

# Active Directory Infrastructure

By  
S.Aathika Erfana

# *Users*

— — —

*=> Users are one of the most common object types in Active Directory.*

*=> Users can be authenticated by the domain and can be assigned privileges over resources like files or printers.*

*Users can be used to represent two types of entities:*

*=> People*

*=> Services*

# ***Machines / Computers***

— — —

=> *A computer account represents your desktop or laptop to the active directory.*

=> *There is an account name and an account ID associated with your computer account you have the password, you can use it to log in.*

## ***Domain Admins***

=> *Users of this group have administrative privileges over the entire domain. By default, they can administer any computer on the domain, including the DCs.*

# *Understanding Users Account*

— — —

*Three types of user accounts can be created and configured in Windows Server 2008:*

*=> Local accounts.*

*=> Domain accounts.*

*=> Built-in user accounts.*

Carol O. Watts Properties

Published Certificates	Member Of	Password Replication	Dial-in	Object
Security	Environment	Sessions	Remote control	
Remote Desktop Services Profile	COM+	Attribute Editor		
General	Address	Account	Profile	Telephones
				Organization

Carol O. Watts

First name:  Initials:

Last name:

Display name:

Description:

Office:

Telephone number:  Other...

E-mail:

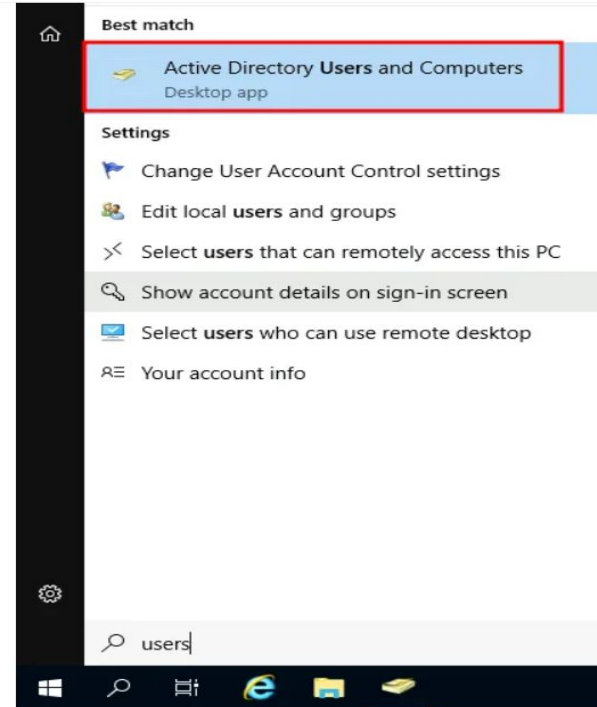
Web page:  Other...

OK Cancel Apply Help

# *Active Directory Users and Computers*

— — —

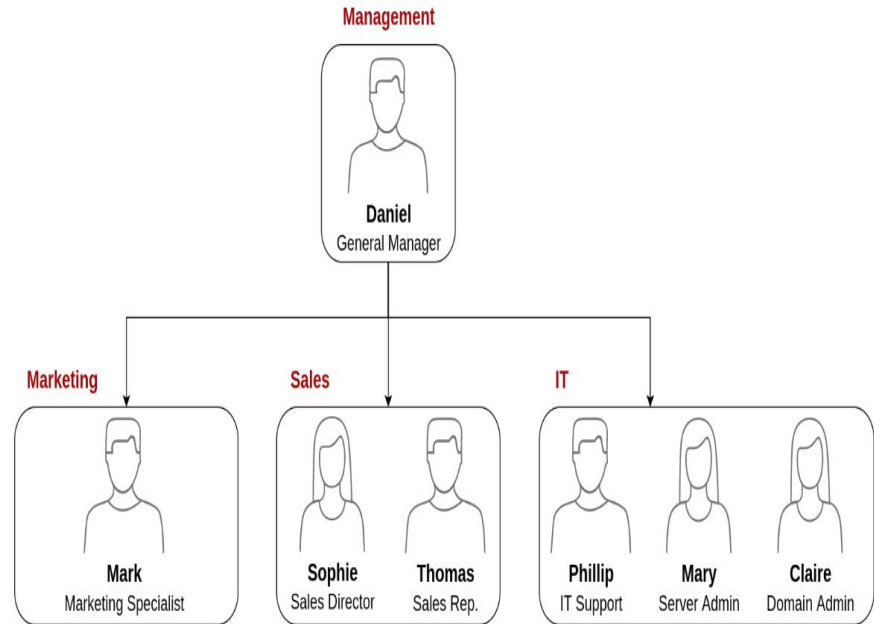
*To configure users, groups, or machines in Active Directory, we need to log in to the RDP and run “Active Directory Users and Computers” from the start menu:*



