Configuring Active Directory and Central File Access

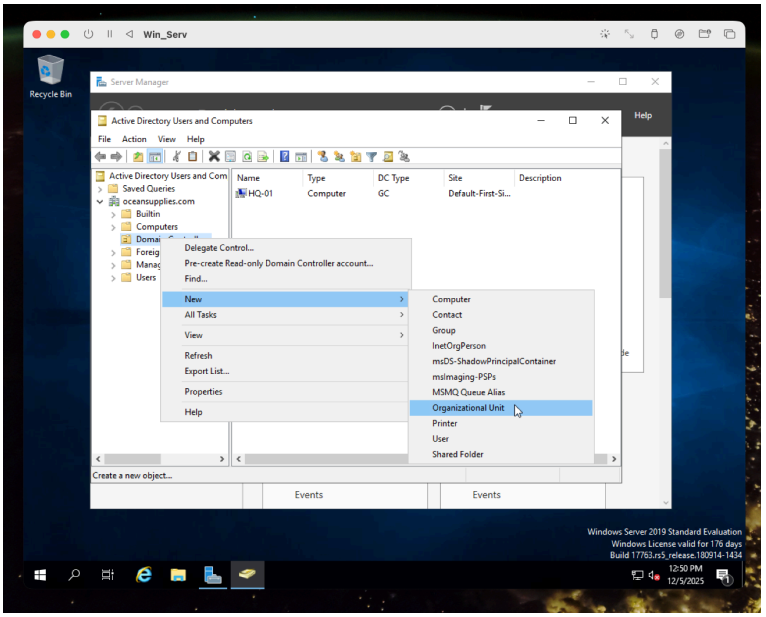
In this section, I'll walk through how I set up the Organizational Units, security groups, and user accounts for the Ocean Supplies domain. The goal here is to build a clean and realistic Active Directory structure that reflects how a small retail business organizes its teams, devices, and administrative roles.

By laying out the OUs first and then creating groups and users inside them, I'm able to keep everything organized and make permissions much easier to manage later in the project.

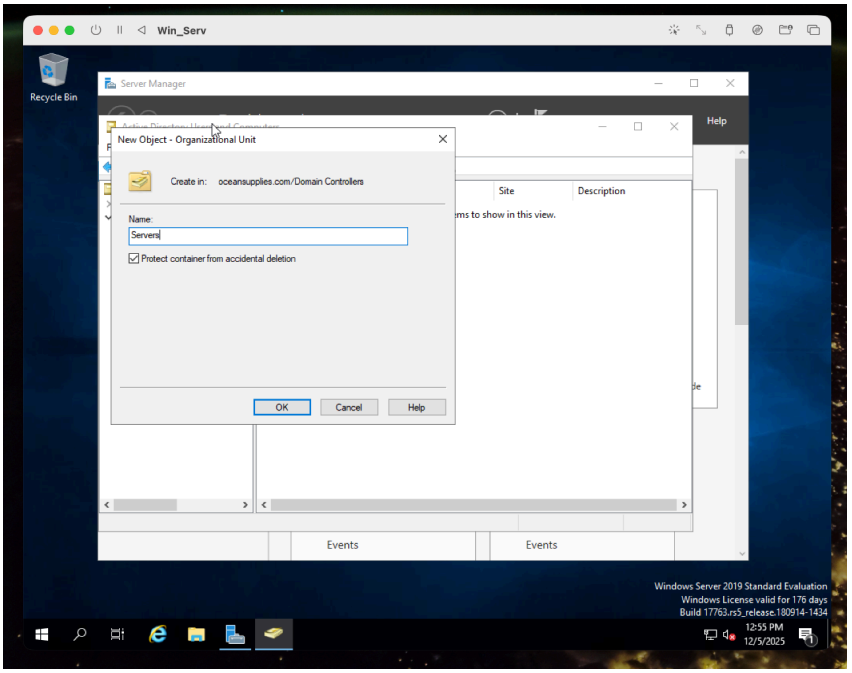
Create top-level OUs

To start, we'll create the Organizational Units to enable ... We'll create OUs for Admins, Users, Computers, and Servers.

To create an OU, expand the directory `oceansupplies.com`, right-click on Domain Controller > New > left click on Organizational Unit.



