UNIVERSITI TEKNIKAL MALAYSIA MELAKA

FAKULTI TEKNOLOGI MAKLUMAT DAN KOMUNIKASI (FTMK)

SEMESTER 2 SESI 2018/2019

BITC

BITU 3923

WORKSHOP II

FINAL REPORT

SUPERVISOR: MUHAMMAD SYAHRUL AZHAR

EVALUATOR: DR SYARULNAZIAH BINTI ANAWAR

AHLI KUMPULAN:

1. AIMAN FIKRI BIN ASMADI B031810068
2. AHMAD FAISAL BIN MD JAMAL B031810091
3. AMIRUL AZIM BIN ABDUL RASHID B031710036
4. MUHAMMAD SHOLEHIN BIN RAHMAT B031710037
5. MUHAMMAD HELMI AQMAR BIN MAT RAWI B031810020

ACKNOWLEDGEMENTS

First and foremost, we would like to thank to our supervisor of this project, En. Muhammad Syahrul Azhar for her valuable guidance and advice. Both of them inspired us greatly to work in this project. They willingness to motivate us contributed tremendously to our project. We also would like to thank them for showing us some examples that are related to the services in our project which helped us understand our project better. This helped us complete our project on time. We would also like to thank our evaluator for this workshop, Dr Syahrulnaziah binti Anawar for taking the time to evaluate us. This evaluation gave us a deeper understanding of our services and network infrastructure.

Besides that, we would like to thank the authority of Technical Malaysia University (UTeM) for providing us with a good environment and facilities to complete this project. Finally, an honourable mention goes to our families and friends for their understandings and supports on us in completing this project. With the help of the particular that mentioned above, we completed our project successfully on time.

ABSTRACT

In this Workshop II project, we have to define, implement and manage tasks which start from selecting a leader to lead this project from the beginning until the end of this project. A task has been given to each member and we create a schedule for the task to finish on time. It is very important to manage and organizes every task in order to avoid any problems and error later on.

Our main objective in this Workshop II is for this project to be successful and able to go through the obstacles and challenges faced while completing the task given. We are grateful to experience this as it helped us to be more prepared in our industrial training. Our group had decided to use Windows 2008 Server in server 1 (Window), Sun Solaris 10 in server 2 (Sun) and Ubuntu 14.04 in server 3 (Linux).

Our group also was assigned to set up 15 services listed. The 15 networks services listed are Server Virtualization; with minimum of 1 application service installed in the VM, Network Management System, AAA (Authentication, Authorization, and Accounting) using Radius, Linux Email Server, IPsec site-to-site tunneling, DNS (IPv4 & IPv6), DHCP (IPv4 & IPv6), Routing & NAT, Proxy Server, Secure FTP; with authentication and ecryption, Access Control List (ACL); with minimum of 4 rules, Web, SSL & Virtual Hosting, IPv6 Web with IPv6 Tunneling (testing IPv6 Web from remote site), Active Directory; with minimum of 2 UAC/GPO, Wireless user authentication using Radius server (AD user account/Mac Address). During the Workshop II, we faced several problems but still managed to overcome it and make this project successful.

ABSTRAK

Dalam Projek Bengkel II ini, kami perlu menentu, melaksana dan menguruskan tugasan yang diberikan bermula dengan memilih ketua yang berdedikasi dalam memimpin Projek Bengkel 2 ini. Tugas- tugas telah diberikan kepada setiap ahli kumpulan dan jadual telah dibuat bagi memudahkan setiap individu membuat tugasan dalam tempoh yang telah ditetapkan. Hal ini sangat penting dalam mengurus dan mengatur setiap tugasan agar tidak menghadapi masalah dan kesulitan di kemudian hari.

Tujuan utama kami dalam Projek Bengkel II ini ialah untuk membuat projek ini berjaya dan kami berjaya mengharungi setiap halangan dan cabaran dalam menyelesaikan tugasan yang diberikan. Kami amat bersyukur dan berterima kasih kerana telah diberikan kesempatan untuk membuat projek sebegini agar kami lebih bersedia pada latihan industri nanti. Kumpulan kami telah memutuskan untuk menggunakan Windows 2008 Server dalam server 1 (Window), Sun Solaris 10 dalam server 2 (Sun) dan Ubuntu 14.04 dalam server 3 (Linux).

Kumpulan kami juga ditugaskan untuk mendirikan 15 servis. 15 Servis yang diperlukan pada rangkaian adalah *Server Virtualization; with minimum of 1 application service installed in the VM, Network Management System, AAA (Authentication, Authorization, and Accounting) using Radius, Linux Email Server, IPsec site-to-site tunneling, DNS (IPv4 & IPv6), DHCP (IPv4 & IPv6), Routing & NAT, Proxy Server, Secure FTP; with authentication and ecryption, Access Control List (ACL); with minimum of 4 rules, Web, SSL & Virtual Hosting, IPv6 Web with IPv6 Tunneling (testing IPv6 Web from remote site), Active Directory; with minimum of 2 UAC/GPO, Wireless user authentication using Radius server (AD user account/Mac Address).* Dalam proses menyiapkan Projek Bengkel II ini, pelbagai kesukaran serta kekangan yang kami hadapi namun kami tetap berjaya untuk menyiapkan projek ini dengan jayanya.

TABLE OF CONTENTS

LIST OF FIGURES

Figure Chapter 5

Figure 6

CHAPTER 1: INTRODUCTION

1.1 INTRODUCTION

Workshop II (BITU 3923) that offer for year 3 student Bachelor Degree student that already past for their workshop 1 in second year. This subject are built for student as an exposure for them what is in their coast and as preparation for their final year project and as a beginning for their career after graduate. In this subject students will experience by themselves work with the real hardware and real situation beside to create the confidence while handle the task.

Students will give a group to complete their task as require, student ask to design an infrastructure to implement a network, install the service using the tools and requirement that has been prepare. Each group will be provided with 3 servers (1 Windows and 2 Linux Distro), 2 network interface card (NIC), one Access Point, 1 router (2 Fast Ethernet), one Manageable Switch, one wireless router, one serial cable, UTP cable, 12 RJ-45 and 1 set of Crimping Tool.

Student need to complete the requirement by up all 15 services in our network infrastructure and need to maintenance and monitor all the activity or all the progress. Physical and logical design are design to for us clearly see how the task will run. Different open source operating system has will use to make sure this scenario are run smoothly which is Windows Server 2012, Linux operating system that is UBUNTU and Debian.

The company given name InfraBerry SDN.BHD is expanding with approximately 100 employees' .This Company provide server room where the main server is home and client connect to the remote site for internal and external communication. The sites are connect with simple point to point that can be use to carry IPv6 packets between the sites. We have setup the infrastructure for company InfraBerry SDN.BHD that covers all the networking functions

1.2 PROBLEM STATEMENT

Below those are the problem statement for Workshop 2:

I. Setup and design the network infrastructure
   - Using all the provided network equipment and setup the design the secure network.

II. Configure the network services
   - By the scenario and the requirement, student need to do the configuration and up all 15 services that has been listed.

III. Create a secure network
   - Implement the policy and protocol to make sure the network infrastructure are safely secure.

IV. Installing operating system
   - Install the three chosen operating system, which is Windows Server 2012, Linux Ubuntu and Debian.

1.3 OBJECTIVE

The purpose of implementation of Workshop 2 is to build a network in difference operating system in LAN and WAN connection. There are a few objective of network development:

- To fulfill all the requirement of Workshop 2
- To design network infrastructure by using the available requirement and equipment
- To learn how to manage the network
- To be able to implement designated network services.
- To be able to install and integrate network services infrastructure to suit the environment.

1.4 PROJECT PLAN

In the second week of the semester, all the student that take subject BITU 3923 had attend the briefing of the workshop two which is the workshop committee gave the explanation about how the workshop two will be going. Students already assign to their group which is consist of five student per group. Student meet their supervisor for the first meeting to know each other also another detail explanation. Within the week, all group members would have the first group meeting to discuss and prepare the project proposal that includes the details of the project such as the executive summary, logical and physical network design. The design is to show the network topology, gantt chart to show the timeline of the project and project distribution where the project manager will distribute the tasks to all the members.

On the third week, student need to submit the proposal to the supervisor for an approval. After that, every group need to take all the equipment to implement the workshop two such as router, switch, UTP cable, networking interface card and wireless access point. To run the workshop two students need to terminate the utp cable by ourselves and setup the device by install the operating system into three server that had been choose which is Ubuntu server, Windows server and Debian server. By continues week until week eight which is first phase student should apply or implement any five services in their network that will present to supervisor on progress one and prepare the Progress One report.

After the midsem break on week nine, student continue installing their services start week 10. Each person in group need to make any progress for the following progress presentation. Before week 14, our group target to implement the rest of services which is server virtualization, network management system, AAA (Authentication, Authorization, and Accounting) with radius, IPSec site-to-site tunneling, DHCP (IPv4 & IPv6), routing & nat, proxy server, access control list, IPv6 Web with IPv6 tunneling and wireless user authentication using RADIUS server. During this period our group also prepare a video and a poster that shows one of the services that has been set up. After the completion of the network, we will demonstrate our respective task individually to

the supervisor and evaluator while the video and poster prepared will be present during the project demonstration for the purpose of updates for the final exhibition at week 14.

At week 13, the final report and individual logbook will be revised if there is any error and improve. At week 14, the video and poster have been create during week 11 to week 12 will be use in the video and poster exhibition. The completed video and poster will be evaluate by the supervisors and evaluator. The finalized final report will be submitted during the evaluation by supervisor and evaluator

`

1.5 CONCLUSION

The Workshop II project are help expose the student to design, implement, install, configure, and manage the basic component of computing resources and basic services in this project. The Workshop two also helps us to explore something new in network environment using all real devices that gives to us in any different platform operating system. This is very important because we can train our team to work not only industrial training but in the future as well. In addition, we can apply the learning and understand theory we gained in class through practical which can suite with the future environments which is the use of IPv6. Finally, we can gain extra knowledge, experience and prepare to face the future challenges from this project.

CHAPTER 2:PROJECT REQUIREMENT

2.1 Introduction

The secure network infrastructure will be designed by using the available tools. The network to be developed will consist of three servers with combination of different platforms. Besides that, we need to setup 15 services and it will be divided among the servers. There is 15 services of computer networking. The servers will be using mainstream operating system to simulate real environment and superior services for the users. It is very important to make sure that the network system operate at the desired performance and the technologies used will be the best possible, depend on the allocated budget.

2.2 Types of Operating System Use in the Project

An operating system is to manage the computer's memory, processes, software and hardware. To let the user gain a good experience when they operate the computer, a high-quality operating system is needed to integrate network services infrastructure to suit the network environment that have been set. The operating systems use in the project are Window Server 2012 R2, Ubuntu 18.04 LTS amd64 (Linux) and Debian 9.

2.3 Operating System Bakground

2.3.1 Windows Server 2012 R2

Windows Server 2012 R2 is the sixth version of the Windows Server family of operating systems. It was unveiled on June 3, 2013 at TechEd North America, and released on October 18, 2013. A further update, formally designated Windows Server 2012 R2 Update, was released in April 2014. It is a cumulative set of security, critical and other updates. Windows Server 2012 R2 was succeeded by Windows Server 2016.

2.3.2 Ubuntu 18.04

Ubuntu is a free and open-source Linux distribution based on Debian. Ubuntu is officially released in three editions: Desktop, Server, and Core (for internet of things devices and robots). Ubuntu is a popular operating system for cloud computing, with support for OpenStack. Ubuntu is released every six months, with long-term support (LTS) releases every two years. The latest release is 19.04 ("Disco Dingo"), and the most recent long-term support release is 18.04 LTS ("Bionic Beaver"), which is supported until 2028. Ubuntu is developed by Canonical and the community under a meritocratic governance model. Canonical provides security updates and support for each Ubuntu release, starting from the release date and until the release reaches its designated end-of-life (EOL) date. Canonical generates revenue through the sale of premium services related to Ubuntu. Ubuntu is named after the African philosophy of ubuntu, which Canonical translates as "humanity to others" or "I am what I am because of who we all are".

2.3.3 Debian 9

Debian is a Unix-like operating system consisting entirely of free software. Ian Murdock founded the Debian Project on August 16, 1993. Debian 0.01 was released on September 15, 1993 and the first stable version, 1.1, was released on June 17, 1996. The Debian Stable branch is the most popular edition for personal computers and network servers, and is used as the basis for many other Linux distributions.

Debian is one of the earliest operating systems based on the Linux kernel. The project is coordinated over the Internet by a team of volunteers guided by the Debian Project Leader and three foundational documents: the Debian Social Contract, the Debian Constitution, and the Debian Free Software Guidelines. New distributions are updated continually, and the next candidate is released after a time-based freeze.

Debian has been developed openly and distributed freely according to the principles of the GNU Project. Because of this, the Free Software Foundation sponsored the project from November 1994 to November 1995. The popular Linux operating system Ubuntu was also released based on Debian. When the sponsorship ended, the Debian Project formed the nonprofit Software in the Public Interest to continue financially supporting development. The Intel 586 (Pentium), Intel 586/686 hybrid (Pentium with MMX) and PowerPC architectures are no longer supported as of Stretch.

2.4 Operating System Justification

2.4.1 Windows Server 2012 R2

Windows Server 2012 R2 is the successor to Windows Server 2012, Microsoft's enterprise server operating system. Developed under the Windows Server Blue codename, Windows Server 2012 R2 made its official debut in late 2013. Among its many improvements, Windows Server 2012 R2 includes an enhanced Hyper-V hypervisor (Hyper-V 2012 R2) that provides the ability to compress virtual machines (VMs) during live migrations, automatic reallocation of memory between VMs running Linux as a guest on Hyper-V hosts, remote direct memory access (RDMA) support during live migrations, VM live cloning, and support for shared VHDX files.

2.4.2 Ubuntu 18.04

Ubuntu 18.04 keeps the same trend and will feature the latest GNOME (i.e., version 3.28) at the time of its release. Canonical promised better boot speed in Ubuntu 18.04. Using systemd's features, bottlenecks will be identified and tackled to boot Bionic as quickly as possible. Ubuntu 18.04 is removing the redundancy here. Now if add a new repository with add-apt-repository command, it will run the apt-get update command automatically. No need to run this command manually. Ubuntu 18.04 provides native support for color emojis by default. Until now, only monochrome emojis are supported out of the box on Ubuntu. Canonical has initiated a collaborative project to develop a new theme set for Ubuntu 18.04 with contribution from the community.

2.4.3 Debian 9

Debian 9 (Stretch) was released on 17 June 2017, two years and two months after last release Debian 8 (Jessie), and contained more than 51,000 packages and the latest minor update, called a "point release", is version 9.9, released on April 27, 2019; 19 days ago. Major upgrades include the Linux kernel going from version 3.16 to 4.9, GNOME desktop version going from 3.14 to 3.22, KDE Plasma 4 was upgraded to Plasma 5, LibreOffice 4.3 upgraded to 5.2 and Qt upgraded from 4.8 to 5.7. LXQt has been added as well. The Intel 586 (Pentium), Intel 586/686 hybrid (Pentium with MMX) and PowerPC architectures are no longer supported as of Stretch.

2.5 Hardware Requirement

2.5.1 Hardware Requirements for Windows Server 2012 R2

Component	Minimum	Recommended
Processor	1.4 Ghz	2 GHz or faster
Memory	512 MB RAM	2 GB RAM or greater
Available Disk Space	32 GB	40 GB or greater
Optical Drive	DVD-ROM drive	DVD-ROM drive
Display	Super VGA (800x600) monitor	XGA (1024x768) monitor

2.5.2 Hardware Requirements for Ubuntu 18.04

Component	Minimum Requirements
Processor	2 GHz dual core processor
Memory	2 GB RAM
Available disk space	25 GB of hard drive space
Display	VGA capable of 1024x768 screen resoltuion

2.5.3 Hardware Requirements for Debian 9

Component	Minimum Requirements
Processor	1 GHz Pentium 4 processor
Memory	512 MB RAM
Available disk space	10 GB HDD
Installation Media	USB / DVD

2.6 Hardware Justification

2.6.1 Servers

- Three servers will be installed with Windows Server 2012 R2, Ubuntu 18.04, and Debian 9.
- In Windows Server 2012 R2 we have installed Active Directory, DNS, DHCP, Server Virtualization, Web SSL & Virtual Hosting, and IPv6 Web with IPv6 Tunelling.
- For Ubuntu 18.04, we have installed Proxy Server and Secure FTP.
- For Debian 9, we have installed Network Management System and Linux Email Server.

2.6.2 Network Interface Card (NIC)

- NIC is a circuit board or card that is installed in a computer so that it can be connected to a network.
- Network interface card provides the computer with a dedicated, full-time connection to a network.
- Network interface cards also have can supplying a basic addressing system that can be used to get data from one computer to another on the network.
- Each NIC will be used for each server and will be able to provide network communication capabilities to and from a computer.

2.6.3 UTP Cable

- We are given about 15 meters long UTP cable for this project.
- Unshielded Twisted Pair (UTP) is a type of transmission media that can transmit voice or data signals in a LAN that's way we choose to use this cable in our project.

2.6.4 RJ-45 Connector

- An 8-pin/8-position plug or jack is commonly used to connect computers onto Ethernet-based local area networks (LAN).
- The standard connector used for the UTP cable.
- RJ45 is the connection for the cable, we use from switch to other client computer to make connection over internet once cable are plugged in switch.

2.6.5 Switch

- The switch is used to connect all the three servers and the client.
- Also use to connect Computer to Internet.
- It is a multiport network bridge that uses hardware addresses to process and forward data at the data link layer of the OSI model.

2.6.6 Router

- It is a networking device that forwards data packets between computer networks and performs “traffic directing” functions on the internet.
- To set IP address and to make connection between servers and client.
- To route your information to server. Other configuration routing we set at each server in router to make connection that we need.

2.6.7 Conclusion

Last but not least, we should ensure that all the computer meet the minimum requirements before installing Operating System. It is complicated for us to install and integrate three different types of Operating System with at least 15 different services in a network infrastructure. We have to consider the demand of the operating system and decide which the best to implement is that we set to each server. We also need to make a good decision on install the core and main services into Window Server 2012 R2 and the least important services into Ubuntu 18.04 or Debian 9. This is because Windows Server 2012 R2 is easier to install services and provide many services that needed.

Additionally, we likewise need to drill down and explore about the equipment necessities to ensure circumstantially of system. We need to ensure those prerequisites are appropriate and stand to help our administrations for every server before we introduced it. Immaculate setting can make quality association over web.

CHAPTER 3: DESIGN

3.1 Introduction

In this workshop II, we have to define, design, implement and manage network services. Every group need to implement their own network design which is needed to be applied in real device. Stated in the requirements, that need us to design the network that include three different servers, one CISCO router, one CISCO switch and a client host for the design. Our group already designs the networks that have two clients that are from internal and external. We have been supplied with RJ-45, UTP cable, console cable and a set of crimping tools. We also required using different operating system to set the network environment.

3.2 Physical Design

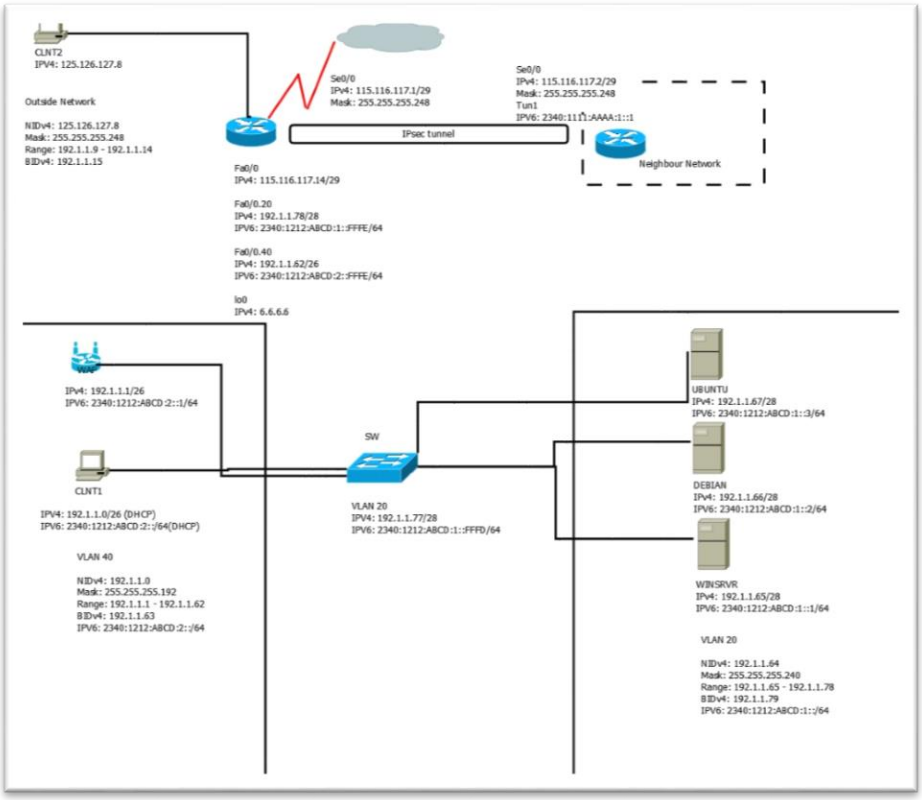


Figure 3.1: Physical Design

3.4 Logical Design

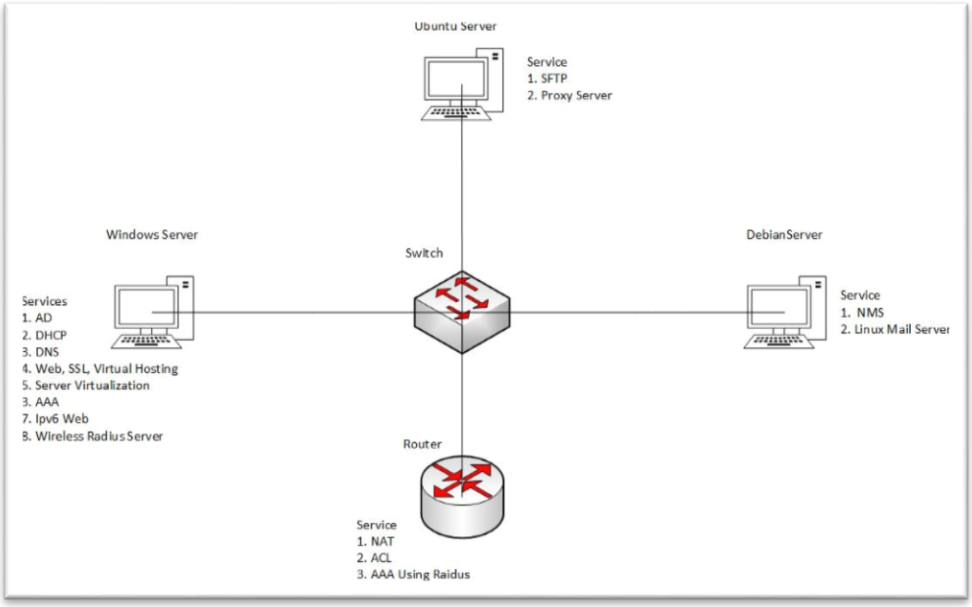


Figure 3.2 Logical Design

3.5 Conclusion

System planning is a significant part while making a system. Without system configuration there is no thought on the most proficient method to start the execution of the system. There are not many fundamental factors that should be considered while executing system structure that incorporate, the arranging of system multifaceted nature must be in accordance with the system manager, repetition, principles and systems for upkeeps factor. Those components are having to guarantee the system can be executing, expandable for future usage and simple to keep up.

In the wake of considering on those elements, we had executed system as structured physically and experience to the following dimension of actualizing that is arranging the usage of system administrations

CHAPTER 4: SERVICES

4.1 Introduction

In this chapter, each service that was installed will be listed and explained. Explanation will include the function of the service, what are the problems that are solved by installing the service, and what type of software use.

4.2 Types Of Softrware

4.2.1 List Of Operating System

1. Windows Server 2012
2. Ubuntu Server
3. Debian Server

4.2.2 List Of Services

1. Server Virtualization
2. Network Management System
3. AAA (Authentication, Authorization, and Accounting) using Radius
4. Linux Email Server
5. IPSec site-to-site tunneling
6. DNS (IPv4 & IPv6)
7. DHCP (IPv4 & IPv6)
8. Routing & NAT
9. Proxy Server
10. Secured FTP
11. Access Control List (ACL)
12. Web, SSL & Virtual Hosting
13. IPv6 Web with IPv6 Tunneling
14. Active Directory
15. Wireless user authentication using RADIUS server

4.3 Brief Overview Of Services

4.3.1 Windows Server 2012

Windows Server 2012, once in the past codenamed Windows Server 8. The successor of Windows Server 2008 R2, its enhancements incorporate generally speaking redesigns in cloud computing storage infrastructure. Windows Server 2012 was made with the Metro structure language so it has indistinguishable look and feel from Windows 8 except if introduced in Server Core mode. Managers can switch between Server Core and the Server with a GUI choices without a full reinstallation. Windows Server 2012 has an IP address management (IPAM) role for discovering, monitoring, auditing and managing the network's IP address space. A few changes have been made to Active Directory. The PowerShell-based Deployment Wizard can work remotely, enabling administrators to elevate cloud-based servers to domain controllers without the Wizard running on the server itself. Following the fulfillment of this process, PowerShell scripts containing duplicates of command utilized in the process can help with the computerization of additional domain controllers, allowing for large-scale Active Directory deployments.

4.3.2 Ubuntu Server

Ubuntu Server is a server operating system, created by Canonical and open source developers around the globe, that works with almost any equipment or virtualization platform. It can serve up website, file shares, and containers, just as grow your organization contributions with an incredible cloud presence. One advantage that makes Ubuntu Server so engaging is it's practical. Anybody can download a copy of the most recent variant of Ubuntu Server and send it on the same number of machines as important at zero cost (minus hardware and time). Another advantage Ubuntu Server has over many platforms in its class is the new snap package feature. Snap packages are universal packages that contain all necessary dependencies and can be installed with a simple command (such as sudo snap install nextcloud). Snaps can also be easily updated with a single command (sudo snap refresh), so there are fewer administrative tasks.

4.3.3 Debian Server

Debian is a popular and openly accessible computer operating system that utilizes the Linux kernel and other program components acquired from the GNU project. Debian can be downloaded over the Internet or, for a little charge, got on CD. As Open Source software, Debian is created by more than 500 contributing software engineers who by and large structure the Debian Project. New releases are given every now and then. Ongoing service is available through subscription to a mailing list. Debian is a popular choice for servers, for example as the operating system component of a LAMP stack

4.3.4 Server Virtualization

Server virtualization is the veiling of server resources, including the number and character of individual physical servers, processors, and operating system, from server clients. The server administrator utilizes a software application to separate one physical server into numerous disconnected virtual situations. The virtual situations are once in a while called virtual private servers, yet they are otherwise called guests, instances, containers or emulations. There are three popular approaches to server virtualization: the virtual machine model, the paravirtual machine model, and virtualization at the operating system (OS) layer.

4.3.5 Network Management System

A network management system (NMS) is an application or set of application that lets network engineers manage a network's independent components inside a greater network management framework and performs several key functions. An NMS identifies, configures, monitors, updates and troubleshoots network devices both wired and remote in a venture arrange. A system management control application at that point shows the execution information gathered from each network component, permitting network engineers to make changes as required**.**

4.3.6 AAA (Authentication, Authorization, and Accounting)

Authentication refers to unique identifying data from every system user, for the most part as a username and password. System administrators monitor and add or delete authorized users from the system.

Authorization alludes to the way toward adding or denying individual user access to a computer network and its resources. Users might be given diverse authorization levels that limit their entrance to the network and related resources. Authorization determination may be based on geographical location restrictions, date or time-of-day restrictions, frequency of logins or multiple logins by single individuals or entities. Other associated types of

authorization service include route assignments, IP address filtering, bandwidth traffic management and encryption.

Accounting refers to the record-keeping and tracking of user activities on a computer network. For a given time period this may include, however is not limited to, real-time accounting of time spent accessing the network, the network services employed or accessed, capacity and trend analysis, network cost allocations, billing data, login data for user authentication and authorization, and the data or data amount accessed or transferred.

4.3.7 Linux Email Server

A mail server capable of sending and receiving mail across the internet. Use Simple Mail Transfer Protocol (SMTP) for send mail from one host to another. It is also system-independent, which means that the sender and receiver could have different operating systems.

4.3.8 IPSec site-to-site tunneling

Site-to-Site IPSec VPN Tunnels are used to allow the secure transmission of data, voice and video between two sites (e.g. offices or branches). The VPN tunnel is created over the Internet public network and encrypted using a number of advanced encryption algorithms to provide confidentiality of the data transmitted between the two sites.

4.3.9 DNS (IPv4 & IPv6)

Translate domain names into IP Addresses, which computers can understand. It also provides a list of mail servers which accept Emails for each domain name. Each domain name in DNS will nominate a set of name servers to be authoritative for its DNS records.

4.3.10 DHCP (IPv4 & IPv6)

A protocol for assigning dynamic IP addresses to devices on a network. With dynamic addressing, a device can have a different IP address every time it connects to the network. In some systems, the device's IP address can even change while it is still connected. DHCP also supports a mix of static and dynamic IP addresses. Dynamic addressing simplifies network administration because the software keeps track of IP addresses rather than requiring an administrator to manage the task.

4.3.11 Routing & NAT

Routing is the process of selecting a path for traffic in a network, or between or across multiple networks. routing is the higher-level decision making that directs network packets from their source toward their destination through intermediate network nodes by specific packet forwarding mechanisms.

Network Address Translation (NAT) is designed for IP address conservation. It enables private IP networks that use unregistered IP addresses to connect to the Internet. NAT operates on a router, usually connecting two networks together, and translates the private (not globally unique) addresses in the internal network into legal addresses, before packets are forwarded to another network.

4.3.12 Proxy Server

In computer networks, a proxy server is a server (a computer system or an application) that acts as an intermediary for requests from clients seeking resources from other servers. When using a proxy server, the user is connected to the server, not the Web site in their browser, because the proxy acts as a client on behalf of the user. It uses one of its own IP addresses to request the page from the server located on the Internet. Once the page is returned, the proxy server forwards it to the user, isolating them from the Internet.

4.3.13 Secure FTP

Secure FTP is a broad term that refers to two different technologies that can encrypt both authentication information and data files in transit using FTPS and SFTP. Secure FTP protocols protect data only while it is being transmitted. Once data files have been written to a secure FTP server, the data is no longer protected unless the files were encrypted before transmission.

4.3.14 Access Control List

Access Control List (ACL) are filters that enable to control which routing updates or packets are permitted or denied in or out of a network. Specifically used by network administrators to filter traffic and to provide extra security for the network.

4.3.15 Web, SSL & Virtual Hosting

The Web is the common name for the World Wide Web, a subset of the Internet consisting of the pages that can be accessed by a Web browser. Web pages are formatted in a language called Hypertext Markup Language (HTML).

SSL (Secure Sockets Layer) is the standard security technology for establishing an encrypted link between a web server and a browser. This connection guarantees that all information goes between the web server and programs stay private and basic.

Virtual hosting is a method for hosting multiple domain names (with separate handling of each name) on a single server (or pool of servers). This enables one server to share its resources, such as memory and processor cycles, without requiring all services provided to use the similar host name.

4.3.16 IPv6 Web with IPv6 Tunneling

IPv6 (Internet Protocol version 6) is a set of specifications from the Internet Engineering Task Force (IETF) that's essentially an upgrade of IP version 4 (IPv4). IPv6 use 128 bits rather than IPv4 only using 32 bits. This extension anticipates considerable future growth of the Internet and provides relief for what was perceived as an impending shortage of network addresses.

4.3.17 Active Directory

Active Directory (AD) is a Microsoft product that comprises of several services that run on Windows Server to manage permissions and access to networked resources. It authenticates and authorizes all users and computers in a Windows domain type network assigning and enforcing security policies for all computers and installing or updating software.

4.3.18 Wireless user authentication using RADIUS server

RADIUS is a protocol for carrying information related to authentication, authorization, and configuration between a Network Access Server that desires to authenticate its links and a shared Authentication Server.

CHAPTER 5: INSTALLATION AND CONFIGURATION

5.0 CHAPTER V INSTALLATION AND CONFIGURATION

5.1 Introduction

All the services that had been done have different methods and ways of configuration. This section will show how to install and configure all the services follow the correct setup. All services had been installed and configured to integrate network services infrastructure to suit the network environment and security policies that have been set. We have used different operating systems such as Windows, Ubuntu, and Fedora. Each operating system had been categories with their services. The configuration is to ensure the functioning of the service are successfully installed and configure.

5.2 Services and Corresponding Person-In-Charge

NAME	SERVICE
AHMAD FAISAL B. MD JAMAL	1. DOMAIN NAME SERVICE 2. SERVER VIRTUALIZATION 3. ROUTING & NAT
AIMAN FIKRI B. ASMADI	1. WEB, SSL & VIRTUAL HOSTING 2. WIRELESS RADIUS SERVER 3. IPSEC SITE-TO-SITE TUNNELING
AMIRUL AZIM B. ABDUL RASHID	1. AAA USING RADIUS 2. SECURE FTP 3. ACCESS CONTROL LIST
MUHAMMAD HELMI AQMAR B. MAT RAWI	1. DHCP (IPV4 & IPV6) 2. LINUX EMAIL SERVER 3. IPV6 WEB WITH IPV6 TUNNELLING
MUHAMMAD SHOLEHIN B. RAHMAT	1. NETWORK MANAGEMENT SYSTEM 2. PROXY SERVER 3. ACTIVE DIRECTORY

5.3 SERVICE INSTALLATION AND CONFIGURATION

5.3.1 Server Virtualization

Step 1 : First, install hyperv inside server manager

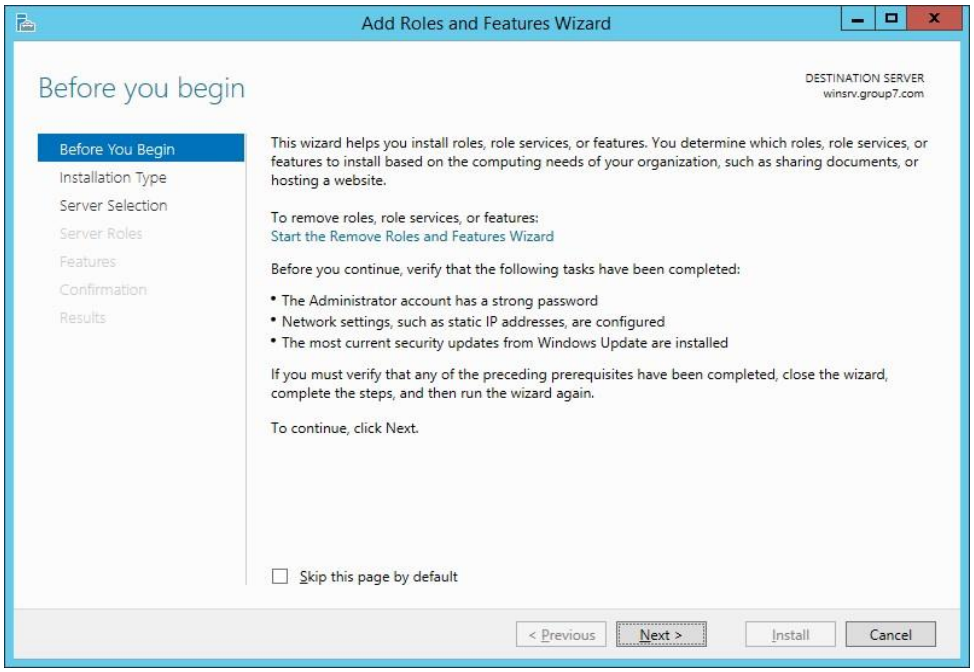


Figure 5. 1 : Install hyperv

Step 2: Choose installation type by click on role-based or feature-based installation

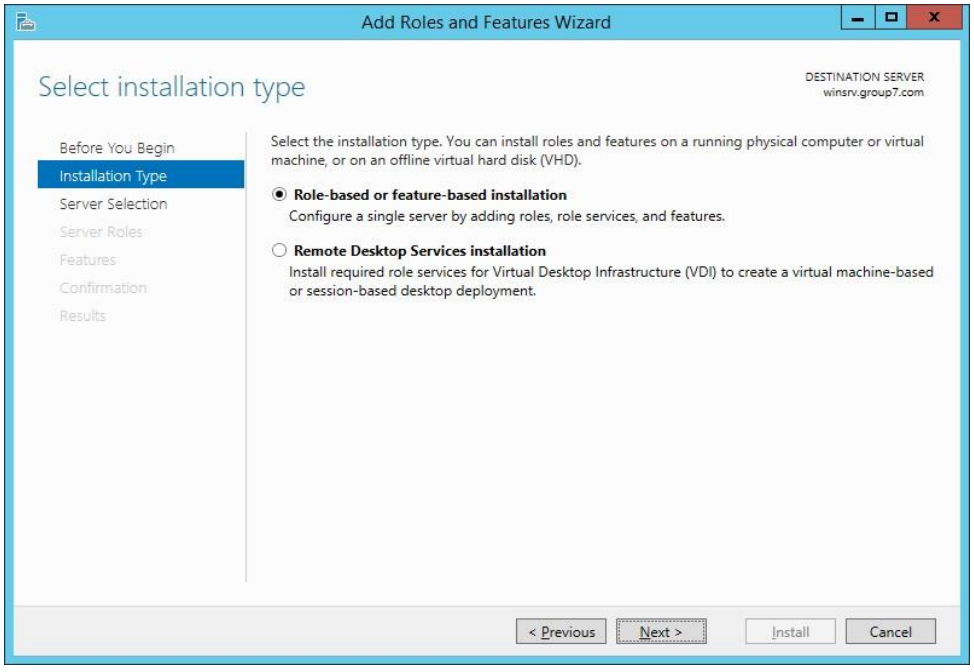


Figure 5. 2 : Installation type

Step 3: Click on add features to add features for Hyper-V

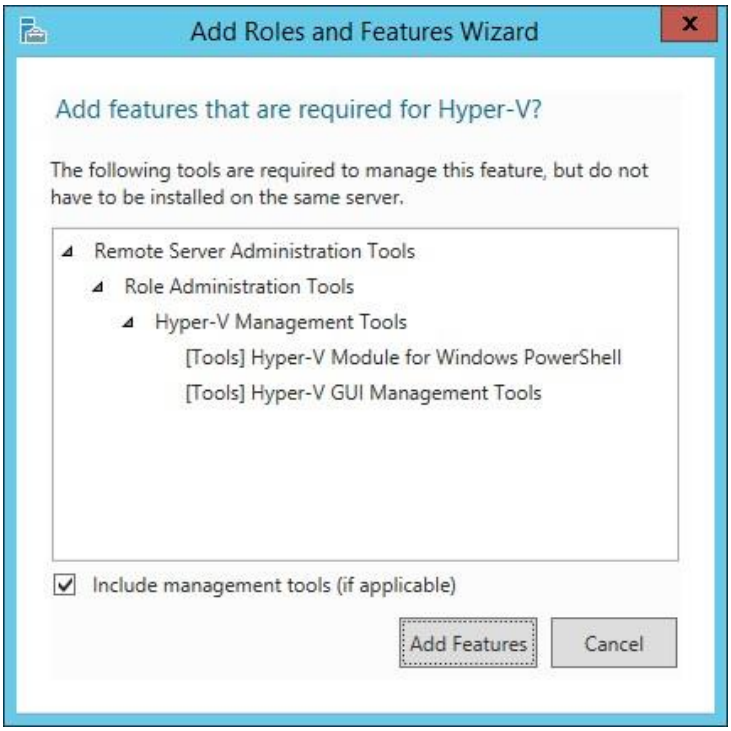


Figure 5. 3 : Add features

Step 4: Tick the check box for Hyper-V installation then click next

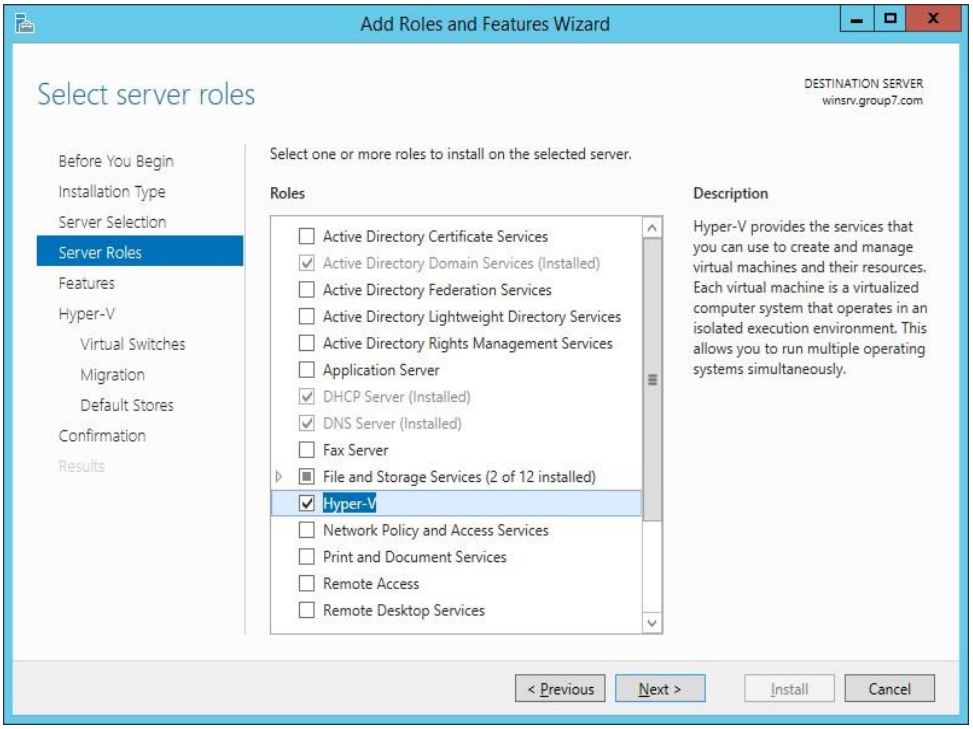


Figure 5. 4 : Server roles

Step 5: Then, choose NET Framework 4.5 features and click next

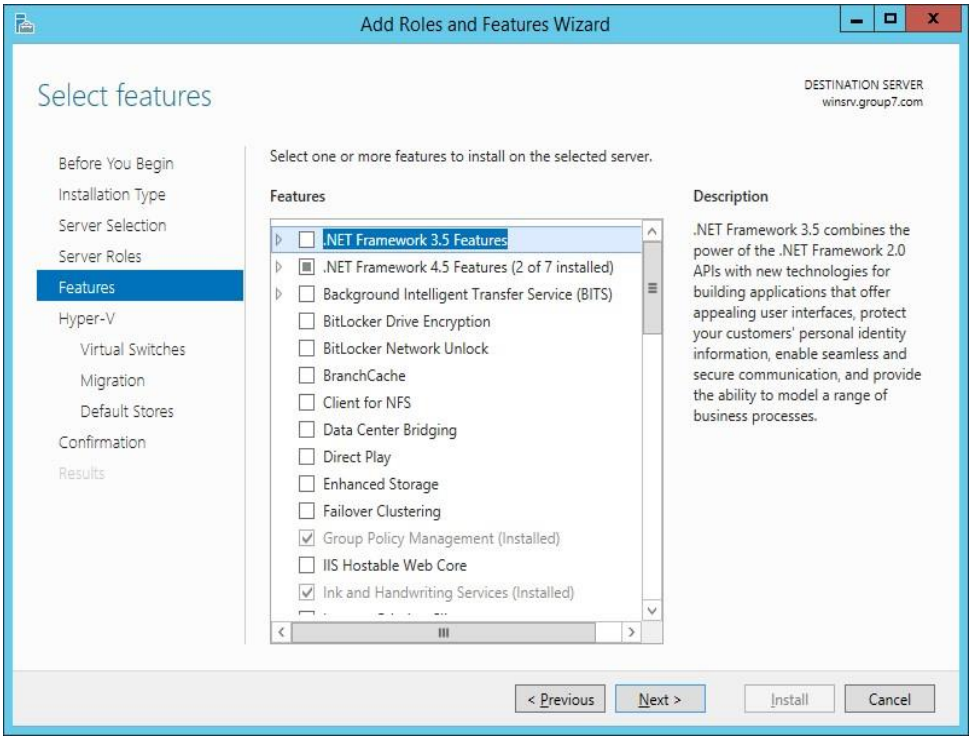


Figure 5. 5 : Features

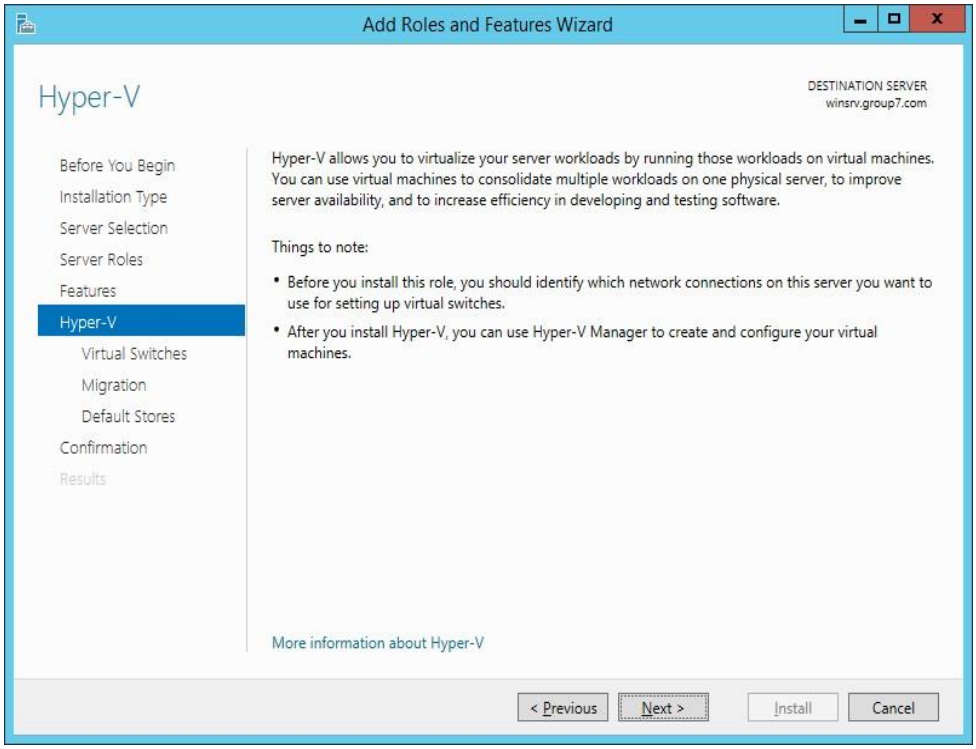


Figure 5. 6 : hyperv installation

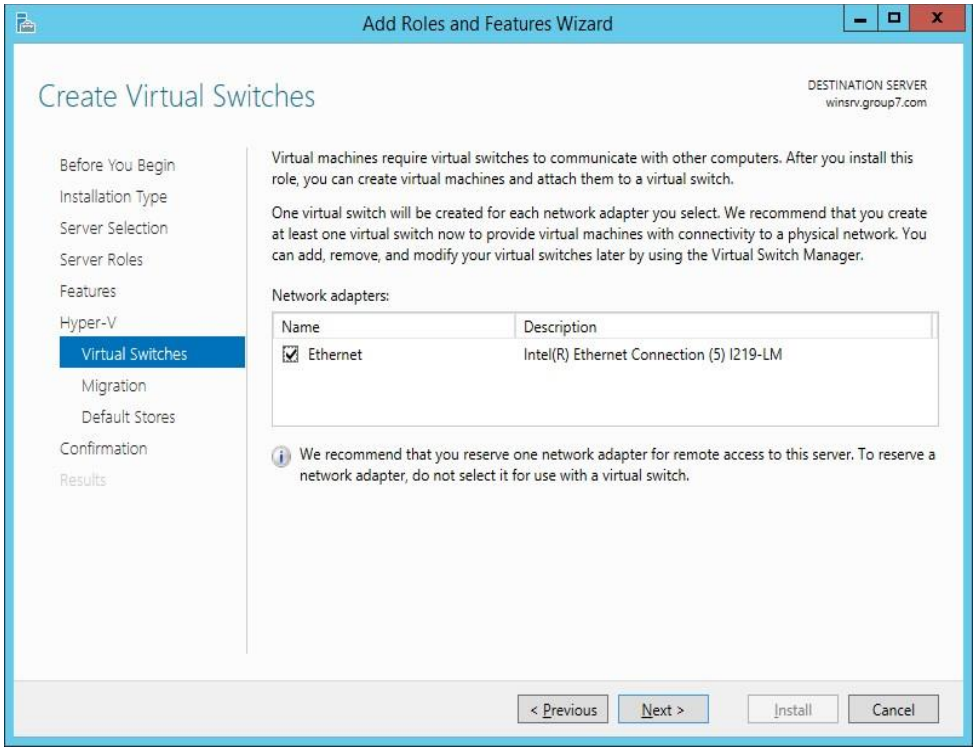


Figure 5. 7 : Virtual switch manager

Step 6: Click Use Credential Security Support Provide (CredSSP) for authentication protocol and then click next

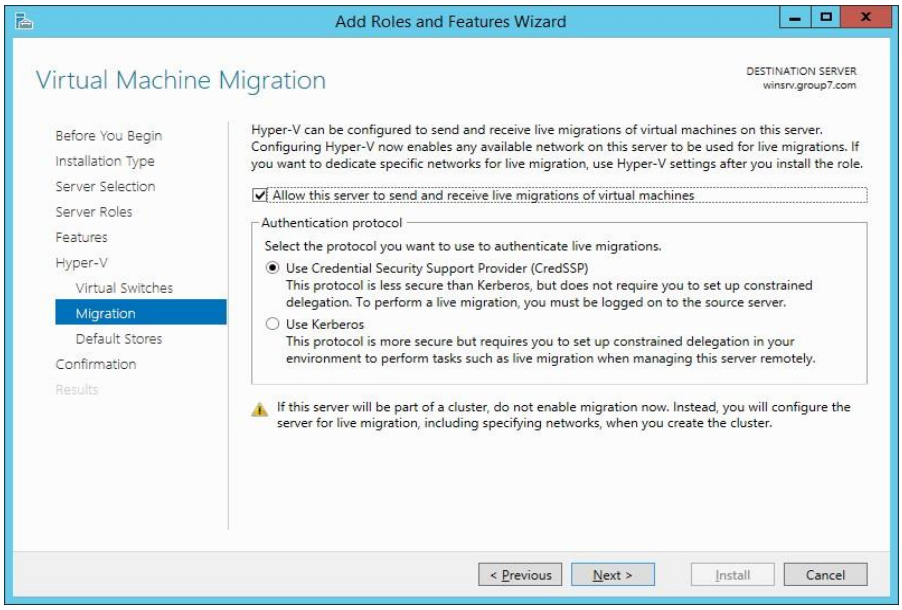


Figure 5. 8 : Authentication protocol

Step 7: Browse the default location for virtual hard disk files and virtual machine configuration files.

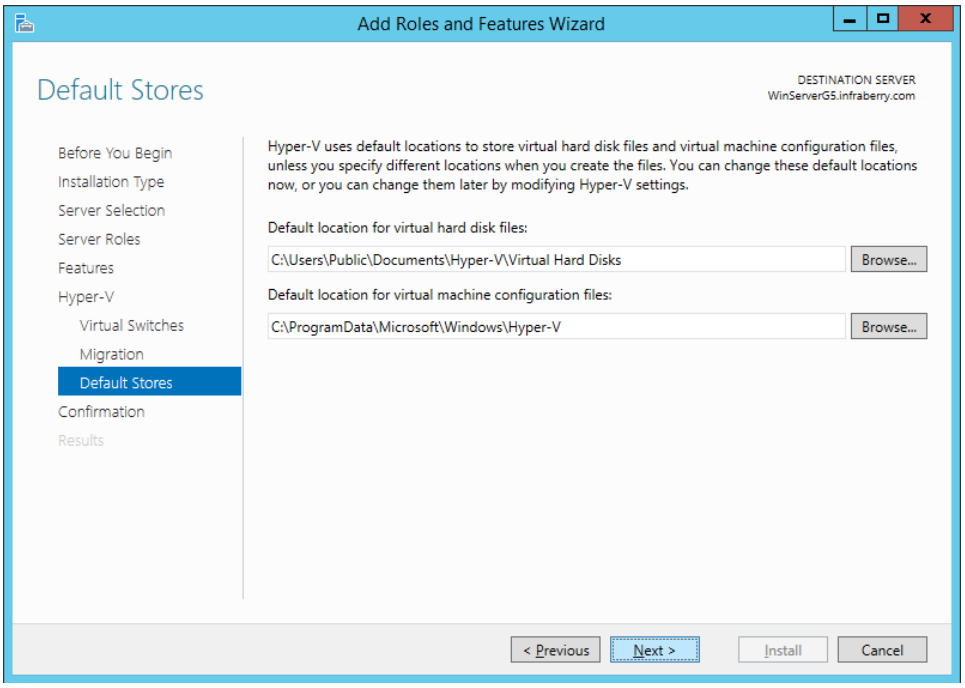


Figure 5. 9 : Default location for hard disk files

Step 8: Click install to install roles and features Hyper-V

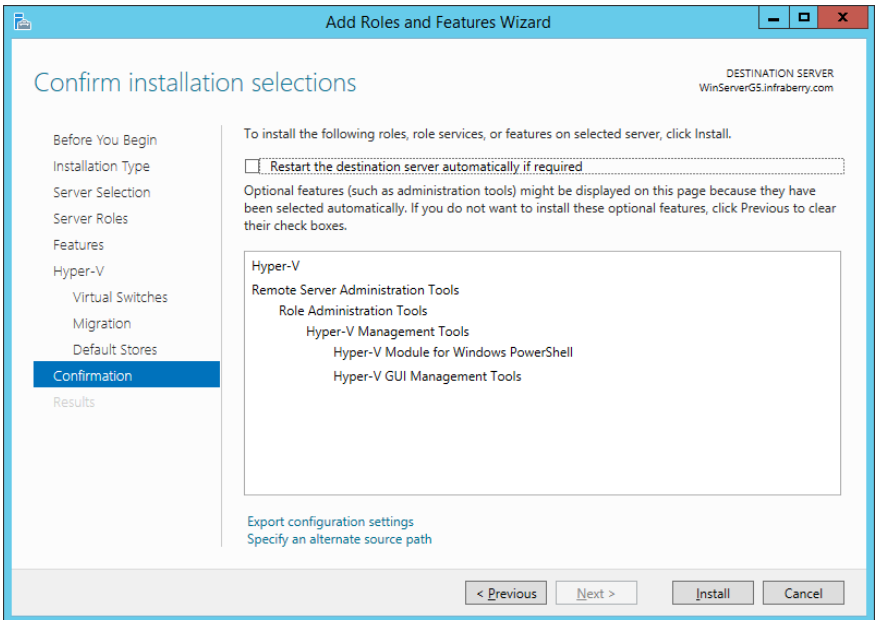


Figure 5. 10: Confirm installation hyperv

Step 9: After HyperV was installed, install a new virtual machine inside hyperV manager

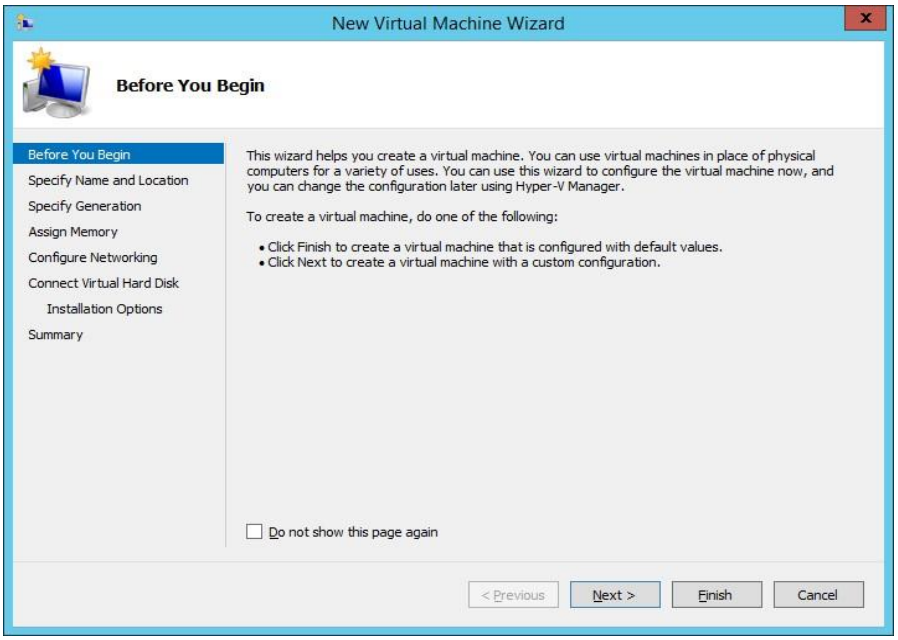


Figure 5. 11 : Install virtual machine

Step 10: Choose a name and location for the virtual machine. The name will display in Hyper-V manager

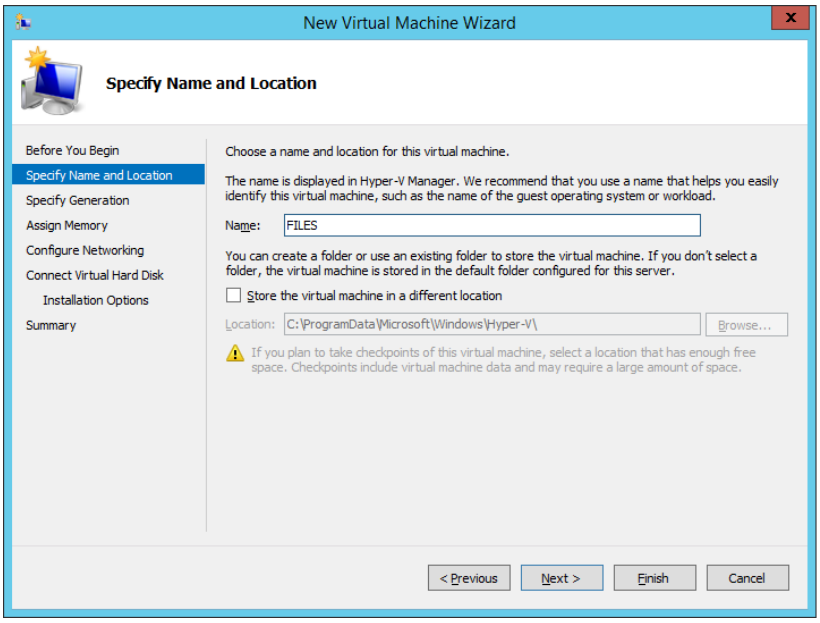


Figure 5. 12 : Name and location virtual machine

Step 11: Assign the memory to 8096 MB to improve the performance of the virtual machine

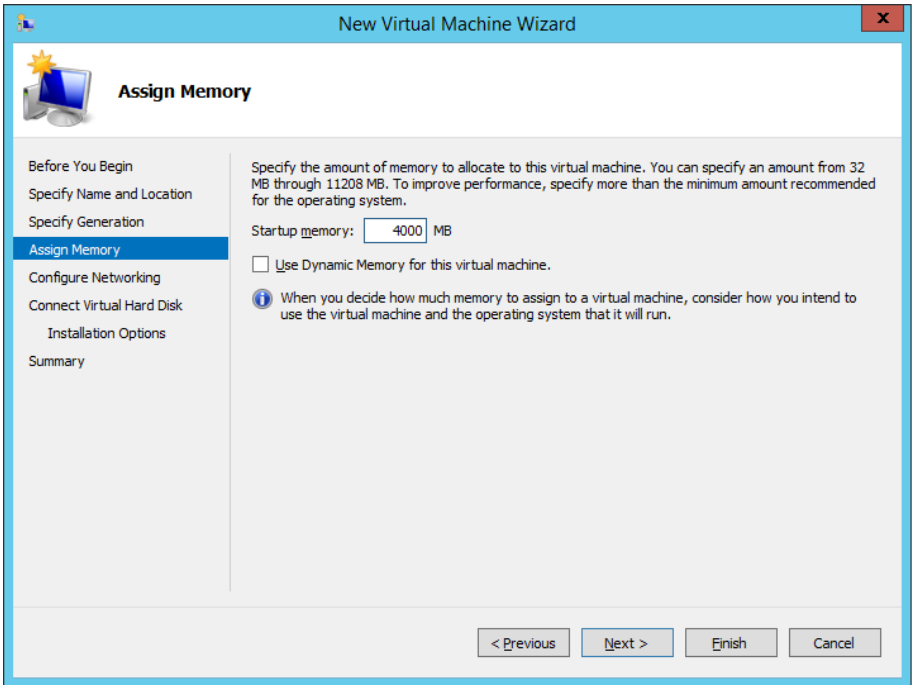


Figure 5. 13 : Assign memory

Step 12: Click on create a virtual hard disk then click next to continue

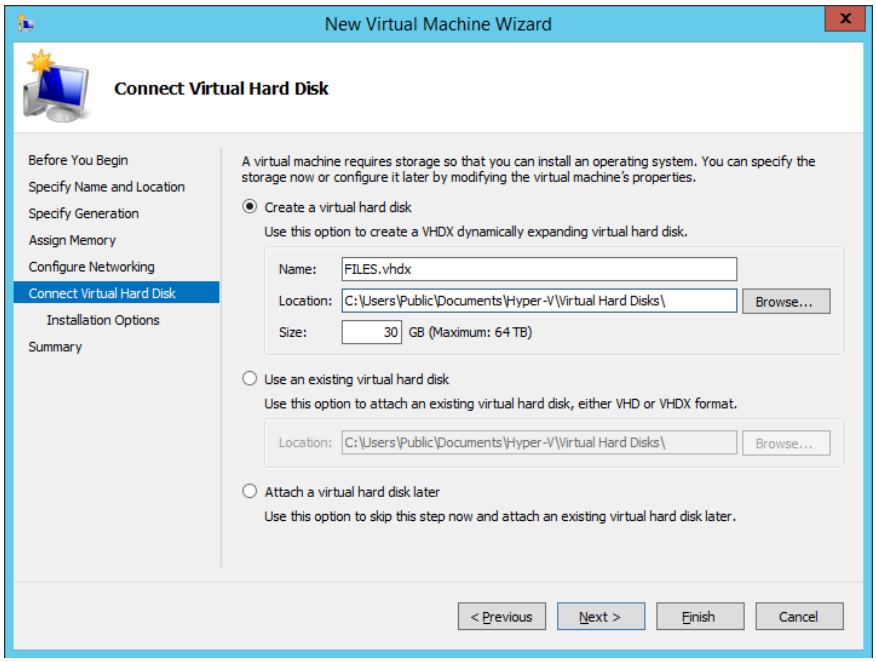


Figure 5. 14 : Create virtual hard disk

Step 13: After Windows Server successfully installed in HyperV then click finish

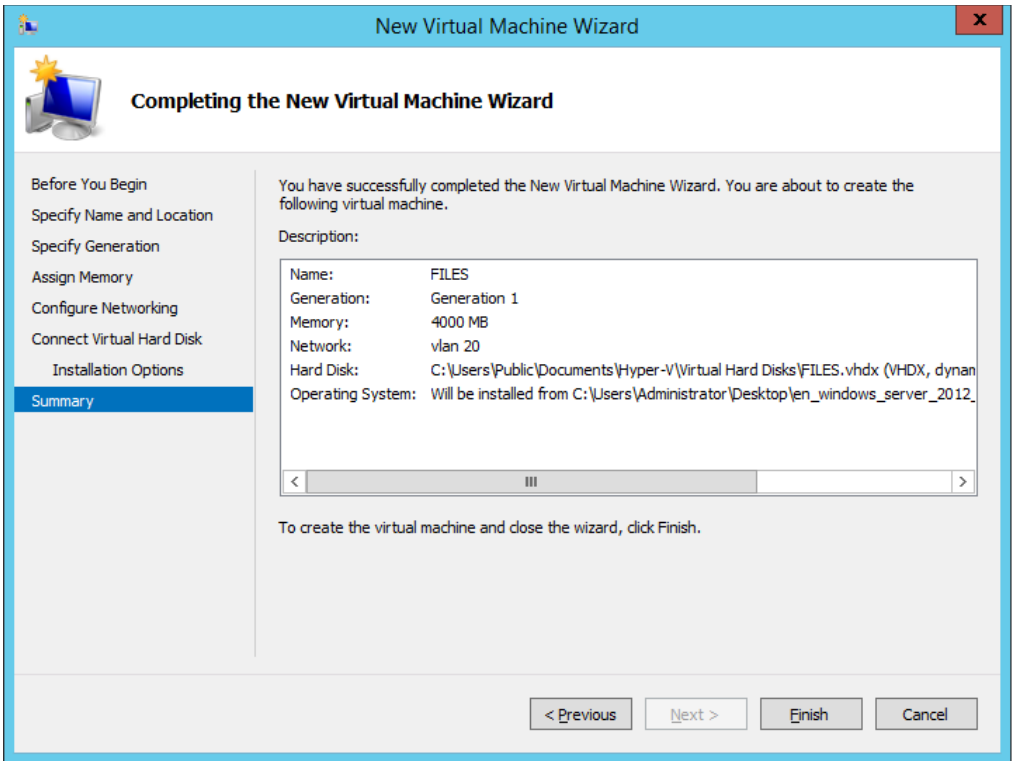


Figure 5. 15 : Windows Server installed

5.3.2 DOMAIN NAME SERVICE

Primary DNS

Step 1: Open server manager, click Start and select “Server Manager”. The Server Manager main windows will view the detailed snapshot of the server’s identity information, selected security configuration options, and installed roles and features.

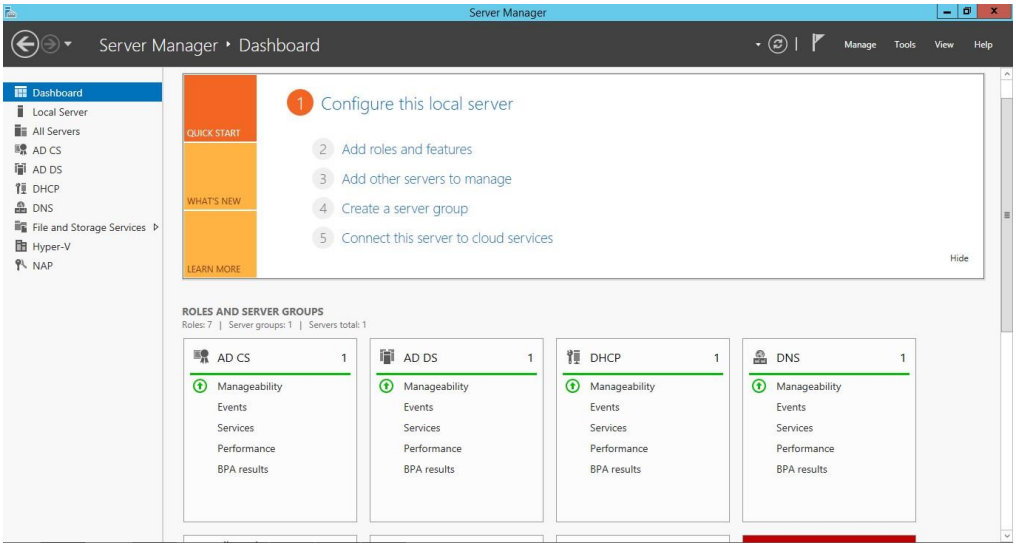


Figure 5-16: Main page Server Manager

Step 2: Click on Manage and click Add Roles and Features

The Roles Summary area of the Server Manager main windows shows a list of all roles that are installed on the computer. The names of roles installed on the computer are displayed. In the Roles Summary or Features Summary areas of the Server Manager main window, click either Add Roles or Add Features, depending on the software that we want to install.

