

Windows Server Final Project

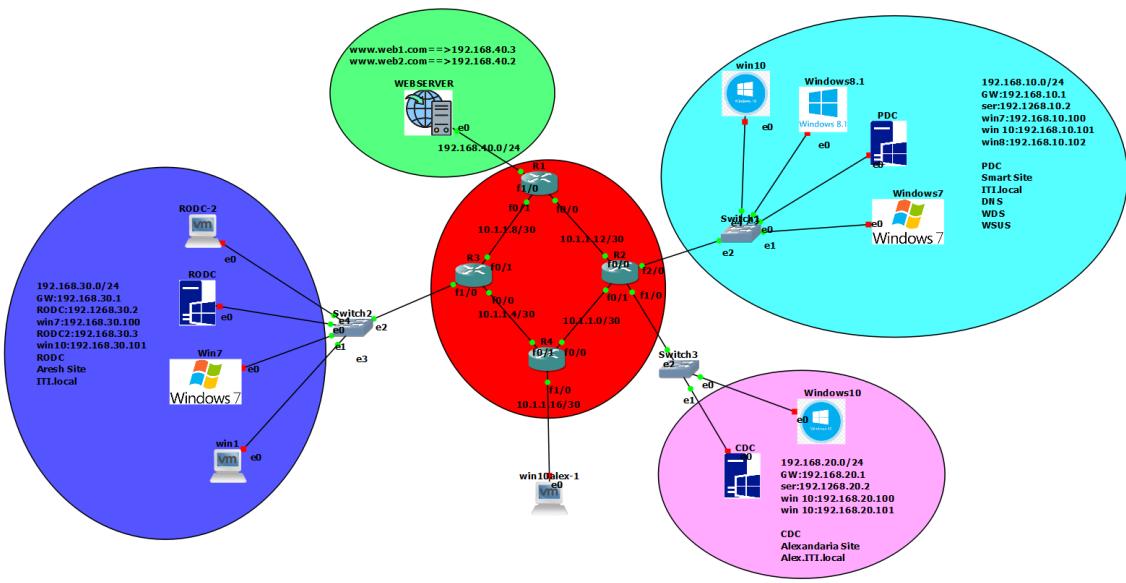
Under supervision of

Eng/Peter Kamel

By

Mahmoud Mohamed Yousef

Network Topology

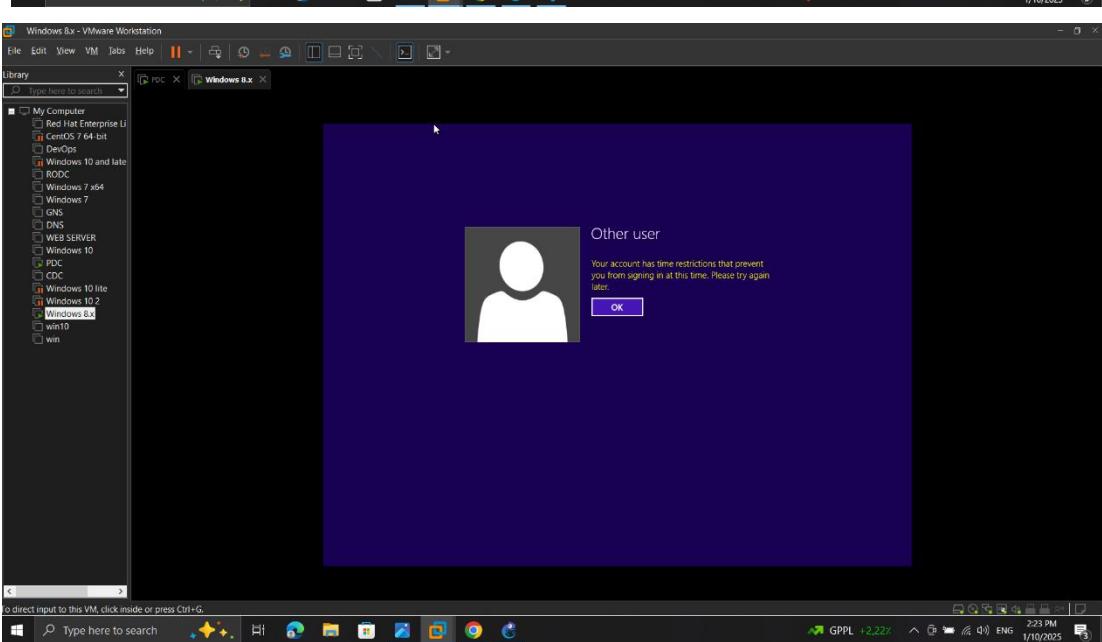
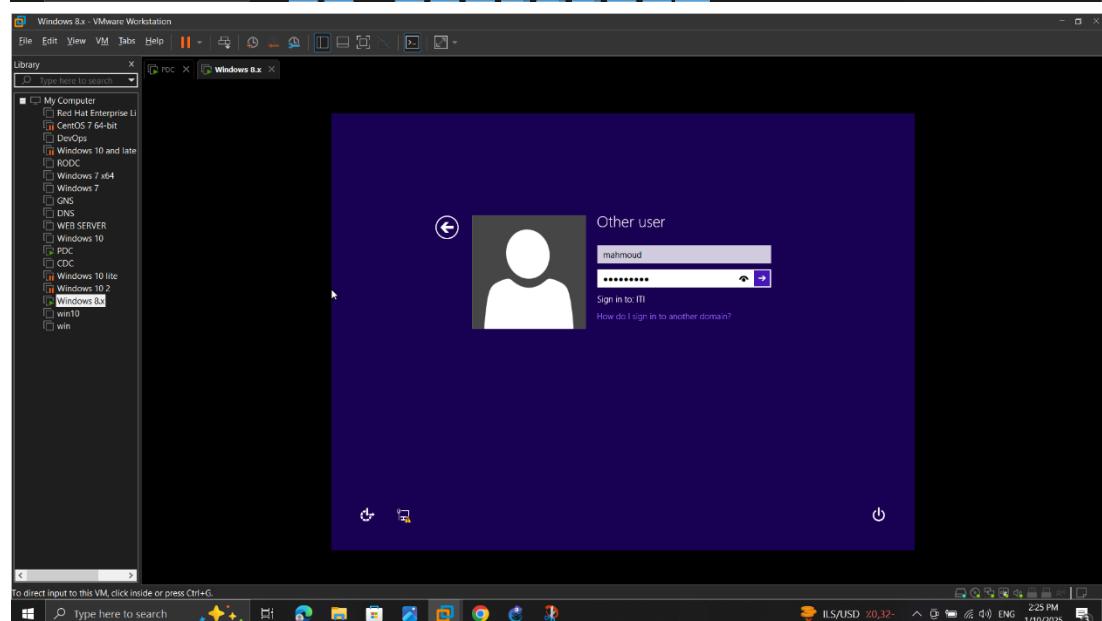
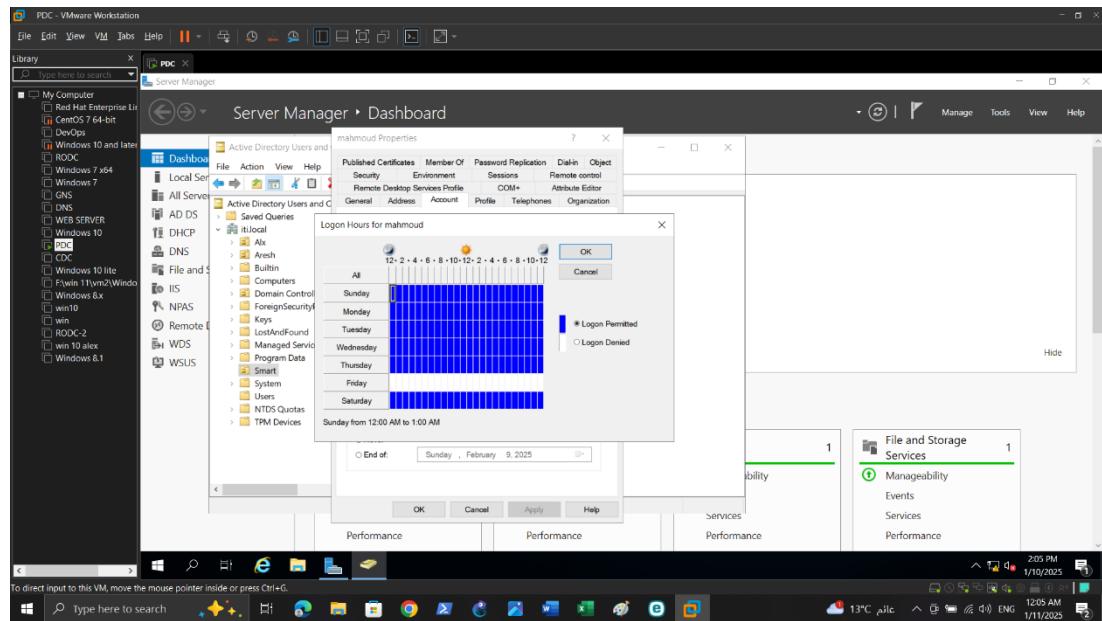


Name	IP Configurations		Users
PDC(parent domain controller) ITI.local	IP	192.168.10.2	mahmoud dina adam mazen omiama hazem memma
CDC(child domain controller) Alex.it.i.local	SUBNET MASK	255.255.255.0	asmaa basel
RODC(read only domain controller) ITI.local	IP	192.168.30.2	
	SUBNET MASK	255.255.255.0	
PC01	IP	192.168.10.100	
	SUBNET MASK	255.255.255.0	
PC02	IP	192.168.20.100	
	SUBNET MASK	255.255.255.0	
PC03	IP	192.168.30.100	
	SUBNET MASK	255.255.255.0	
PC04	IP	10.1.1.18	
	SUBNET MASK	255.255.255.252	
WEB SERVER	IP	192.168.40.2 192.168.40.3	
	SUBNET MASK	255.255.255.0	
RODC-2(read only domain controller) ITI.local	IP	192.168.30.3	
	SUBNET MASK	255.255.255.0	
PC05	IP	192.168.10.101	
	SUBNET MASK	255.255.255.0	
PC06	IP	192.168.10.102	
	SUBNET MASK	255.255.255.0	
PC07	IP	192.168.30.101	
	SUBNET MASK	255.255.255.0	
Router1	f0/0 f1/0 f0/1	10.1.1.14 192.168.40.1 10.1.1.9	
Router2	f0/0 f1/0 f0/1 f2/0	10.1.1.13 192.168.20.1 10.1.1.1 192.168.40.1	
Router3	f0/0 f1/0 f0/1	10.1.1.5 192.168.30.1 10.1.1.10	
Router4	f0/0 f1/0 f0/1	10.1.1.2 10.1.1.17 10.1.1.6	

Users	Config
mahmoud	can't login to pc1 on Friday
dina	can login to pc1 and can login remotely on PDC, he is not a domain
adam	when login to pc1 found that firefox program installed on his machine from domain admin
mazen adam	can't use a flash memory and can't use control pannel and there desktop wallpaper is ITI logo
omiama	can login only to RODC and can't create users but can shut down the RODC
hazem	can login to pcs in Aresh site and can replicate there password to the RODC
memma	can browse http://www.web2.com and FTP
basel	can access remotely the webserver with administrative privileges and can create and delete users on HR Department in Alex.it.i.local and can browse http://www.web1.com
asmaa	can't login to pc1 on Friday

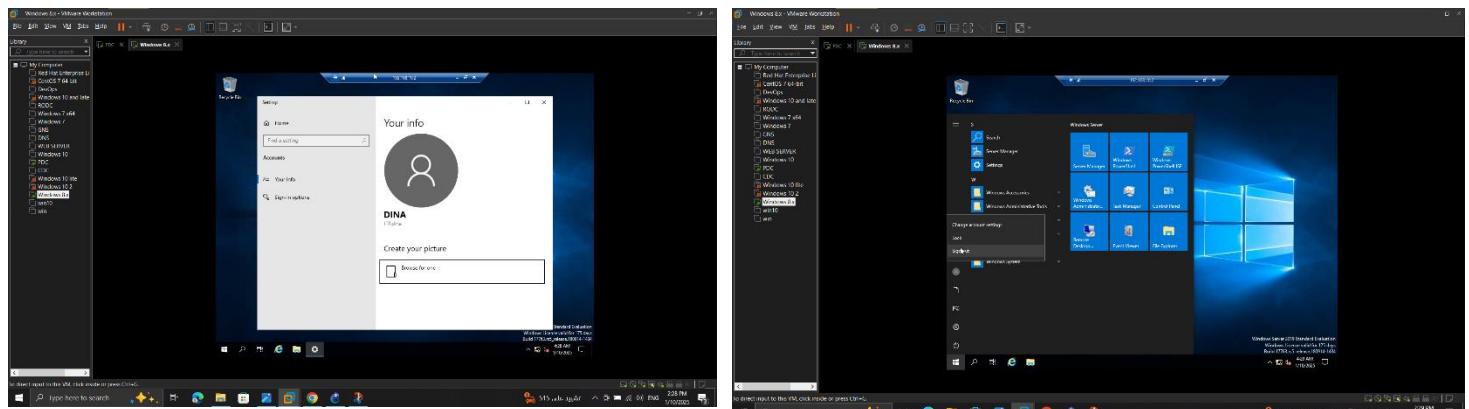
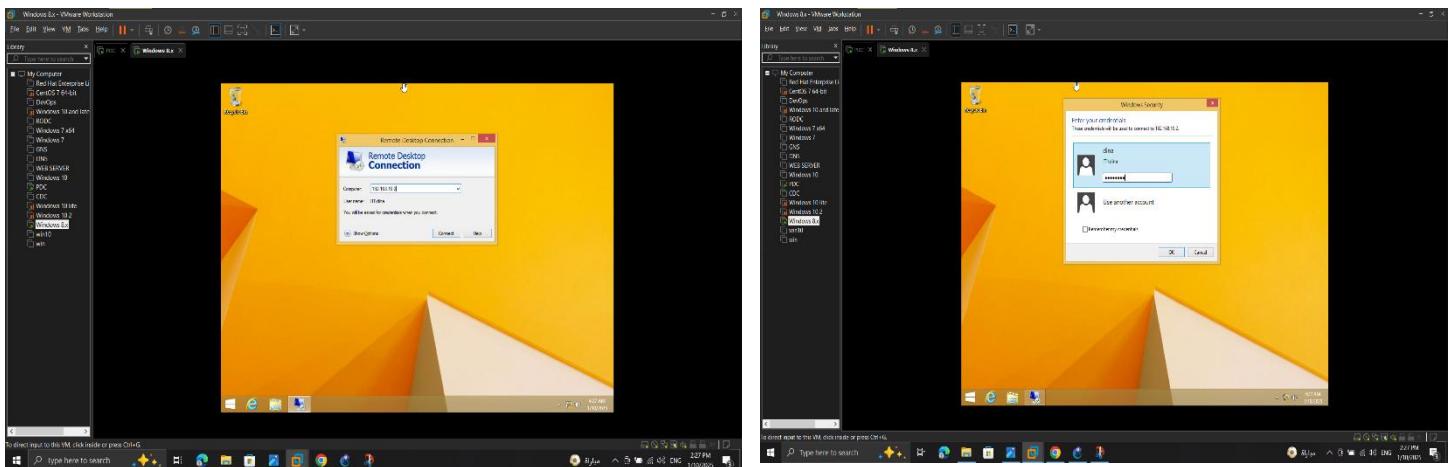
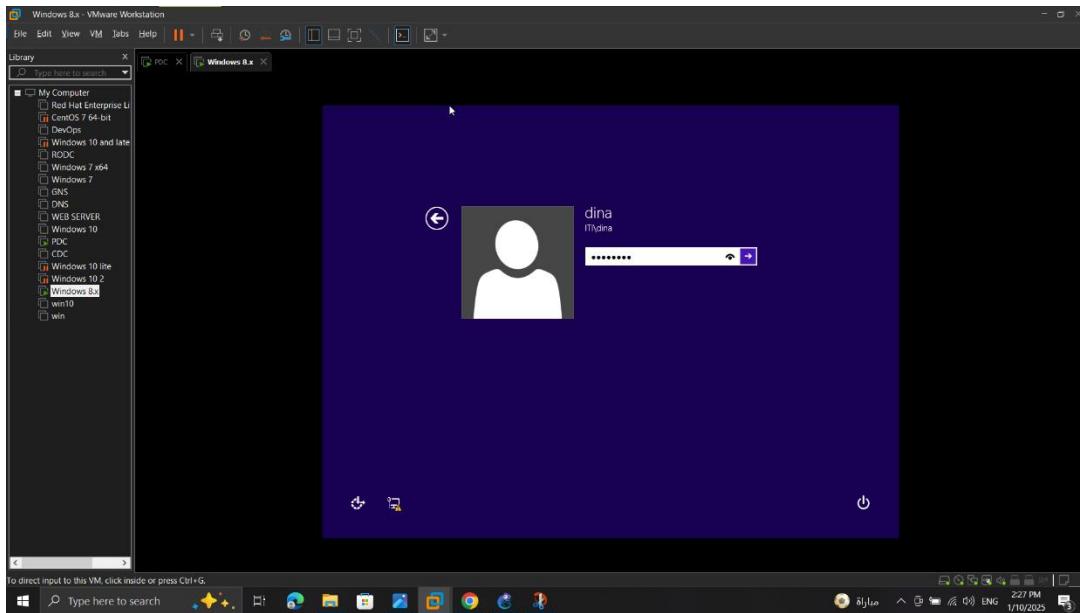
mahmoud@iti.local:

- can't login in pc1 on Friday.



