Table of Contents

Introduction:

Welcome to the comprehensive system documentation report prepared by our team for our client XYZ solutions. In this report we have outlined the analysis, design, implementation, and documentation of a networked system developed to meet the future needs of XYZ Tech solutions, a start-up based in Silicon Valley. XYZ solutions is rapidly expanding its network and workforce in various locations globally. This report is a detailed roadmap of our journey to upgrade the existing IT infrastructure to meet the expanding requirement of XYZ Tech Solutions. We have included a network diagram, a detailed Ip table, necessary server roles, detailed server configuration steps, backup, and disaster recovery documentation. The proposed system is developed through meticulous analysis and strategic planning and will not only meet the technical specifications but also remain accessible to stakeholders within the organization. Every step of the configuration process is included with clear explanation and screenshots, for ease of use and troubleshooting.

Network Diagram:

Given network diagram shows how the framework for XYZ Tech Solutions is designed. We have included how the internet connection, router/firewall, servers (web, backup, DHCP, AD, roaming profiles, RDS, NPAS, and group policy) are interconnected and how they relate to one another within the network. Each component is essential to the smooth performance of the organization's IT infrastructure, supporting user administration, data storage, access control, and communication.

XYZ Tech Solution Network Diagram

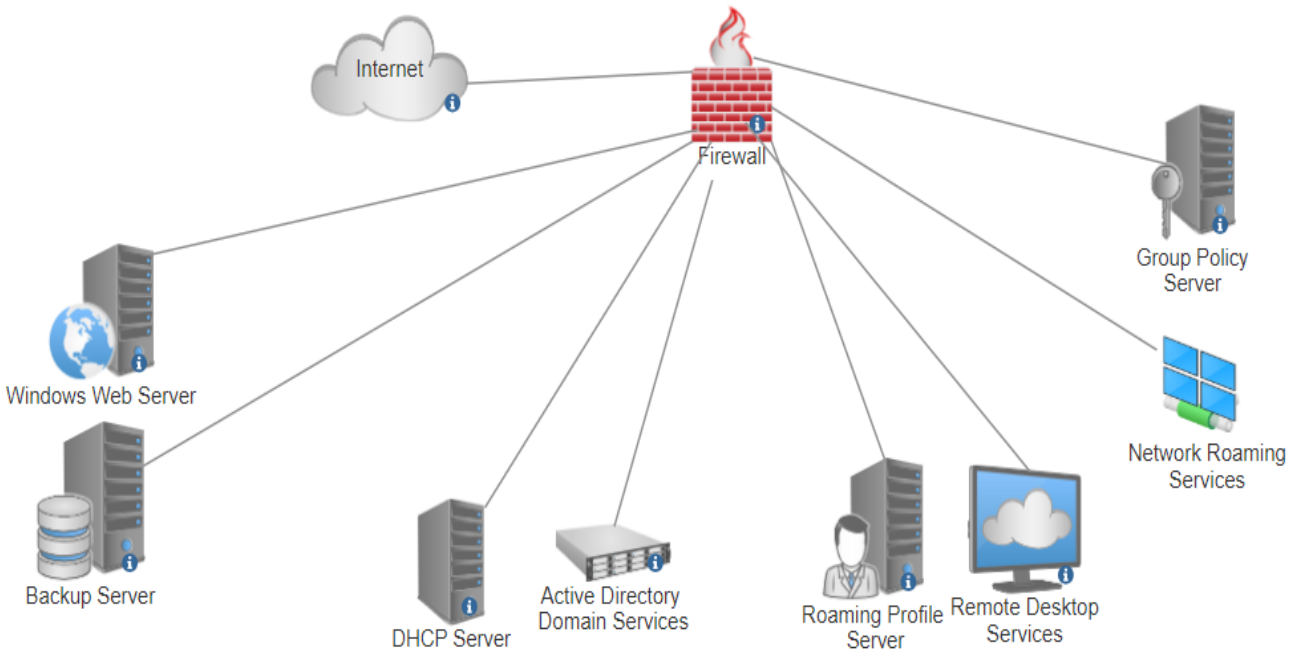

Fig.0

Requirement Analysis and identification of server roles & technologies with IP address Assignment table:

As per the scenario provided by XYZ Tech solutions, we have examined clients' requirements and distinguished the necessary server roles and technologies to implement the networked system.

Windows Web Server:

The firm's website is hosted by the Windows Web Server (IIS) in its primary role. This server supports the use of HTML, CSS, JavaScript, and PHP as they are used in the development of this website. [1] The web server is responsible for making sure that partners, customers, and staff can access the company's online presence. The server also needs to be set up to manage sudden rise traffic and provide a steady uptime.

For hosting any sort of content on the Internet, Internet Information Services (IIS) is an adaptive, secure, and control-based Web server. Web apps and video streaming are among the tasks that IIS's open and expandable design can handle with ease.

Backup Server:

Backup Server's role is crucial to maintain the data integrity and availability. It is responsible for backup data regularly from the web server and many other important servers in case of device failures, cybersecurity threats and attacks or other anomalies. This server should have a high storage capacity,

continuous flow of power supply, reliable and capable features to handle any backup needs of the company [2].

The backup server has a file and storage services role. It allows this server to store, manage, share, and provide backup access of all the data and configurations.

DHCP server:

DHCP stands for Dynamic Host IP Configuration Protocol. The DHCP server automatically assigns Ip addresses to devices in the network. It simplifies management of network by allowing devices to connect without manually assigning the Ip addresses. [3] To maintain consistent network settings, this server is set up to provide workstations and laptops dynamic IP addresses while assigning fixed IP addresses to other servers based on their MAC addresses.

Dynamic Host setup Protocol, or DHCP, server roles provide a consistent method of automatically assigning IP addresses and other network configuration settings to devices.

Active Directory Domain Services (AD DS):

To maintain users, groups, and resources on a network AD DS are required. It provides authorization and authentication facilities as well as centralized domain management. This server is important for upholding security regulations, streamlining administrative processes, and ensuring that users have appropriate access to resources based on their roles [4].

Active Directory Domain Services: With this role, the server manages the directory and responds to requests for authorization and authentication, operating as a domain controller.

Roaming Profiles:

Roaming profiles guarantees that user proclivity and information transfer between them with networked workstations. This gives users a consistent desktop environment across all devices, which enhances productivity and user experience. [5] To secure user privacy and data integrity, this service should be dependable and secure.

File Services and User Profiles: This role makes it practicable to manage user profiles, ensuring that they are kept in one location and accessible from any networked workstation.

Remote Desktop Services:

Users can remotely access their desktops and programs via RDS. This is especially essential to provide connections to employees who work remotely and part-time contractors. It is of vital importance that RDS be set up to offer higher level performance, dependable, and secure remote access so that users may operate actively, securely, and effectively from any location.

Remote Desktop Services: This function allows the server to run desktops and apps that users can access remotely.

Network Policy and Access Services (NPAS):

Network access control and authentication services are offered by NPAS. By establishing rules and regulations for network access and monitoring compliance to the organization's security protocols, it ensures that only legitimate devices and users may access the network, enhancing security [6].

Network Policy and Access Services - This role provides the tools needed to generate and impose network access policies for client health, authentication, and authorization.

Group Policy:

In an Active Directory context, Group Policy is used to direct and arrange user settings, applications, and operating systems. Imposing security policies, such password policies, is essential for XYZ Tech Solutions to ensure compliance with security standards and practices [7].

Group Policy Management: With group policies, it is possible to control user and computer settings centrally.

IP Address Assignment Table:

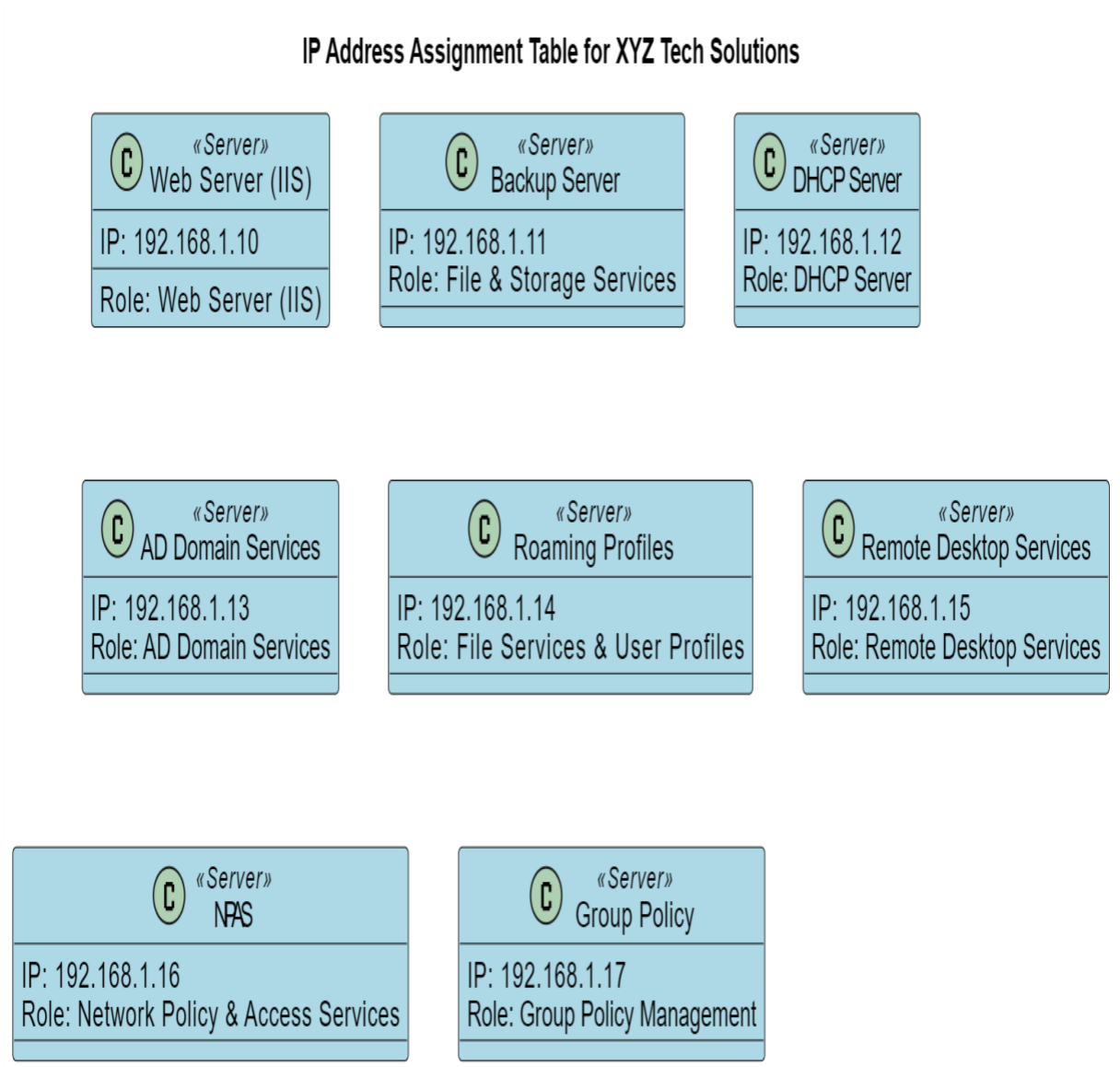

Fig.1

Configuration Process Description:

We have used windows server 2016 as our server management software. Below are the configuration steps with attached screenshots as a guideline to assemble the servers in the future and make it easier to troubleshoot.

Windows Web Server (IIS):

i. Open the server manager window.

ii. Click on add roles and features.

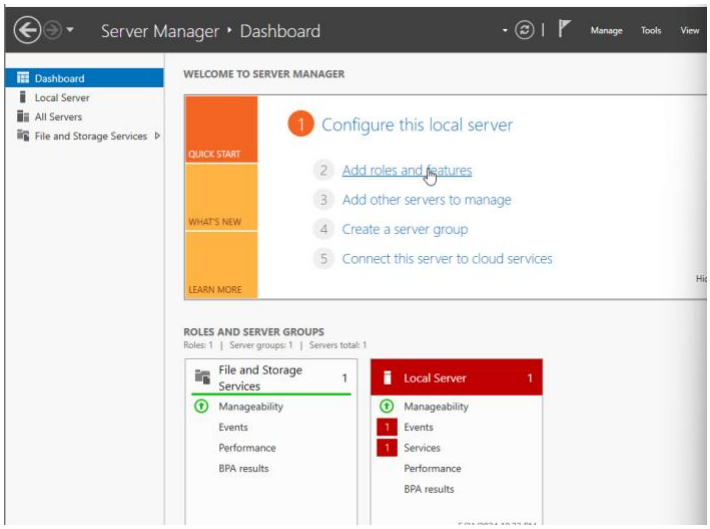

Fig.2

iii. Click on next, choose the first option and then click next again.

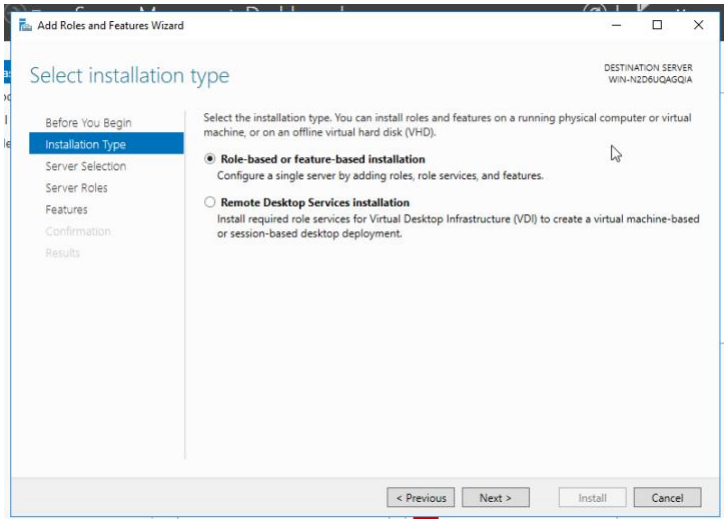

Fig.3

iv. Click next again. On server roles choose Web Server (IIS) and then click on next.