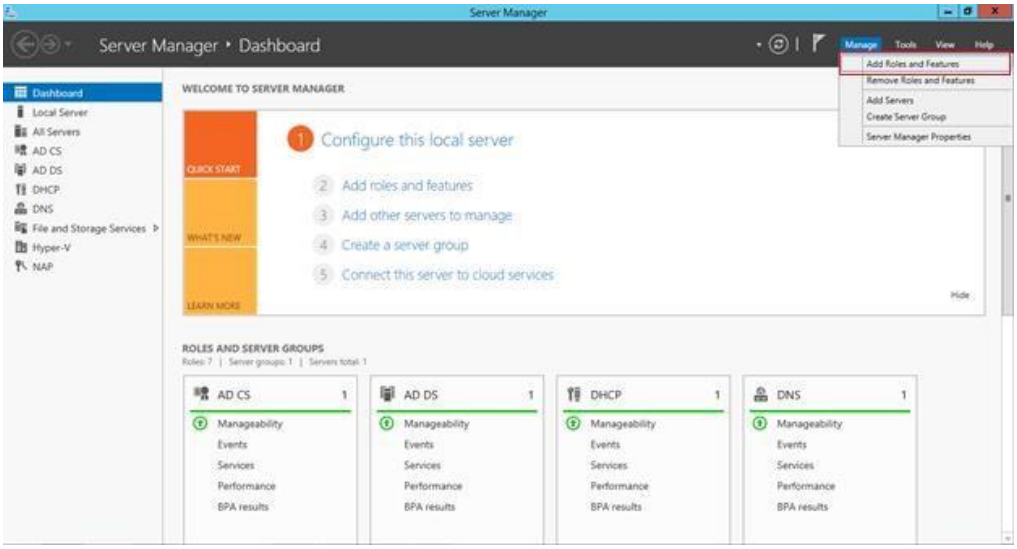


Figure 5-17: Select Add Roles and Features

Step 3: To select the installation type. For DNS servers, select the add roles and features, choose **role-based or** f**eature-based installation**

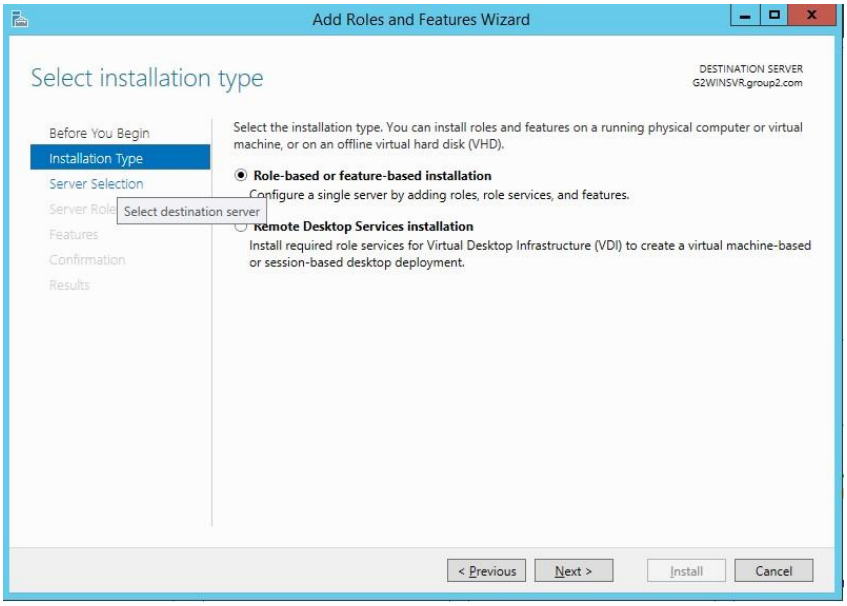


Figure 5-18: Installation type

Step 4: Add features in the DNS Server

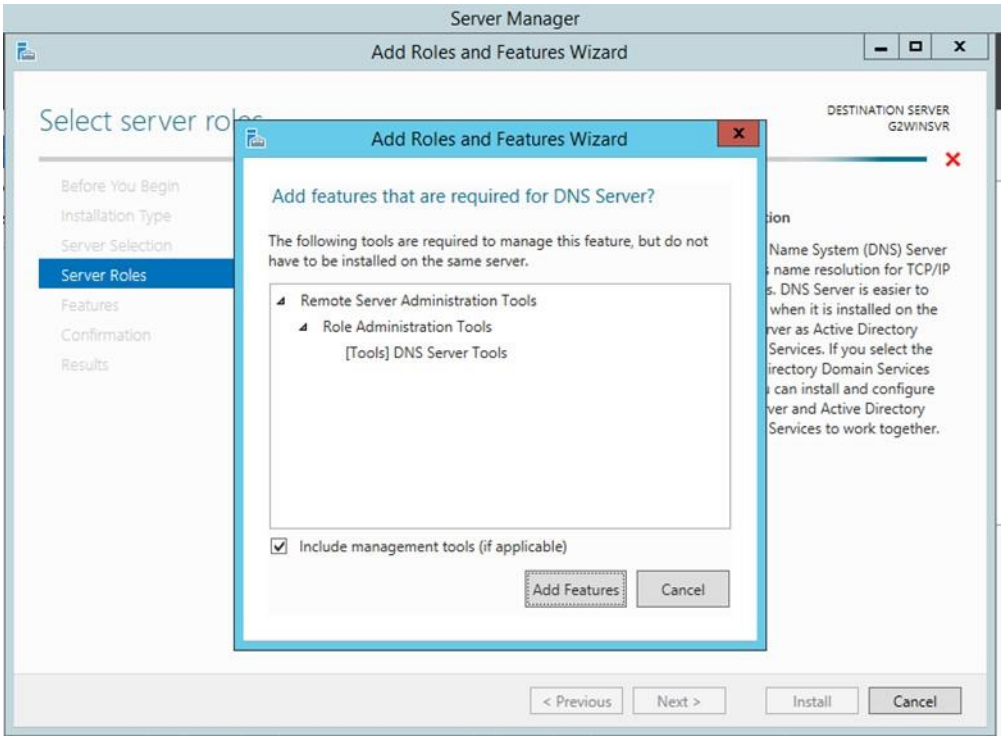


Figure 5-19: Add features

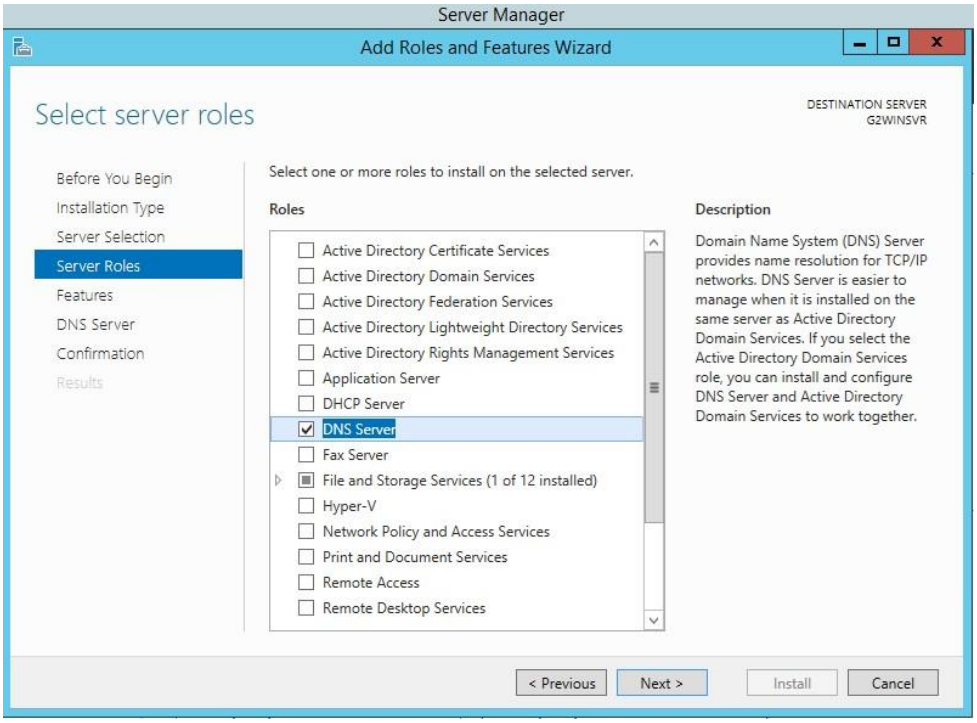


Figure 5-20: The feature

Step 5: Click next to finish the installation

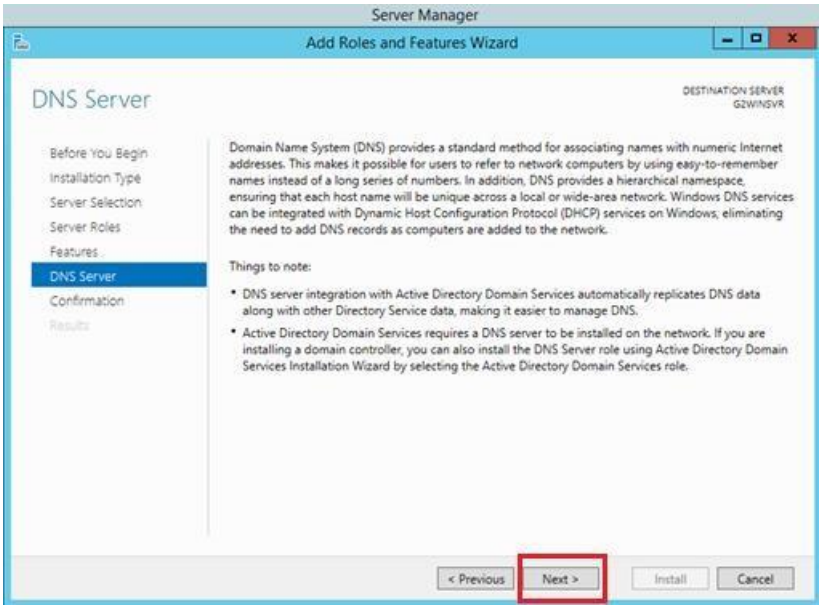


Figure 5-21: Click next

Step 6: Confirm installation of DNS server

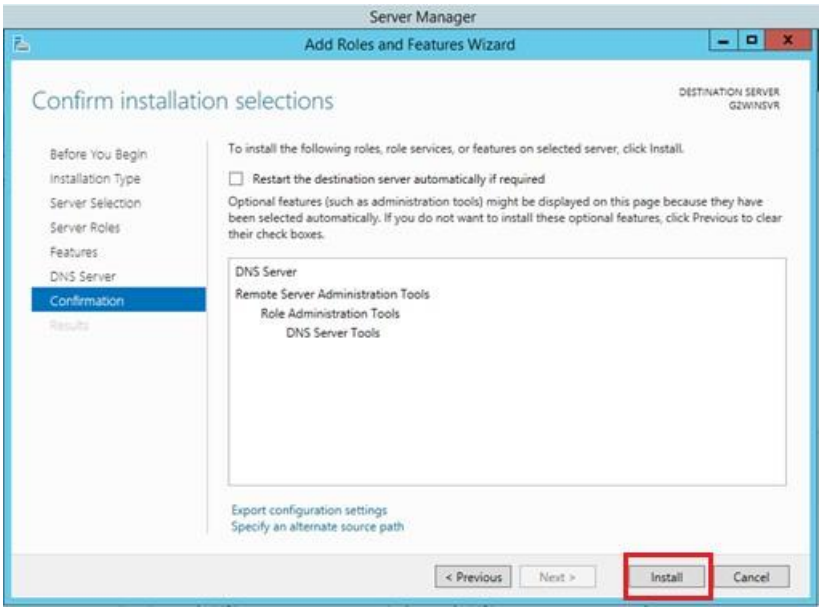


Figure 5-22: Confirm installation

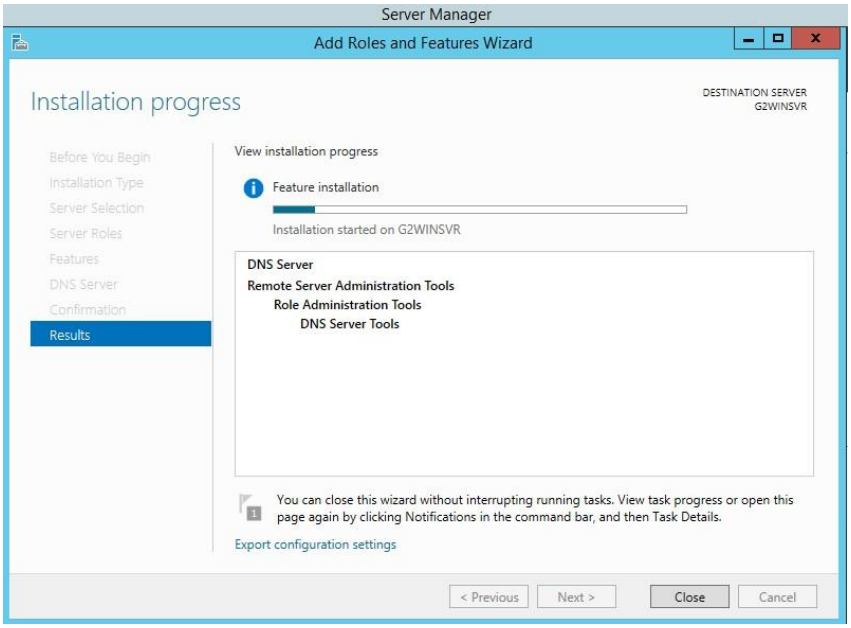


Figure 5-23: Installation process

Step 7: To create the forward lookup zone and click next to proceed.

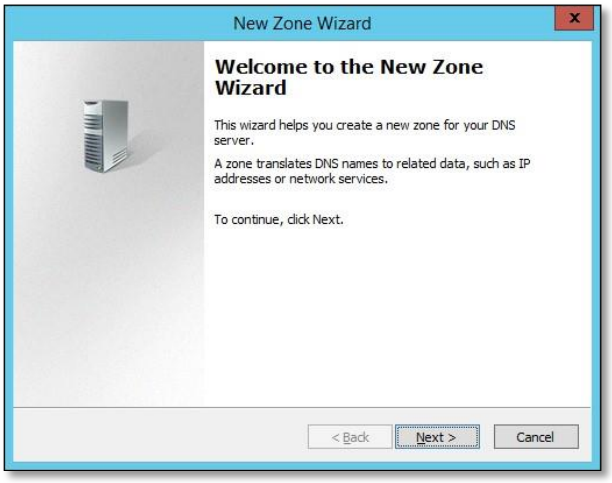


Figure 5. 24: DNS Server Wizard

Step 8: Select the primary zone then click button Next.

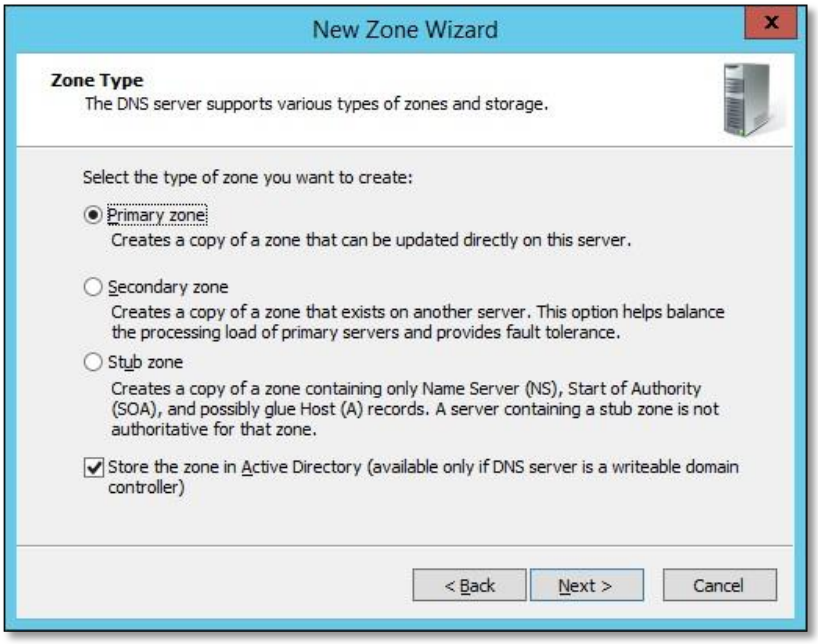


Figure 5. 25 Select zone

Step 9: Select how we want the zone to replicate.

Figure 5. 26: Select Active Directory Zone Replication Scope

Step 10: In Zone Name window enter the Group 5's Zone name: infraberry.com

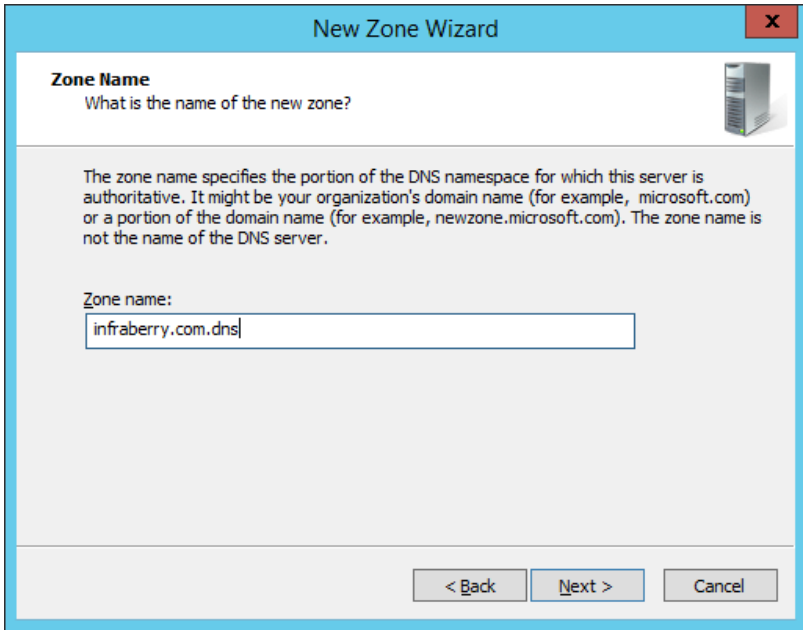


Figure 5. 27: Zone Name

Step 11: Select the type of dynamic updates you want to allow and click next.

Figure 5. 28: Dynamic Update

Step 12: In Configure a DNS Server Wizard click Next > to proceed

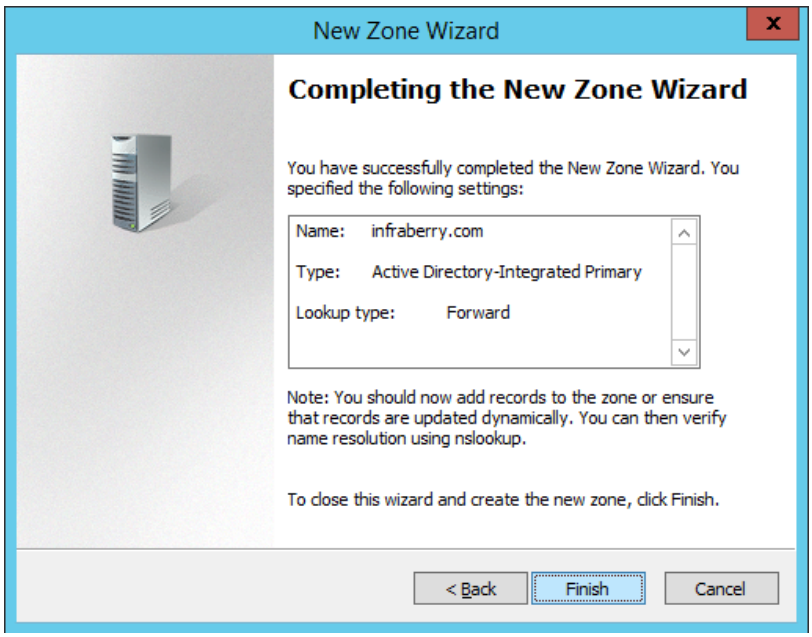


Figure 5. 29: DNS Server Wizard

Reverse Lookup Zones (IPv4)

Step 1: Next, we will add new zone for reverse lookup. Right click on Reverse Lookup Zone and click New Zone. Reverse lookup zone is the opposite way of Forward Lookup Zone.

When a computer requests the hostname of an IP address, the reverse lookup zone is queried, and the result is returned. When we create the reverse lookup zone, we specify this address in a format so that it can be recognized by the DNS server as pertaining to the address in a reverse lookup query.

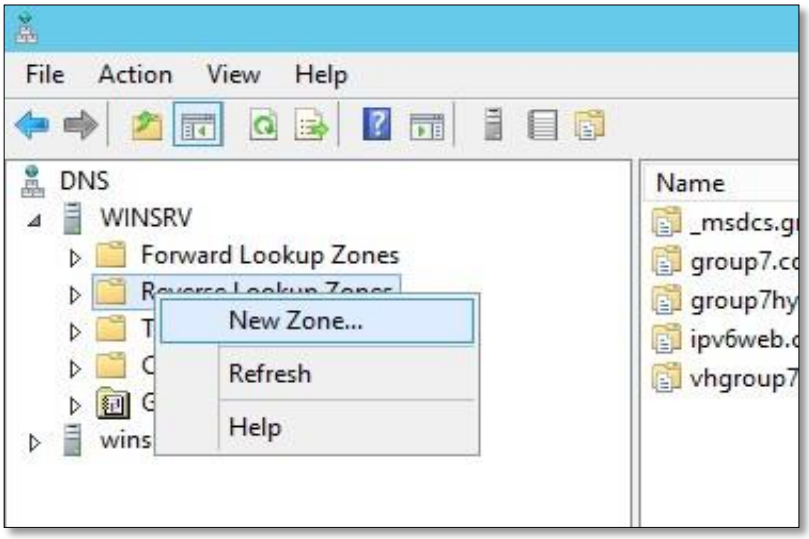


Figure 5. 30: New Zone (Reverse Lookup Zone)

Step 2: Next, we start create the reverse lookup zone.

Figure 5. 31: DNS Server Wizard

Step 3: Next, choose the primary zone and click next to proceed.

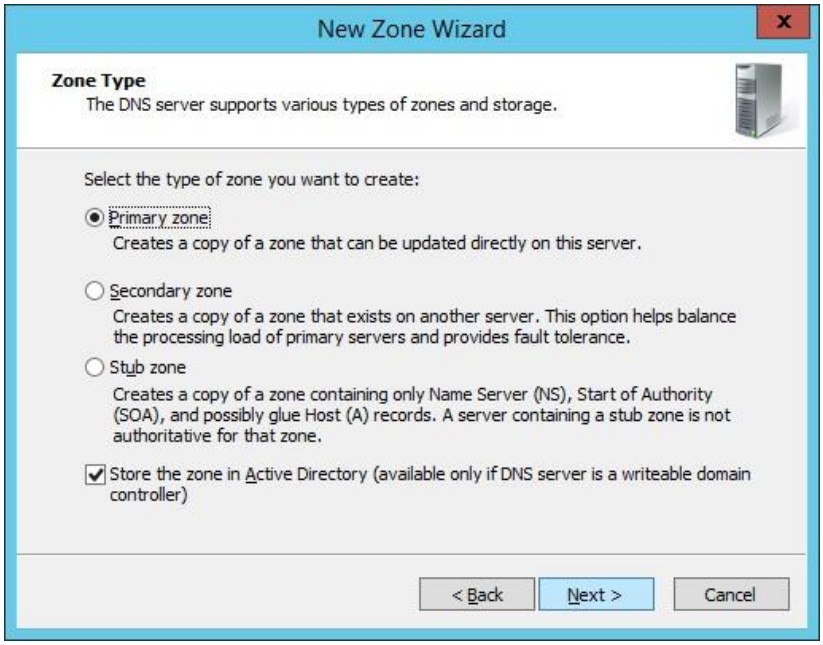


Figure 5. 32: Zone type

Step 4: Next, choose how we want the zone to replicate.

Figure 5. 33: Zone replication

Step 5: Next, we choose for IPv4 Reverse Lookup Zone and click Next>

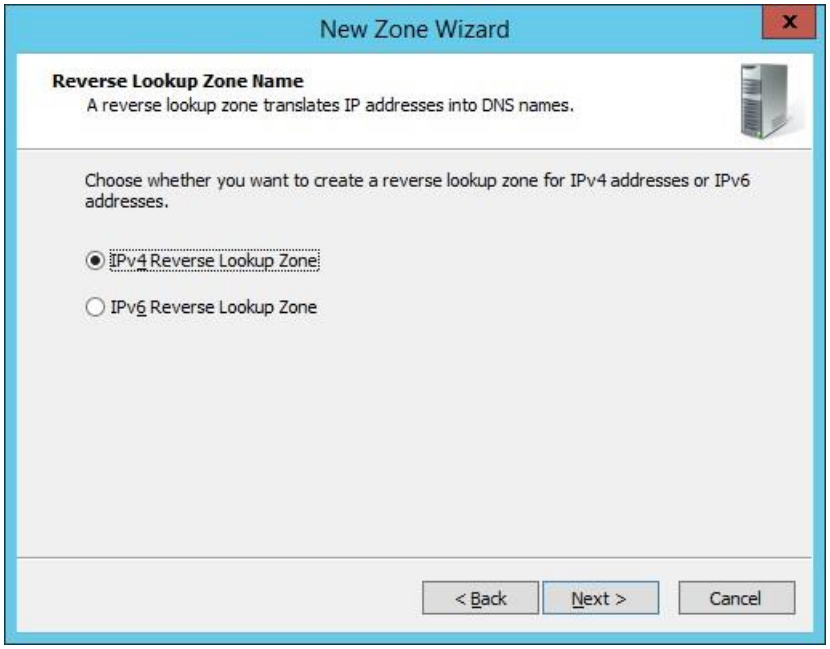


Figure 5. 34 **:** *Select IPv4 Reverse Lookup Zone Name (IPv4)*

Step 6: Then, we choose Network ID. Group 7's Network ID: 192.168.10.

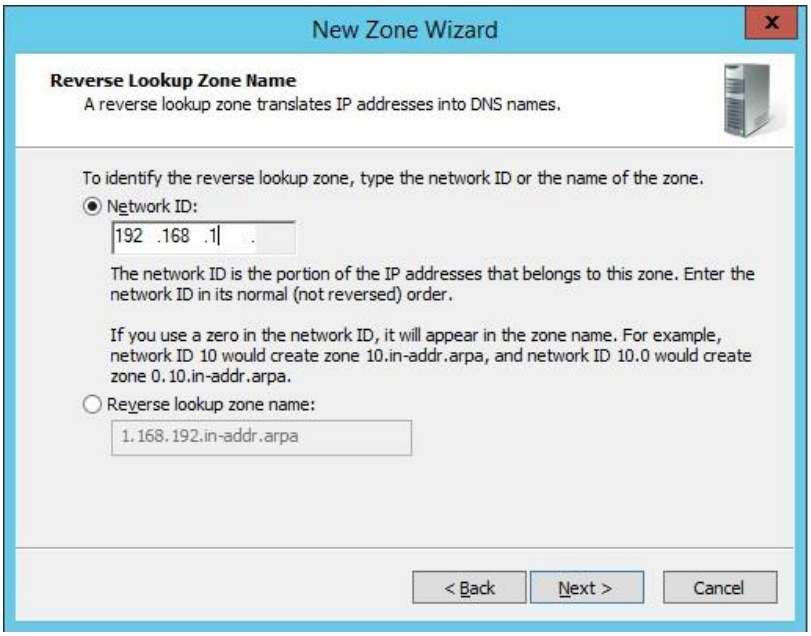


Figure 5. 35: Reverse Lookup Zone Name

Step 7: For Dynamic Update, choose to not allow dynamic updates and click Next.

Figure 5. 36: Dynamic Update

Step 8: In Completing the New Zone Wizard it will display the information we have created. Click Finish to end it.

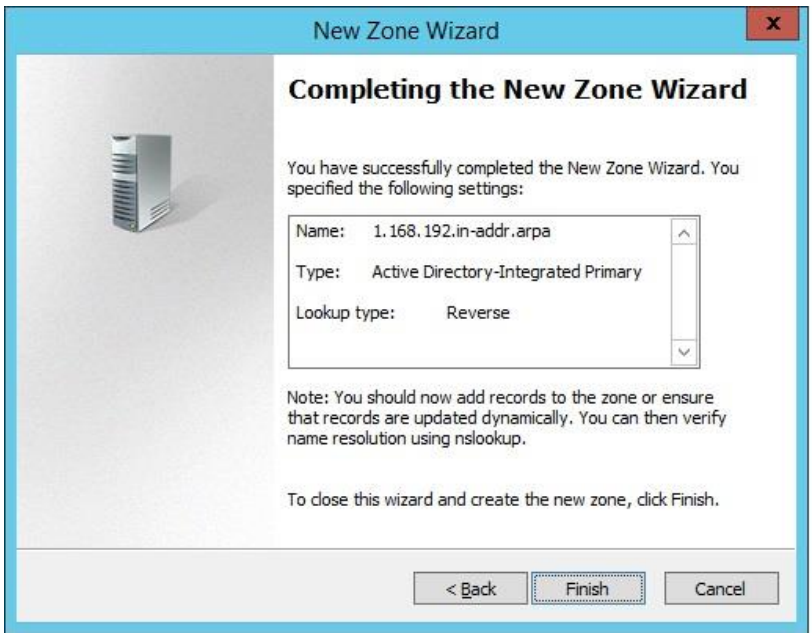


Figure 5. 37: Completing the New Zone Wizard

Step 9: Next, right click on Reverse Lookup Zones and click New Pointer (PTR).

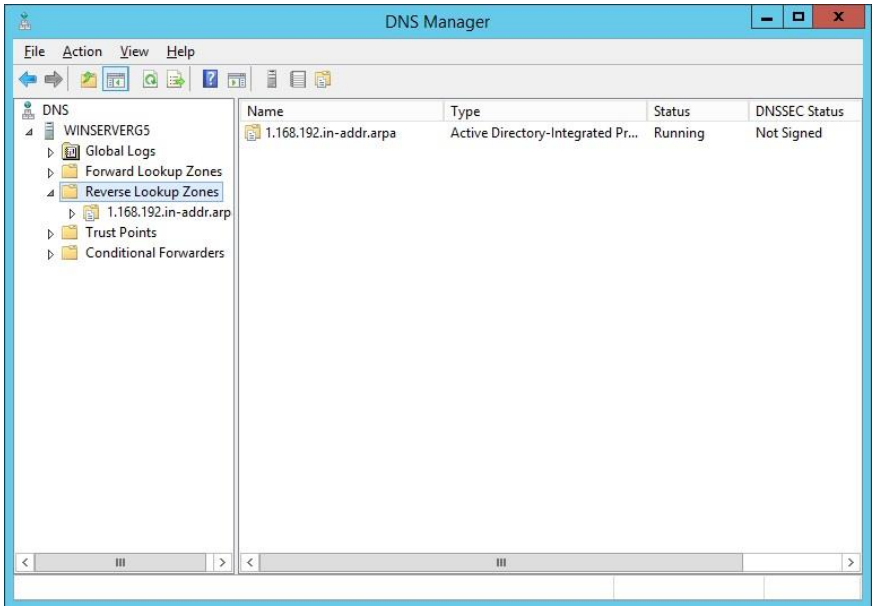


Figure 5. 38: Pointer (PTR)

Step 10: Enter the Host IP Address and host name. Then click OK.

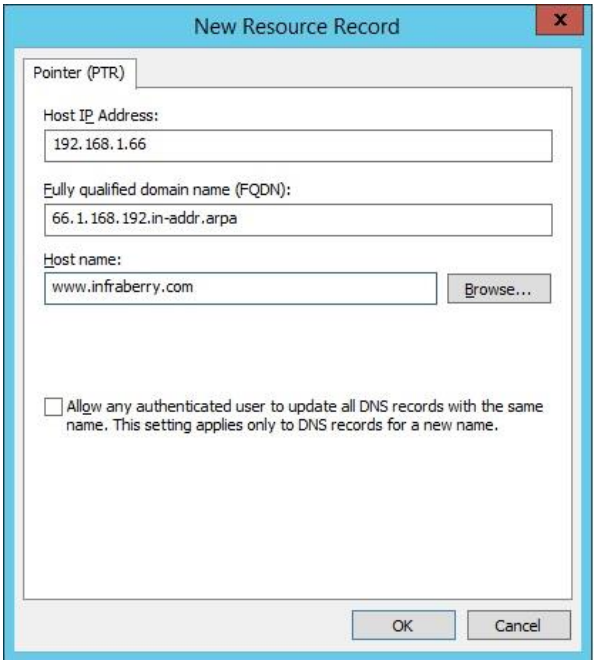


Figure 5. 39: Enter the Host IP Address

Step 11: Click on infraberry.com and right click then click on New Host (A or AAAA).

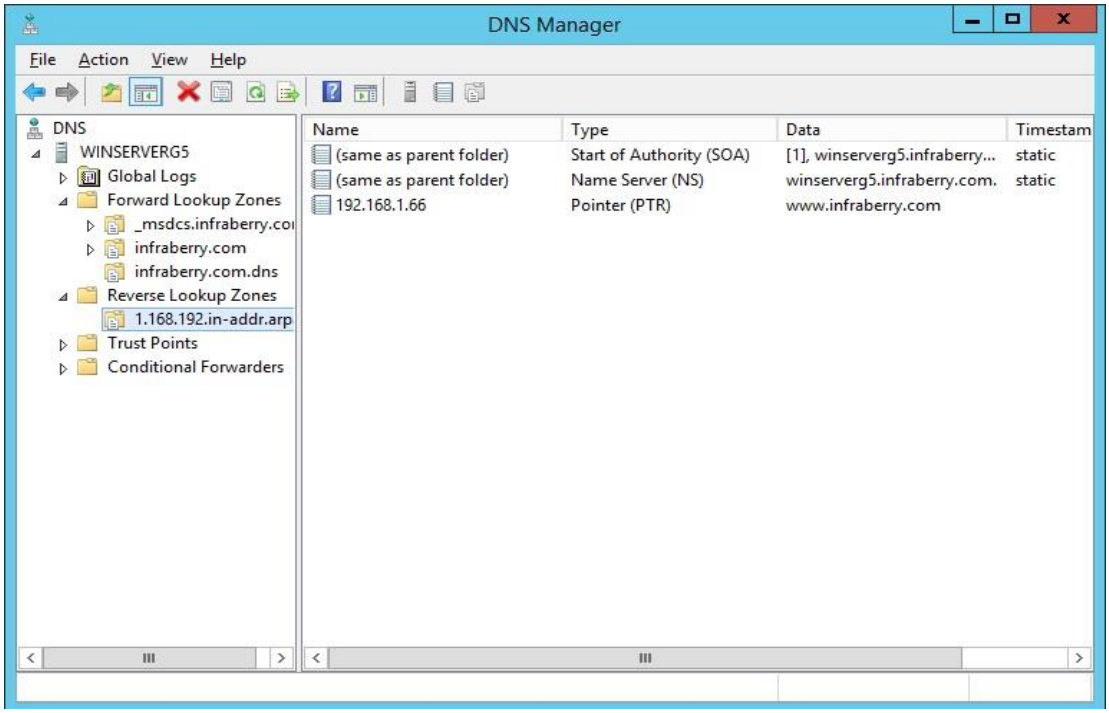


Figure 5. 40: New Host (A or AAAA)

Step 12: Enter the Name winsrv and IP address 192.168.1.10. Then click Add Host.

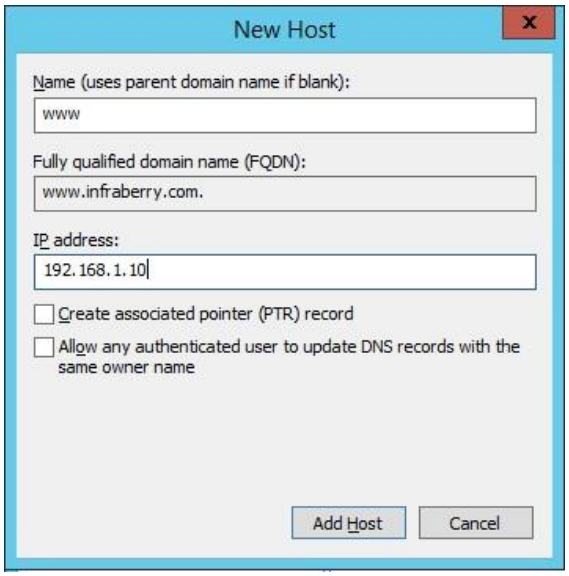


Figure 5. 41: New Host IPv4

Primary DNS - Forward Lookup Zones (IPv6)

Step 1: Right click on Reverse Lookup Zones and click New Zone.

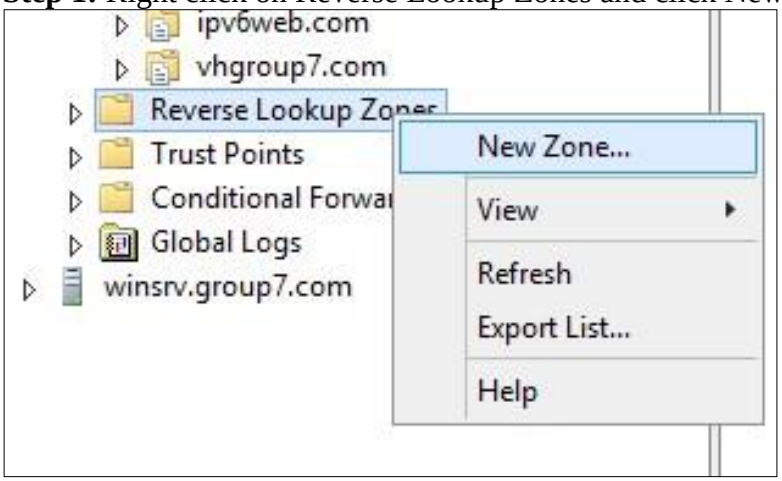


Figure 5. 42: New Zone

Step 2: In Welcome to New Wizard click Next>

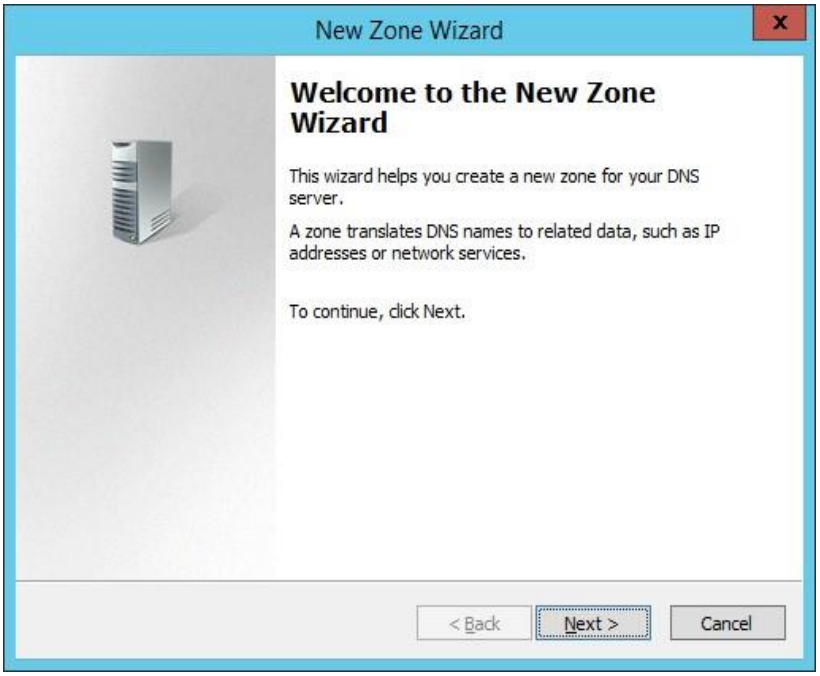


Figure 5. 43: Welcome the New Zone Wizard

Step 3: Then choose Primary zone. Tick on Store the zone in active AD. Then click next. We tick store the zone in Active Directory because DNS server running on domain controllers can store their zones in Active Directory Domain Services.

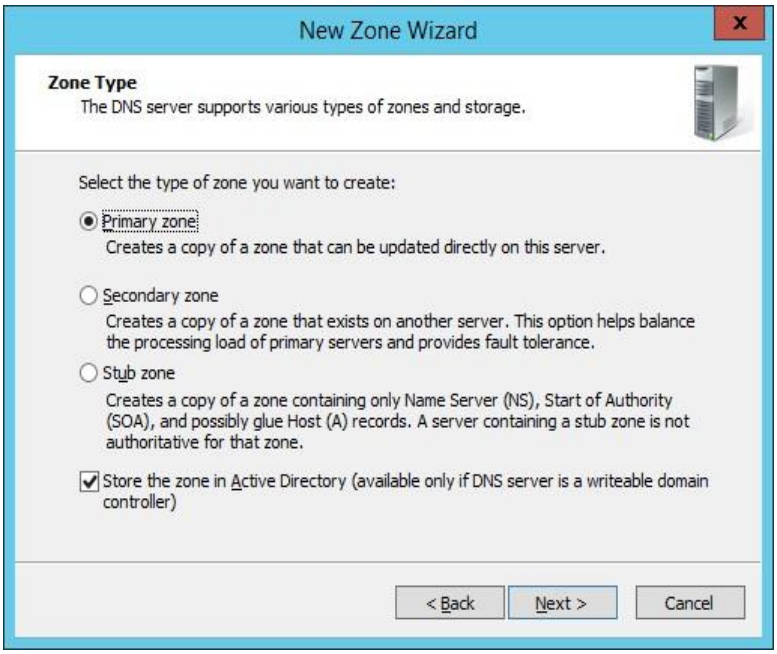


Figure 5. 44: Zone Type

Step 4: Select how we want the zone to replicate and click Next.

Figure 5. 45: Zone Type

Step 5: Next, choose IPv6 Reverse Lookup Zone.

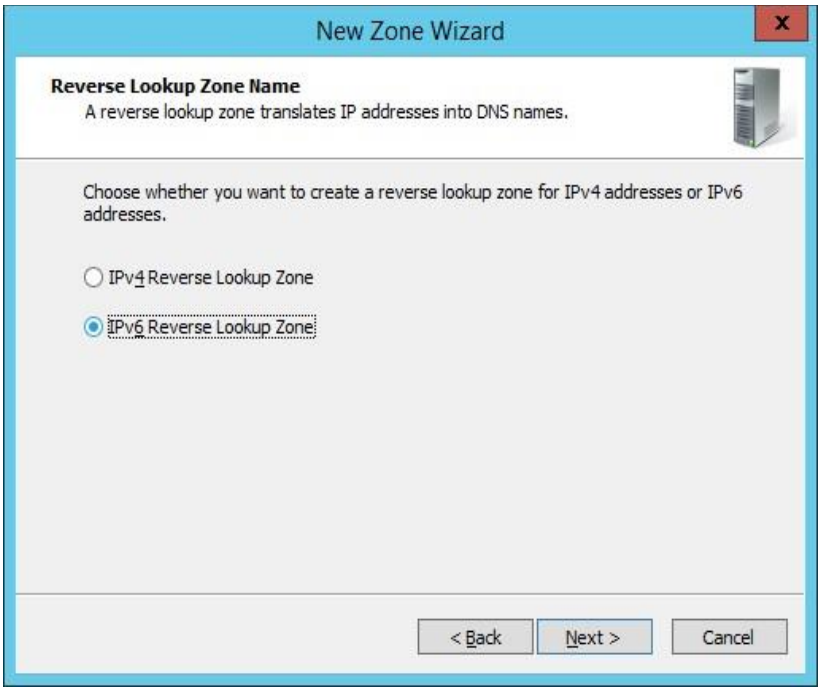


Figure 5. 46: IPv6 Reverse Lookup Zone

Step 6: In IPv6 Address Prefix, we enter 2340:1212:ABCD:1::/64 and Reverse Lookup Zones will automatically create.

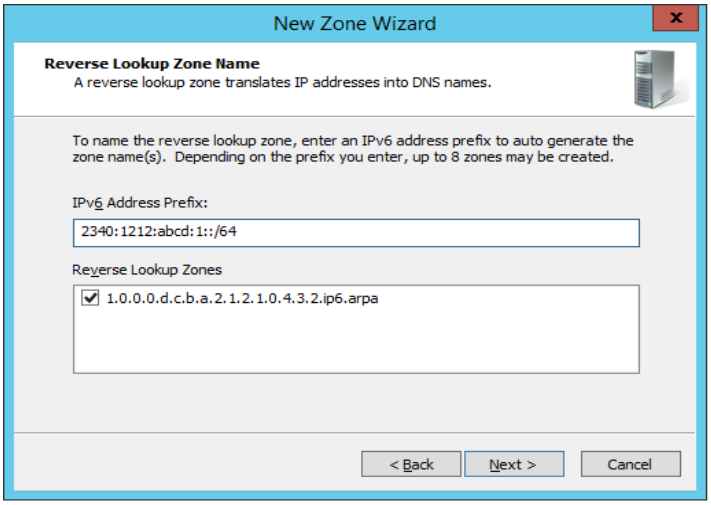


Figure 5. 47: IPv6 Address Prefix

Step 7: Select Allow both nonsecure and secure dynamic updates and click Next.

Figure 5. 48: Dynamic Update

Step 8: In Completing the New Zone Wizard click Finish to end it.

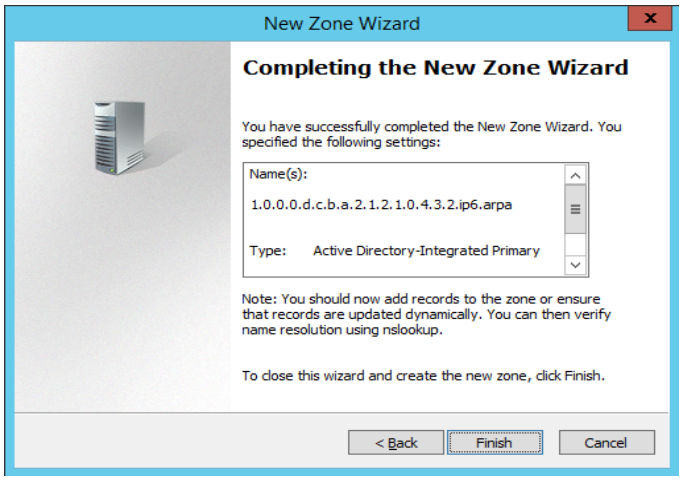


Figure 5. 49 : Completing the New Zone Wizard of IPv6 Reverse Lookup Zone

Step 10: Next, right click on IPv6 in Reverse Lookup Zones and click New Pointer (PTR).

PTR record resolves an IP address to a fully-qualified domain name (FQDN) as an opposite to what A record does which is the A record points a domain name to an IP address, the PTR record resolves the IP address to a domain/hostname. PTR records are also called Reverse DNS records.

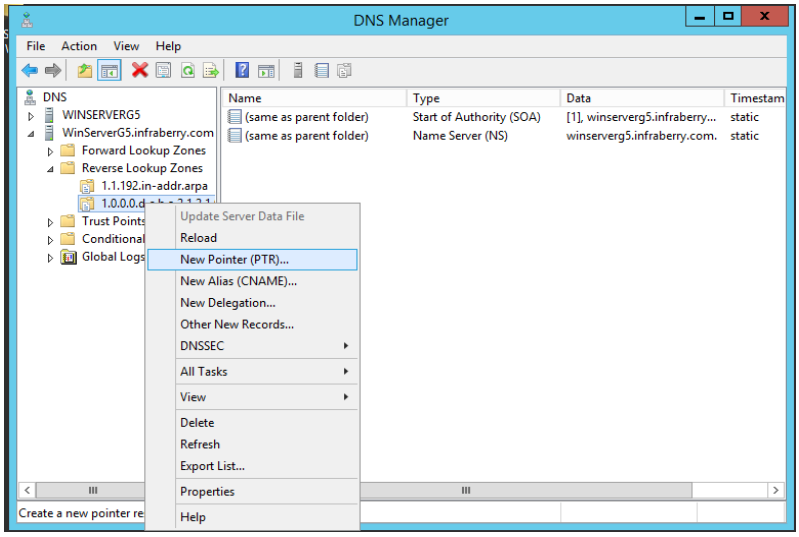


Figure 5. 50 New Pointer (PTR)

Step 11: Enter the Host IP Address and host name. Then click OK.

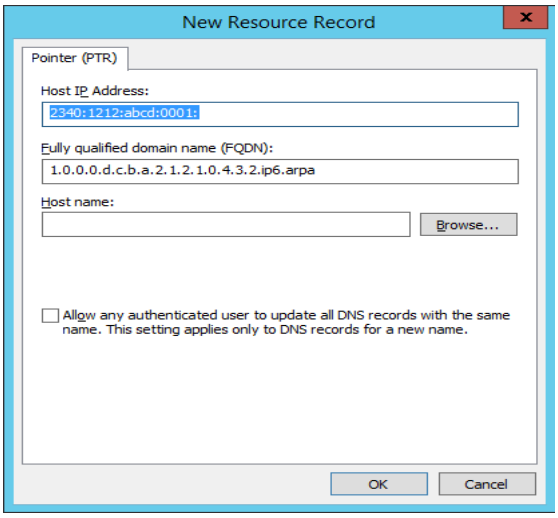


Figure 5. 51 Enter the Host IP Address and Host name

5.3.3 ROUTING & NAT

Step 1: Assign the NAT in each interface and sub-interface on Router.

```
#int f0/1
#ip address 125.126.127.9 255.255.255.248
#ip nat outside


#ip access-list standard NAT
#permit 192.1.1.0 0.0.0.63
#permit 192.1.1.64 0.0.0.15
```

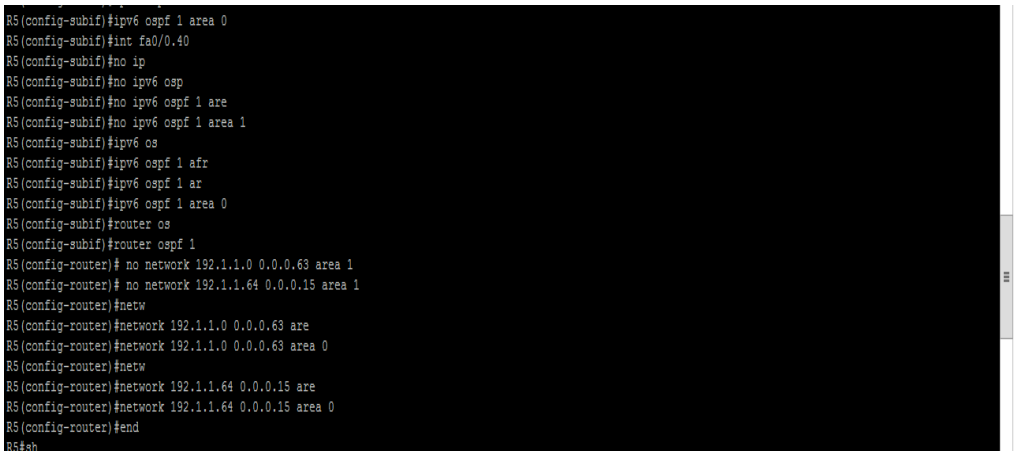


Figure 5. 52: Configuration of NAT.

Step 2: Display the configuration that have been configure using command *show run*.

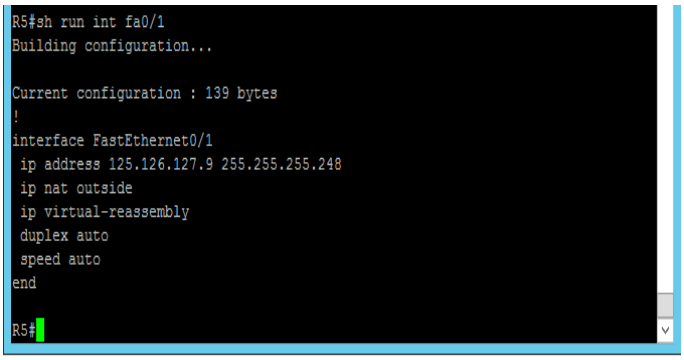


Figure 5. 53: List of cconfiguration

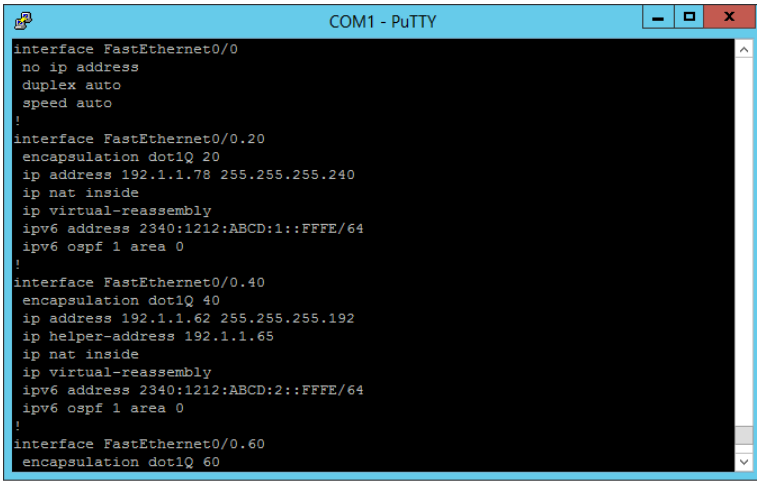


Figure 5. 54: List of cconfiguration

5.3.4 DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP)

5.3.4.1 DHCP IPv4

Step 1: Go to Start > Control Panel > Administrative Tools > Server Manager.

Step 2: Expand and Click on Roles > Add roles

Step 3: Choose Add Roles and features.

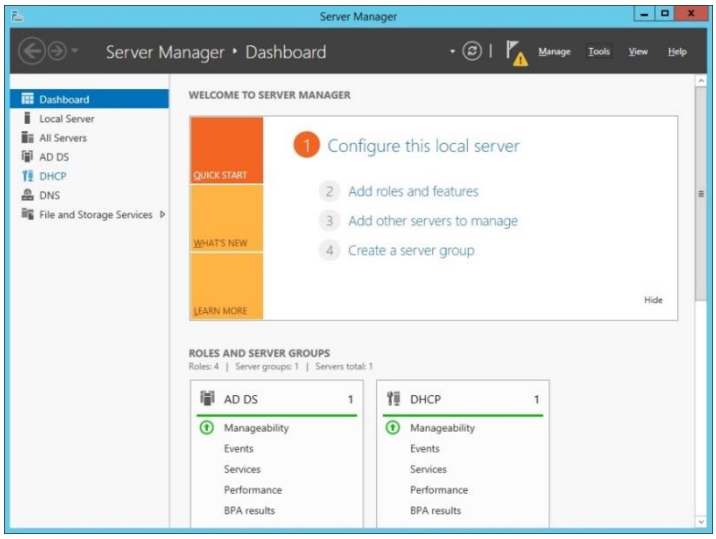


Figure 5. 55 : Add Roles

Step 4: Before you run the installation wizard, make sure that an administrator account has a strong password, static IP is configured, and security updates from Windows updates are installed. When you are done, click Next.

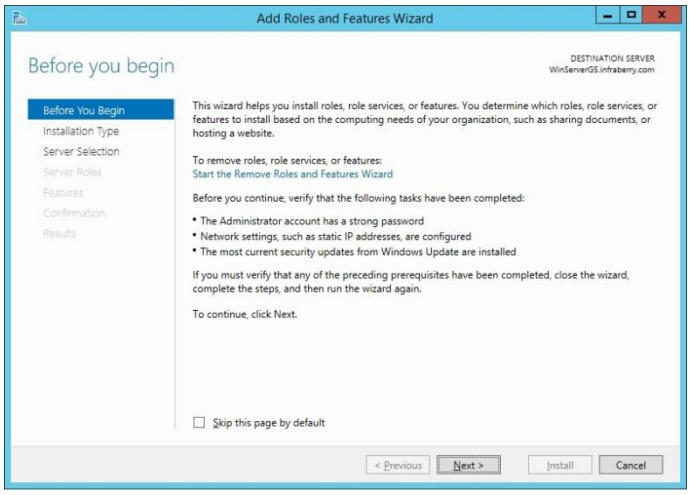


Figure 5. 56 : Before You Begin page

Step 5: Select Role-based or feature-based installation and click Next

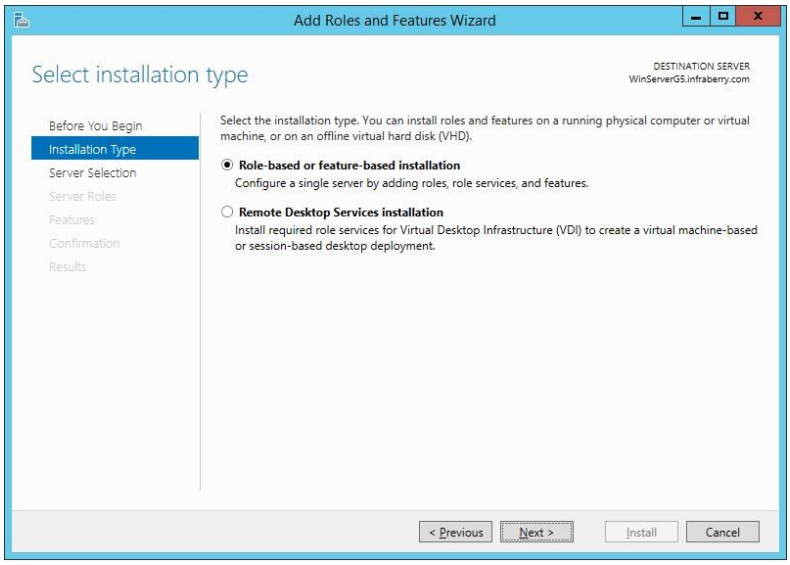


Figure 5. 57 : Select Server Roles page

Step 6: Select a destination server on which you want to install the DHCP server. In our case, there is only one server which is local server and it is selected by default. Click Next

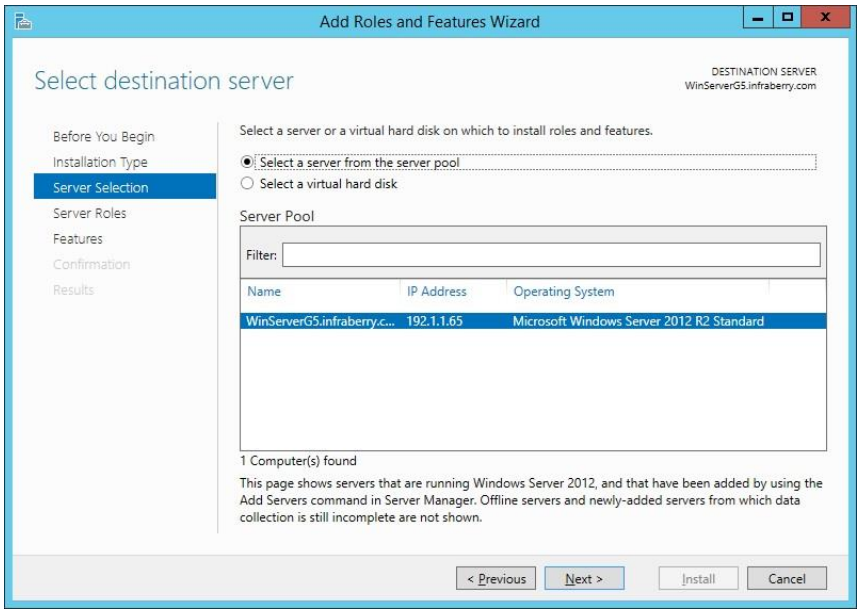


Figure 5. 58 : Select Network Connection Bindings page

Step 7: Open Server Manager and click notifications icon. A small window will appear. Click Complete DHCP configuration.

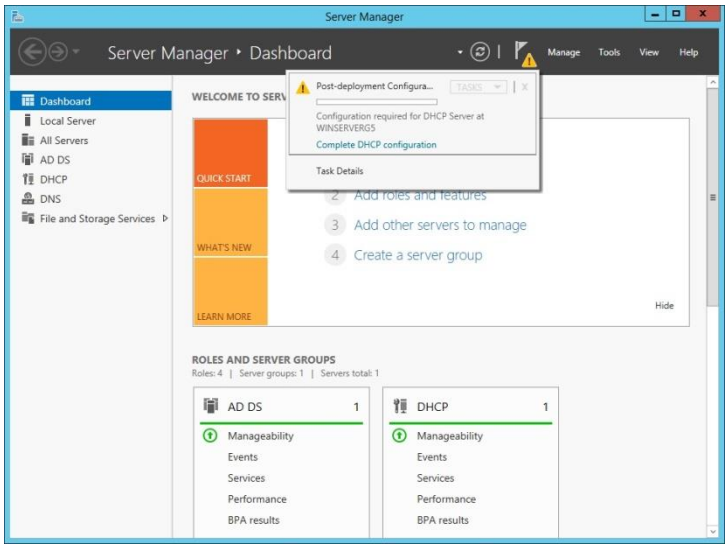


Figure 5. 59 : Open Server Manager

Step 8: Click Next

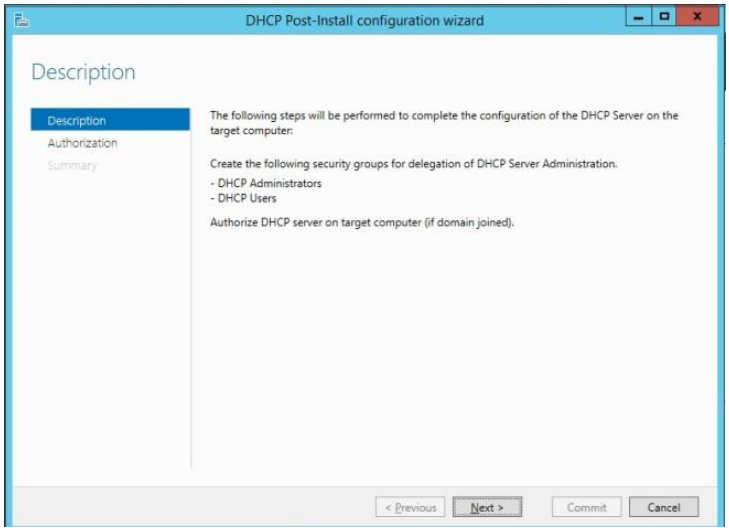


Figure 5. 60 : DHCP Post-Install configuration wizard

Step 9: Choose Skip AD authorization since we do not have any AD configured and click Commit

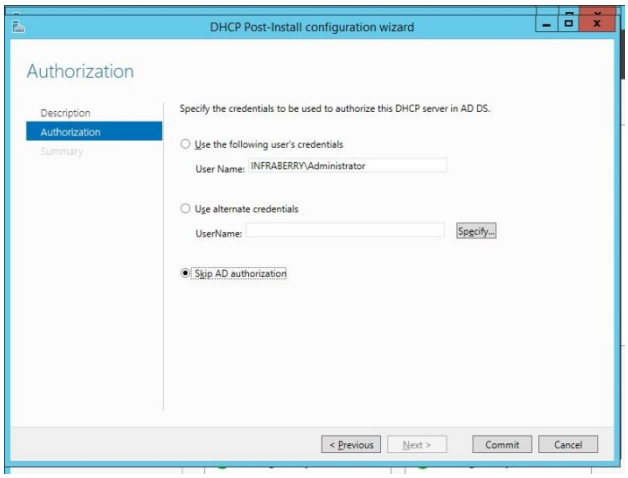


Figure 5. 61 : Skip AD authorization

Step 10: In management console, right click on IPv4 and scroll to New Scope and click it

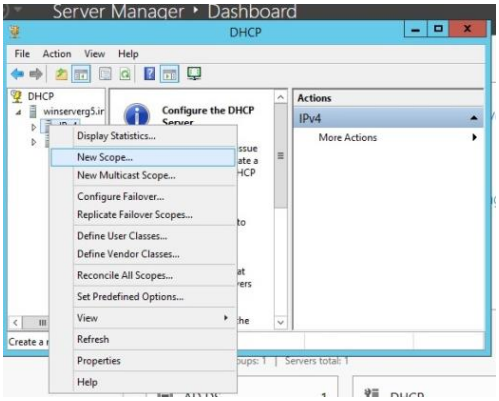


Figure 5. 62: Add new DHCP Scopes pages

Step 11: Click Next

Figure 5. 63 : New scope wizard pages

Step 12: Provide name and meaningful description of this new scope and click Next

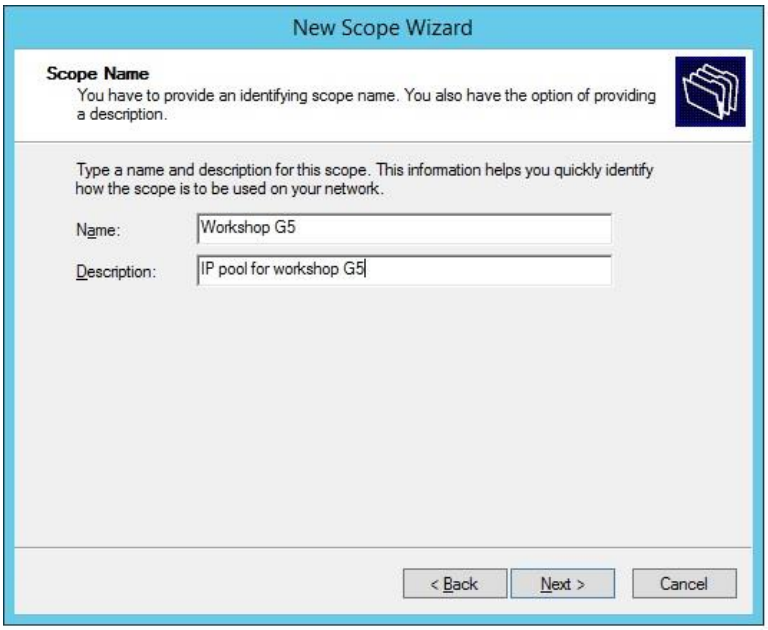


Figure 5. 64 : Scope name for DHCP IPv4

Step 13: Provide IP address range along with sub net you need to distribute to client machines and click Next

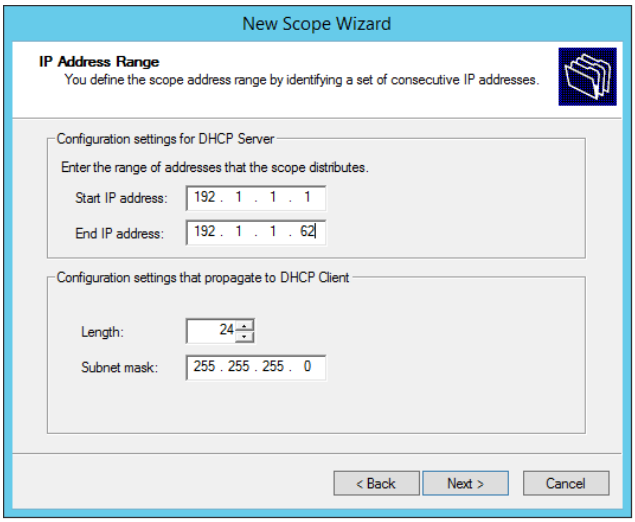


Figure 5. 65: Enter IP address range for DHCP

Step 14: Provide any IP addresses you need to exclude from pool and click Add. I have excluded a first IP address which is statically assigned to my DHCP server. Click Next

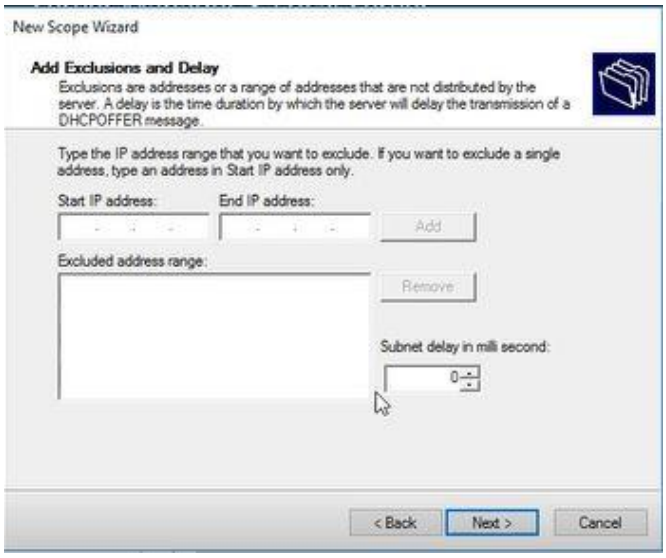


Figure 5. 66 : Add exclusion and delay

Step 15: Keep lease duration as 8 days and click Next.