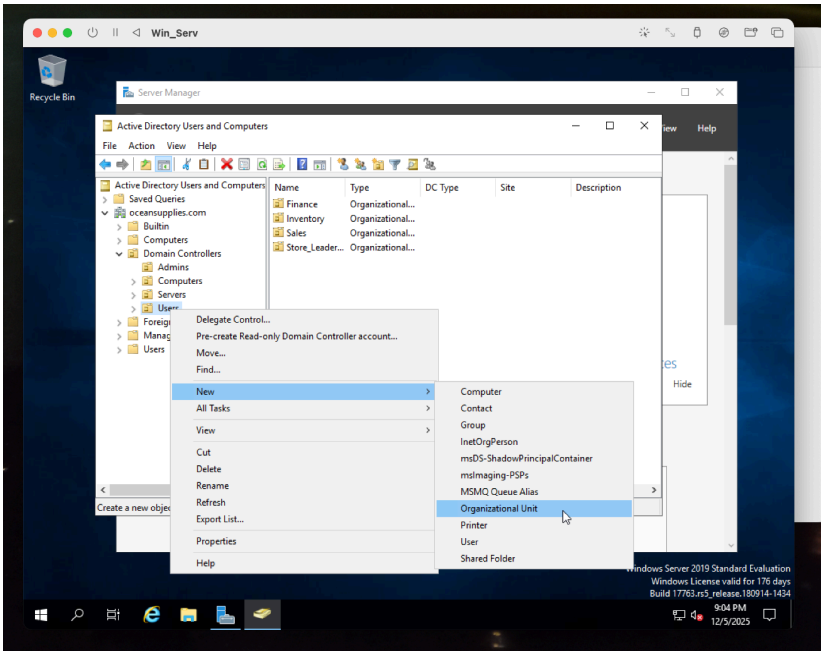
Next, you'll type in a desired name for the OU and click on OK. We'll create OUs for Admins, Computers, Servers, and Users.



Create department OU inside the Users OU

After creating all the OUs, we'll proceed to creating departments inside each OU.

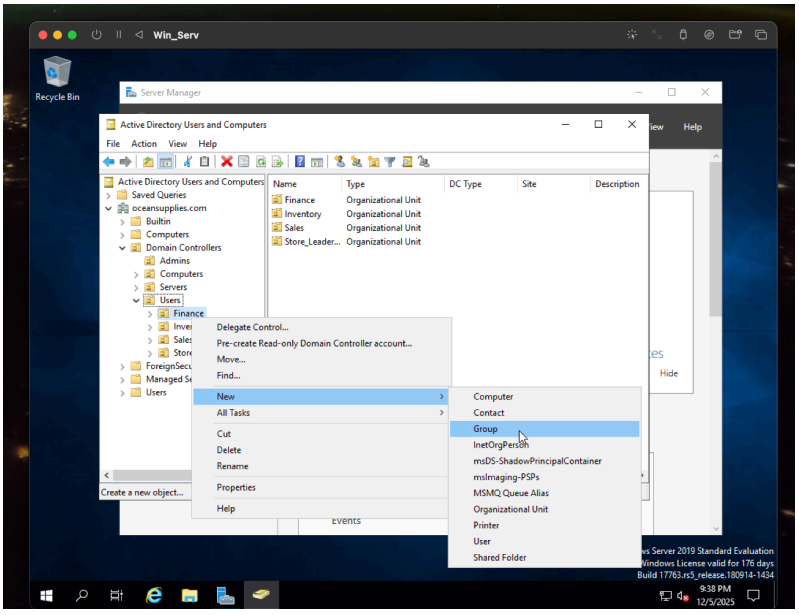
The steps for creating a department OU are the same as creating the top-level OU.