# Cont.,

— — —

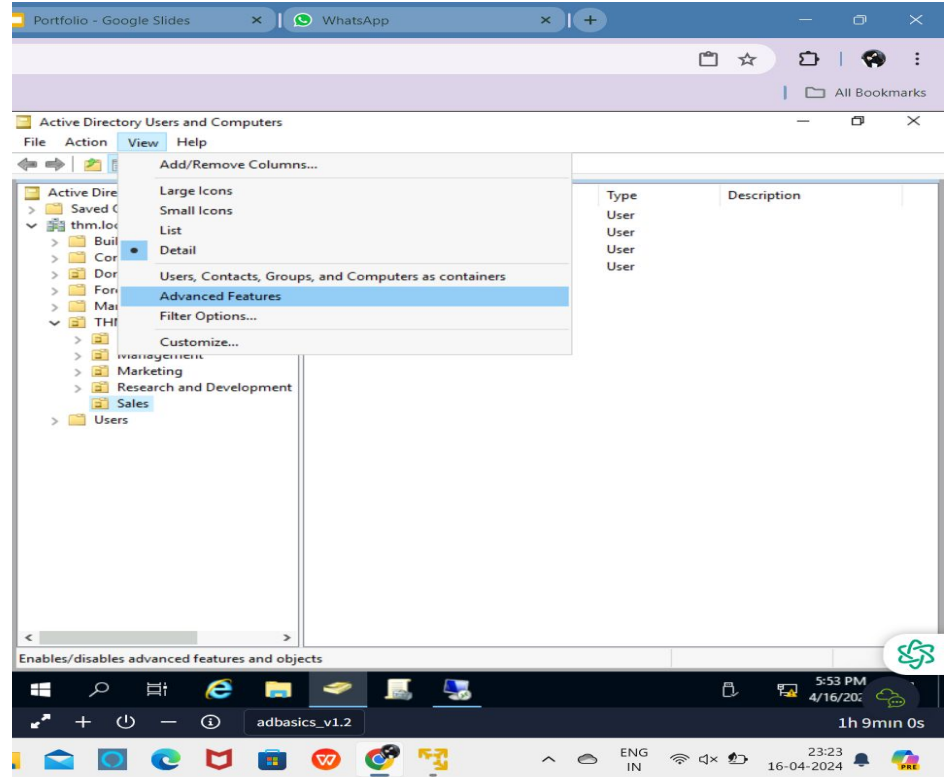
*As the new domain administrator is to check the existing AD OUs and users, as some recent changes have happened to the business.*