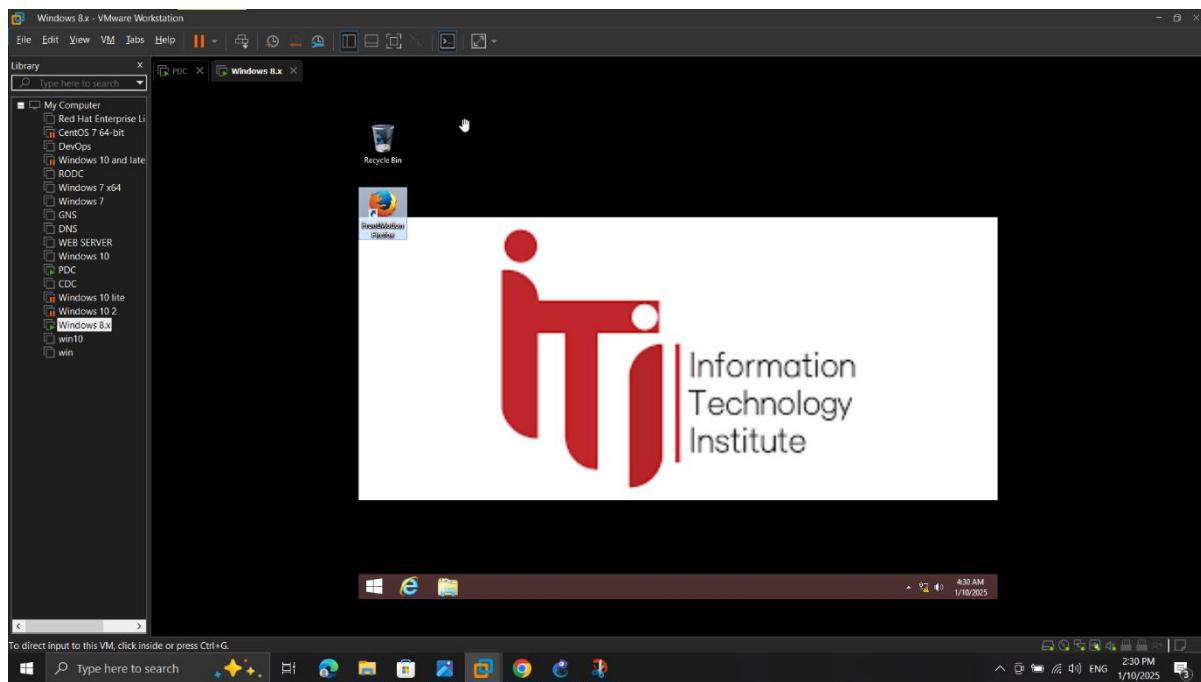
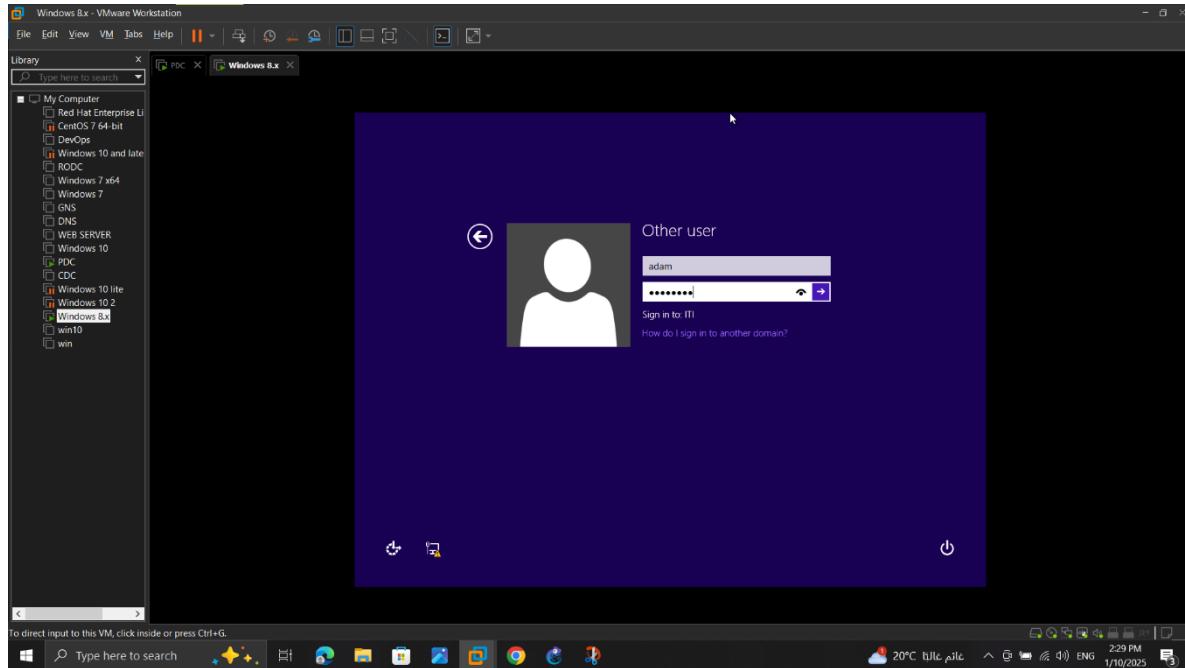
dina@iti.local:

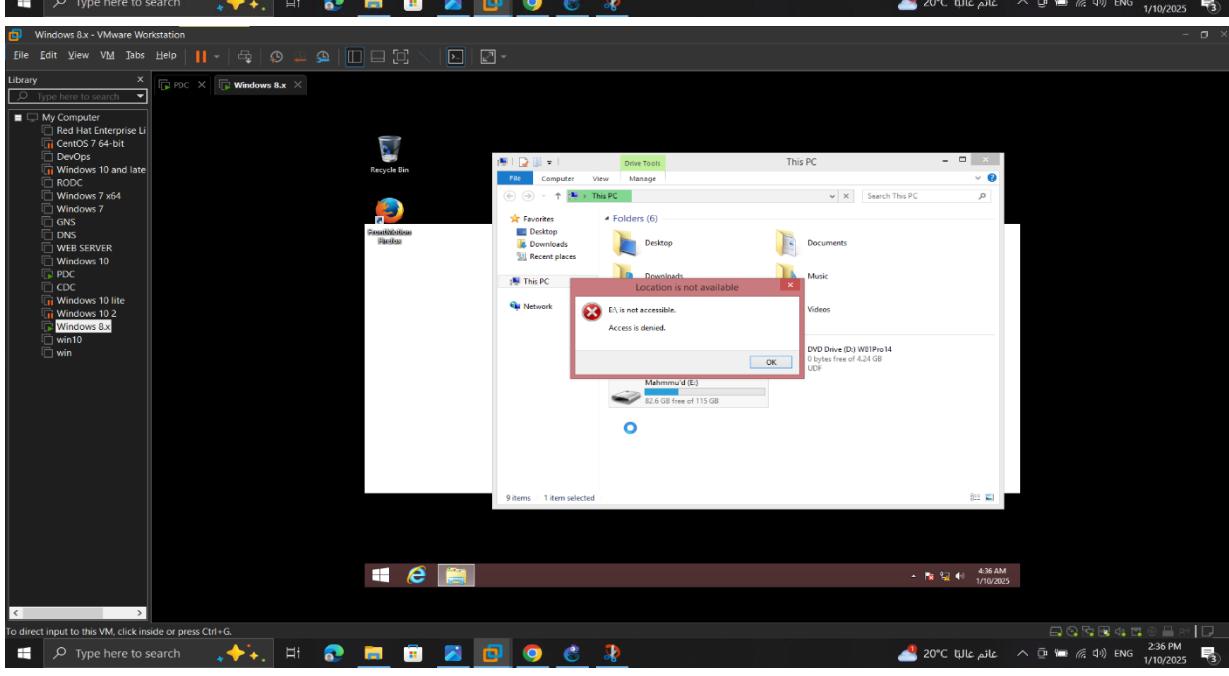
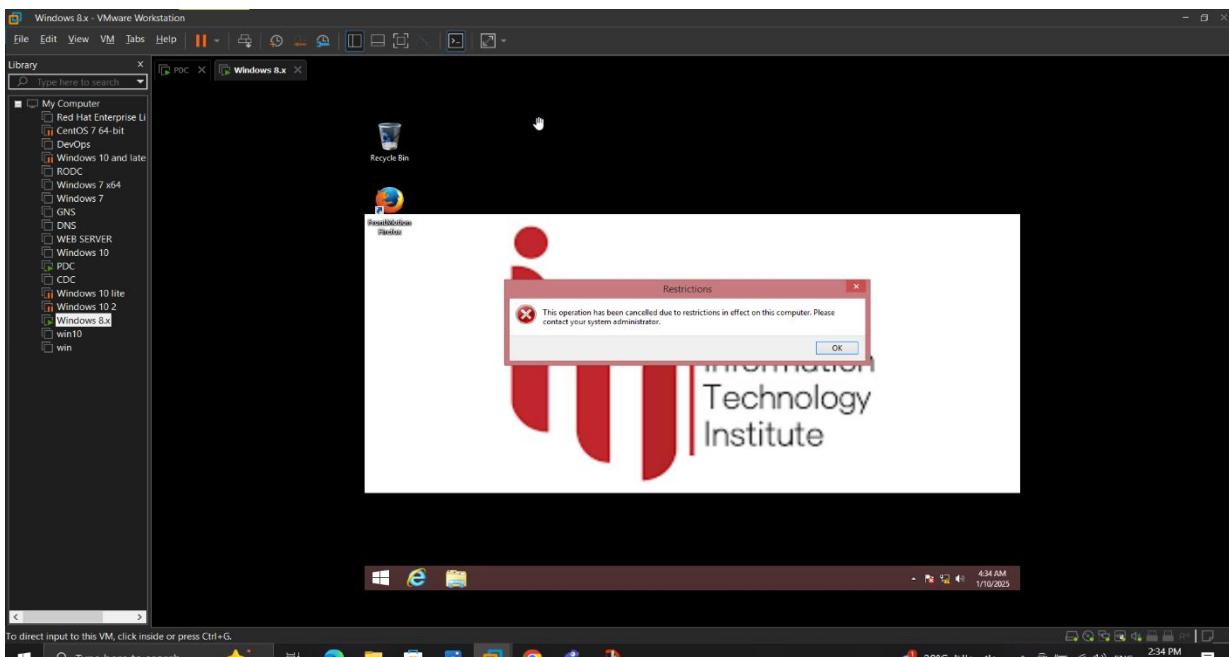
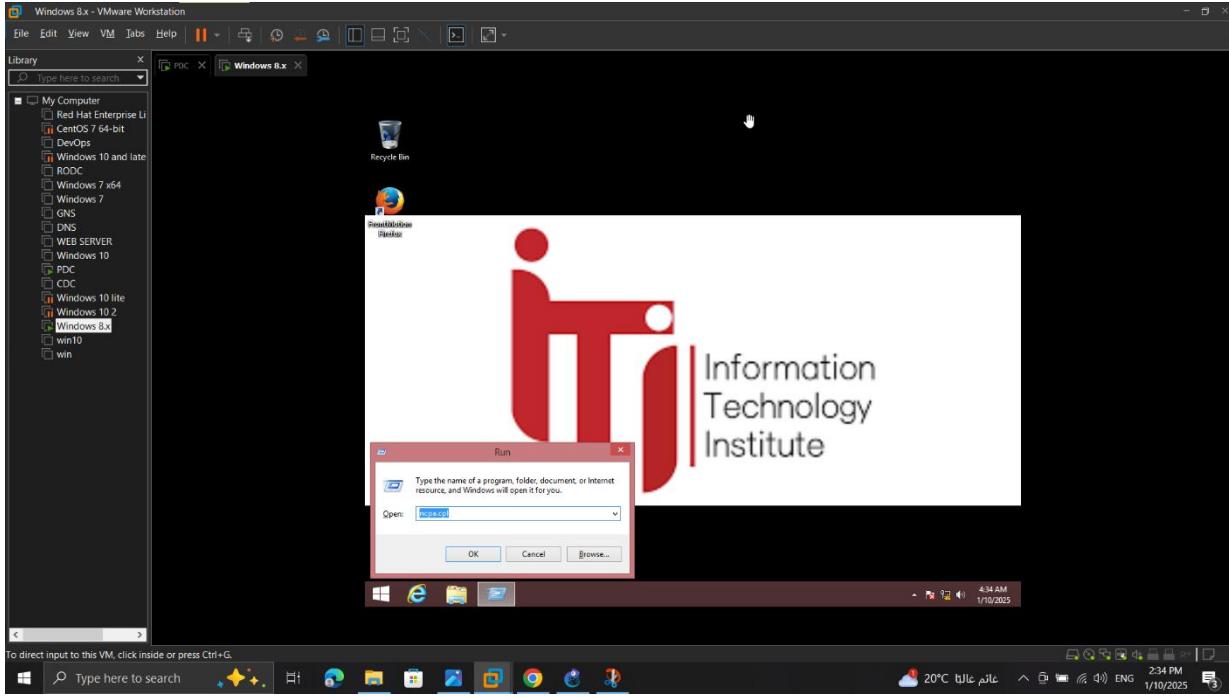
- can login to pc1 and can login remotely on PDC, she is not a admin when login to it .



adam@iti.local:

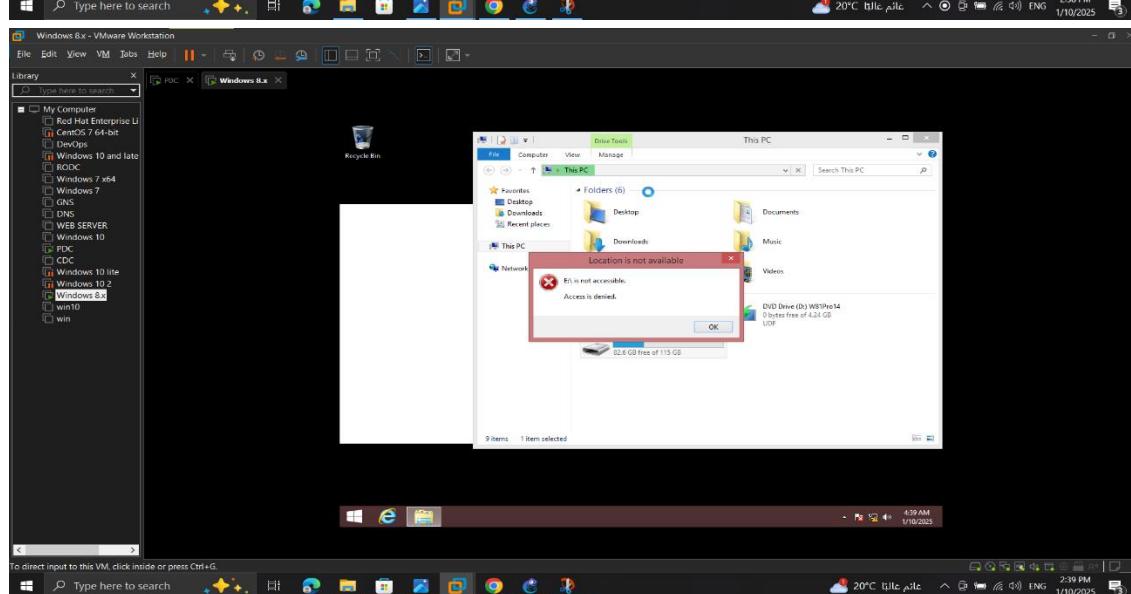
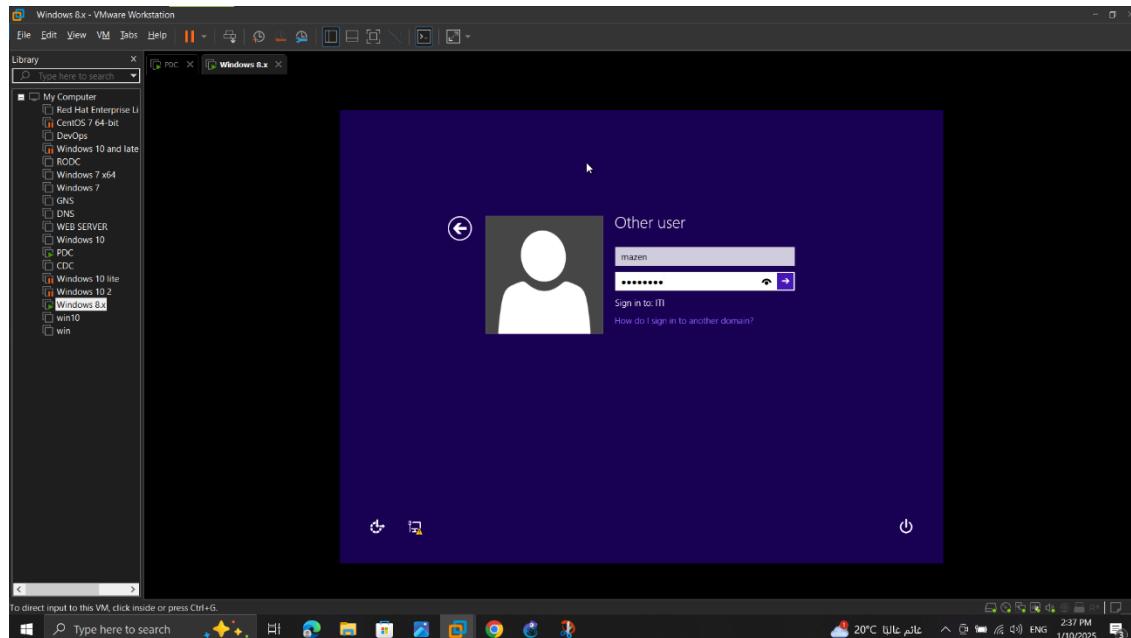
- found that Firefox program installed on his machine from domain admin , can't use a flash memory and can't use control panel and there desktop wallpaper is ITI logo.

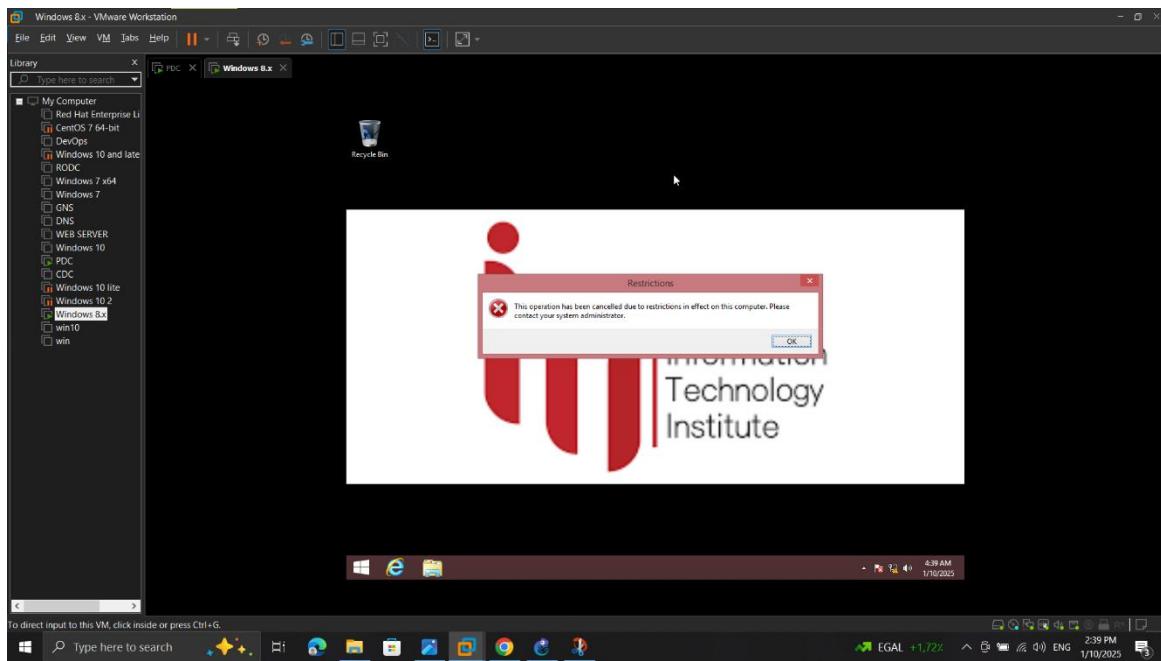
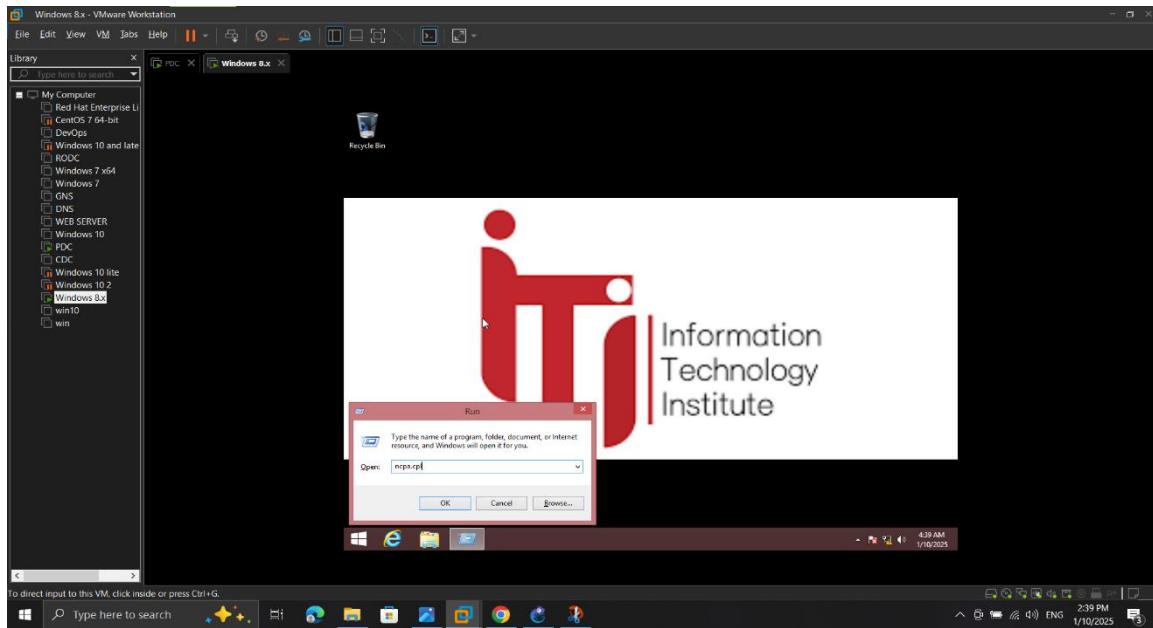




mazen@iti.local:

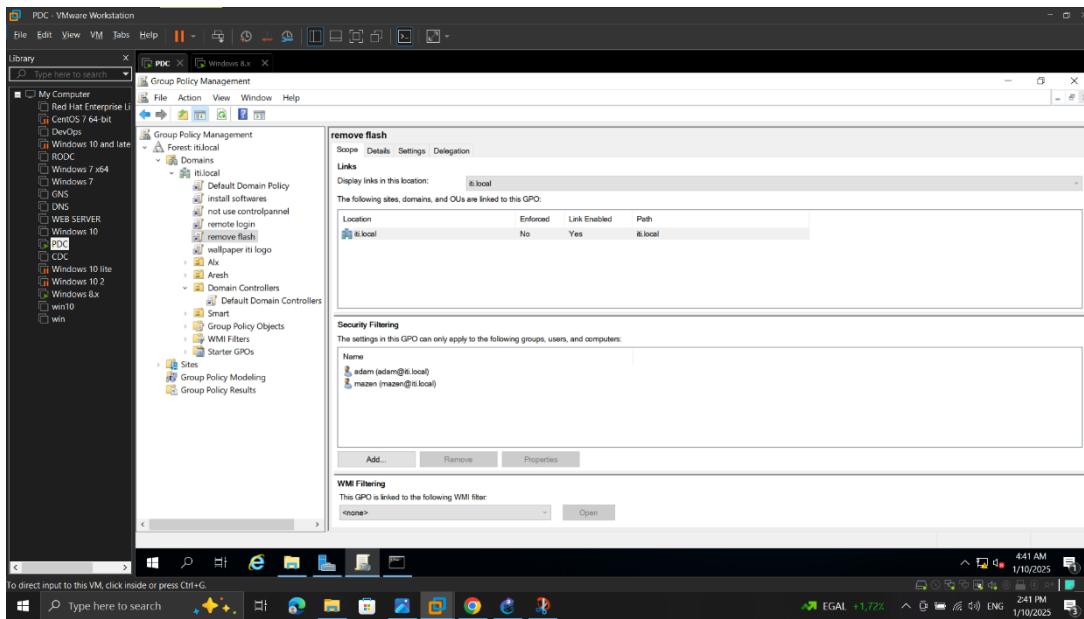
- can't use a flash memory and can't use control panel and their desktop wallpaper is ITI logo.



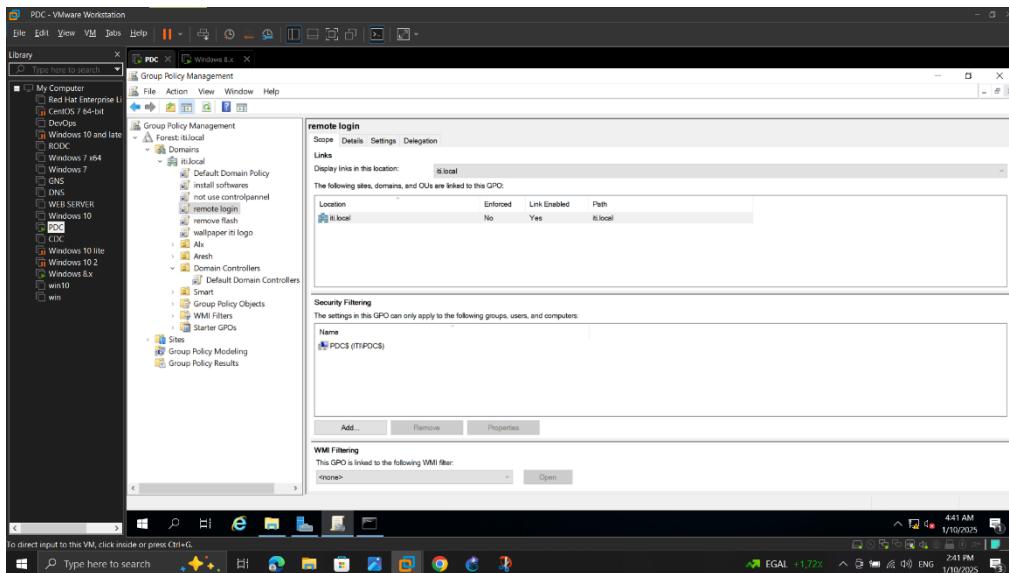


pdc.it.local:

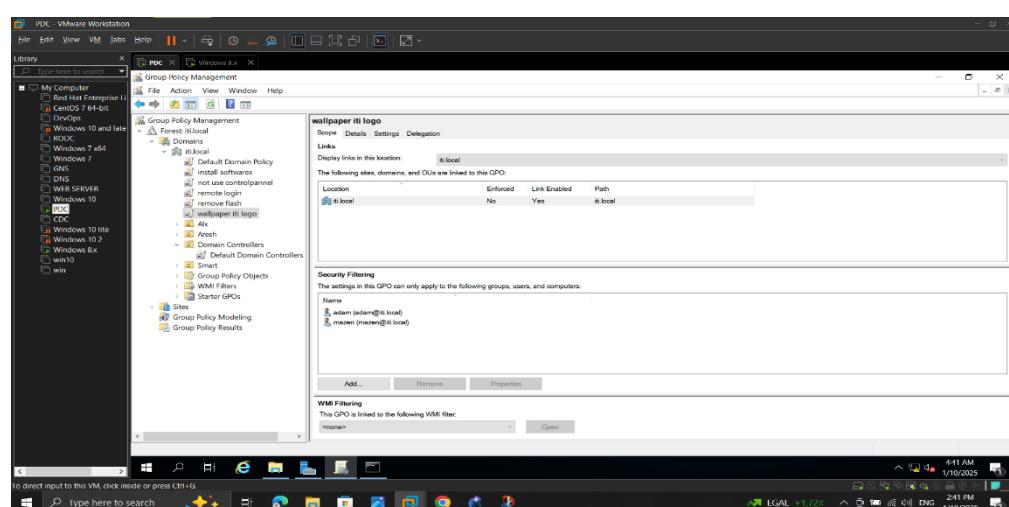
- group policy and using security filtering on it
 - a. remove flash



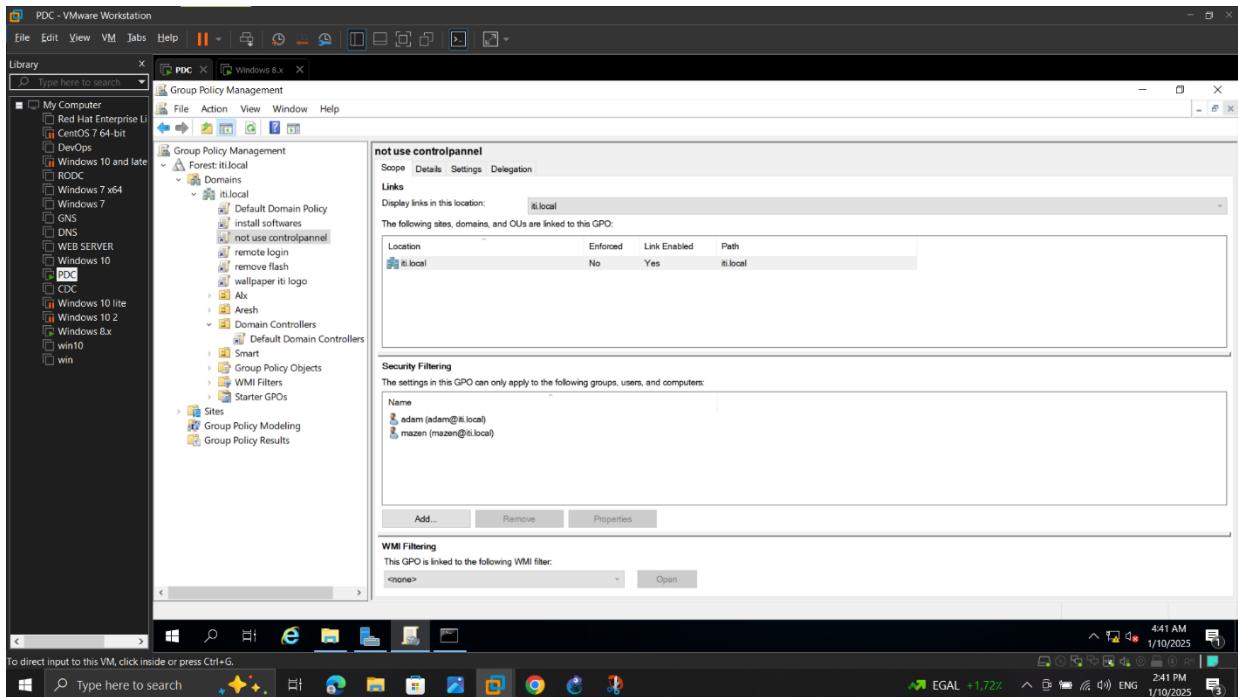
b. remote login



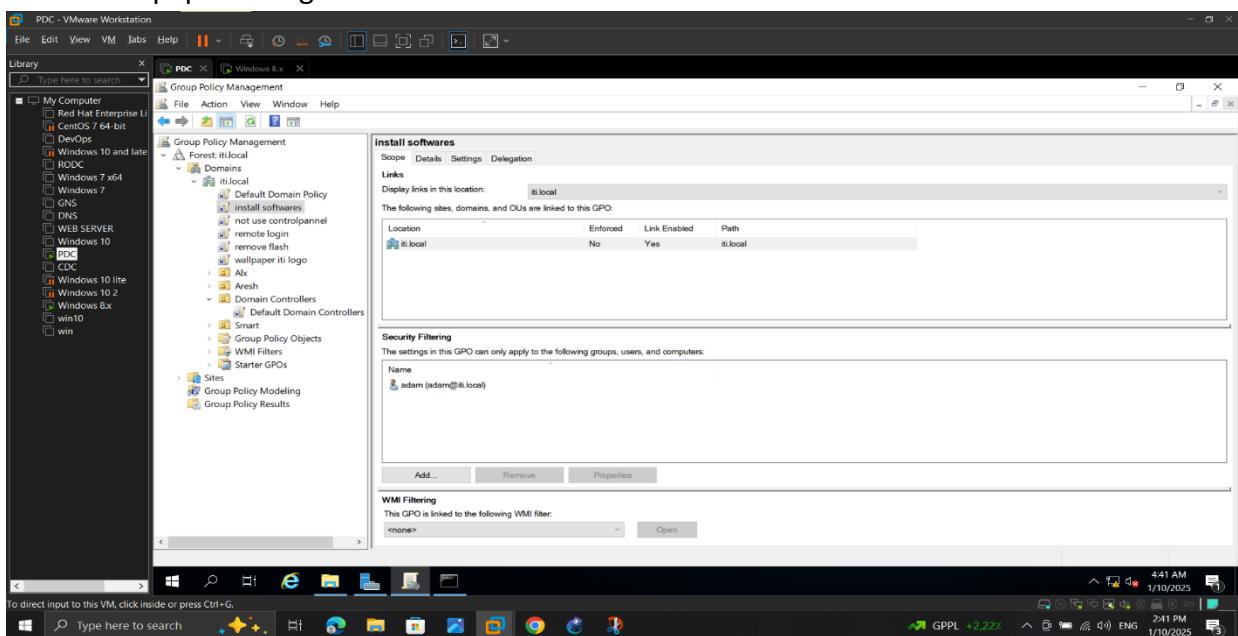
c. remote login



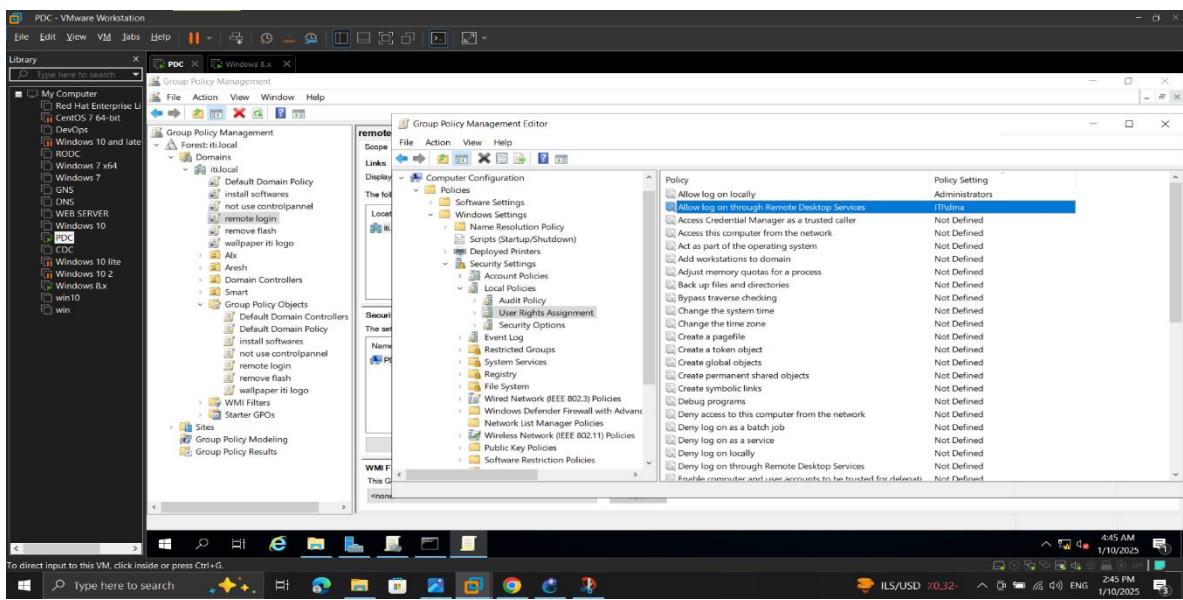
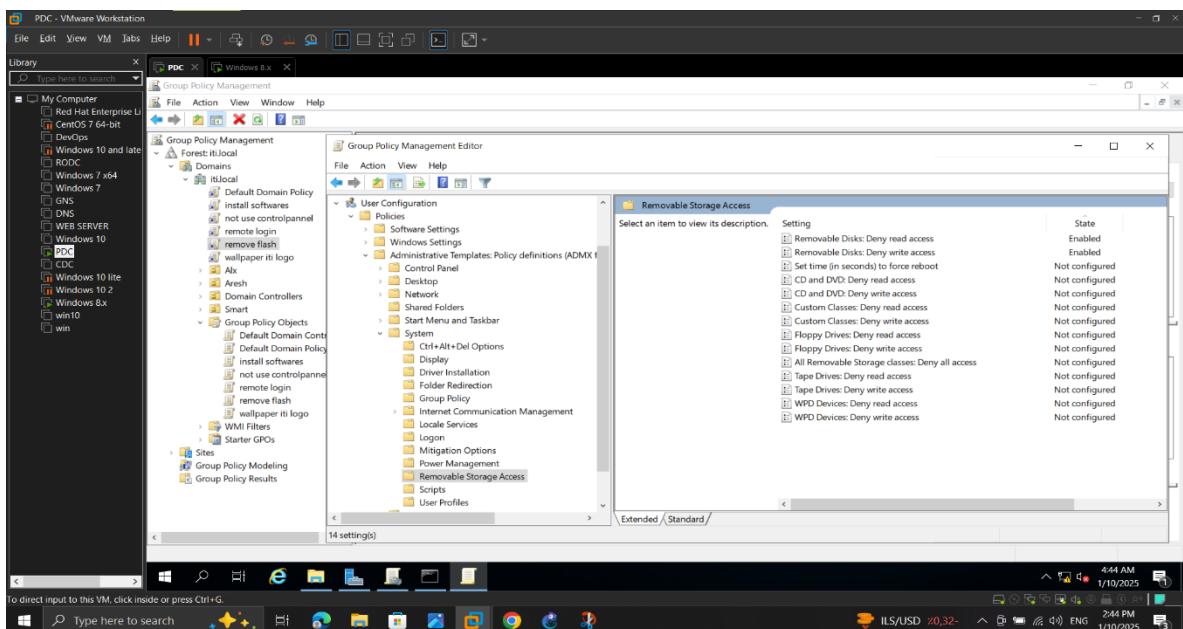
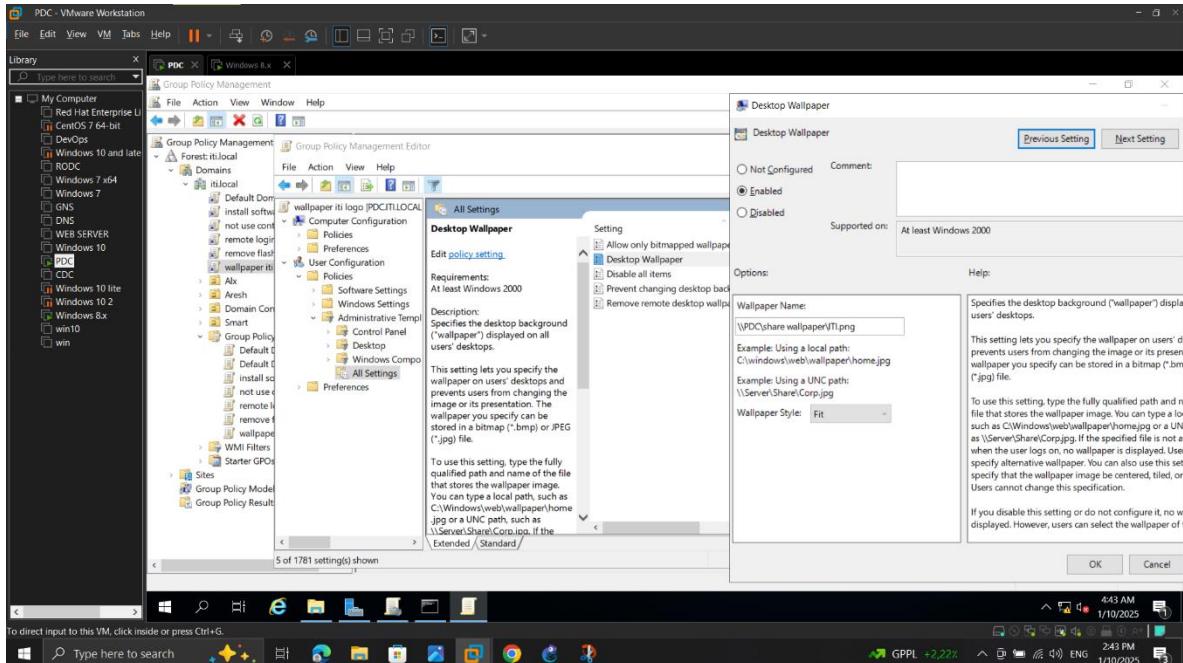
d. Not using control panel