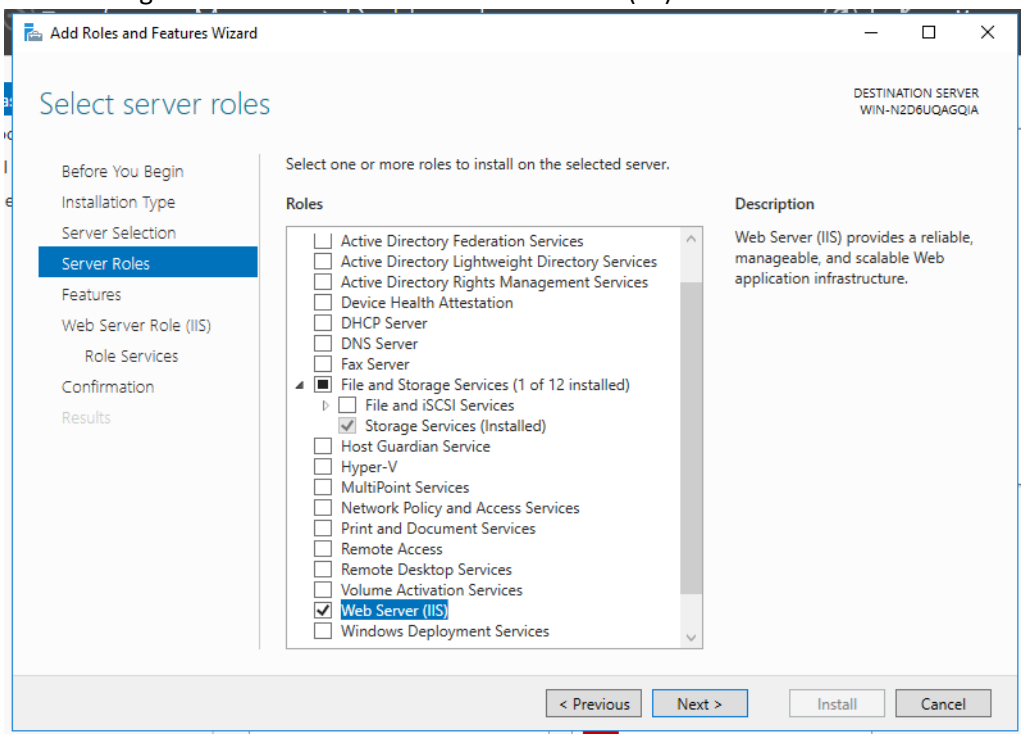

Fig.4

v. Keep all the default settings and click on next until the installation tab appears and then click on install.

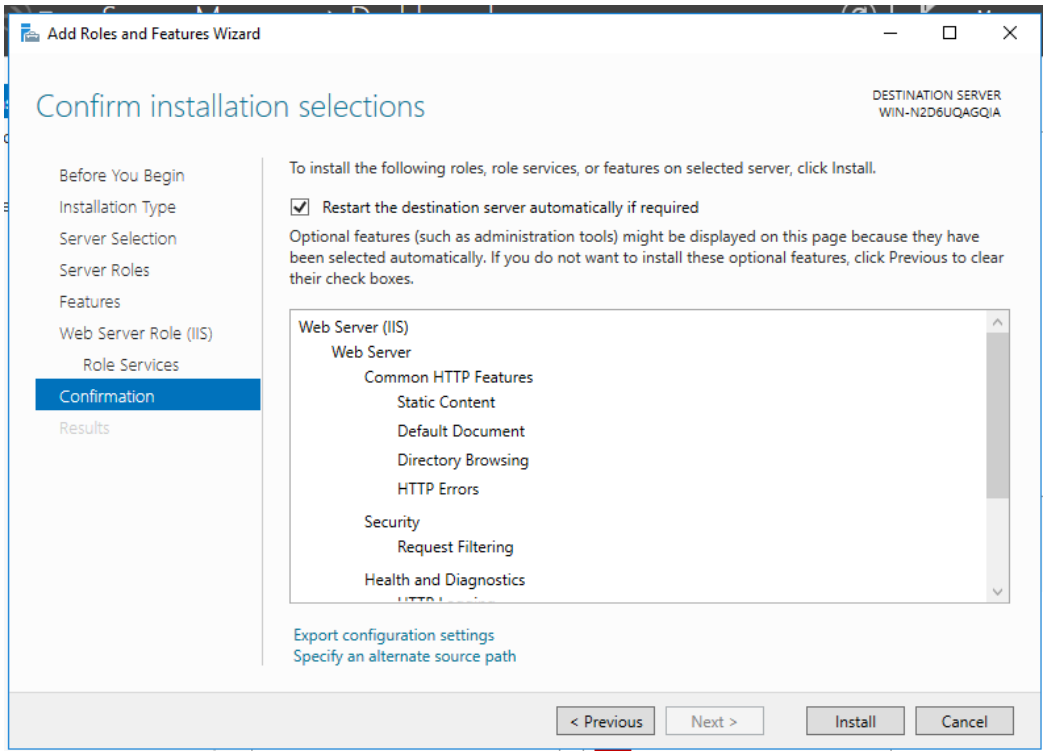

Fig.5

vi. Finally, the server is installed. Now go to the windows tab on taskbar, select administrative tools.

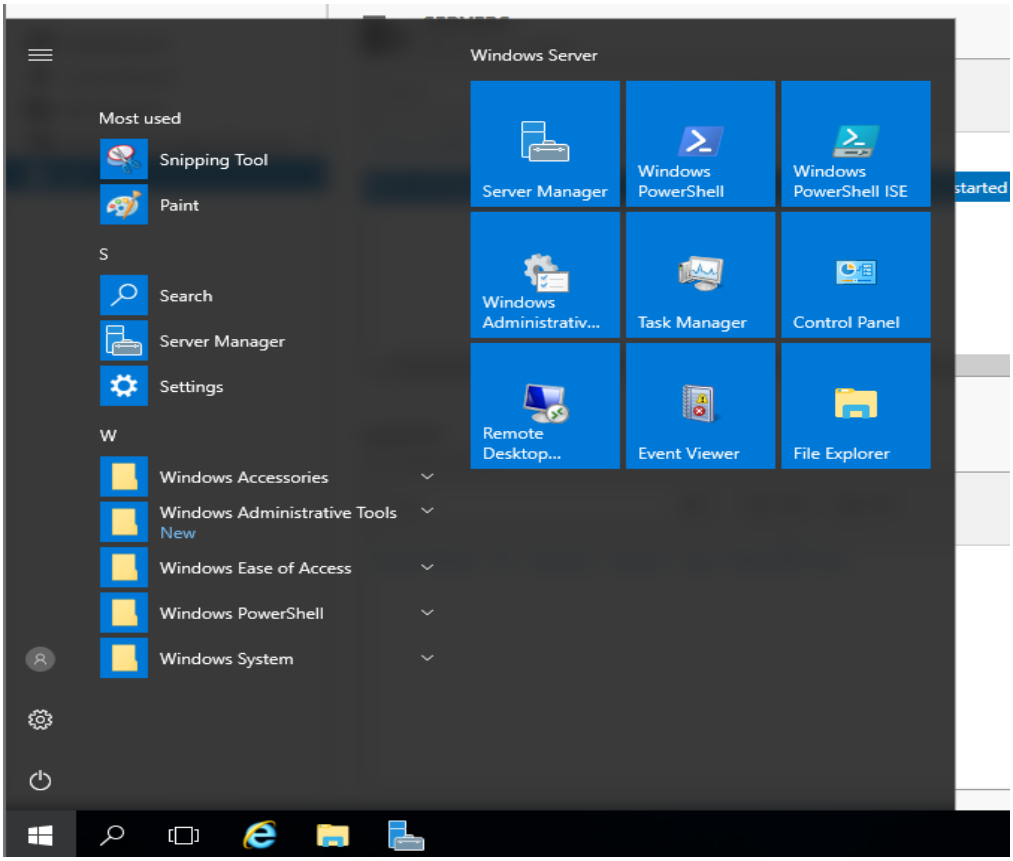

Fig.6

vii. Left click on Internet Information Services (IIS) Manager.

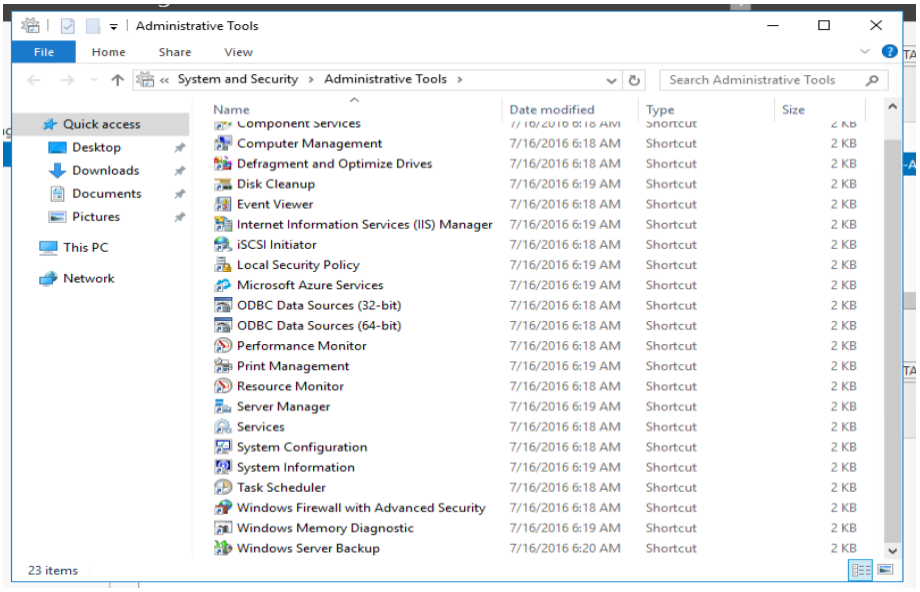

Fig.7

viii. The internet Information Services Manager window will appear which can help you to host and manage your websites.

Windows backup server

i. Open server manager and go to add roles and features click next until the features tab appears. Select Windows Server Backup.

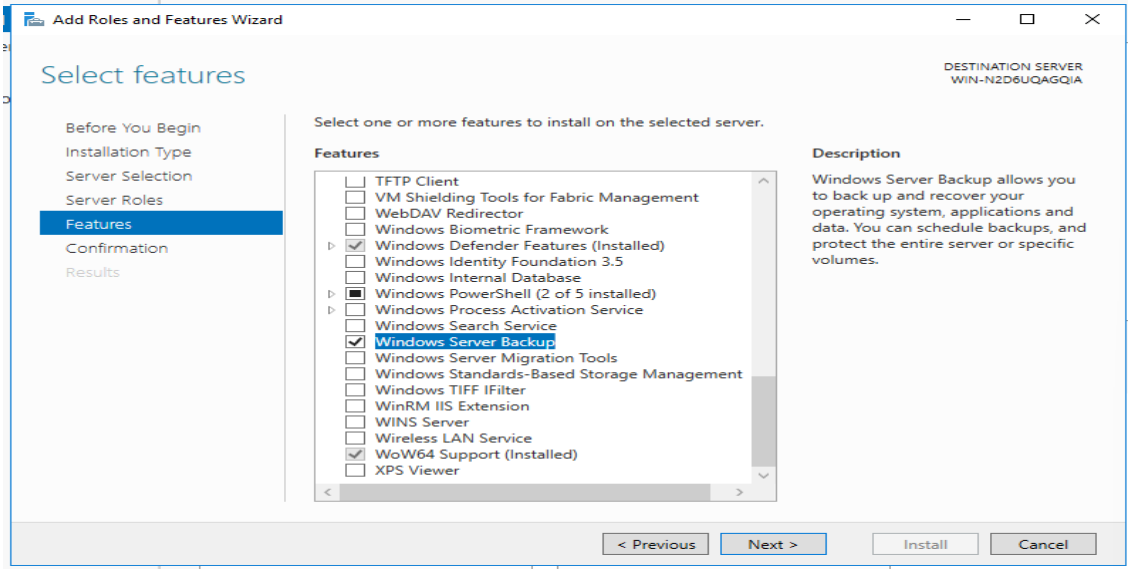

Fig.8

ii. Click on next and then click on install.

iii. Finally when the installation is complete close the windows.

iv. Click on tools>Windows Server Backup.

v. Click on Local Backup. On the right-hand side, you can see the options to backup and recover. Using this option, you can either backup or recover on the server as per your needs.

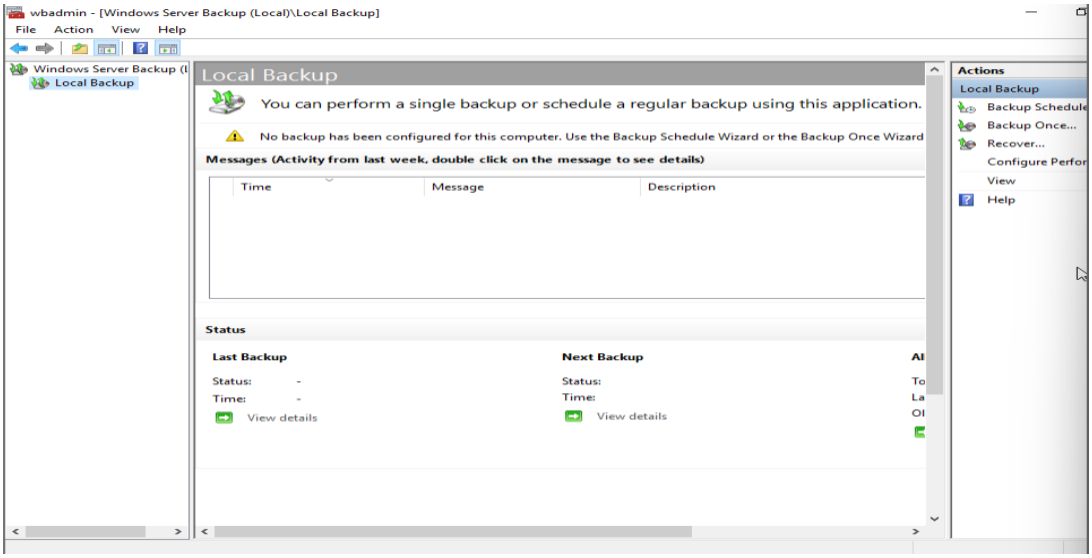

Fig.9

DHCP server

i) Open server manager, click add roles and features click on next until the server roles tab appears. Here, select the windows DHCP server.

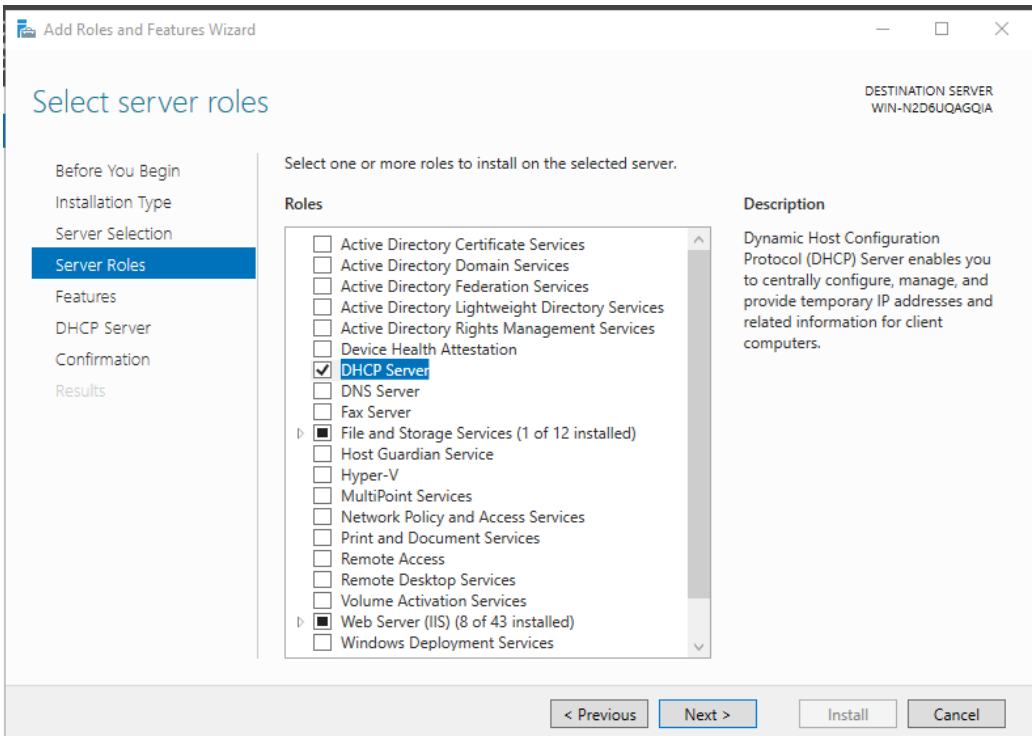

Fig.10

ii) Click next and then press install. And close the window.