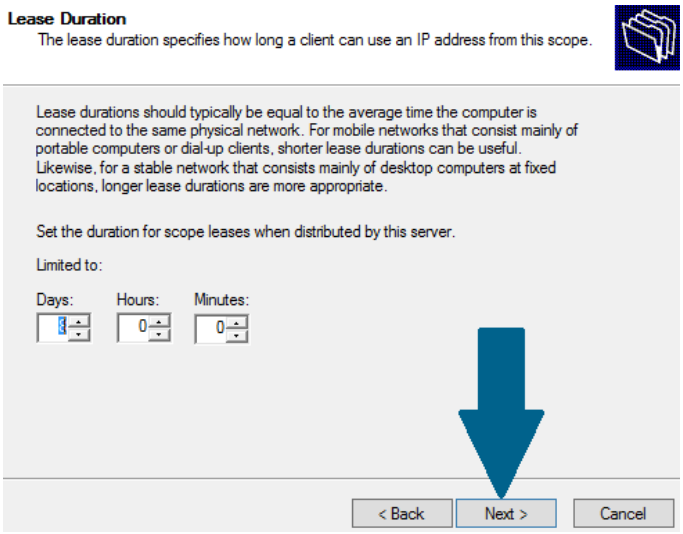


Figure 5. 67 : Lease duration

Step 16: Click Finish to end the new scope wizard.

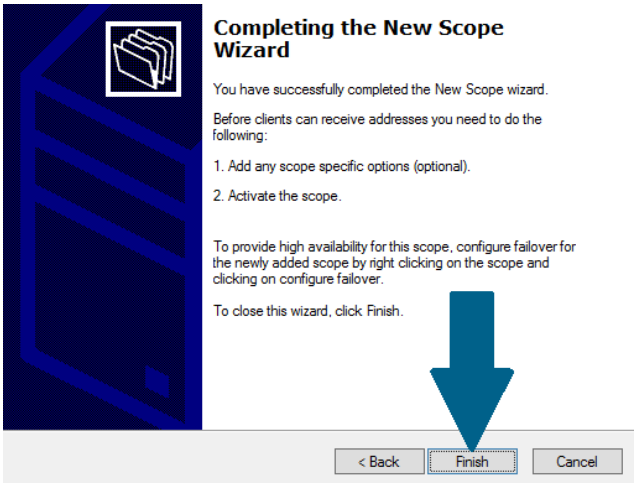


Figure 5. 68 : Completing the new scope wizard

Step 17: Right-click on new scope you just created in above step and click Activate.

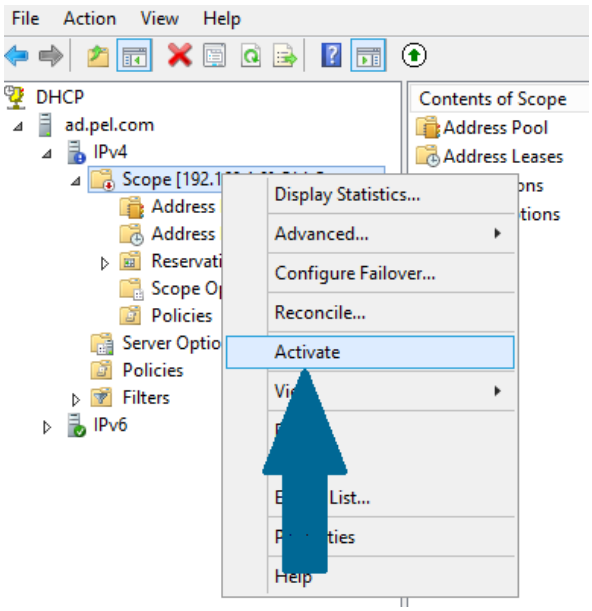


Figure 5. 69: Activated scope

Step 18: Right-click on your server, scroll to All Tasks and then click Restart to finish with configuration.

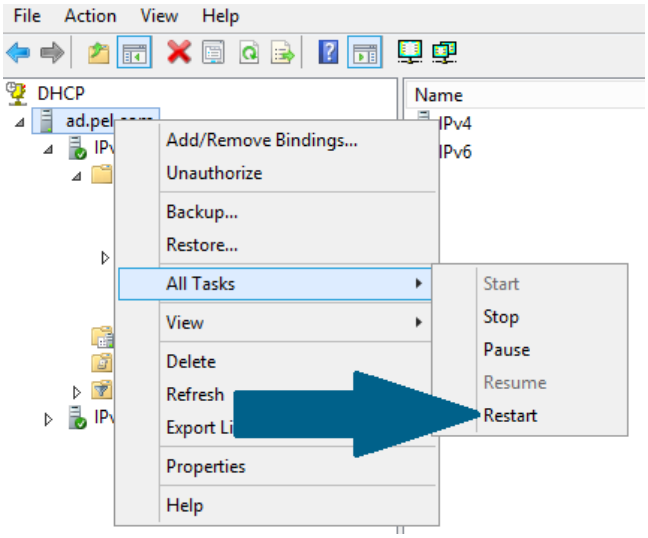


Figure 5. 70: Restart window server

5.3.4.2 DHCP IPV6

Step 1: In management console, right click on IPv6 and scroll to New Scope and click it

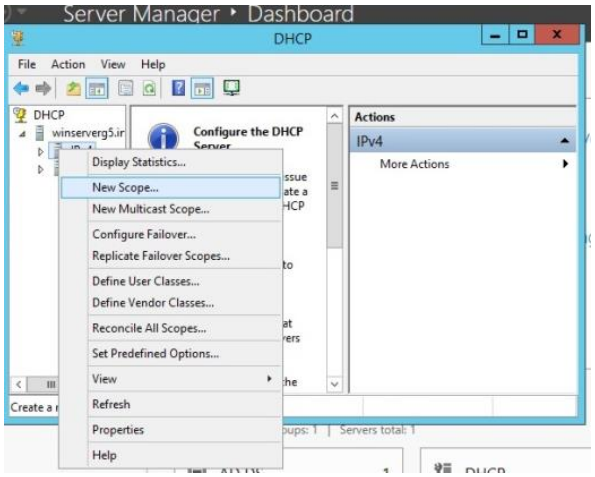


Figure 5. 71 : Add new DHCP Scopes pages

Step 2: Click Next

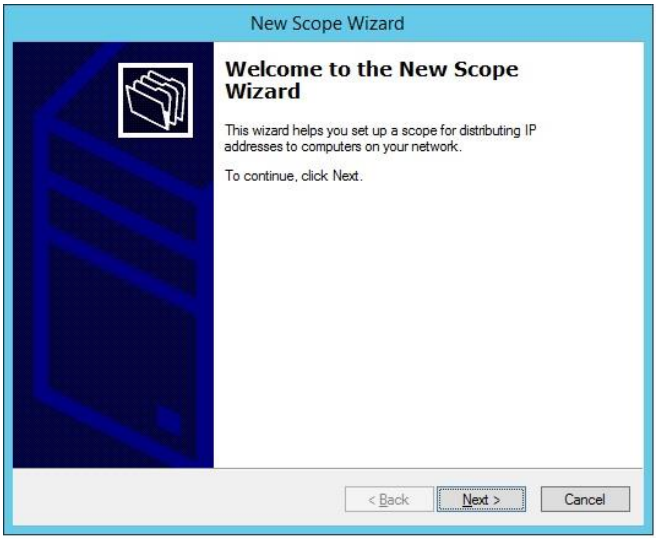


Figure 5. 72 : New scope wizard pages

Step 3: Provide name and meaningful description of this new scope and click Next.

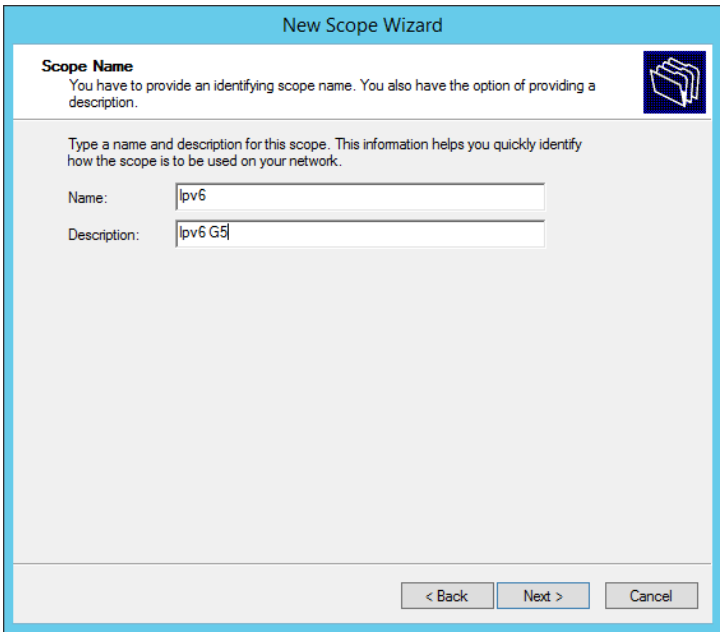


Figure 5. 73 : Scope name for DHCP IPv6

Step 4: Enter the IPv6 prefix addresses to the scope and click Next.

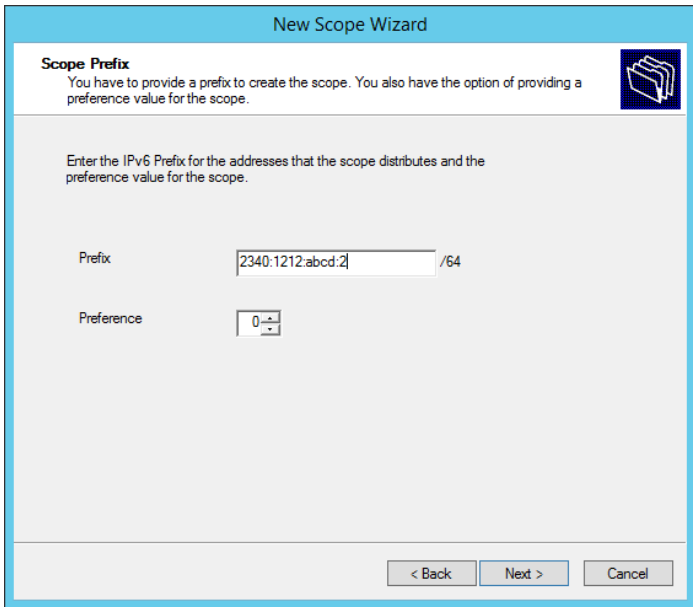


Figure 5. 74 : IPv6 prefix address

Step 5 : Provide any IP addresses you need to exclude from pool and click Add. I have excluded a first IP address which is statically assigned to my DHCP server. Click Next.

Step 6 : Available range for DHCP IPv6.

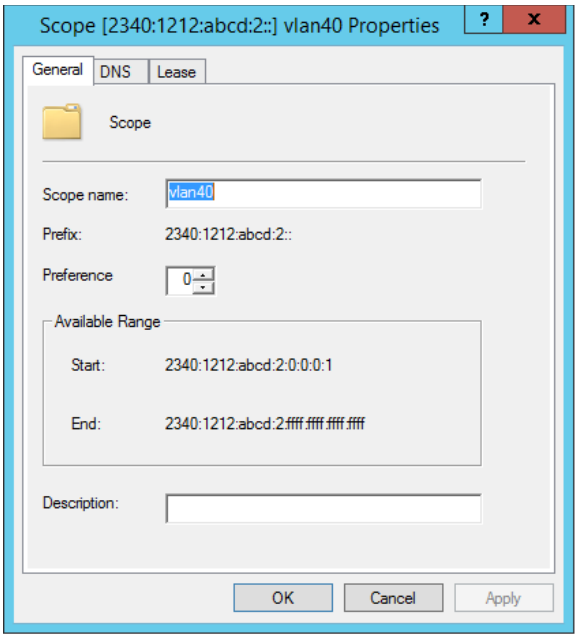


Figure 5. 75 : Range for DHCP IPv6

5.3.5 IPV6 WEB WITH IPV6 TUNNELLING

Step 1: Go to Start -> Administrative Tools -> IIS Manager

Step 2: At ISS manager > Right click at site and click to Add Web Site > Fill the requirement

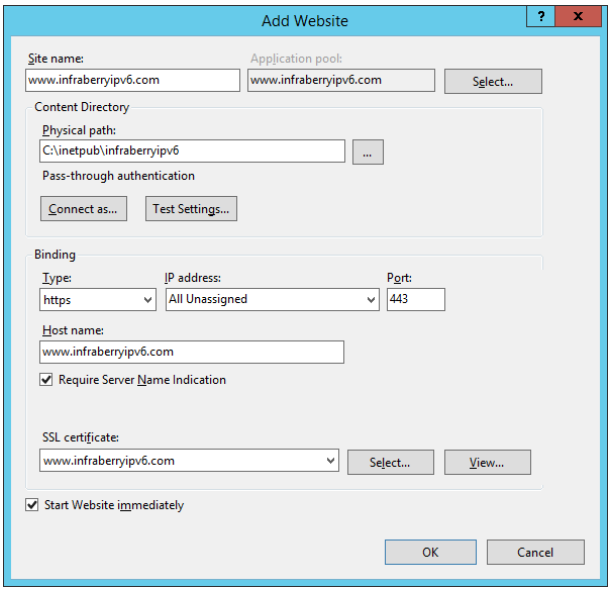


Figure 5. 76 : Add Web Site

Step 3: After finish new website has been created with name www.infraberryipv6.com

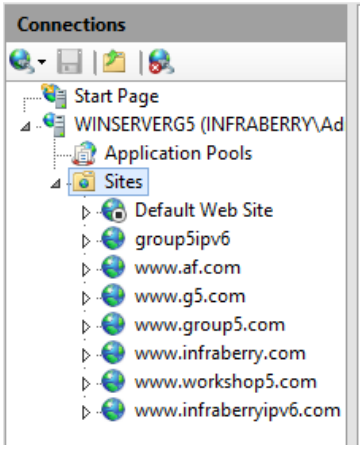


Figure 5. 77 : Web site has been created.

Step 4: After finish new website has been created with name www.infraberryipv6.com

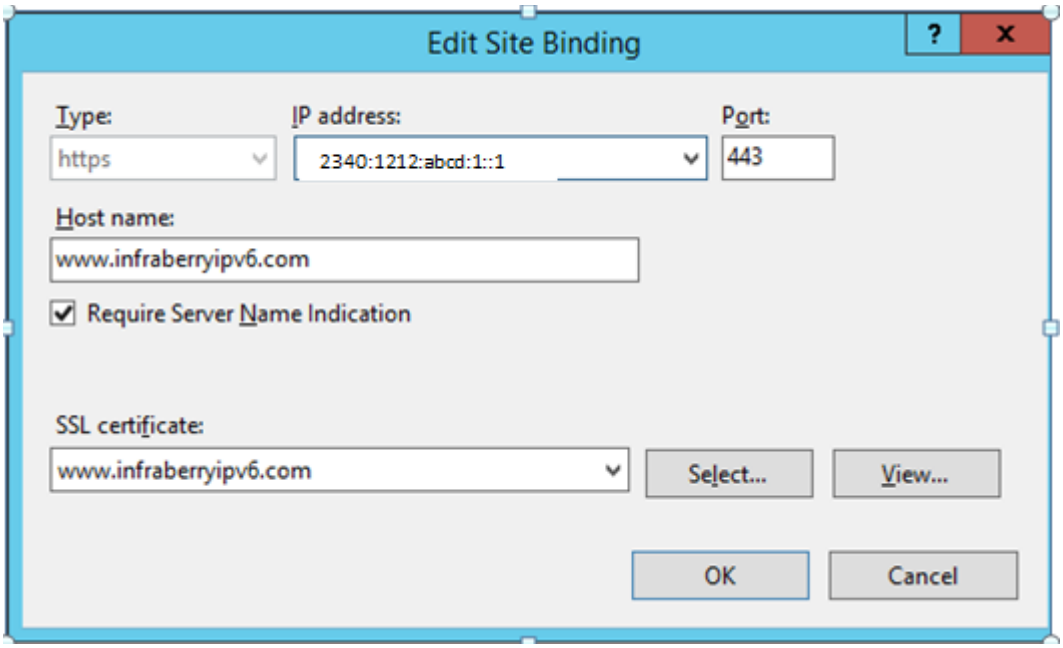


Figure 5. 78 : Edit Bindings

Step 5: Create certificate for www.infraberryipv6.com

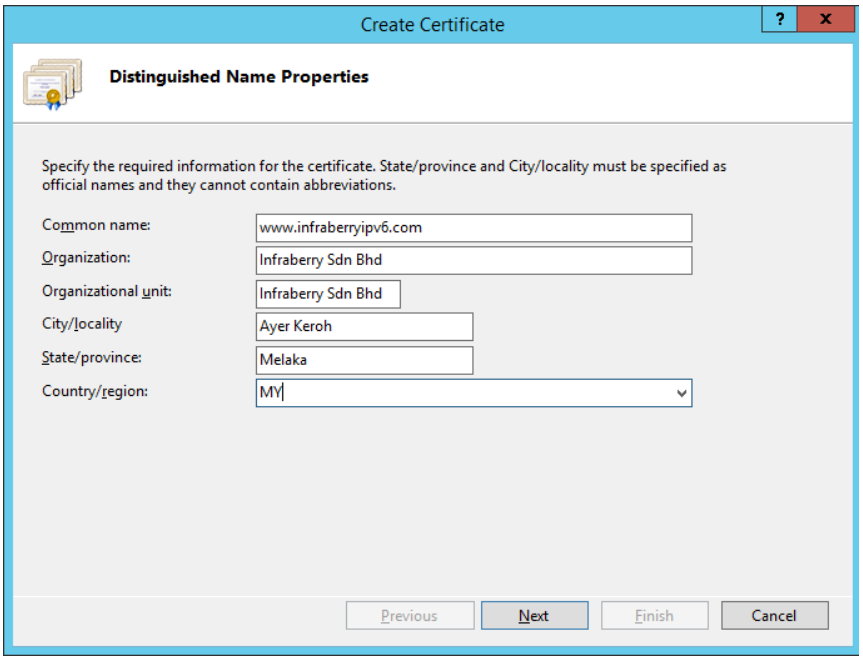


Figure 5. 79 : Create certificate

Step 6: Insert zone name www.infraberryipv6.com

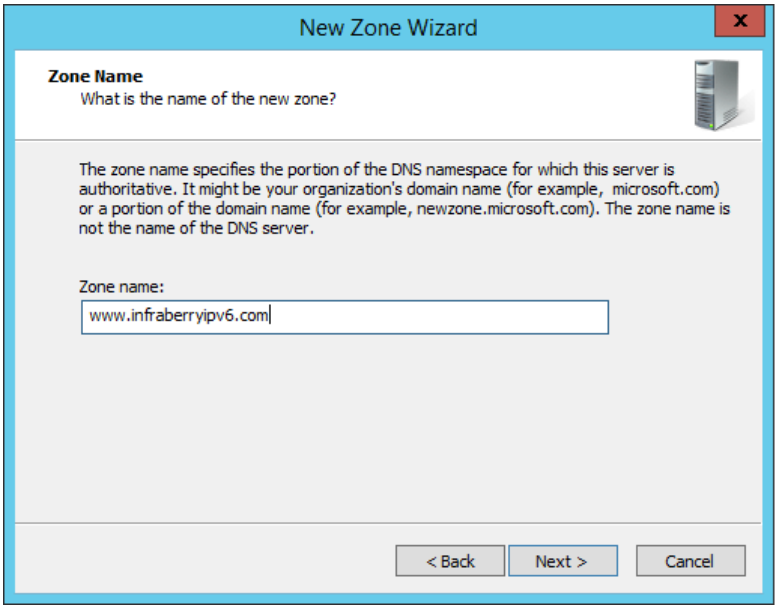


Figure 5. 80: Set zone name

Step 7: Finish the setting

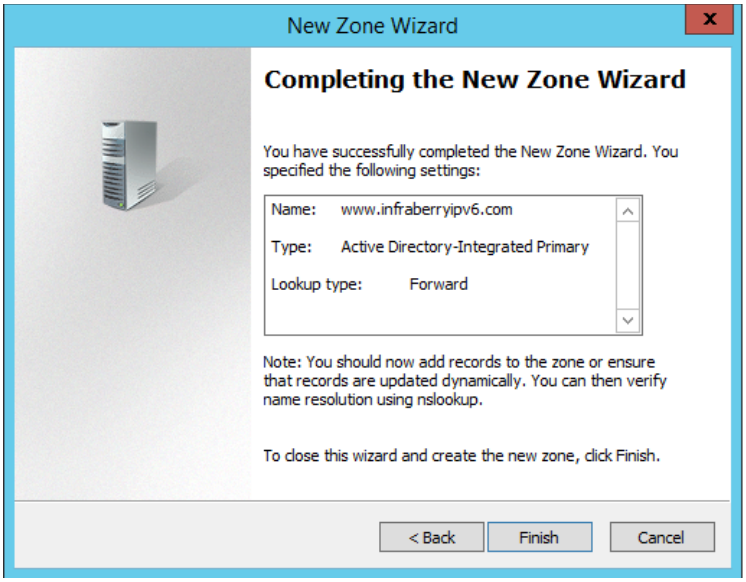


Figure 5. 81 : Finish Setting

Step 8: Right click > Set the Host

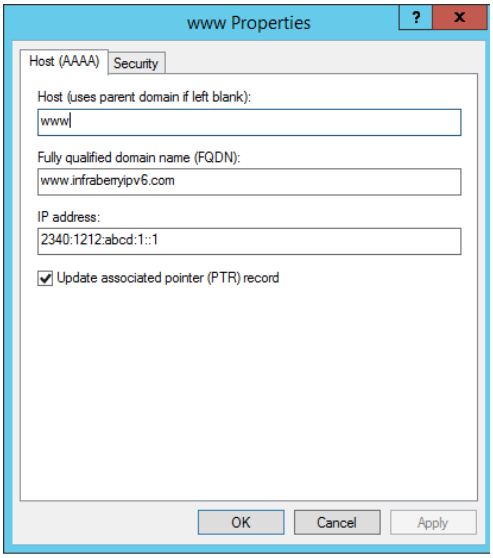


Figure 5. 82 : Set the Host

Step 9: Right Click > Set the CNAME

Step 10: Create a new zone at Forward Lookup Zones > infraberryipv6.com

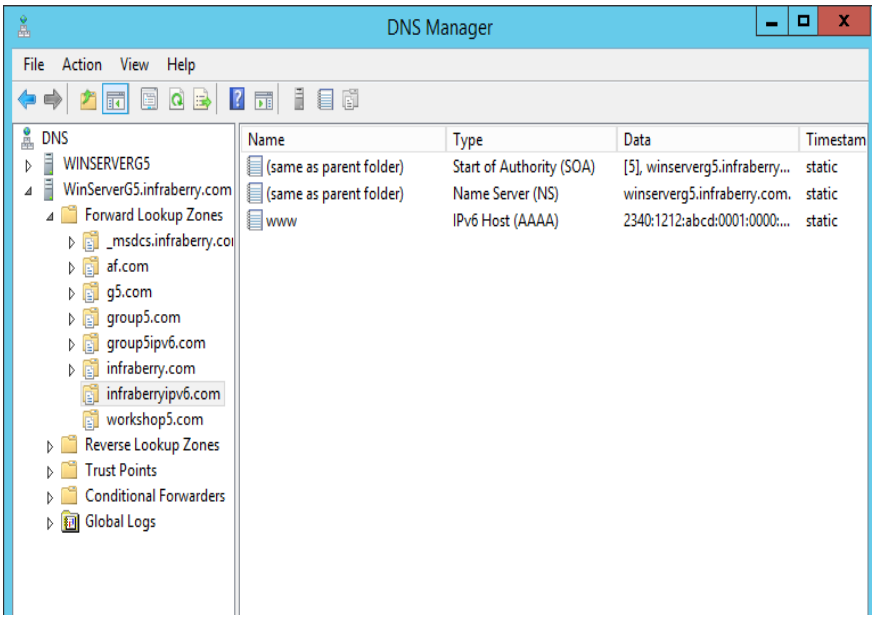
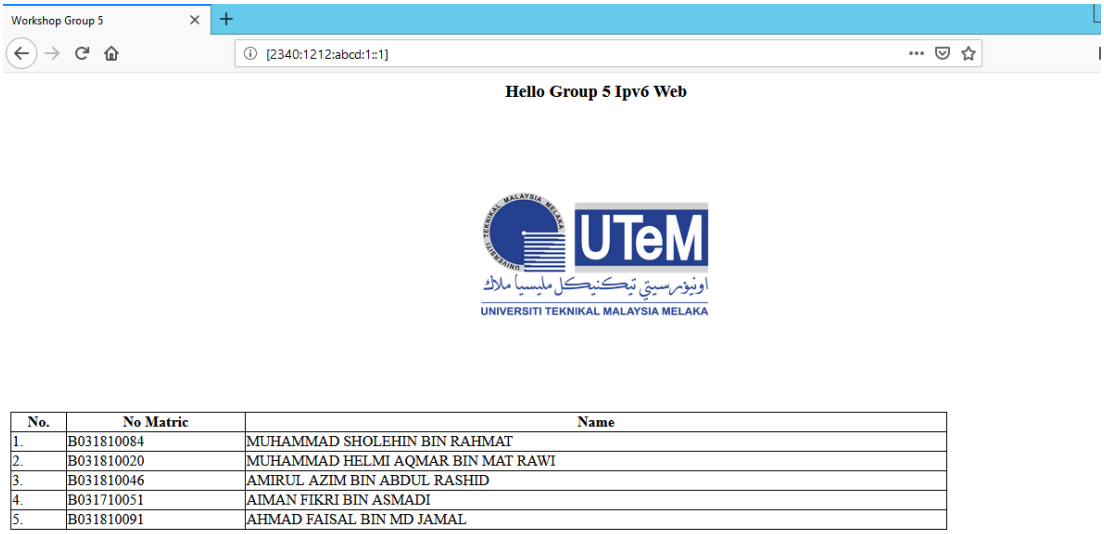


Figure 5. 83 : DNS Manage

Step 11: Open IE then type https://[2340:1212:abcd:1::1] then the website will appear.



No.	No Matric	Name
1.	B031810084	MUHAMMAD SHOLEHIN BIN RAHMAT
2.	B031810020	MUHAMMAD HELMI AQMAR BIN MAT RAWI
3.	B031810046	AMIRUL AZIM BIN ABDUL RASHID
4.	B031710051	AIMAN FIKRI BIN ASMADI
5.	B031810091	AHMAD FAISAL BIN MD JAMAL

Figure 5. 84 : Show the site

5.3.5.1 IPV6 TUNNELLING

To configure 6to4 tunnelling, we first need to create a tunnel interface on each dual-stack edge router. There are three key components relevant to 6to4:

- The tunnel mode (6to4)
- The tunnel source (IPv4 interface or address)
- The 6to4 IPv6 address

On our router, we create the tunnel interface.

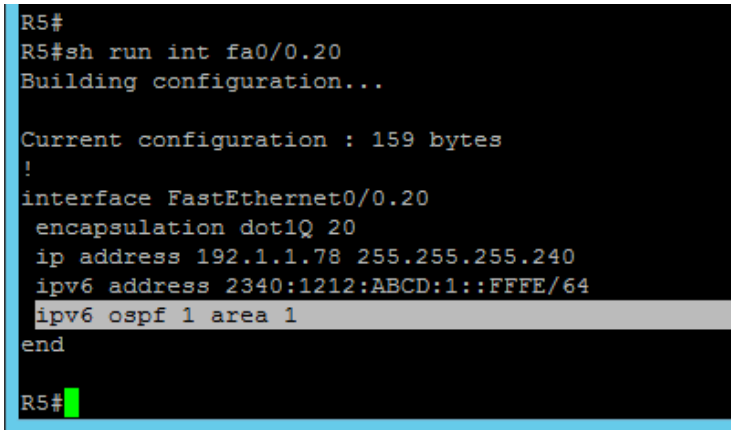


Figure 5. 85: Configure using PuTTY

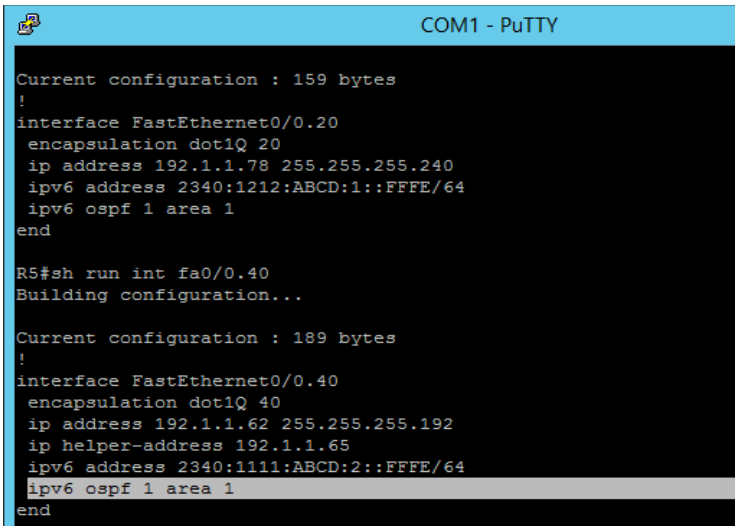


Figure 5. 86: Configure using PuTTY

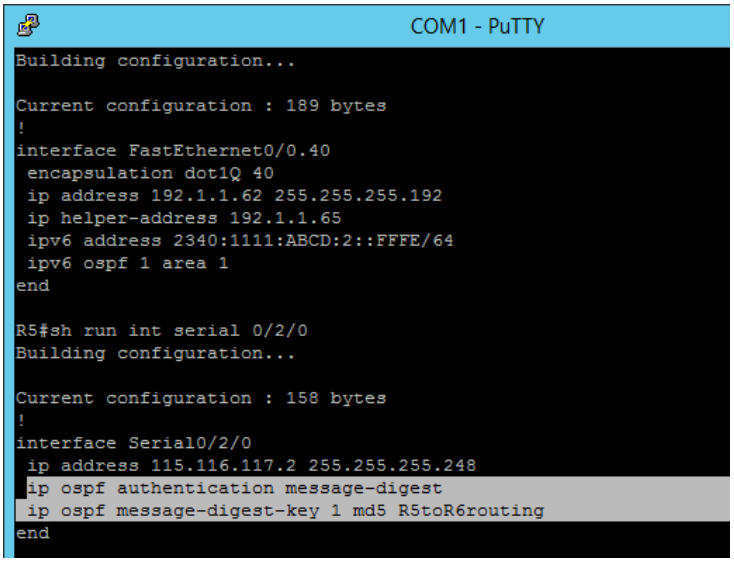


Figure 5. 87 Configure using PuTTY

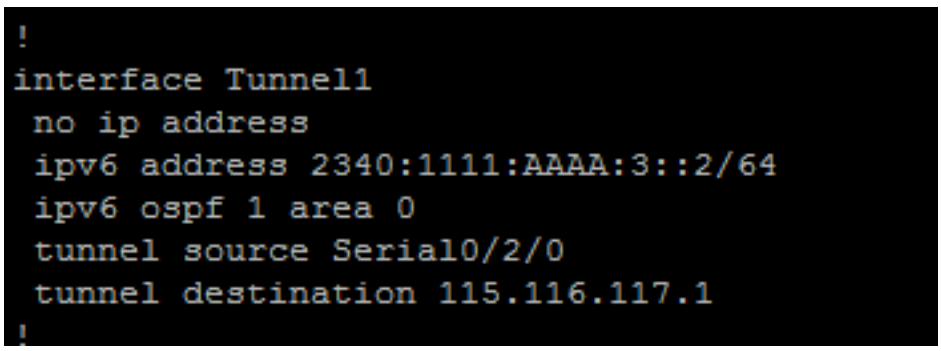


Figure 5. 88: Show interface Tunnel

5.3.6 LINUX EMAIL SERVER

Step 1: Install both Apache2 & PHP7 packages

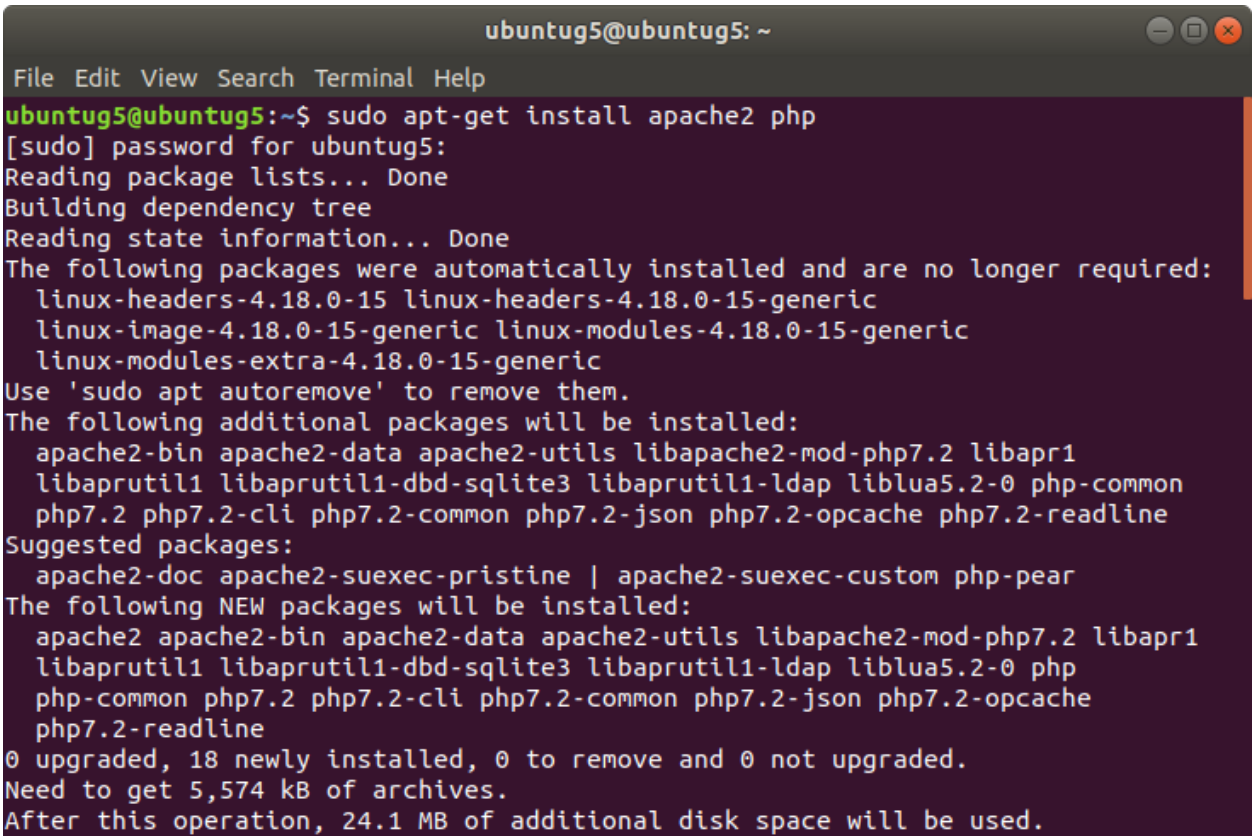


Figure 5. 89 Install Apache & Php

Step 2: Install Postfix Mail Server

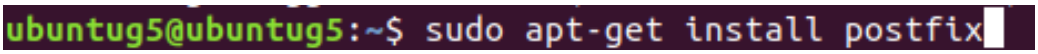


Figure 5. 90 sudo apt-get install postfix

Step 3: During installation, you will be asked to choose the default file configuration for your server

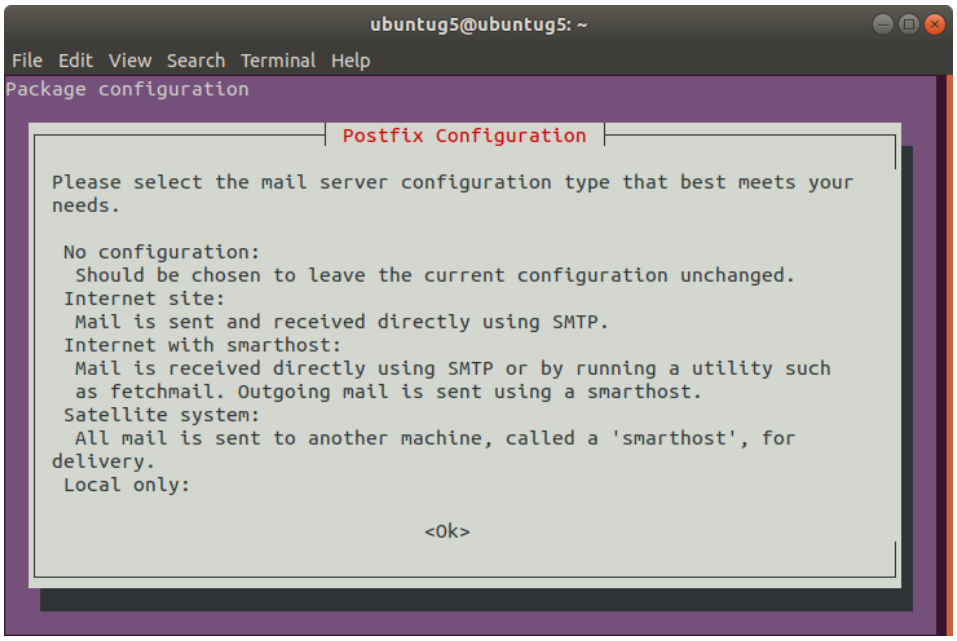


Figure 5. 91 : Postfix Configuration

Step 4: To select type of mail configuration, choose “Internet Site”.

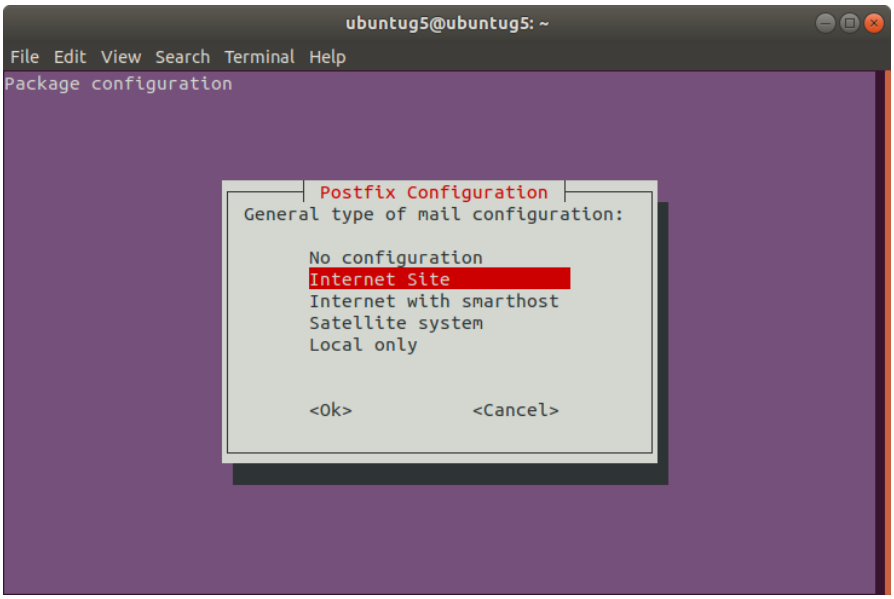


Figure 5. 92 : Postfix Configuration

Step 5: Now enter the fully qualified domain name that you want to use for send and receive mails. In this case, we use group5.com

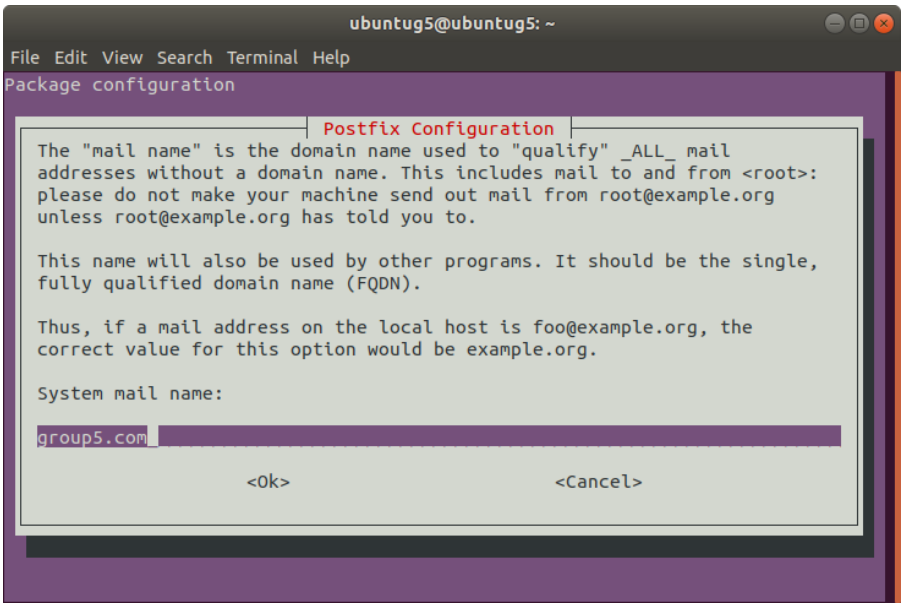


Figure 5. 93 : group5.com

Step 6: Once the FQDN set, restart the Postfix mail server using.

```
ubuntug5@ubuntug5:~$ sudo service postfix restart
```

Figure 5. 94 Restart Postfix Command

Step 7: Dovecot is a mail delivery agent (MDA), it delivers the emails from/to the mail server, to install it, run the following command.

```
ubuntug5@ubuntug5:~$ sudo apt-get install dovecot-imapd dovecot-pop3d
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  dovecot-core
Suggested packages:
  dovecot-gssapi dovecot-ldap dovecot-lmtpd dovecot-managesieved dovecot-mysql
  dovecot-pgsql dovecot-sieve dovecot-solr dovecot-sqlite ntp
The following NEW packages will be installed:
  dovecot-core dovecot-imapd dovecot-pop3d
0 upgraded, 3 newly installed, 0 to remove and 0 not upgraded.
Need to get 2,925 kB of archives.
After this operation, 9,358 kB of additional disk space will be used.
Do you want to continue? [Y/n]
```

Figure 5. 95 Install Dovecot

Step 8: Next, restart Dovecot service using the following command.

```
ubuntug5@ubuntug5:~$ sudo service dovecot restart
```

Figure 5. 96 Restart Dovecot

Step 9: Install Rainloop for webmail access.

```
ubuntug5@ubuntug5:~# mkdir rainloop
```

Figure 5. 97: Install Rainloop

Step 10: You can now access the mail server by going to mail.group5.com/rainloop

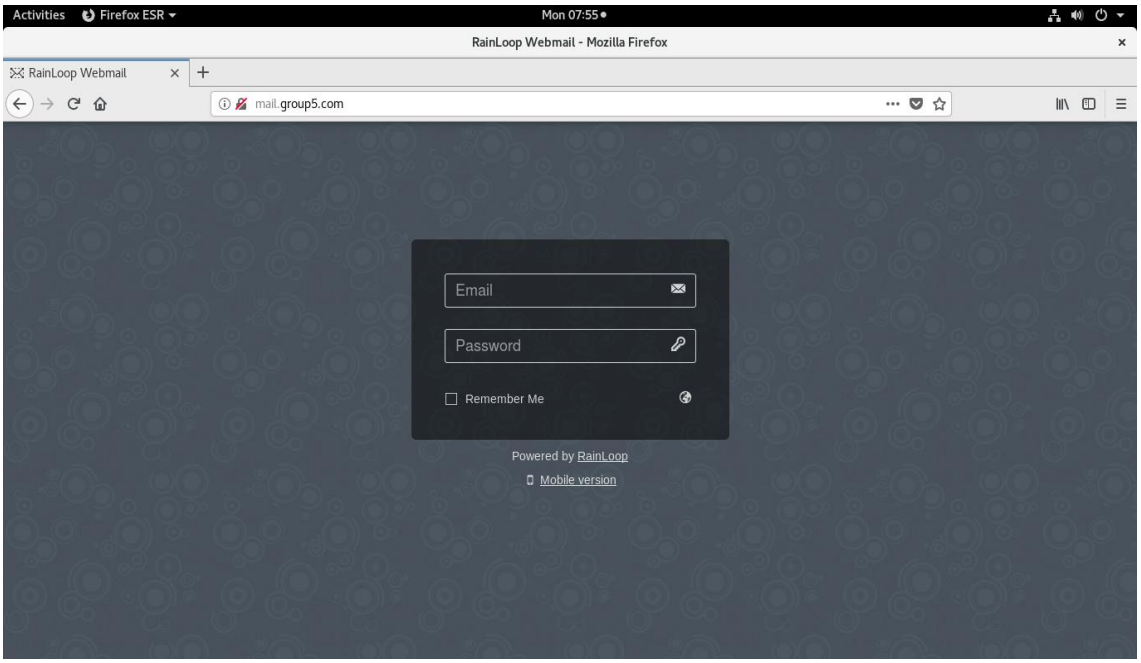


Figure 5.98 : Rainloop Web Interface

Step 11: In order to start using rainloop webmail, you'll have to create a new user, to do so, run.

```
root@group5:~# sudo useradd user1
```

Figure 5. 99 : Add User

Step 12: Create a password for the new user by running.

```
root@group5:~# sudo passwd user1
```

Figure 5. 100 : Create Password

Step 13: Create a home folder for the user in /var/www/html/test and make it default home directory.

```
root@group5:~# mkdir -p /var/www/hmtl/user1
```

Figure 5. 101 : sudo mkdir -p /var/www/html/user1

```
root@group5:~# usermod -m -d /var/www/hmtl/user1
```

Figure 5. 102 : usermod -m -d /var/www/html/test test

Step 14: Give the user “user1” the complete permissions on its home folder.

```
root@group5:~# chown -R user1:user1 /var/www/hmtl/user1
```

Figure 5. 103 : Full Permission on User Folder

Step 15: Now go back to the login page and enter the user name and the password of newly created user.

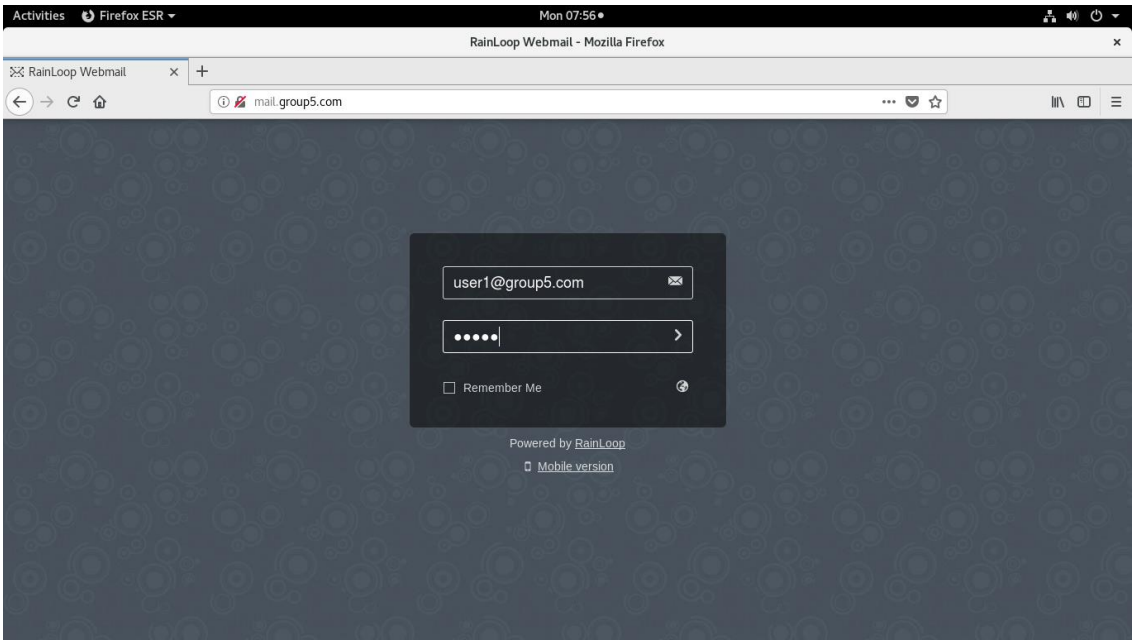


Figure 5. 104 : Rainloop User Interface

5.3.7 WEB, SSL & VIRTUAL HOSTING

Step 1: Install a Web Server (IIS) by Go to ***Server Manager*** and click ***Add Roles***.

This wizard will prompt to start installation.

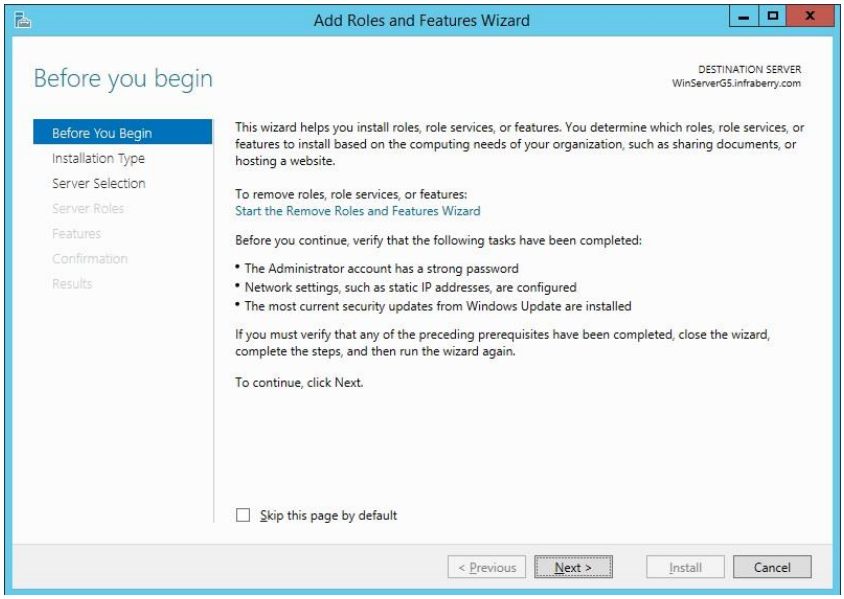


Figure 5. 105: Add role in server

Step 2: Choose Role-based or feature-based installation

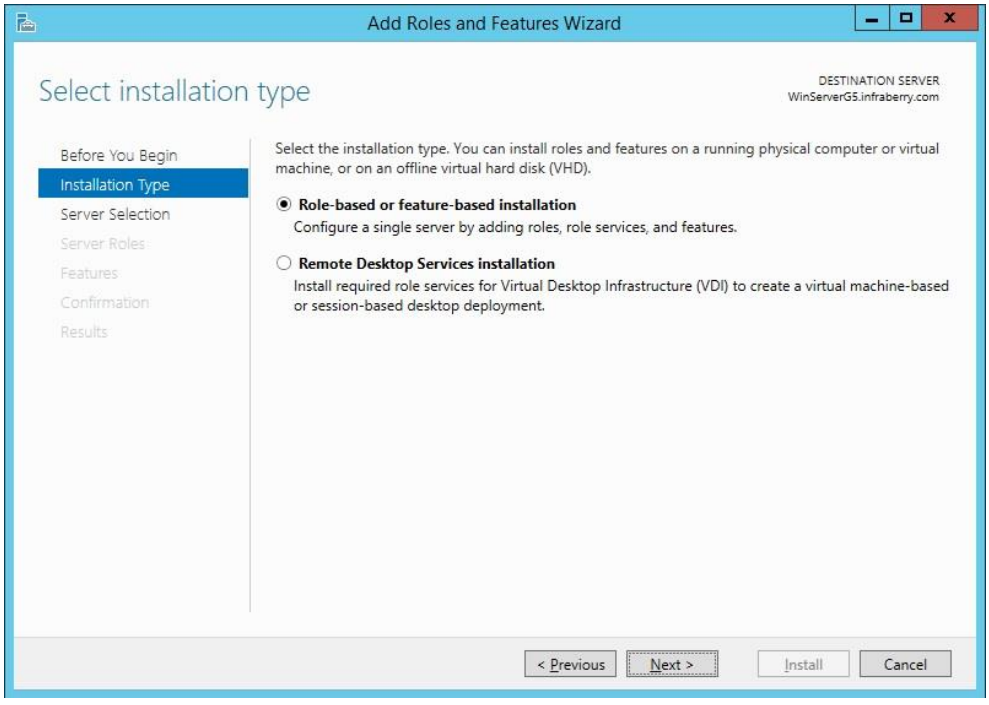


Figure 5. 106: Choose installation type

Step 3: Select a server from the server pool

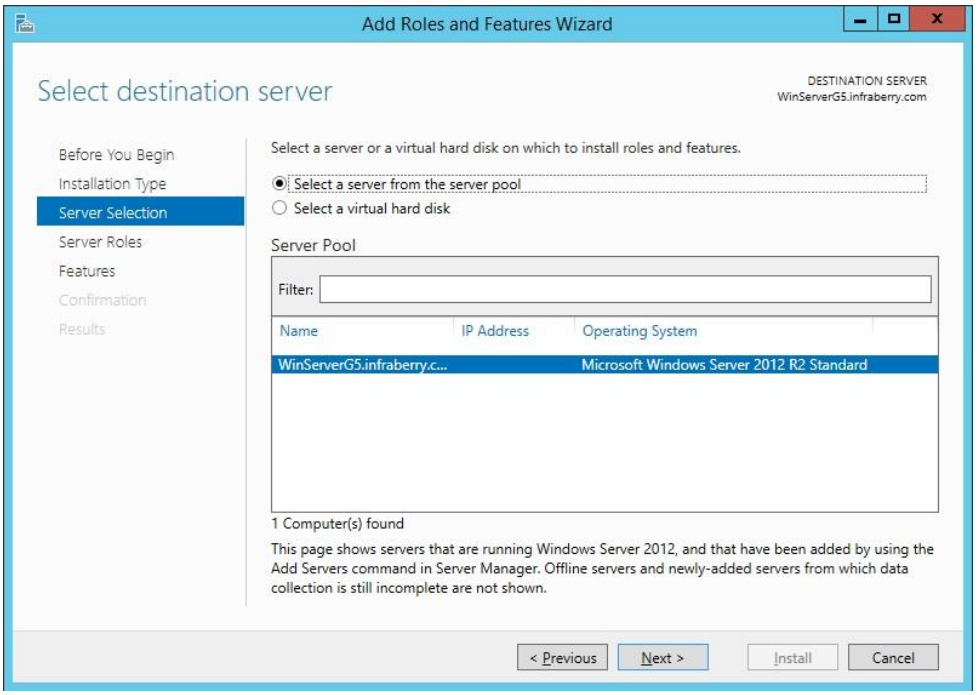


Figure 5. 107: Choose server selection

Step 4: Tick ***Web Server (IIS)*** on server roles

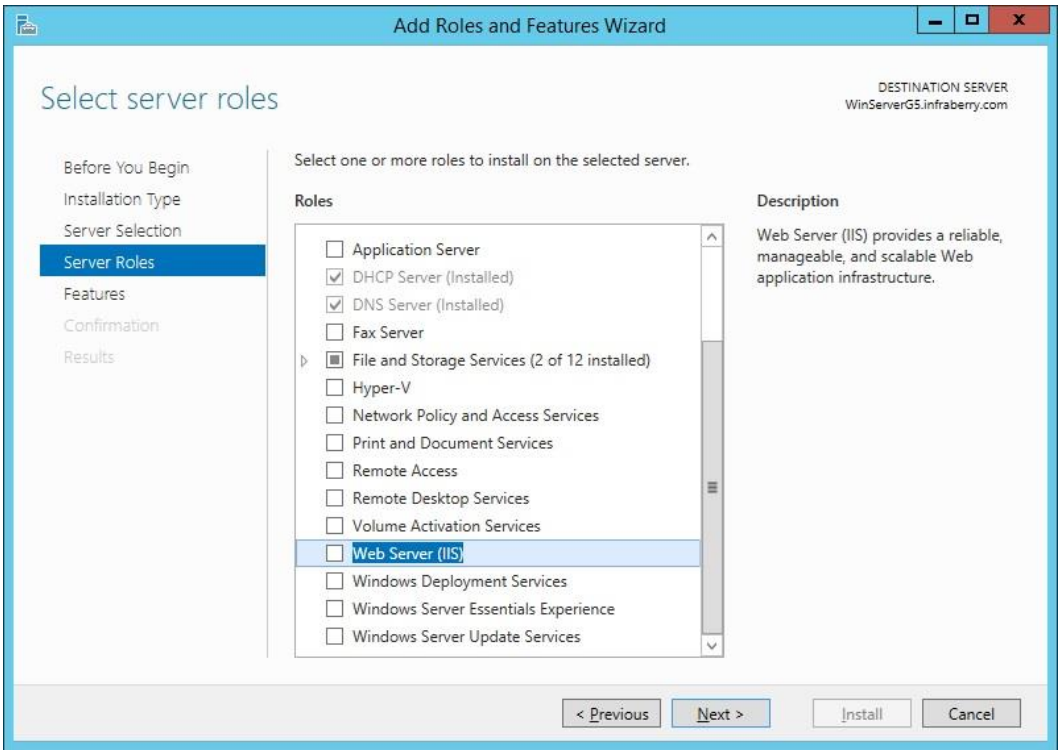


Figure 5. 108: Choose server roles

Step 5: Click button ***Add Features*** for ***Web Server (IIS)***

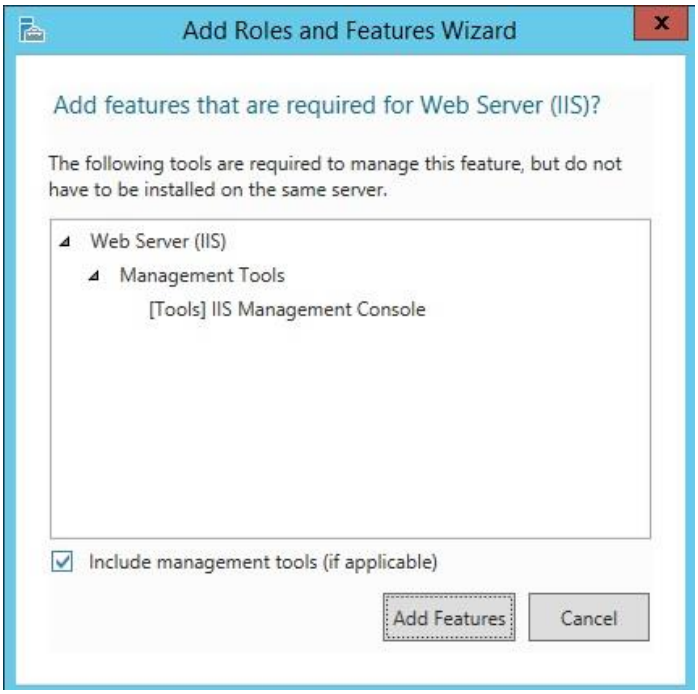


Figure 5. 109: Add Features Web Server (IIS)

Step 6: Click button ***Next*** after ***Web Sever (IIS)*** has been ticked.