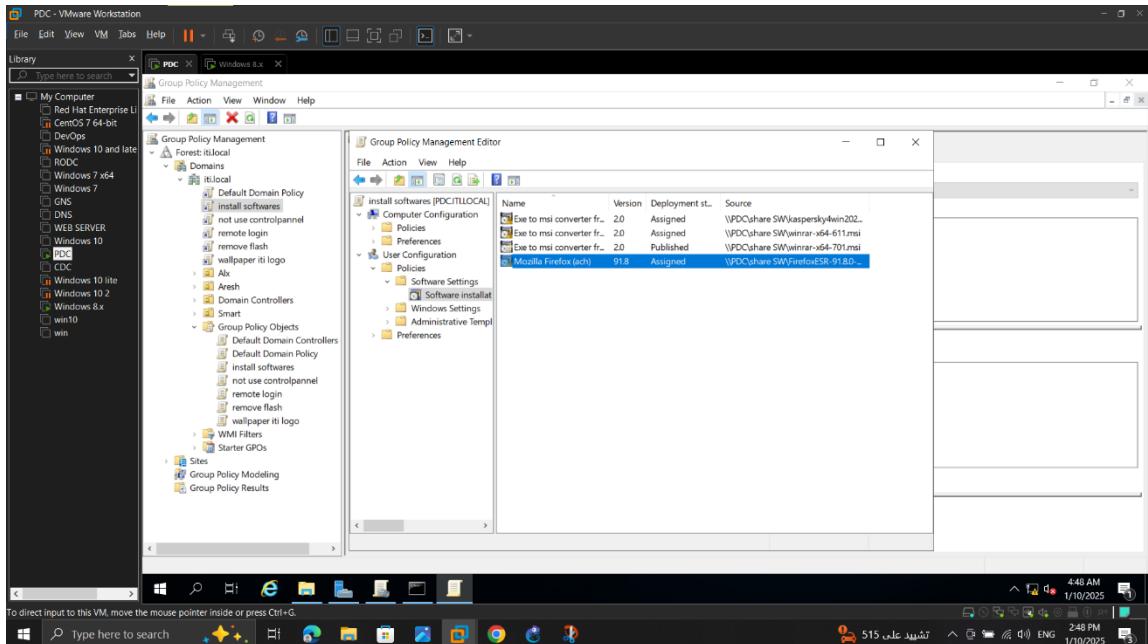
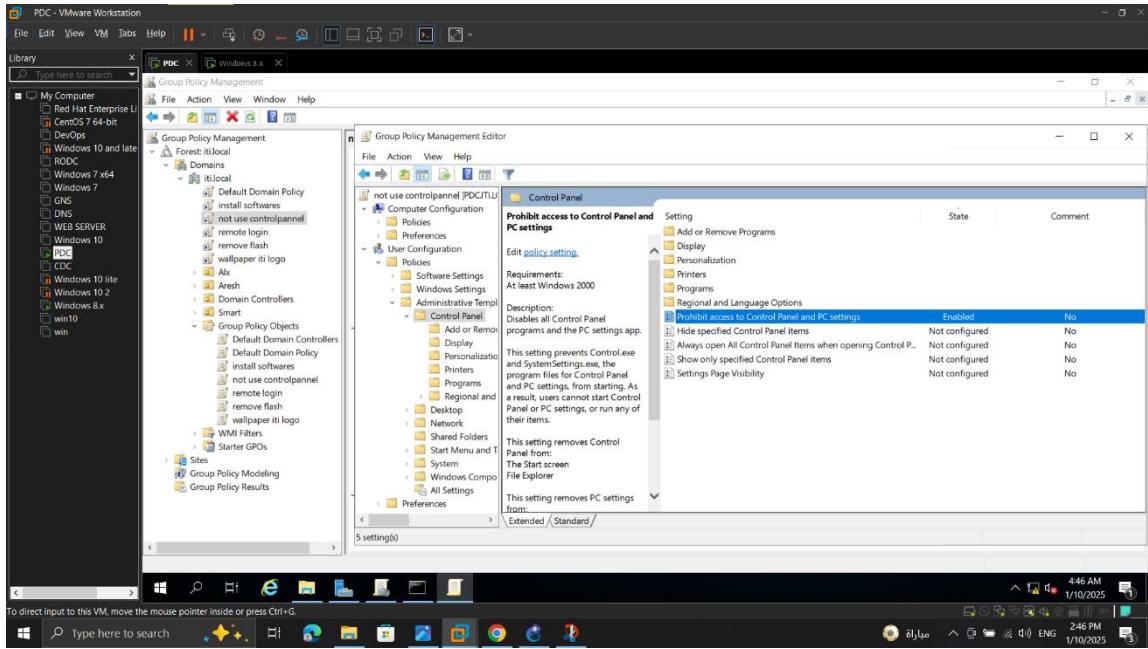


e. wallpaper ITI logo

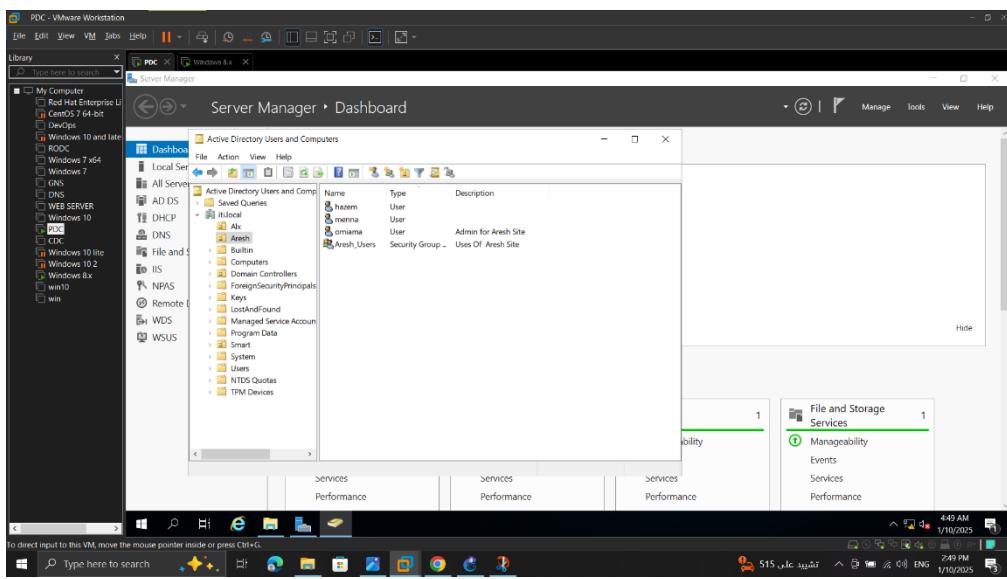


Group policy in detail

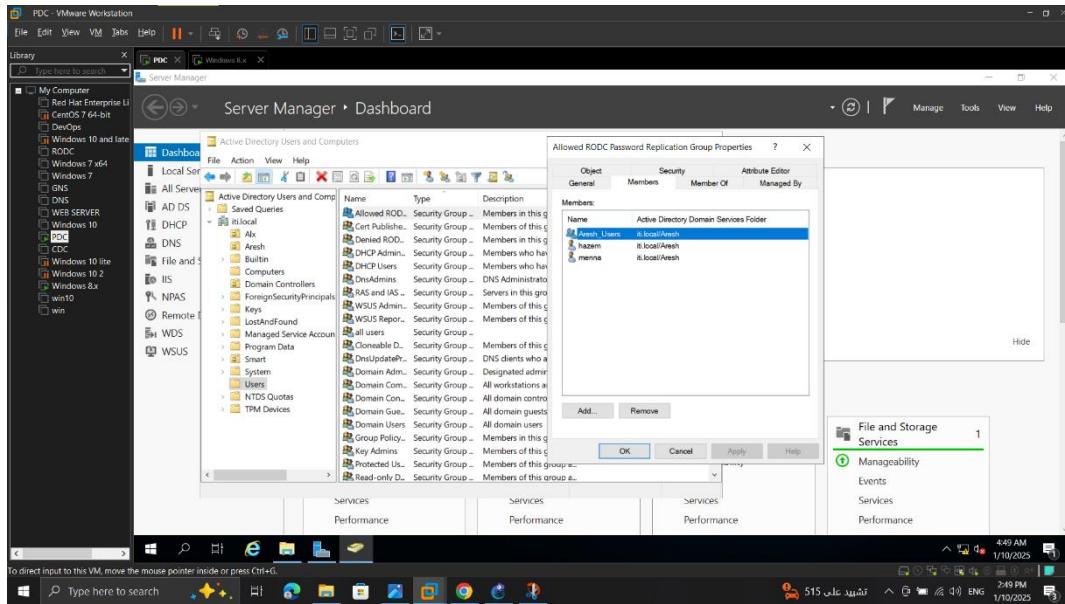




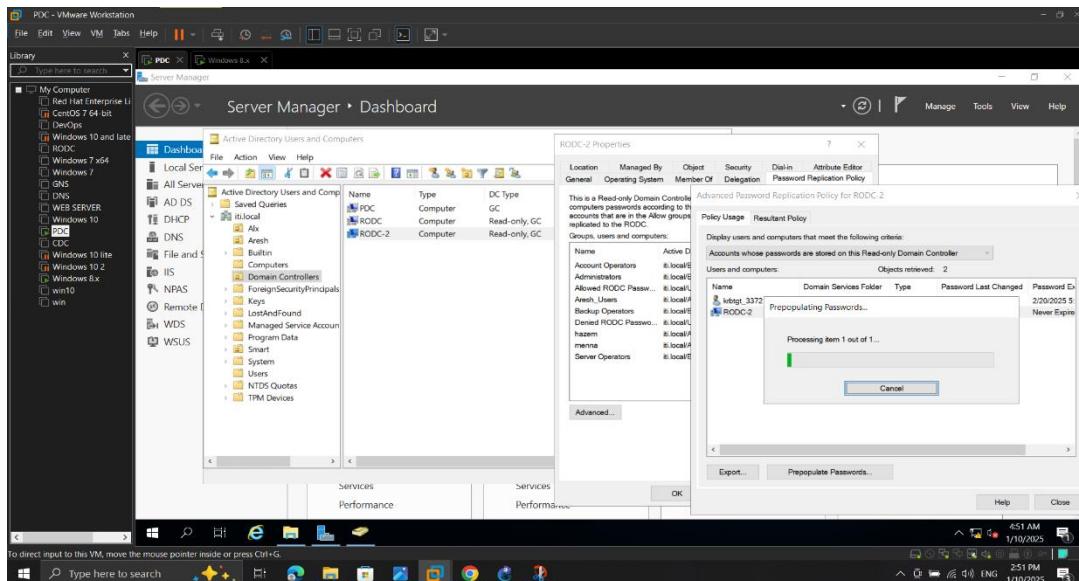
- Organization Units in PDC:



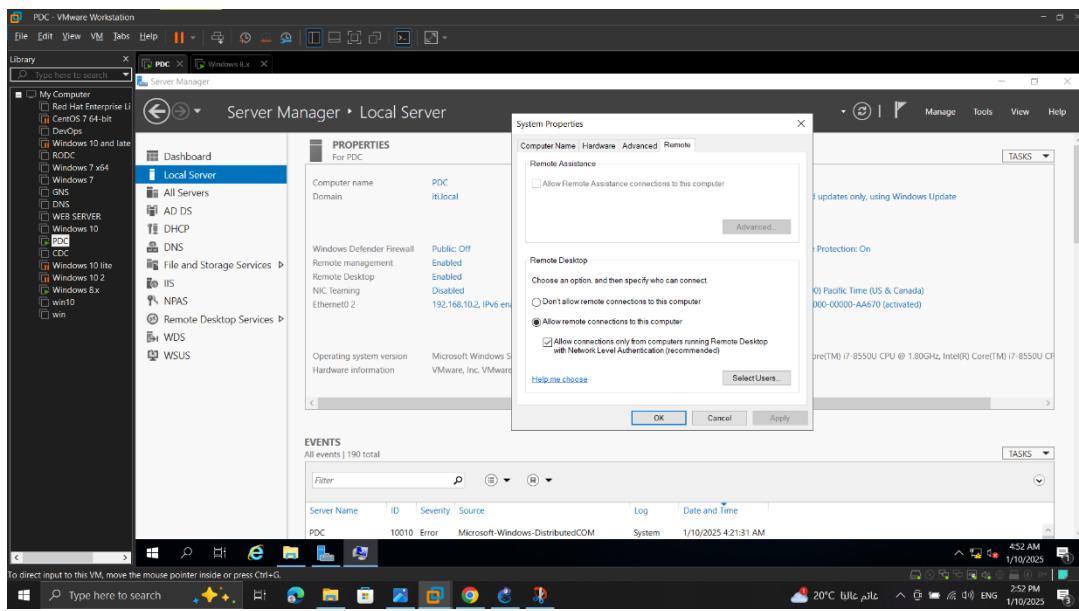
- Allow RODC password replication group



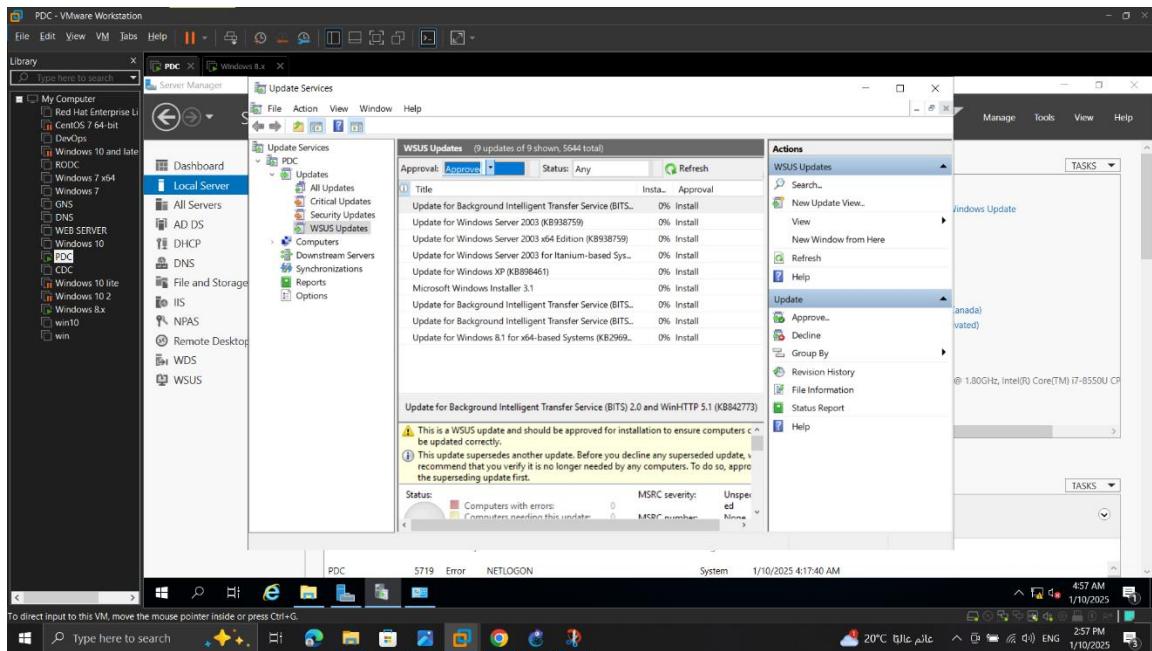
- Repopulate password to RODC to replicated password now (if first time login and PDC is off)



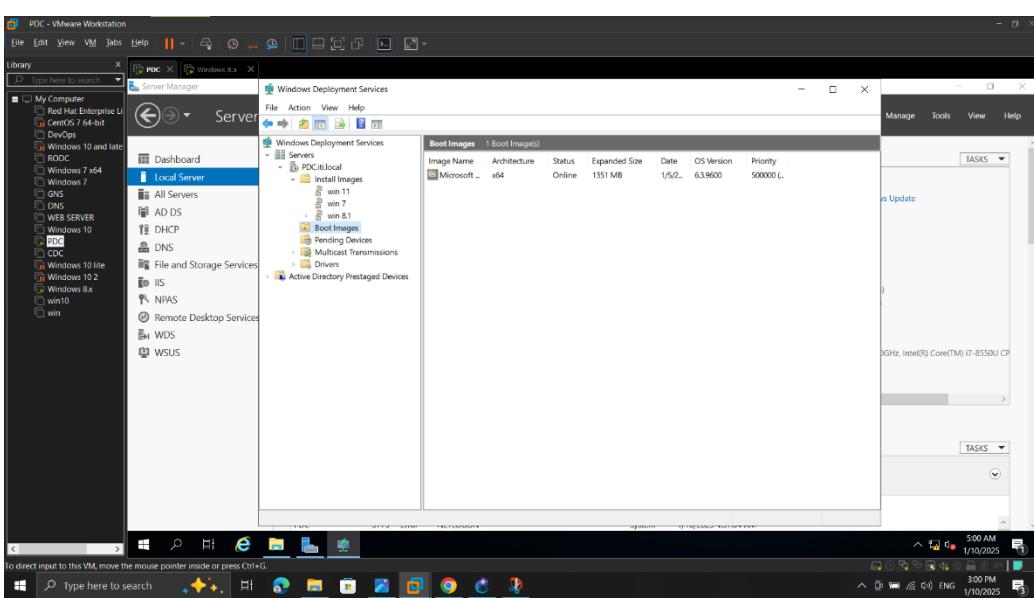
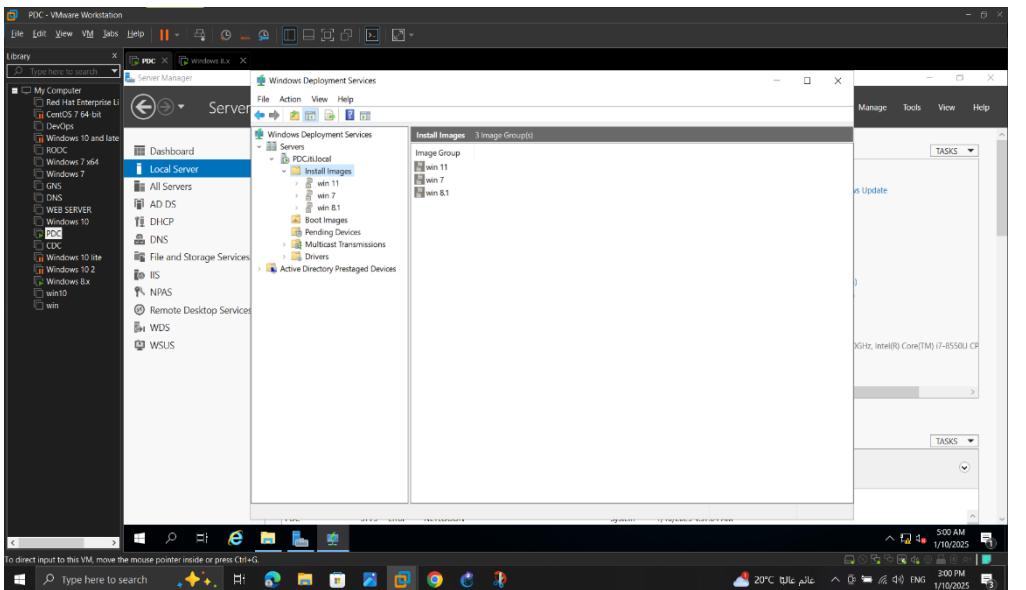
- Enable Remote Desktop (RDP) in PDC:



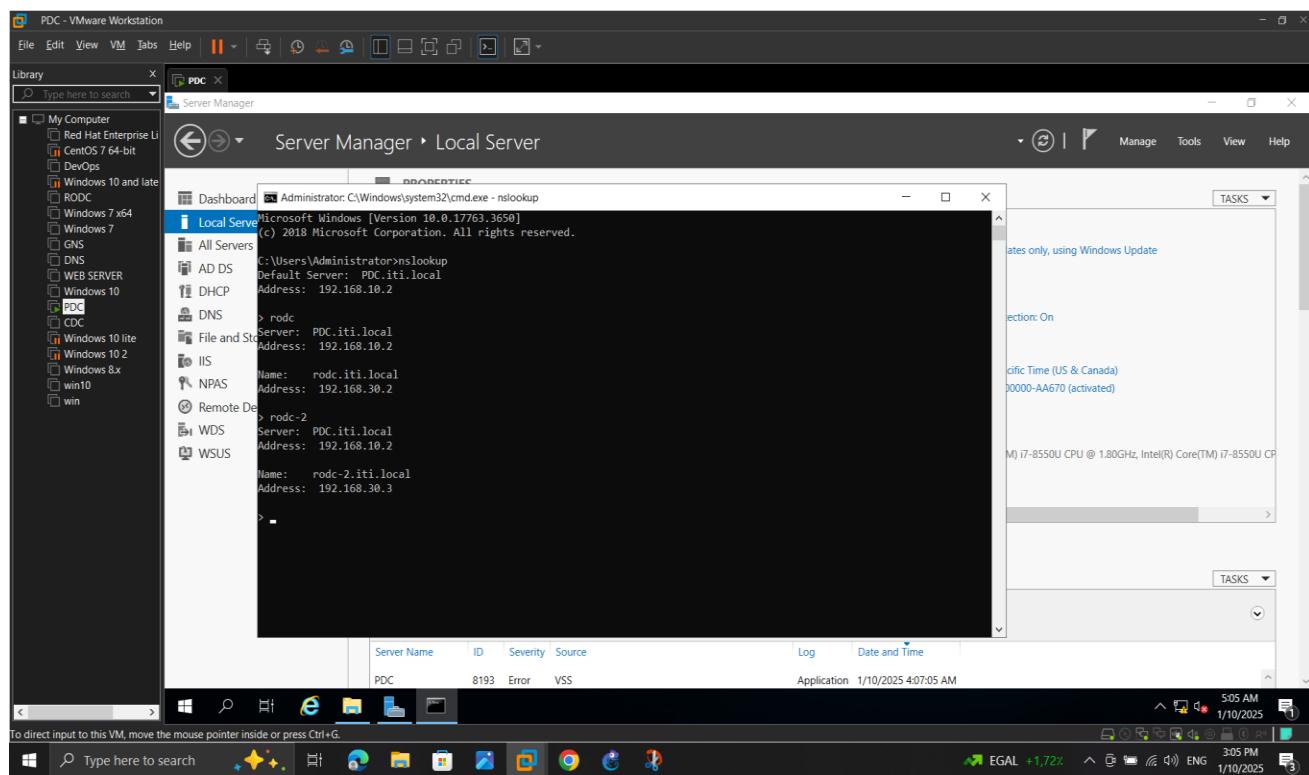
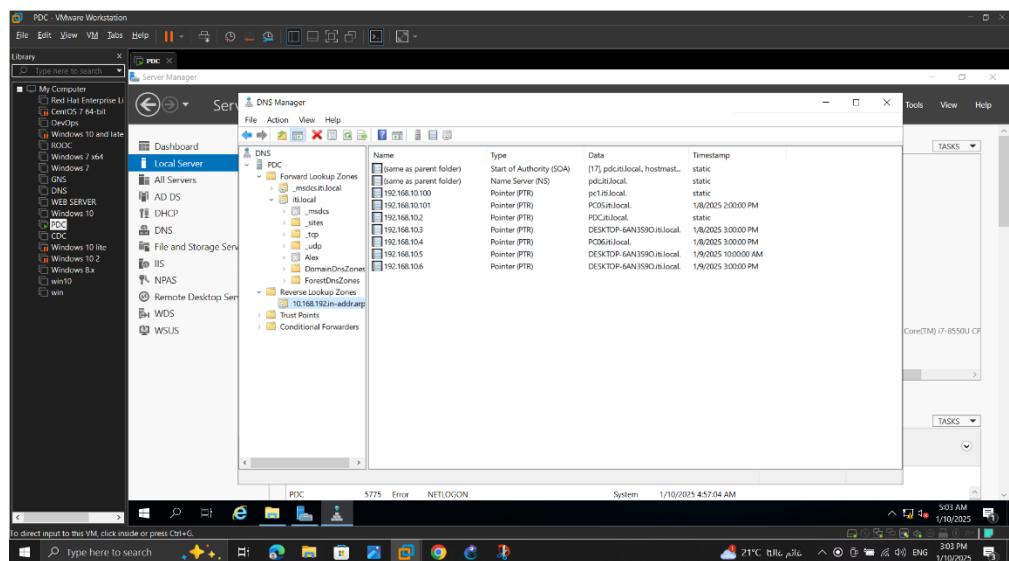
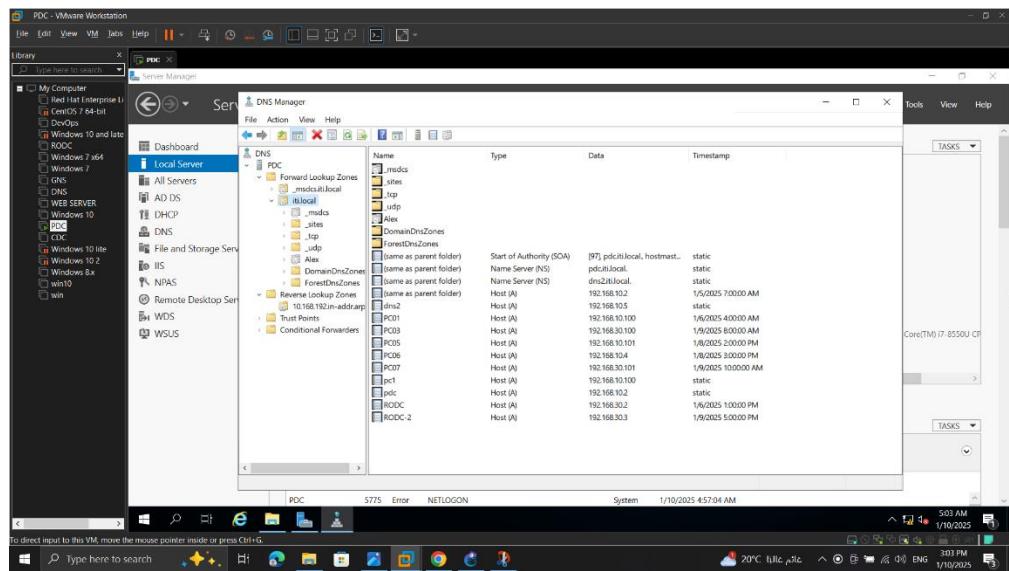
- Windows Server Update Services (WSUS)



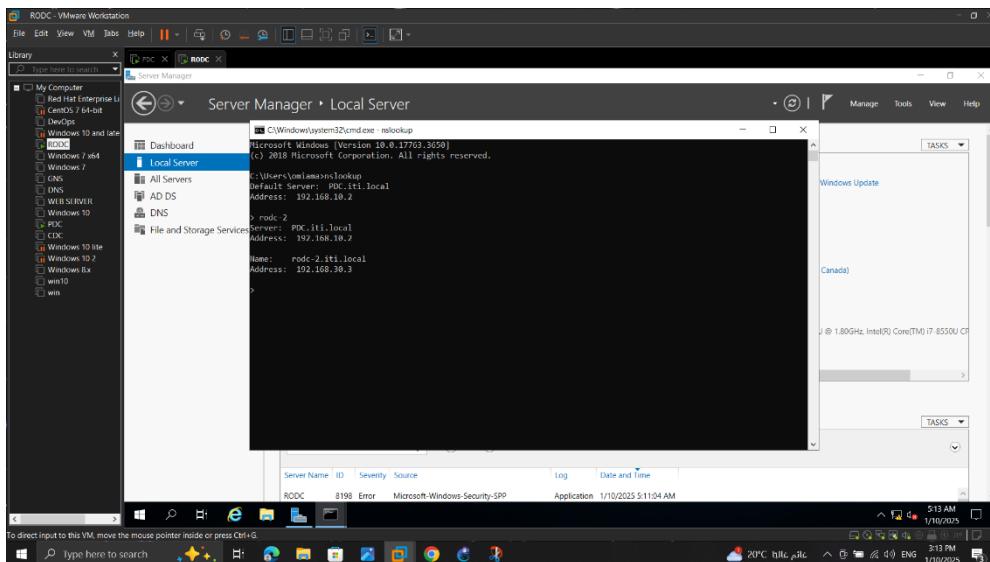
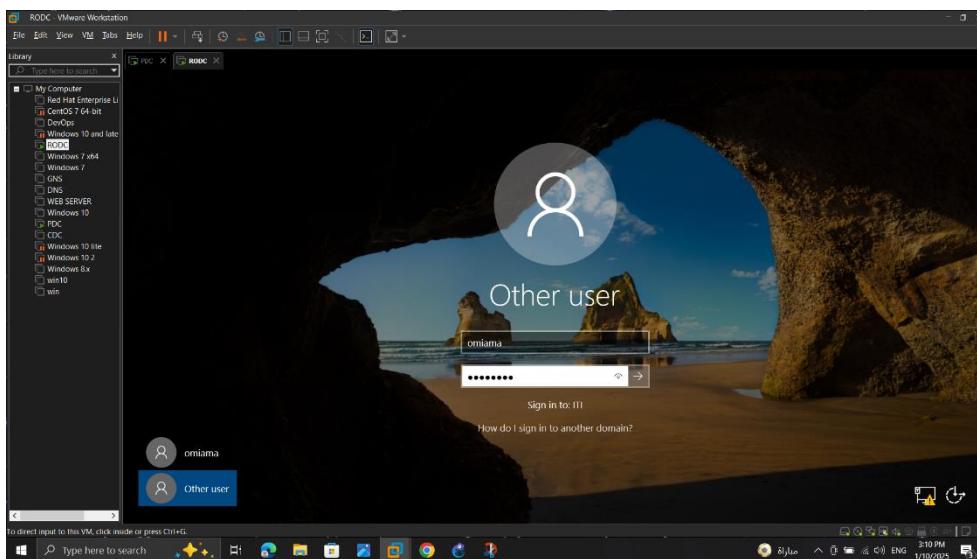
- Windows Deployment Services (WDS) ==> (install image and boot image)



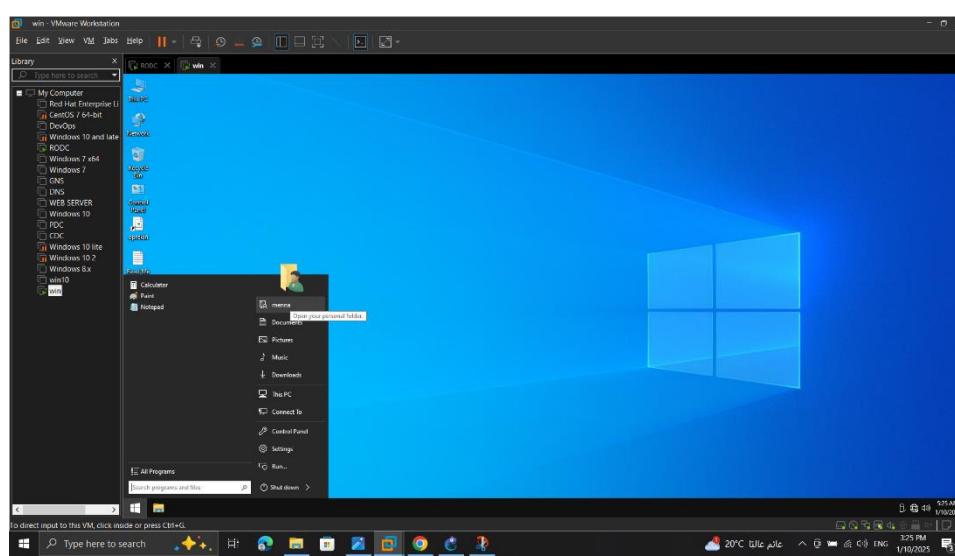
- Domain Name Server (DNS) → primary zone forward and reverse lookup

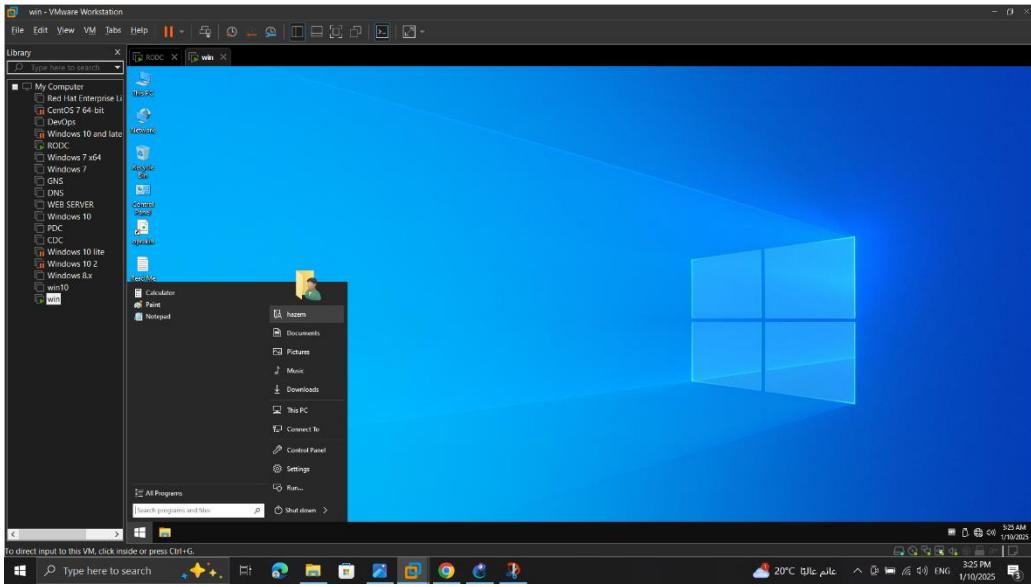


- Read Only Domain Controller (rodc.iti.local)
 - Omama is delegated as admin for RODC (Not Writable Domain)
 - Password of hazem and menna are allowed to replicate in RODC by PDC
 - DNS is PDC → 192.168.10.2

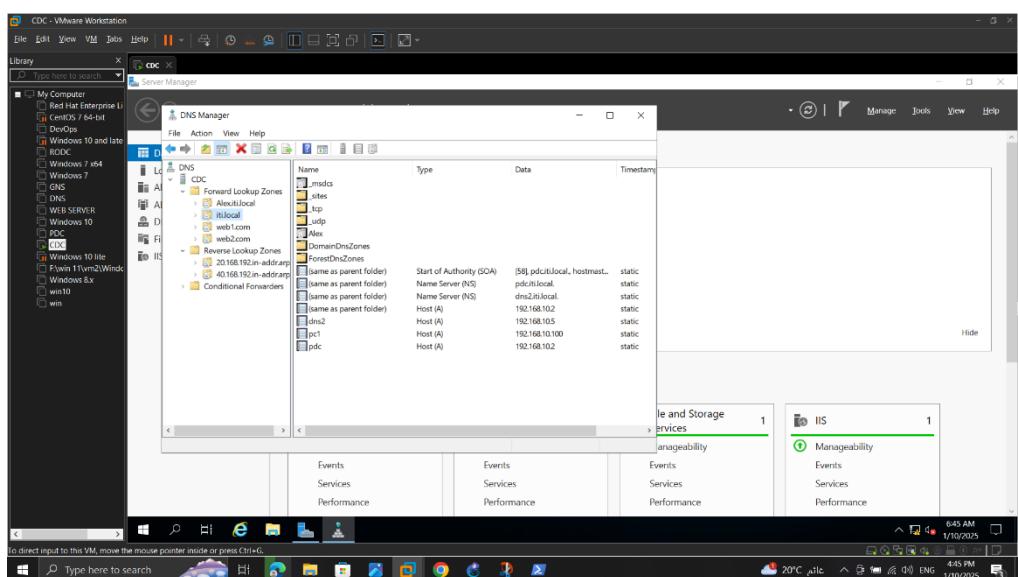
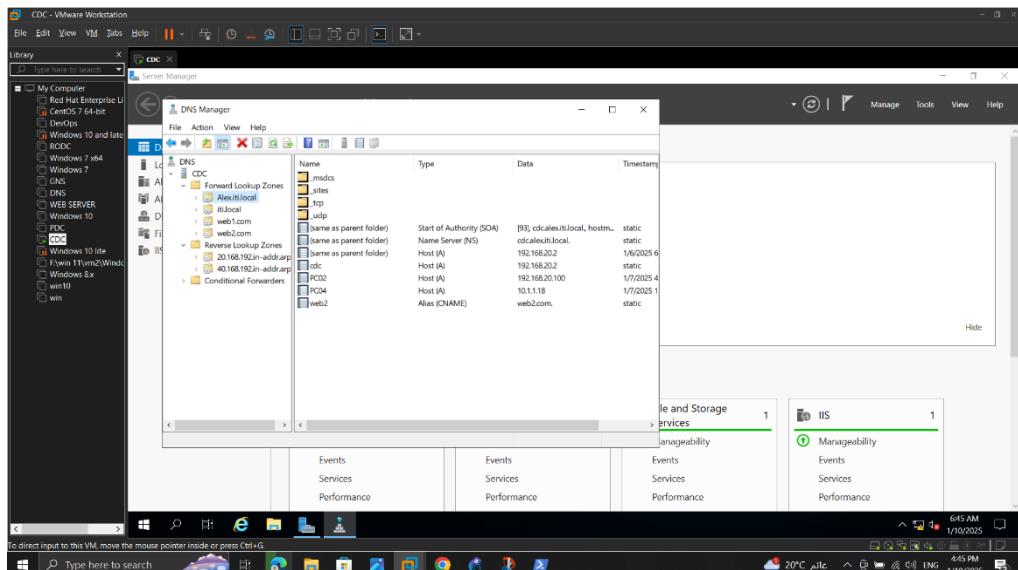


