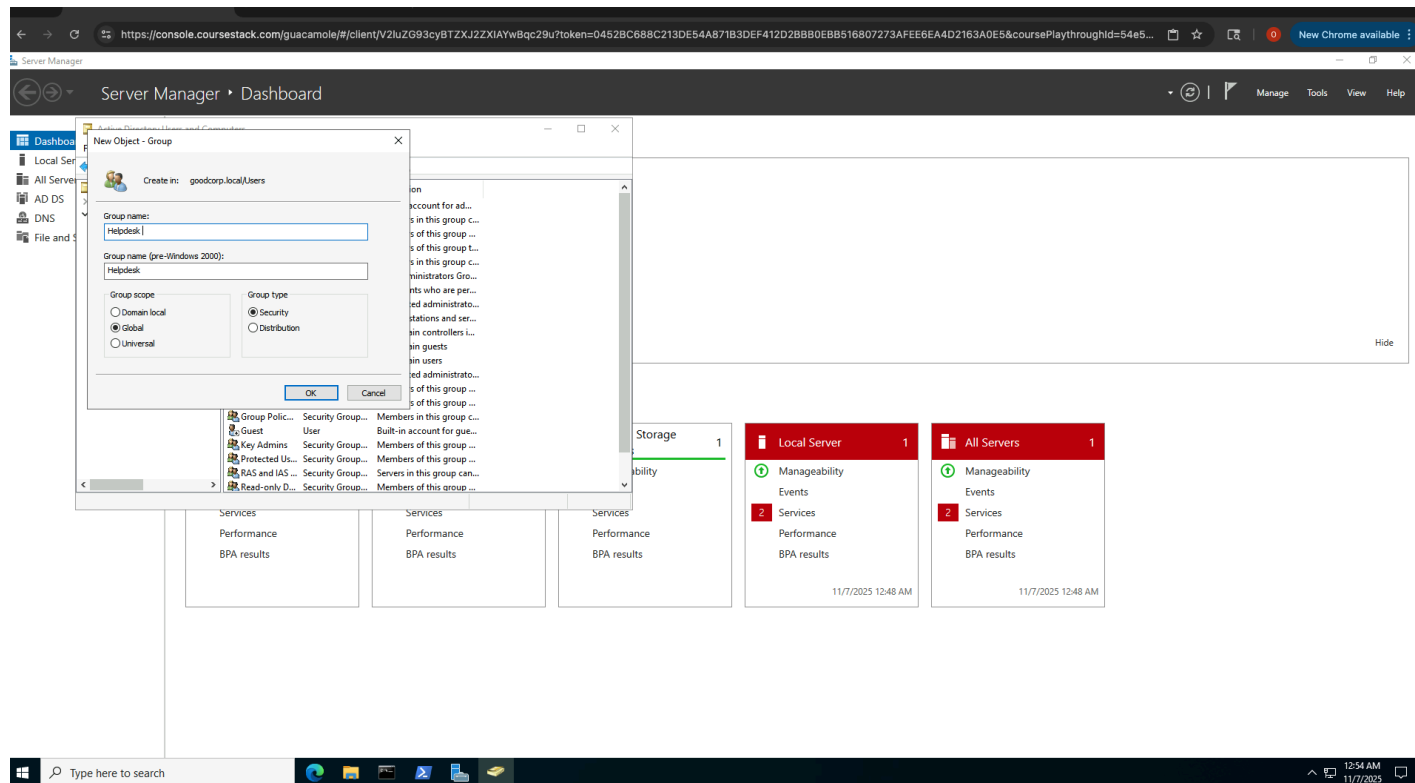
Step 1 - Create the Helpdesk Team:

My first task was to open Server Manager and install Active Directory Domain Services (AD DS) so I could set up Active Directory. Once it was installed, I promoted the server to a Domain Controller. This basically made the server the main system that controls all the users, groups and permissions across the network.