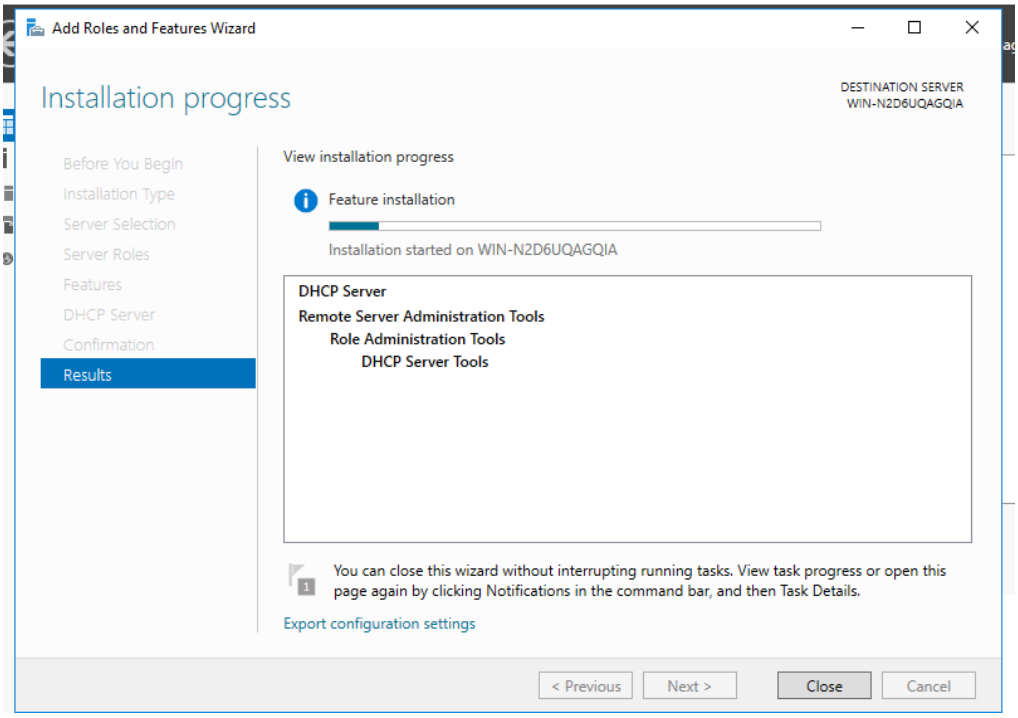

Fig.11

iii) Open the server manager, tools and click DHCP.

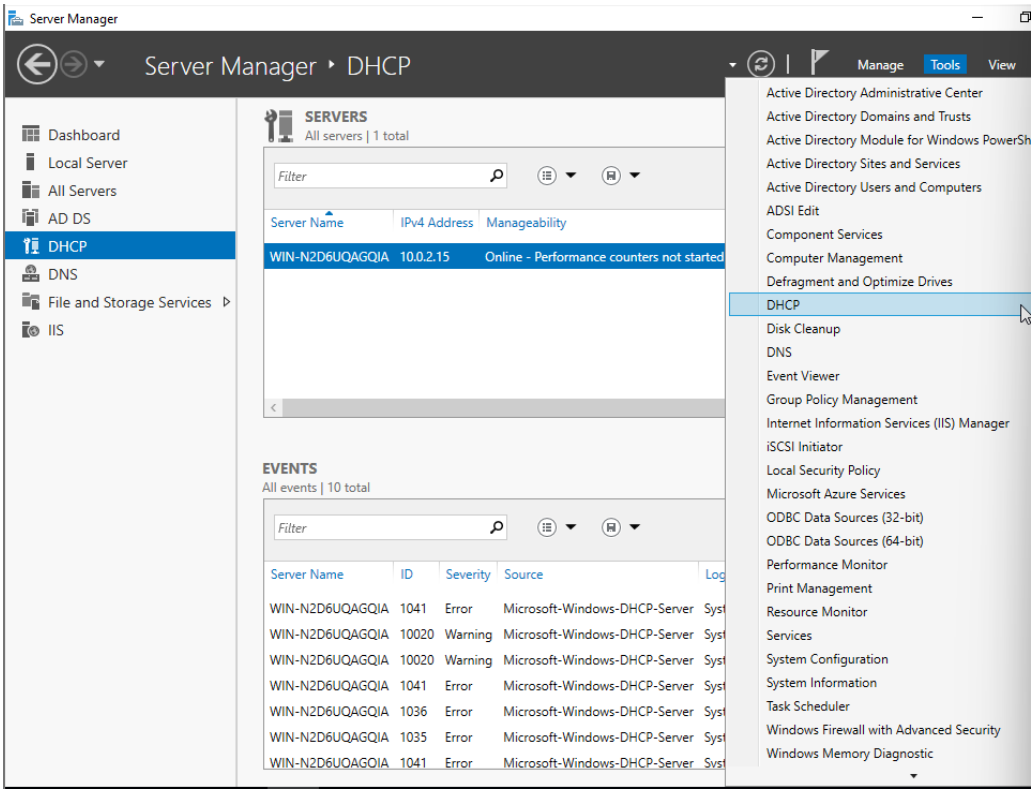

Fig.12

iv) Expand the win and then IPv4. On the right-hand side IPv4, More actions, New Scope.

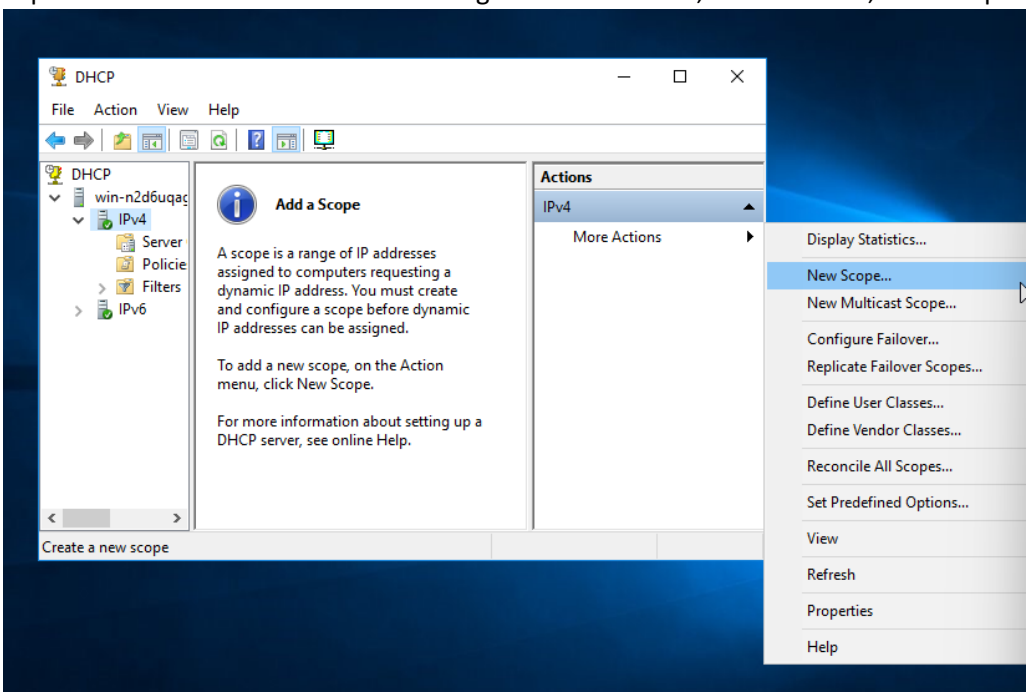

Fig.13

v) The new scope wizard opens. Give the scope name and description as you feel appropriate. Click next.

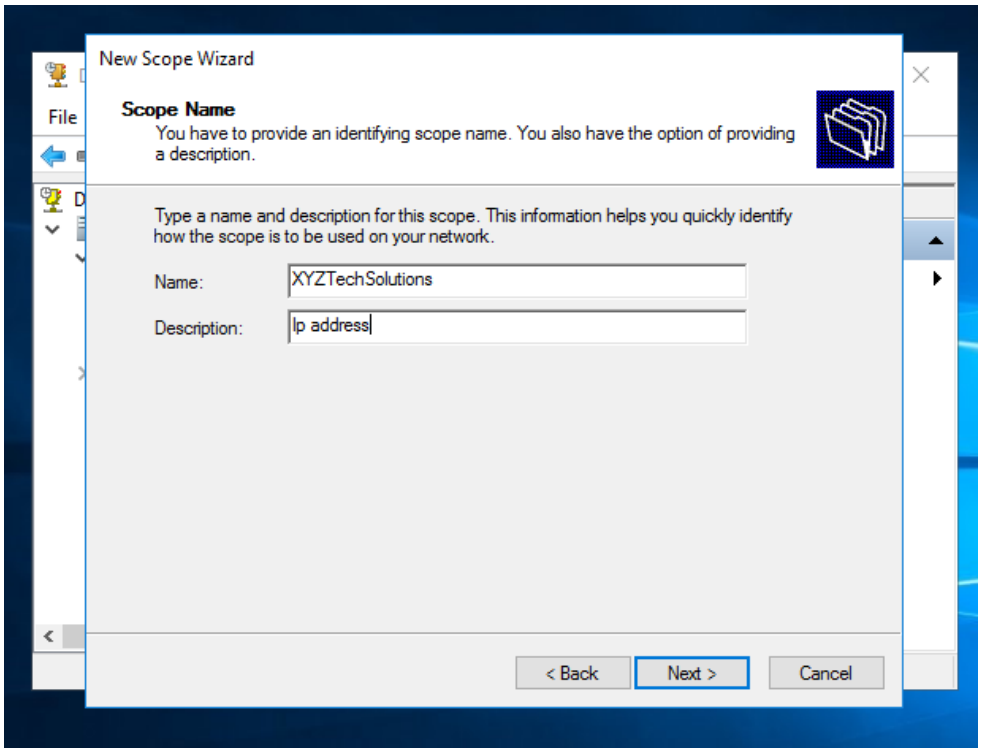

Fig.14

vi) Choose the Ip address range you want to use and enter the subnet mask. Click next.

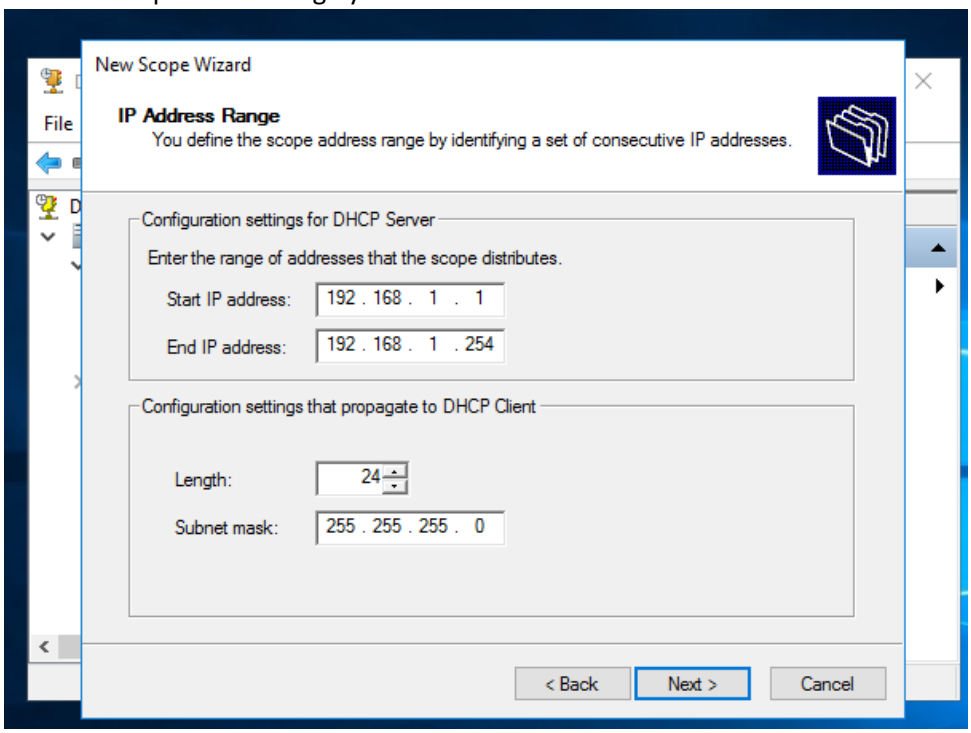

Fig.15

vii) Set the time you want the Ip to be assigned to the computers after this time a new Ip will be assigned. Click next, select yes.

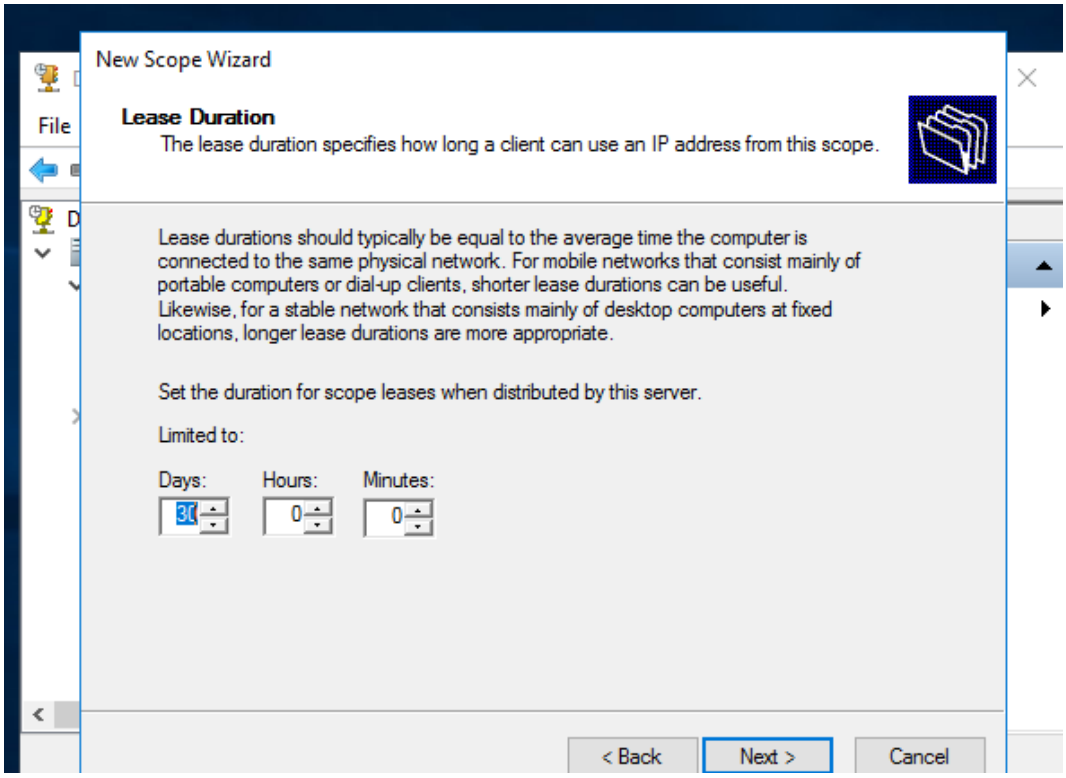

Fig.16

viii) Keep selecting next, and at last close the windows.

ix) Now, expand, DHCP, win, IPv4, Scope, Reservations, More actions, and new reservation.