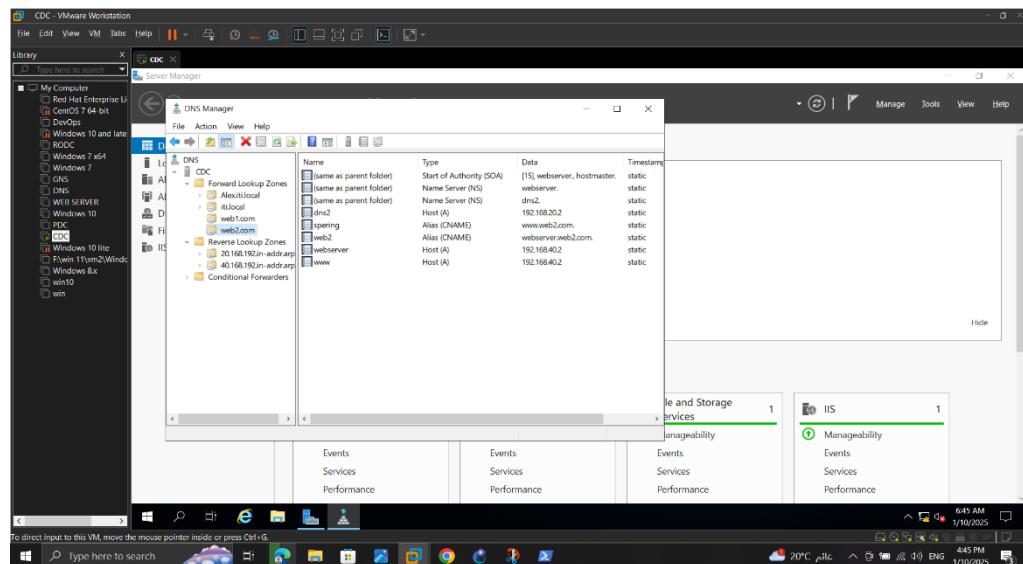
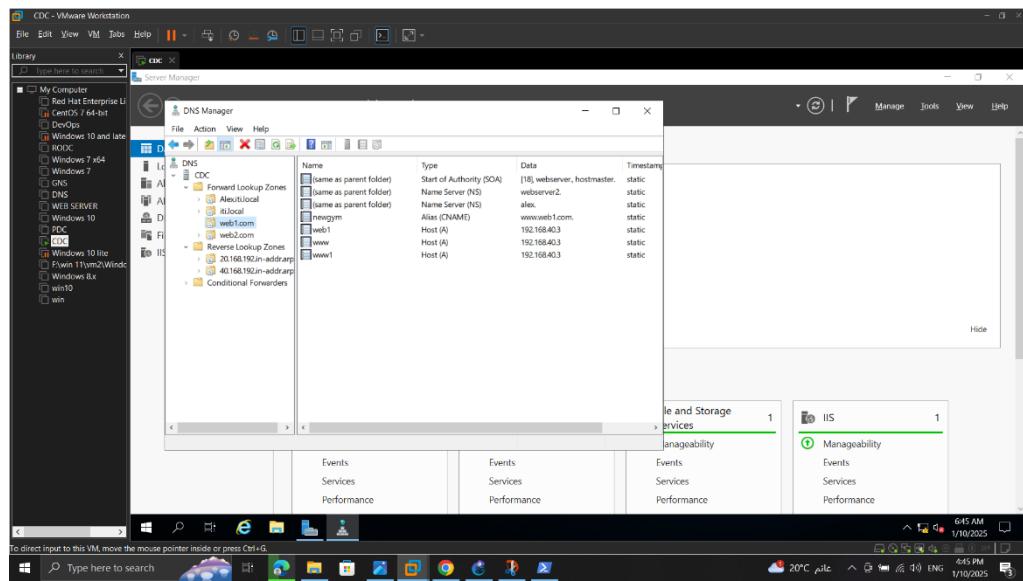
- PC03.iti.local can login in it menna and hazem only if PDC down



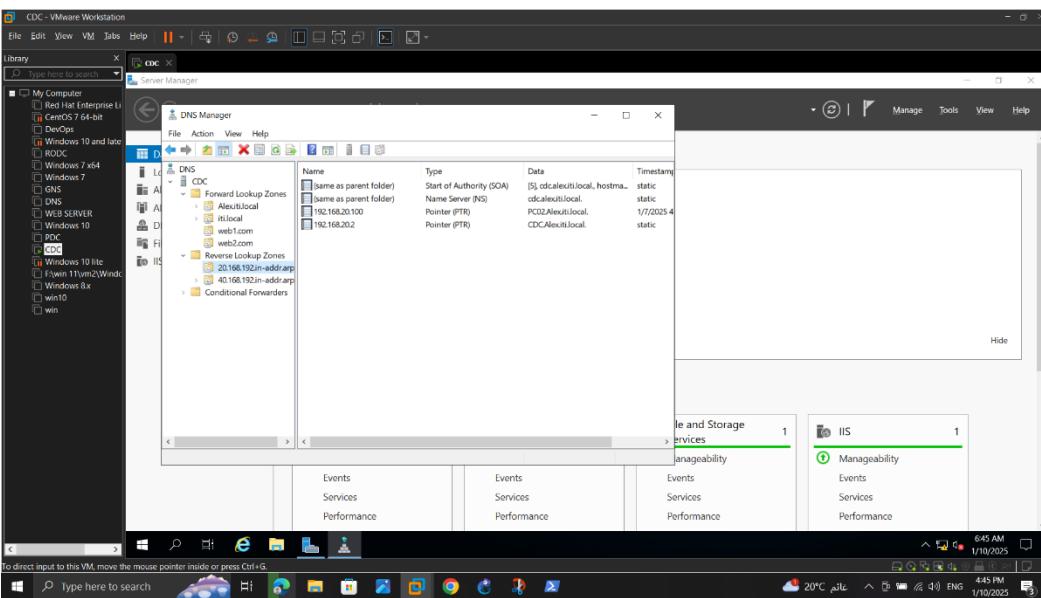


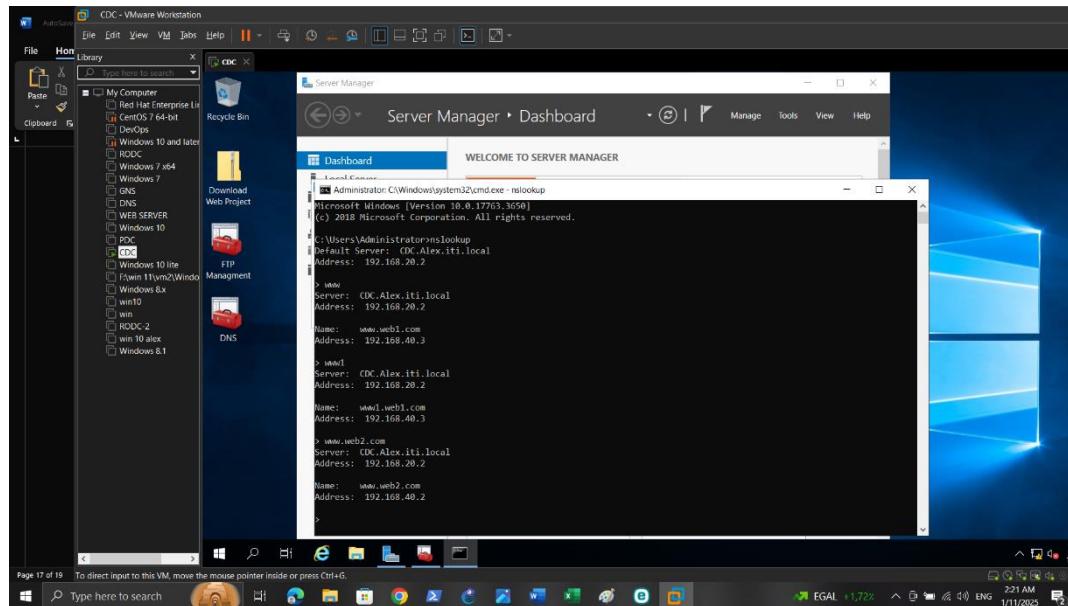
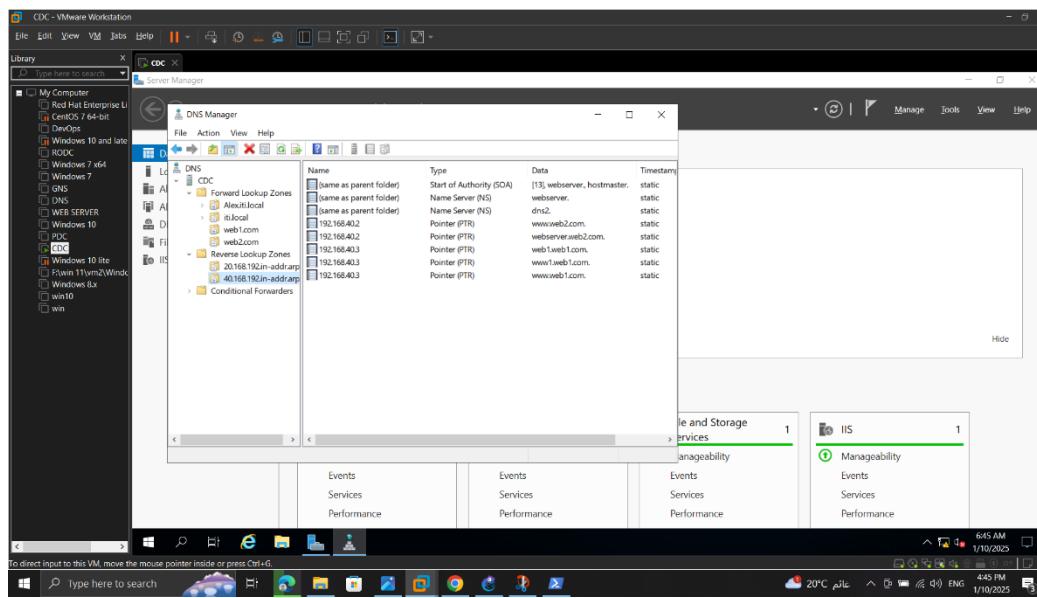
- CDC (Child Domain Controller) ➔ Alex.iti.local
 - DNS of that domain contain primary zone(alex.iti.local) and three secondary zones (iti.local, web1.com, web2.com)





➤ Two reverse lookup zone for two subnets (192.168.20.0 and 192.168.40.0).

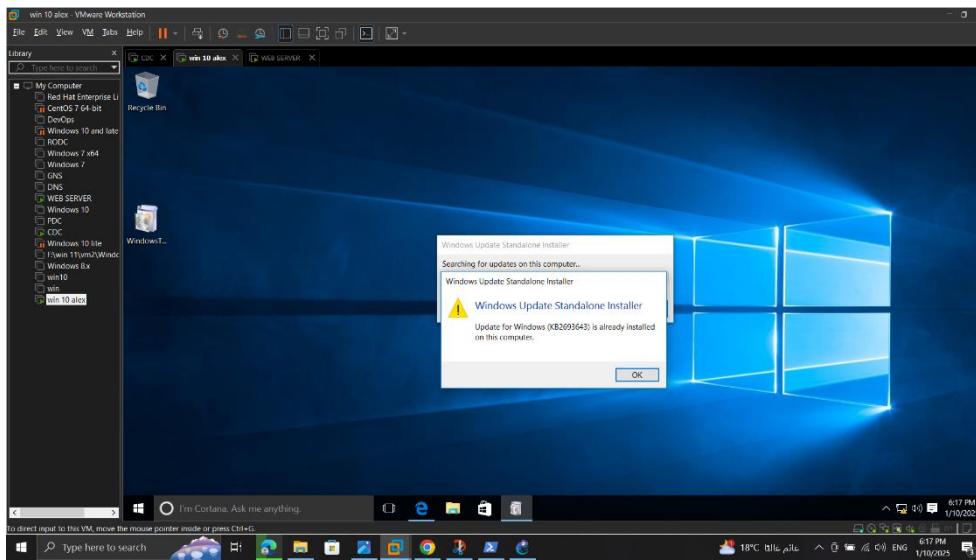




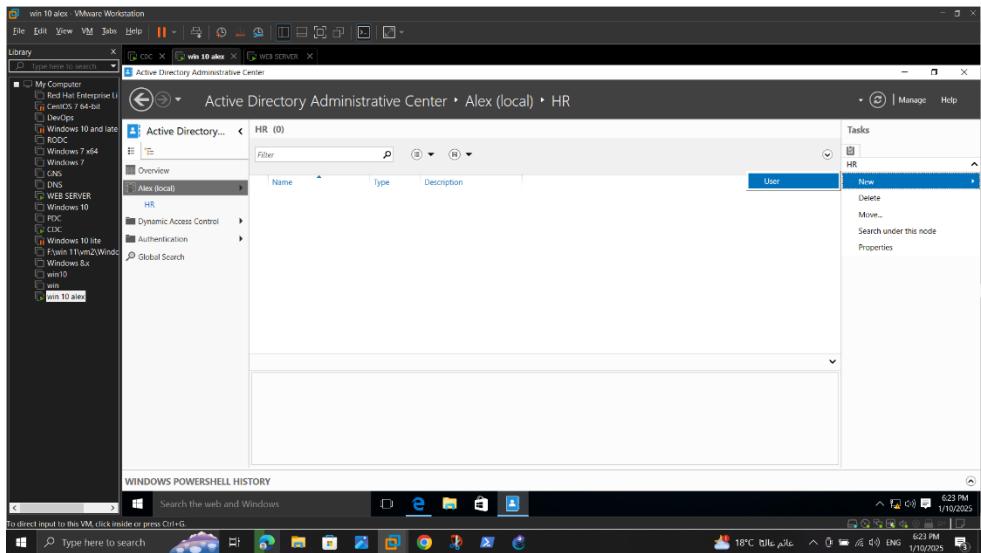
➤ asmaa@alex.iti.local

can access remotely the webserver with administrative privileges and can create and delete users on HR Department in Alex.iti.local and can browse <http://www.web1.com>.

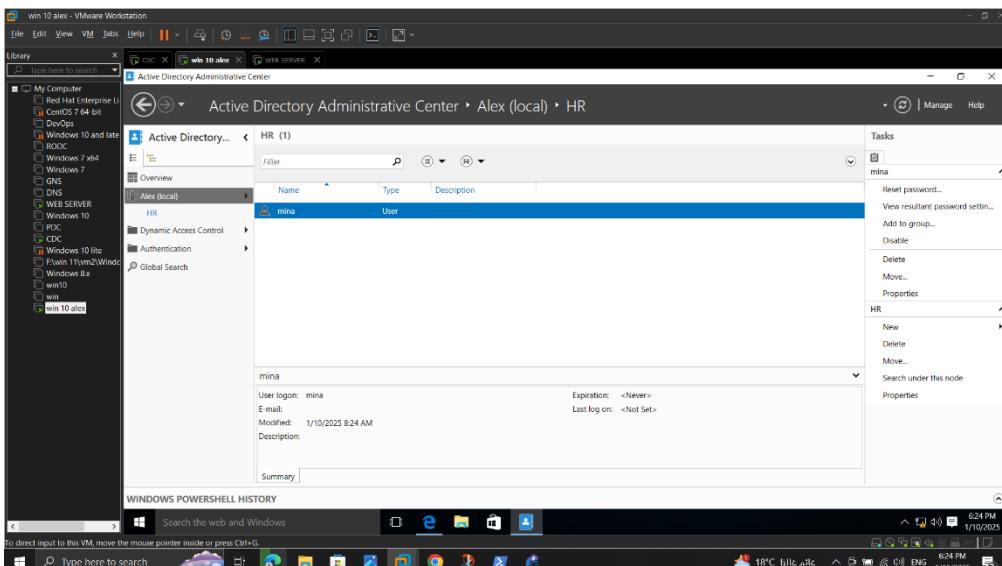
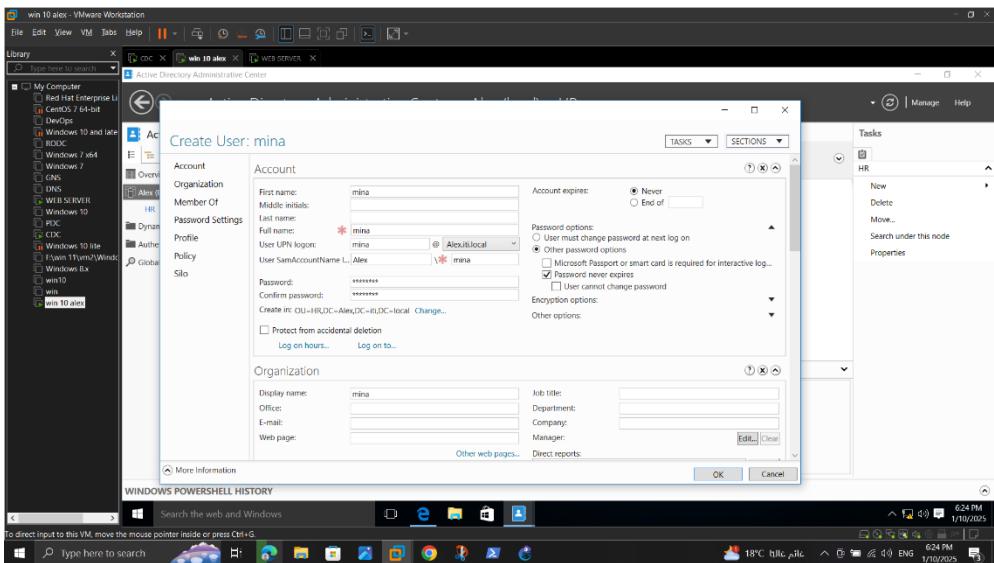
- Install RSAT (Remote Server Administration Tools)