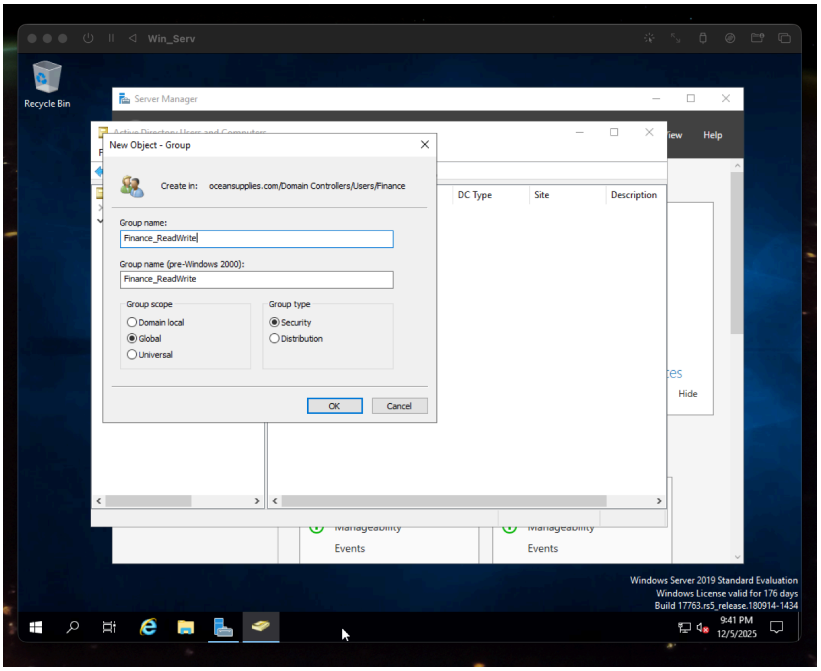
We'll create OUs for the following departments: Finance, Inventory, Sales, and Store_Leadership.

Create security groups for each department

Security groups are useful for defining what roles users in a group can have. To create security groups, right-click on the department name, hover over New then click on Group.



Next, you'll get the **New Object - Group** dialog window. In this window, we'll enter the group name, scope, and type.



Group scope can be any of the following:

- **Domain local:** Used to assign permissions to resources that exist only within the same domain.
- **Global:** Best for grouping users by department or role so you can apply permissions across the domain.
- **Universal:** Used in multi-domain forests to group objects and assign permissions across the entire forest.

Group type can be any of the following:

- **Security:** Allows you to assign permissions and control access to files, folders, and other resources.
- **Distribution:** Used only for email distribution lists and cannot be used for permissions.

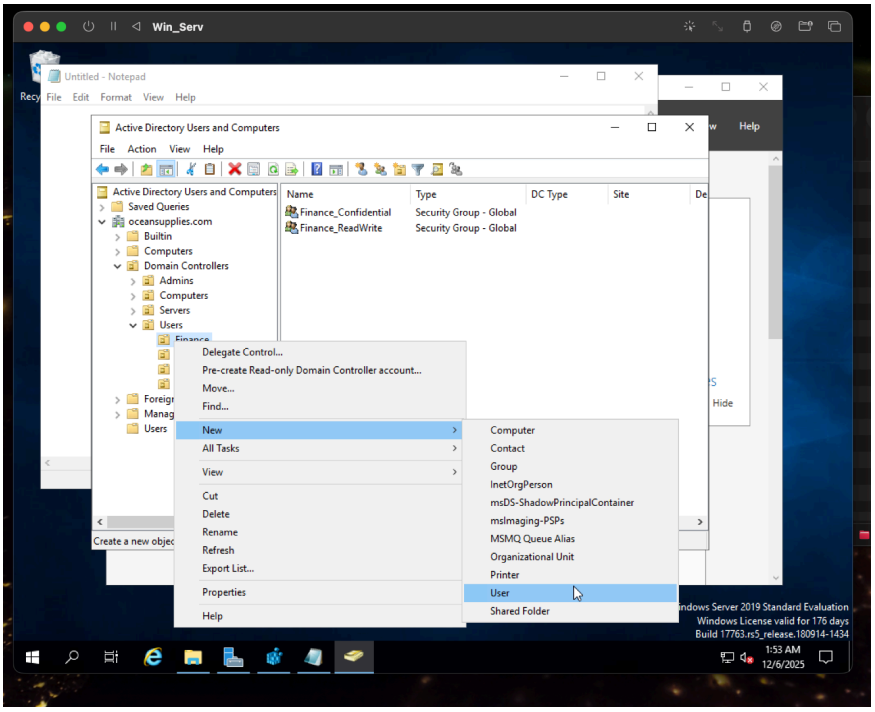
Below are the security groups we'll create:

Departments	**Groups**
Finance	Finance_Confidential Finanance_ReadWrite
Inventory	Inventory_ReadWrite Inventory_RestrictedAccess
Sales	Sales_ReadShare Sales_WriteShare
Store_Leadership	Leadership_AdminAccess Leadership_ReportAccess