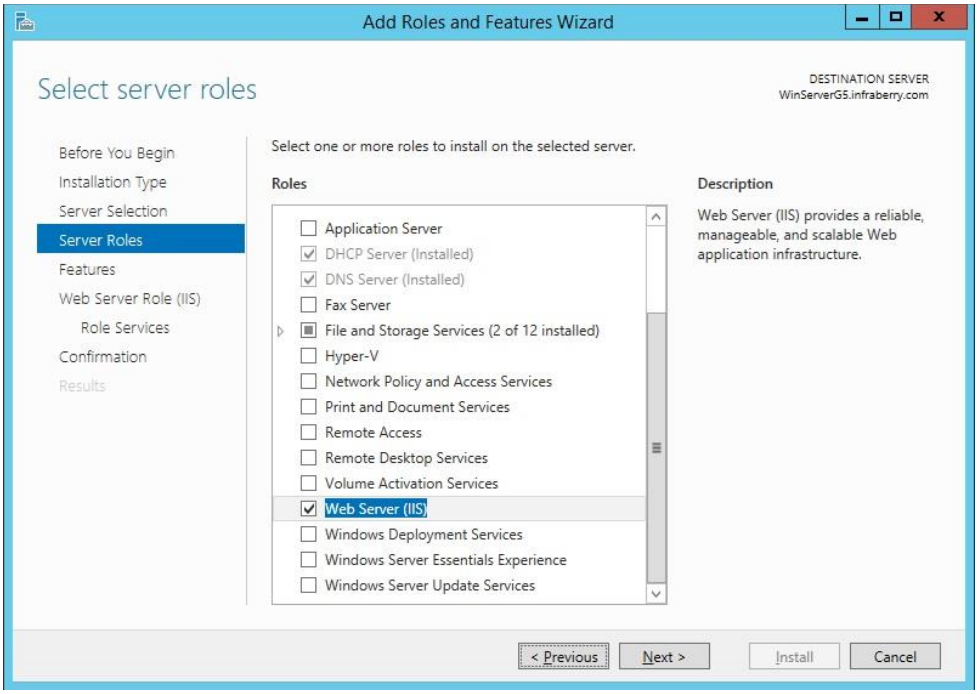


Figure 5. 110: Add Web Server (IIS) in server roles

Step 7: Click button *Next*

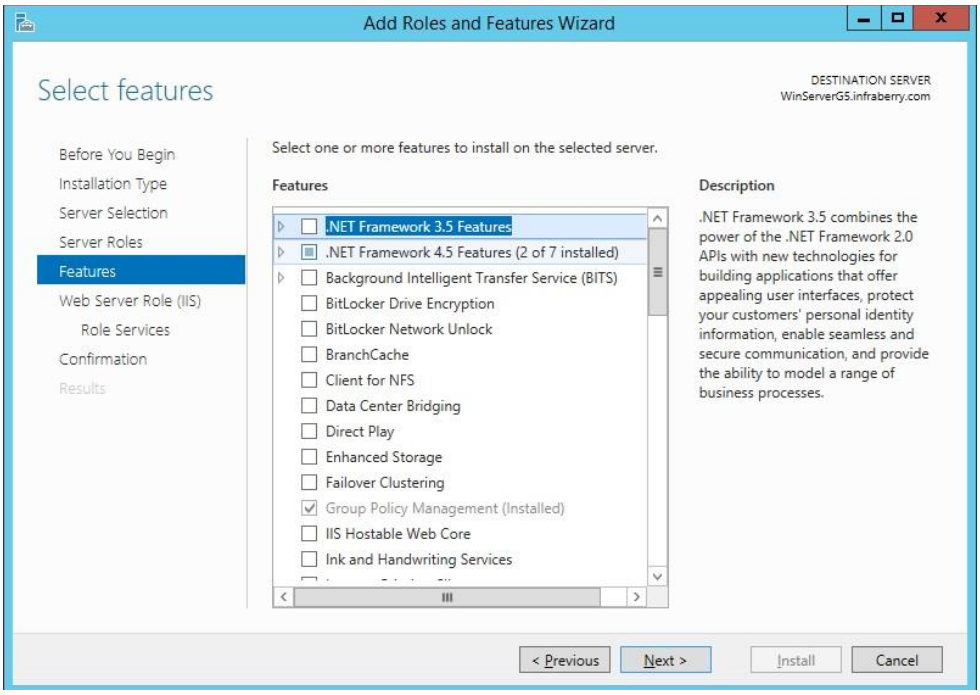


Figure 5. 111: Select features on selected server

Step 8: Click button Next

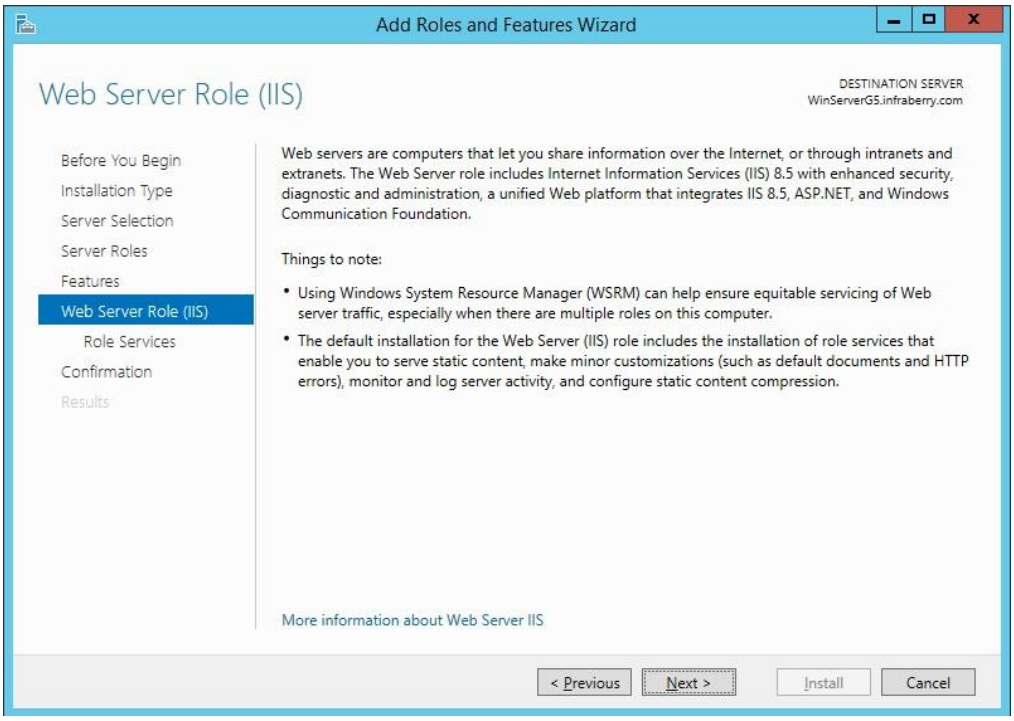


Figure 5. 112: Web Server Roles (IIS)

Step 9: Choose ***Role Services*** to install for Web Server (IIS)

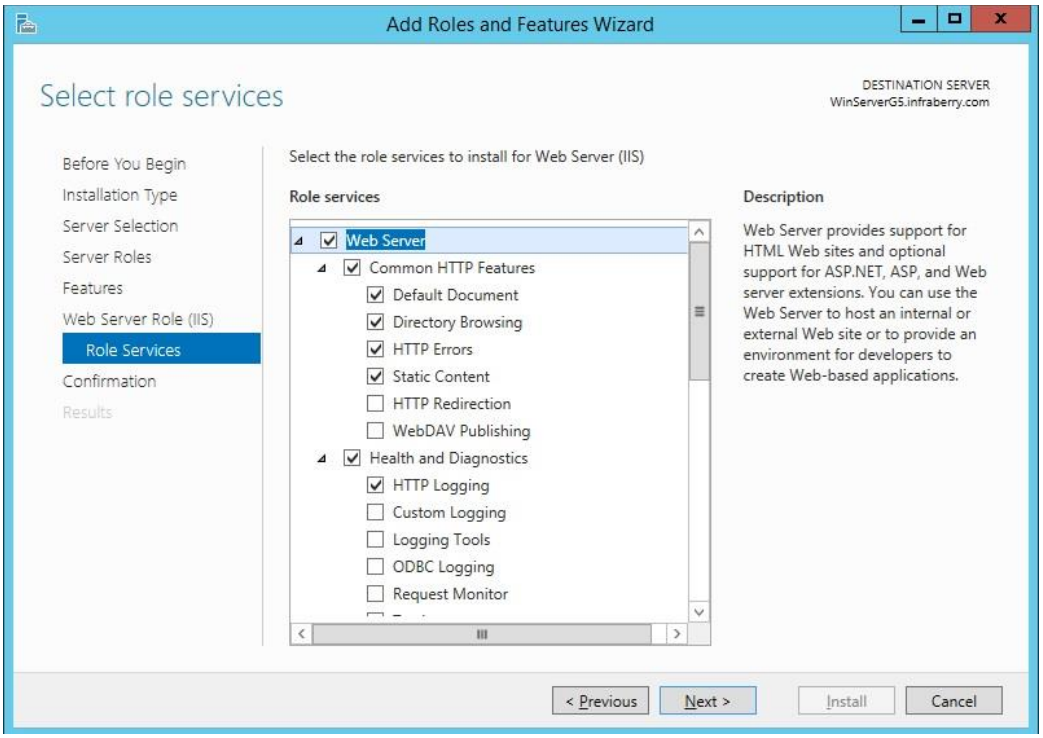


Figure 5. 113: Choose Role Services

Step 10: Click button ***Install***

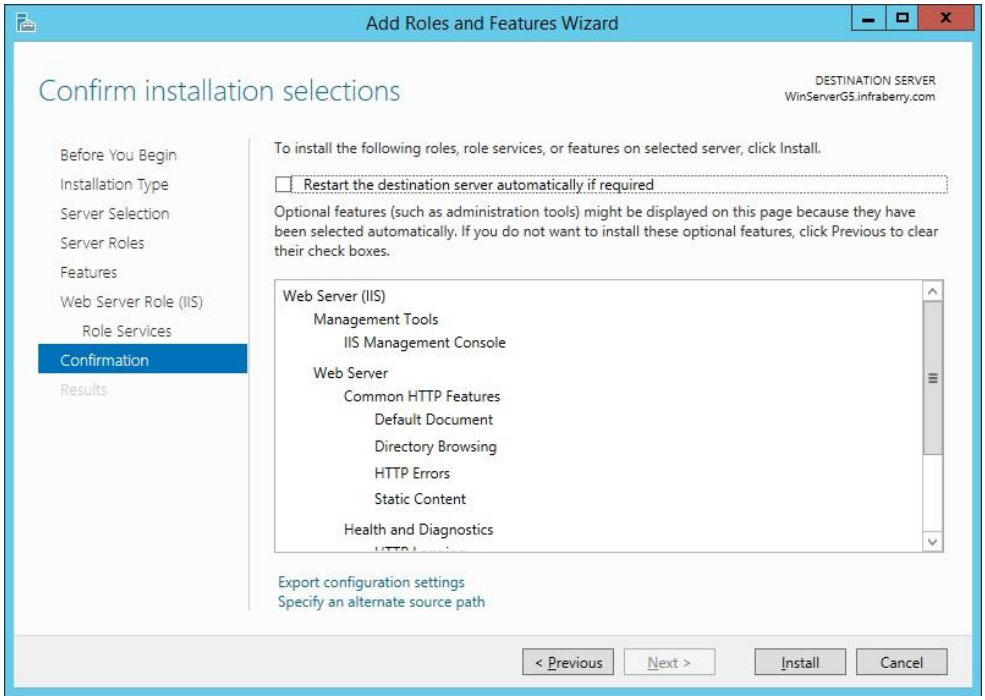


Figure 5. 114: Confirm installation selections

Step 11: Installation complete then click button ***Close.***

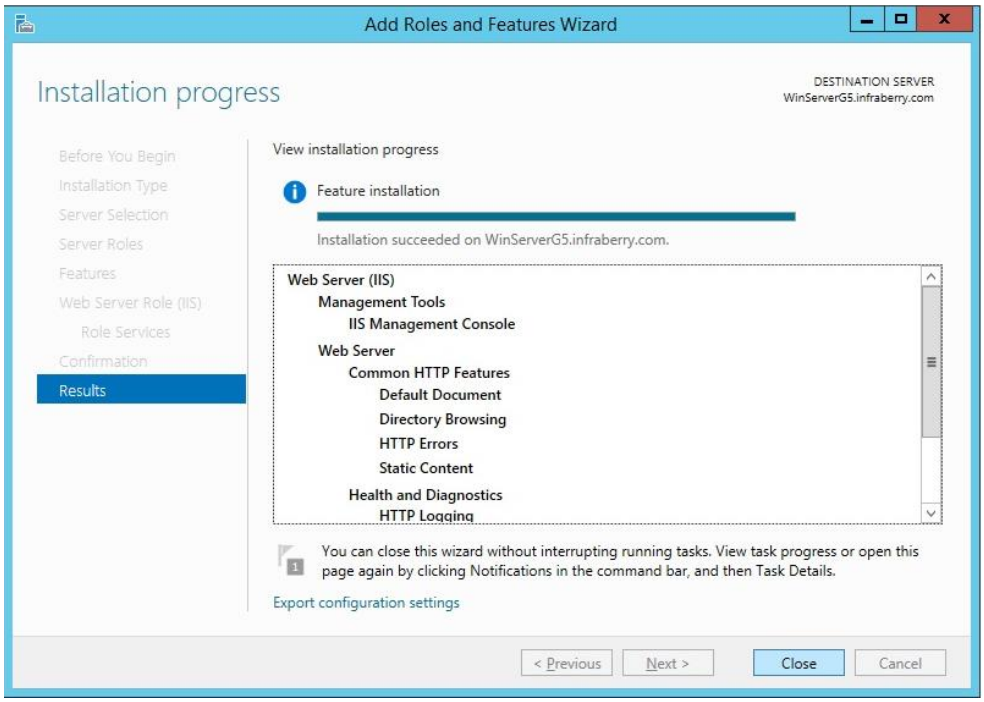


Figure 5. 115: Installation complete

Step 12: Add new sever roles for ***Active Directory Certificate Services (ADCS)***

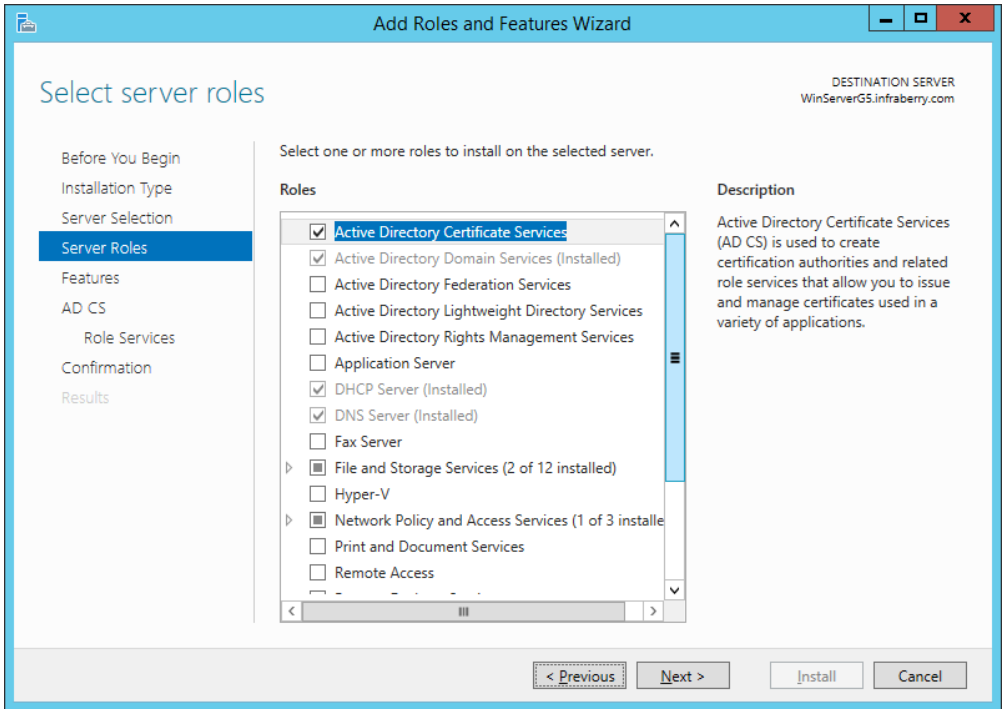


Figure 5. 116: Add new server role

Step 13: Click Next

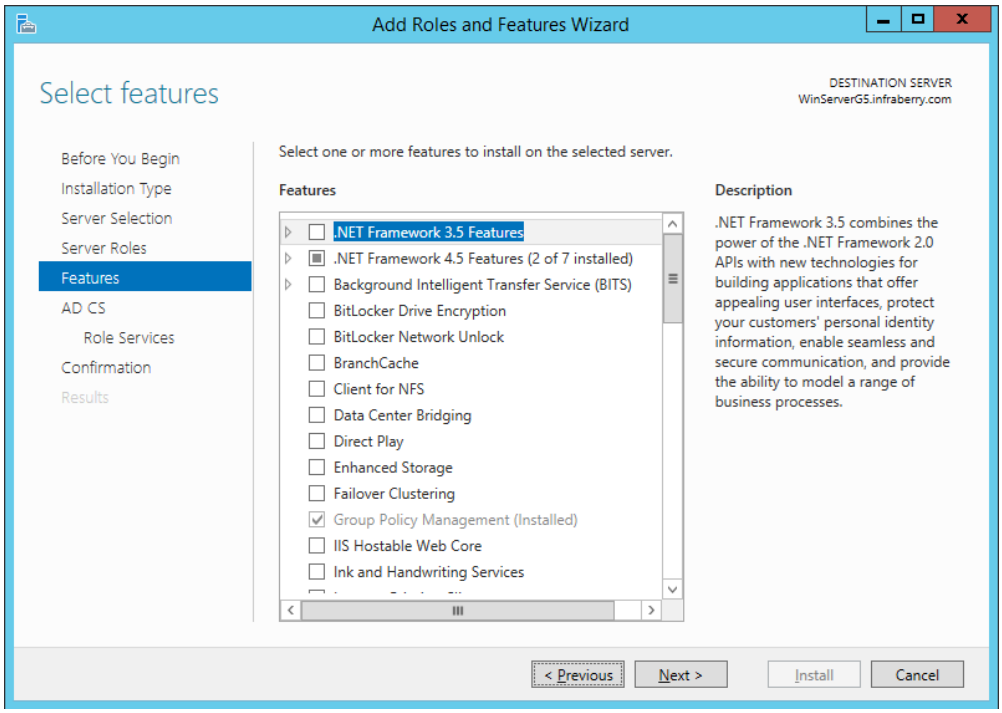


Figure 5. 117: Add feature

Step 14: Click Next

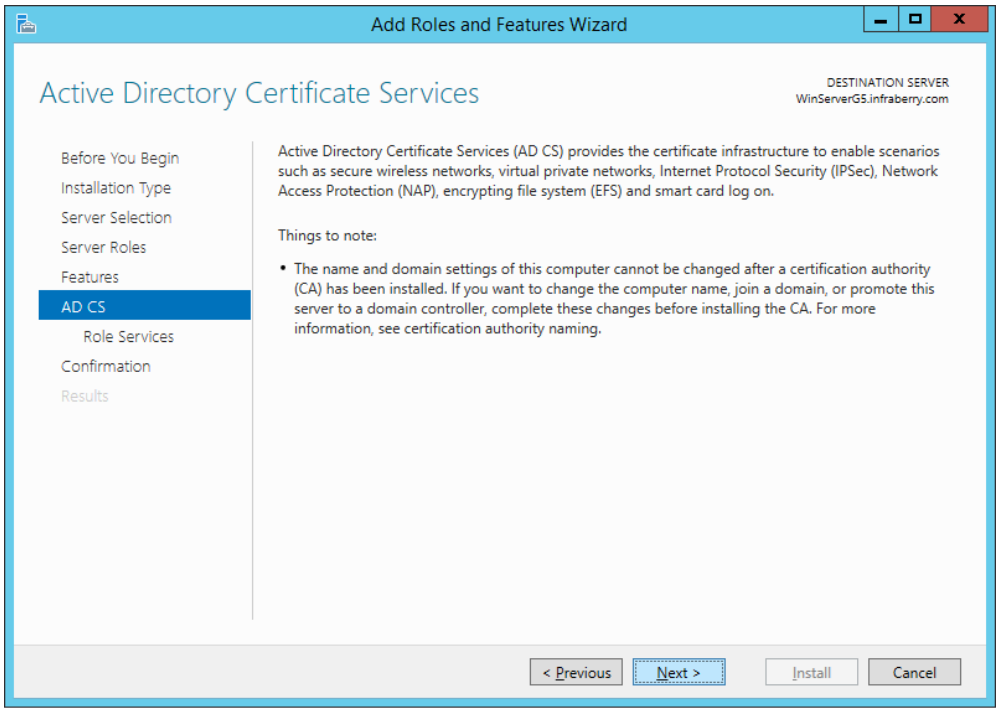


Figure 5. 118: Active Directory Certificate Services

Step 15: Tick on ***Certification Authority*** & ***Certification Authority Web Enrollment***

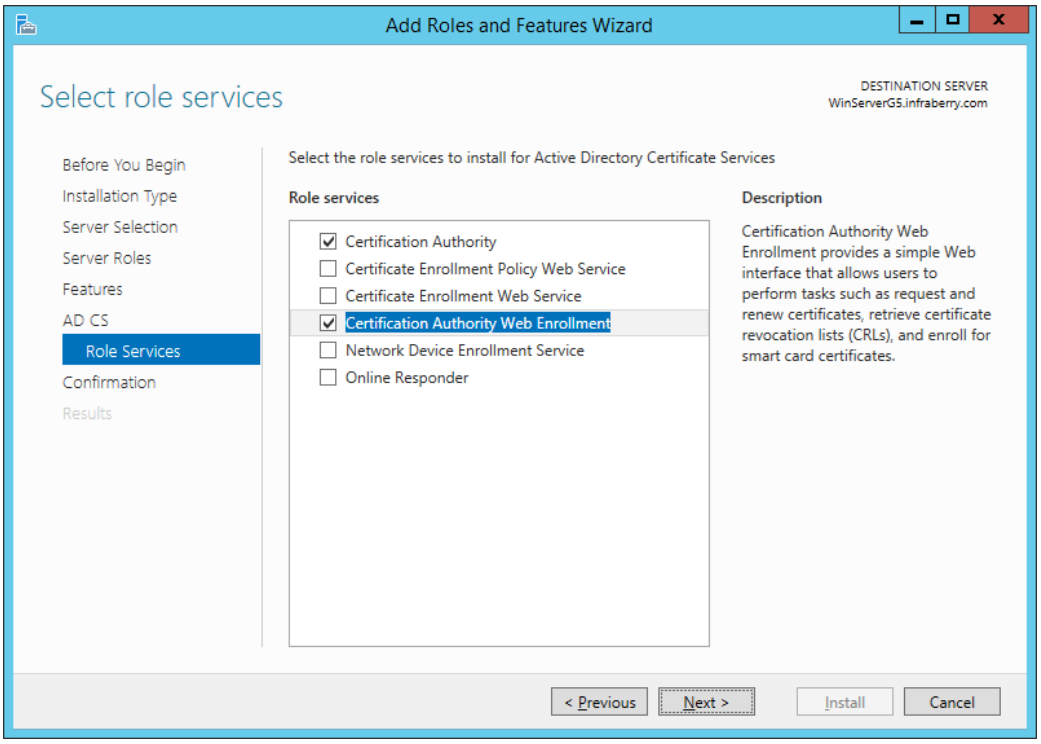


Figure 5. 119: Add Role Services

Step 16: Click button ***Install.***

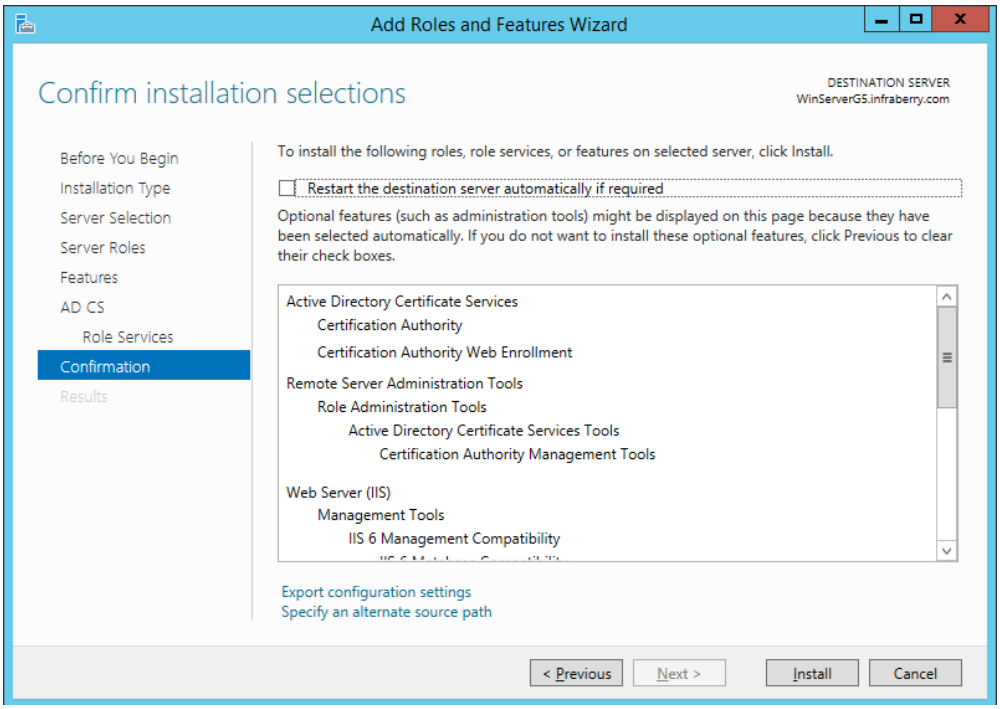


Figure 5. 120: Confirm Installation Selections

Step 17: Click button ***Close*** after finish installation.

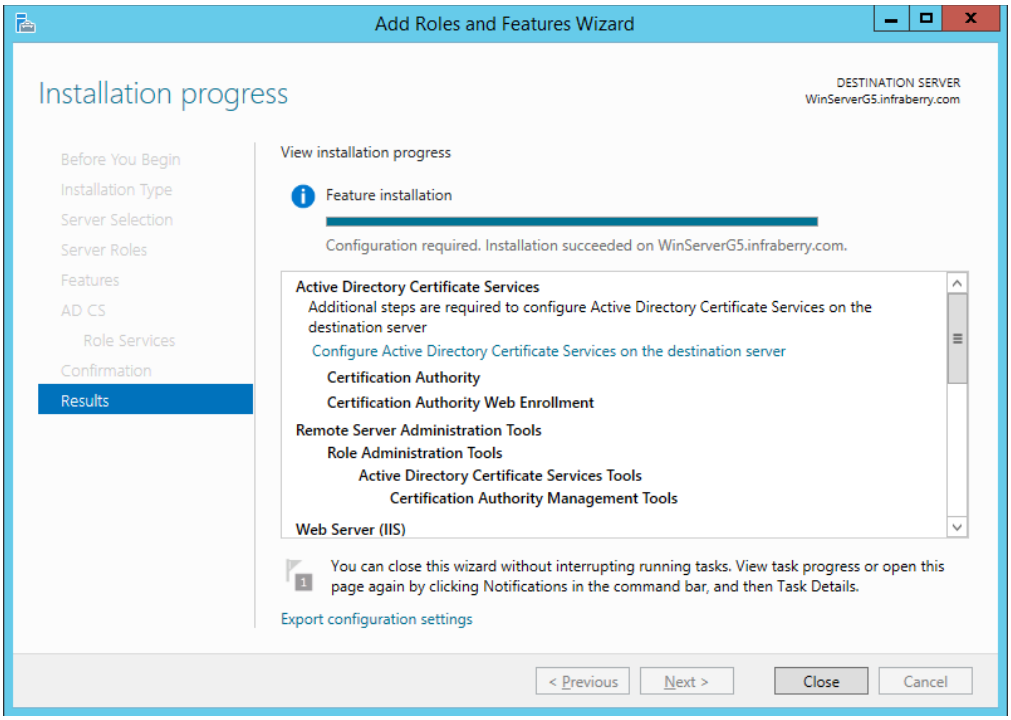


Figure 5. 121: Installation Progress

Step 18: Click Flag on tab then click on ***Configure Active Directory Certificate Services on the server.***

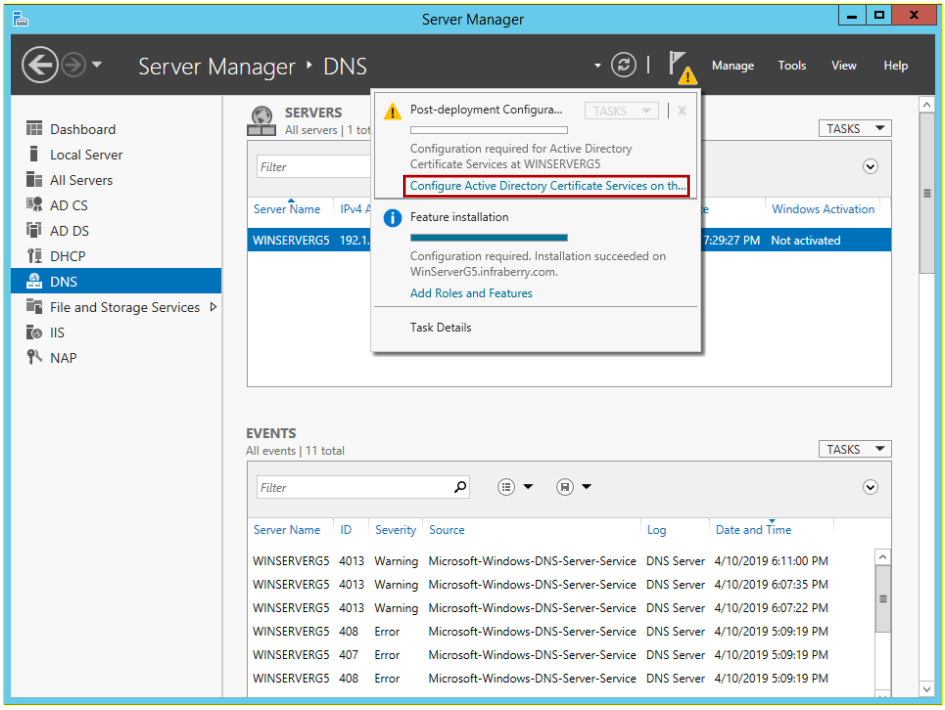


Figure 5. 122: Configure Active Directory Certificate Services

Step 19: Fill up ***Credentials*** form and click button ***Next***

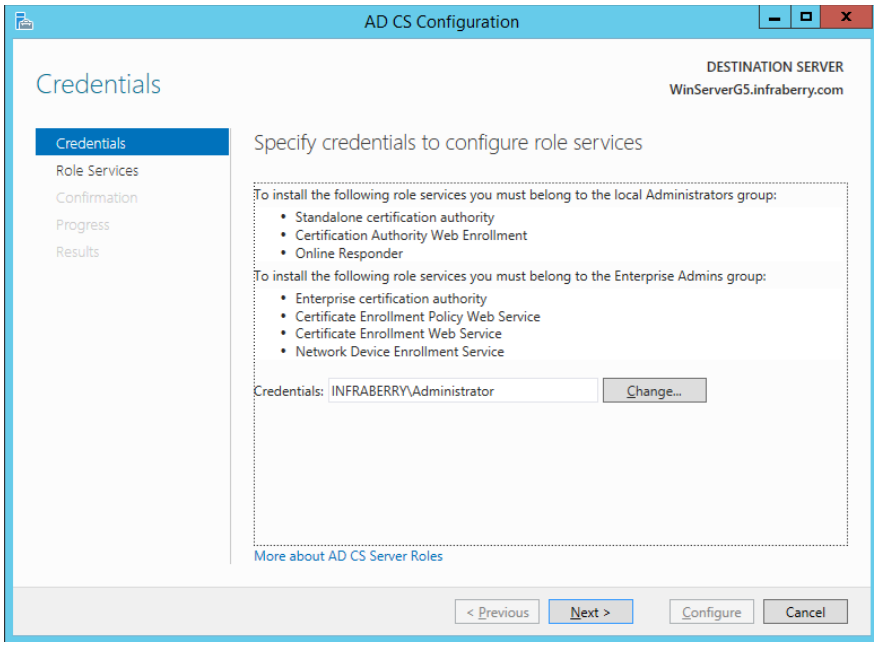


Figure 5. 123: Specify credentials to configure role services

Step 20: Tick on ***Certification Authority*** & ***Certification Authority Web Enrollment*** then click Next

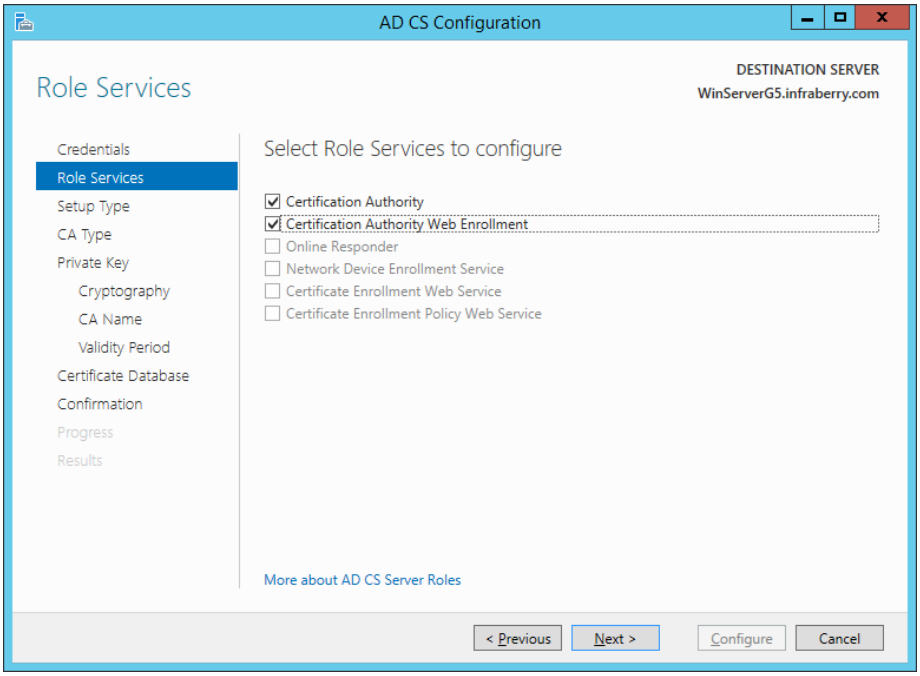


Figure 5. 124: Select Role Services to configure

Step 21: Choose ***Enterprise CA*** then click ***Next***

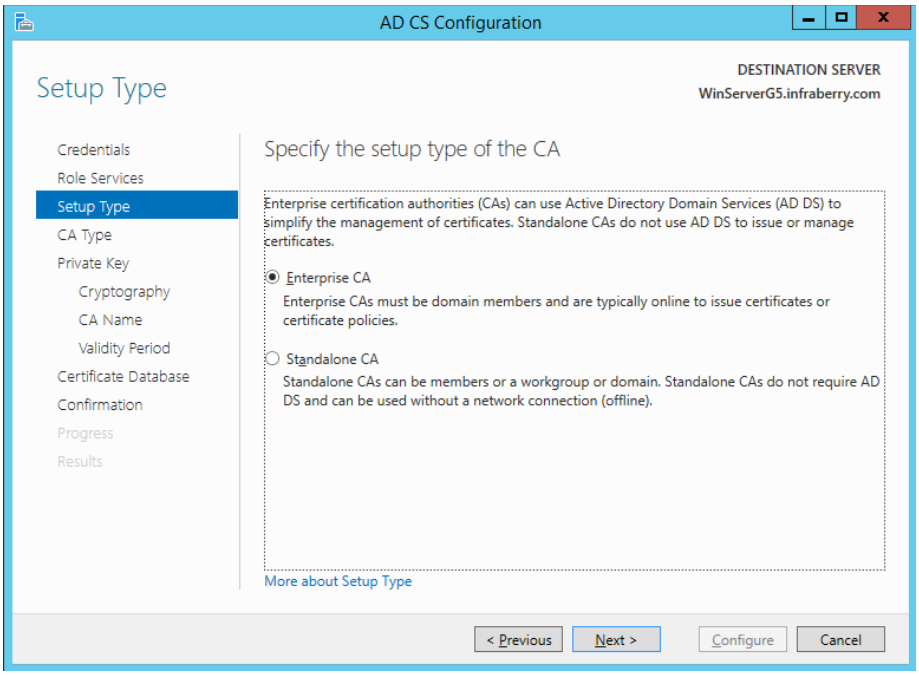


Figure 5. 125: Select Role Services to configure

Step 22: Choose ***Root CA*** then click ***Next***

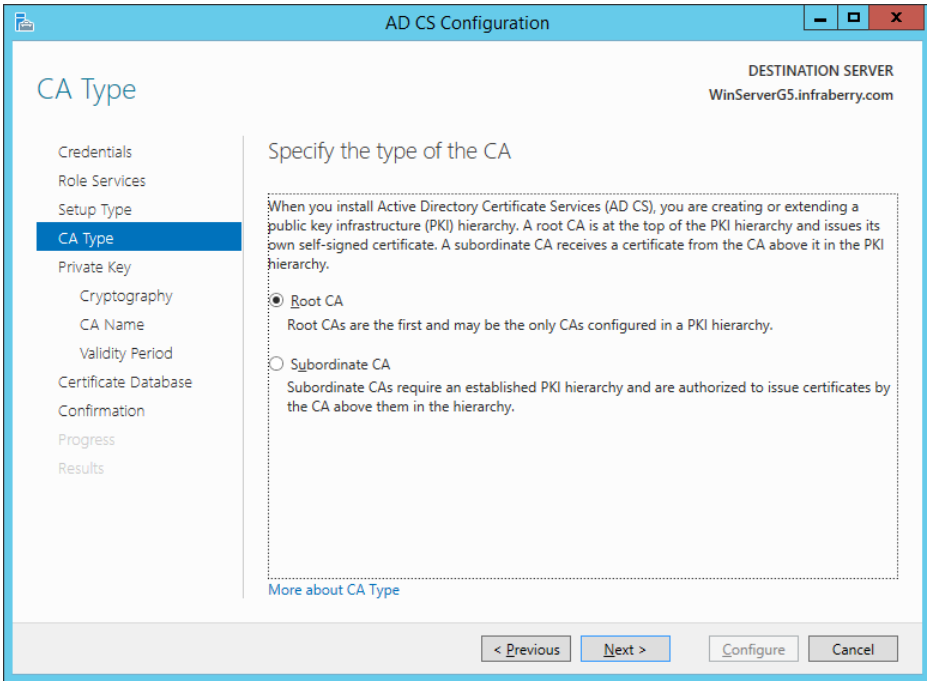


Figure 5. 126: Select Role Services to configure

Step 23: Tick on ***Create a new private key*** then click ***Next***

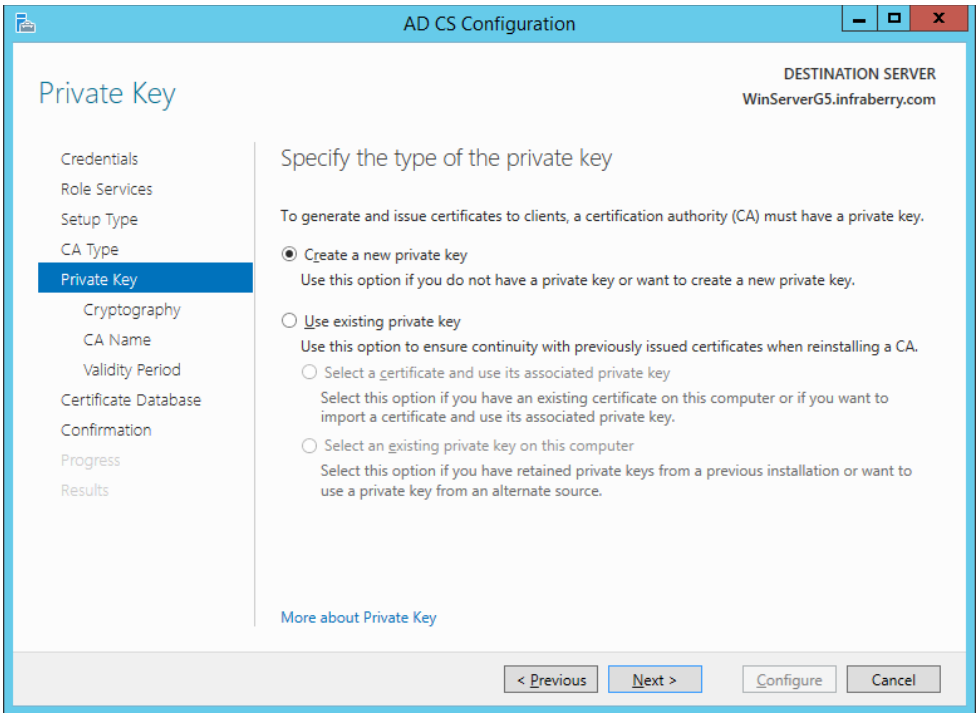


Figure 5. 127: Specify the type of the private key

Step 24: Specify the cryptographic options then click ***Next***

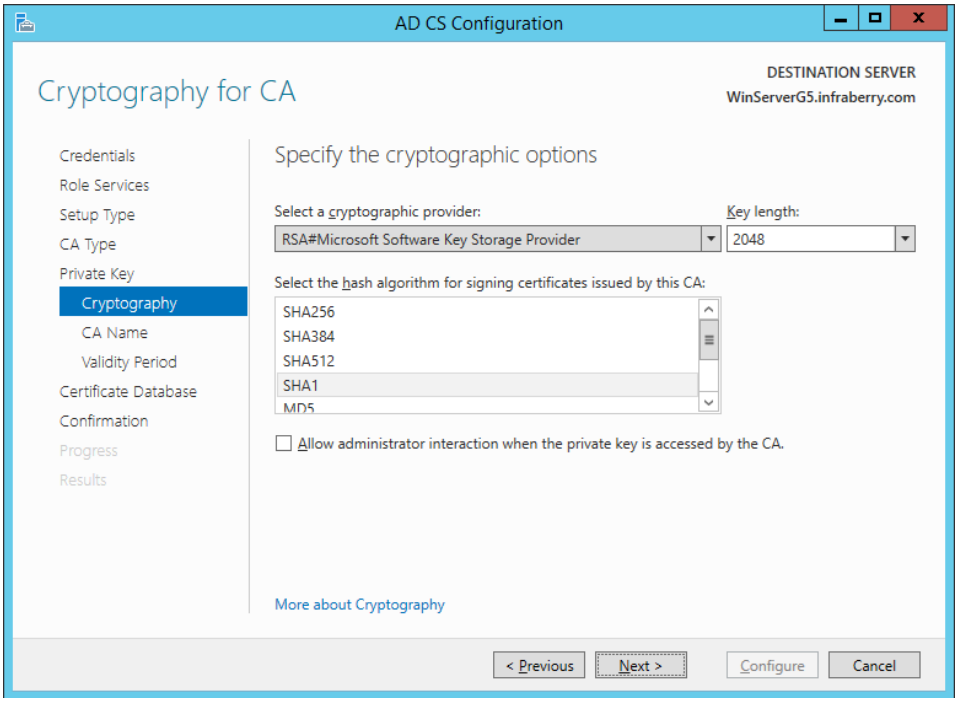


Figure 5. 128: Cryptographic

Step 25: Specify the name of the CA then click ***Next***

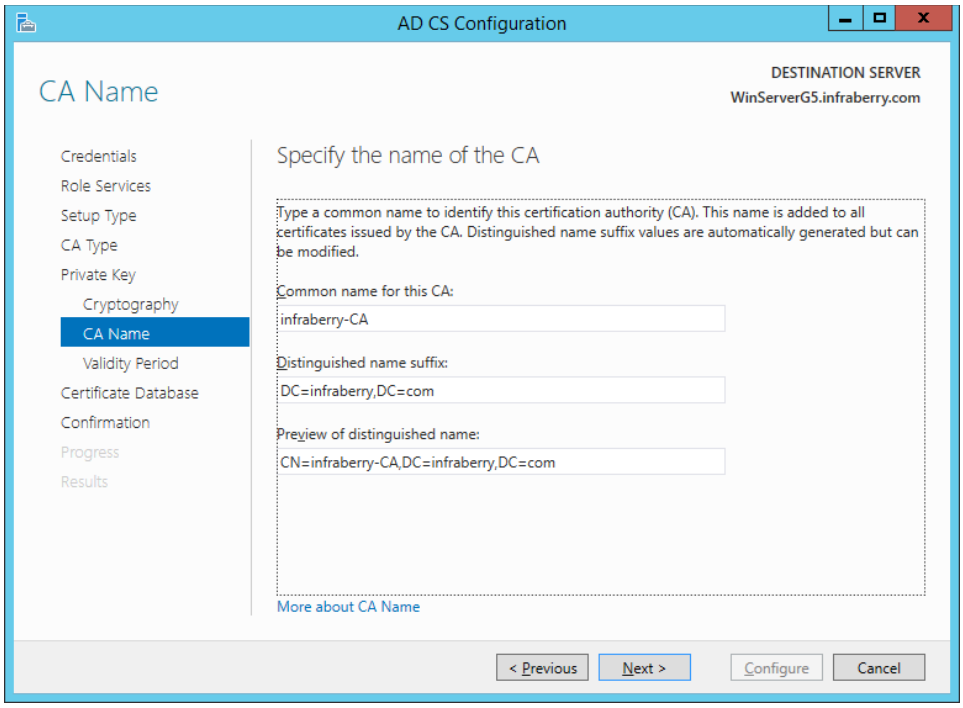


Figure 5. 129: CA Name

Step 26: Specify the validity period then click button ***Next.***

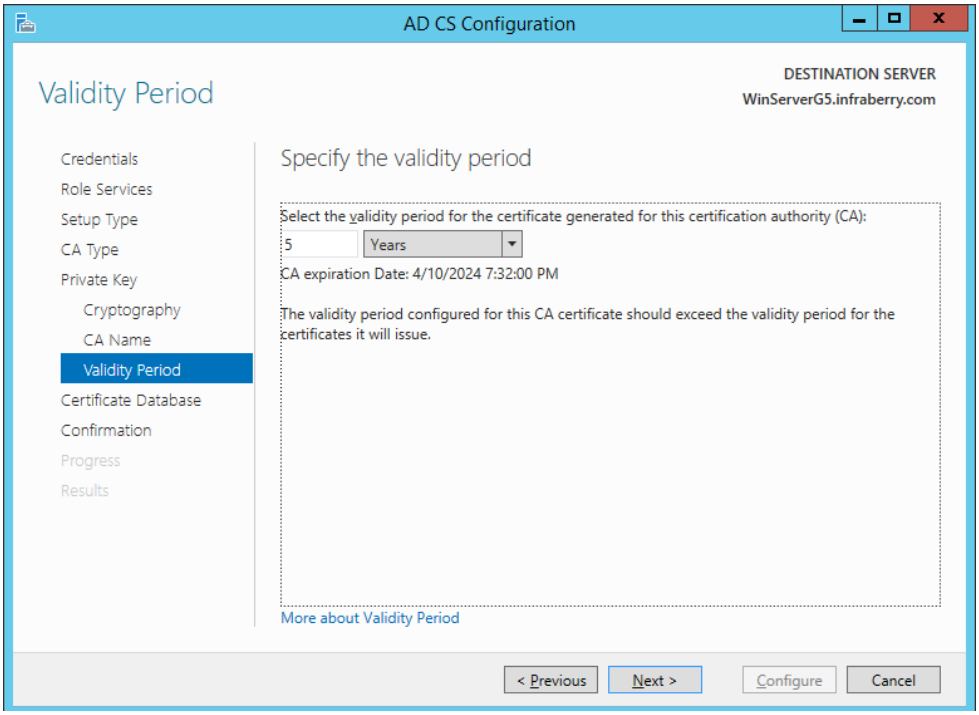


Figure 5. 130: Validity Period

Step 27: Specify the database locations then click button ***Next.***

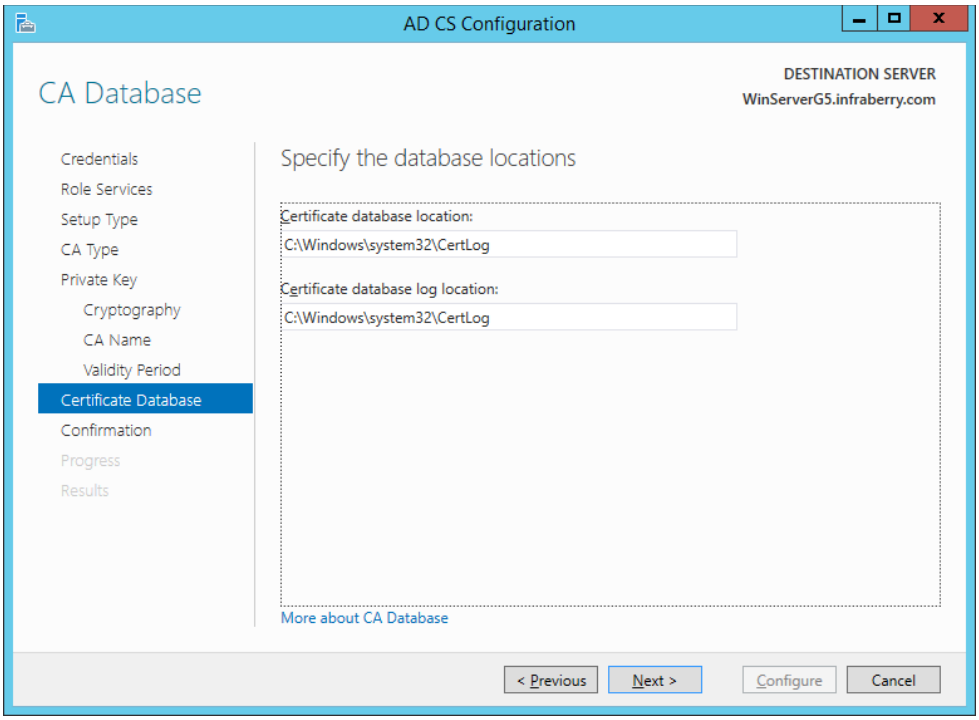


Figure 5. 131: Certificate Database

Step 28: Confirmation of configuration then click button ***Configure.***

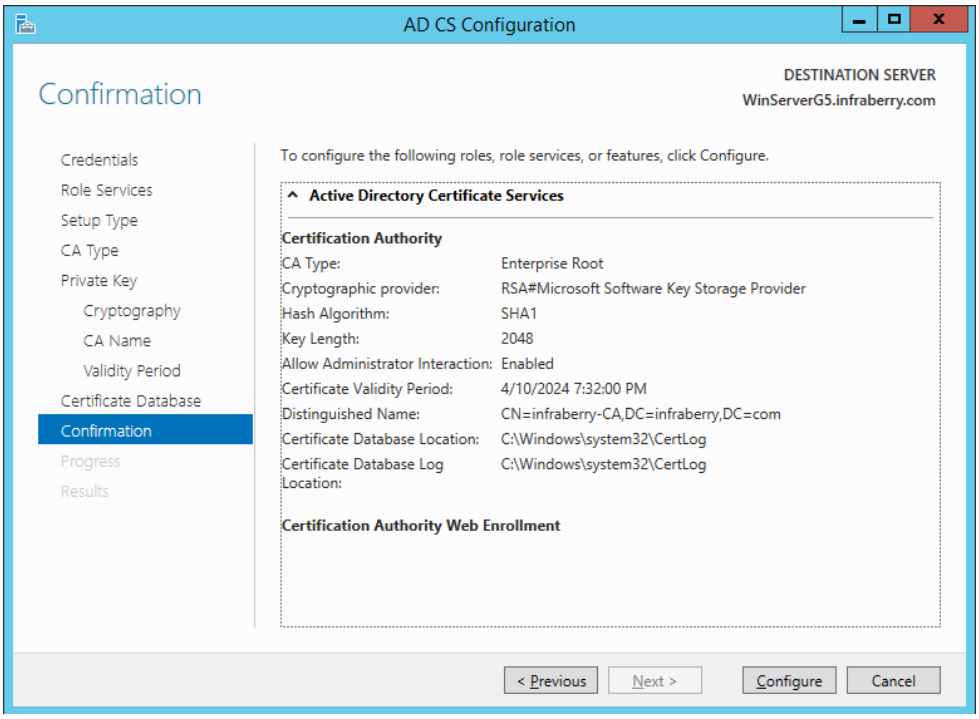


Figure 5. 132: Confirmation of configuration

Step 29: Configuration succeeded then click button ***Close.***

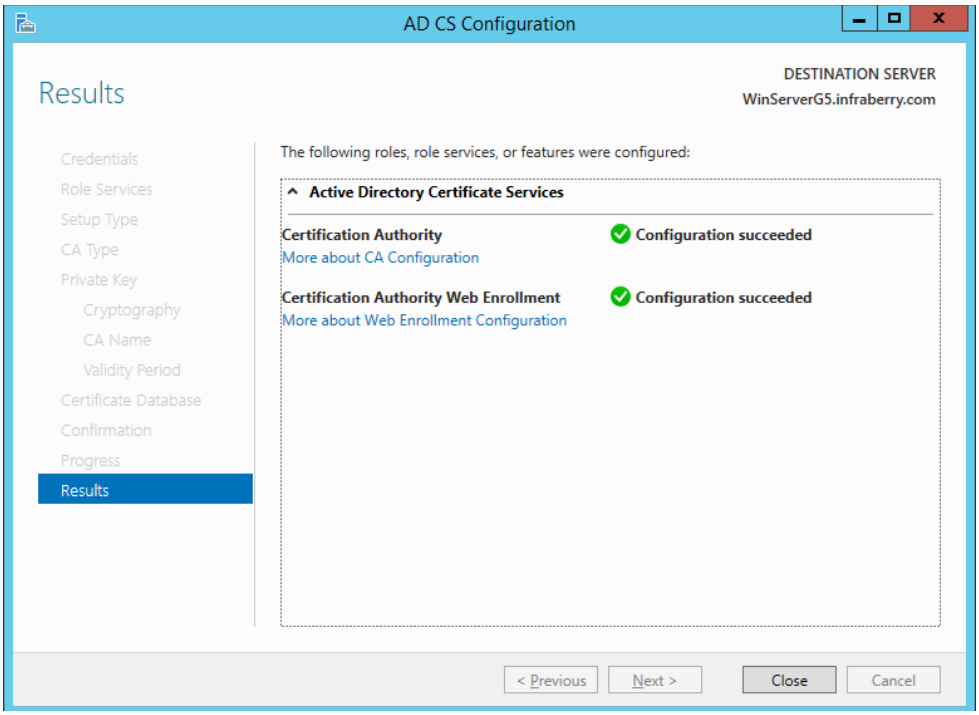


Figure 5. 133: Result of configuration

Step 30: Open ***Internet Information Services (IIS)*** then click on ***Server Certificates.***

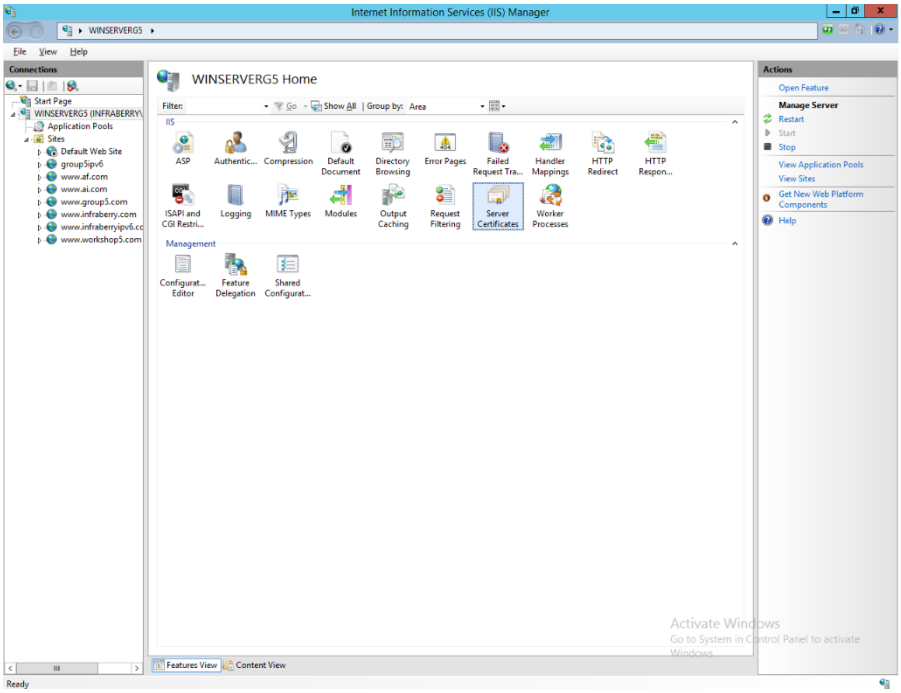


Figure 5. 134: Internet Information Services (IIS) Manager

Step 31: ***Create Domain Certificate*** in Server Certificates

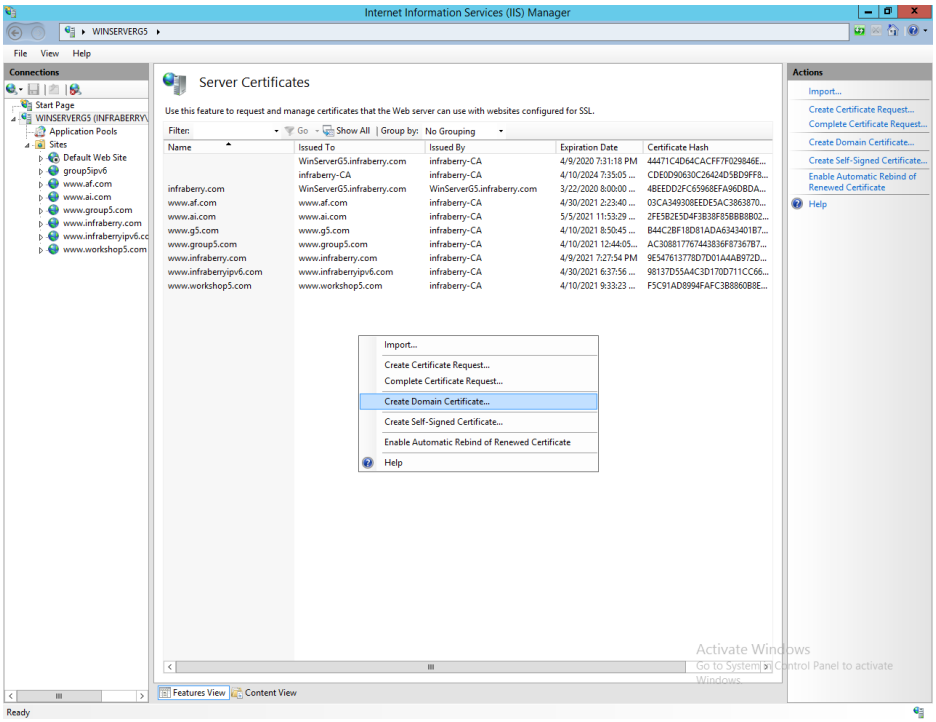


Figure 5. 135: Create Domain Certificate

Step 32: Fill up the form then click button ***Next.***

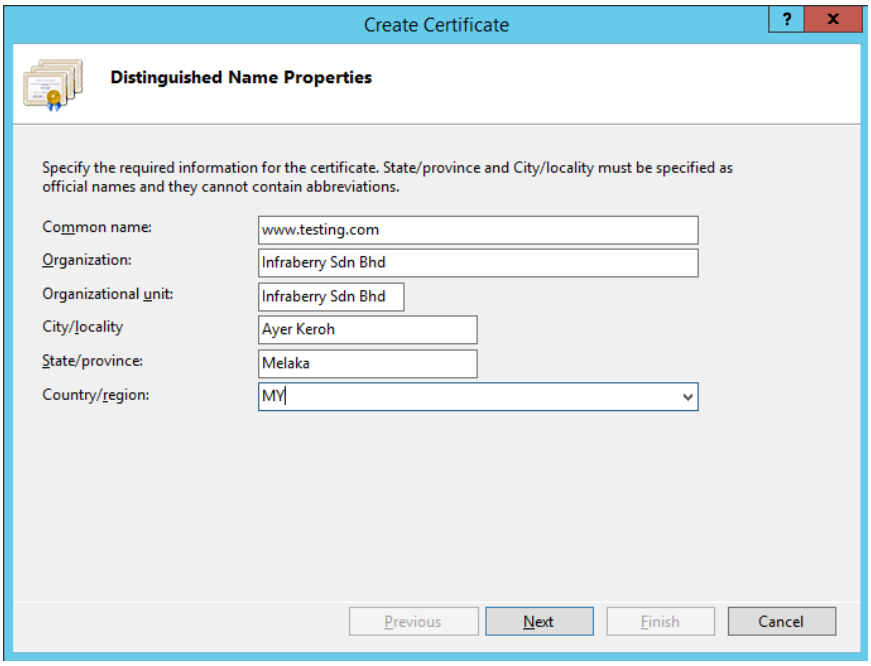


Figure 5. 136: Create Certificate

Step 33: Select ***Certification Authority*** and fill up ***Friendly Name*** then click button ***Finish***

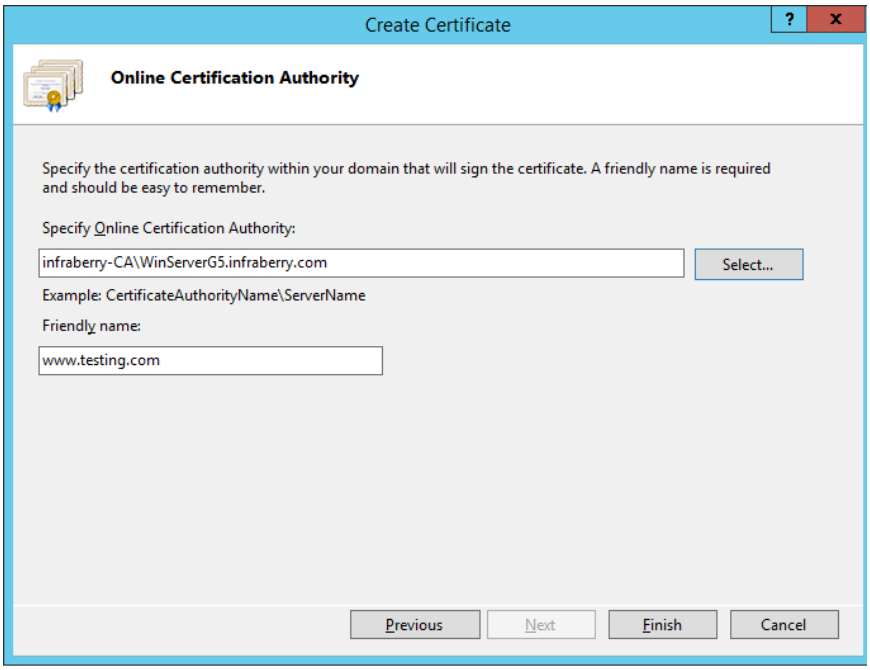


Figure 5. 137: Create Certificate

Step 34: Certificate has been created on the list ***Server Certificates***

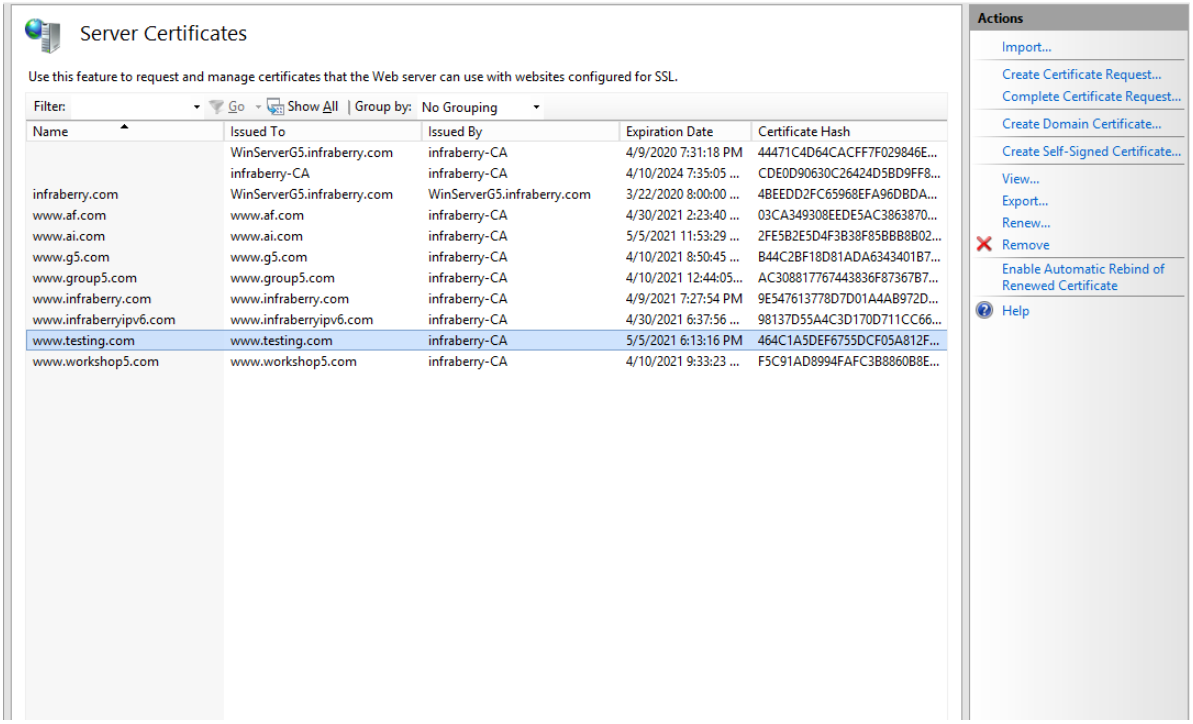


Figure 5. 138: Create Certificate

Step 35: Create new folder and html files on C:\inetpub

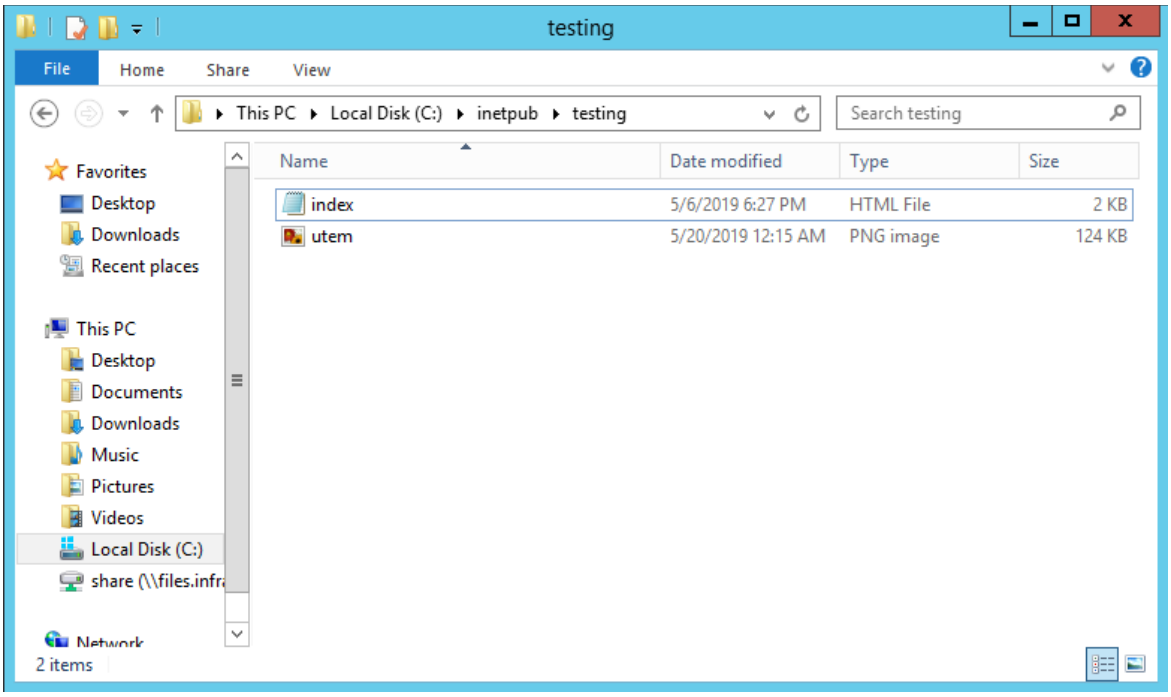


Figure 5. 139: Create folder and HTML files

Step 36: Add Website at ***Sites*** in ***Internet Information Services (IIS) Manager.***

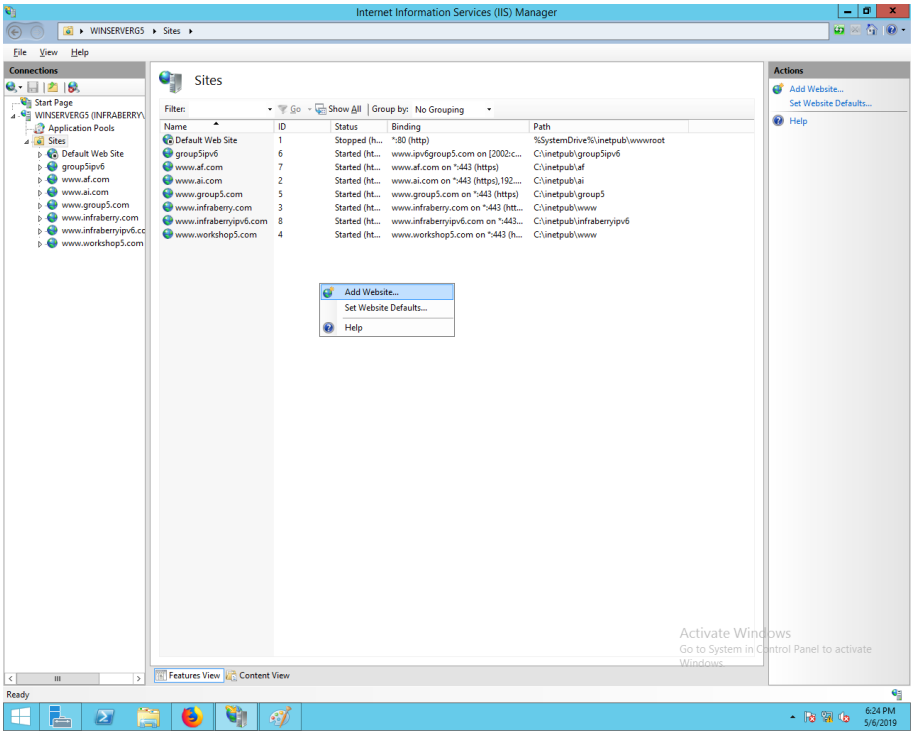


Figure 5. 140: Add Website

Step 37: Configure website form then click button ***OK***

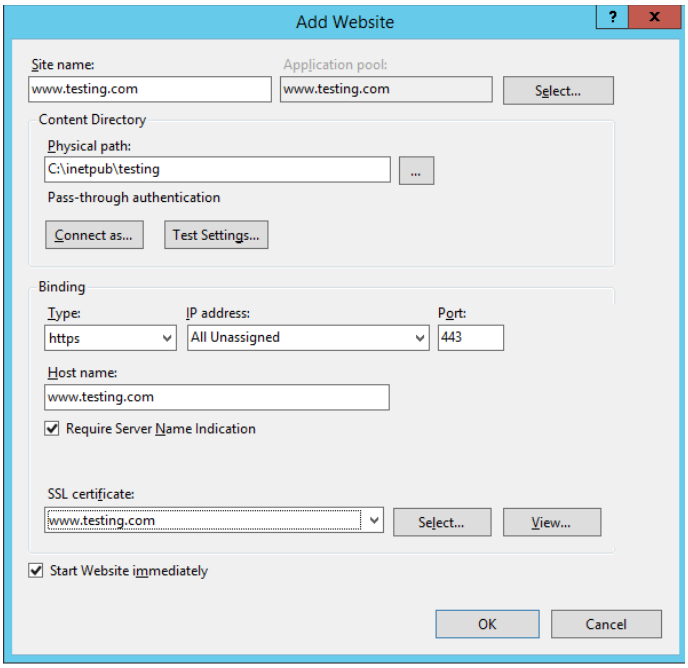


Figure 5. 141: Configure Website

Step 38: Show website that has been created

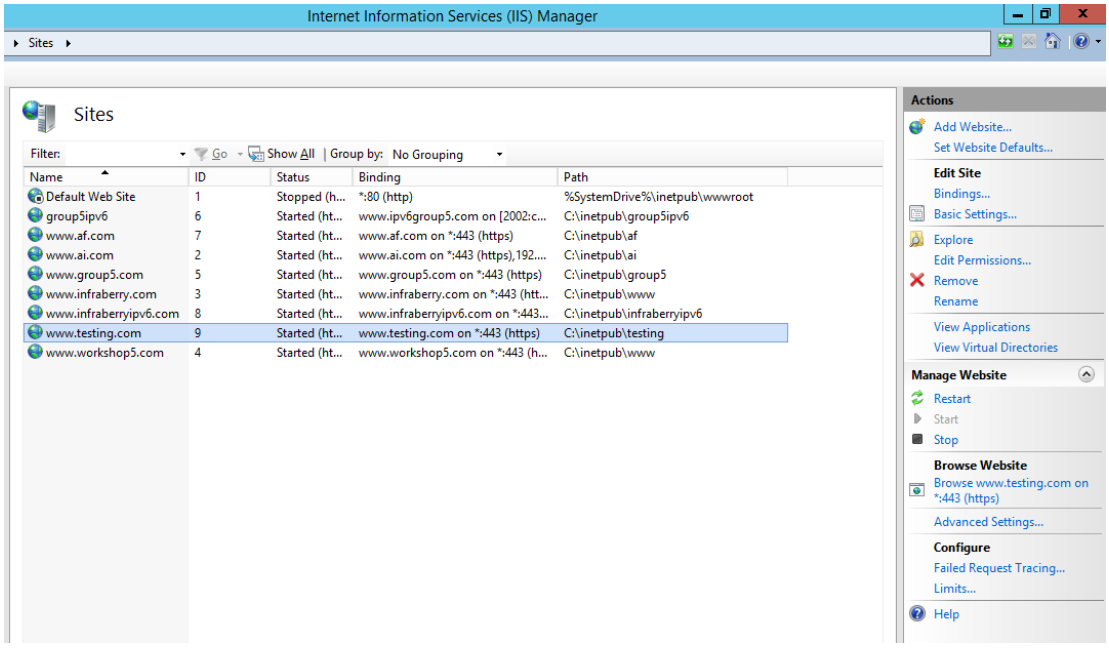


Figure 5. 142: Sites

Step 39: Open ***DNS Manager*** then create ***New Zone*** in ***Forward Lookup Zones.***

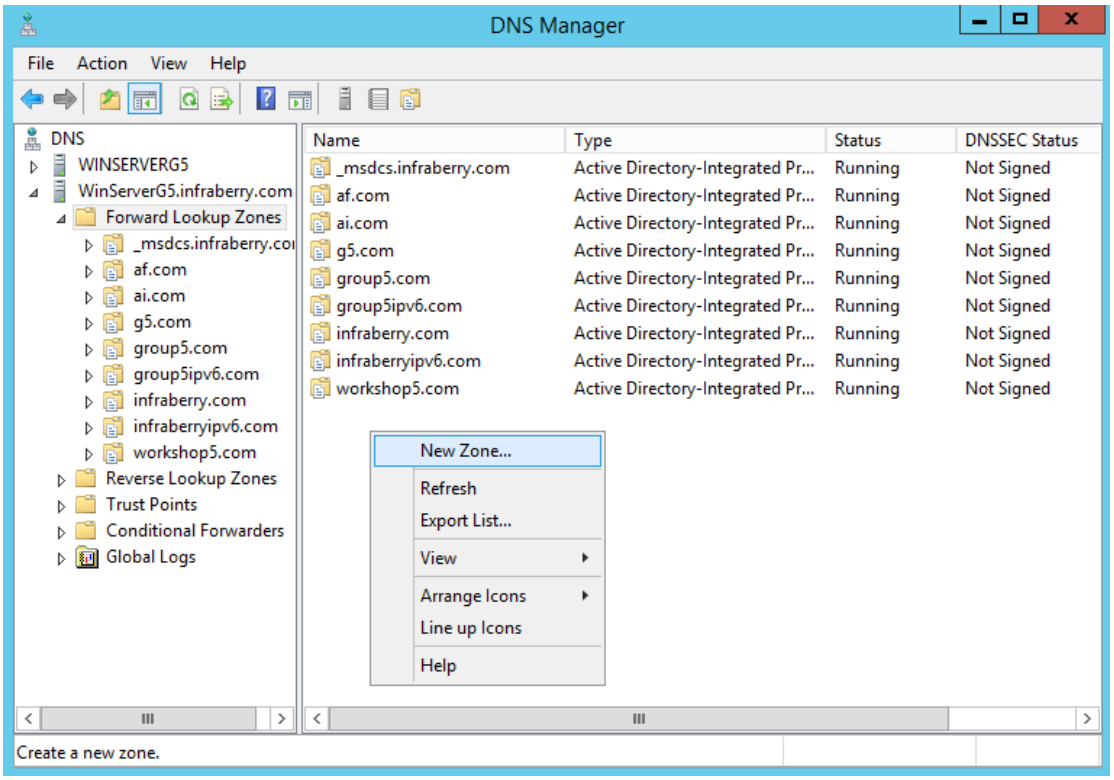


Figure 5. 143: DNS Manager

Step 40: Click button ***Next.***

Figure 5. 144: New Zone Wizard

Step 41: Choose type of zone then click button ***Next***

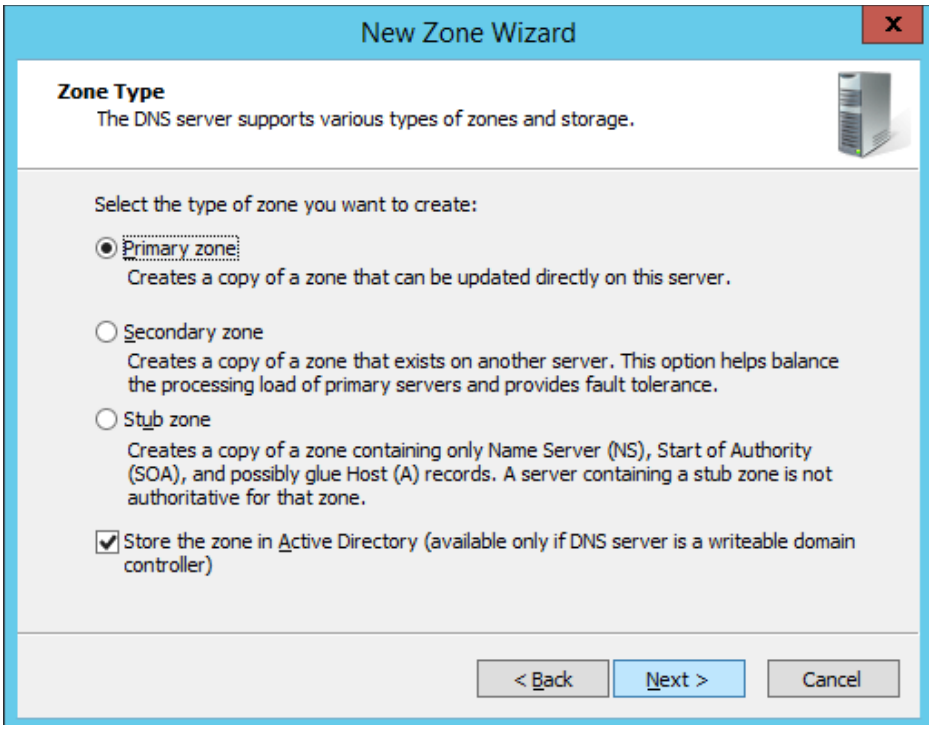


Figure 5. 145: Zone type

Step 42: Choose ***Active Directory Zone Replication Scope*** then click button ***Next.***

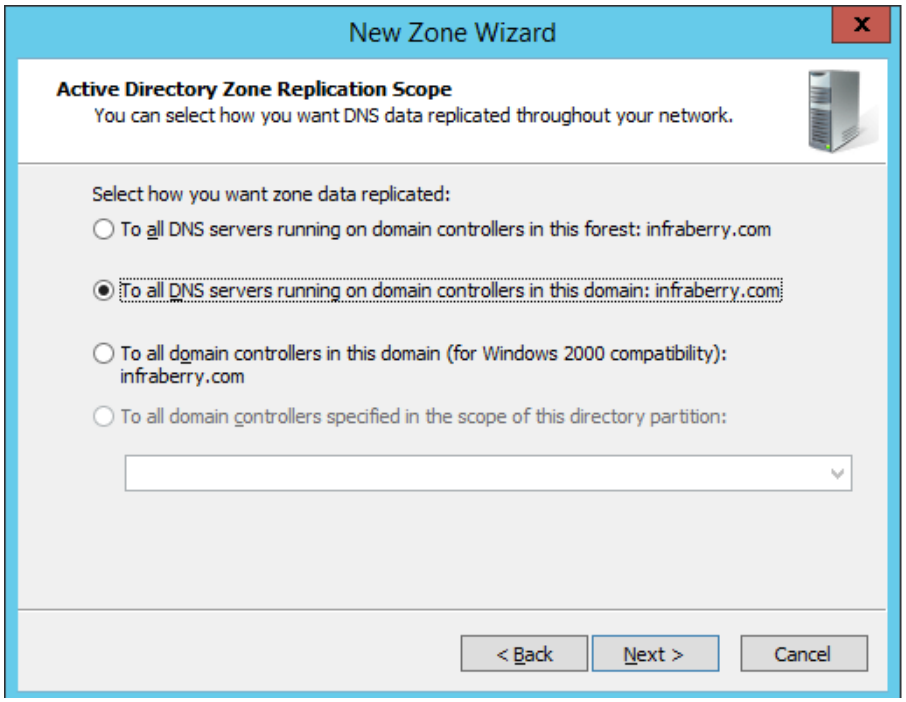


Figure 5. 146: Active Directory Zone Replication Scope

Step 43: Fill up ***Zone Name*** then click ***Next.***

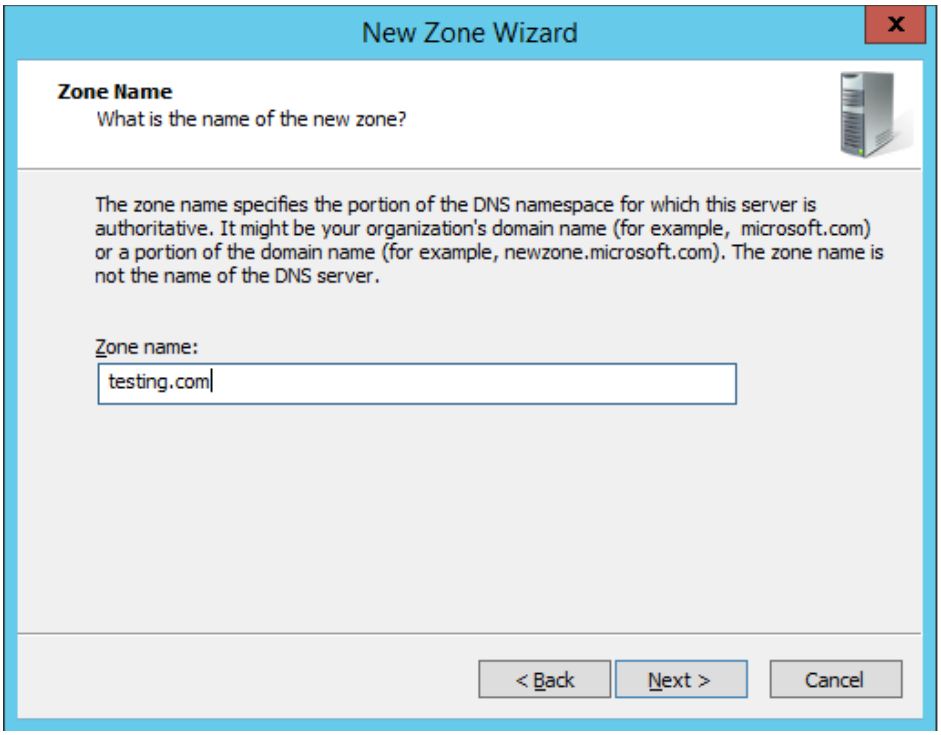


Figure 5. 147: Zone Name

Step 44: Choose ***Dyanamic Update*** then click button ***Next.***

Figure 5. 148: Dynamic Update

Step 45: ***New Zone Wizard*** has been created then click button ***Finish***.