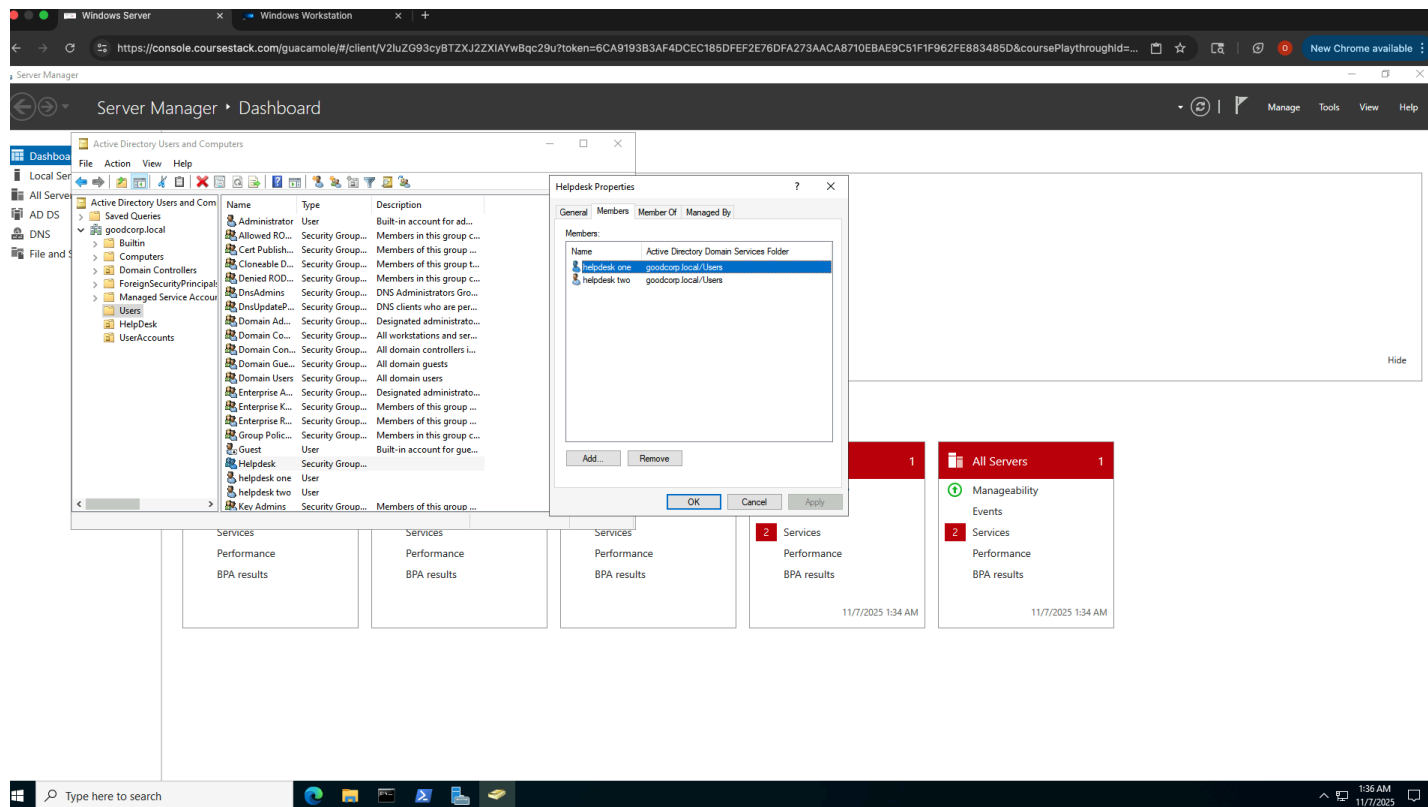
Step 2 - Create the Helpdesk Group

Next, I went into Active Directory Users and Computers and created a security group called Helpdesk to represent the Helpdesk team. This group would be used later when assigning permissions, so anyone added to it would have automatically the same access rights.