# Deleting Extra OUs and Users

— — —

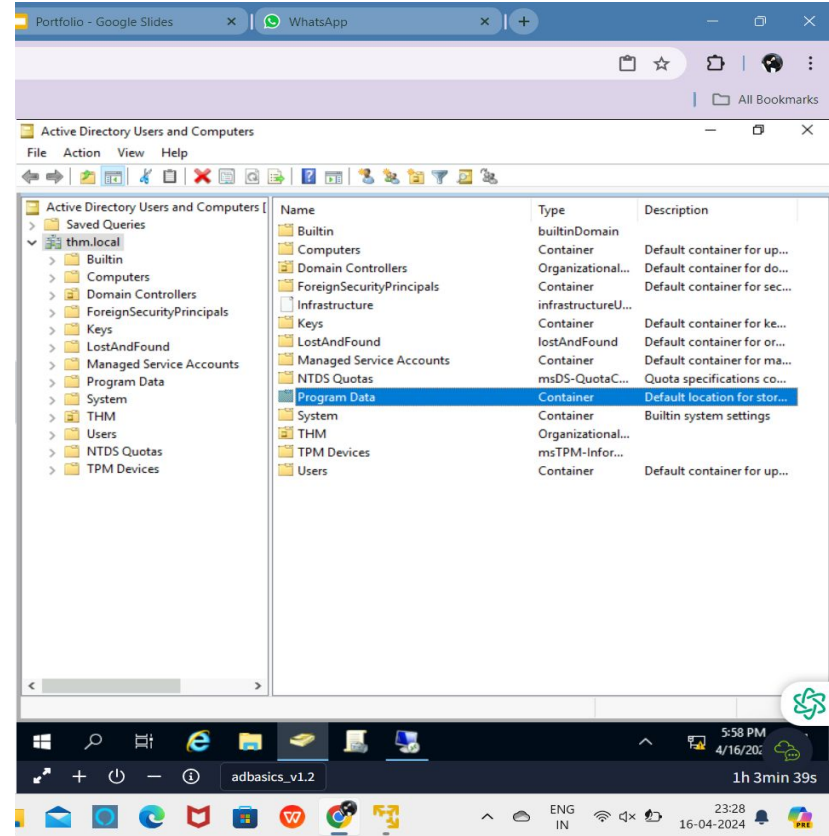
*To delete the OU, we need to enable the Advanced Features in the View menu:*



# Cont.,

— — —

*Next, right-click the OU and go to Properties. You will find a checkbox in the Object tab to disable the protection:*