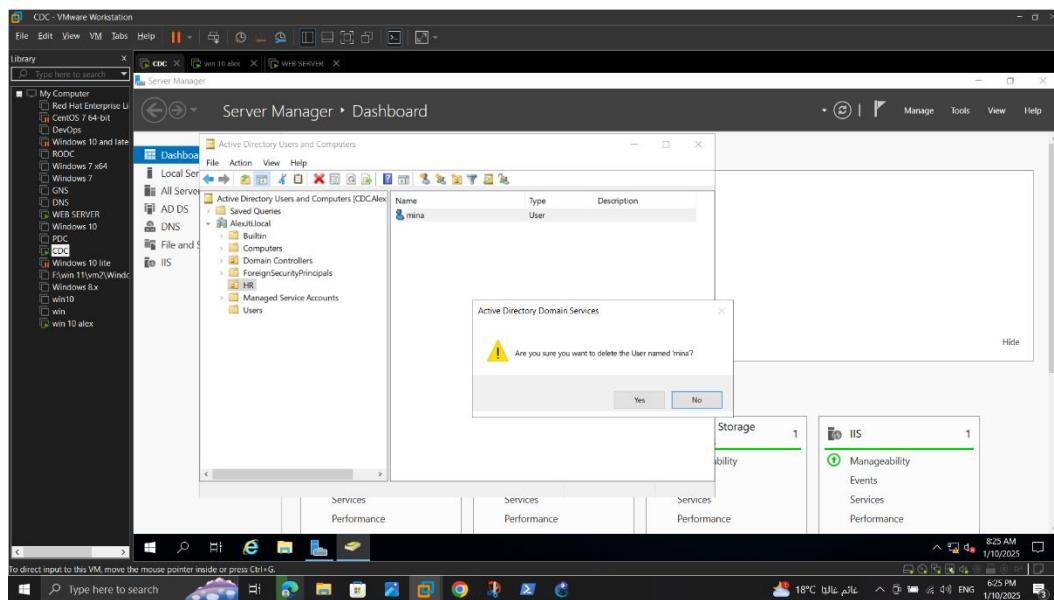
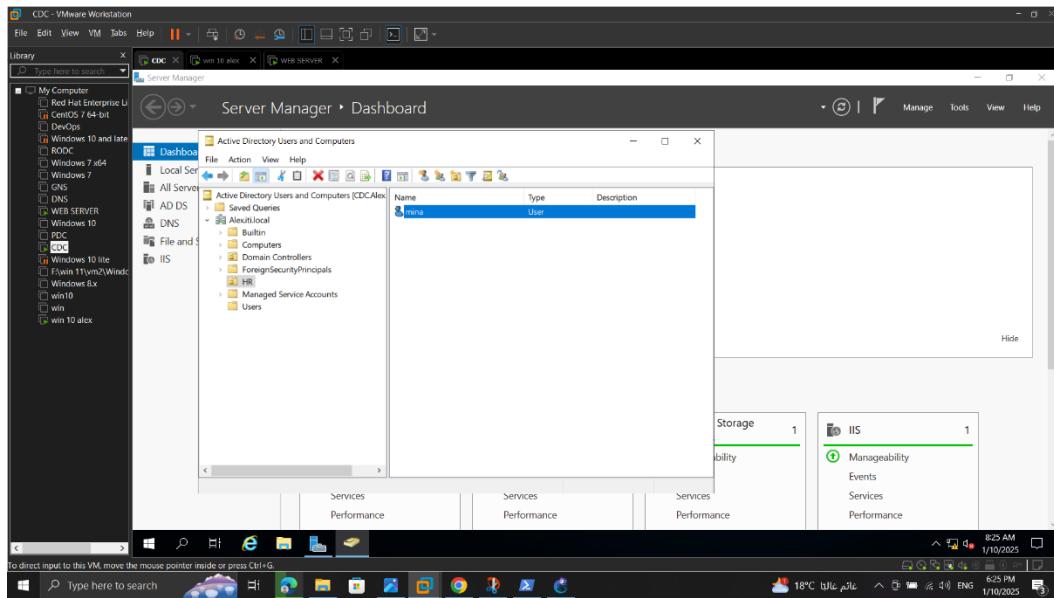
- open Active Directory Administrative Center (ADAC)



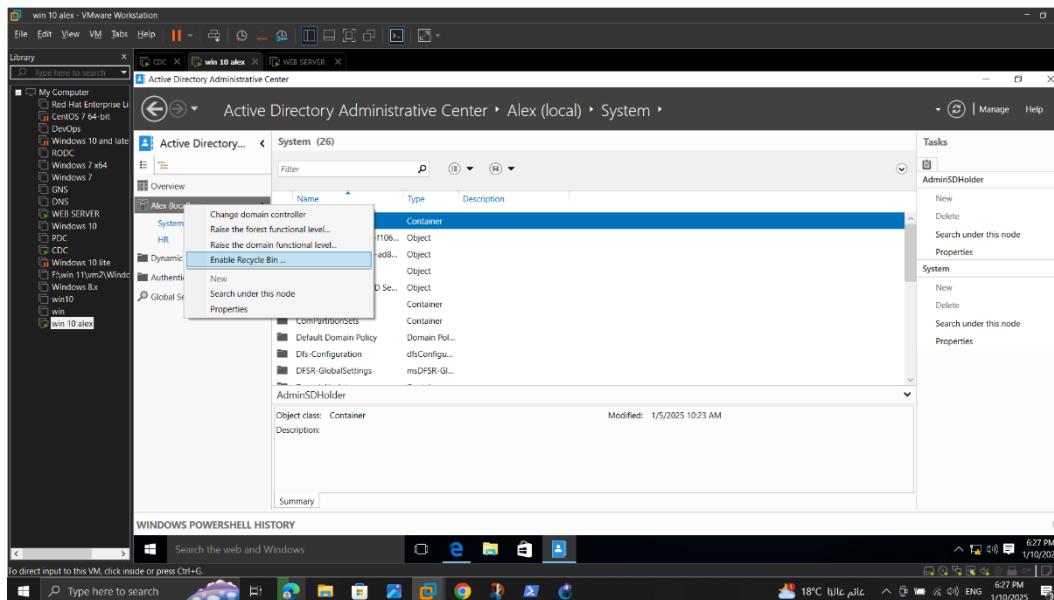
- Asmaa delegated to add and delete users in HR → add user mina



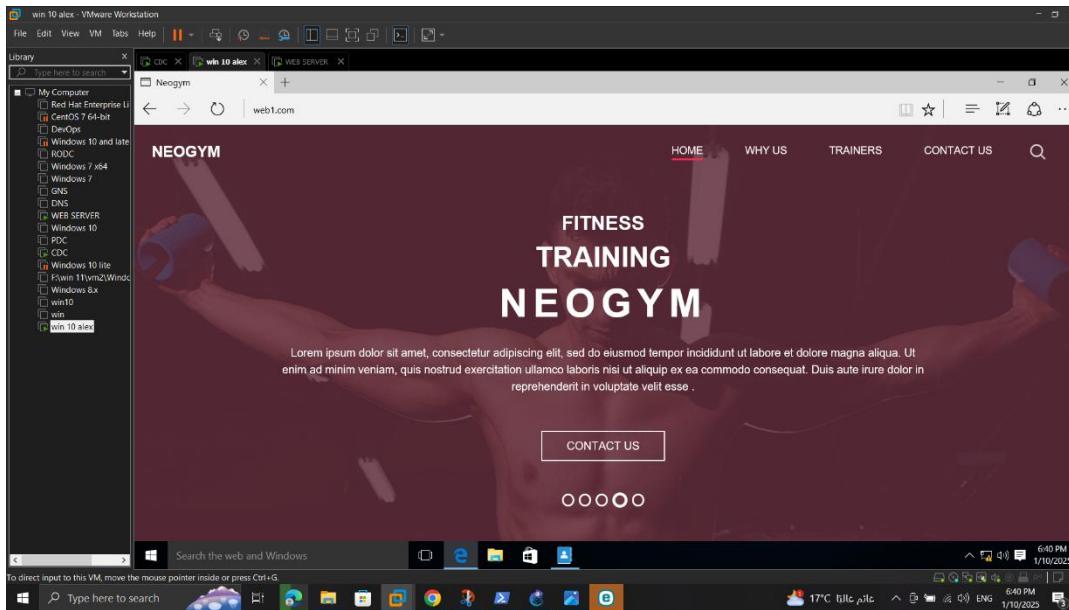
▪ Return to CDC



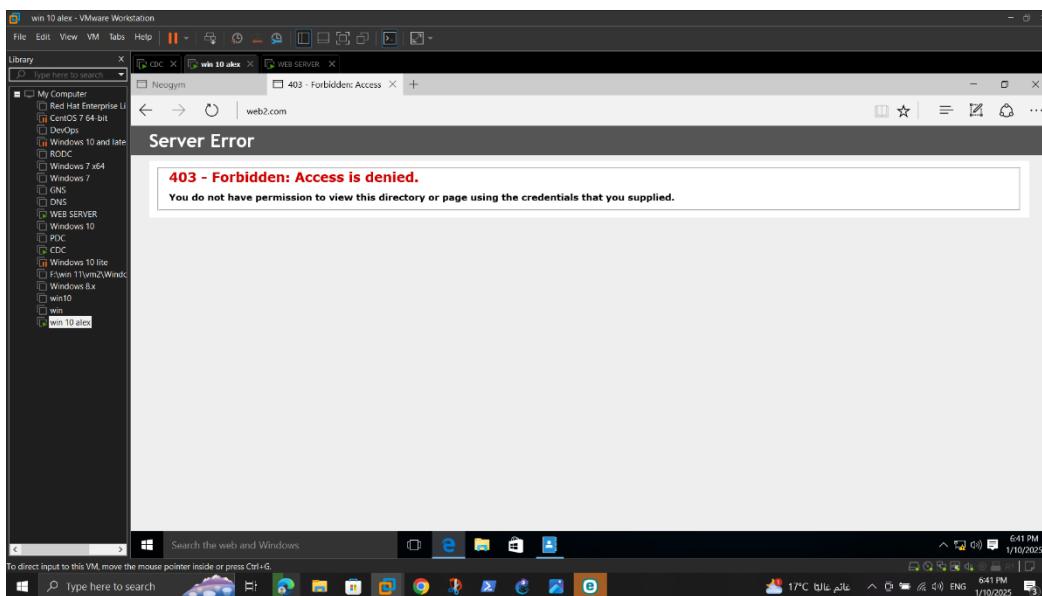
▪ Enable bin to return the deleted object



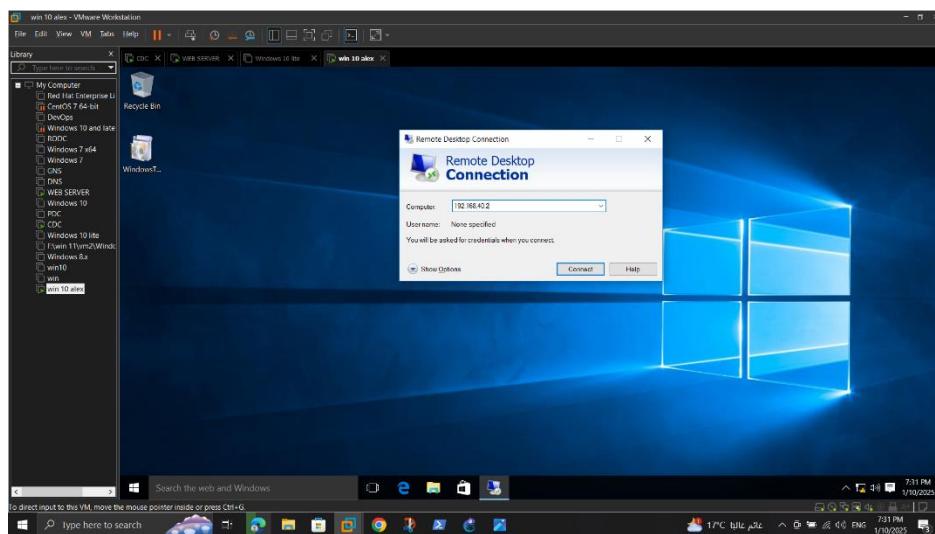
- Access web1

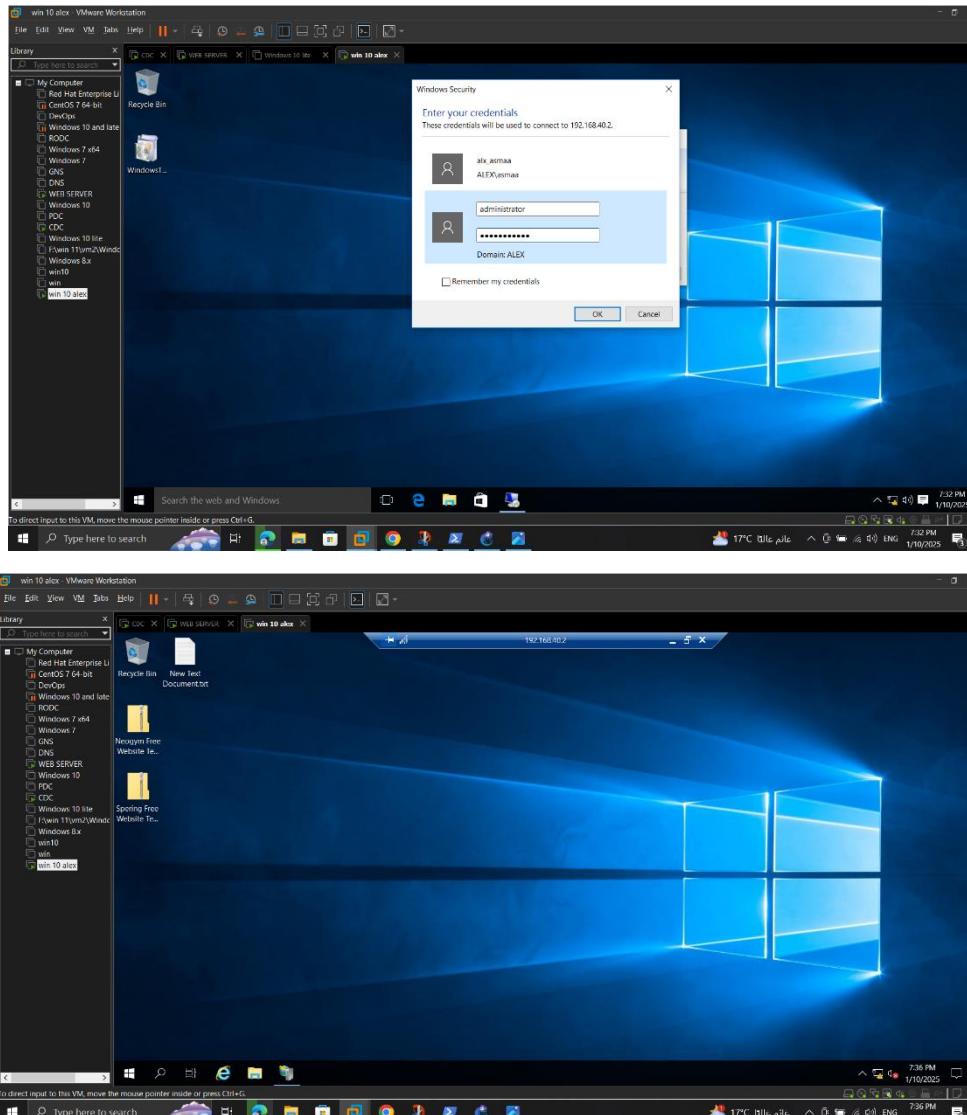


- If she tries to access web2 will be denied by WEB SERVER

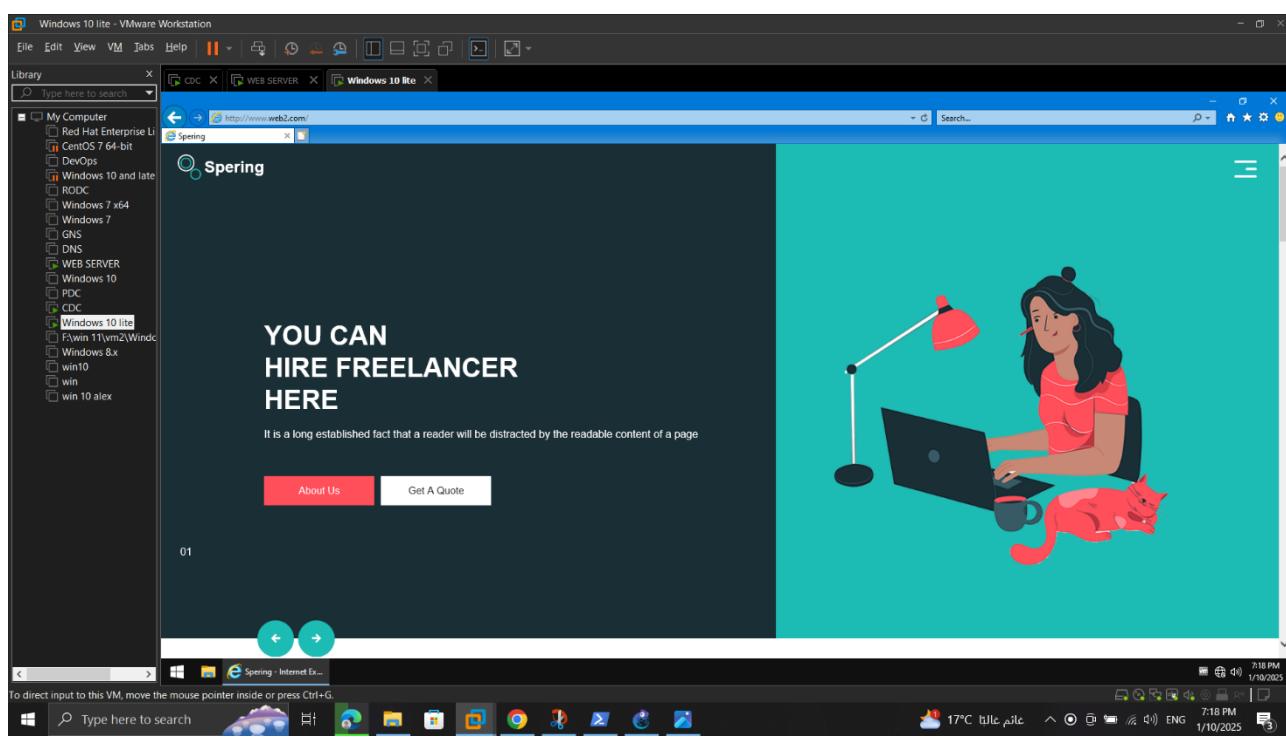


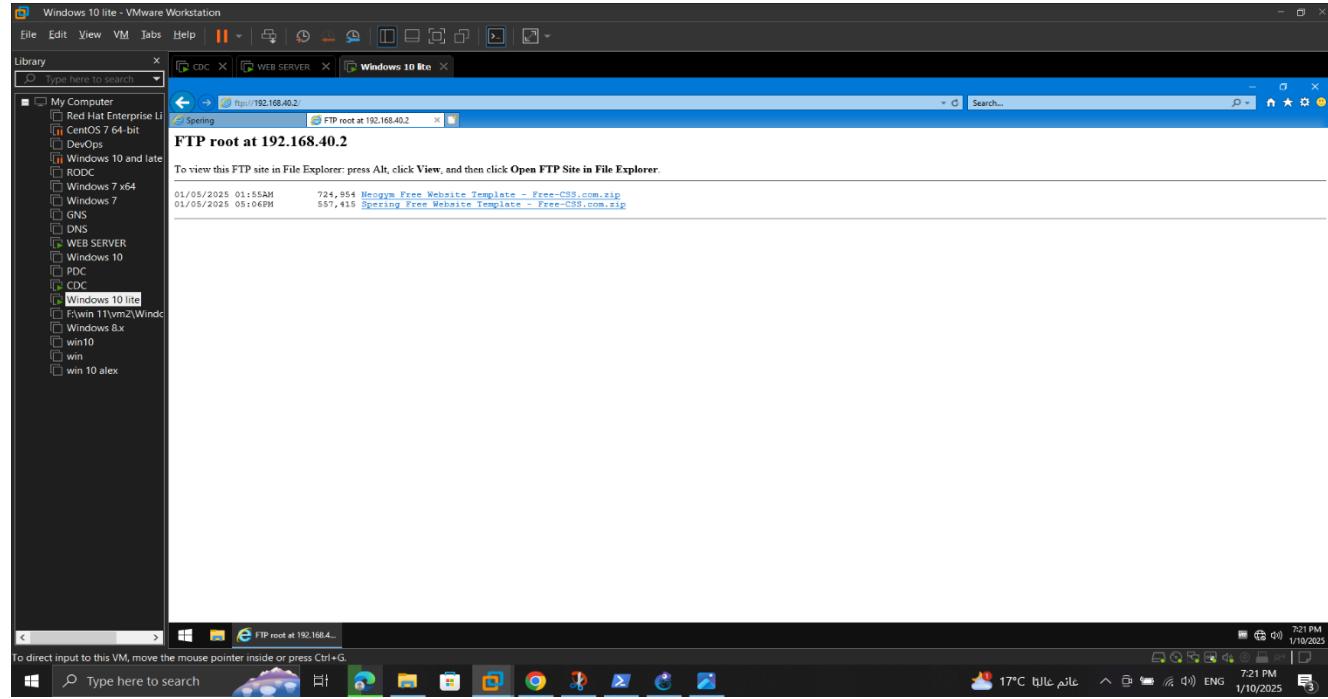
- Access WEB SERVER remotely with administrative privileges.