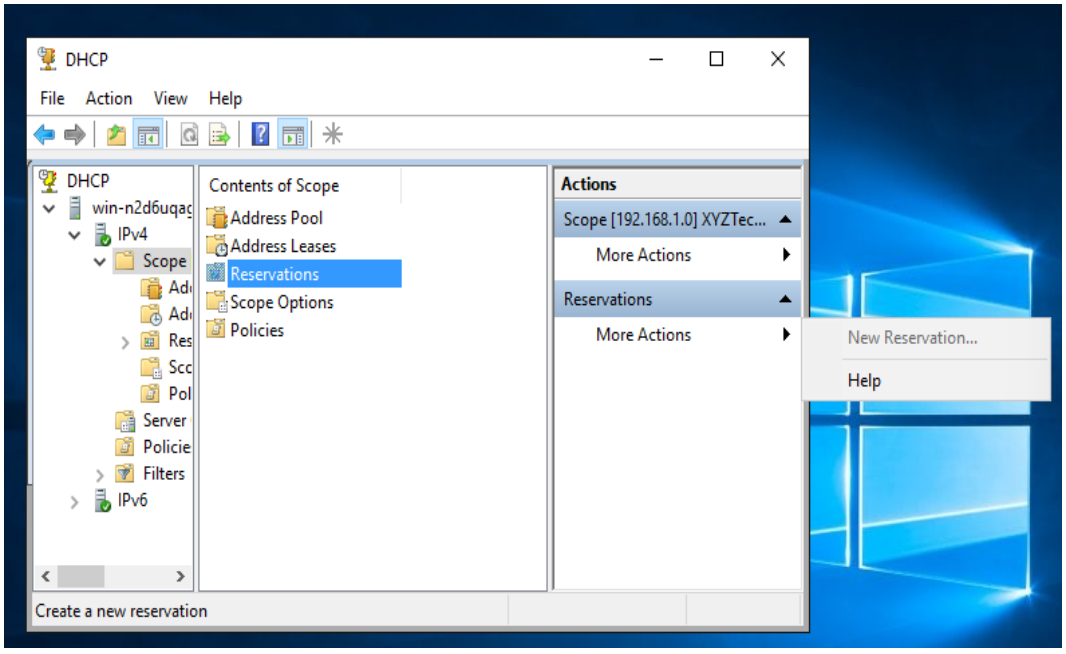

Fig.17

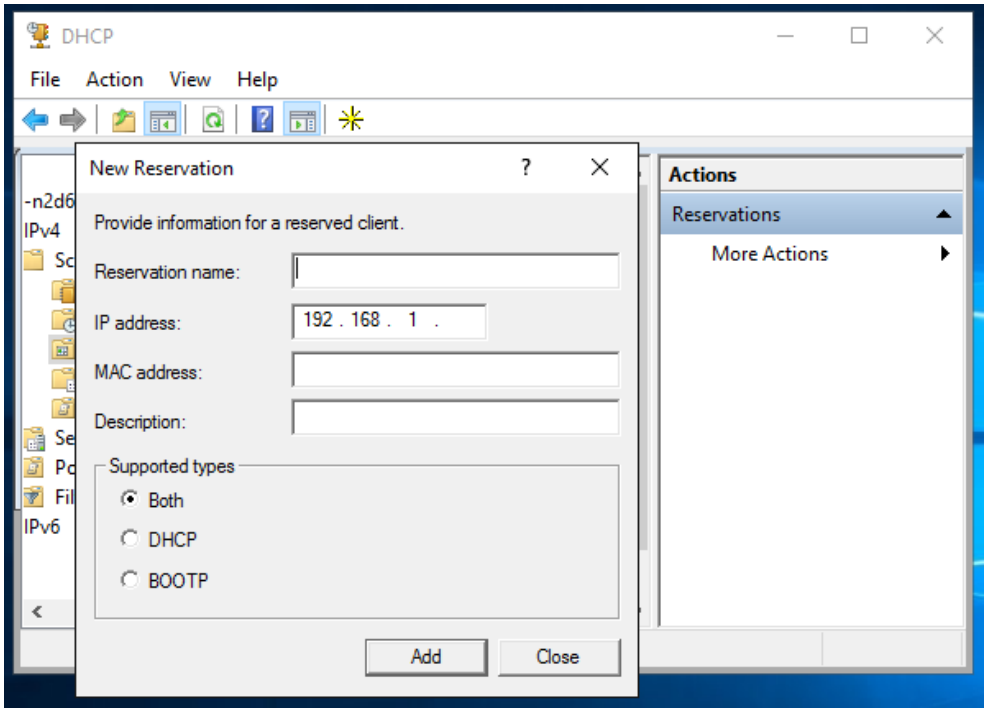

Fig.18

x)At the name tab write the server's name and at the Ip address write the reserved Ip and server's MAC address. Repeat the action until all the Ip addresses for the servers are included. Finally, your DHCP configuration is done.

AD DS

i) Follow the same steps as before and on server roles choose the AD DS. Click on add features, click next and then install.

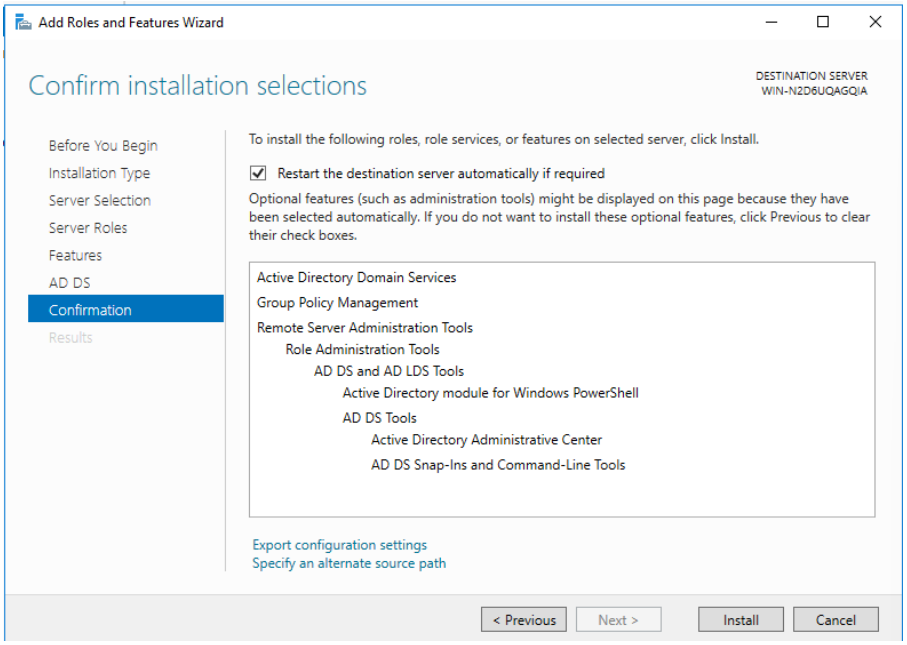

Fig.19

ii) Click the flag icon and click on promote AD DS to domain controller.

iii) The configuration wizard will then appear, select add a new forest and write, XYZtechSolutions.com.

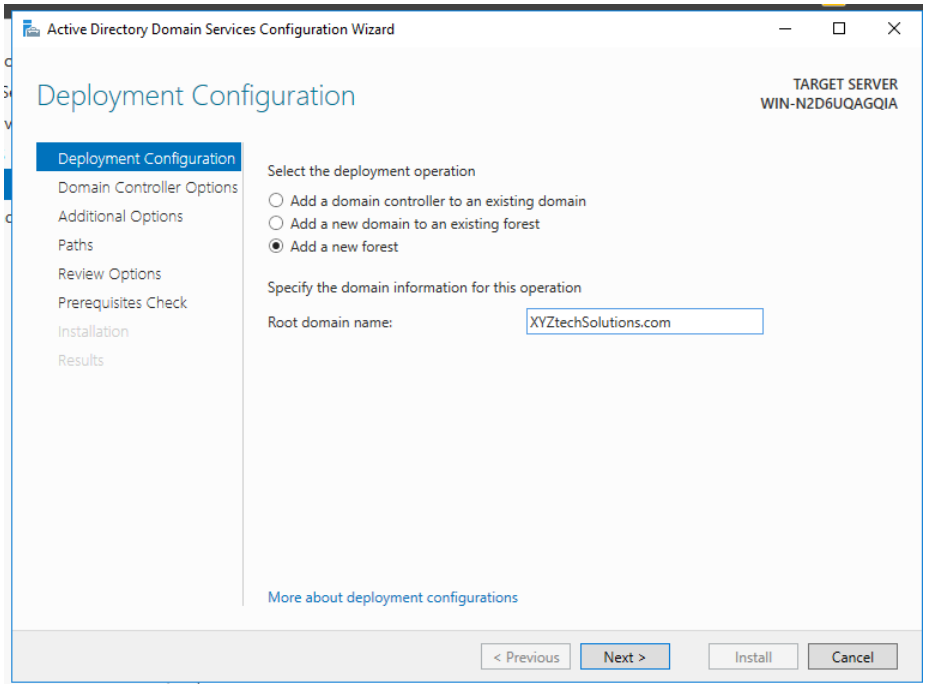

Fig.20

iv) Click next and then choose a password, such as “XYZTechSolution123”. Click next until the installation button appears and then click install.

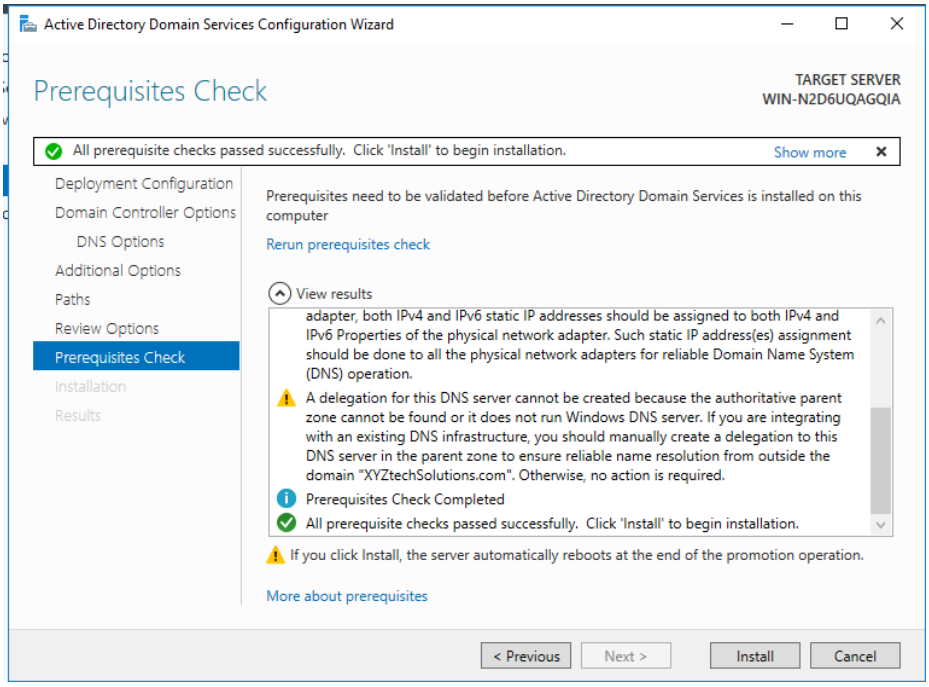

Fig.21

After the installation is complete wait for the computer to reboot and your ad ds setup for XYZTechSolutions is complete.

Roaming profile for users

i) Open network manager. Go to tools and right click AD users and computers.

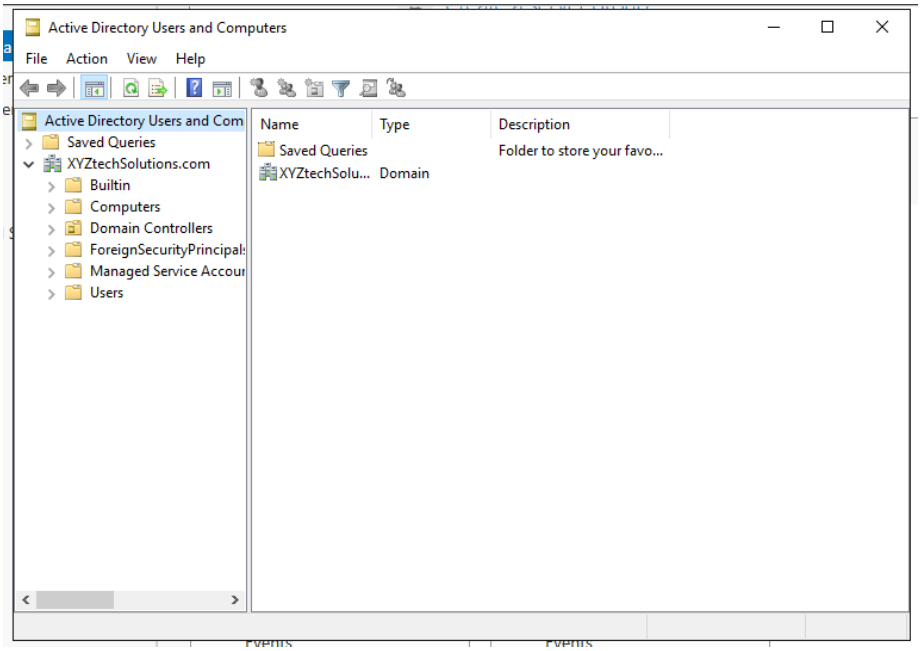

Fig.22

ii) Right click on XYZTechSolutions, then select new. From here you can add organizational units and users. Select OU and give a name 'Admin' and create another OU and give a name "user".