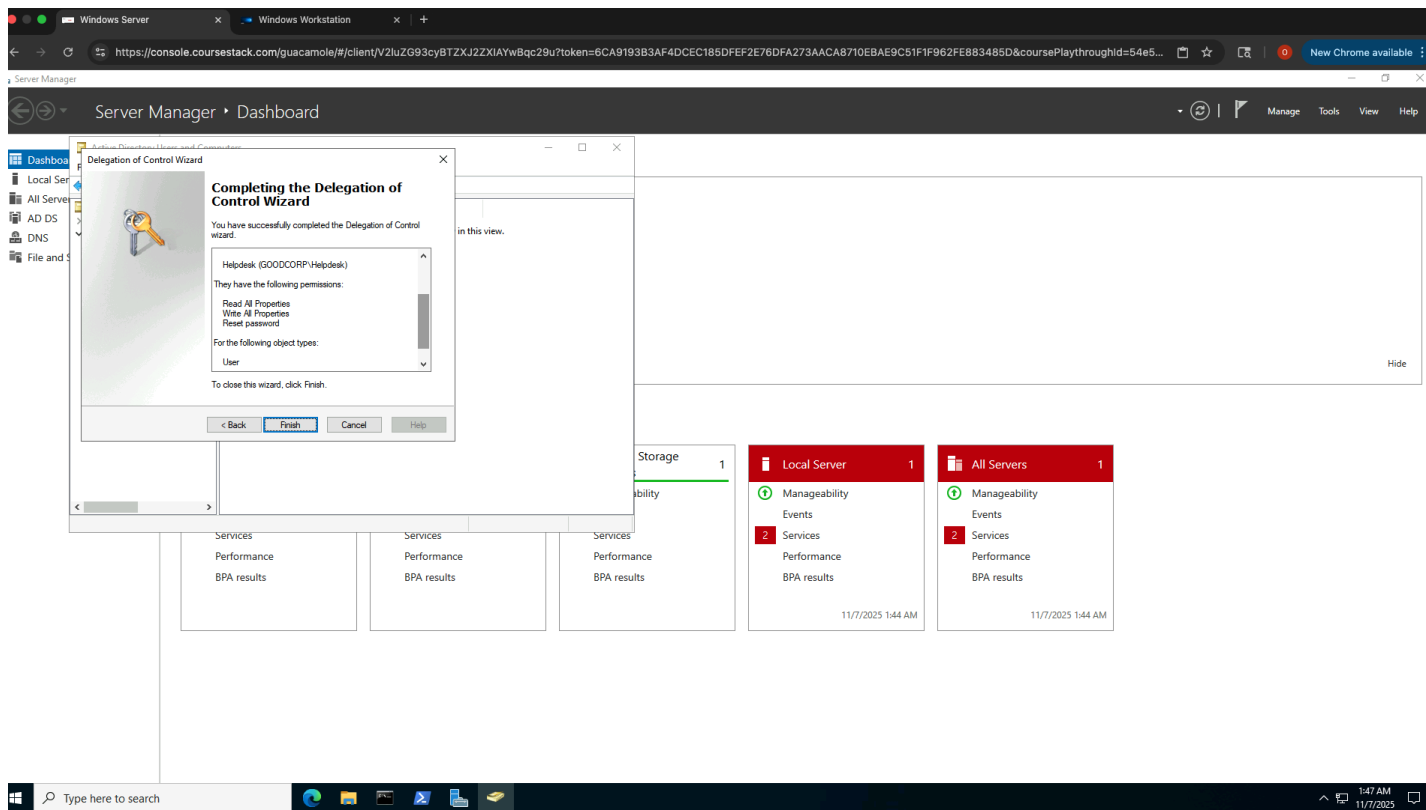