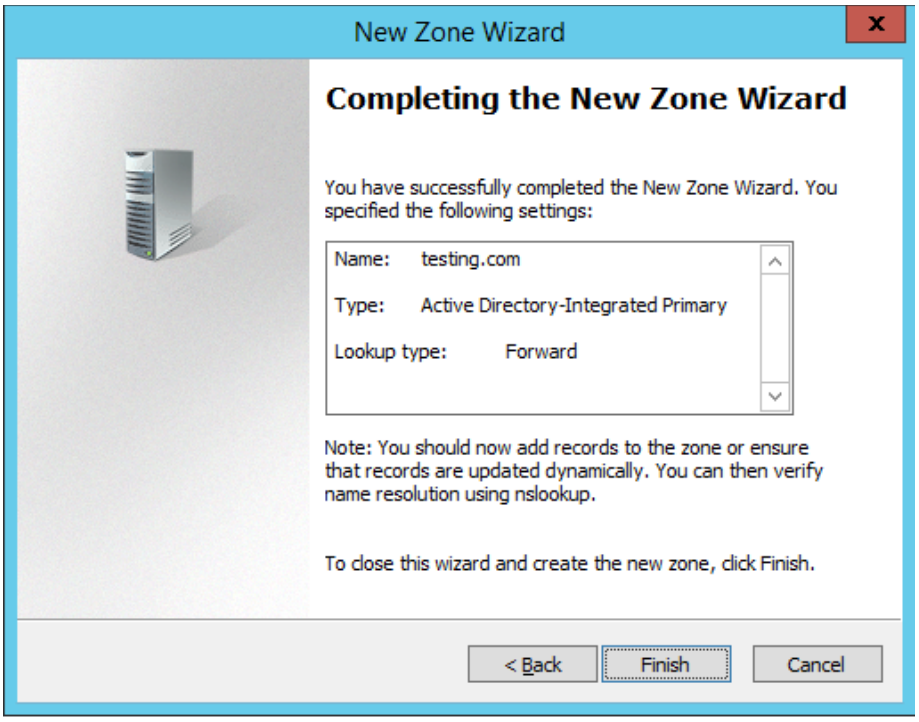


Figure 5. 149: Completing the New Zone Wizard

Step 46: List ***New Zone*** that has been created in ***Forward Lookup Zones***.

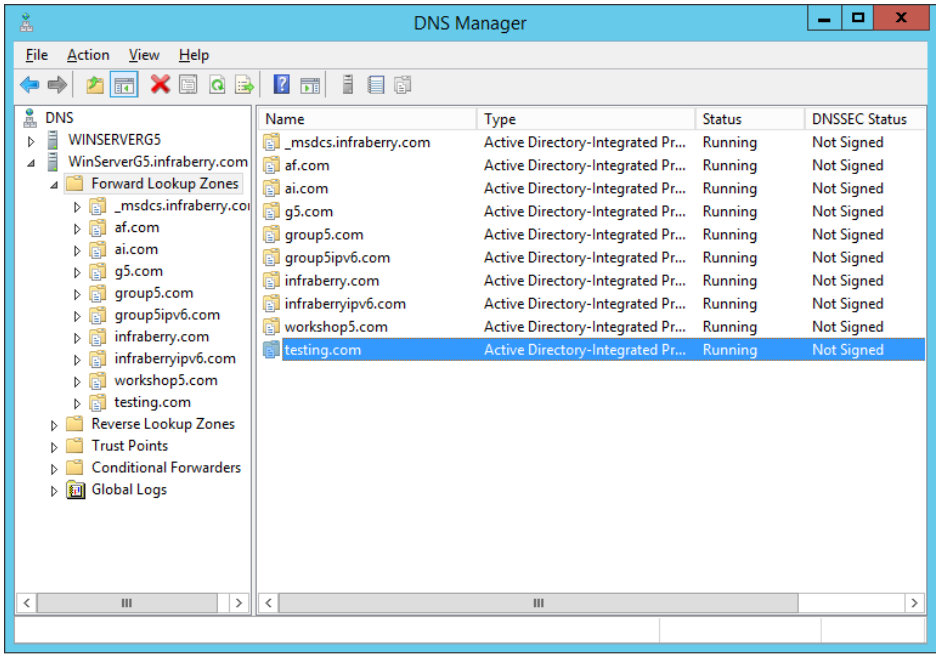


Figure 5. 150: Forward Lookup Zones

Step 47: Open ***Zone*** that has been create then create ***New Host (A or AAAA).***

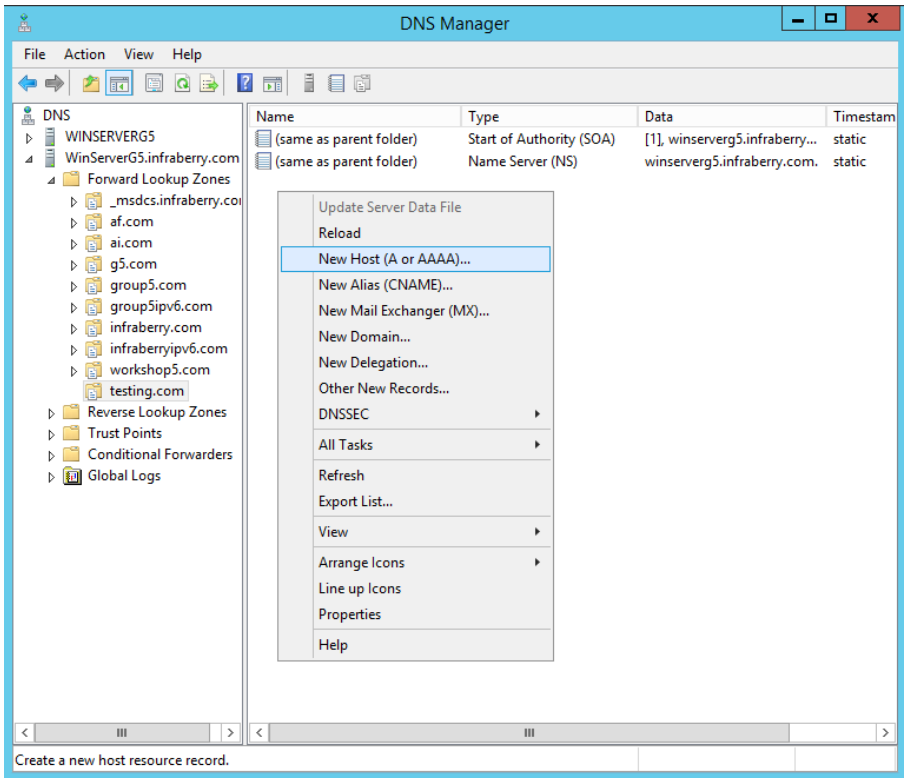


Figure 5. 151: New Host (A or AAAA)

Step 48: Fill in the ***Name*** and ***IP Address*** then click button ***Add Host.***

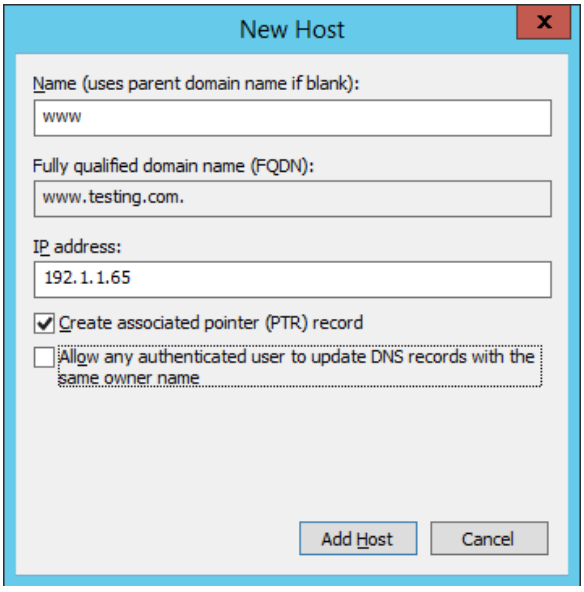


Figure 5. 152: New Host (A or AAAA)

Step 49: Show the ***New Host (A or AAAA)*** that has been create.

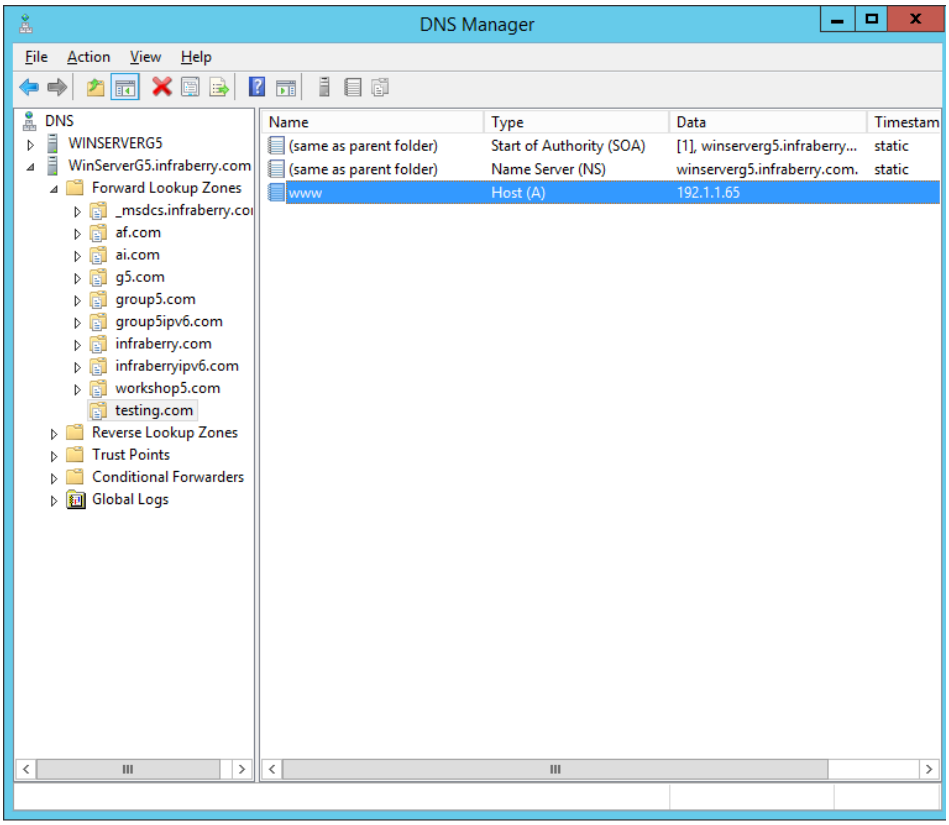


Figure 5. 153: New Host (A or AAAA)

5.3.8 Wireless User Authentication Using Radius Server

Step 1: Open ***Server Manager*** then click ***Add Roles and Features.***

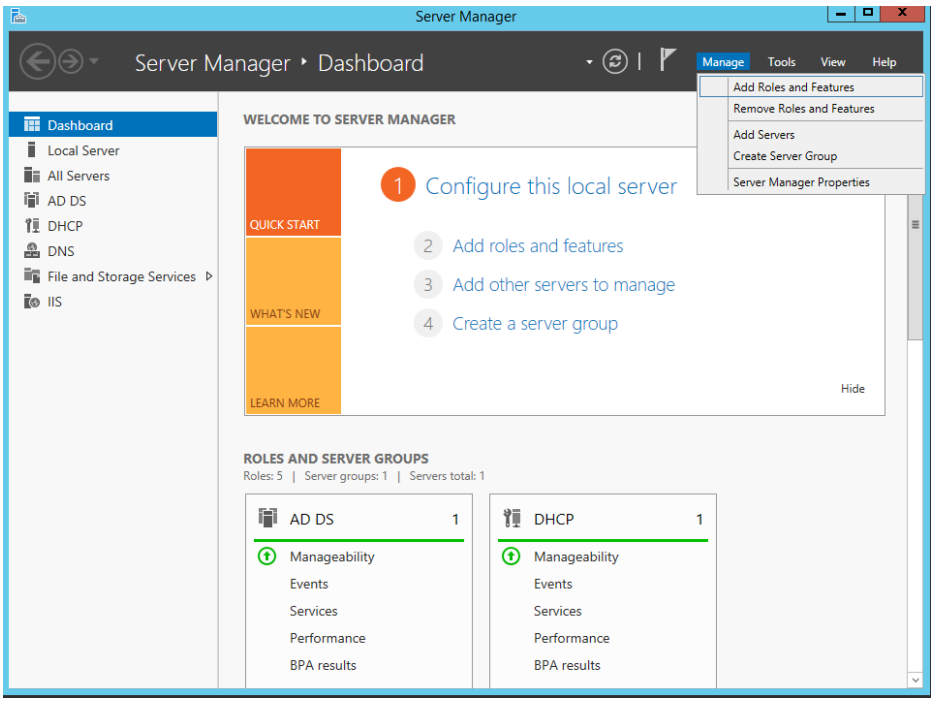


Figure 5. 154: Server Manager

Step 2: Click button ***Next.***

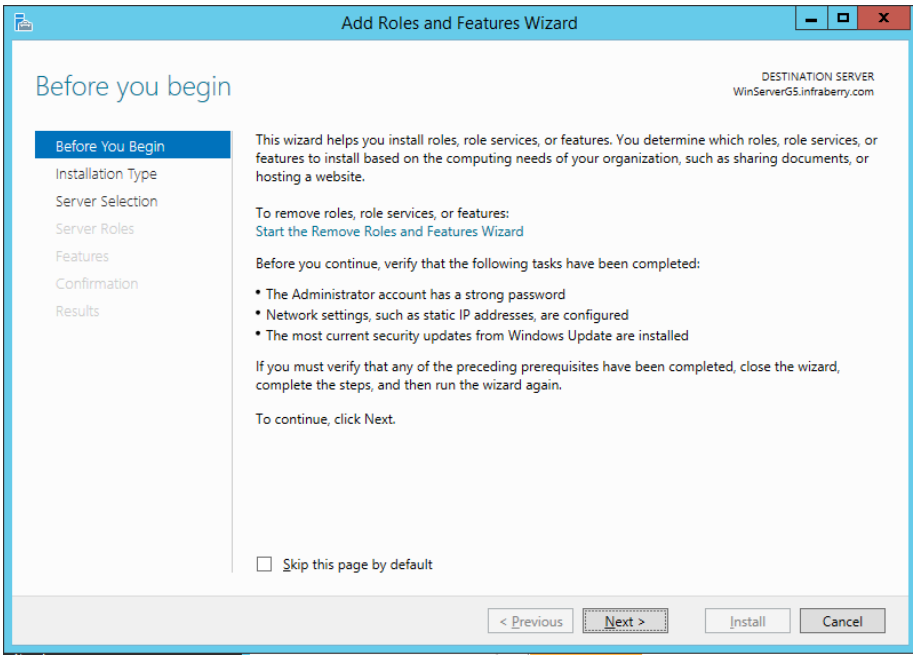


Figure 5. 155: Add Roles and Features Wizard

Step 3: Choose ***Installation Type*** then click button ***Next***.

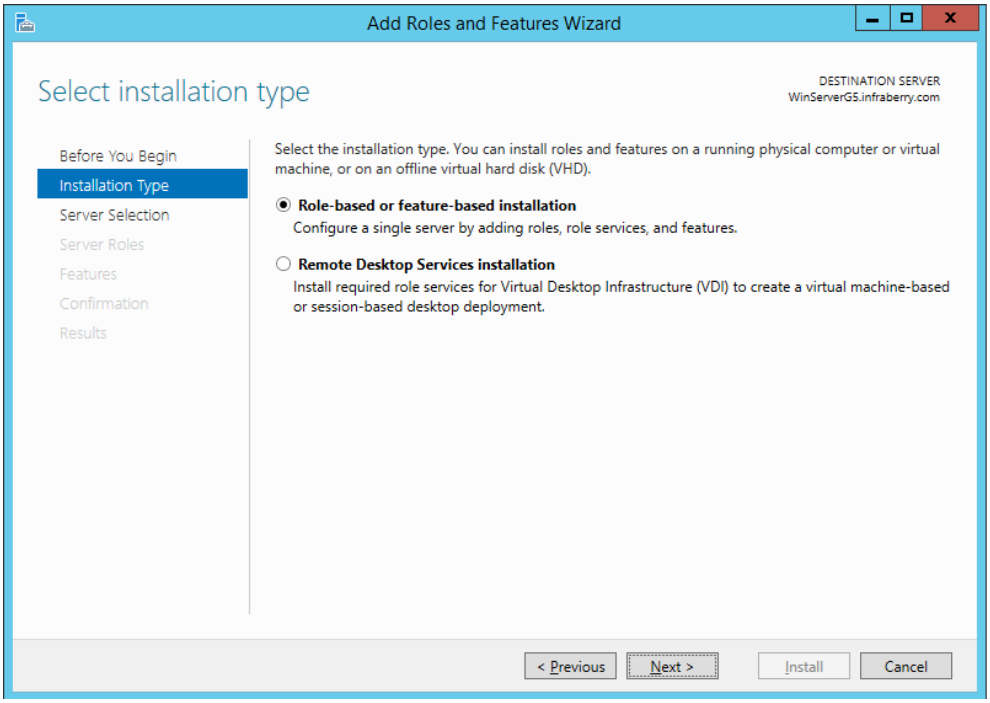


Figure 5. 156: Add Roles and Features Wizard

Step 4: Choose ***Server Selection*** then click button ***Next.***

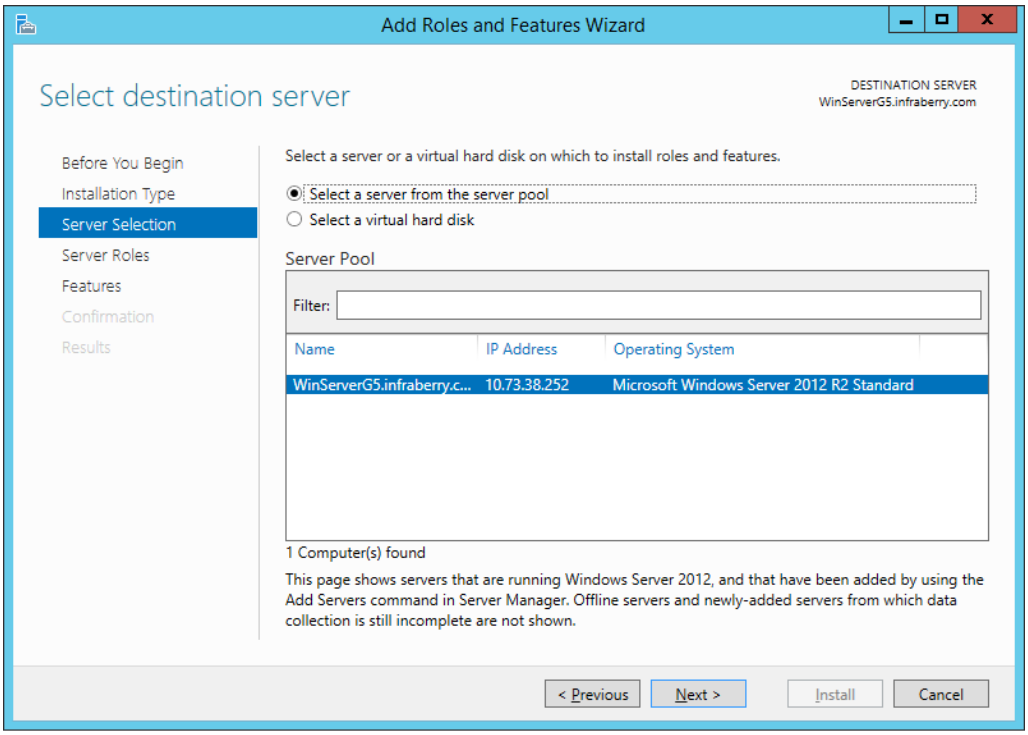


Figure 5. 157: Server Selection

Step 5: Tick on ***Network Policy and Access Services*** then click button ***Next.***

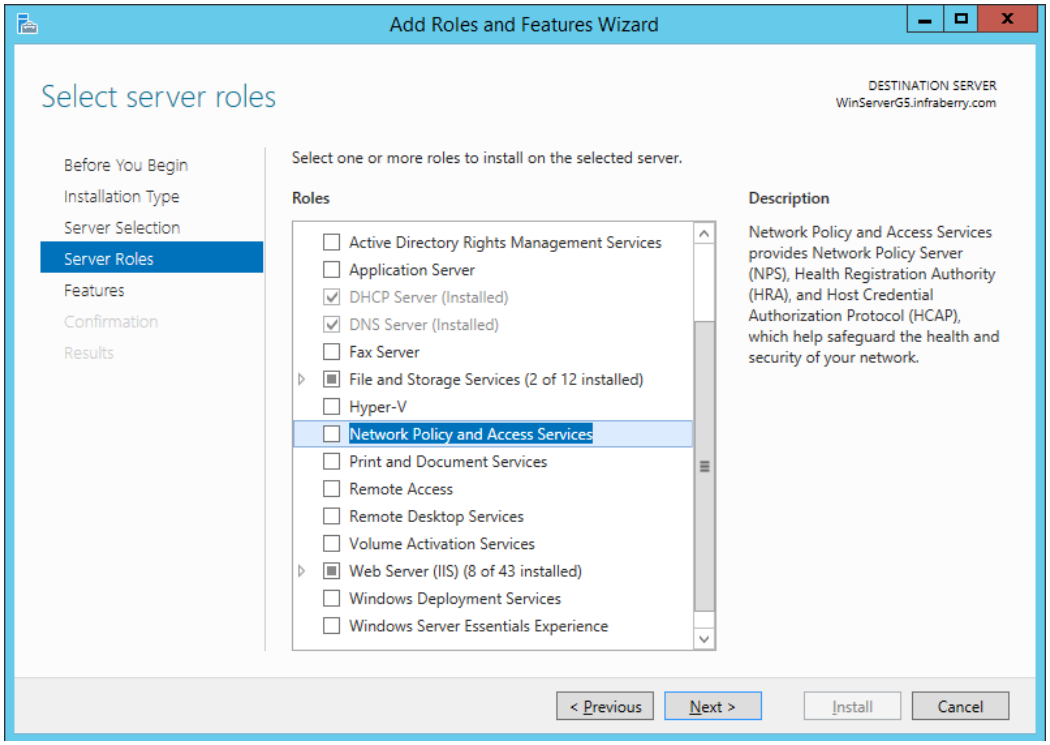


Figure 5. 158: Server Roles

Step 6: Click button ***Add Features.***

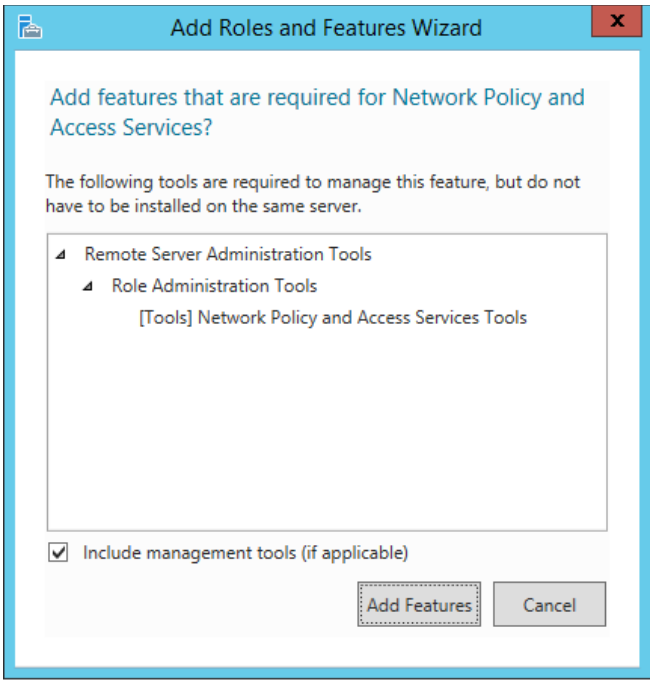


Figure 5. 159: Add Features

Step 7: ***Network Policy and Access Services*** has been tick then click button ***Next***

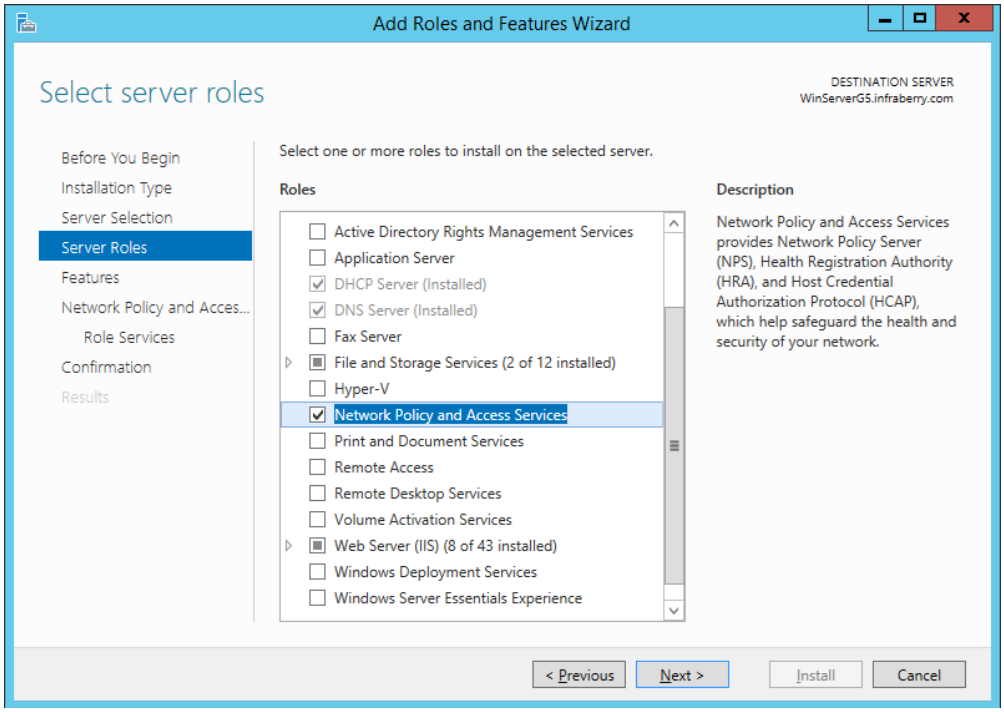


Figure 5. 160: Server Roles

Step 8: Click button ***Next***

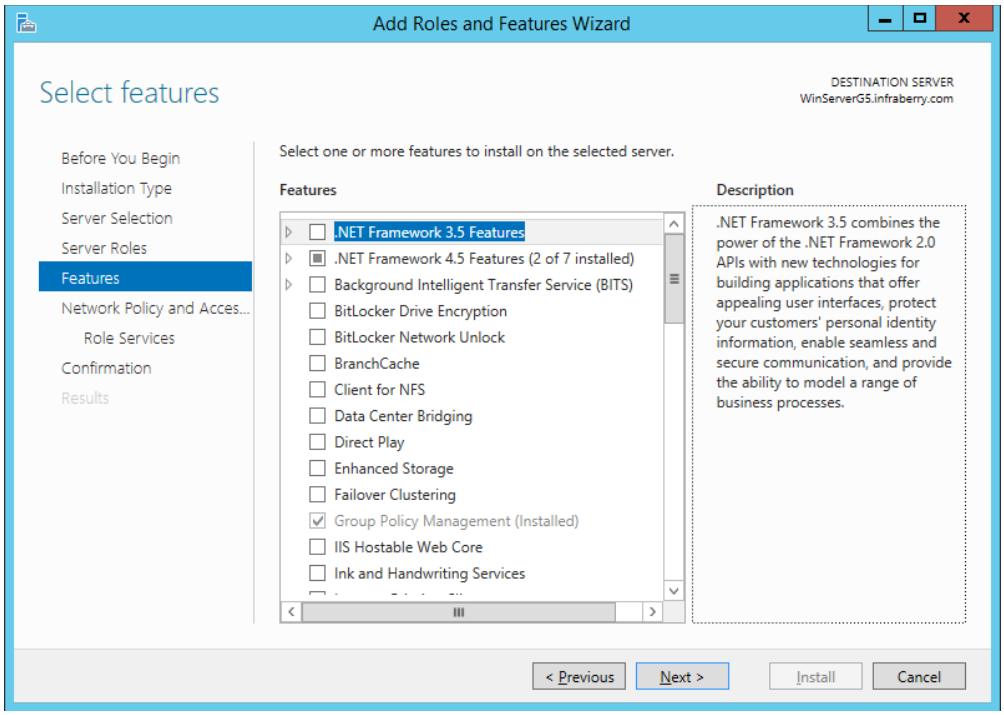


Figure 5. 161: Features

Step 9: Click button ***Next.***

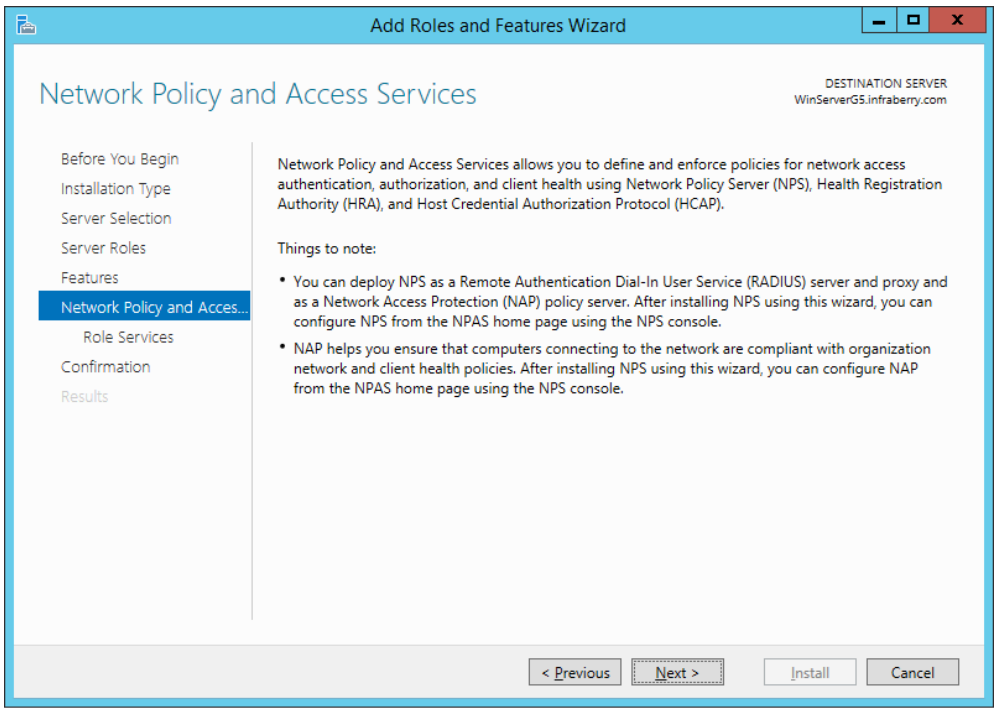


Figure 5. 162: Features

Step 10: Tick ***Network Policy Server*** then click button ***Next.***

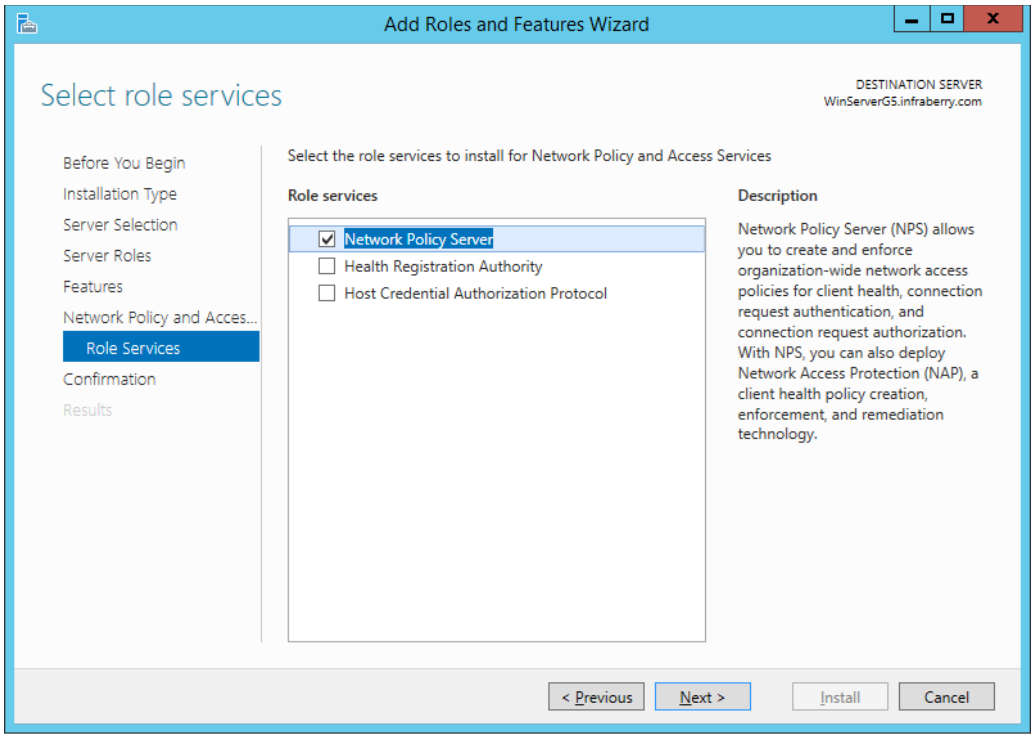


Figure 5. 163: Features

Step 11: Click button ***Install.***

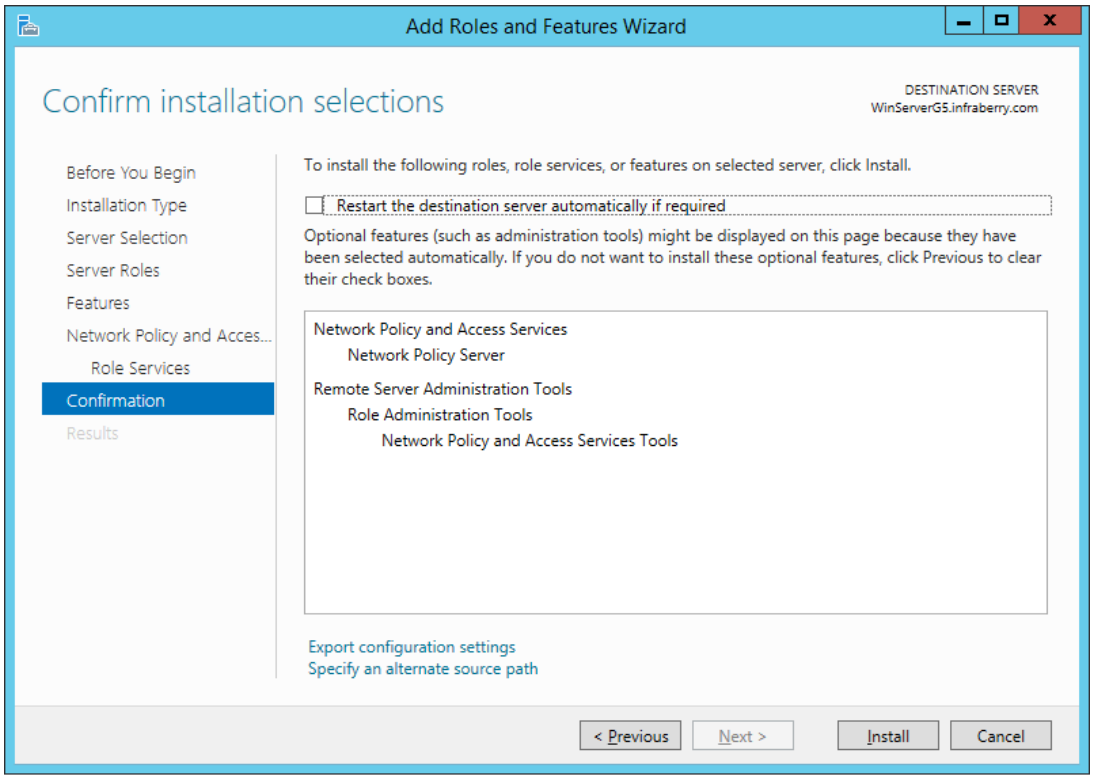


Figure 5. 164: Features

Step 12: Open ***Network Policy*** Server then ***Register server in Active Directory.***

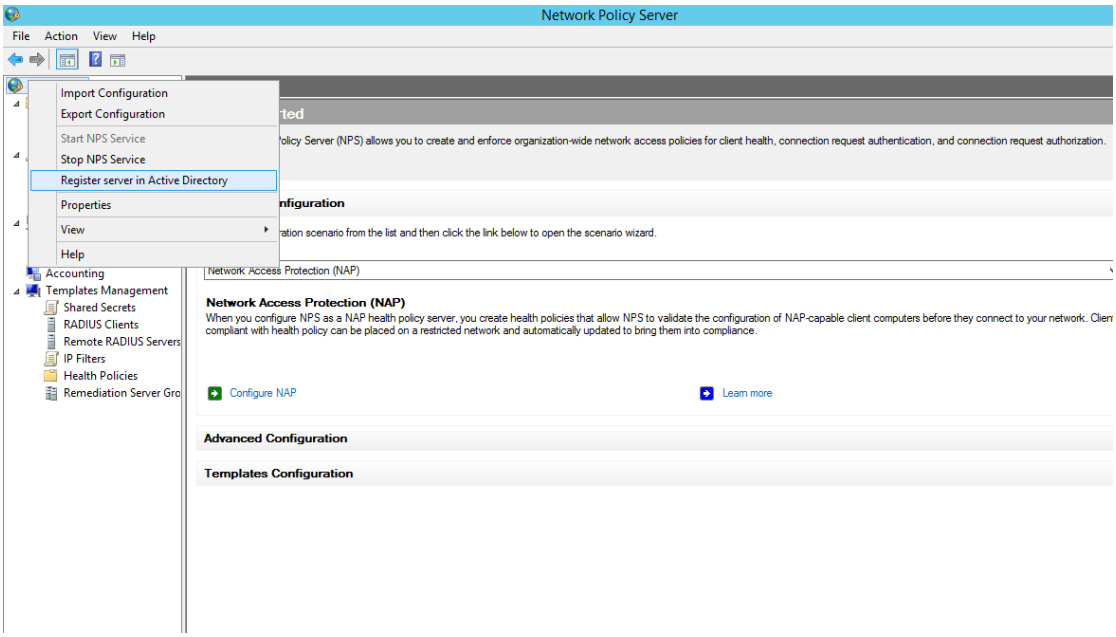


Figure 5. 165: Network Policy Server

Step 13: Click button ***OK.***

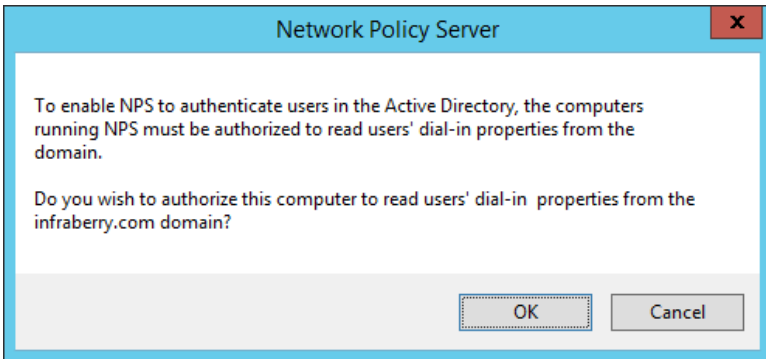


Figure 5. 166: Network Policy Server

Step 14: Click button ***OK.***

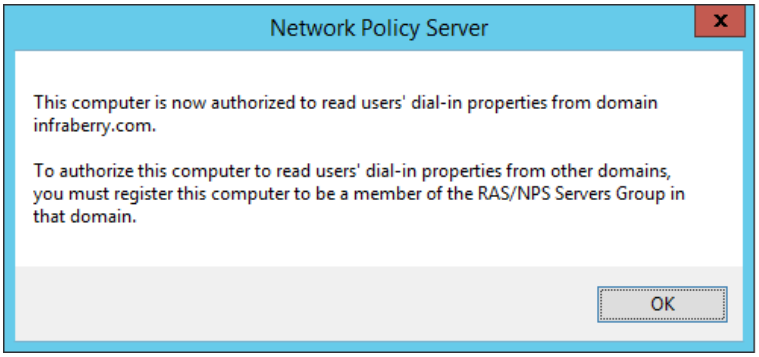


Figure 5. 167: Network Policy Server

Step 15: Create ***New RADIUS Clients*** in Network Policy Server.

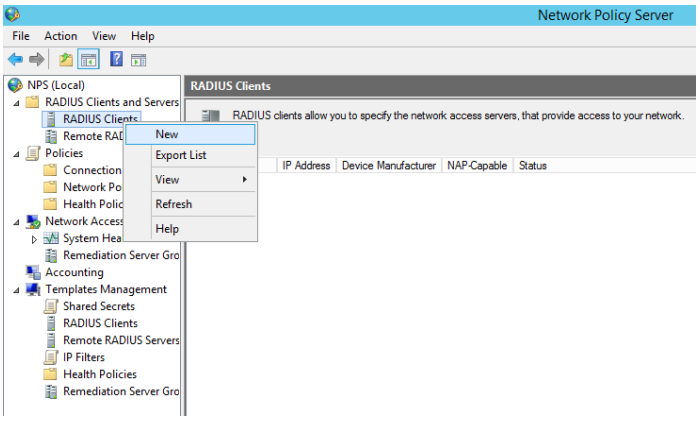


Figure 5. 168: RADIUS Clients

Step 16: Fill up the form in ***wap Properties.***

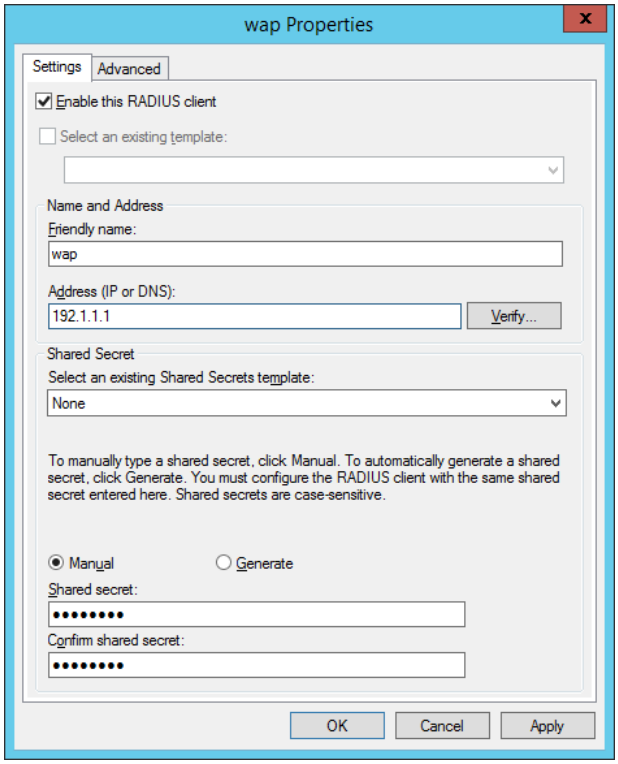


Figure 5. 169: wap Properties

Step 17: Create ***New User*** in ***Active Directory Users and Computers***.

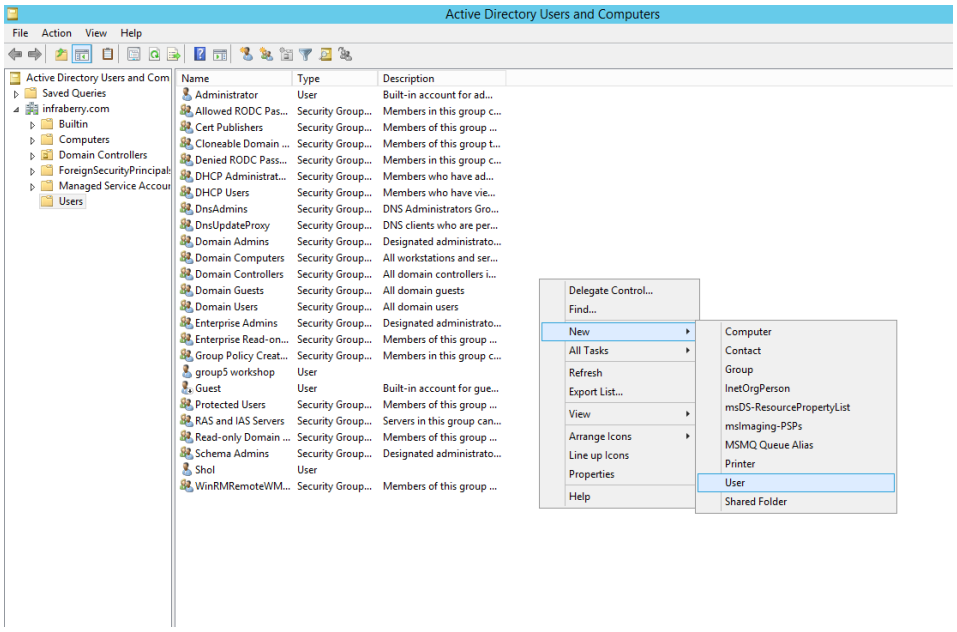


Figure 5. 170: Active Directory Users and Computers

Step 18: Create ***New Object – User*** then click button ***Next***.

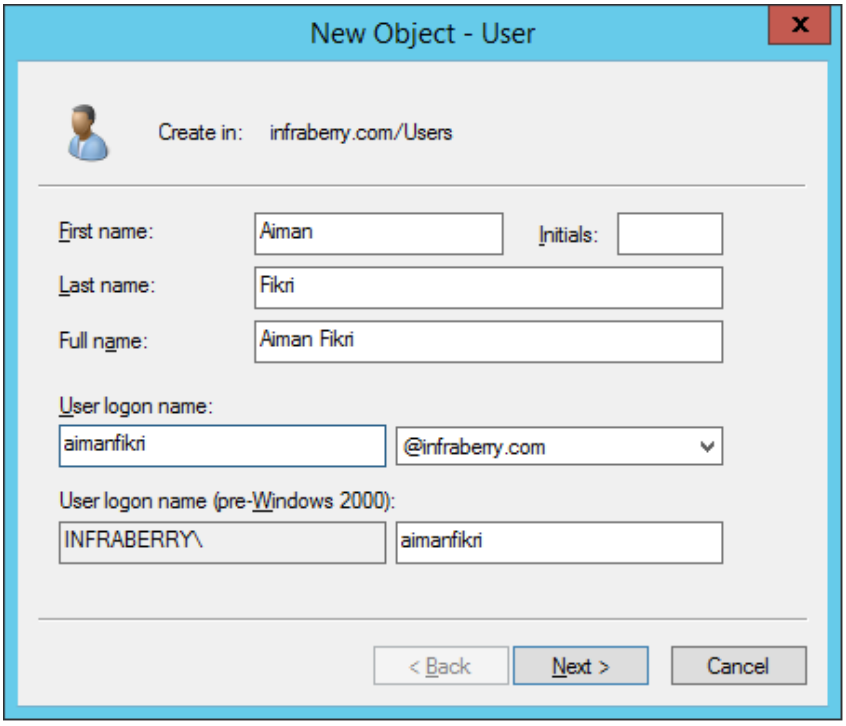


Figure 5. 171: New Object – User

Step 19: Fill up password and tick ***Passord never expires*** then click button ***Next.***

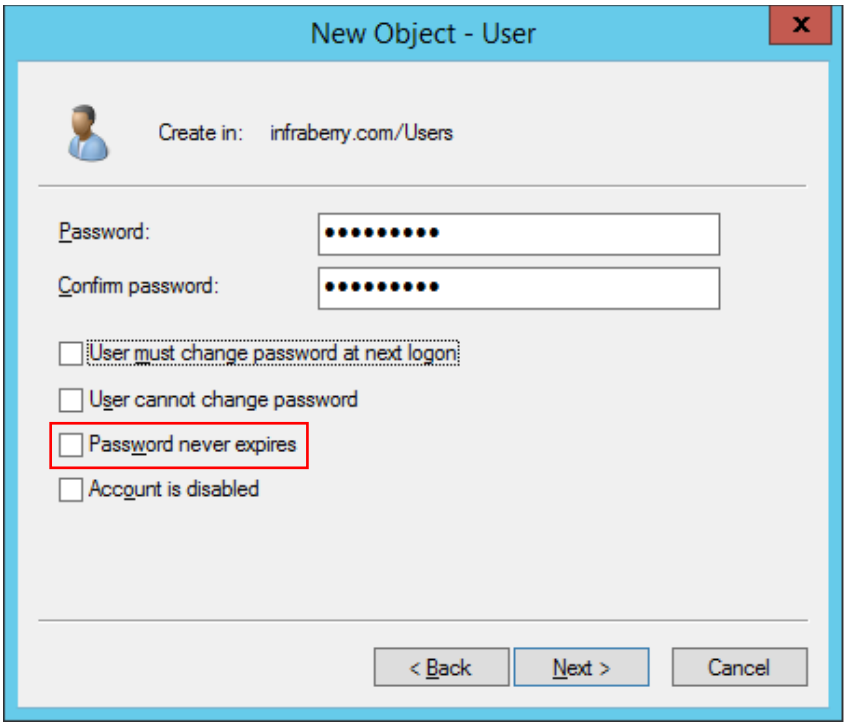


Figure 5. 172: New Object – User

Step 20: Click button ***Finish.***

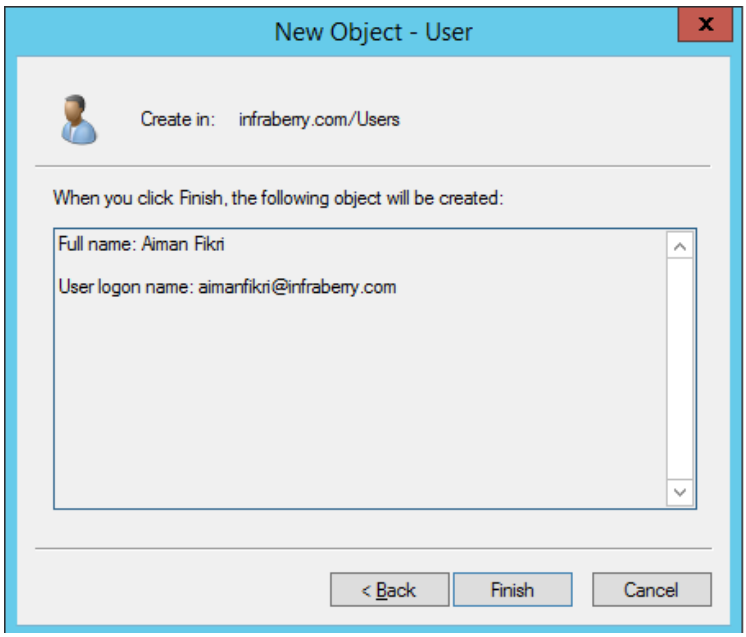


Figure 5. 173: New Object – User

Step 21: Show user that has been create.