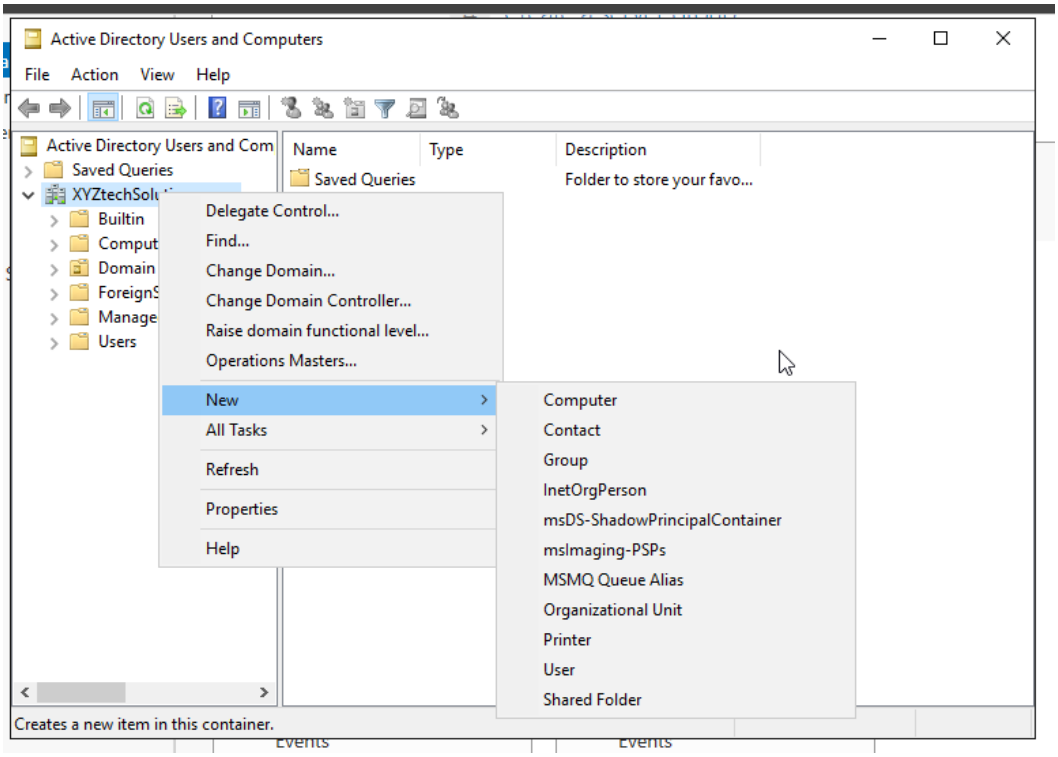

Fig.23

iii) Right click on admin, then new, then user.

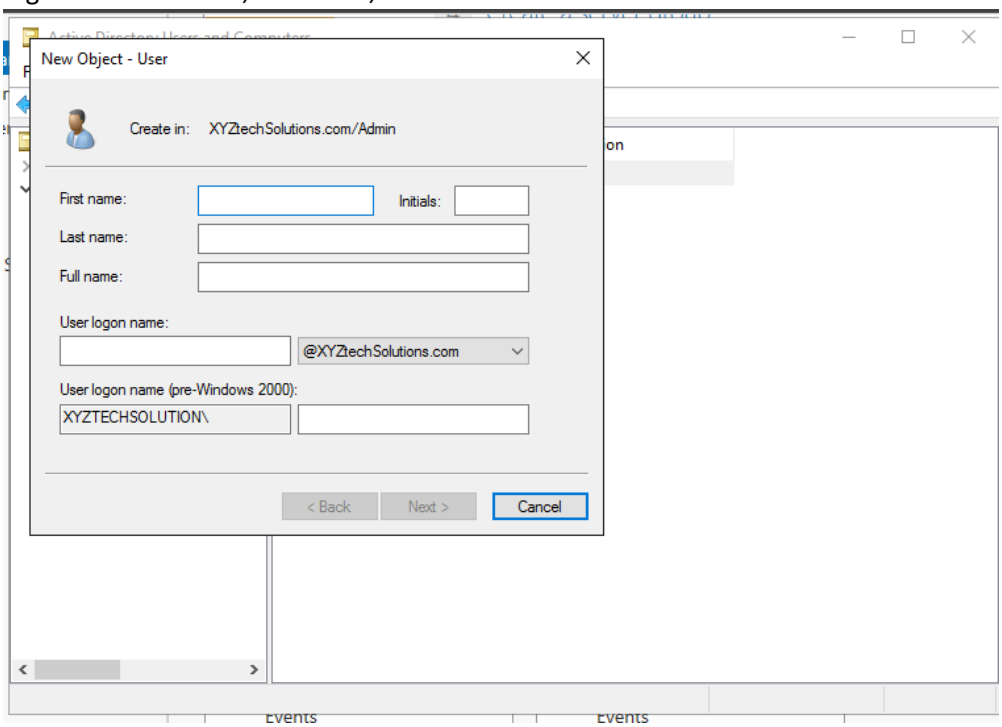

Fig.24

iv) Fill in the user credentials and press next. Provide a suitable password and select the first option. Click on next and then finish.

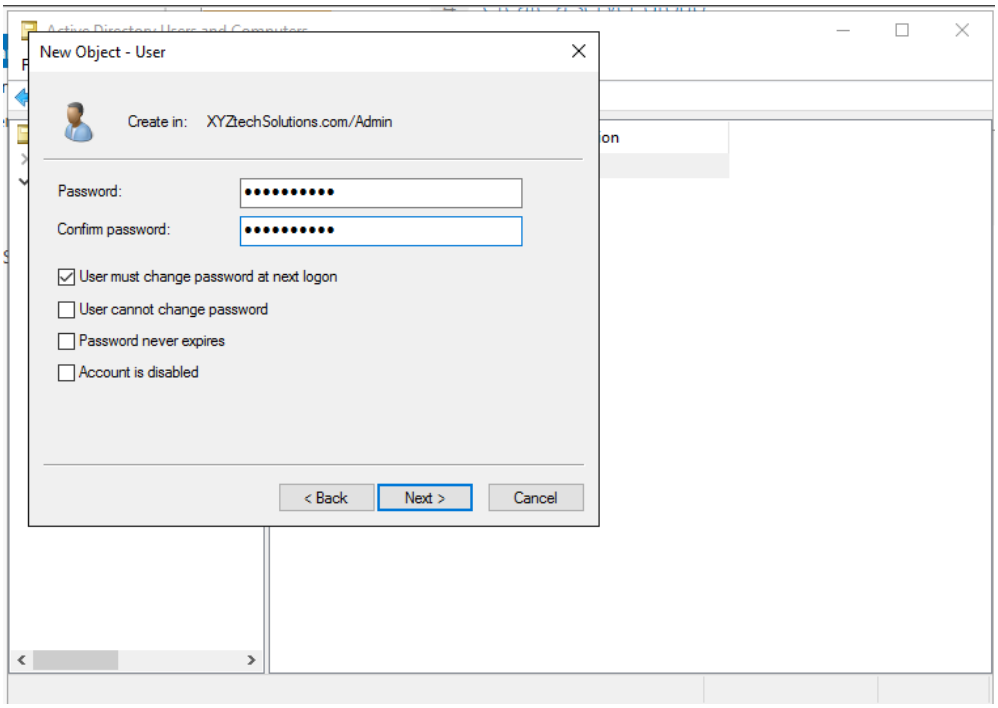

Fig.25

v) By following the same steps create a new group called group1. Then right click on user1, select add to group and write group1 on the search tab. And click ok.

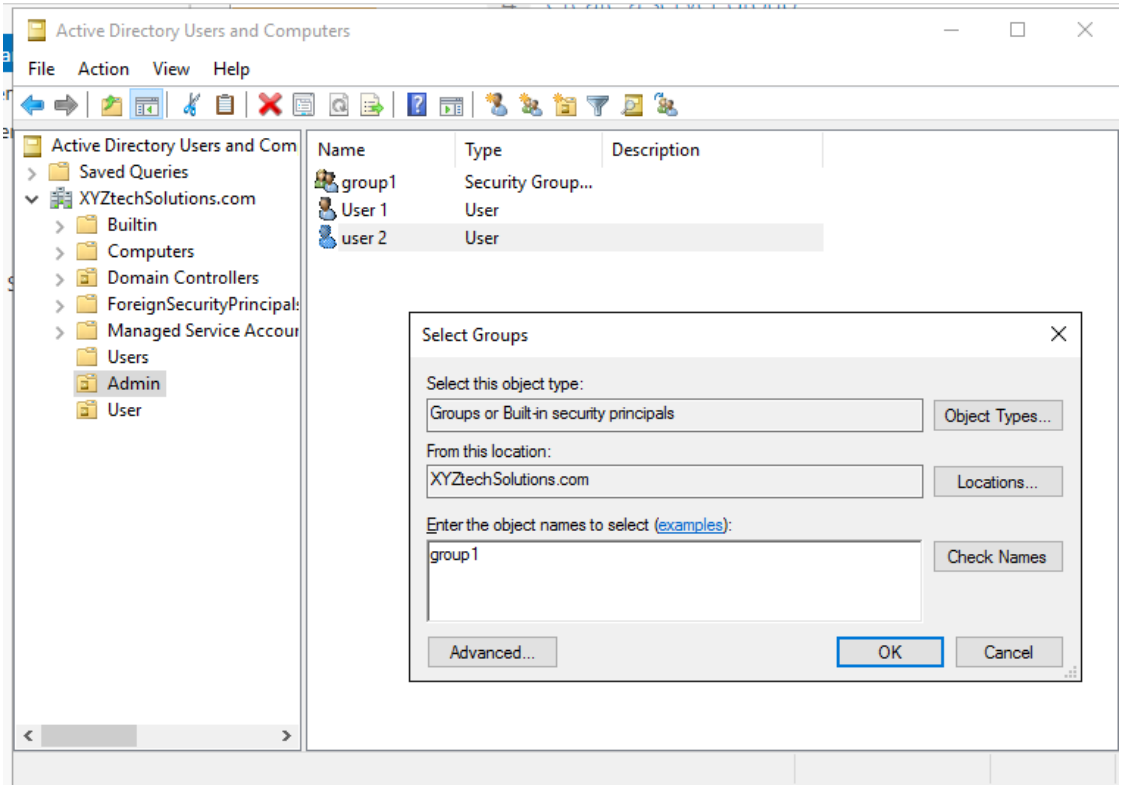

Fig.26

vi) Now navigate to ThisPC from windows tab in taskbar. Goto Local Disk C, create a new folder name profile.

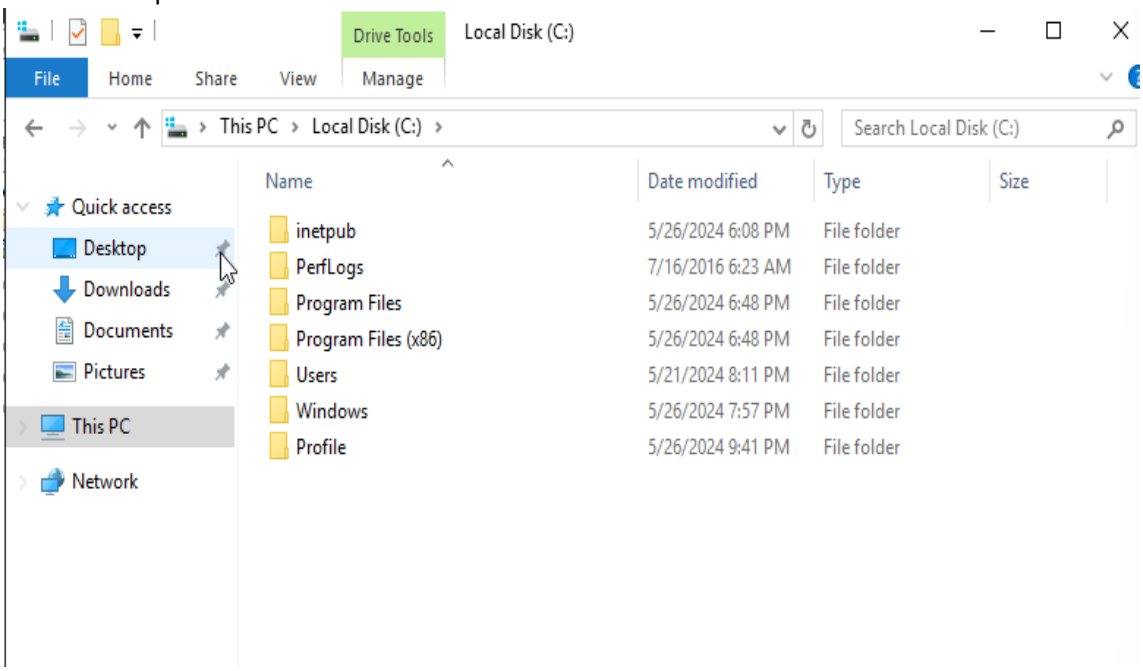

Fig.27

vii) Right click on the profile folder, navigate to properties, sharing and click on advanced sharing. Select, share this folder.

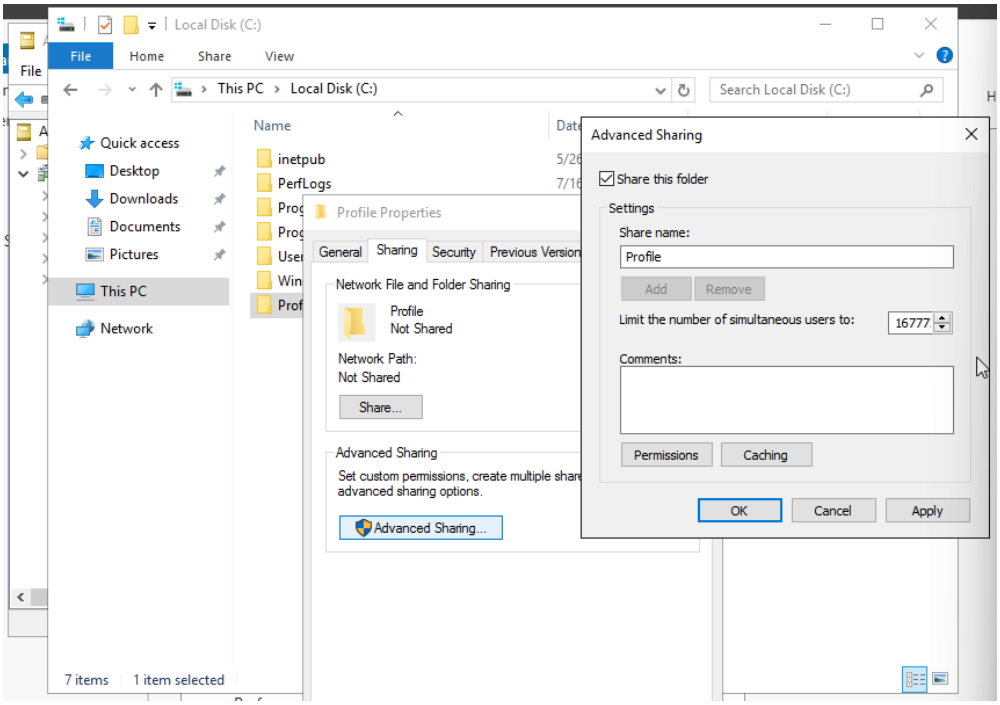

Fig.28

viii) Left click on permissions. A new window will open then select full control and click apply and then okay.

ix) Then navigate to security, click on edit and then remove Users as the full control permission is for admins only.