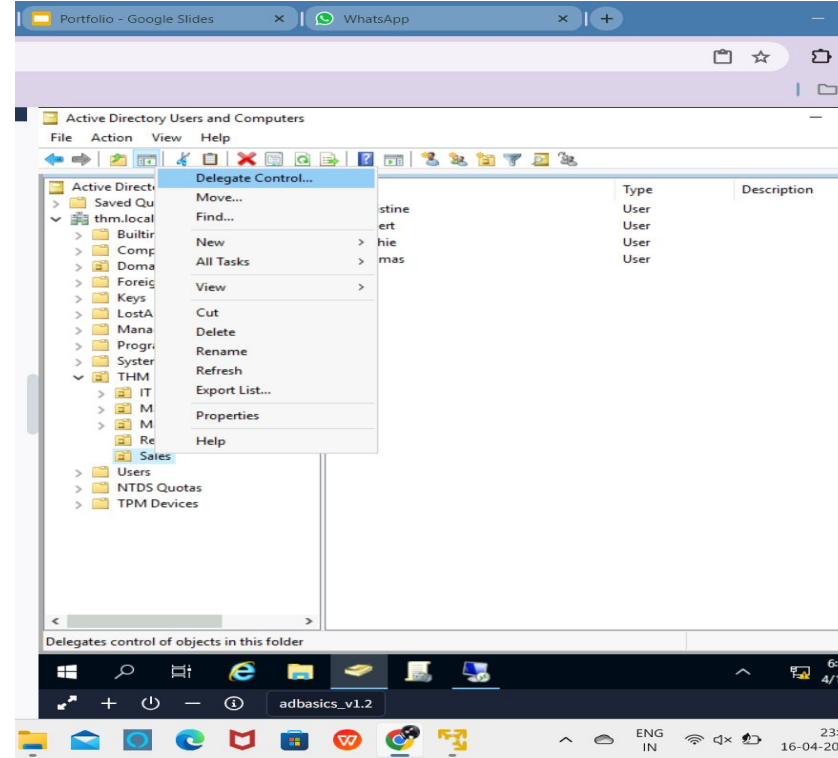




# Delegation

— — —

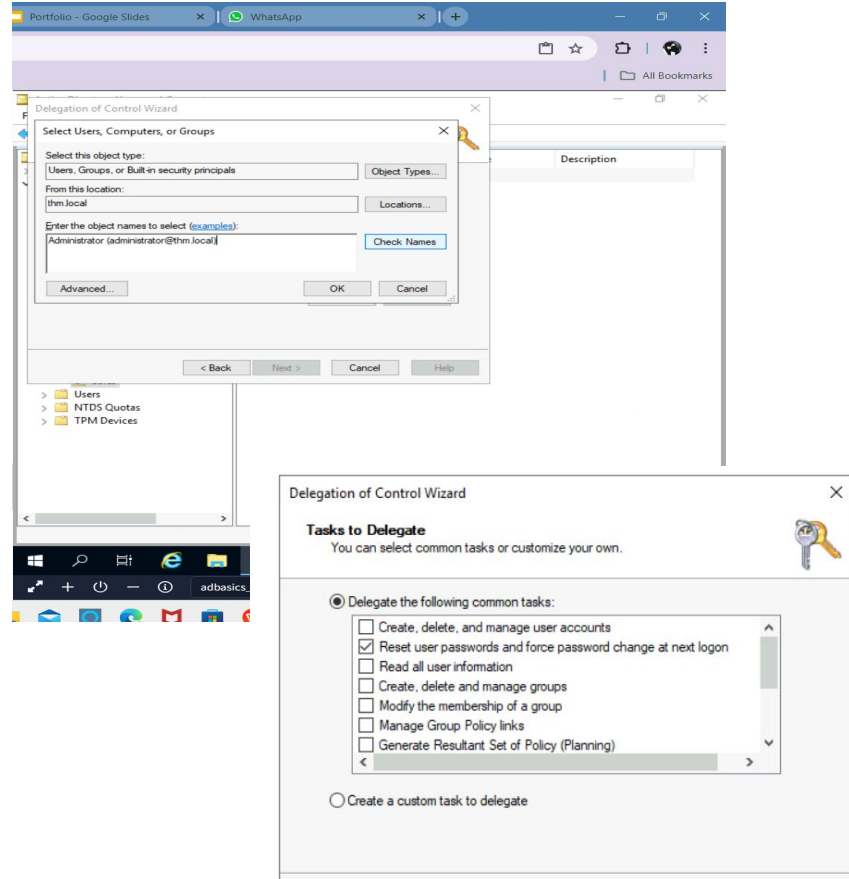
To delegate control over an OU, you can right-click it and select Delegate Control:



# Cont.,

Windows will autocomplete the user for you.

While you'd probably want to repeat these steps to delegate the password resets of the Marketing and Management departments, we'll leave it here for this task.