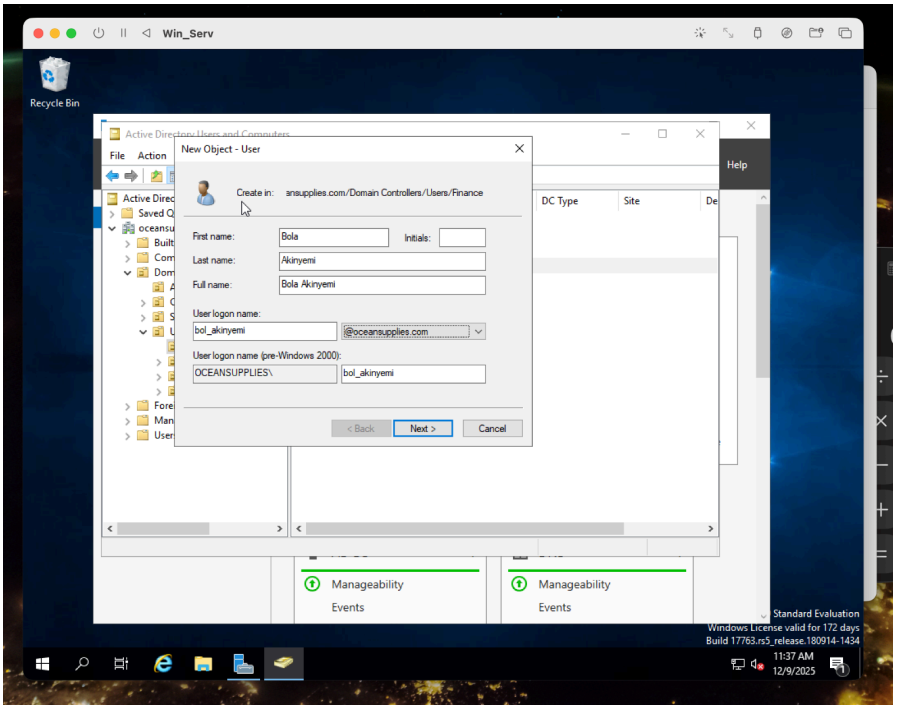
Create user accounts

After creating the Security Group, we'll proceed to creating users under each department. Since we've created security groups first, each user can be easily added to a security group.

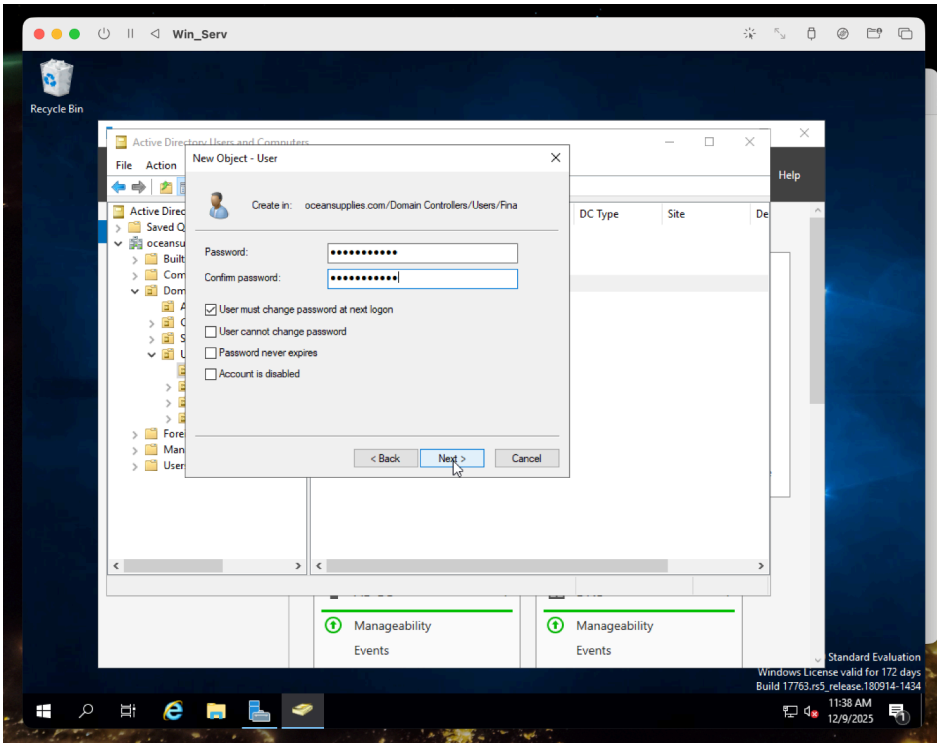
To create users in a department, right-click on the department > New > User.