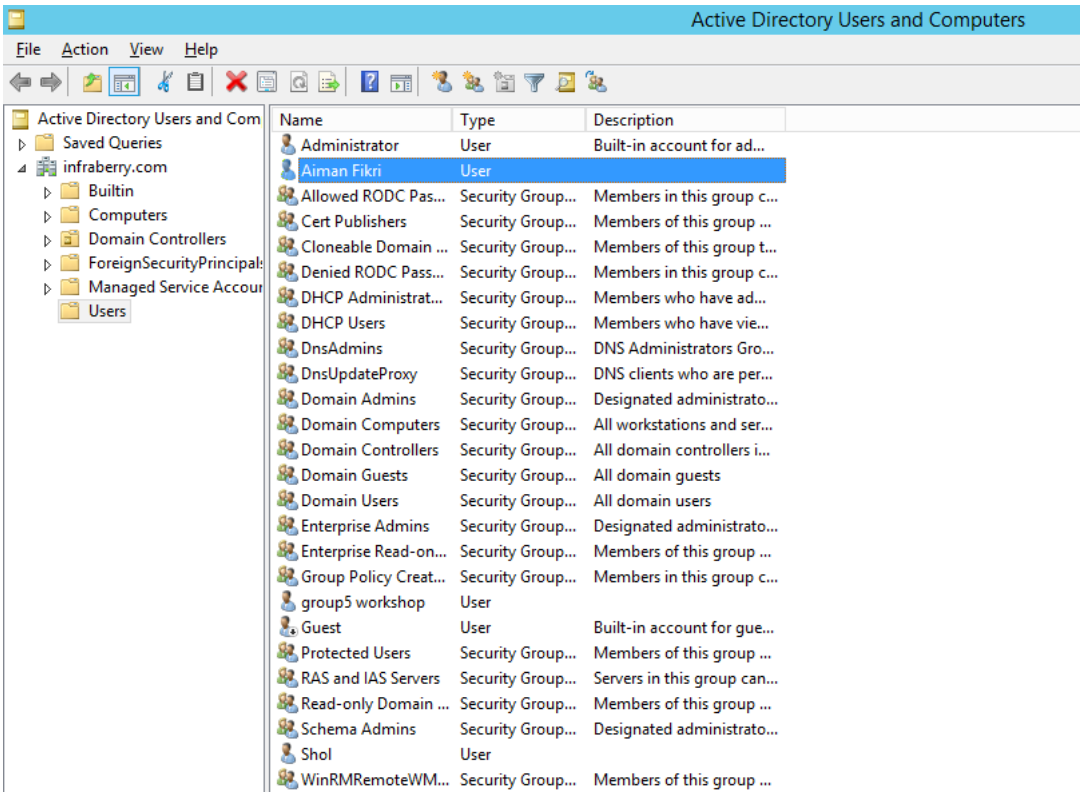


Figure 5. 174: Active Directory Users and Computers

Step 22: Create ***New Group*** in ***Active Directory Users and Computers.***

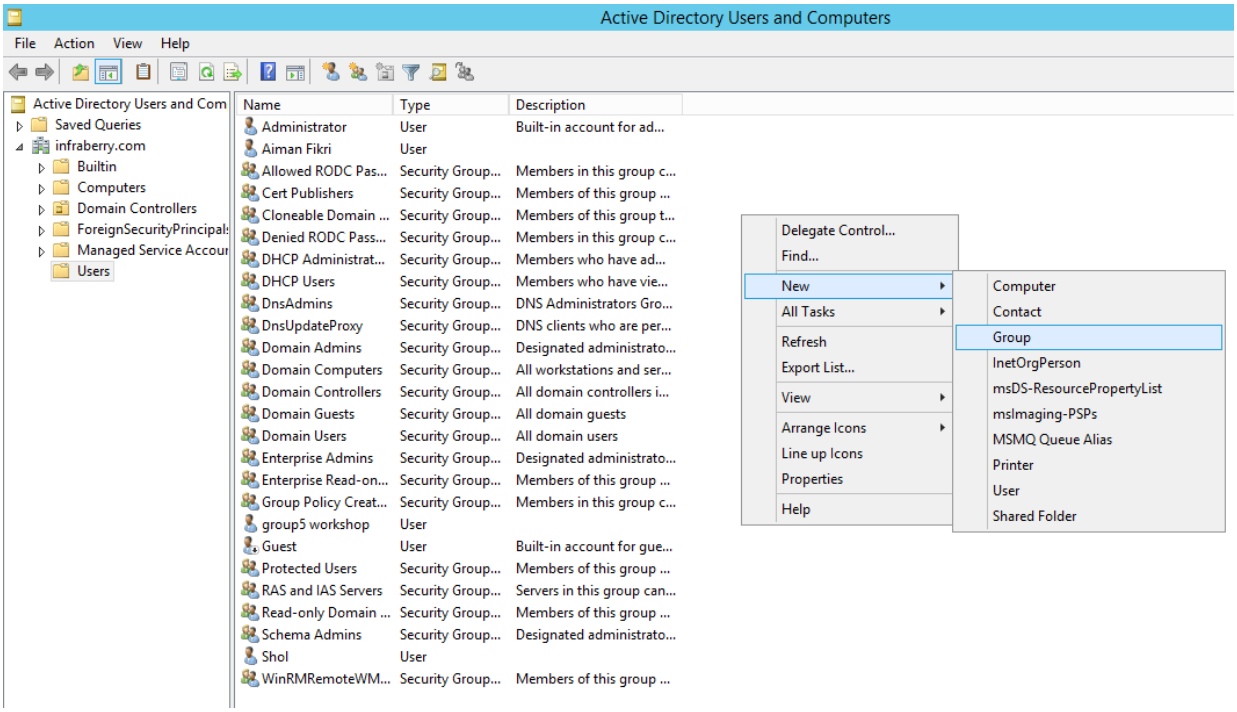


Figure 5. 175: Active Directory Users and Computers

Step 23: Fill up ***New Object – Group*** then click button ***OK.***

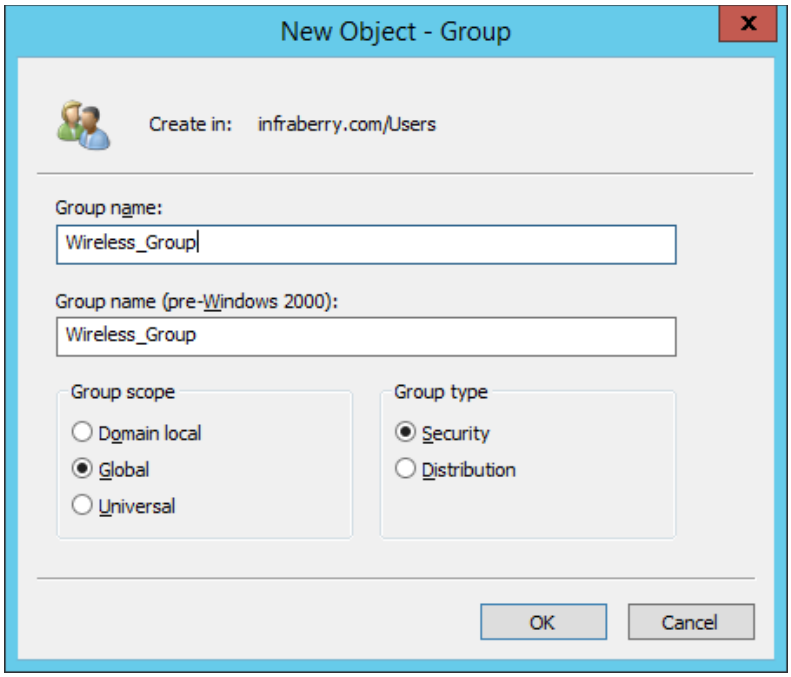


Figure 5. 176: Active Directory Users and Computers

Step 24: Select User that has been create to Wireless_Group then click button ***OK.***

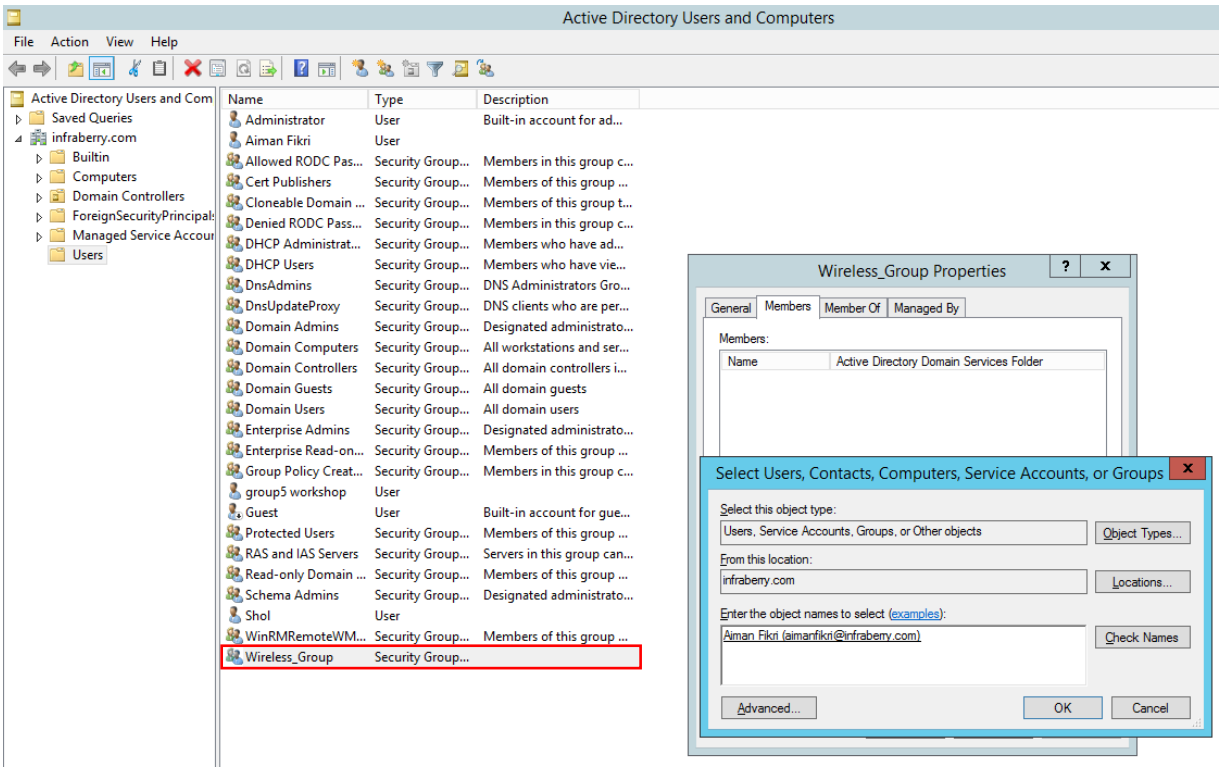


Figure 5. 177: Wireless_Group Properties

Step 25: Click button ***OK.***

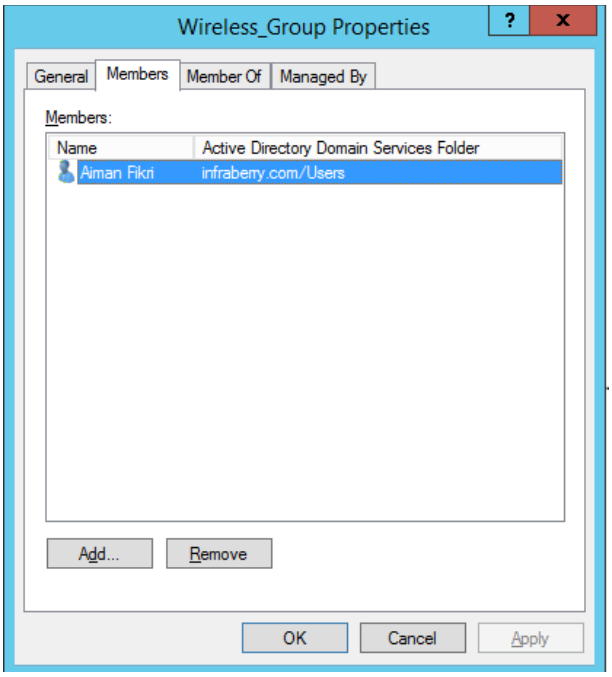


Figure 5. 178: Wireless_Group Properties

Step 26: Create ***New Connection Request Policy***

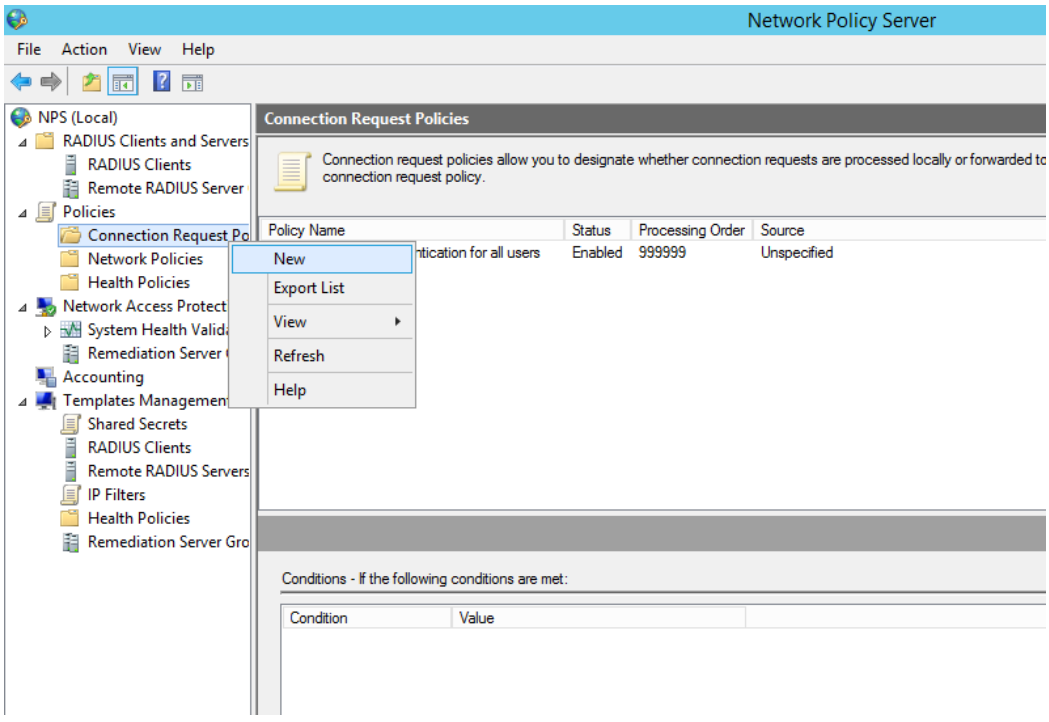


Figure 5. 179: Network Policy Server

Step 27: Fill in ***Policy Name*** then click button ***Next.***

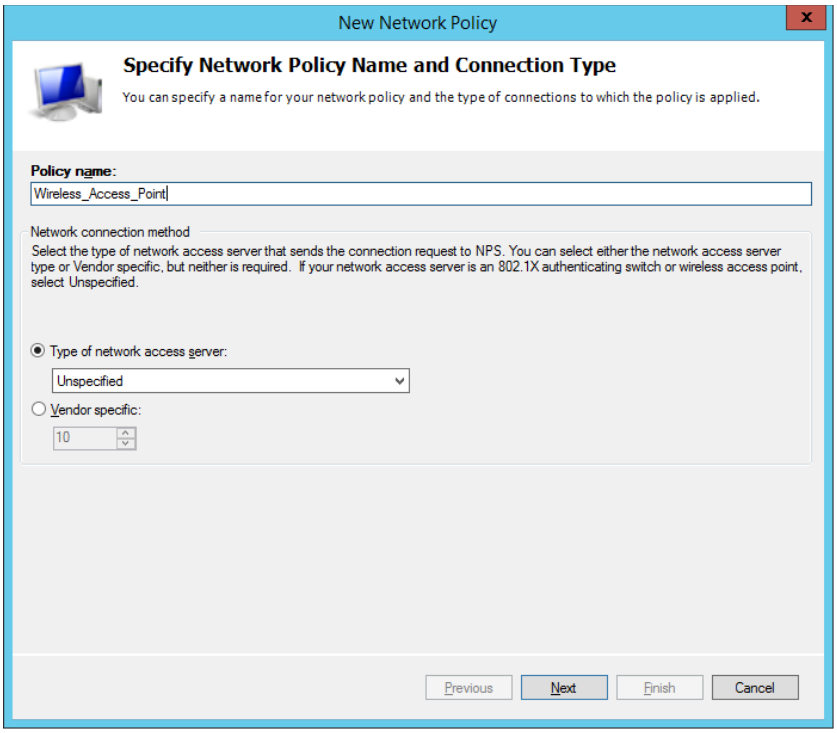


Figure 5. 180: New Network Policy

Step 28: Select condition then click button ***Add.***

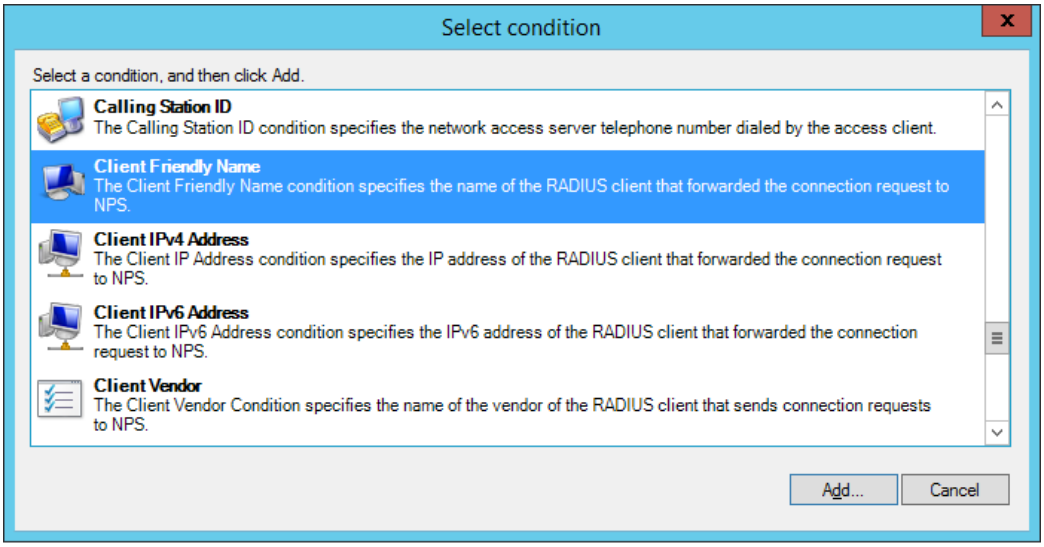


Figure 5. 181: Select Condition

Step 29: Click button ***OK.***

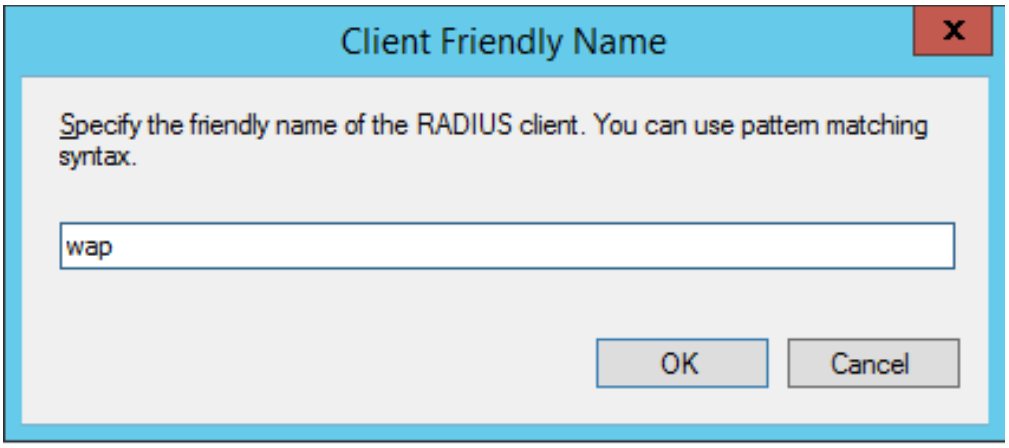


Figure 5. 182: Client Friendly Name

Step 30: Click button ***Next.***

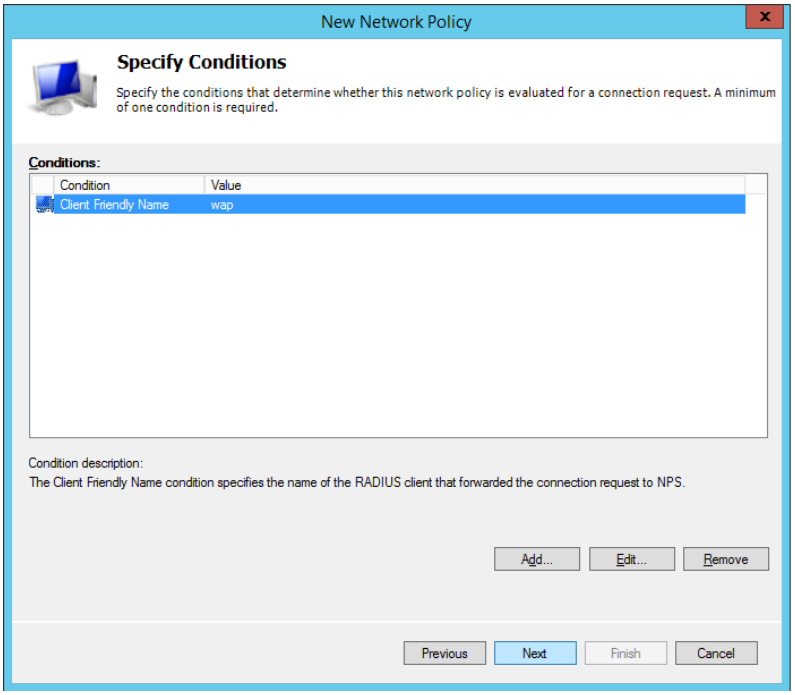


Figure 5. 183: New Network Policy

Step 31: Click button ***Next.***

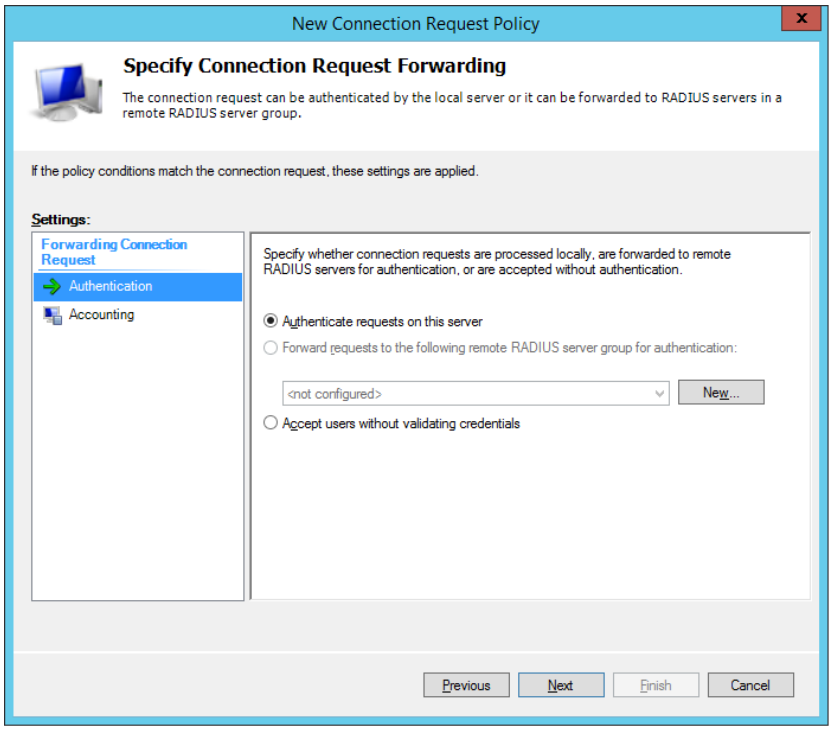


Figure 5. 184: New Connection Request Policy

Step 32: Click button ***Next.***

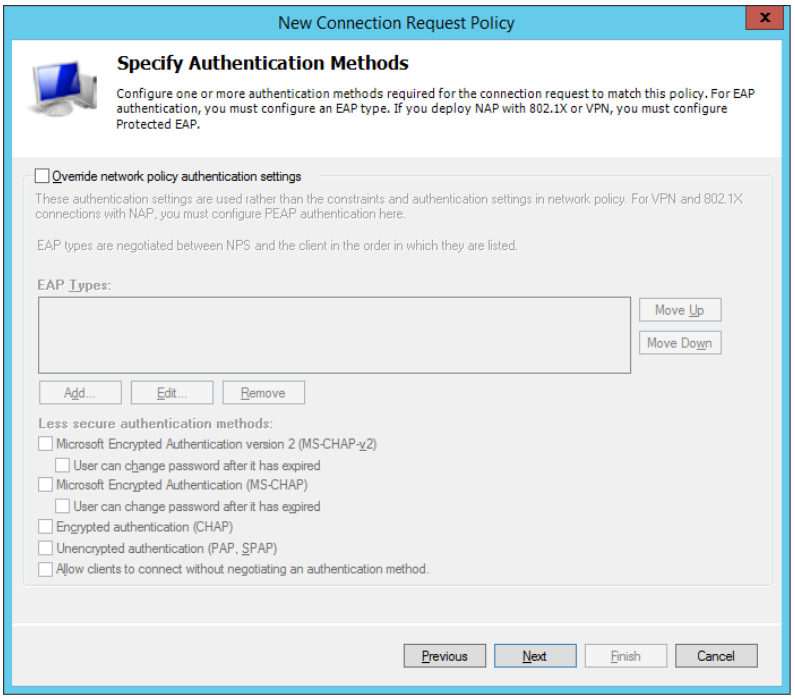


Figure 5. 185: New Connection Request Policy

Step 33: Click button ***Next.***

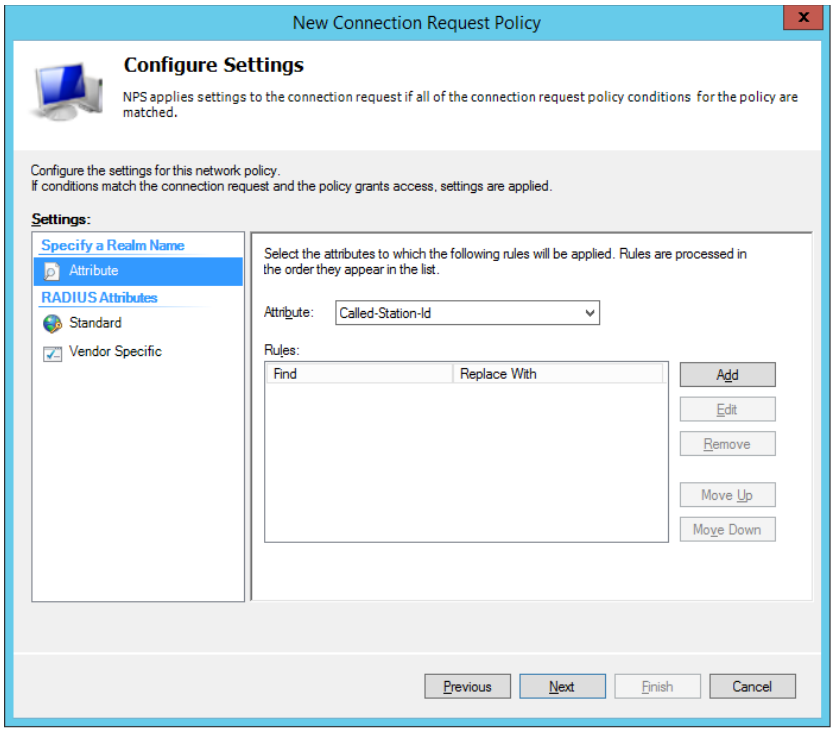


Figure 5. 186: New Connection Request Policy

Step 34: Click button ***Finish.***

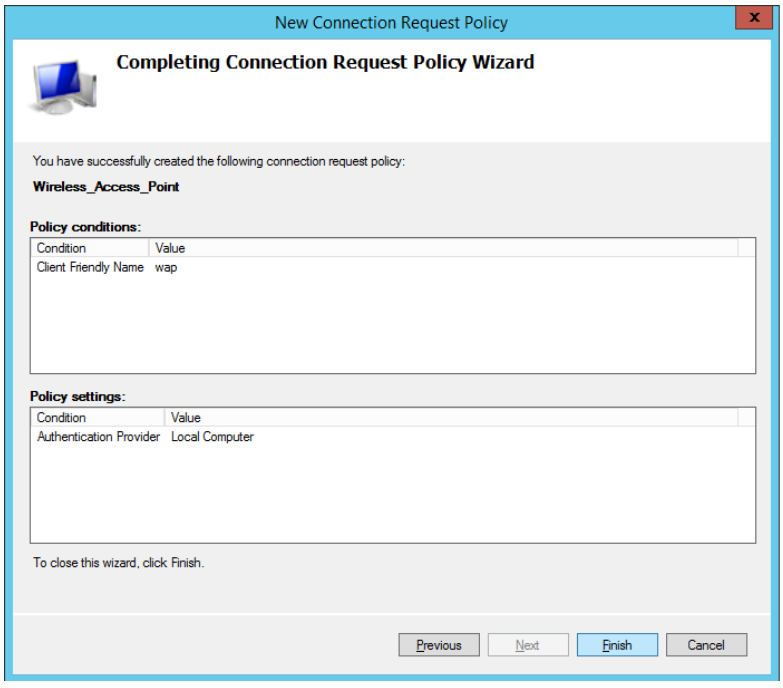


Figure 5. 187: New Connection Request Policy

Step 35: Show New Connection Request Policy that has been create.

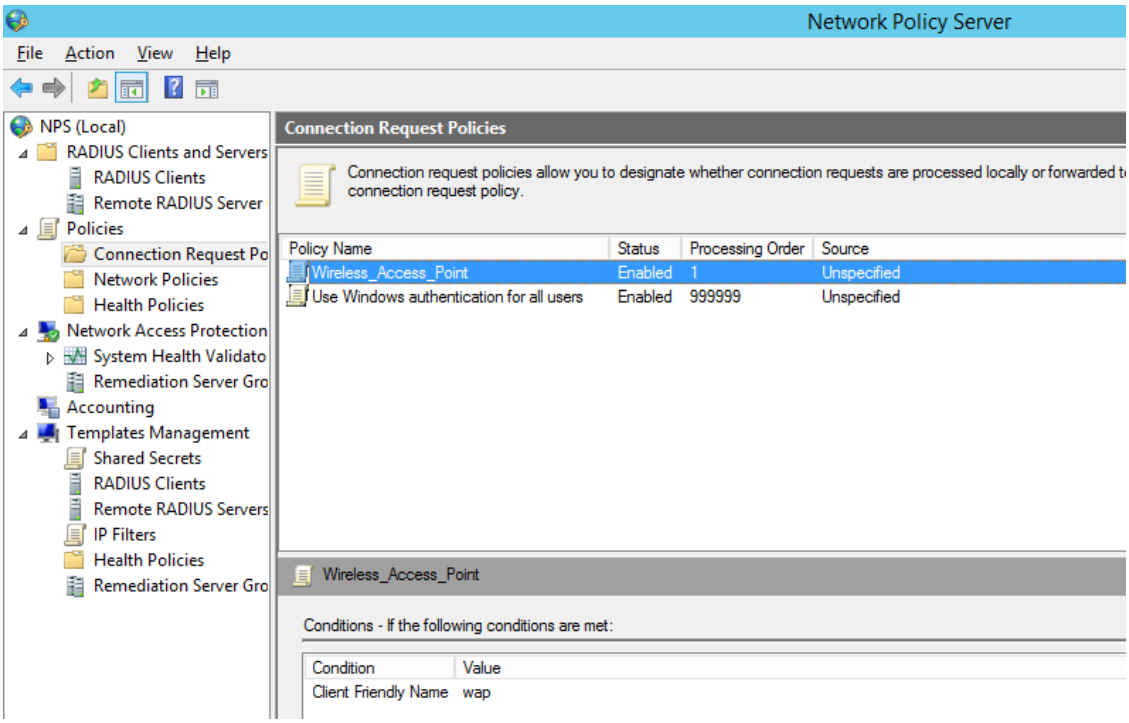


Figure 5. 188: Network Policy Server

Step 36: Create New Network Policies

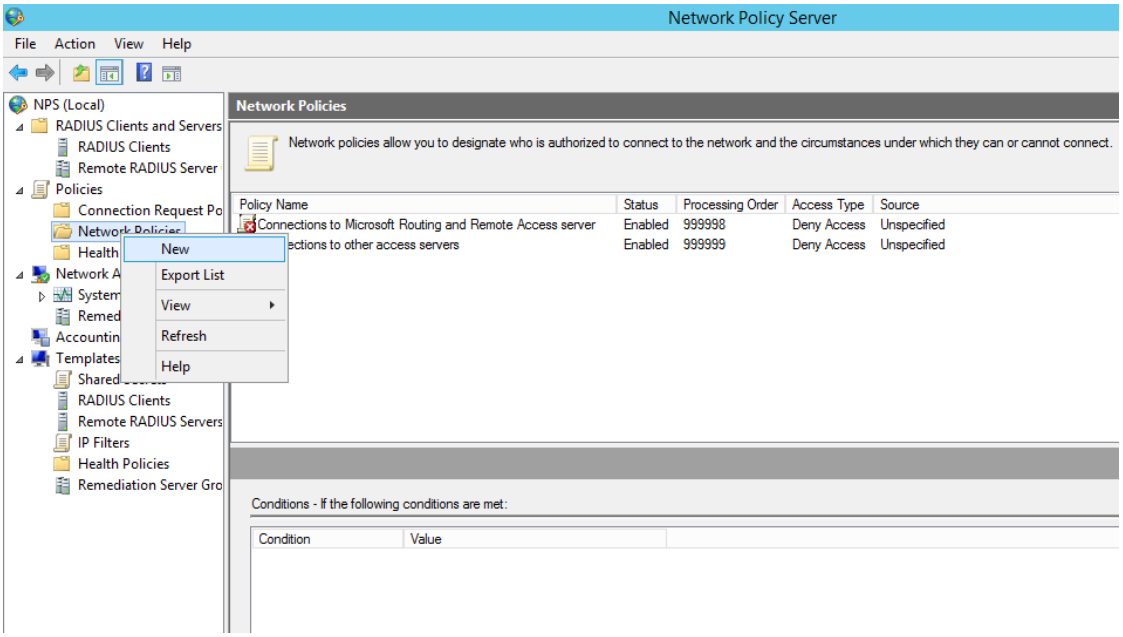


Figure 5. 189: Network Policy Server

Step 37: Click button ***Next.***

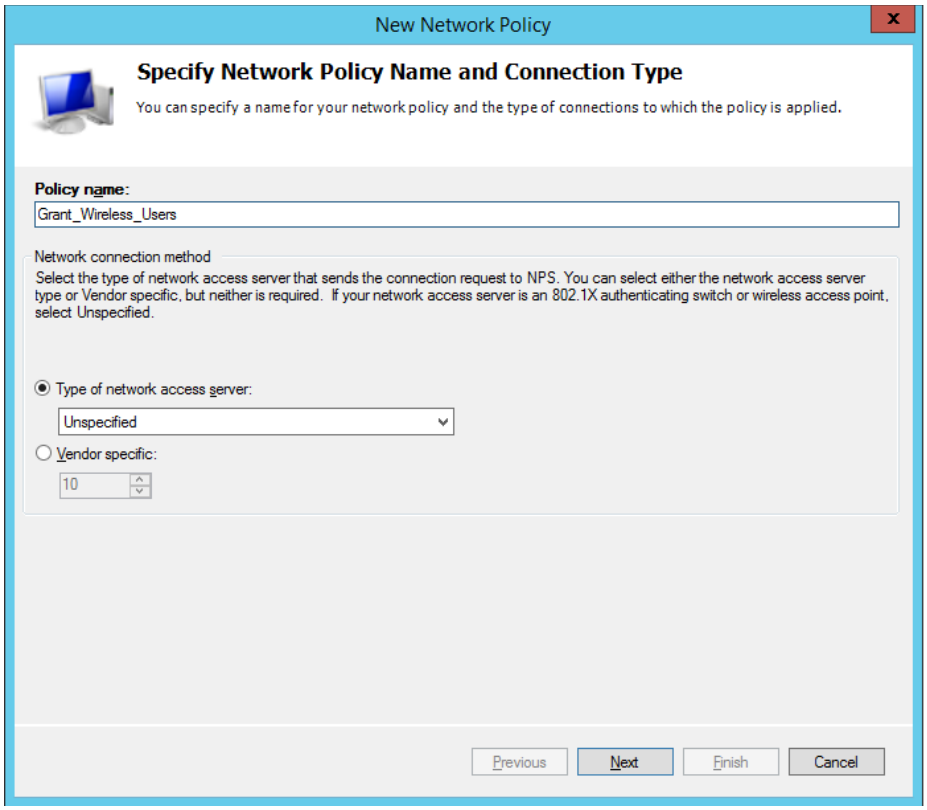


Figure 5. 190: Network Policy Server

Step 38: Select condition then click button ***Add.***

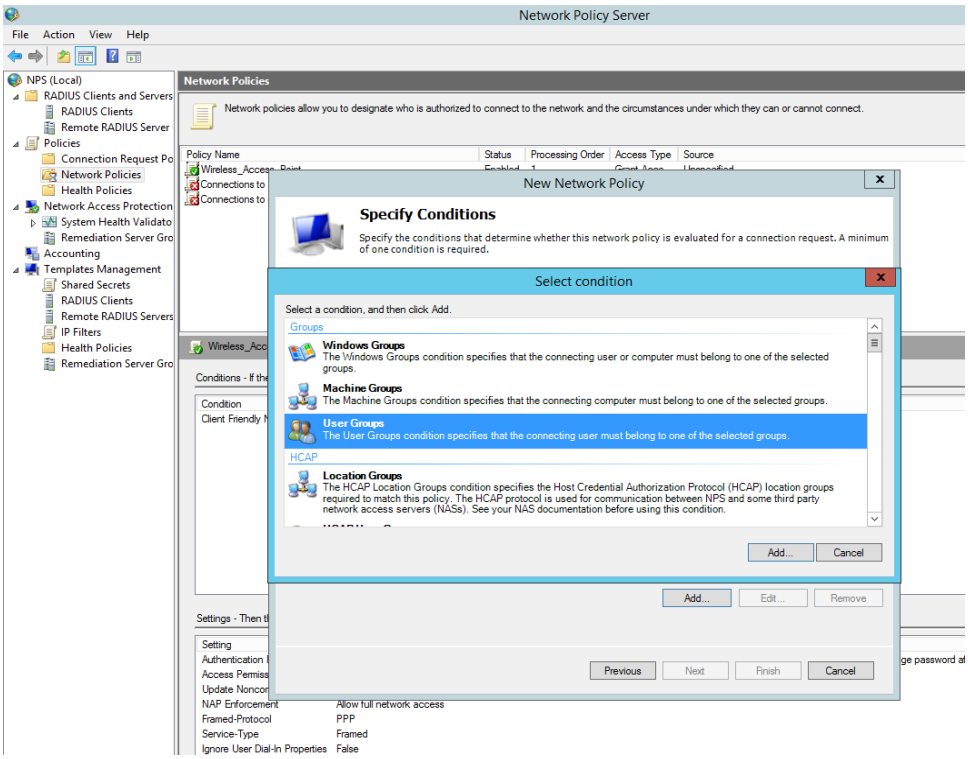


Figure 5. 191: Select Condition

Step 39: Click button ***Add Groups.***

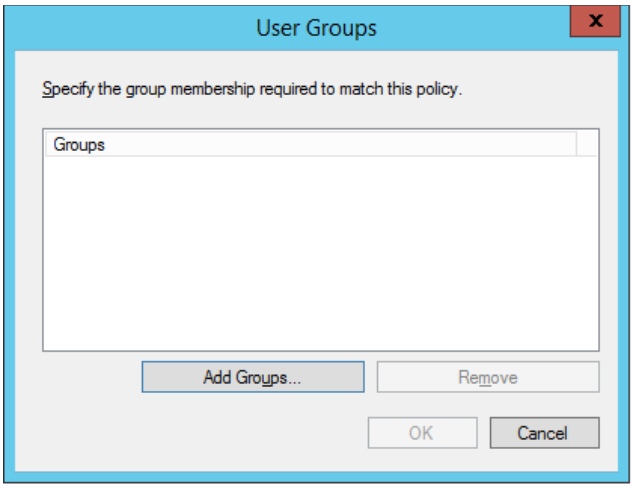


Figure 5. 192: User Groups

Step 40: Select Group that has been create in ***Active Directory User and Computers***

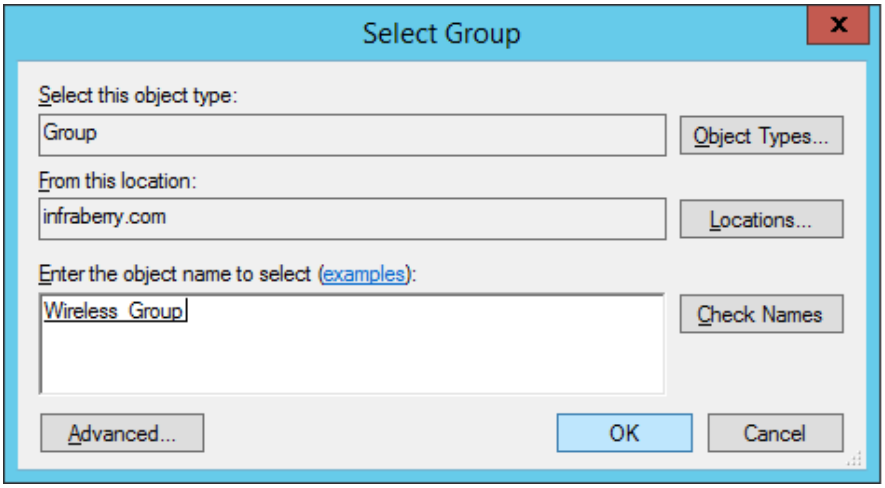


Figure 5. 193: Select Group

Step 41: Show group that has been choose then click button ***OK.***

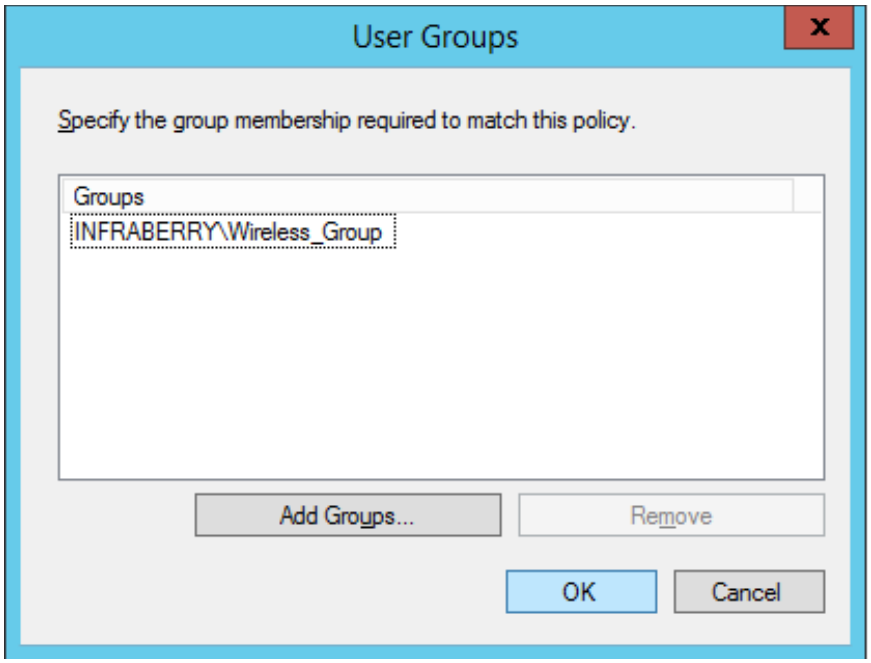


Figure 5. 194: User Groups

Step 42: Click button ***Next.***

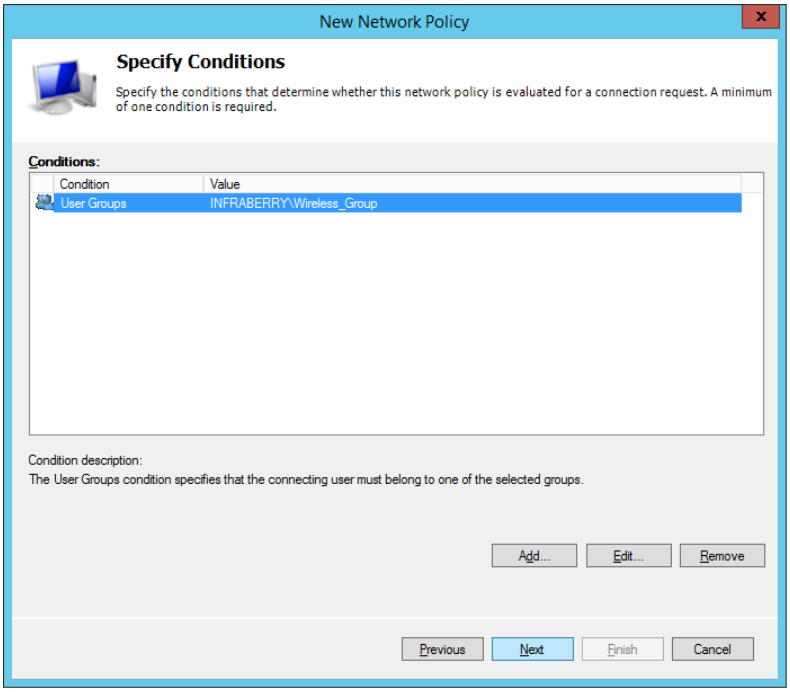


Figure 5. 195: Specify Condition

Step 43: Click button ***Next.***

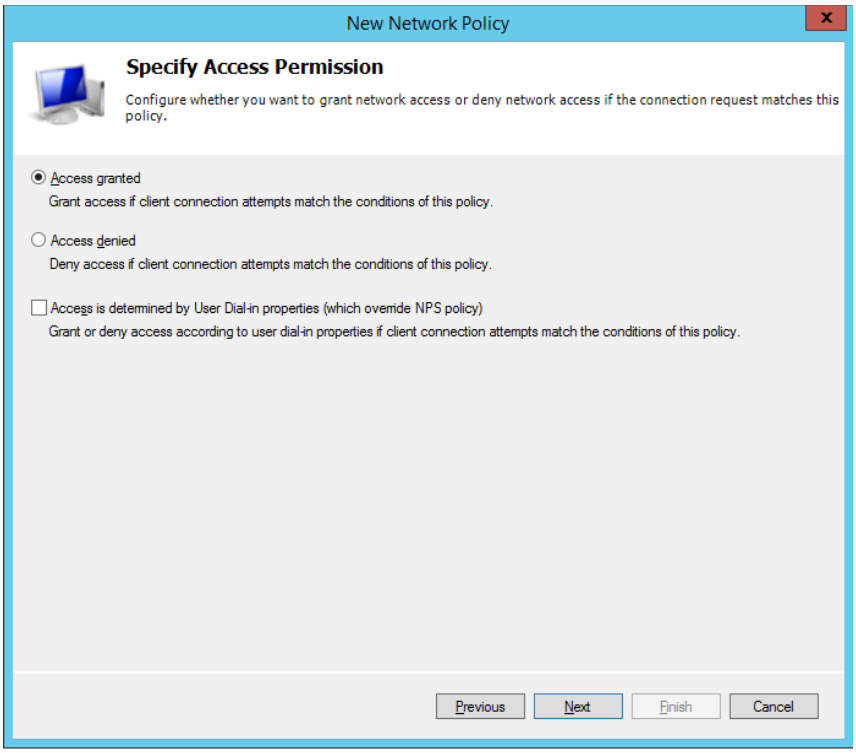


Figure 5. 196: Specify Access Permission

Step 44: Click button ***Next.***

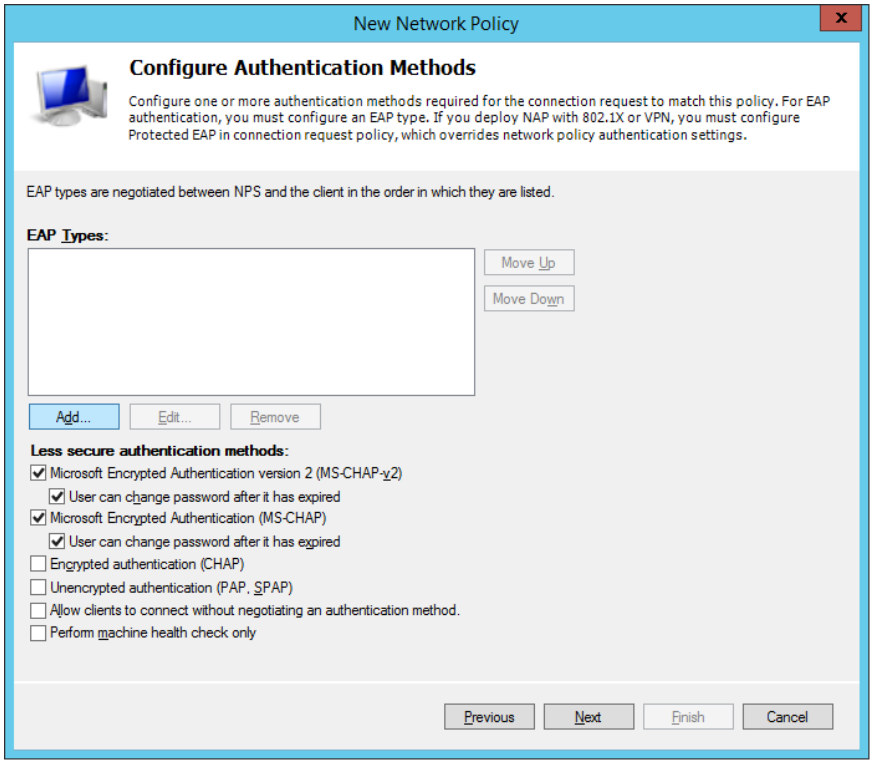


Figure 5. 197: Configure Authentication Methods

Step 45: Click button ***OK.***

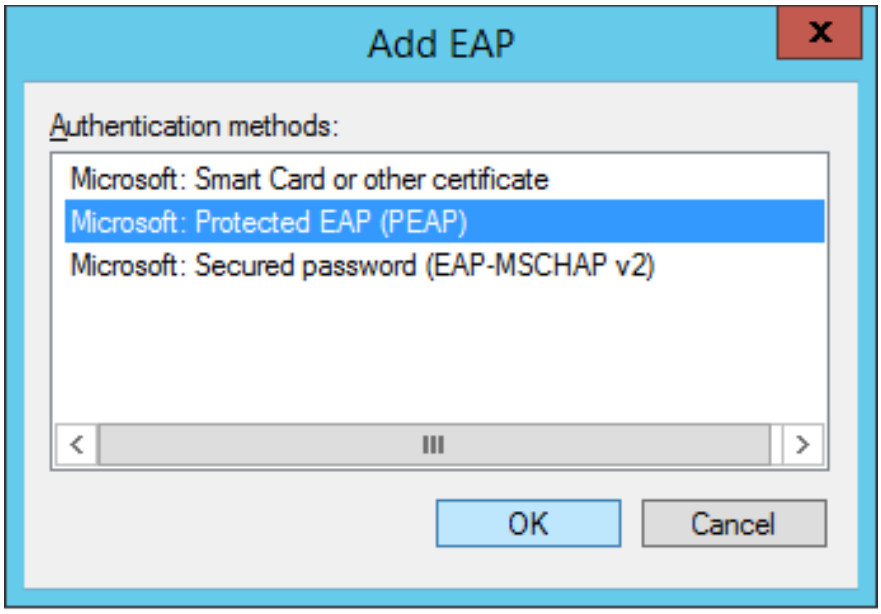


Figure 5. 198: Add EAP

Step 46: Click button ***Next.***

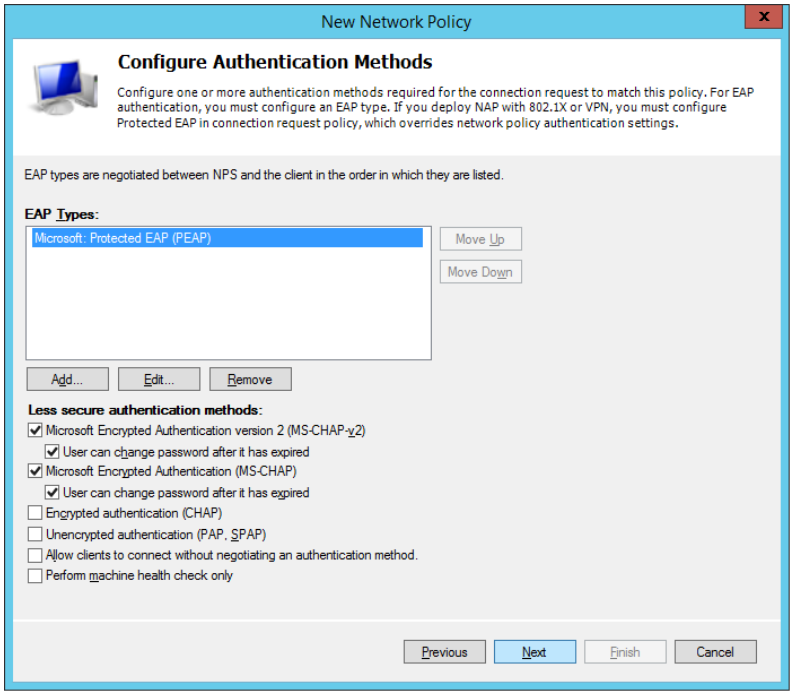


Figure 5. 199: Configure Authentication Methods

Step 47: Click button ***Next.***

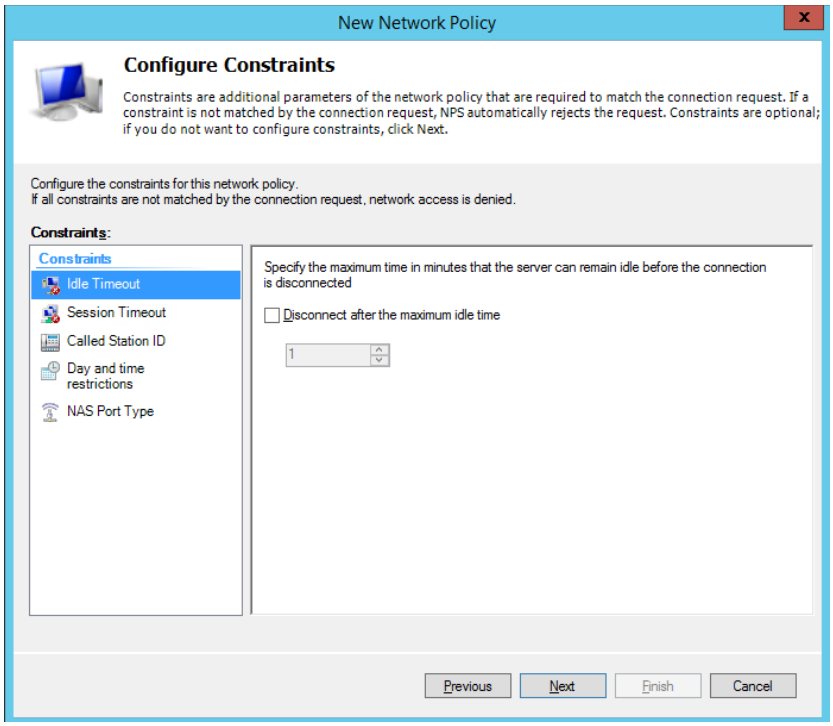


Figure 5. 200: Configure Constraints

Step 48: Click button ***Next.***

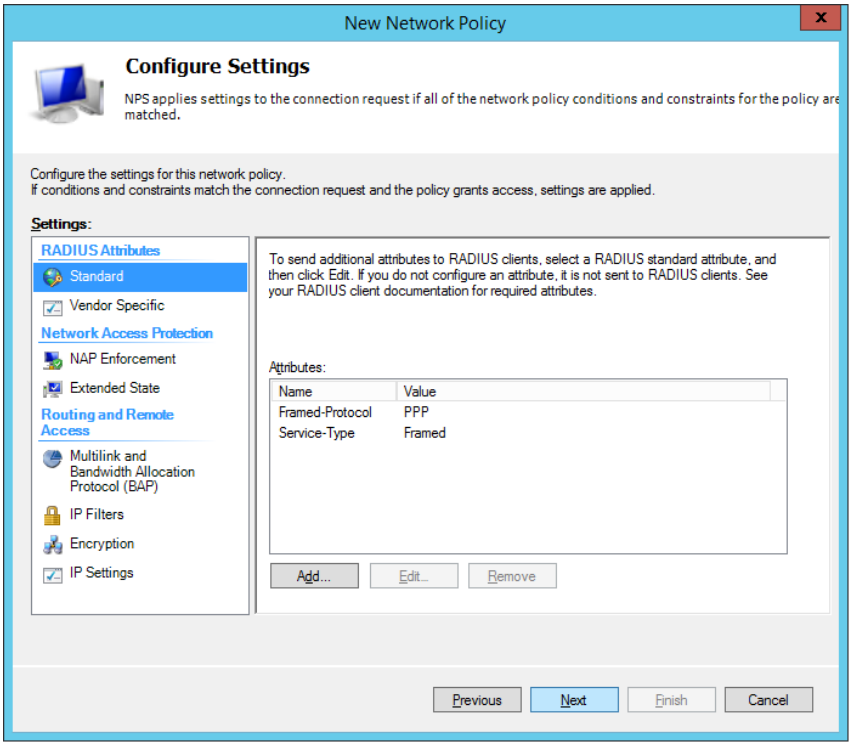


Figure 5. 201: Configure Settings

Step 49: Click button ***Next.***

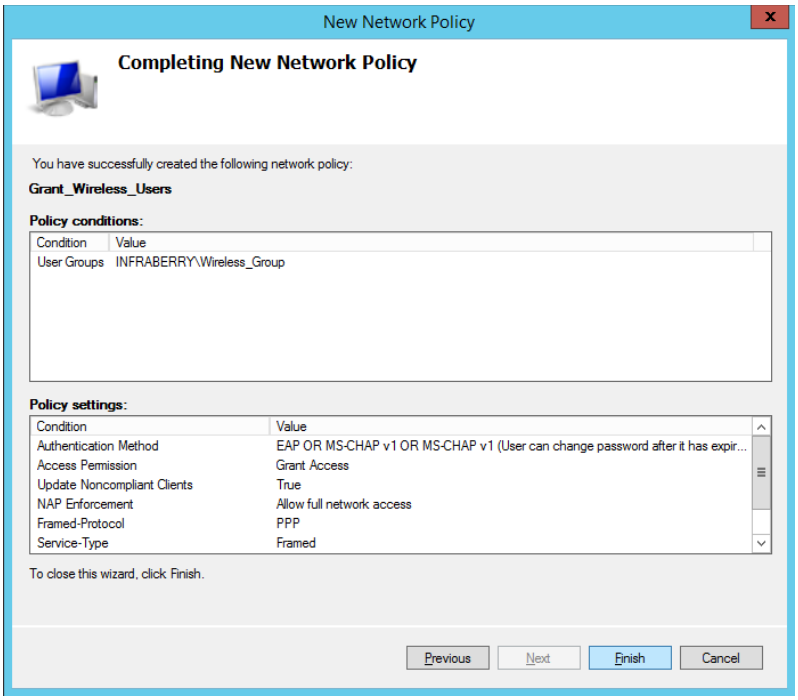


Figure 5. 202: Completing New Network Policy

Step 50: Show New Network Policies that has been create.

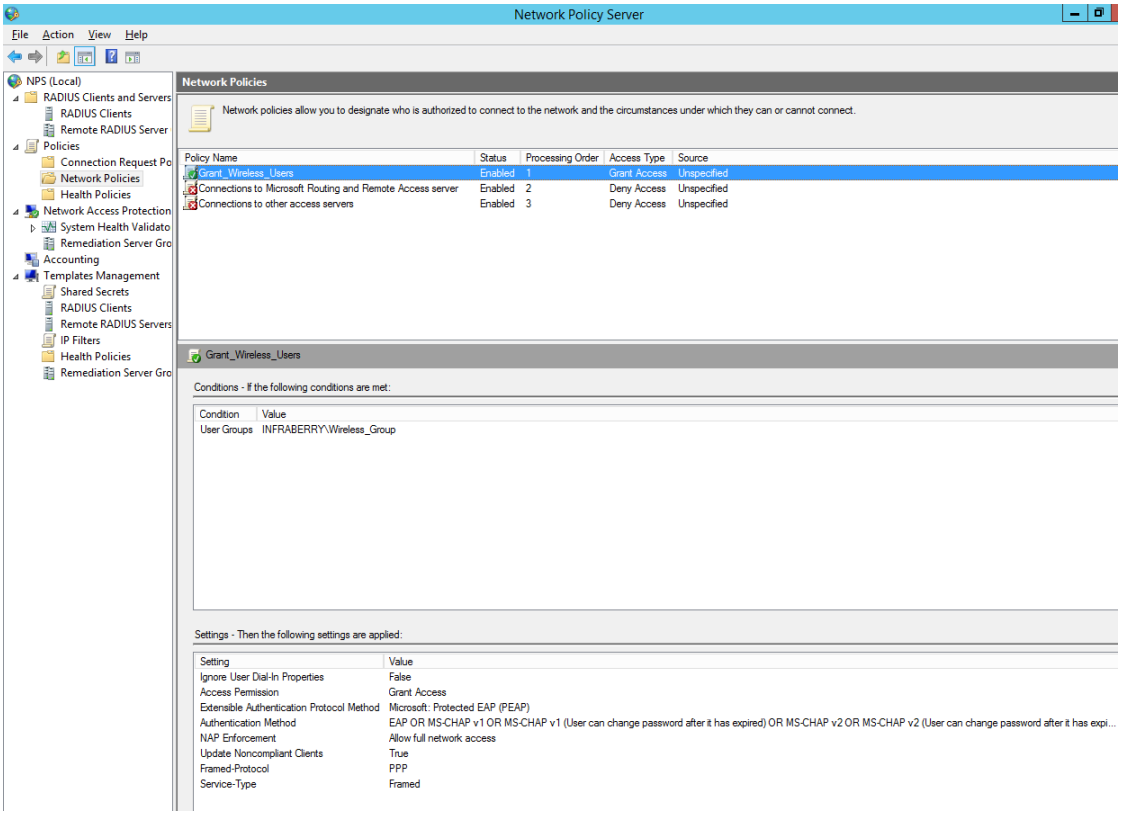


Figure 5. 203: Grant_Wireless_Users Properties

Step 51: Open ***Grant_Wireless_Users*** Properties then click button ***Add.***

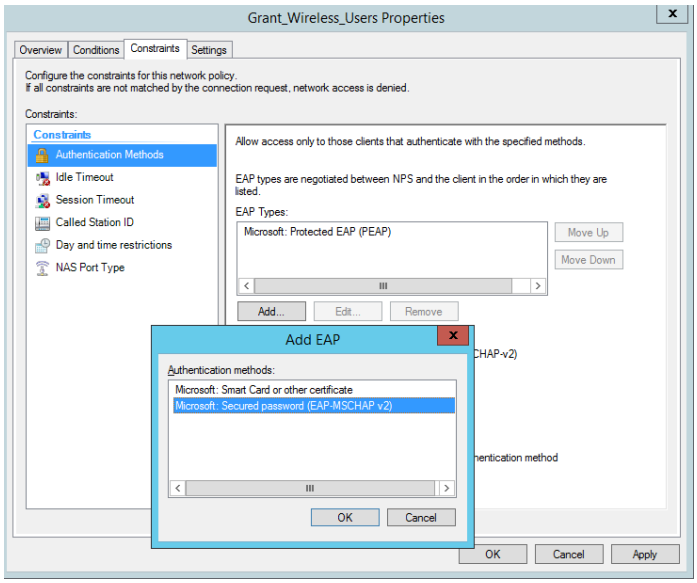


Figure 5. 204: Add EAP

Step 52: Move up EAP that has been add then click button ***OK.***

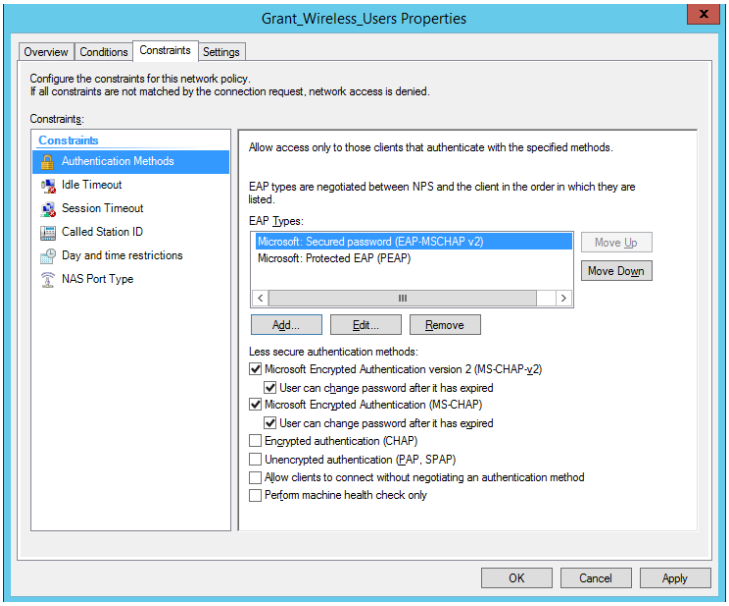


Figure 5. 205: Grant_Wireless_Users Properties

Step 53: Setup WAN then click button ***Save*** and ***Apply***.

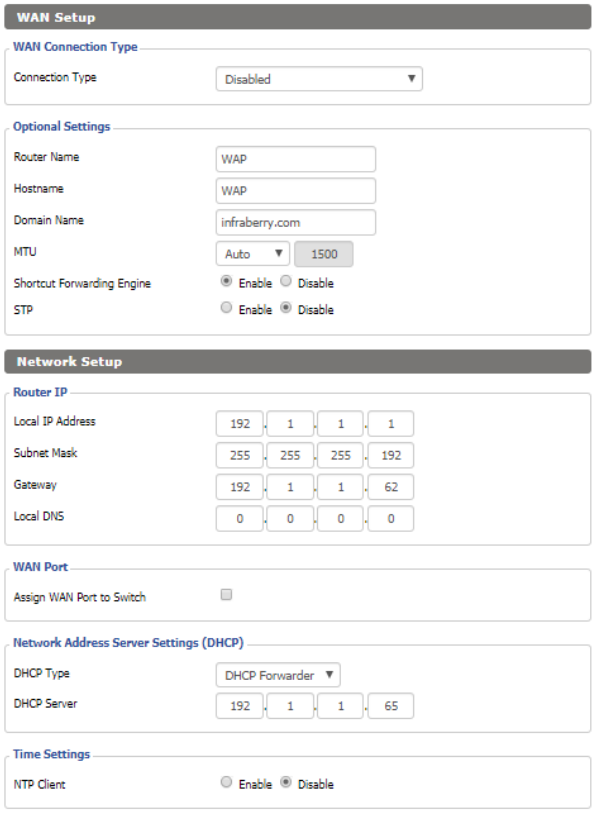


Figure 5. 206: WAN Setup

Step 54: Setup ***Wireless Basic Setting*** then click button ***Save*** and ***Apply Settings.***

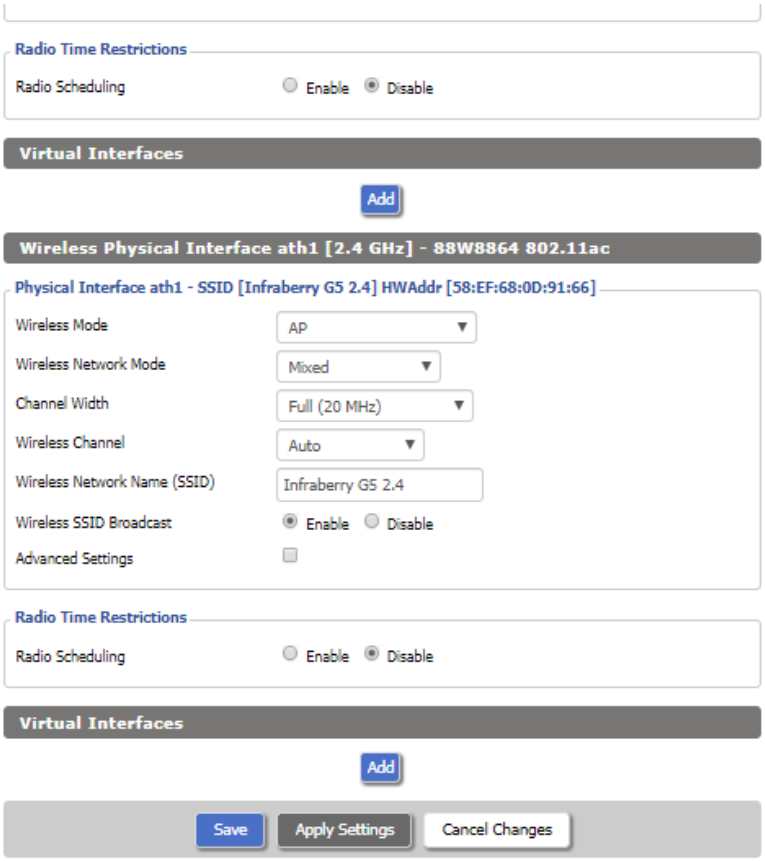


Figure 5. 207: Basic Setting Wireless

Step 55: Setup ***Wireless Security*** then click button ***Save*** and ***Apply Settings.***

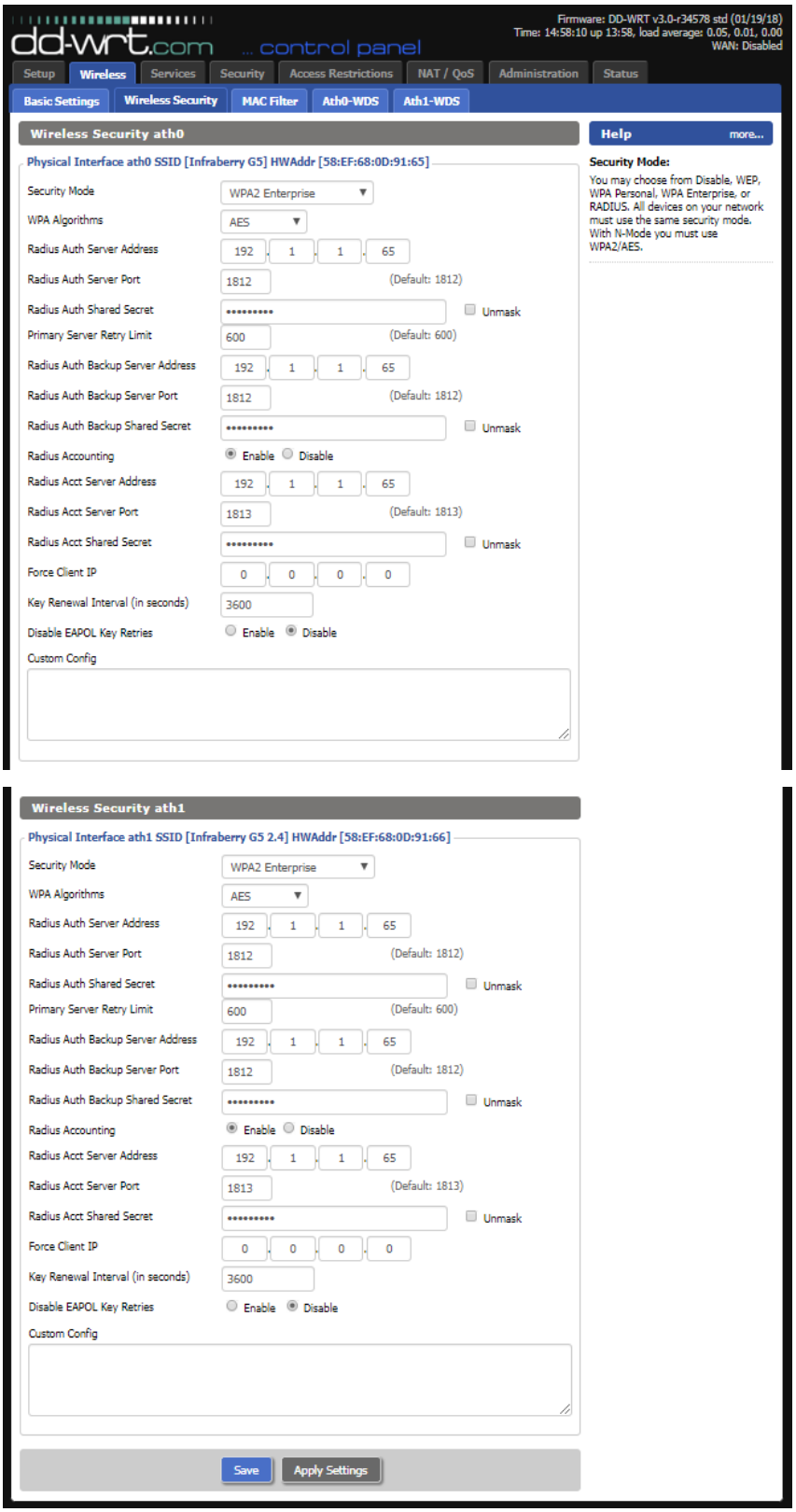


Figure 5. 208: Wireless Security

5.3.9 Ipsec Site-To-Site Tunneling

Step 1: Key in username and password then write the command.