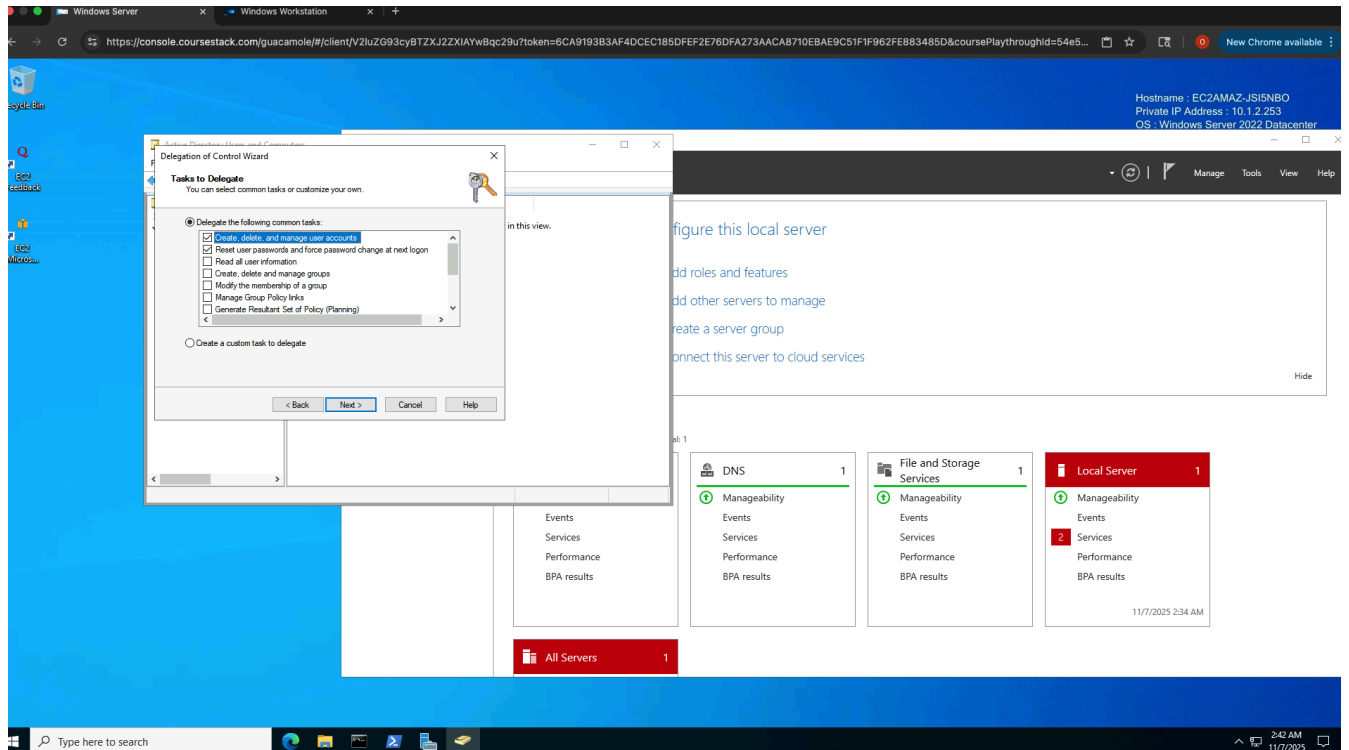
Step 3 - Add the Helpdesk Technicians