When you click on User, a dialog Window opens for you to enter the user information.



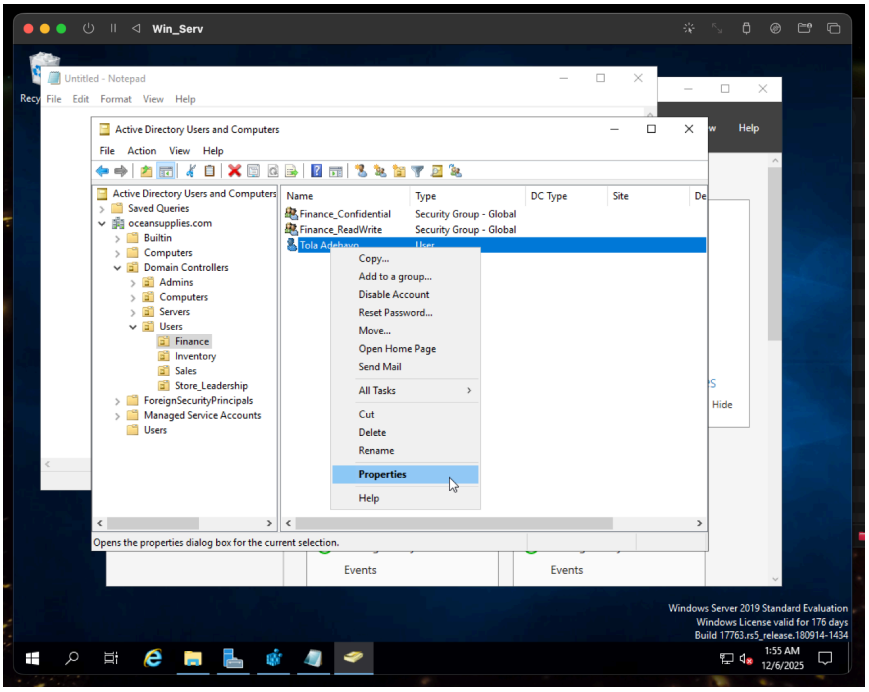
Once you're done filling in the user information, you click Next and next window prompts you define the user password and associated features.



Below is a table of users and their respective departments.

Departments	Users
Finance	Bola Akinyemi, Seun Ojo
Inventory	Amina Bello, Emeka Nwosu
Sales	Damenso Kefas, Sunday Okoro, Tola Adebayo
Store_Leadership	Kemi Adeyemi, Taiwo Ajadi

For each user, there are several settings that can be configured. To configure the settings for a user, right-click on the user and select Properties.



Here are some of the common settings you can adjust from the Properties window. In the Properties window, there are 13 tabs by default, each containing related settings.

Some of the commonly used tabs include:

- MemberOf: to add/remove a user from a group (e.g. the security groups we created earlier).

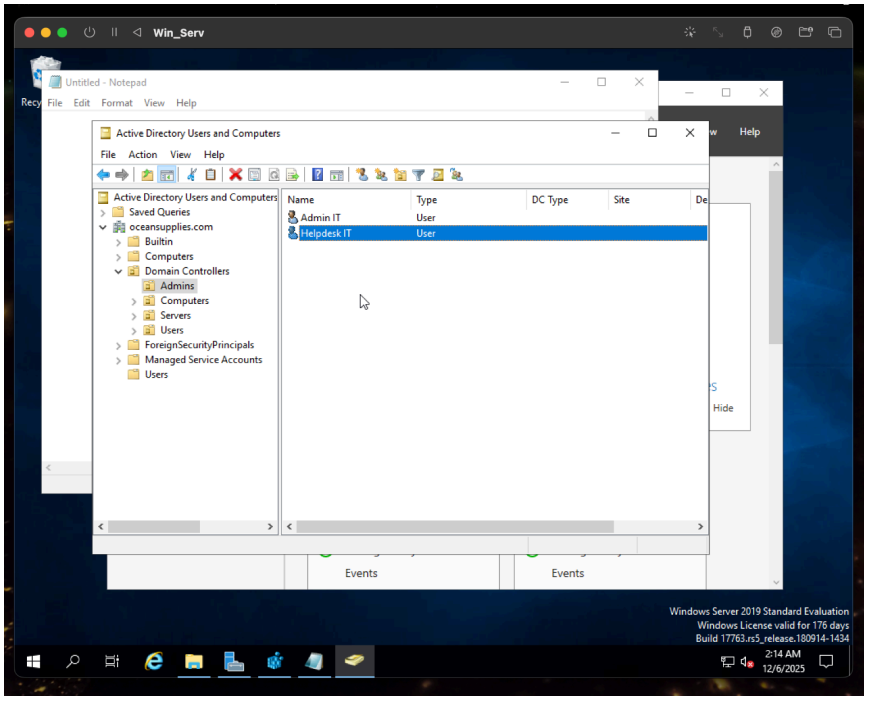
- Account: to adjust account properties such as password, account expiration, logon name, and logon hours (for defining the time range when a user can be logged on. Useful for limiting access to work hours only.)
- Sessions: to set session limits and what happens when a limit is reached.