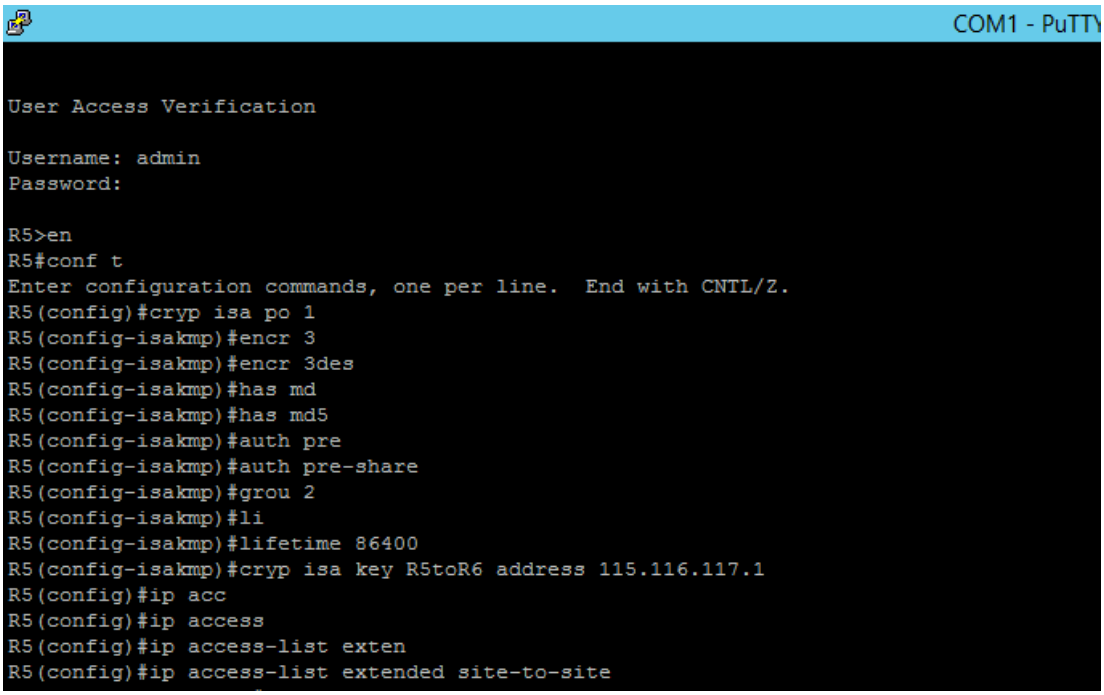


Figure 5. 209: User Access Verification

Step 2: Key in permit ip and cryp ipsec transform-set.

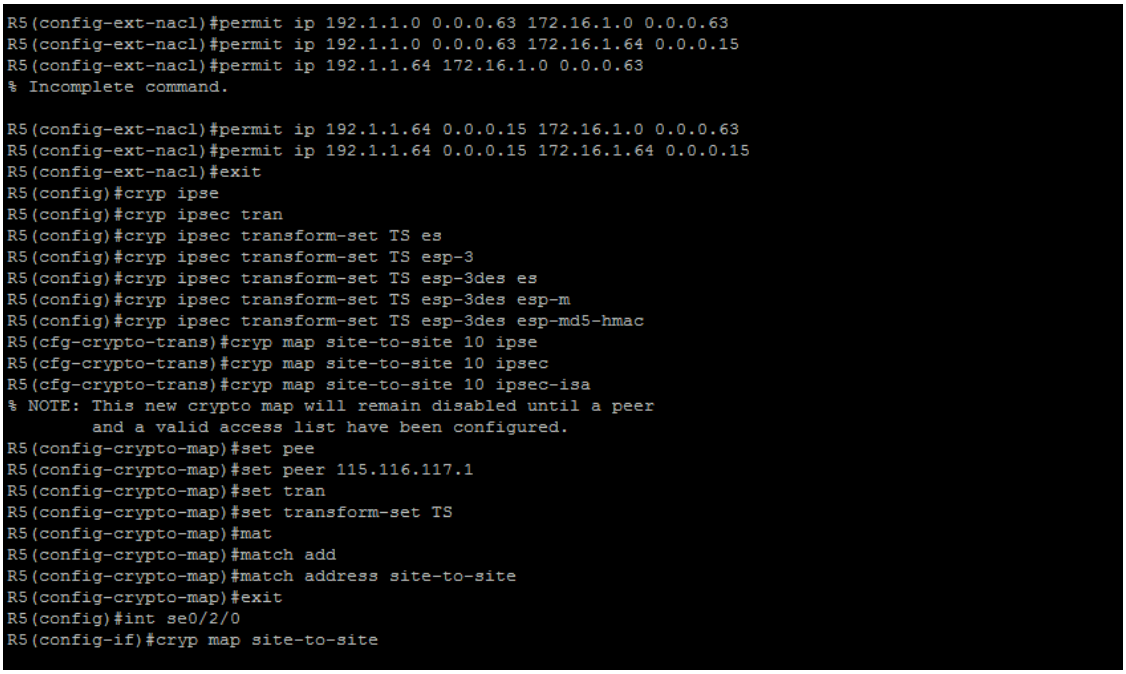


Figure 5. 210: Putty

Step 3: Key in username and password then write the command.

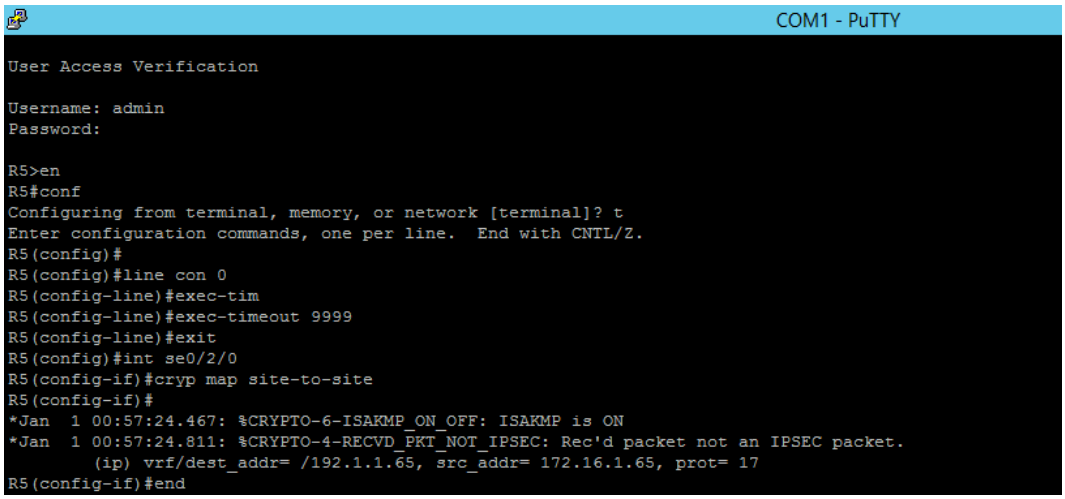


Figure 5. 211: Putty

Step 4: Turn on crypto IPsec debugging

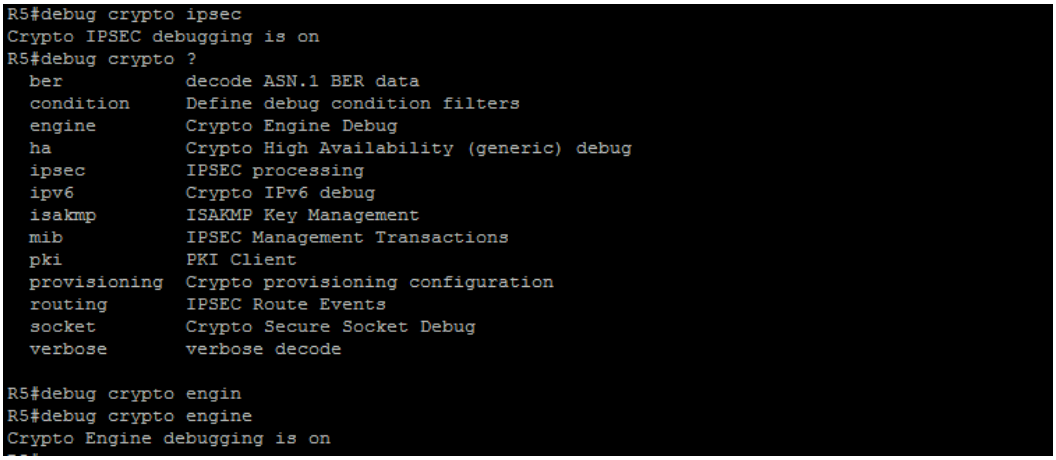


Figure 5. 212: Putty

Step 5: Undebug back the crypto IPsec debugging.

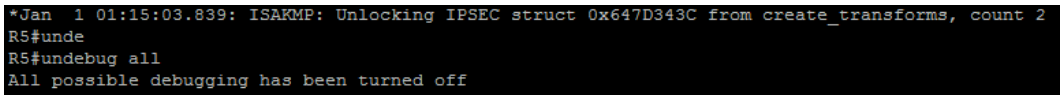


Figure 5. 213: Putty

5.3.10: AAA With Radius

Step 1: Go to Start > Administrative Tools > Active Directory Users and Computers to configure. Right click on Users and select New > User in order to add a new user for AD.

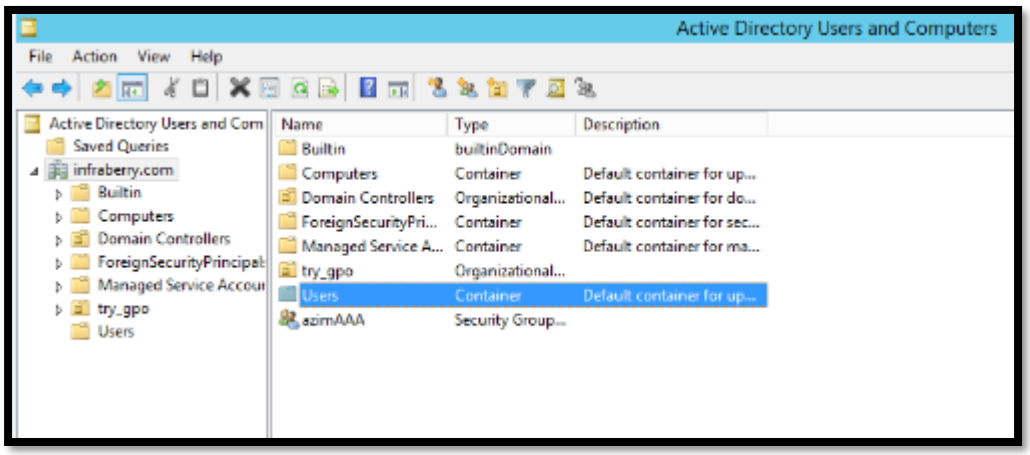


Figure 5.214: Creating User

Step 2: Configure the new user by enter the First name and Full name, and also User login name of the user, click Next when done.

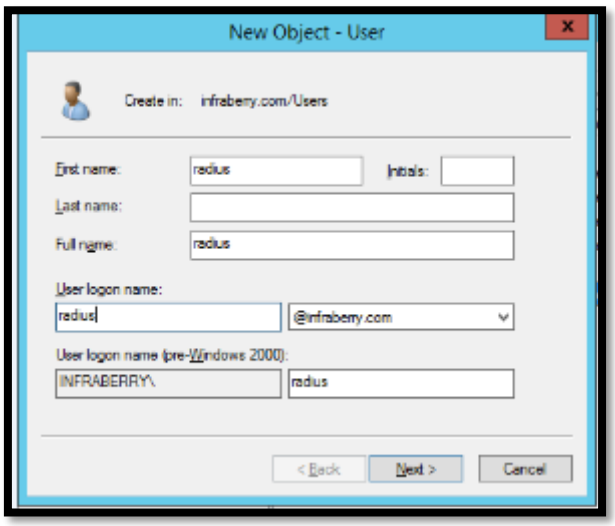


Figure 5.215: Insert user name

Step 3:Create the new group

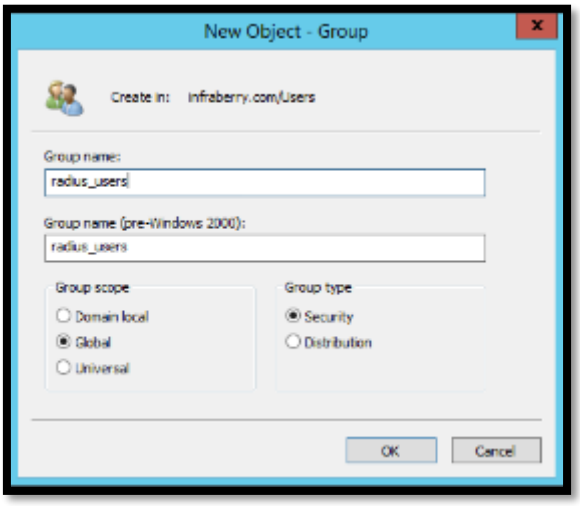


Figure 5.216: Creating user group

Step 4: For the user you have been created or added, right click on that user and choose Add to a group

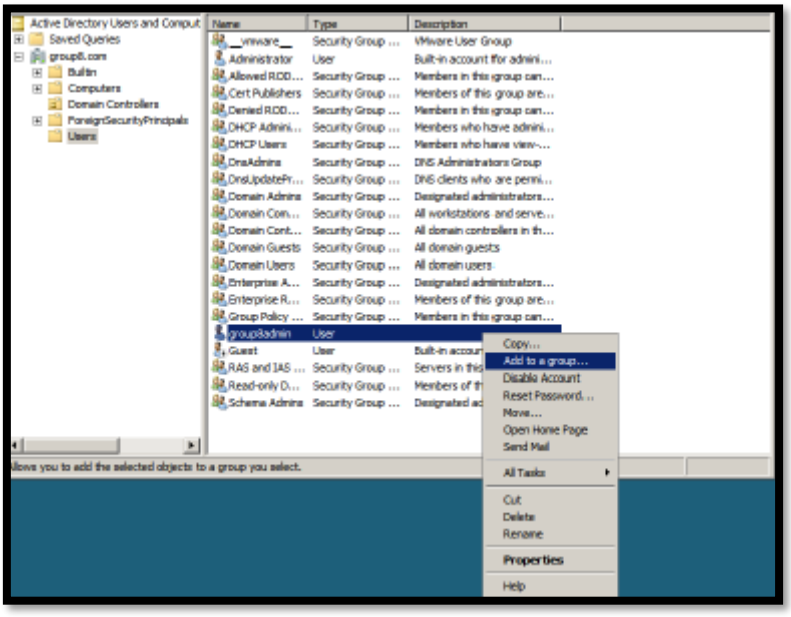


Figure 5.217: Add the user into a new group

Step 5: Create Radius Client

Go to AD → Tool → DNS → Forward Lookup Zones → Workshop5.com→ Right click and create new.

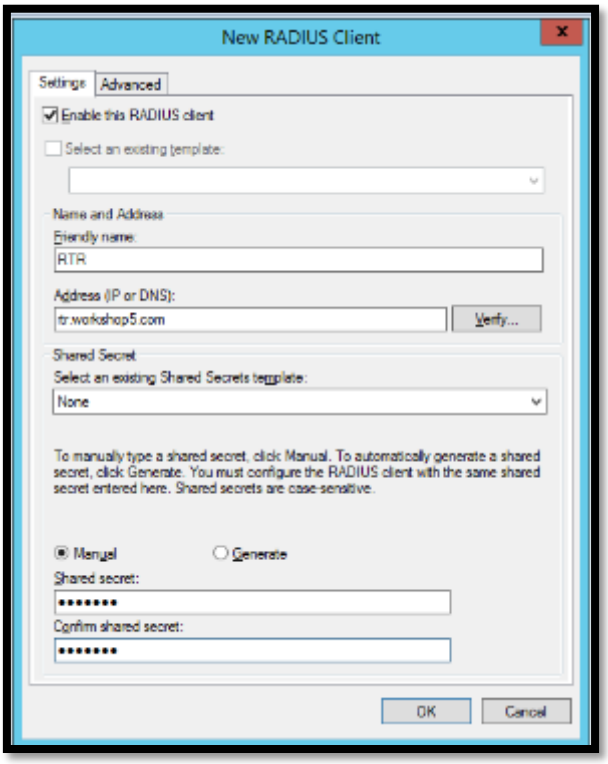


Figure 5.218: Creating radius client

Step 6: Click on verify and click on resolve to verify the address(ip router)

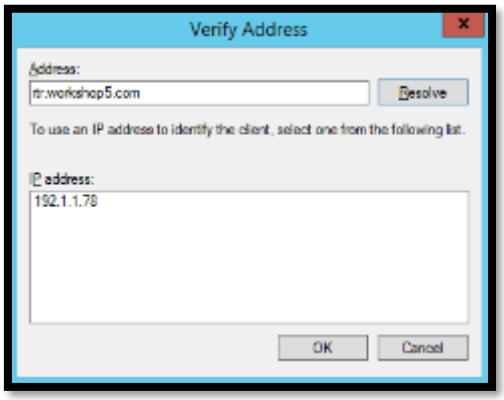


Figure 5.219: Resolve the ip and domain

Step 7: Network Policy Server

Create the new connection policy: Click on connection request policy

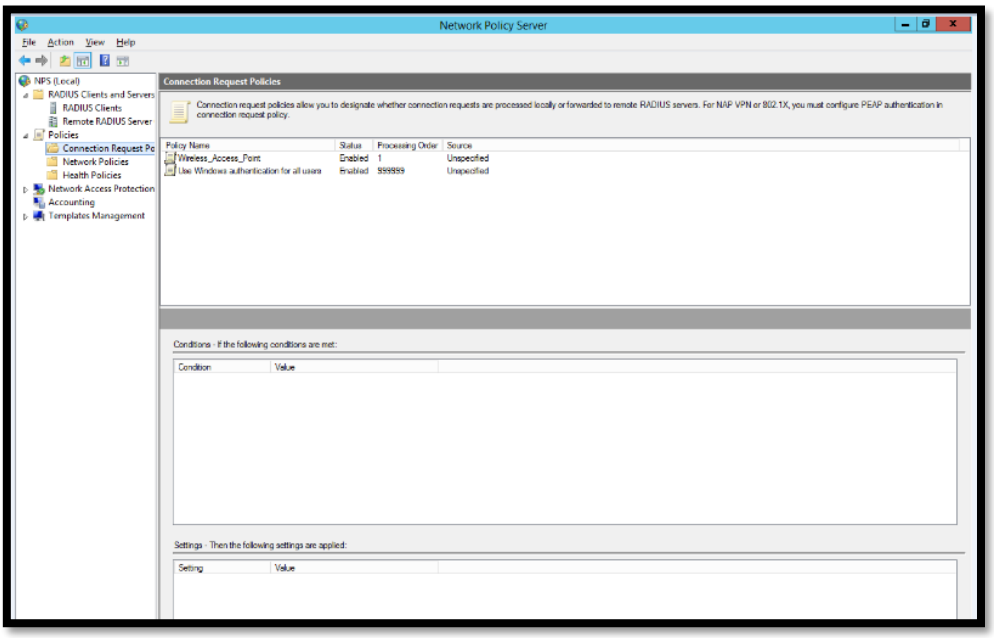


Figure 5.220: Network Policy Server

Click next after insert the name of policy

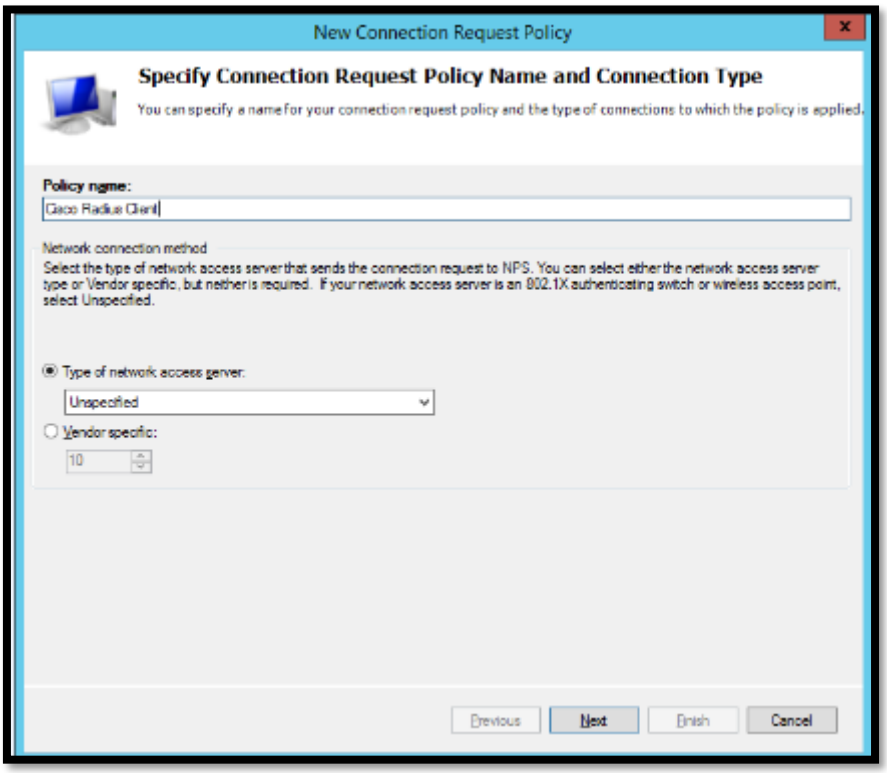


Figure 5.221: Create the new policy name

Choose the “client friendly name”

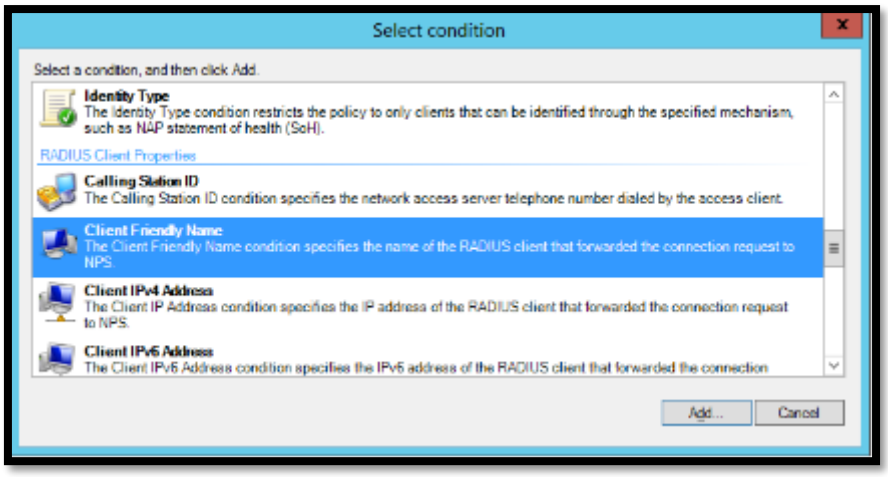


Figure 5.222: Select condition

Insert the any friendly name

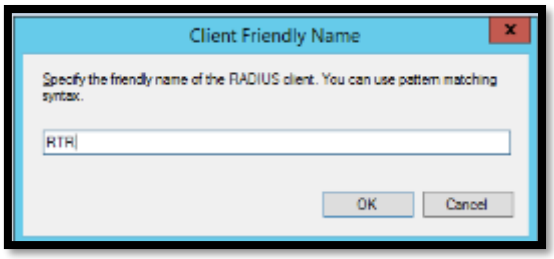


Figure 5.223: Client friendly name

Step 8: Create the vendor policy

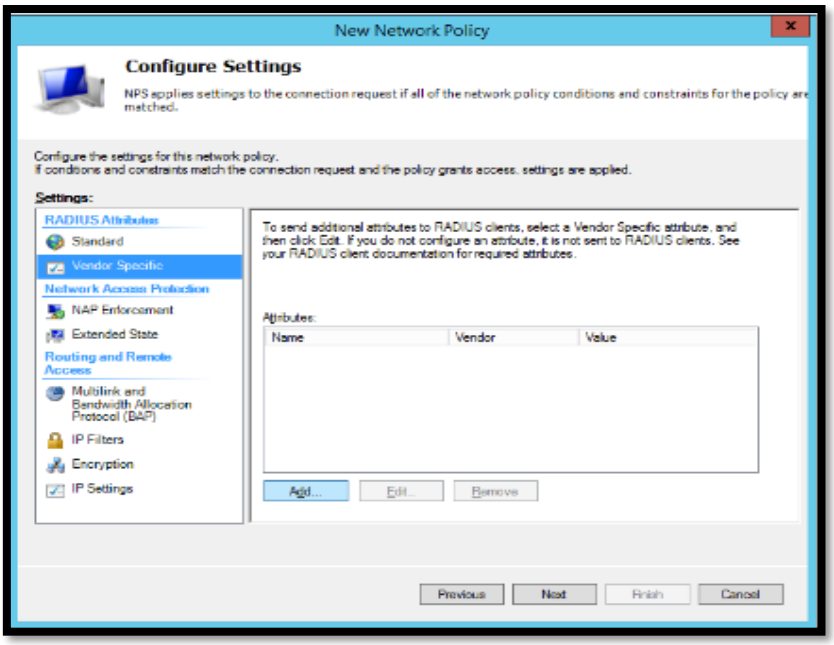


Figure 5.224: Vendor Specific

Set the vendor specific attribute

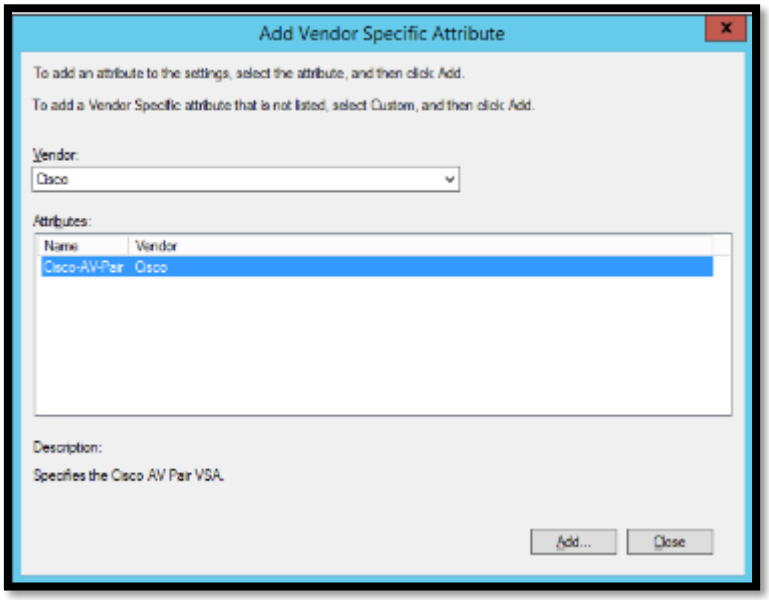


Figure 5.225: vendor specific attribute

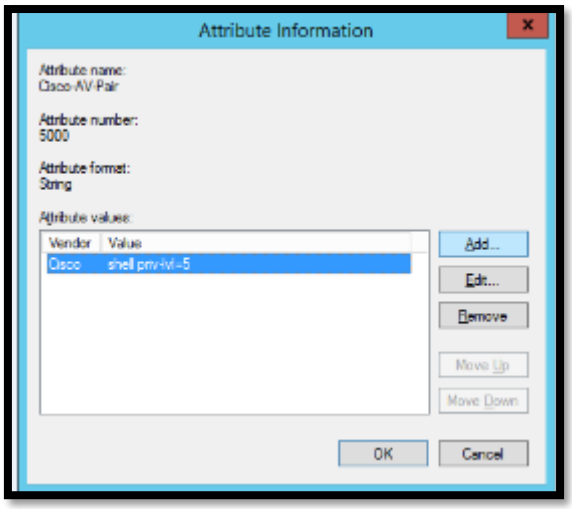


Figure 5.226: attribute information

Step 9: Router Configuration

Login to the router and configure aaa.

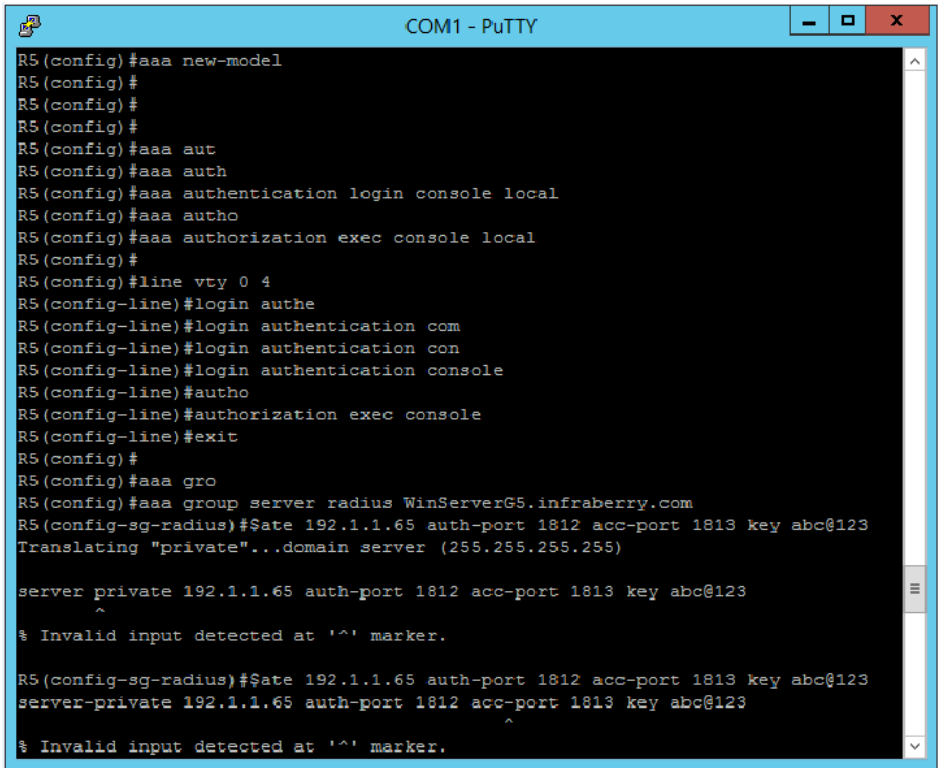


Figure 5.227: Router Configuration

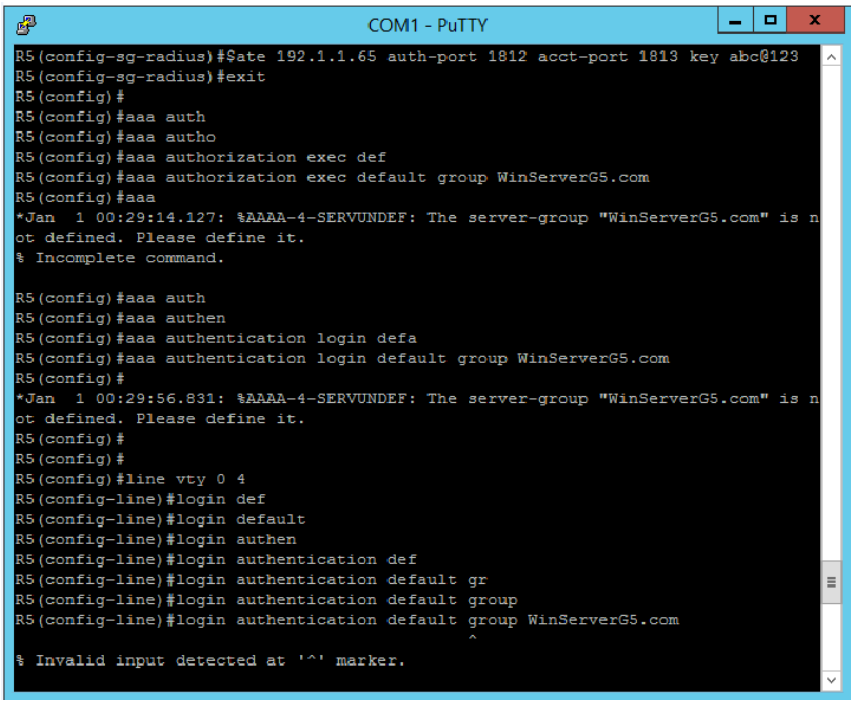


Figure 5.228: Router Configuration

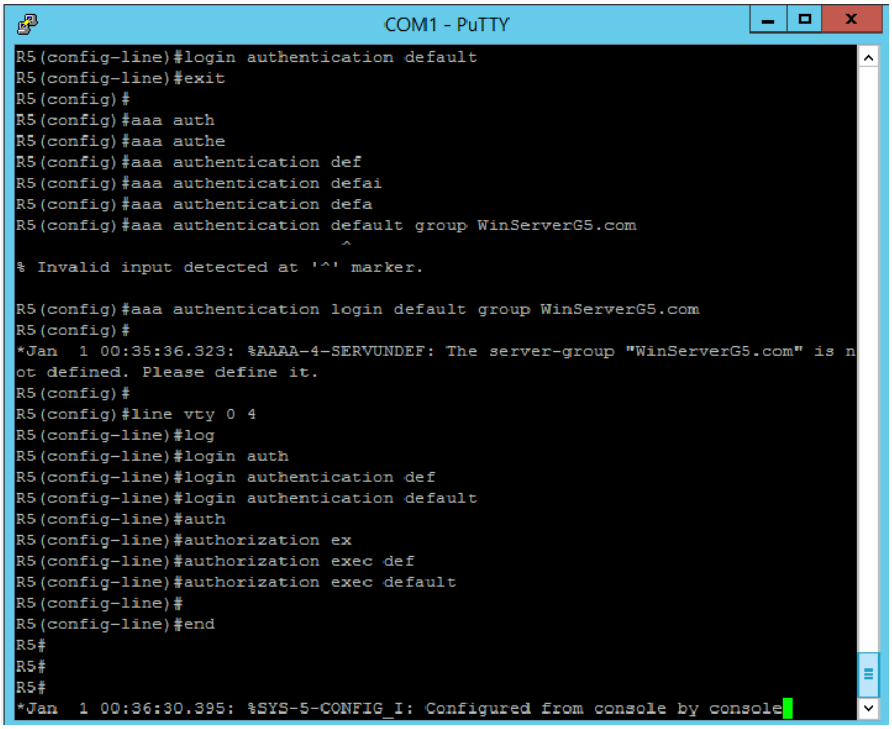


Figure 5.229: Router Configuration

Step 8: Login at router

Login using name and password that you configure using serial and SSH.

5.3.11: Secure Ftp

Step 1: Installing vsftpd

```
ubuntug5@ubuntug5:~$ sudo apt-get install vsftpd
Reading package lists... Done
```

Figure5.230: Install vsftpd

Step 2: When the installation is complete, we'll copy the configuration file so we can start with a blank configuration, saving the original as a backup.

```
ubuntug5@ubuntug5:~$
ubuntug5@ubuntug5:~$ sudo cp /etc/vsftpd.conf /etc/vsftpd.conf.orig
ubuntug5@ubuntug5:~$
```

Figure 5.231: saving original backup

Step 3: Opening the Firewall, We'll check the firewall status to see if it's enabled.

```
ubuntug5@ubuntug5:~$ sudo apt-get install ufw
Reading package lists... Done
Building dependency tree
Reading state information... Done
ufw is already the newest version (0.36-0ubuntu0.18.04.1).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

Figure 5.232: opening the firewall

```
ubuntug5@ubuntug5:~$ sudo ufw enable
Firewall is active and enabled on system startup
ubuntug5@ubuntug5:~$
```

Figure 5.233:enable firewall

Step 4: add rules for FTP traffic.

```
ubuntug5@ubuntug5:~$ sudo ufw allow 20/tcp
Rule added
Rule added (v6)
ubuntug5@ubuntug5:~$ sudo ufw allow 21/tcp
Rule added
Rule added (v6)
ubuntug5@ubuntug5:~$ sudo ufw allow 900/tcp
Rule added
Rule added (v6)
ubuntug5@ubuntug5:~$ sudo ufw allow 40000:50000/tcp
Rule added
Rule added (v6)
ubuntug5@ubuntug5:~$ sudo ufw status
Status: active
```

Figure 5.234: Permit the rules

Step 5: Preparing the User Directory

First, we'll add a user:

```
ubuntug5@ubuntug5:~$ sudo adduser azim
Adding user `azim' ...
Adding new group `azim' (1001) ...
Adding new user `azim' (1001) with group `azim' ...
Creating home directory `/home/azim' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for azim
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] y
```

Figure 5.235: Add new user

Step 6: Create the ftp folder, set its ownership, and be sure to remove write permissions with the following commands:

```
ubuntug5@ubuntug5:~$ sudo mkdir /home/azim/ftp
ubuntug5@ubuntug5:~$ sudo chown nobody:nogroup /home/azim/ftp
ubuntug5@ubuntug5:~$ sudo chmod a-w /home/azim/ftp
ubuntug5@ubuntug5:~$
```

Figure 5.236: Create the folder and the permission

Let's verify the permissions:

```
ubuntug5@ubuntug5:~$ sudo ls -la /home/azim/ftp
total 8
dr-xr-xr-x 2 nobody nogroup 4096 Apr  11 02:26 .
drwxr-xr-x 3 azim   azim    4096 Apr  11 02:26 ..
```

Figure 5.237: Verify the permission

Step 7: Next, we'll create the directory where files can be uploaded and assign ownership to the user:

```
ubuntug5@ubuntug5:~$ sudo mkdir /home/azim/ftp/files
ubuntug5@ubuntug5:~$ sudo chown azim:azim /home/azim/ftp/files
ubuntug5@ubuntug5:~$
```

Figure 5.238:create new directory for the new user

Step 8: A permissions check on the files directory should return the following:

```
ubuntug5@ubuntug5:~$ sudo ls -la /home/azim/ftp
total 12
dr-xr-xr-x 3 nobody nogroup 4096 Apr  11 02:28 .
drwxr-xr-x 3 azim   azim    4096 Apr  11 02:26 ..
drwxr-xr-x 2 azim   azim    4096 Apr  11 02:28 files
```

Figure 5.239: Check the permission of user

Step 9: Finally, we'll add a test.txt file to use when we test later on:

```
ubuntug5@ubuntug5:~$ echo "vsftpd test file" |sudo tee /home/azim/ftp/files/test
.txt
vsftpd test file
```

Figure 5.240: create new file

Step 10: Configuring FTP Access

```
ubuntug5@ubuntug5:~$ sudo nano /etc/vsftpd.conf
ubuntug5@ubuntug5:~$
ubuntug5@ubuntug5:~$ echo "azim"
azim
```

Figure 5.241: Configure ftp

/etc/vsftpd.conf

```
. . .
# Allow anonymous FTP? (Disabled by default).
anonymous_enable=NO
#
# Uncomment this to allow local users to log in.
local_enable=YES
```

Figure 5.242: Configure ftp

/etc/vsftpd.conf

```
. . .
write_enable=YES
. . .
```

Figure 5.243: Configure ftp

/etc/vsftpd.conf

```
. . .
chroot_local_user=YES
. . .
```

Figure 5.245: Configure ftp

/etc/vsftpd.conf

```
user_sub_token=$USER
local_root=/home/$USER/ftp
```

Figure 5.246: Configure ftp

/etc/vsftpd.conf

```
pasv_min_port=40000
pasv_max_port=50000
```

Figure 5.247: Configure ftp

/etc/vsftpd.conf

```
userlist_enable=YES
userlist_file=/etc/vsftpd.userlist
userlist_deny=NO
```

Figure 5.248: Configure ftp

Step 11: Finally, we'll create and add our user to the file. We'll use the -a flag to append to file:

```
ubuntug5@ubuntug5:~$ echo "azim" | sudo tee -a /etc/vsftpd.userlist
azim
```

Figure 5.249: create and add our user to the file

Double-check that it was added as you expected:

```
ubuntug5@ubuntug5:~$ cat /etc/vsftpd.userlist
azim
```

Figure 5.250: Double-check the user

Step 12: Restart the daemon to load the configuration changes:

```
$ sudo systemctl restart vsftpd
```

Figure 5.251: Restart the daemon

Step 13: Testing FTP Access

```
ubuntug5@ubuntug5:~$ ftp -p localhost
Connected to localhost.
220 (vsFTPd 3.0.3)
Name (localhost:ubuntug5): azim
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> bye
221 Goodbye.
ubuntug5@ubuntug5:~$
```

Figure 5.252: Double-check the user

Step 14: Install Open SSH Server

```
sudo apt update
sudo apt install openssh-server
```

Figure 5.253: update and install openssh

Step 15: After installing, the commands below can be used to stop, start and enable the service to always start up when the server boots.

```
sudo systemctl stop ssh.service
sudo systemctl start ssh.service
sudo systemctl enable ssh.service
```

Figure 5.254: enable or disable service

Step 16: Configure SFTP

```
sudo nano /etc/ssh/sshd_config
```

Figure 5.255: configure SFTP

Step 17: Then edit the file and change highlighted line belo, add the # before the first line, then add the highlighted line just below it to enable SFT. This will change the subsystem to internal-sftp only

```
# override default of no subsystems
#Subsystem      sftp    /usr/lib/openssh/sftp-server
Subsystem sftp internal-sftp
```

Figure 5.256: configure SFTP

```
# Example of overriding settings on a per-user basis
#Match User anoncvs
#       X11Forwarding no
#       AllowTcpForwarding no
#       PermitTTY no
#       ForceCommand cvs server
Match Group sftp_users
X11Forwarding no
AllowTcpForwarding no
ChrootDirectory /home
ForceCommand internal-sftp
```

Figure 5.257: Configure SFTP

Save the file and exit

After editing the file, run the commands below to restart OpenSSH Server.

```
sudo systemctl restart ssh.service
```

Figure 5.258: restart ssh service

Step 18: Create SFTP Group

```
sudo groupadd sftp_users
```

Figure 5.259: create group for user

Step 19: Now add any user to the group by runnning the commands below