After creating the Helpdesk security group, my next step was to add the Helpdesk technicians - helpdesk1 and helpdesk2 to that group. This makes them part of the Helpdesk team, so they'll automatically get the same permissions that the group has once delegation is set up.



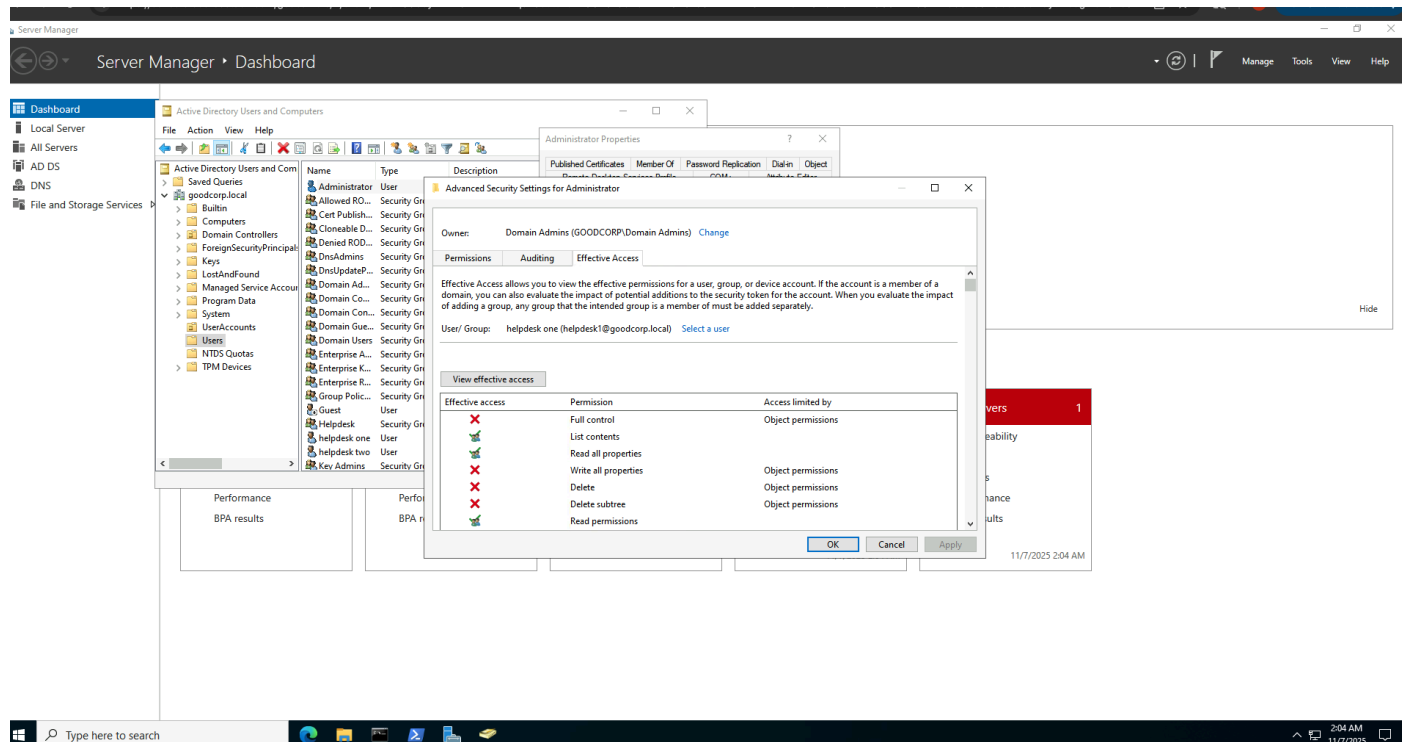
Step 4 - Delegate Permissions

The Next Step was to delegate permissions to the Helpdesk group for the UserAccounts OU. I used the delegation of control Wizards in the Active Directory to give them rights to reset user passwords and create or delete user accounts. This lets the Helpdesk team manage normal user accounts without having full Domain Admin Privileges(Least Privilege)



Step 5 - Verify Access

The final step was to verify that members of the Helpdesk group couldn't modify any admin accounts or make changes outside their delegated permissions. I wasn't able to sign in with the Helpdesk accounts directly, so instead I used the Effective Access tab in Active Directory to check what privileges the Helpdesk group actually had. This showed me that the group could reset and create users inside the UserAccounts OU, but they didn't have permissions to modify admin accounts or domain-wide settings.



Final Summary:

Overall, this lab helped me understand what it's like to work as a system administrator. I got hands-on experience setting up a domain controller, creating security groups, and delegating permissions in Active Directory. I also learned how to apply the principle of least privilege so that the Helpdesk team can do their job without full admin rights. This gave me a better understanding of how real companies manage user accounts securely.