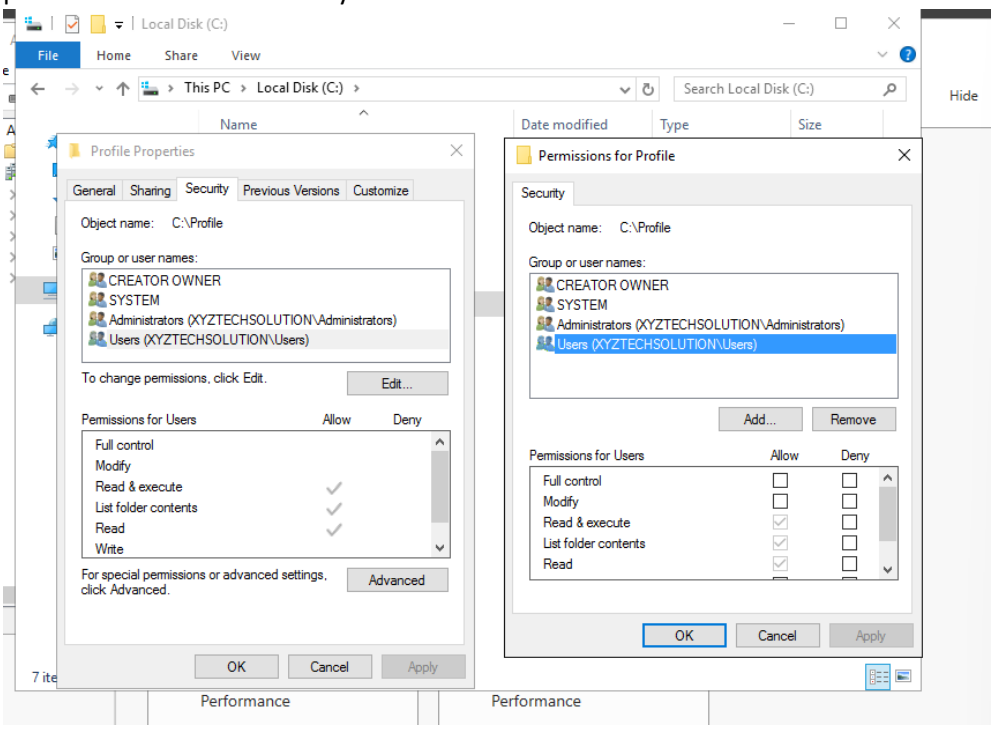

Fig.29

x) Add group1 that we created in the admin OU for the allowance of folder sharing.

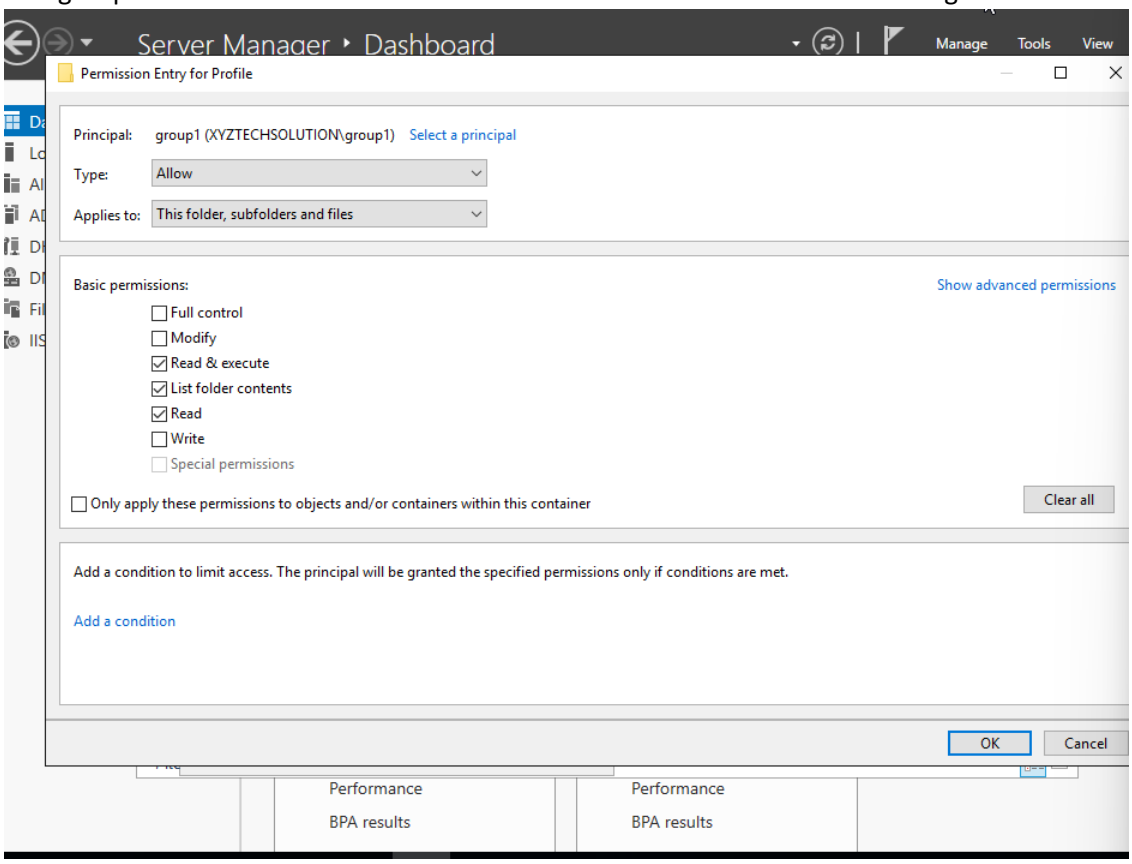

Fig.30

xi) Finally click apply and select okay and your profile roaming, and remote desktop services are ready for the admin group. By this way you can create a particular group add permissions and enable the required services.

Remote Desktop Services

i) To setup remote desktop services, we need to install remote desktop services first. Open network manager, go to add roles and features, select remote desktop services installation on Installation type and click next.

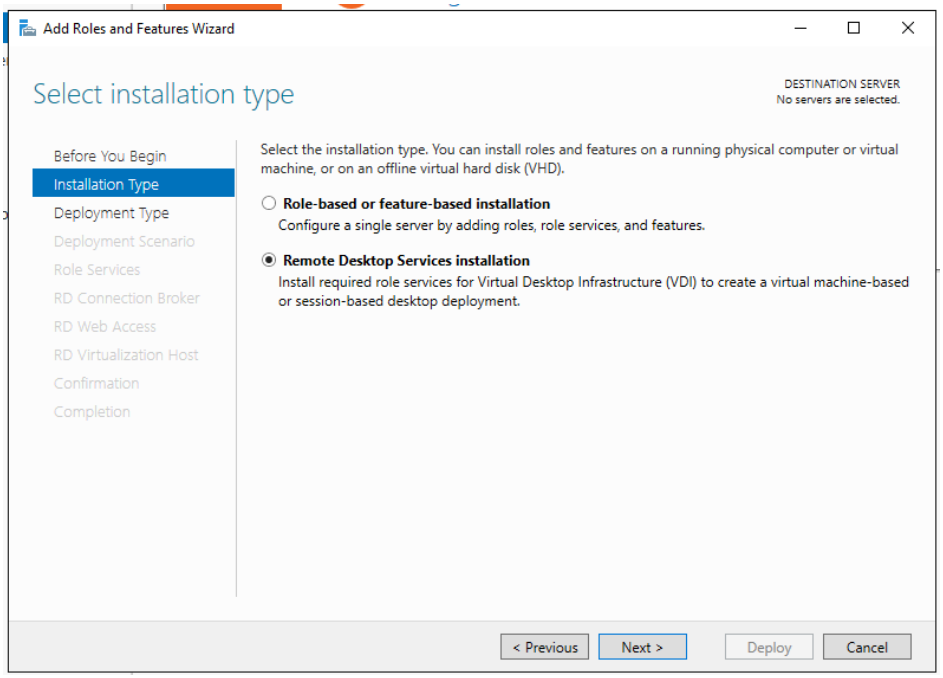

Fig.31

ii) Keep selecting next and select session-based deployment.

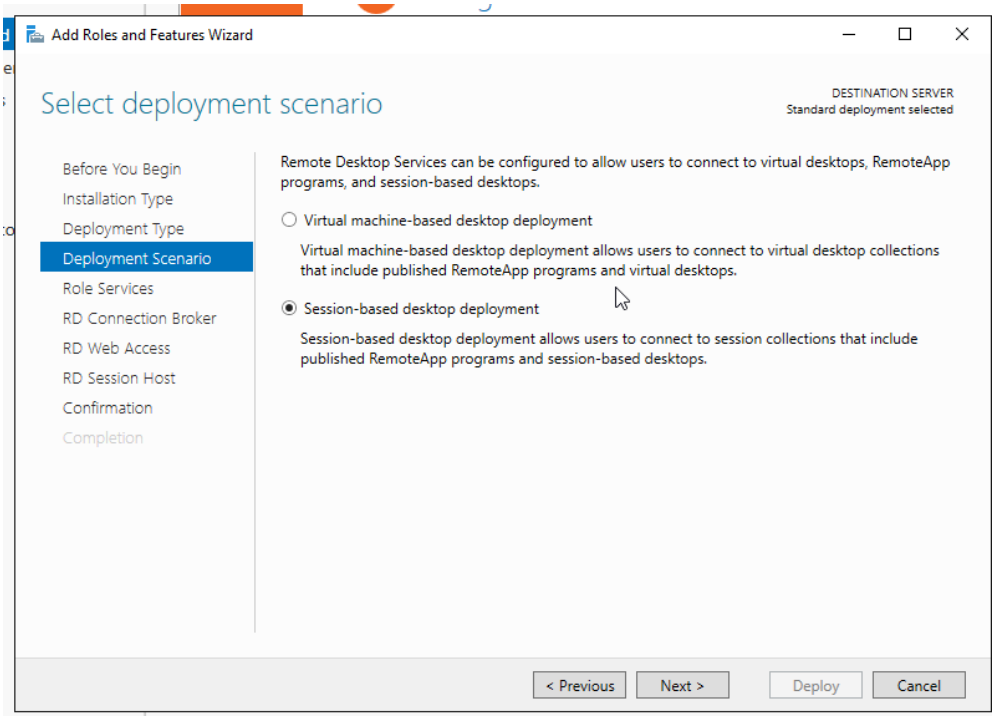

Fig.32

iii) Keep selecting next until the below screen appears and click on deploy. It might take a few minutes for the server to install.

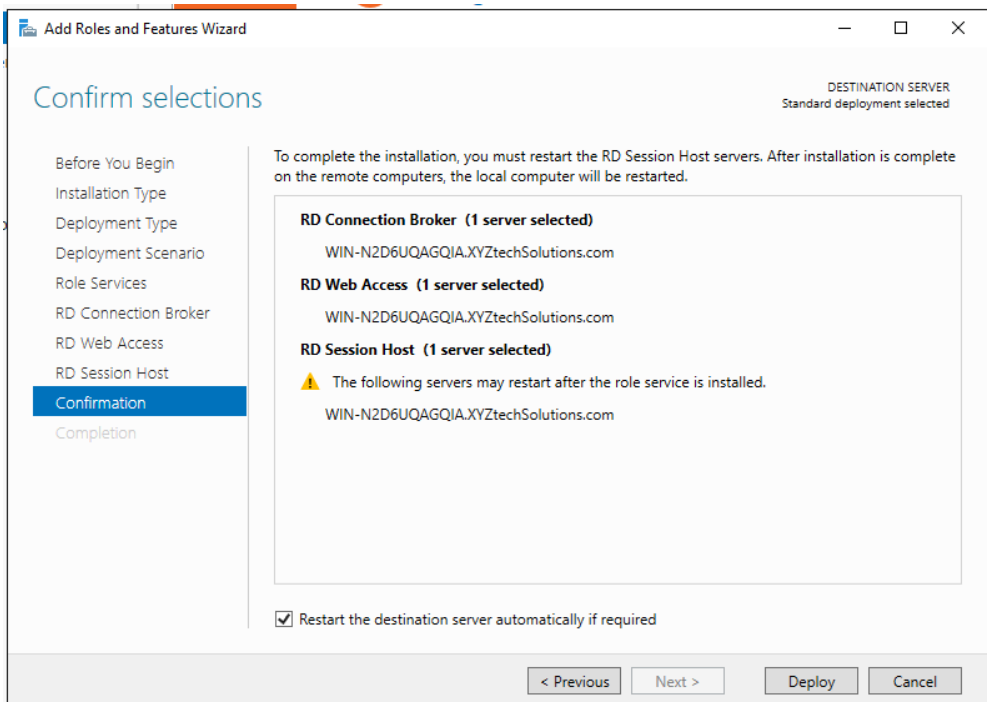

Fig.33

iv) After the installation Is complete the computer will restart. Open network manager, go to remote desktop services.

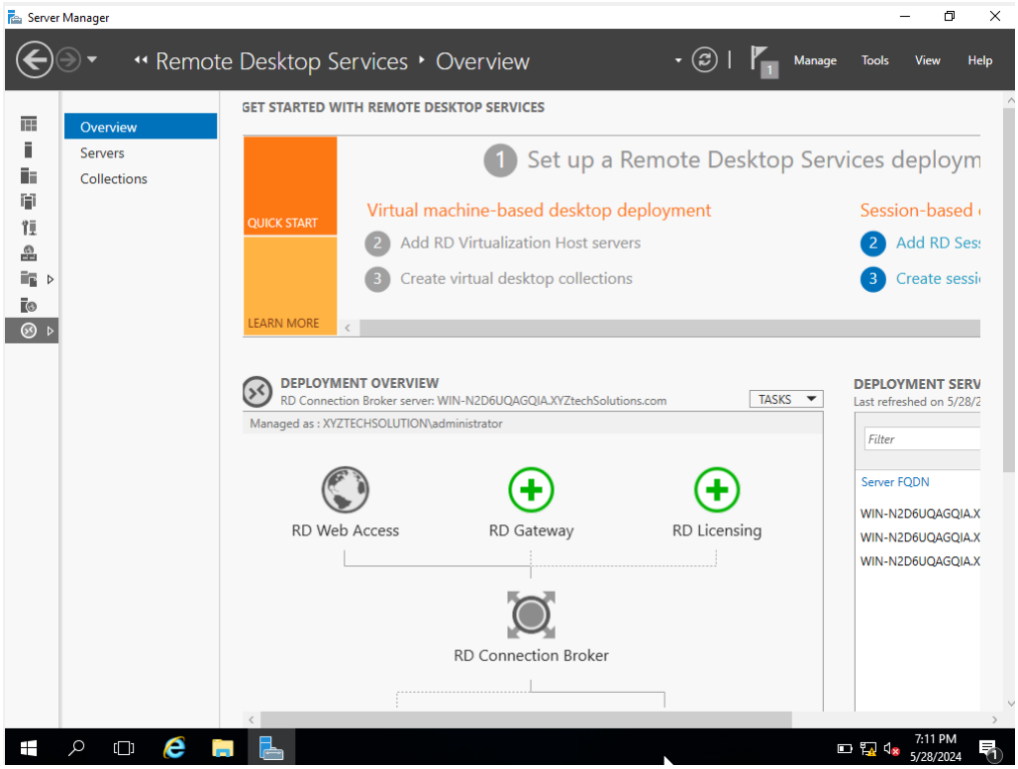

Fig.34

v) Then navigate to collection – tasks- create session collection. Give a name such as “XYZTechSolution”. Select a group for remote desktop access such as group1 we created in admin OU.