# Login credentials via RDP

— — —

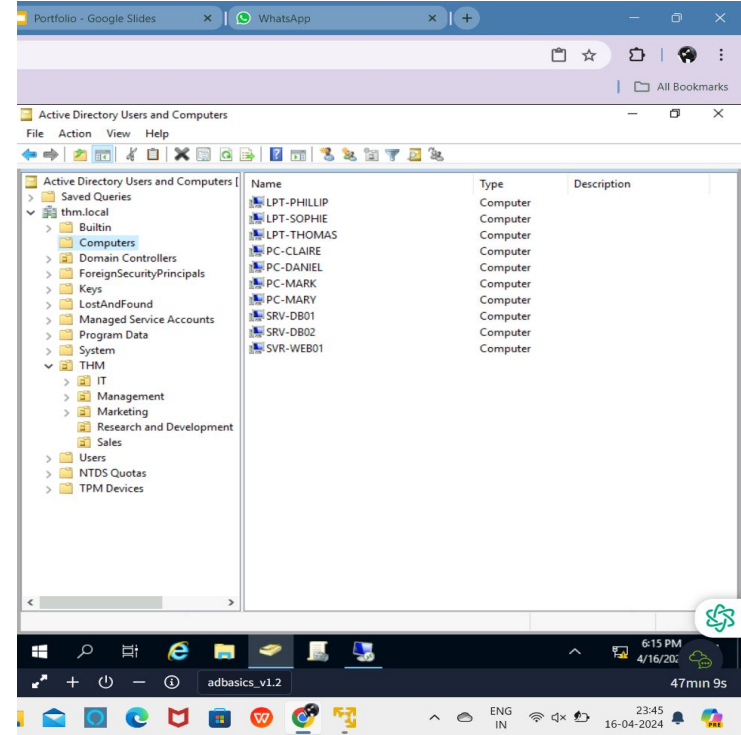
When connecting via RDP, use THM/Administrator as the username to specify you want to login and Password as Password321 on the THM domain

```
$ xfreerdp /u:THM\Administrator /p:Password321 /v:10.10.42.240
[16:59:24:836] [271264:271265] [WARN][com.freerdp.core.nego] - Error
_ALLOWED_BY_SERVER
[16:59:25:241] [271264:271265] [WARN][com.freerdp.core.nego] - Error
_ALLOWED_BY_SERVER
[16:59:29:788] [271264:271265] [ERROR][com.winpr.timezone] - Unable
match for unix timezone: Asia/Kolkata
[16:59:30:498] [271264:271265] [INFO][com.freerdp.gdi] - Local frame
rmat PIXEL_FORMAT_BGRX32
[16:59:30:499] [271264:271265] [INFO][com.freerdp.gdi] - Remote frame
ormat PIXEL_FORMAT_BGRA32
[16:59:30:594] [271264:271265] [INFO][com.freerdp.channels.rdpwnd.c]
static] Loaded fake backend for rdpsnd
[16:59:30:600] [271264:271265] [INFO][com.freerdp.channels.drdrnvc.c]
Loading Dynamic Virtual Channel rdpgfx
[17:00:09:502] [271264:271264] [ERROR][com.freerdp.core] - freerdp_a
ect:freerdp_set_last_error_ex ERRCONNECT_CONNECT_CANCELLED [0x000200

(kali@kali)-[~]
$ xfreerdp /u:'THM\Administrator' /p:Password321 /v:10.10.42.240
[17:00:36:290] [271849:271850] [WARN][com.freerdp.core.nego] - Error
_ALLOWED_BY_SERVER
[17:00:36:109] [271849:271850] [WARN][com.freerdp.core.nego] - Error
_ALLOWED_BY_SERVER
[17:00:41:272] [271849:271850] [ERROR][com.winpr.timezone] - Unable t
match for unix timezone: Asia/Kolkata
[17:00:41:272] [271849:271850] [INFO][com.freerdp.gdi] - Local frame
```

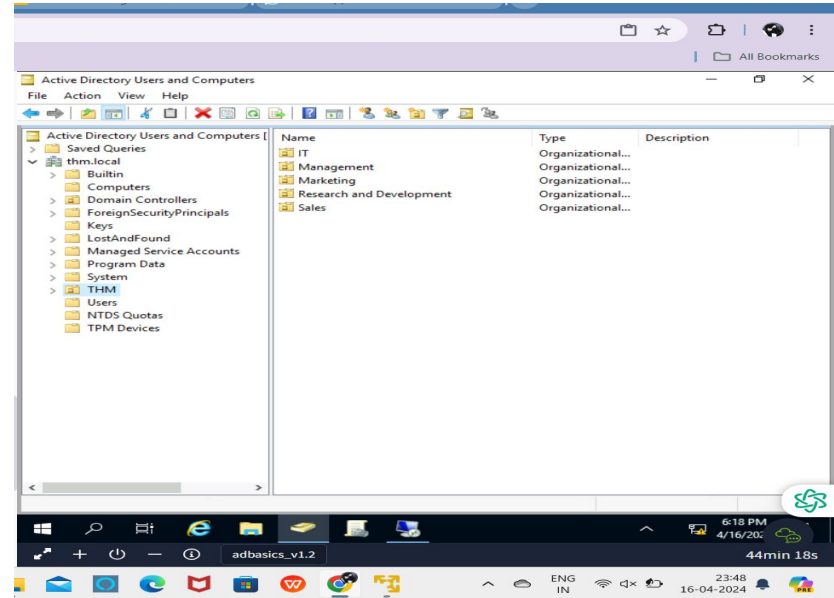
# *Managing Computers in AD*

By default, all the machines that join a domain (except for the DCs) will be put in the container called "Computers".



# Managing Computers in AD

let's create two separate OUs for **Workstations** and **Servers** (Domain Controllers are already in an OU created by Windows). We will be creating them directly under the **thm.local** domain container.



*Thank  
you!*