While researching for this project, I learned that creating user accounts can be done more efficiently using PowerShell with a CSV file containing the user information. That will be very useful for when creating 50 or more users at a go. Our current business case is for a retail store with less than 25 employees so I'll stick with the GUI method.

Create administrative accounts

After creating users in their respective departments, we'll then create administrative accounts. These accounts are created in the dedicated OU "Admin" and are used for diagnostics and troubleshooting purposes.

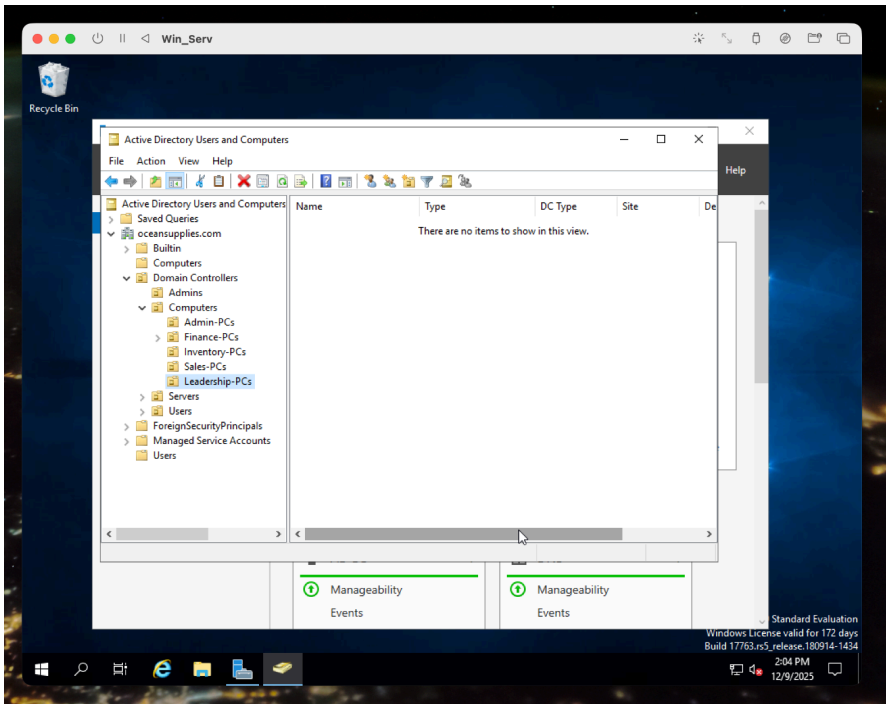
We'll create account for an Admin and Helpdesk personnel.



Create computer objects manually if needed

Next, we'll create computers for each of the departments. The process for creating computers is similar to the process for creating other objects like users and groups.

However, to make management of the computers and devices in a department easier, we'll first create OUs for the computers in each the department.



Now that we have the OUs for the computers, we'll proceed to creating new VMs, join them to the Ocean Supplies domain and move each computer to their respective Computer OU.

Due to the limitation of resources, I'll create just two VMs for two new computers. Practically, different users can log on to the computers one after another in the virtual lab.

Conclusion

This setup gives Ocean Supplies a clear and well-organized Active Directory structure that supports proper user management and controlled access to shared resources. By building out the OUs, groups, users, admin accounts, and computer objects, I've laid the groundwork for smooth authentication and centralized administration across the domain.

With these foundations in place, I can now move on to configuring file shares, permissions, and other services that rely on this structure. Furthermore, I'll be using one of the PCs in this virtual lab to keep experimenting with different IT and cybersecurity configurations, so I can deepen my skills, test new ideas safely, and get more comfortable with real-world scenarios.