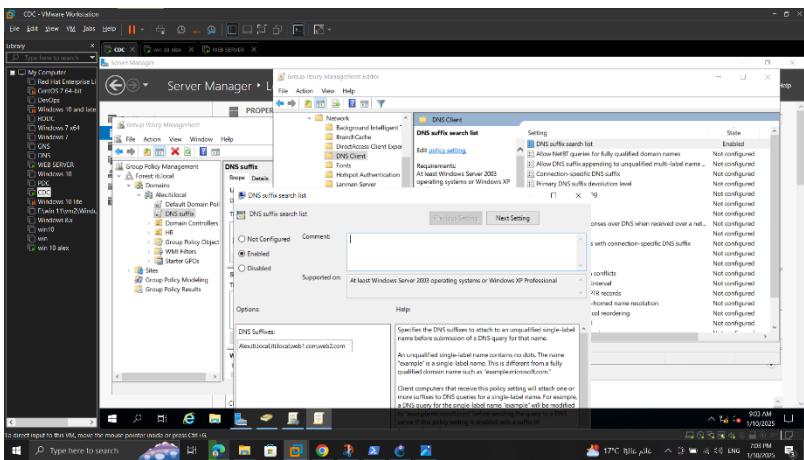


➤ Basel@alex.iti.local : can browse <http://www.web2.com> and FTP.

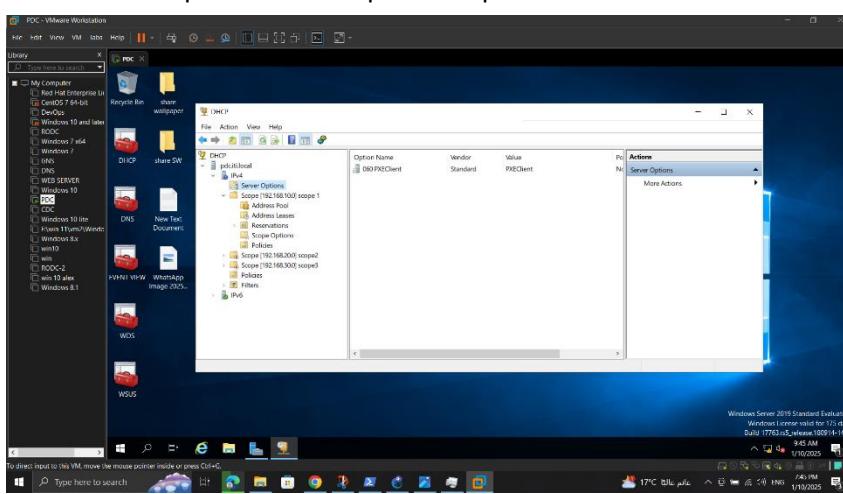




➤ Group policy in CDC (DNS Suffix):

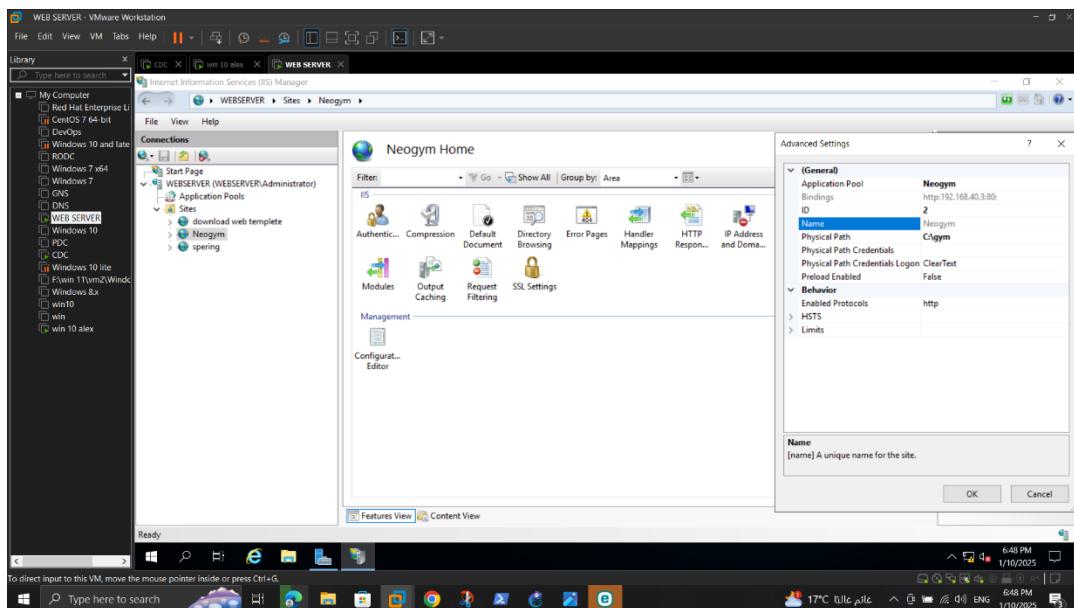


- additional service in PDC but is off is DHCP has 3 scopes (192.168.10.0/24, 192.168.20.0/24, 192.168.30.0/24):
- server option for all scopes PXE option 60 for WDS.

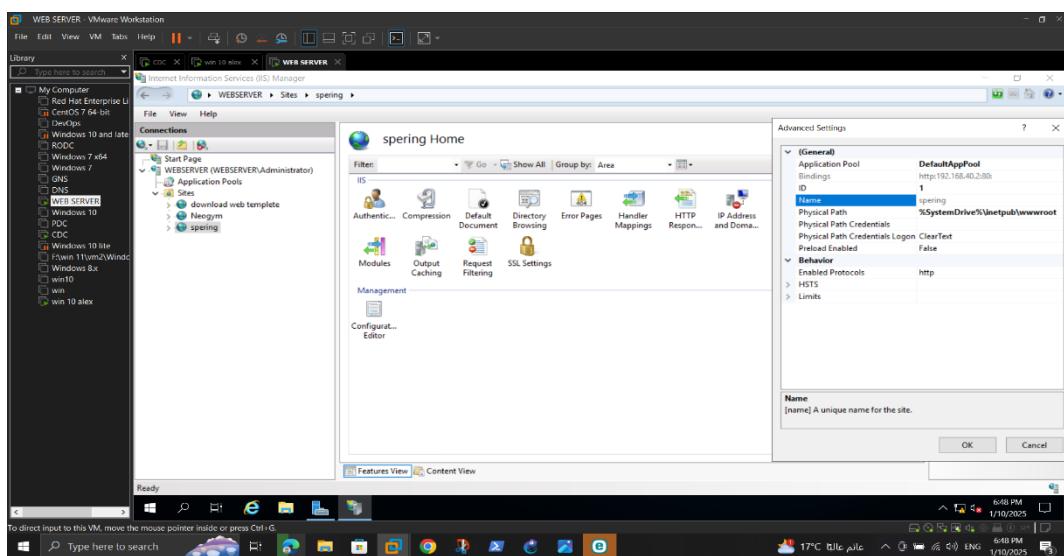


➤ WEB SERVER → IIS (Internet Information Service) role.

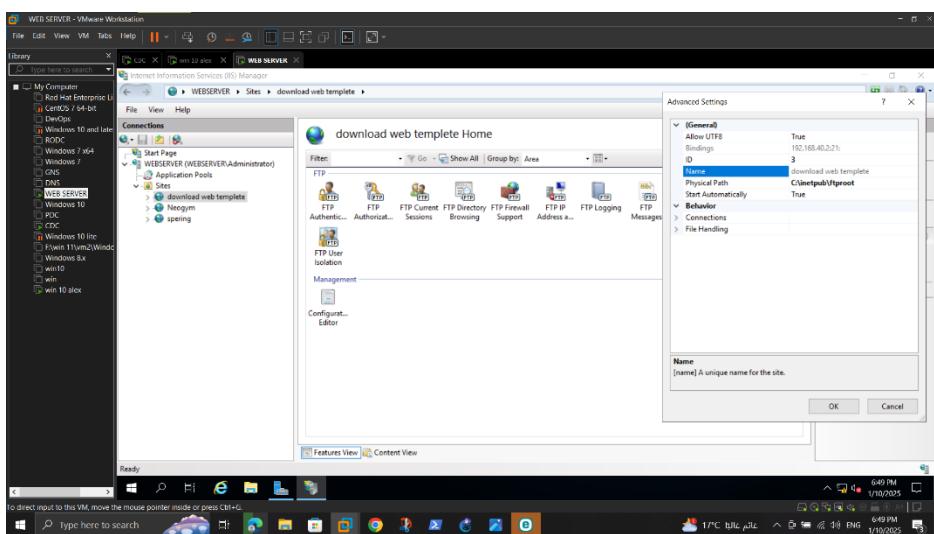
- Web1



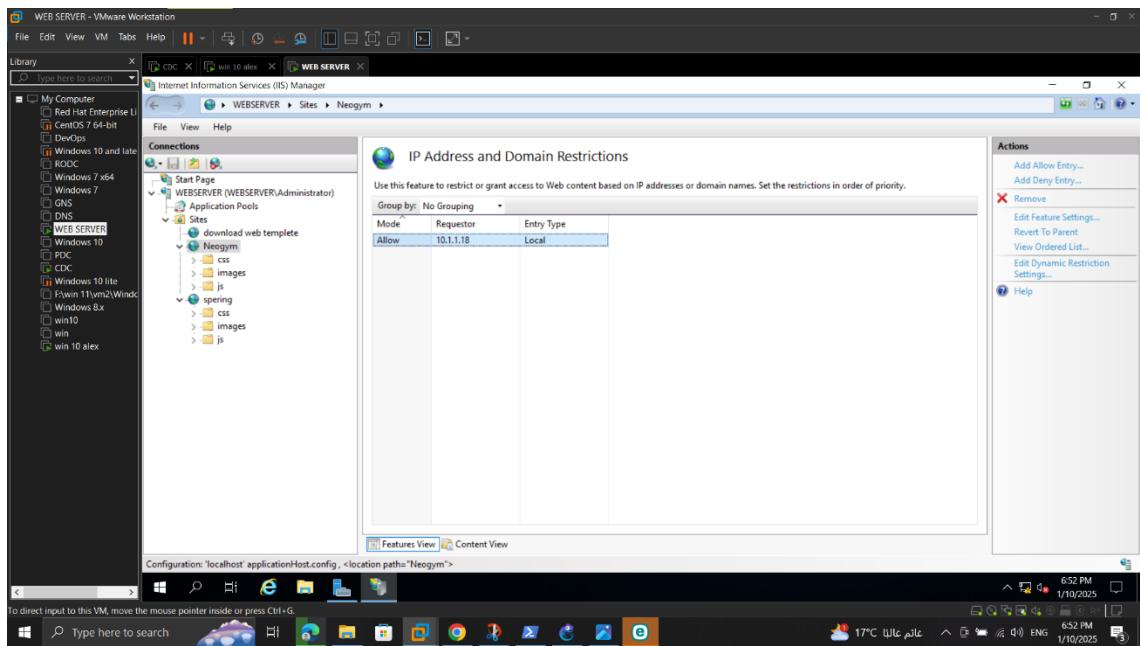
- web2



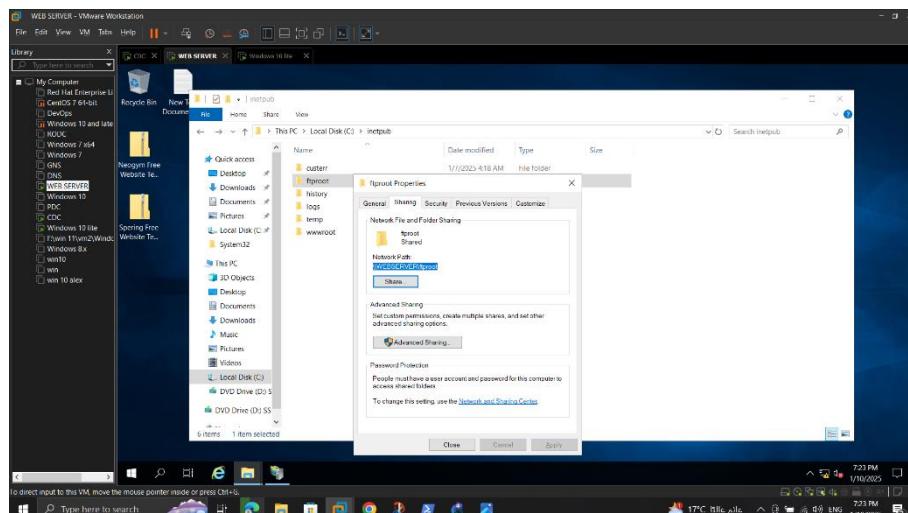
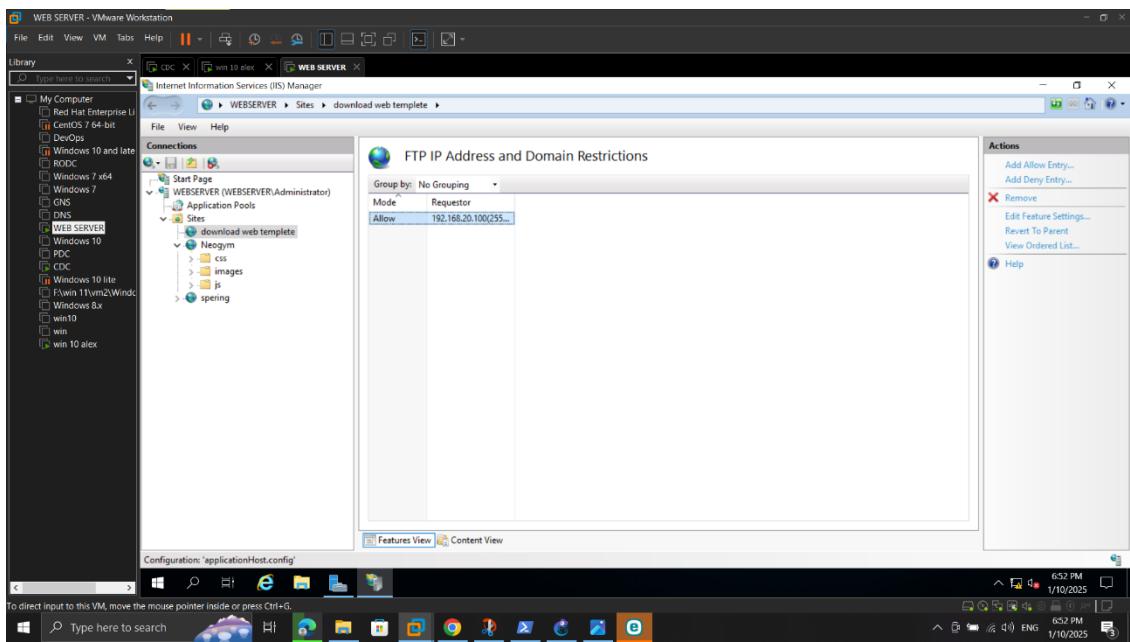
- FTP



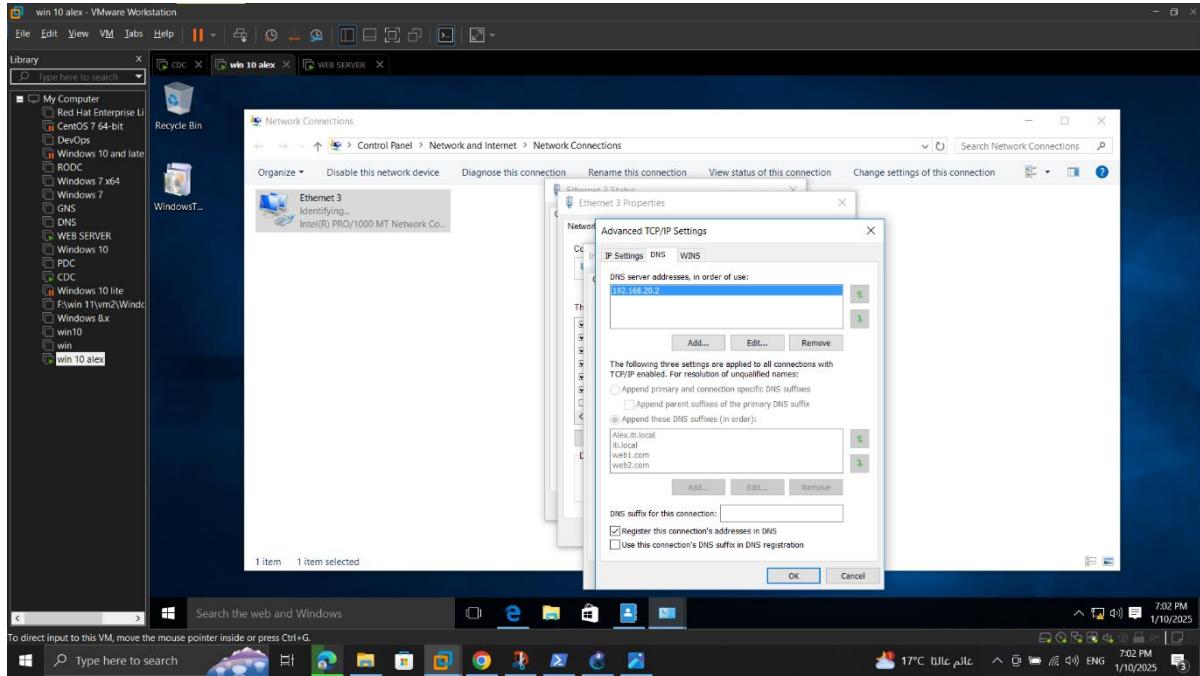
▪ ip and domain restrictions



▪ FTP ip and domain restrictions



➤ Apply suffix policy in pc04



➤ Using OSPF dynamic routing in routers: show ip route in R1