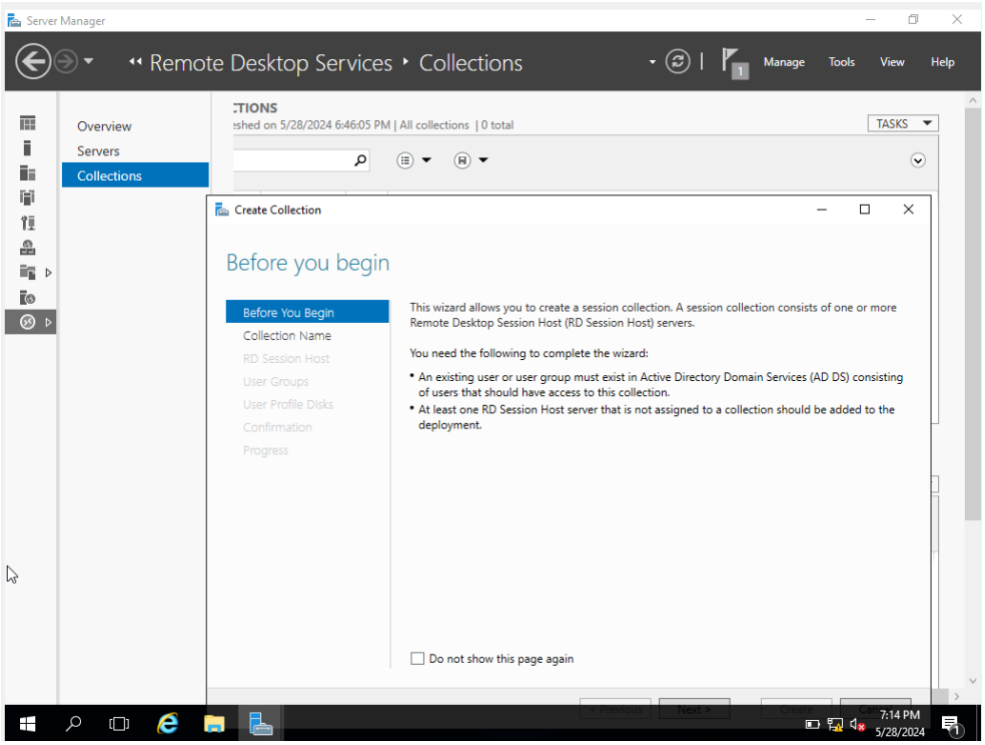

Fig.35

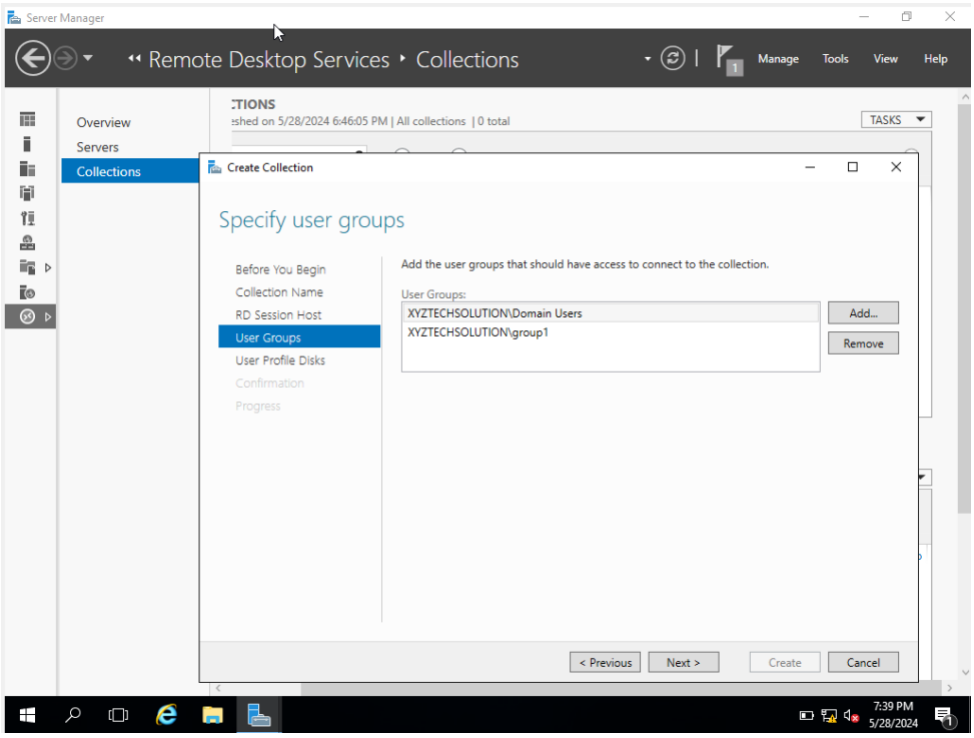

Fig.36

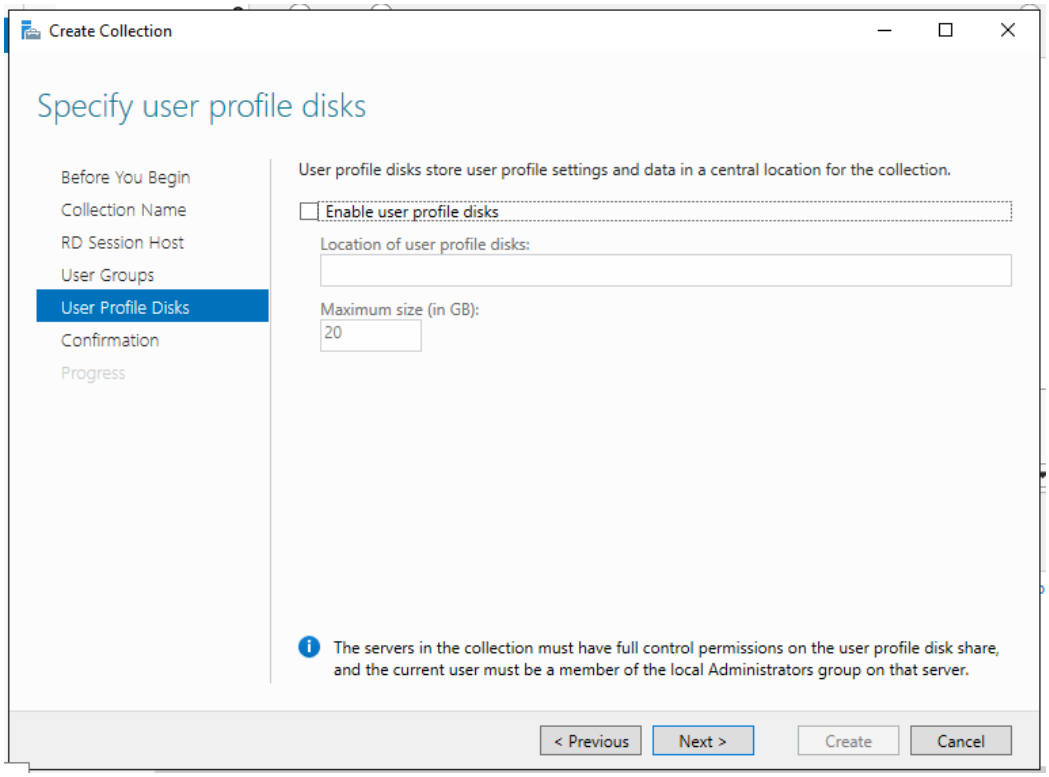

Fig.37

vi) Finally press create.

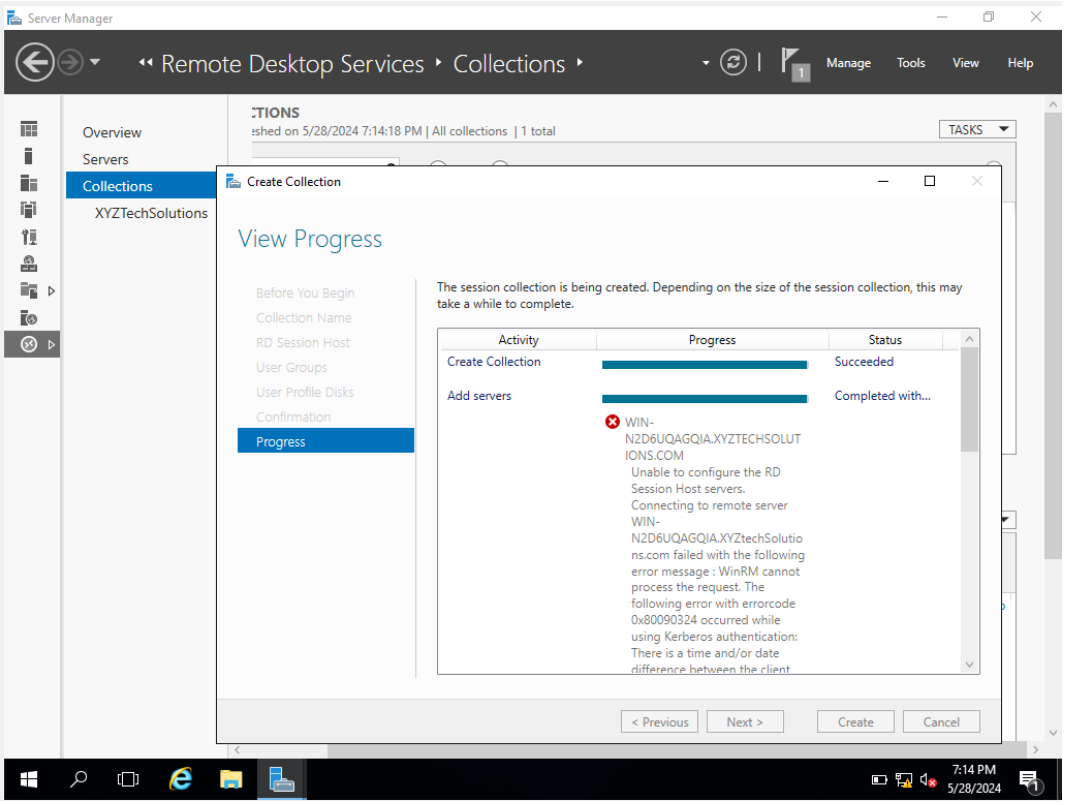

Fig.38

vii) Now press on XYZTechSolutions and add the apps and services you want to host remotely.

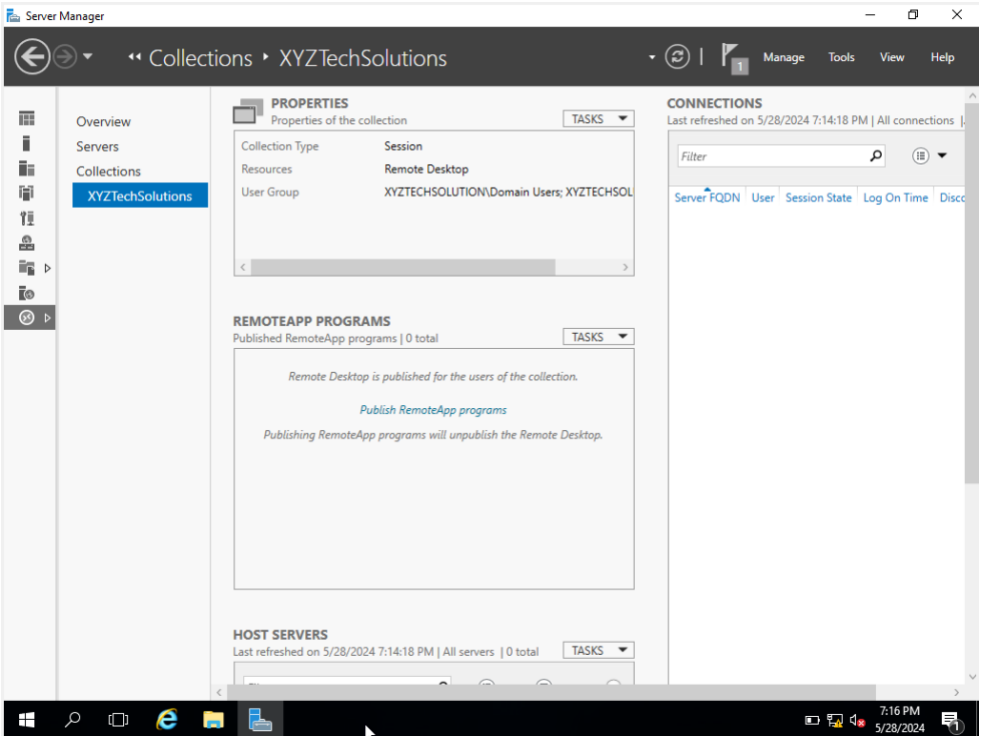

Fig.39

Network Policy

i) To manage the network access policy, we need to install the network policy and access services and configure them. Go to add roles and features and follow the same steps as before until server roles, then you need to select Network policy and access services.

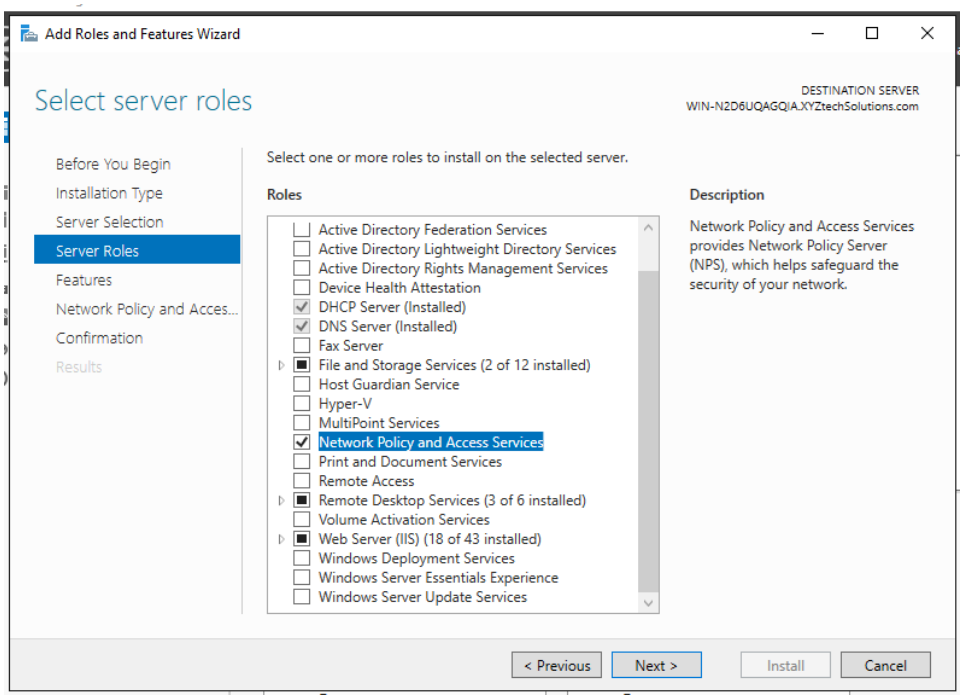

Fig.40

ii) Click next and then install.

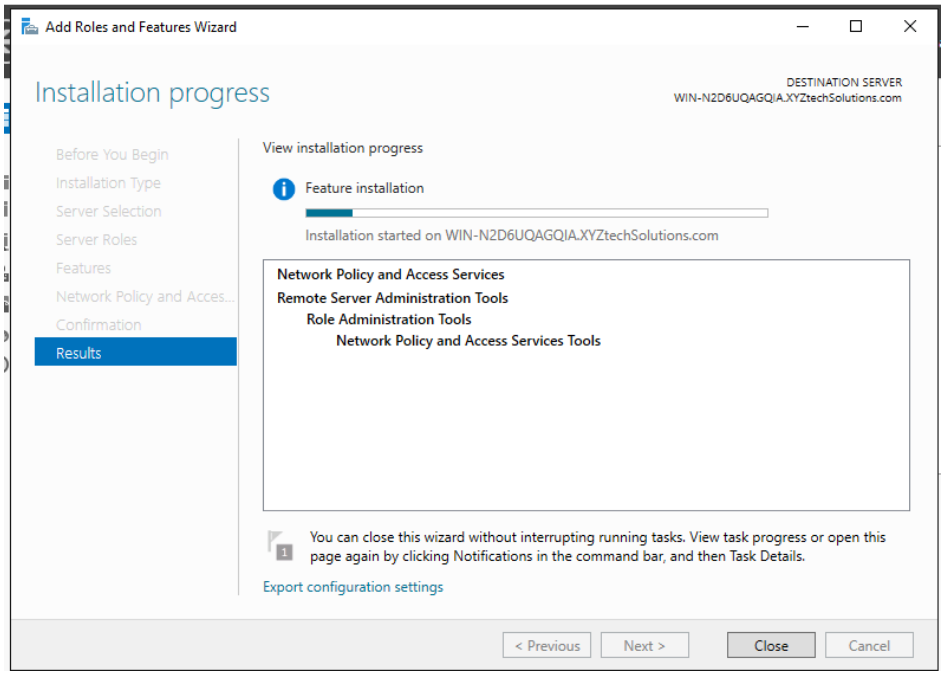

Fig.41

iii) Now go to tools, NPS. From here you can create and manage network and access policies as per your needs.

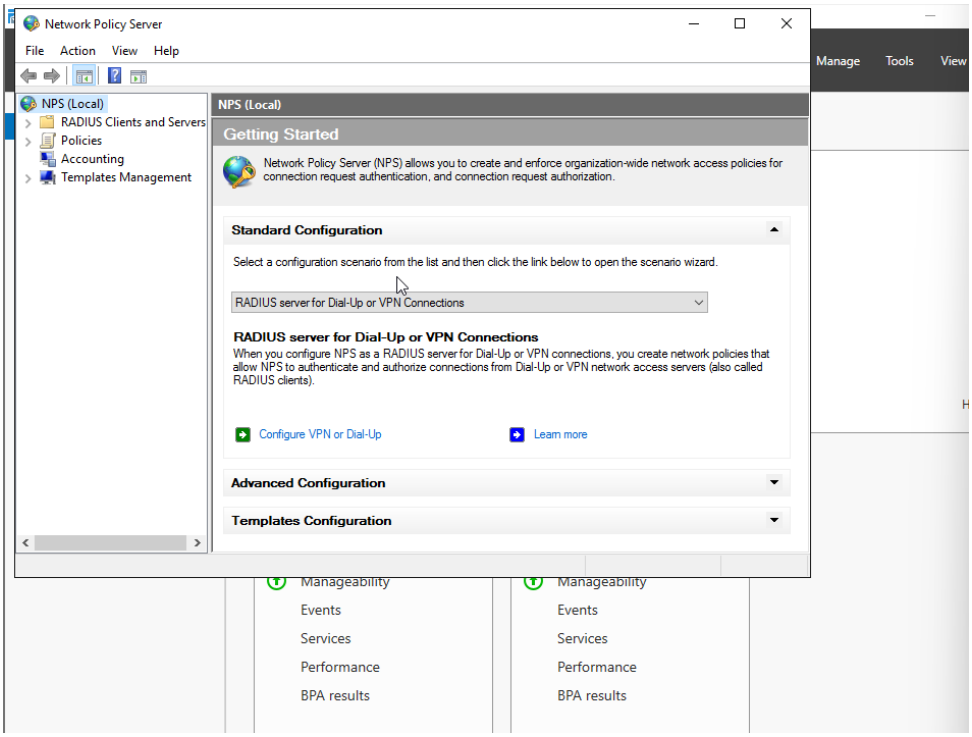

Fig.42

Group policy to enforce password policies.

i) To enforce a password policy, go to tools-GPM-expand XYZdomain-domain and right click on default domain policies and click on edit.

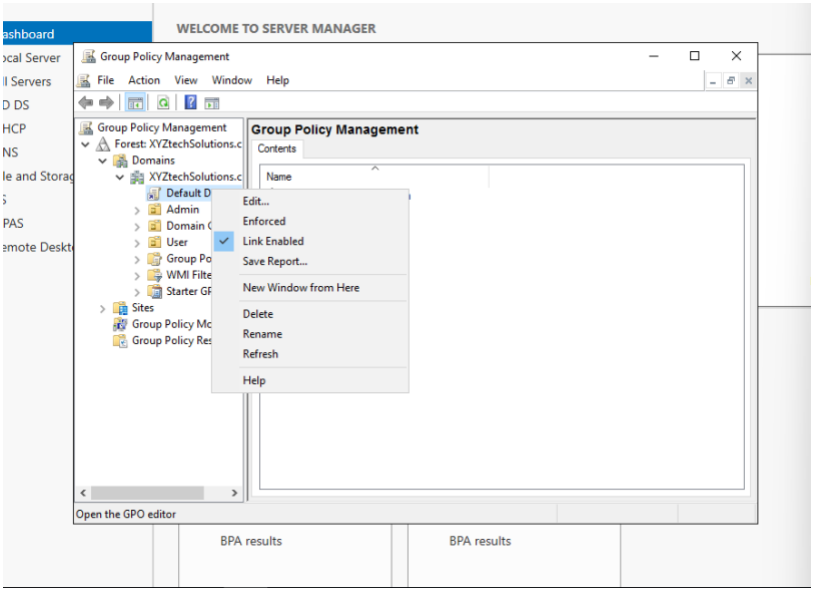

Fig.43

ii) A new window will appear. From there expand policies-windows settings-security settings-account policies- password policies.

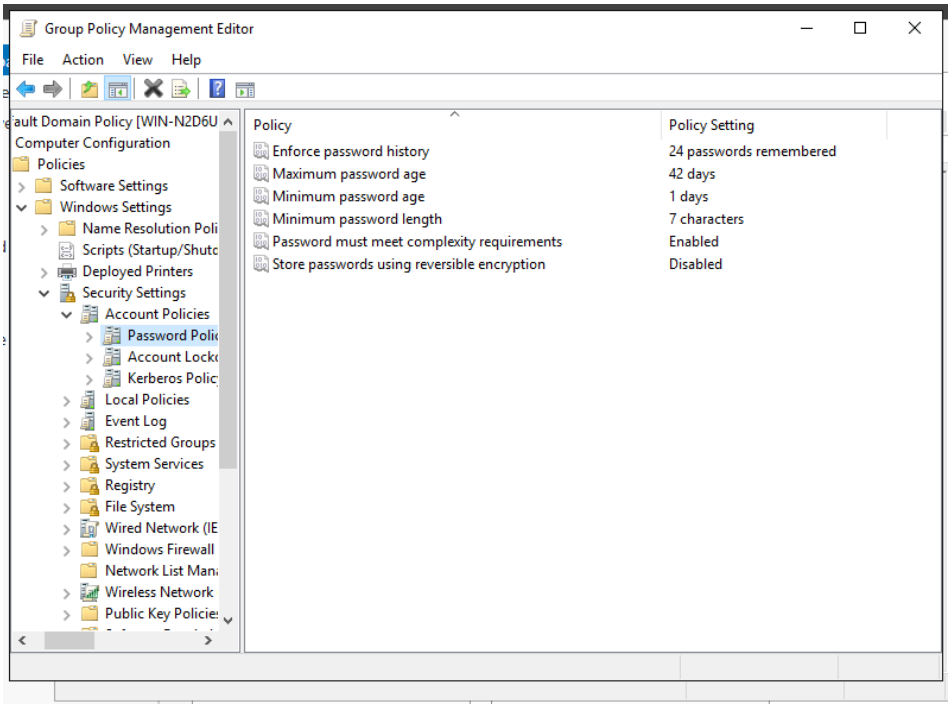

Fig.44

From here we can change and manage password policy as per security requirement of the company.

iii) Now go to account lockout. Here we can manage the settings to lock a user account after certain invalid attempts. In this case we have set the threshold to 3 attempts.

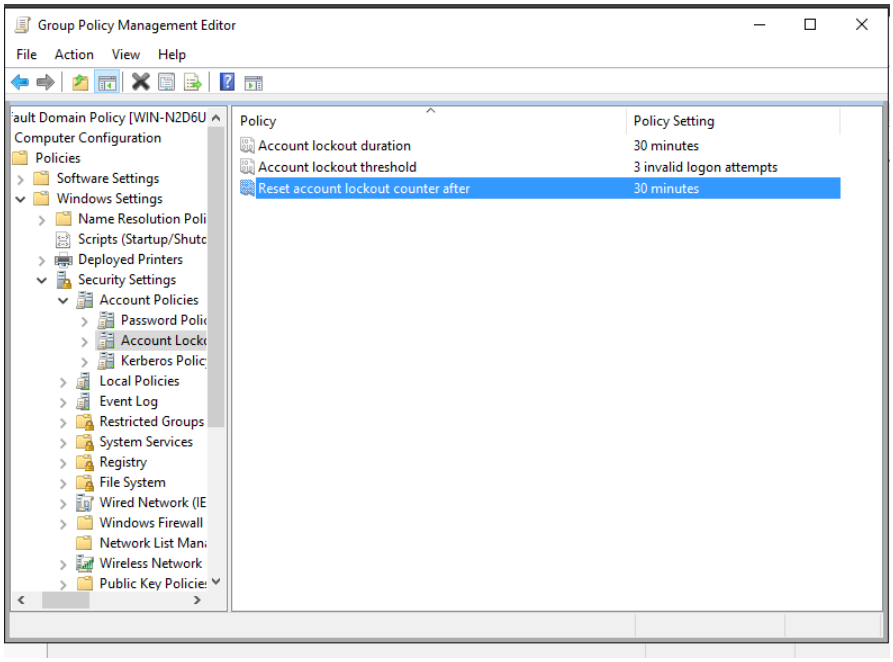

Fig.45

iv) Finally, after managing all the settings click apply and then okay. The policy will be effective after the settings are applied.

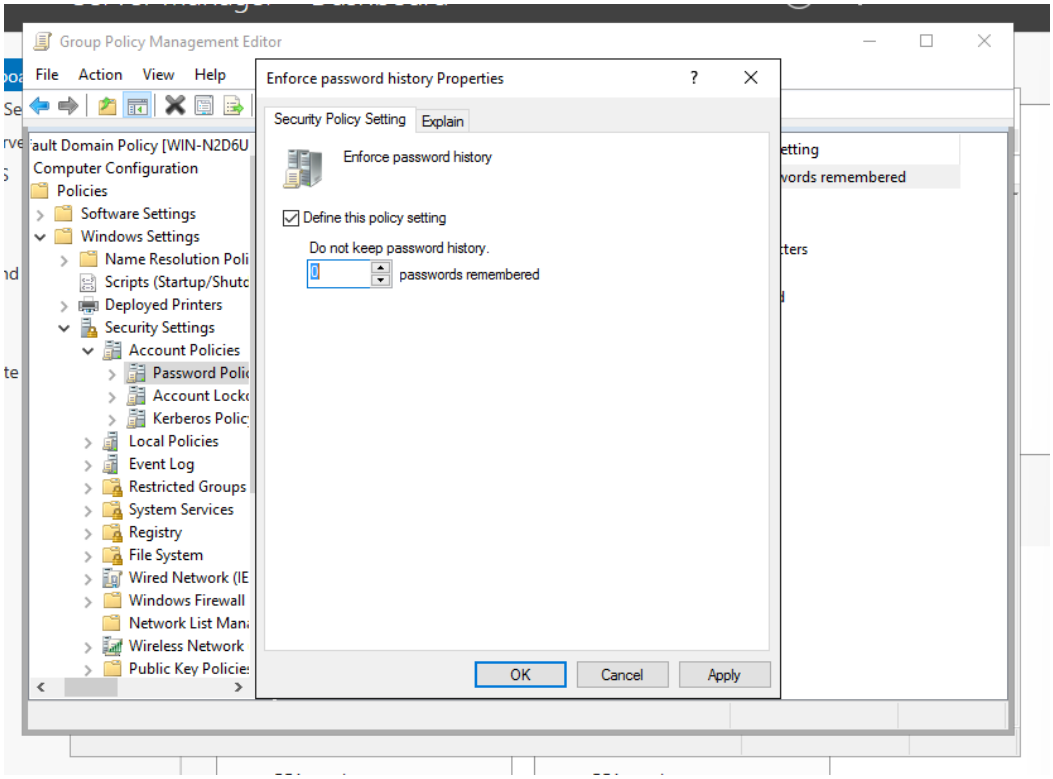

Fig.46

Conclusion

In this project, we used Windows Server 2016 to successfully create an extensive networked system for XYZ Tech Solutions. We have set up Windows Web Server (IIS) to host the company website files, a Backup Server prevent data loss during unexpected events, and a DHCP server to manage IP addresses dynamically to user computers and assigned fixed Ip addresses to all servers. Additionally, we also set up roaming profiles for users to allow flexible access, installed Remote Desktop Services to enable remote working facilities, and established Active Directory Domain Services for centered control. To further improve the network and system security, Network Policy and Access Services were configured, and Group Policy was utilized to enforce strict password policies for users. A strong, safe, and effective IT infrastructure is assured by this system documentation report with configuration guidelines, which will support the company's expansion globally and allow for effortless operations.

References

[1] T. Berners-Lee, R. Cailliau, A. Luotonen, H. F. Neilsen and A. Secret, "The World Wide Web," *Communications of The ACM,* vol. 37, no. 8, pp. 76-82, 1994.

[2] Y. Zhang, L. Zhong, S. Yang and G.-M. Muntean, "Distributed data backup and recovery for software-defined wide area network controllers," *Transactions on Emerging Telecommunications Technologies,* vol. 33, no. 4, p. e4411, 2022.

[3] P. Membrey, T. Verhoeven and R. Agenendt, "Setting Up DHCP," in *The Definitive Guide to CentOS* , Berkely,CA, Apress, 2009, pp. 181-197.

[4] D. Francis, Mastering Active Directory: Design, deploy, and protect Active Directory, Birmingham: Packt Publishing Ltd., 2021.

[5] B. Wright and B. Svidergol, Virtualizing Desktops and Apps with Windows Server 2012 R2 Inside Out, Microsoft Press, 2015.

[6] G. Budigiri, C. Bauman, J. T. Muhlberg, E. Truyen and W. Joosen, "Network Policies in Kubernetes: Performance Evaluation and Security Analysis," Porto,Portugal, 2021.

[7] J. krause, Mastering Windowa Group Policy, books.google, 2018.