```
sudo usermod -aG sftp_users richard
```

Figure 5.260: add user to group

Replace user “richard” with your Ubuntu account name… this will add the user to the sftp_users group you created above

That’ it! Your system should be configured for secure SFTP for your users

5.3.12: Access List Control

Step 1: Access CLI prompt of R5 and enter in global configuration mode and type the command below, this extended access-list used to block specific port from outside client accessing to our network.

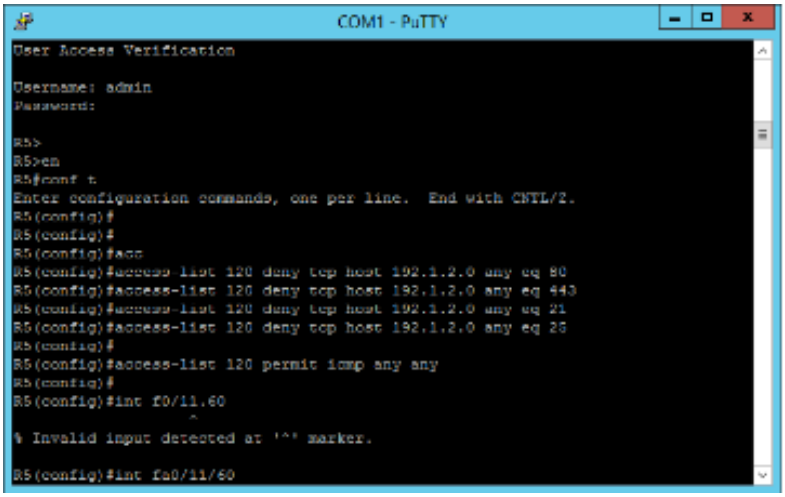


Figure 5.261: Deny the port

Step 2: Verify Rules created. To checked back weather the rules created is like we plan type command

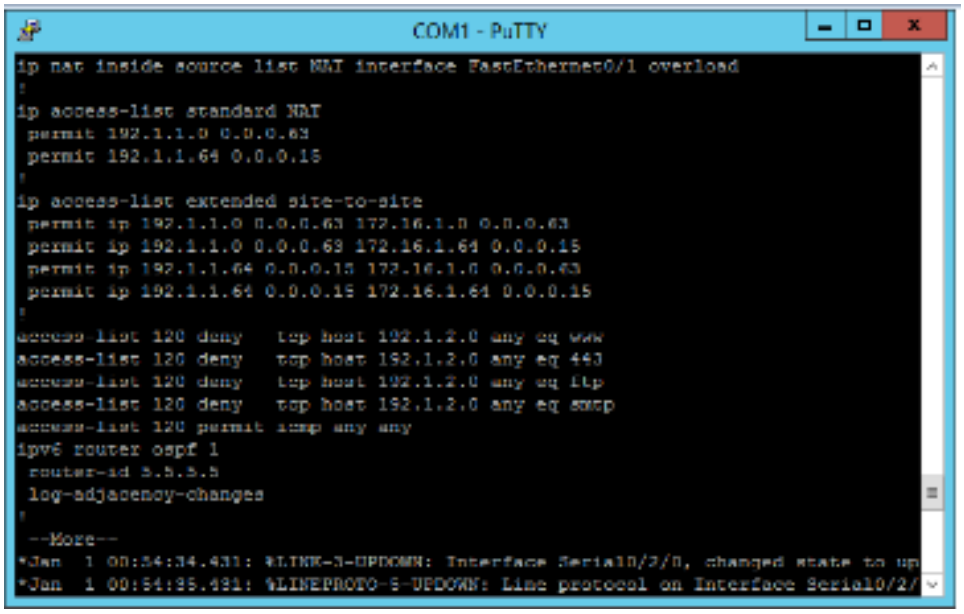


Figure 5.262: check the configuration have been made

Step 3: Once the rules is created, we need to assign ACL to respective interface

R5(config)#interface fa0/0

R5(config-if)#ip access-group 120 in

R5(config-if)#exit

Problem

The client is connected to the internet. With the constantly evolving nature of the Internet, it is vital that we continuously protect the network and their information. The Client need to be restricted from freely connecting to anything using certain services. To increase the effectiveness of the security in the network. A certain measure must be taken to filter the incoming and outgoing packets that going through our network.

Solution

Apply ACL rules on router that will either permit or deny the incoming and outgoing packet through network with while permit or deny specific services.

5.3.13 Active Directory

Active Directory (AD) is a Microsoft product that consists of several services that run on Windows Server to manage permissions and access to networked resources. Active Directory stores data as objects. An object is a single element, such as a user, group, application or device, such as a printer. Objects are normally defined as either resource such as printers or computers or security principals such as users or groups. Below is the step that need to install and configure the Active Directory on Windows Server 2010 R2.

Step1: First step that need to do is open the server manager window and find manage on the top left corner taskbar. To add the Active Directory, click on the Add Roles and Features.

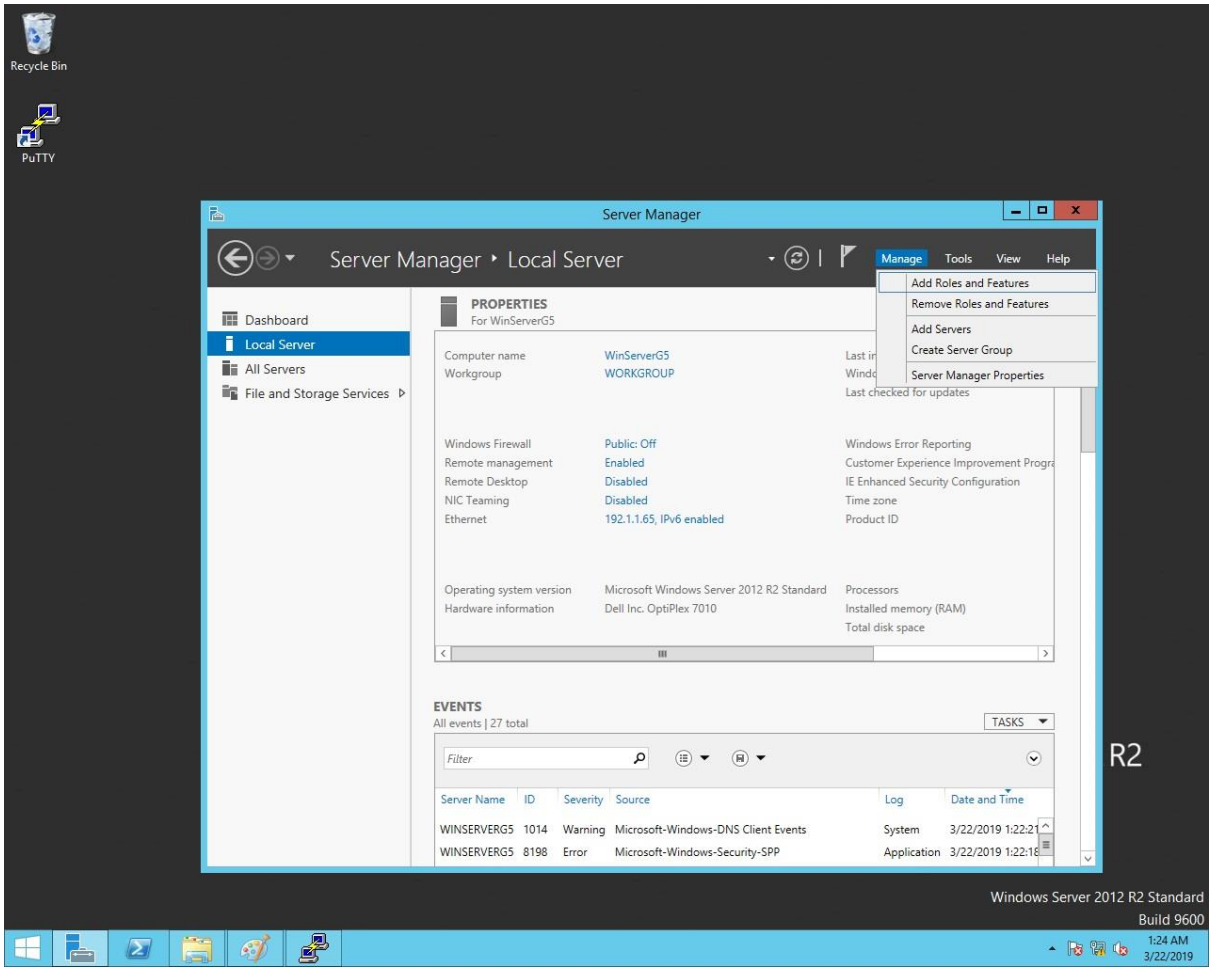


Figure 5.263: Add Roles and Features

Step 2: After the Add Roles and Features Wizard pop up, click next button.

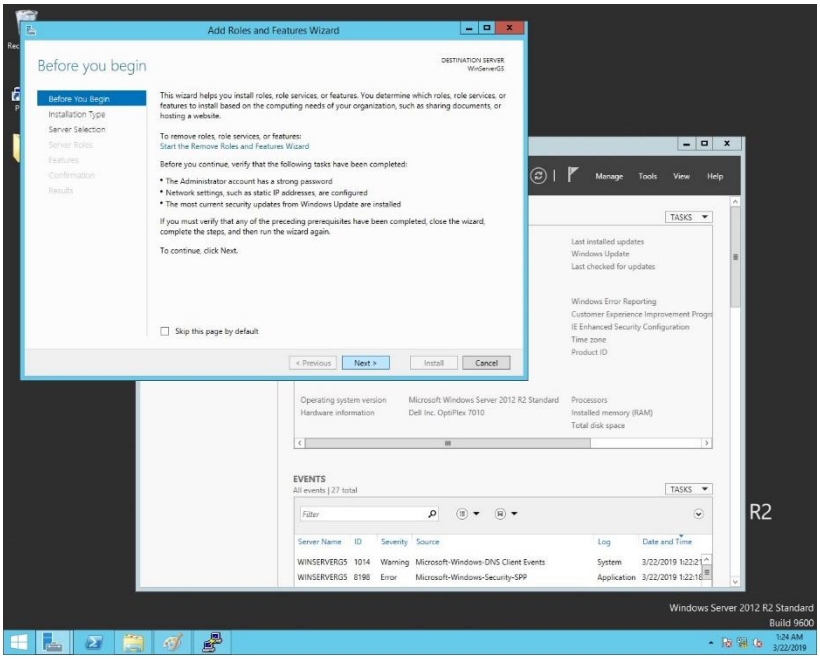


Figure 5.264: Add Roles and Features Wizard

Step 3: In installation type, check the radio button on Role-based or Feature-based Installation and click next.

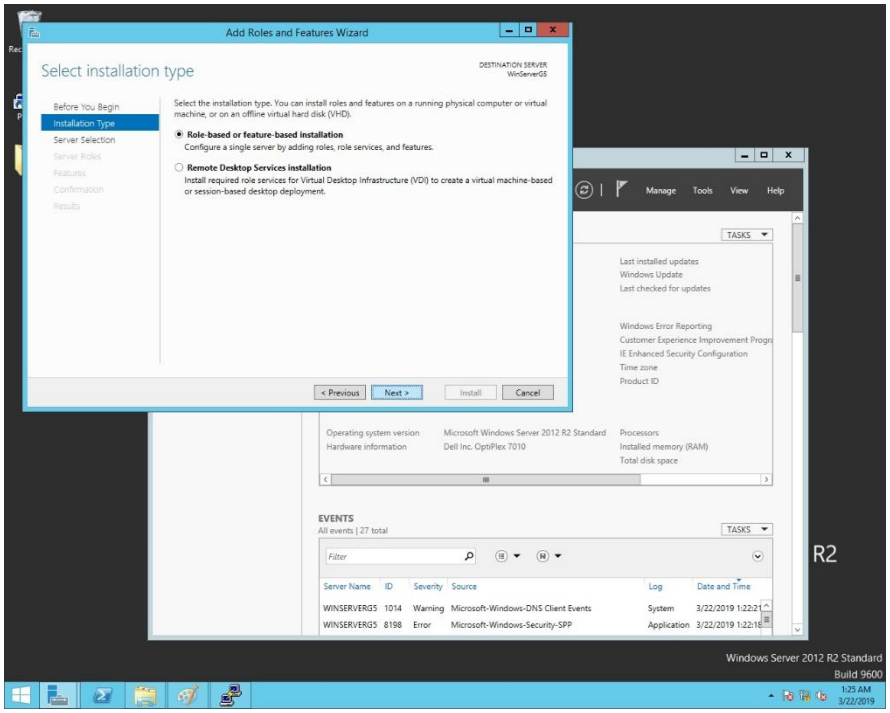


Figure 5.265: Installation type section

Step 4: On server selection, check the select a server from the server pool. This section is to choose where the to install the rules and feature. After that, click next.

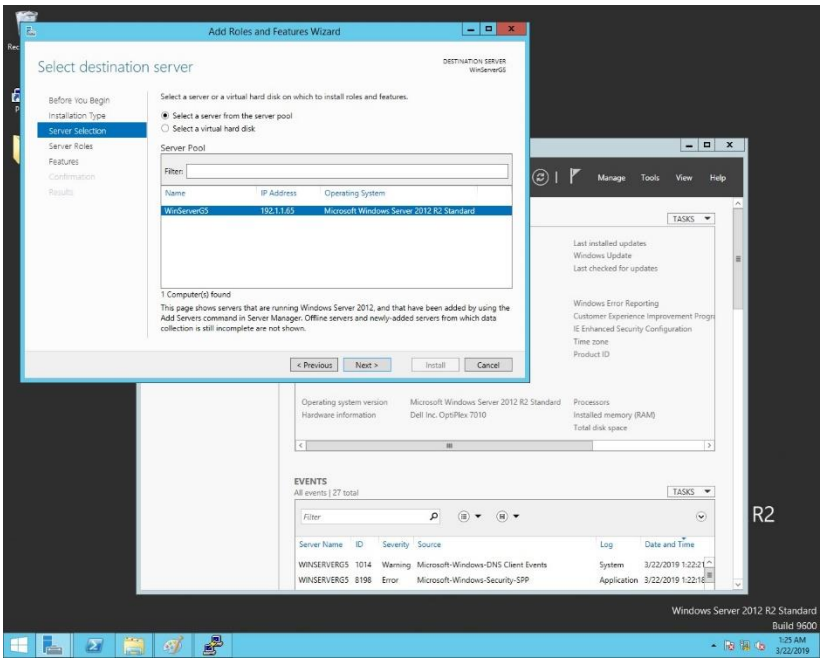


Figure 5.266: Server selection section

Step 5: On the server roles section, click on add features to add a feature to the server.

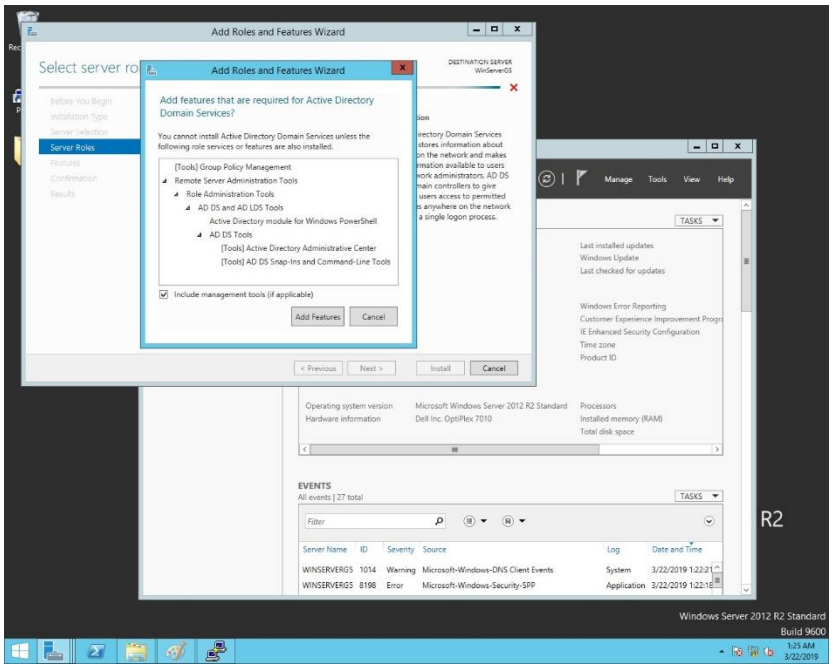


Figure 5.267: Add features

Step 6: Make sure to check the check box for the features we want to add. For install the Active Directory, check the Active Directory Domain Services and click next until confirmation.

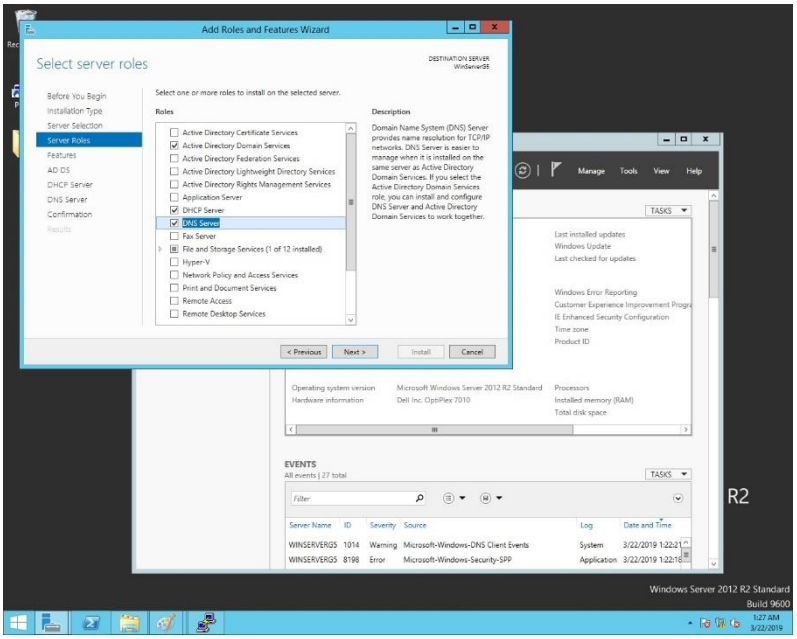


Figure 5.268: Add Server Roles

Step 7: After reach the confirmation part, click install.

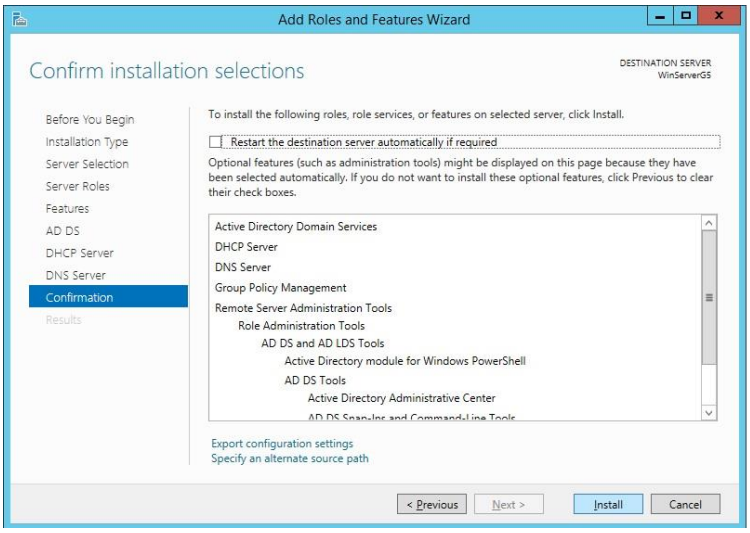


Figure 5.269: Installing Active Directory

Step 8: For this part, just wait for the installation progress to finish their job.

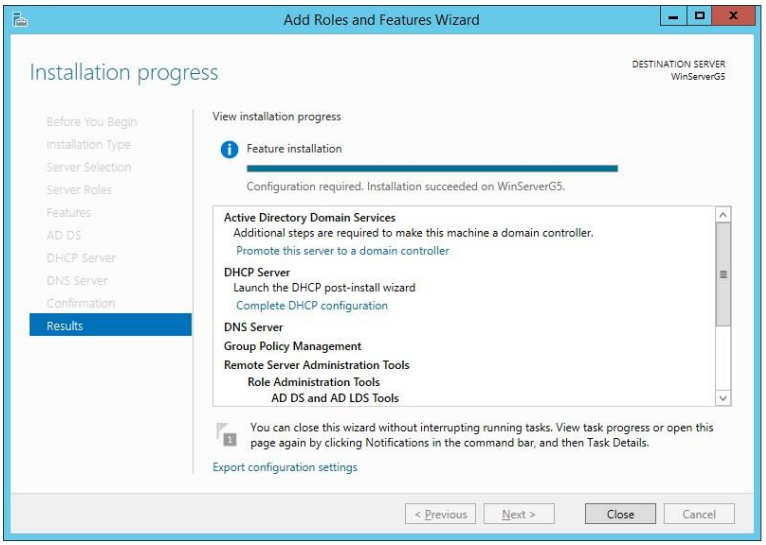


Figure 5.270: Finish installing Active Directory

Step 9: After finished installation, open the server manager. On top right corner, a notification will show at the flag. Now, expand the notification and click the promote the server to a domain controller.

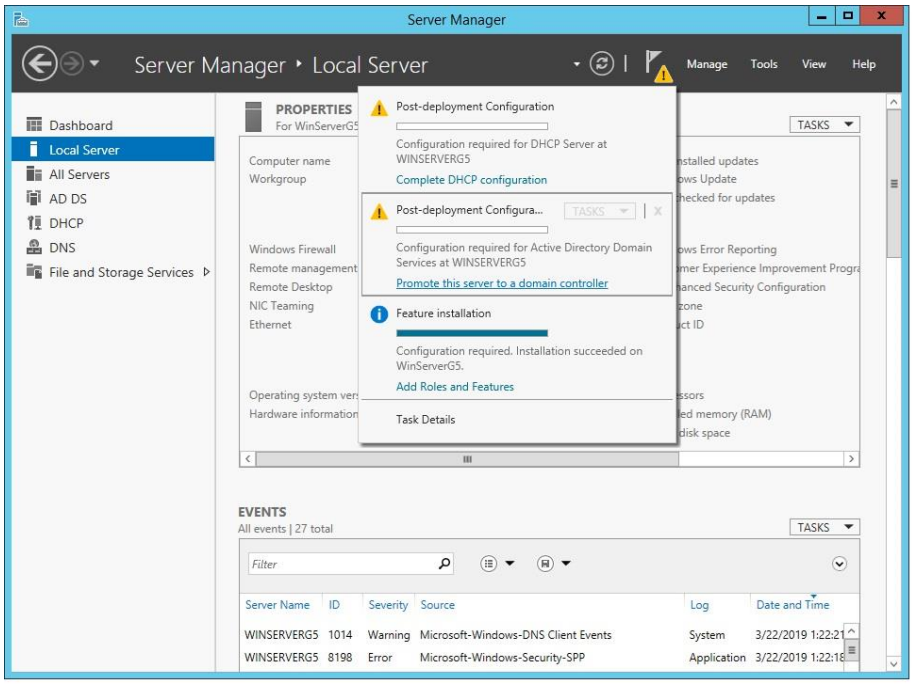


Figure 5.271: Promote server to a domain controller

Step 10: After that, an Active Directory Domain Service Configuration Wizard windows will pop up. To create a new domain. Check the Add a new forest and fill your directory name (ex: infraberry.com). Then click next.

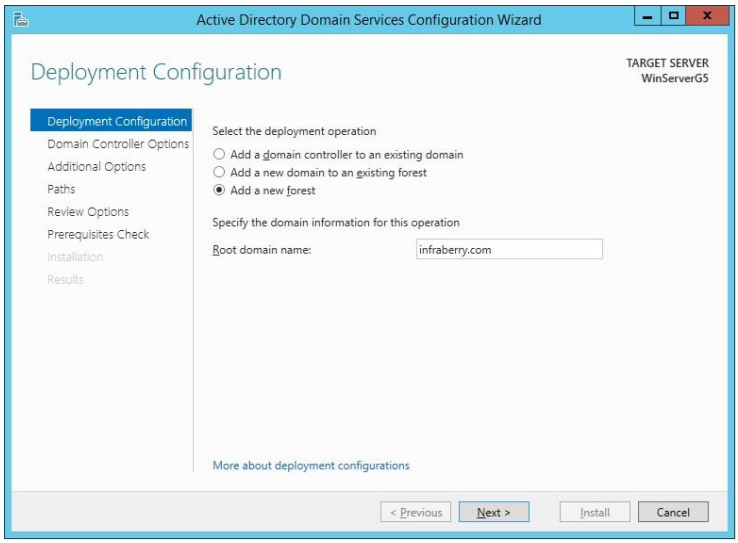


Figure 5.272: Add new forest

Step 11: On domain controller options, enter the domain password and confirmation password below the Type the Directory Services Restore Mode (DSRM) password section. Click next until Prerequisites Check.

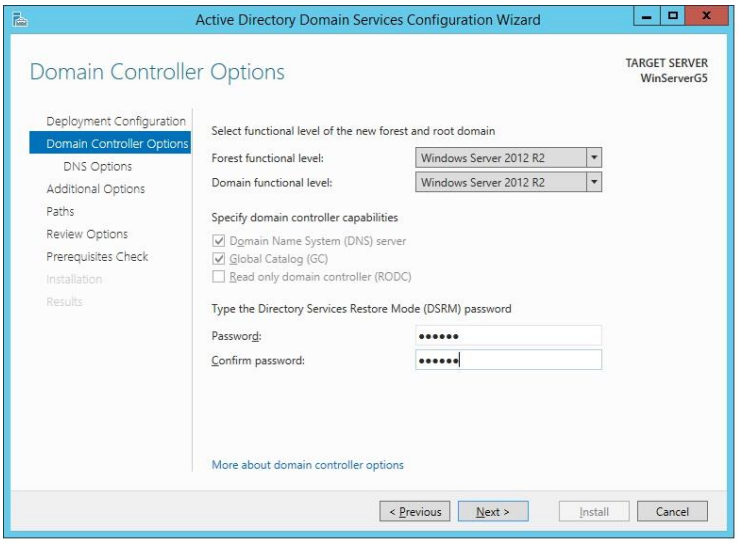


Figure 5.273: Set password for domain

Step 12: On the Prerequisites Check, click install and wait for the installation to finished. After finished, your Domain Controller now is already added.

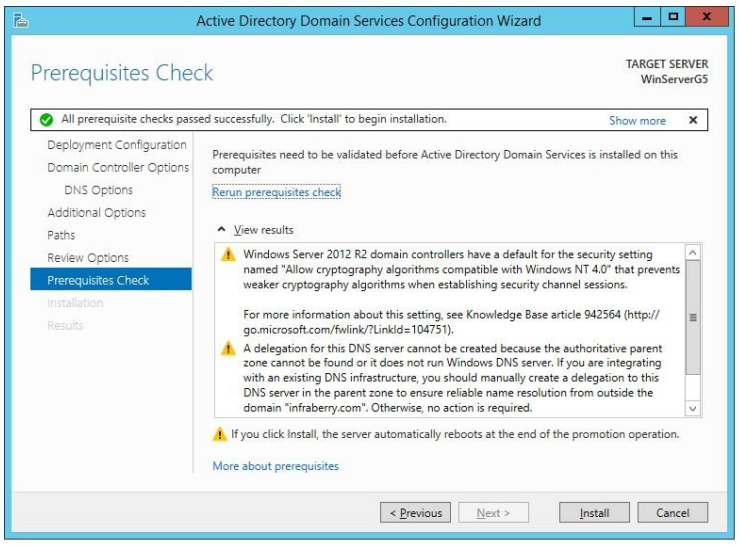


Figure 5.274: Prerequisites check

5.3.14 Proxy Server

Squid is a Unix-based proxy server that caches Internet content closer to a requestor than its original point of origin. Squid supports caching of many different kinds of Web objects, including those accessed through HTTP and FTP.

Below is the step for install and configure the squid proxy server on ubuntu.

Step 1: To install squid proxy server, firstly open the terminal. Type the following command "sudo apt-get install squid squid-common". This command will install a squid proxy server on ubuntu.

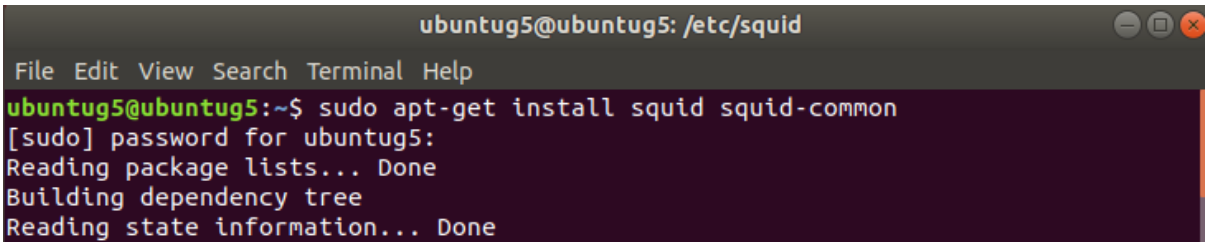


Figure 5.275: Installing squid proxy server

Step 2: After the squid proxy server already installed, go to the squid directory and type "ls" command to show list of files contain in the directory. The errorpage.css and squid.conf file will show in the squid directory. The squid.conf file is important, this file we will use to configure the squid proxy server.

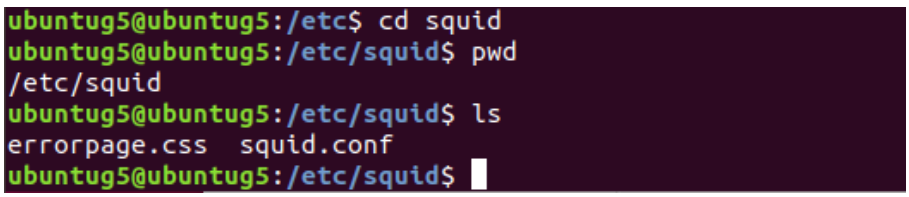


Figure 5.276: File list in squid directory

Step 3: For a safety, recommended to make a backup file for 'squid.conf' file. To do a backup, enter the following command from squid directory "sudo cp squid.conf squid.conf.bak".

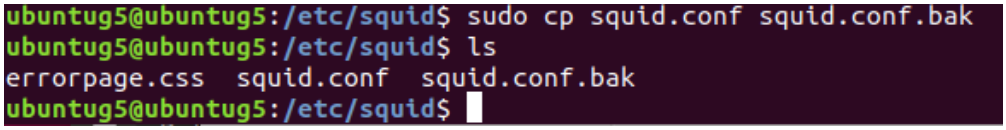


Figure 5.277: Do backup for squid.conf file

Step 4: Open connection settings on Mozilla Firefox browser where squid proxy server is installed. Check manual proxy configuration and insert the IP address for server that install squid server proxy. The default port for squid proxy server is 3128 and tick "use this proxy server for all protocols". Now the squid proxy server is already installed and configure.

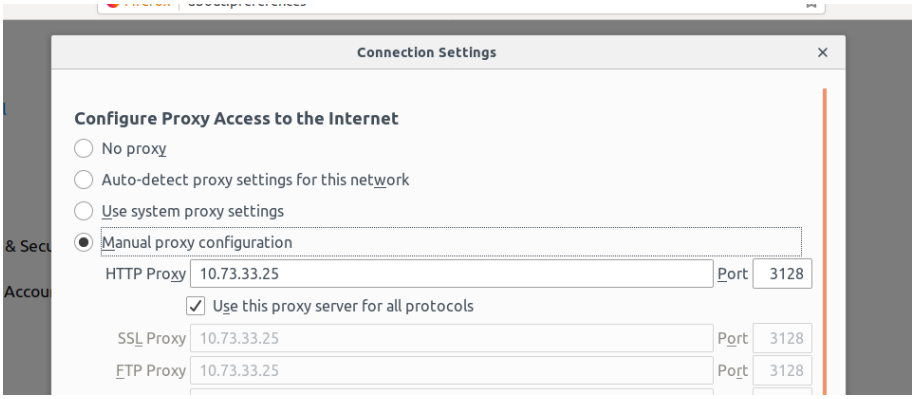


Figure 5.278: Configure proxy Mozilla Firefox browser

5.3.15 Network Monitoring Service

For the network monitoring, we choose Zabbix to monitor the network. Zabbix can monitor Network bandwith usage, packet loss rate, interface error rate, high CPU or memory utilization and many more. Below is the step how to install and configure Zabbix Server on Debian9.

Step 1: Open terminal on the Debian9. Then, enter the root mode. After that, type "wget https://repo.zabbix.com/zabbix/4.0/debian/pool/main/z/zabbix-release/zabbix-release_4.0-2+stretch_all.deb" command to download the Zabbix server repository. Then to install, type "dpkg -i zabbix-release_4.0-2+stretch_all.deb" command. After finish install type "apt update" to updates the package lists for upgrades for packages that need upgrading, as well as new packages that have just come to the repositories.

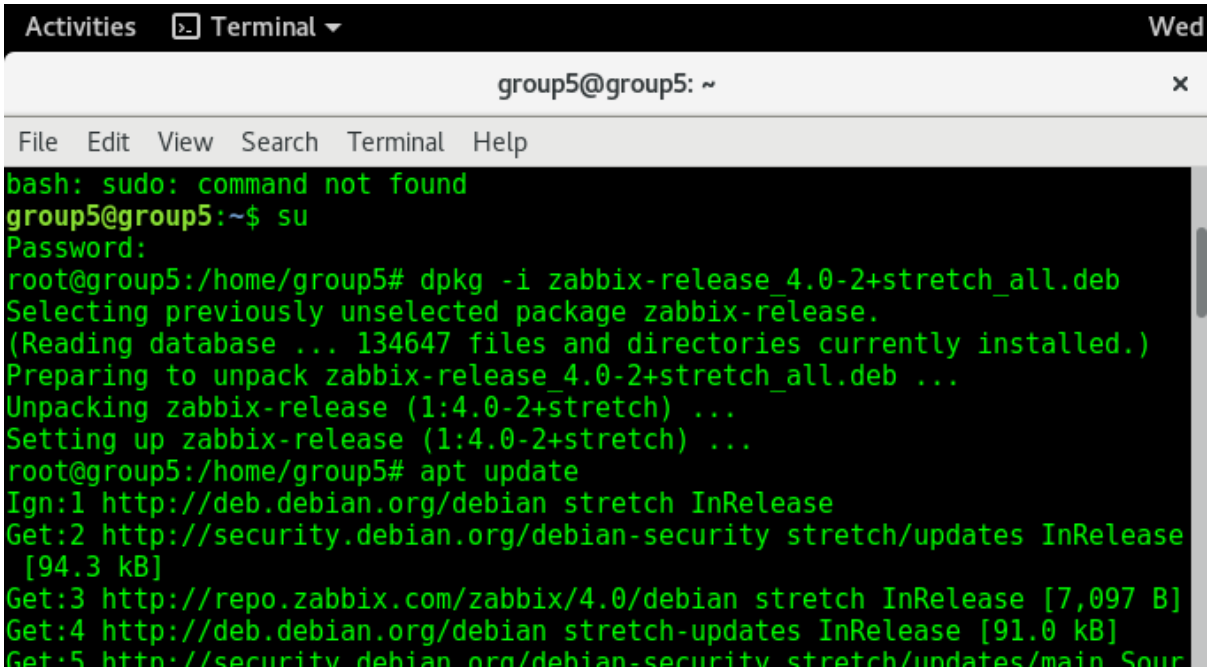


Figure 5.279: Download Zabbix server repository

Step 2: After that, Install Zabbix server, frontend and agent. To do this, type "apt -y install zabbix-server-mysql zabbix-frontend-php zabbix-agent" command.

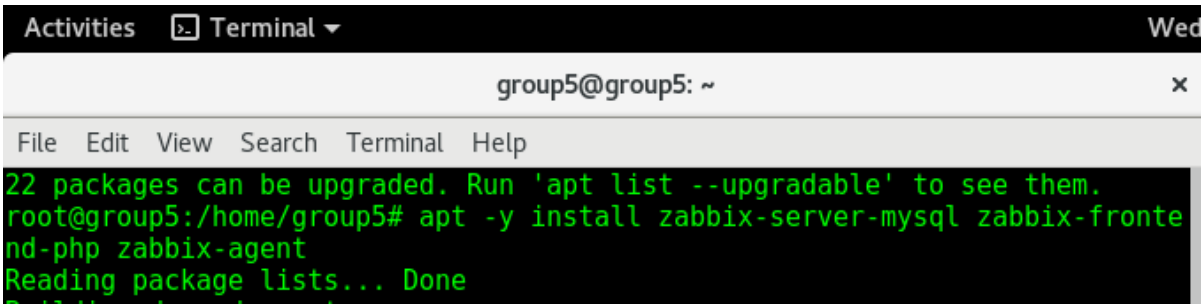


Figure 5.280: Install Zabbix server and frontend

Step 3: After done install Zabbix server, frontend and agent. Create initial database for Zabbix. To do this type “mysql -uroot -p” and enter. Then type “create database zabbix character set utf8 collate utf8_bin;” to create database and type “grant all privileges on zabbix.* to zabbix@localhost identified by 'password';” to grant privileges.

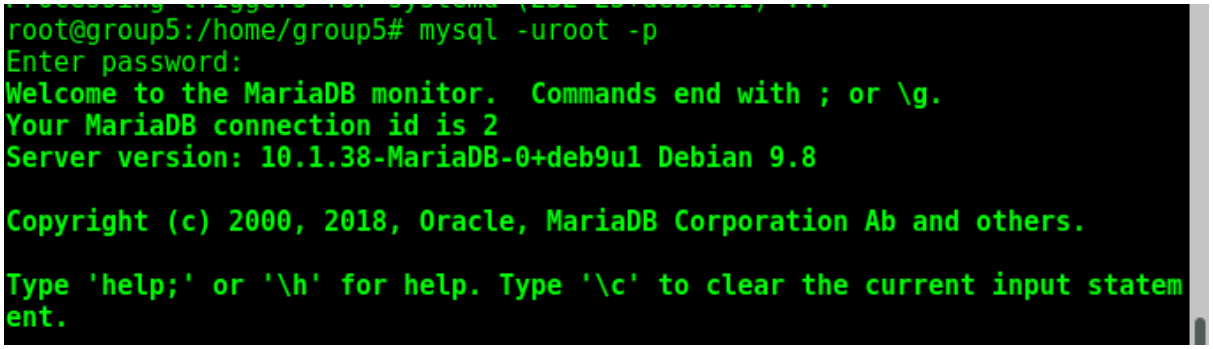


Figure 5.281: Create initial database for Zabbix

Step 4: Now open the frontend of the Zabbix by typing your server ip address (ex:192.1.1.66/zabbix) on the browser. Then click next.

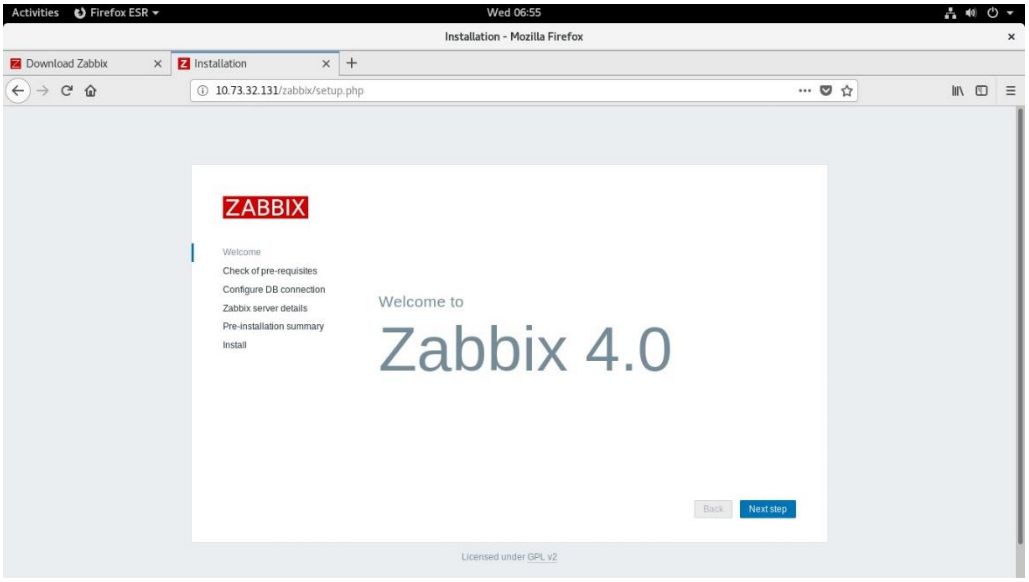


Figure 5.282: Open Zabbix frontend

Step 5: Now it will automatically check the pre-requisites. If no error click next step to continue.

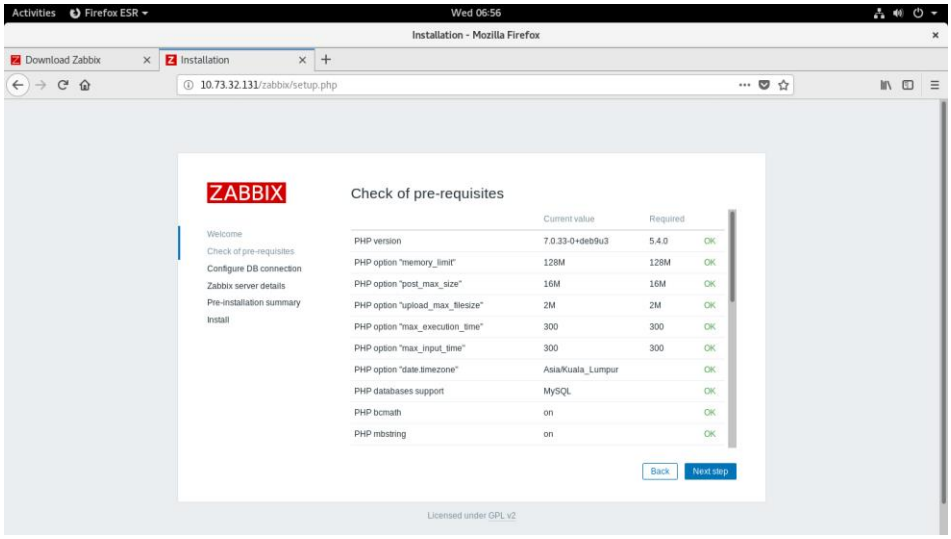


Figure 5.283: Check prerequisites

Step 6: Now, enter your database name, user and password then click next step until finish install.

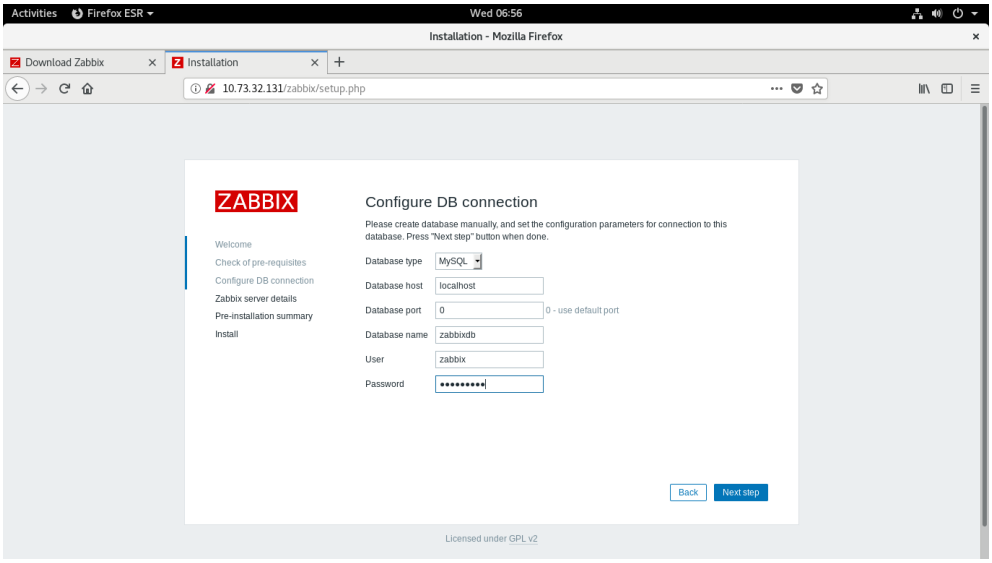


Figure 5.284: Configure DB connection

Step 7: After finish install, it will appear “Congratulations! You have successfully installed Zabbix frontend”. Then click finish and login using default Zabbix username and password.

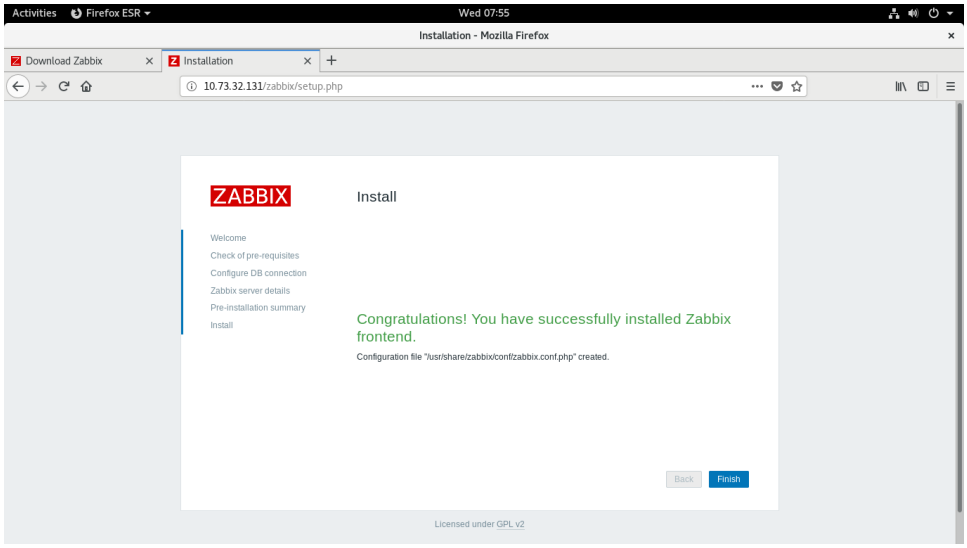


Figure 5.285: Finish installing Zabbix server

Step 8: This is the frontend interface for Zabbix server. Zabbix server is finished install and ready to use.

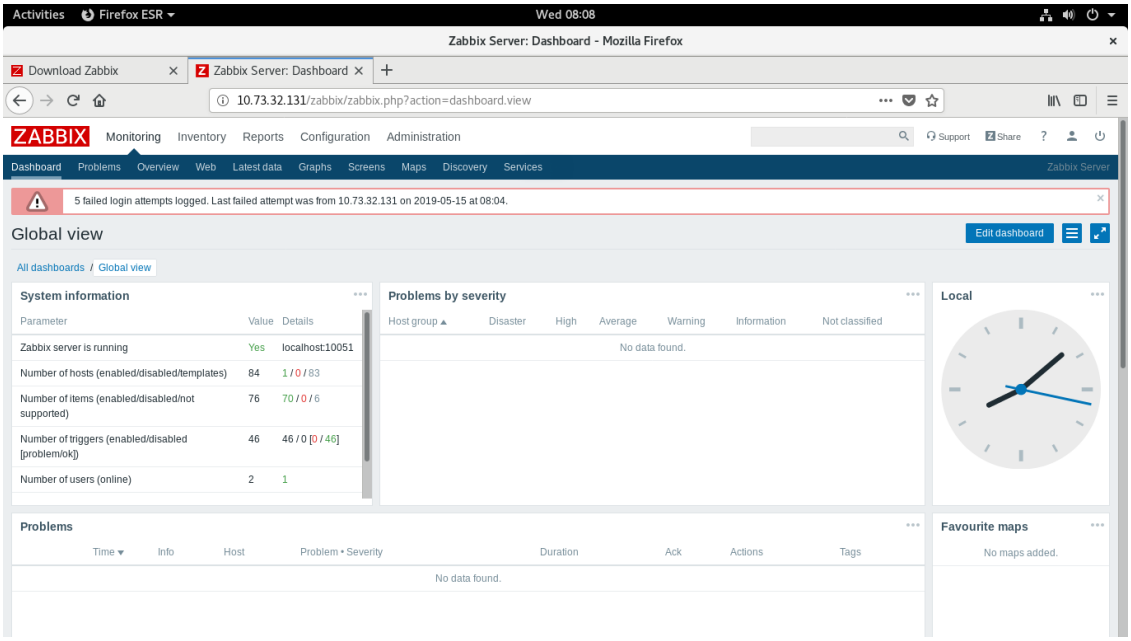


Figure 5.286: Interface of Zabbix monitoring

CHAPTER 6 – TESTING

6.1 Introduction

All of the services that had can be use or access by using different method and different tools. In this chapter will show how to use the service that had been setup and configured. The testing also is to ensure the functioning of the service are successfully up and running. Testing is the practice of making objective judgments regarding the extent to which the system (device) meets, exceeds or fails to meet stated objectives. Moreover, testing is about managing risk.

6.2 Services Testing

6.2.1 Domain Name Service (Dns)

Step 1: We test in the command prompt. Using the command nslookup. If it is successful, it will display the information.

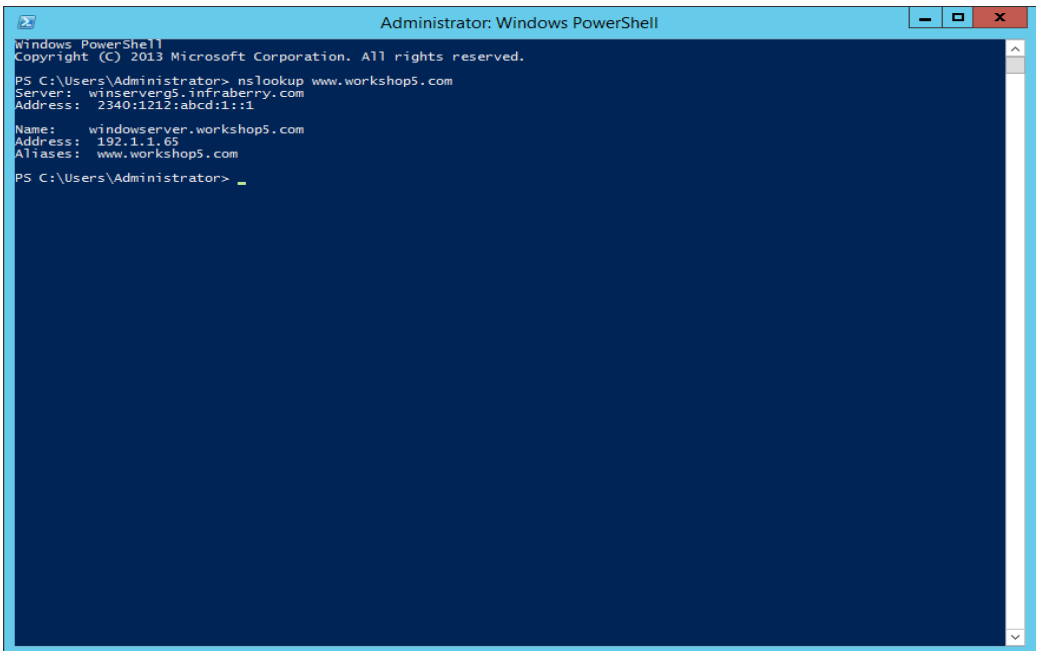


Figure 6-1: Testing DNS

6.2.2 Routing & Nat

Testing Analysis

To test the NAT which has been configured, a few commands will be used. The **"show ip nat translation"** command is used to check is the private address is translated to public and vice versa. Rounting can be seen by using the "show ip route" command to show the connected port and the route of IP address of the router.

Step 1: Show the sub-interface which have been assigned the IP NAT inside and outside.

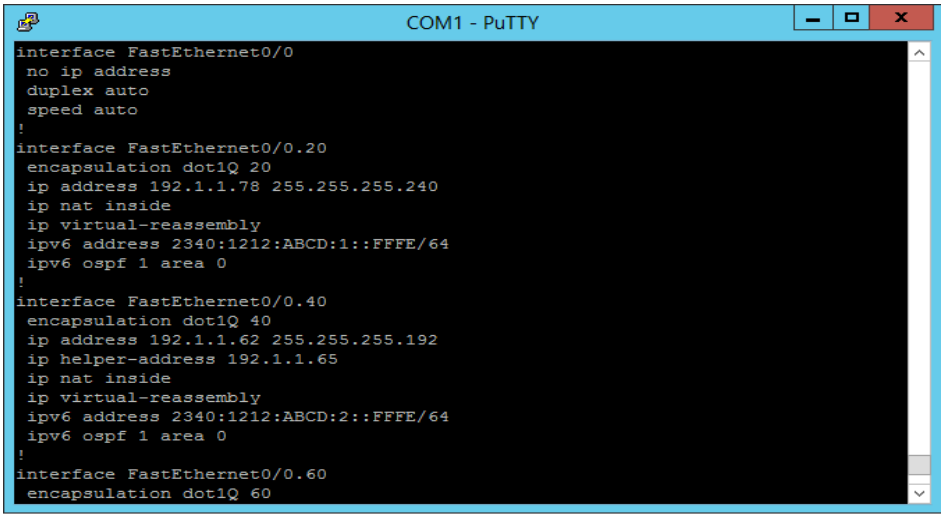


Figure 6-2: IP NAT Inside and Outside of Sub-Interface

Step 2: Show the command **"show ip nat translation".**

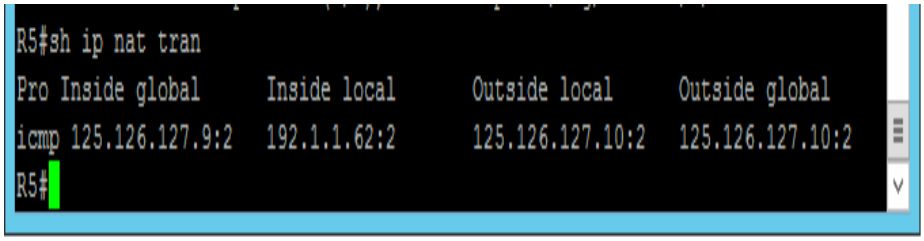


Figure 6-3: IP NAT translation

6.2.3 Server Virtualization

6.2.2.6 Server Virtualization

Step 1: Open the Hyper-V Manager.

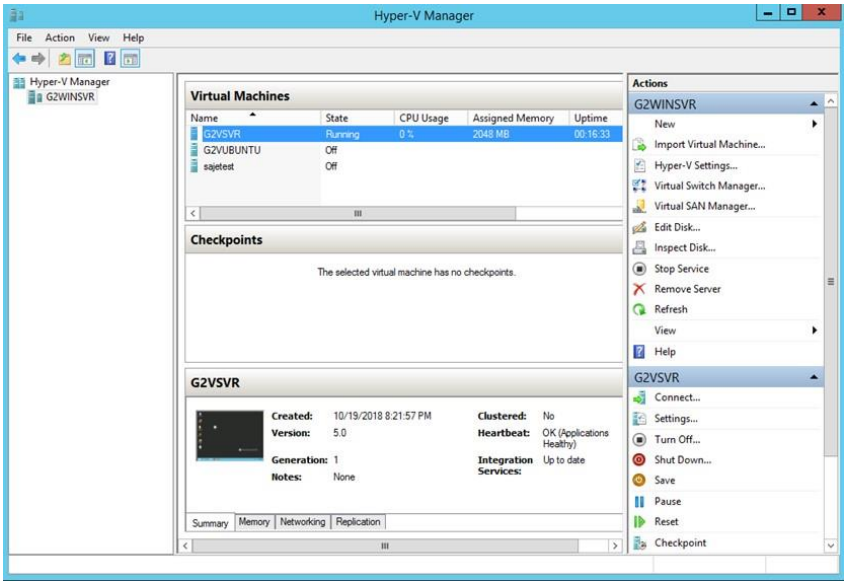


Figure 6-4: Hyper-V Manager

Step 2: Right click on the Virtual Machine and click Connect.. to start.

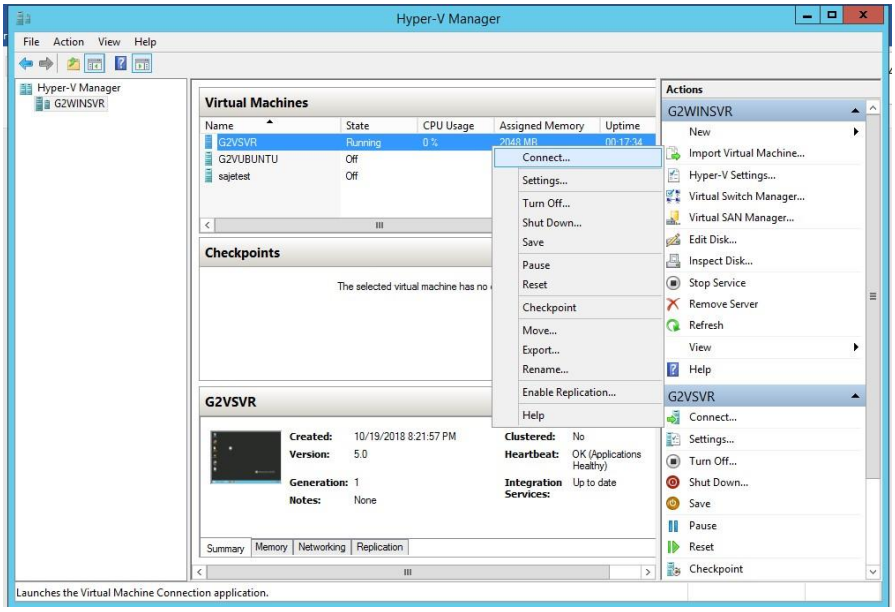


Figure 6-5: Hyper-V Manager

Step 3: Do some command in VM to show the file sharing

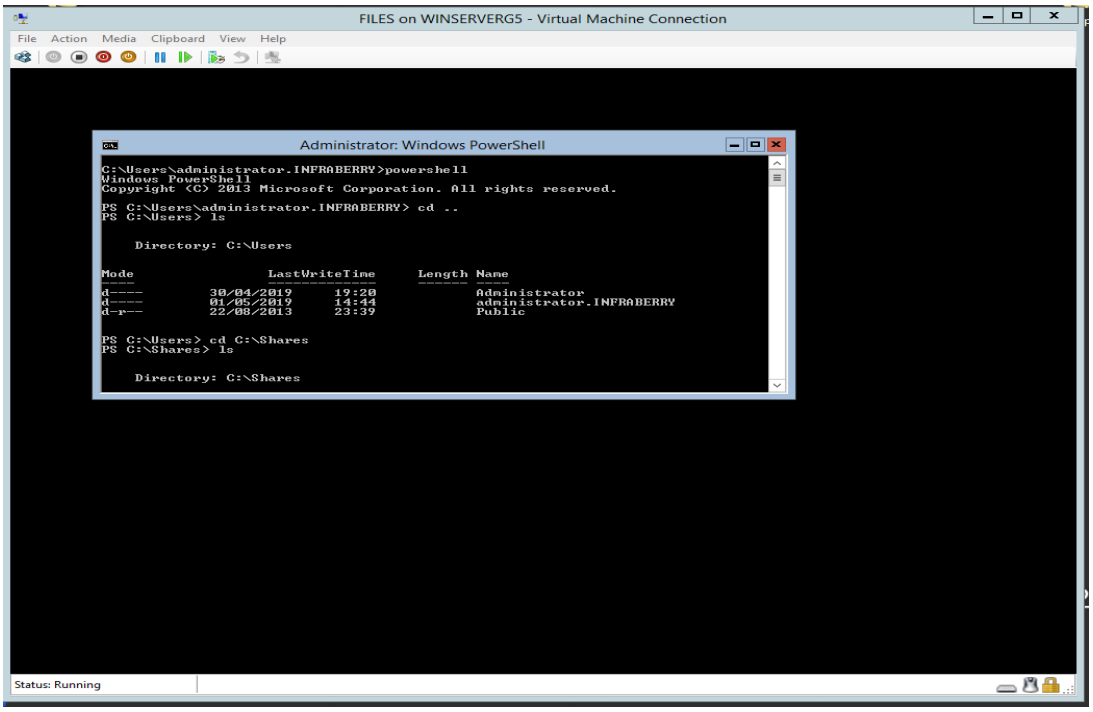


Figure 6-6: file sharing command

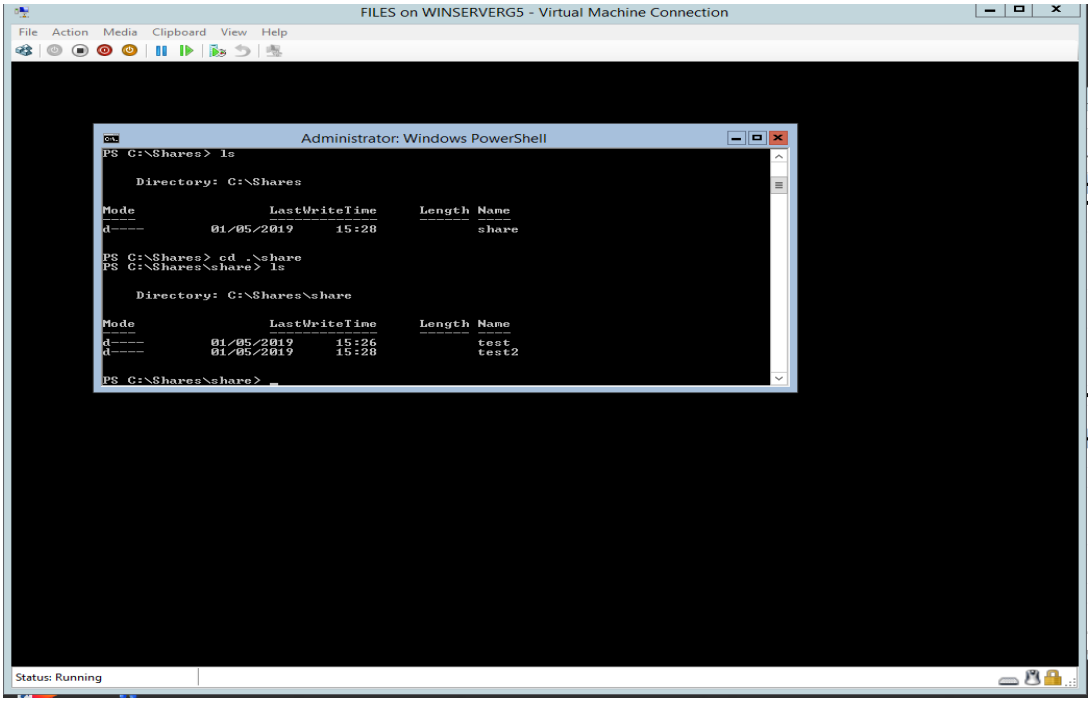


Figure 6-7: file sharing command

6.2.4 DHCP

Testing for DHCP is done by using the command prompt from the client by entering ipconfig /all. The function of this command is to displays all current TCP/IP network configuration values and refreshes Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) settings. From all the information displayed, focus on the IPv4 address and DHCP enabled. The IP should correspond to what has been set for client IP address and the DHCP Enabled should be tick as Yes. If both of these requirements are displayed, then the testing for DHCP is a success.

Step 1: Connect client to client port (fa0/22 – fa0/24).

Step 2 : On client, open CMD and type ipconfig.

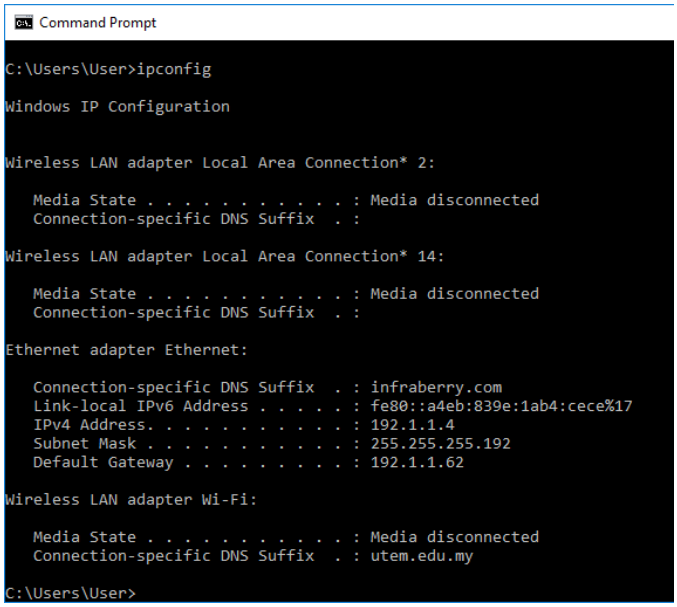


Figure 6-8: Client Testing

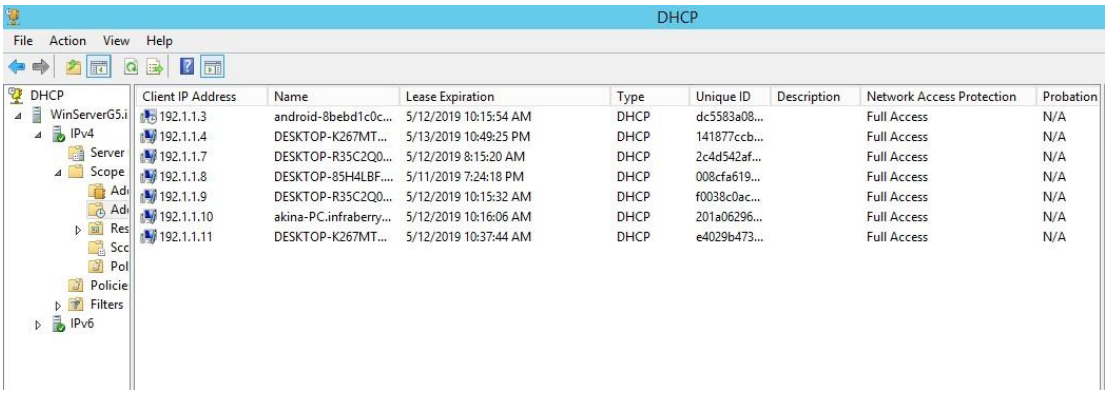
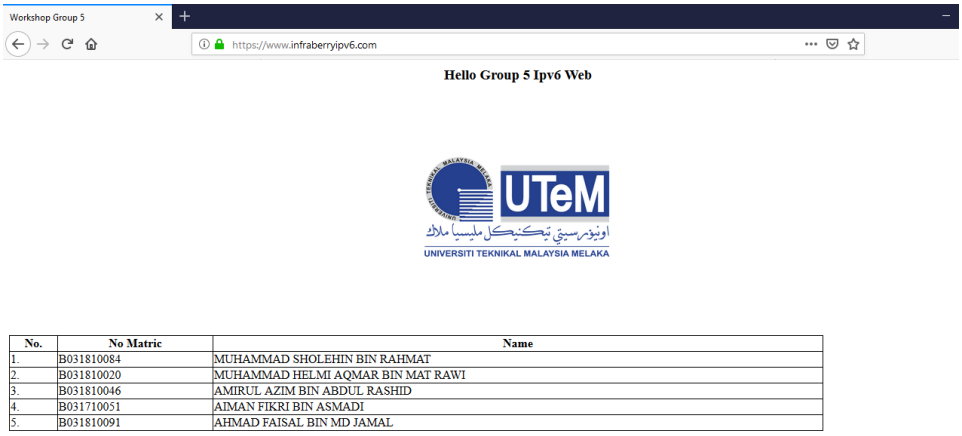


Figure 6-9: The DHCP will display all the user that get the DHCP IPv4.

6.2.5 Ipv6 With Web

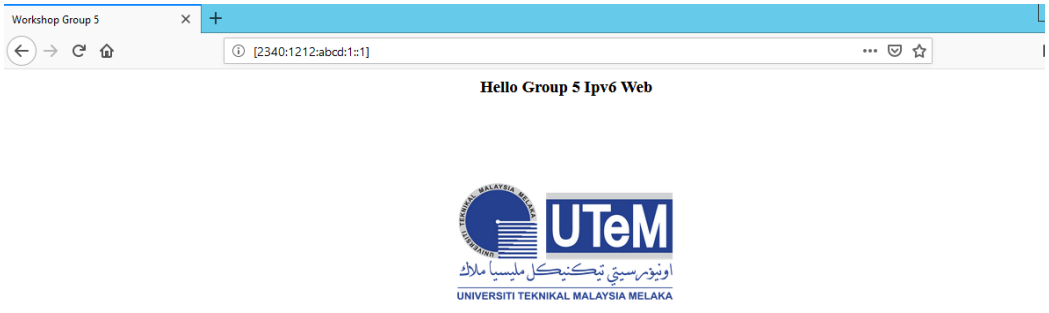
Step 1: Open browser then type https://www.infraberryipv6.com then the website will appear.



No.	No Matric	Name
1.	B031810084	MUHAMMAD SHOLEHIN BIN RAHMAT
2.	B031810020	MUHAMMAD HELMI AQMAR BIN MAT RAWI
3.	B031810046	AMIRUL AZIM BIN ABDUL RASHID
4.	B031710051	AIMAN FIKRI BIN ASMADI
5.	B031810091	AHMAD FAISAL BIN MD JAMAL

Figure 6-10: IPv6 Web page is accessible

Step 2: Open browser then type https://[2340:1212:abcd:1::1] then the website will appear.



No.	No Matric	Name
1.	B031810084	MUHAMMAD SHOLEHIN BIN RAHMAT
2.	B031810020	MUHAMMAD HELMI AQMAR BIN MAT RAWI
3.	B031810046	AMIRUL AZIM BIN ABDUL RASHID
4.	B031710051	AIMAN FIKRI BIN ASMADI
5.	B031810091	AHMAD FAISAL BIN MD JAMAL

Figure 6-11: Show https://[2340:1212:abcd:1::1]

6.2.6 Linux Email Server

Scenario: Send Email from user1 to user2.

Step 1: Open Rainloop Webmail

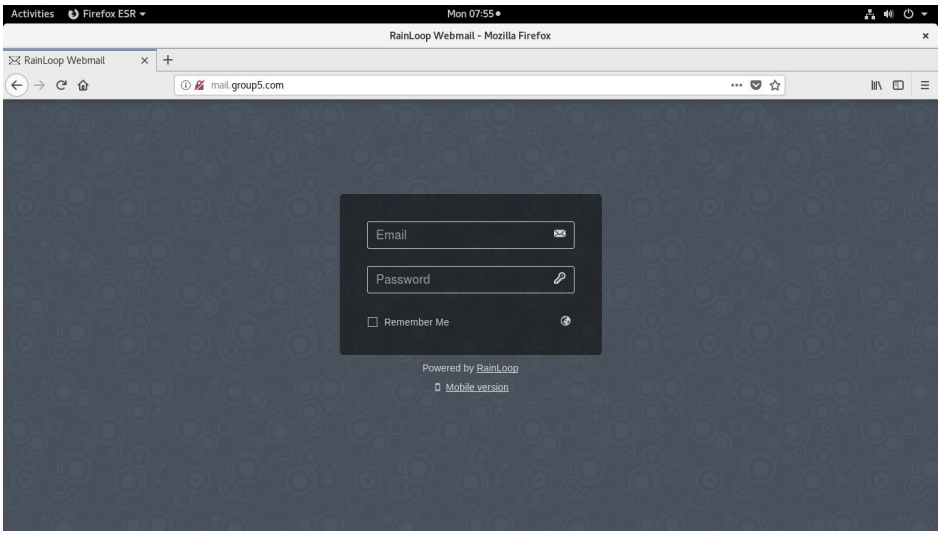


Figure 6-12: Rainloop Webmail URL

Step 2: Login with user1@group5.com

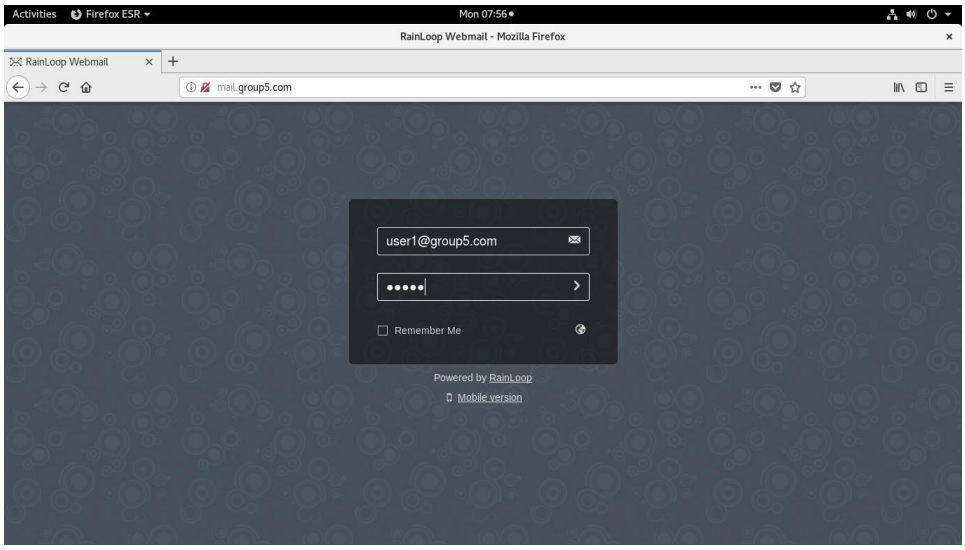


Figure 6-13: Rainloop Webmail Login

Step 3: Compose an email to user2@group5.com

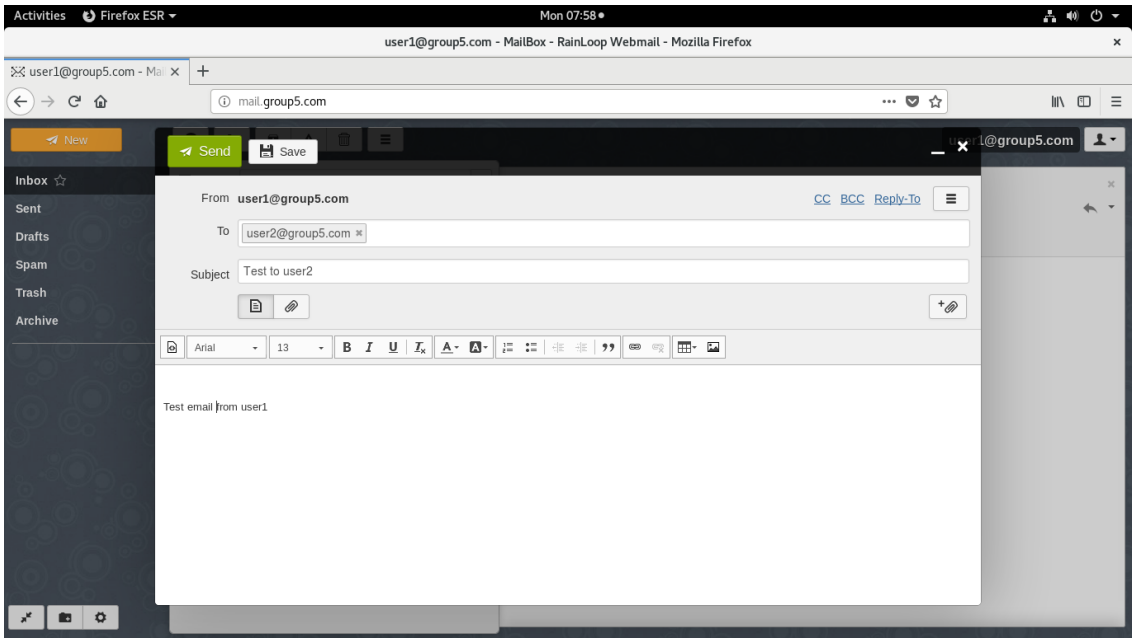


Figure 6-14: Send Email

Step 4: An email send to user2@group5.com

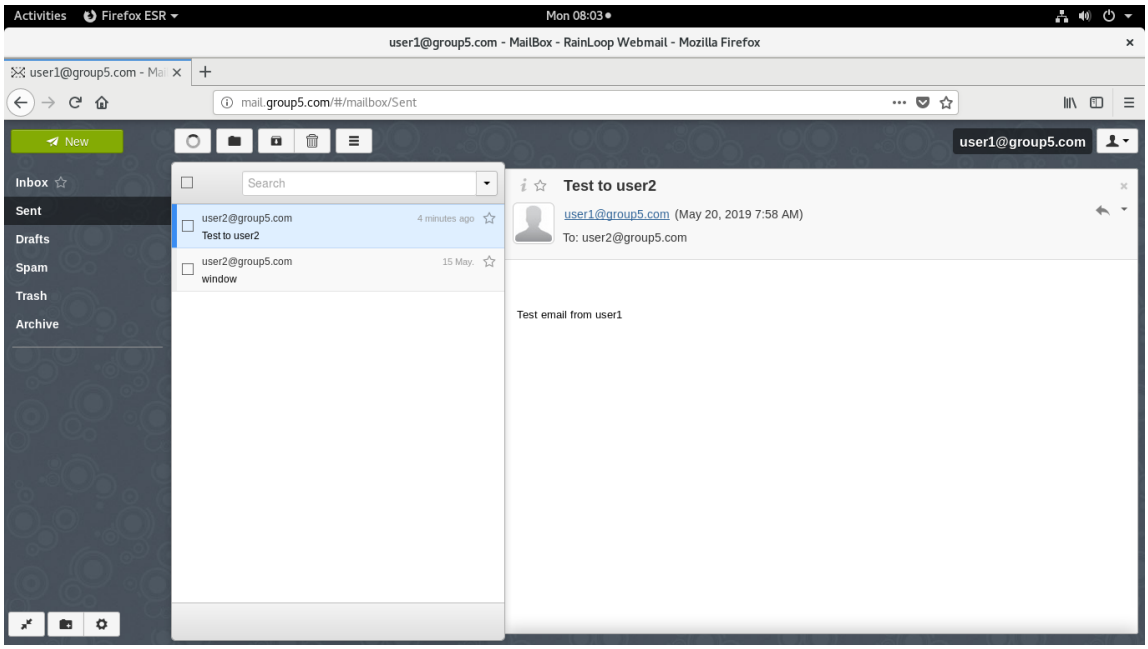


Figure 6-15: Verify Email is send

Step 5: Login again with user2@group5.com

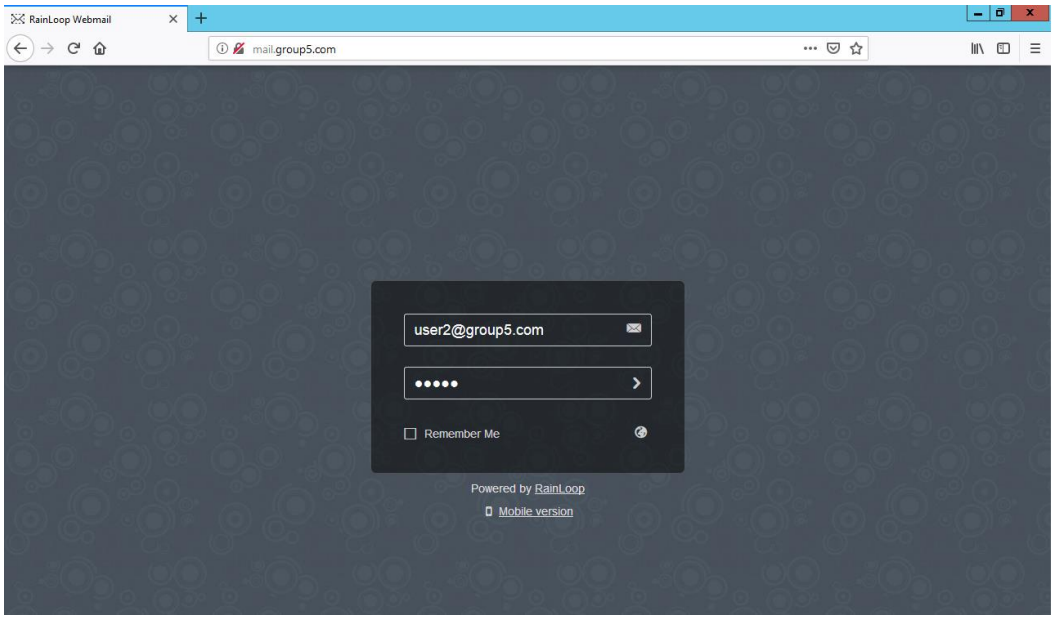


Figure 6-16: Rainloop Webmail Login

Step 6: We should see the new email in inbox.

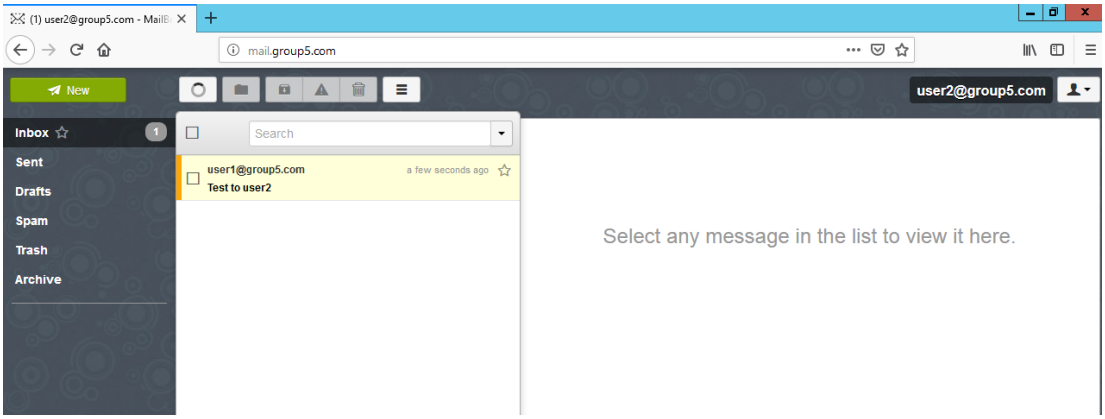


Figure 6-17: Email Inbox

Step 7: Open the email for confirmation.

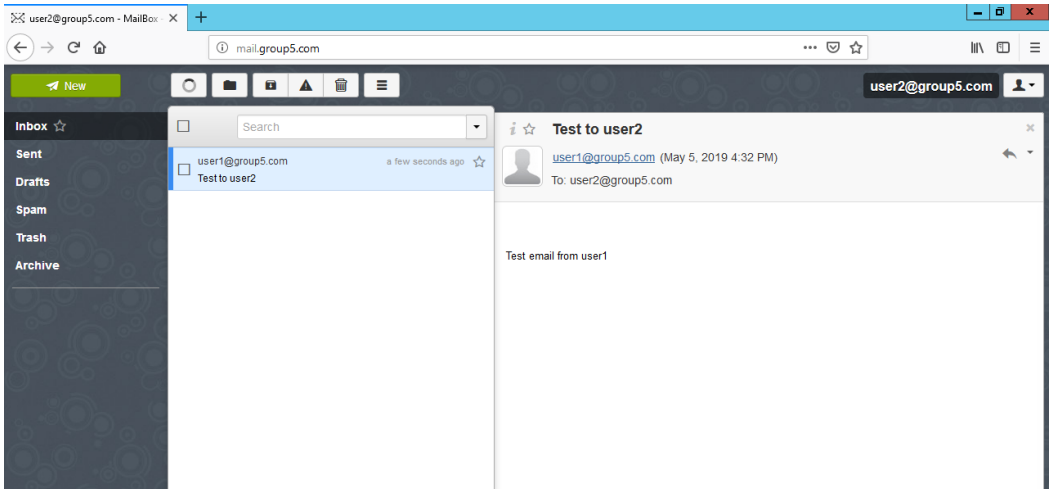


Figure 6-18: Open Email

6.2.7 Active Directory

Scenario: Add new user in a domain and login with client PC.

Step1: Open Sever Manager and click Tools at top right corner and choose Active Directory Users and Computers.

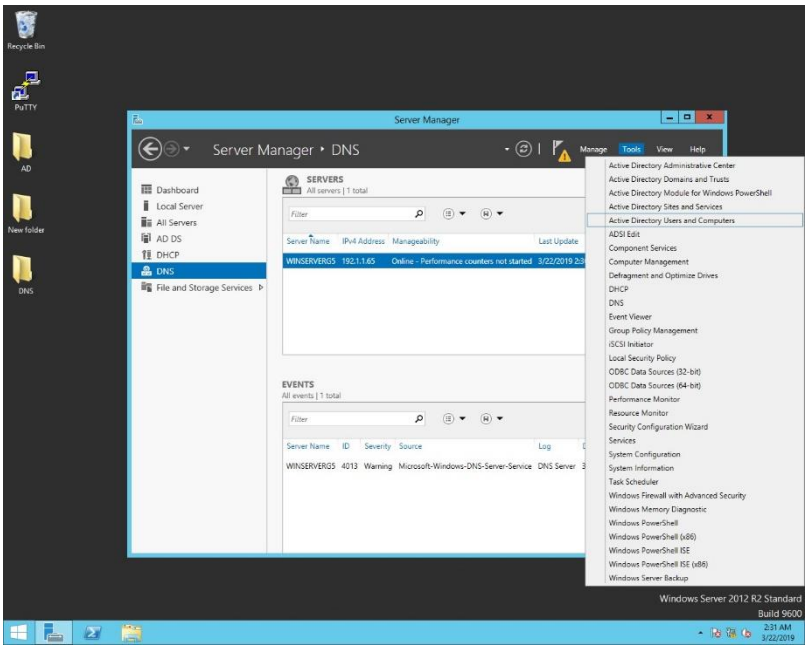


Figure 6-19: Open Active Directory Users and Computers

Step 2: Expand the domain on the left side bar.

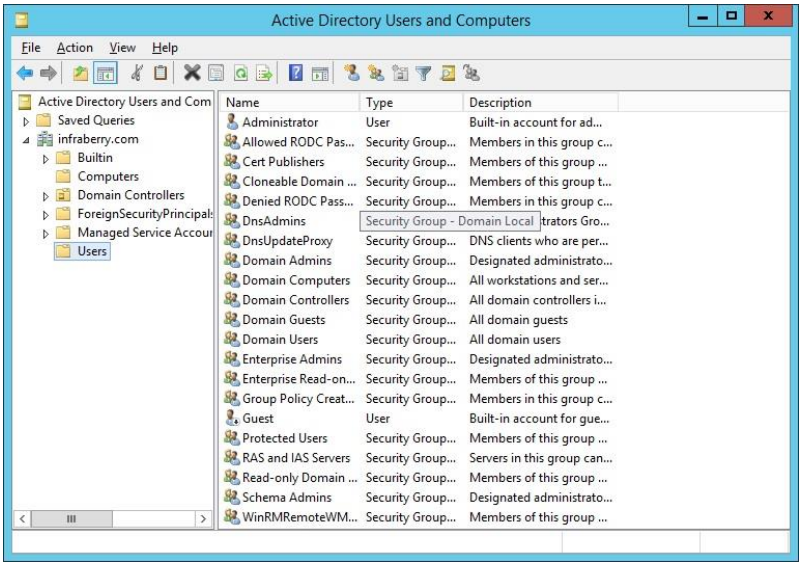


Figure 6-20: Expand the domain section

Step 3: Right click on users and expand New then click User.

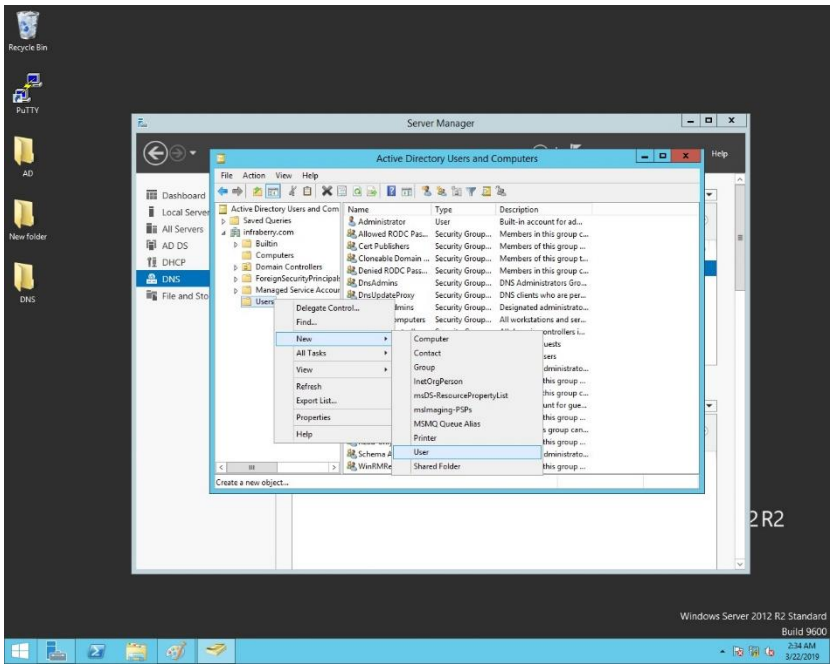


Figure 6-21: Expand New and click User

Step 4: Fill all the blanks field except initial at the New Object – User.

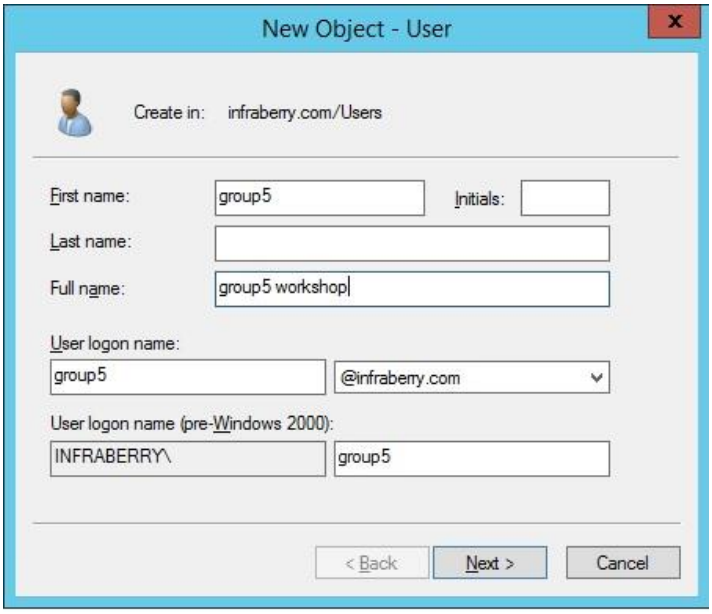


Figure 6-22: Fill all the user details

Step 5: Insert the user password and check any of the check box that u wants.

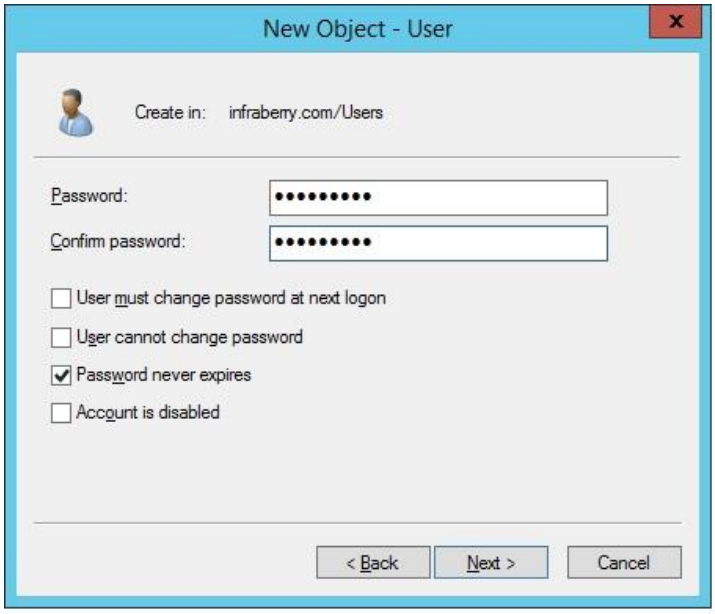


Figure 6-23: Create user password

Step 6: Click finish to completely add new user.

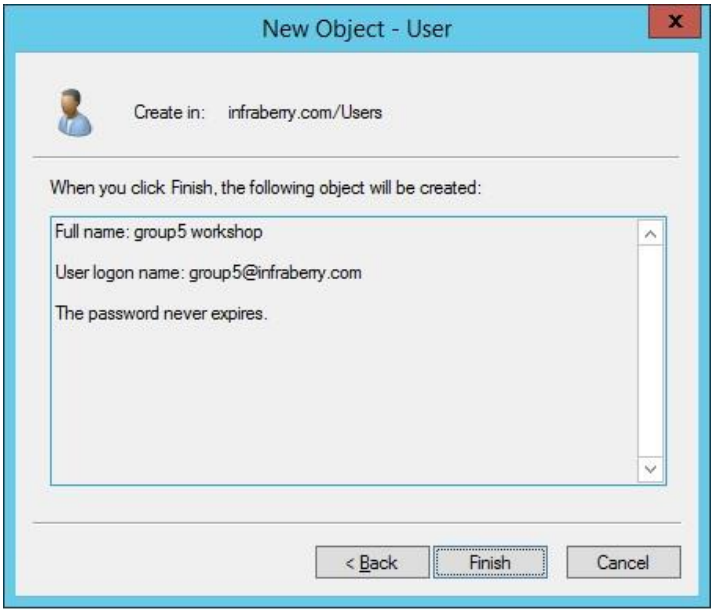


Figure 6-24: Finish to create new user

Step 7: Open system properties and click change on computer name tab.

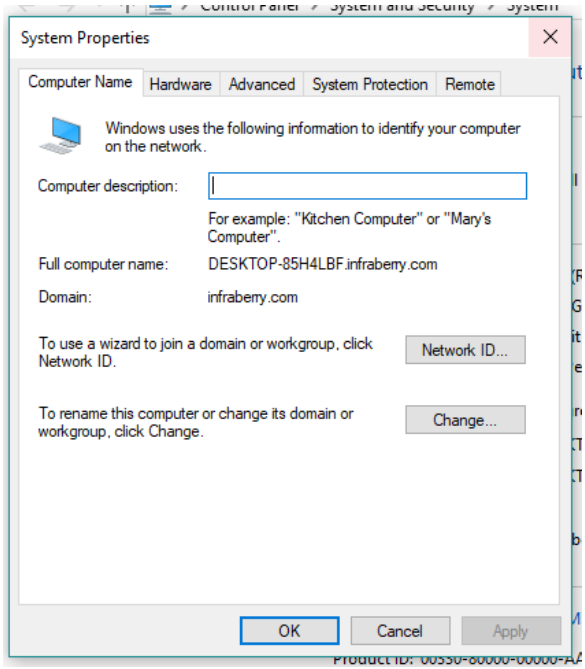


Figure 6-25: System properties windows

Step 8: Check the Domain radio button and insert your domain name.

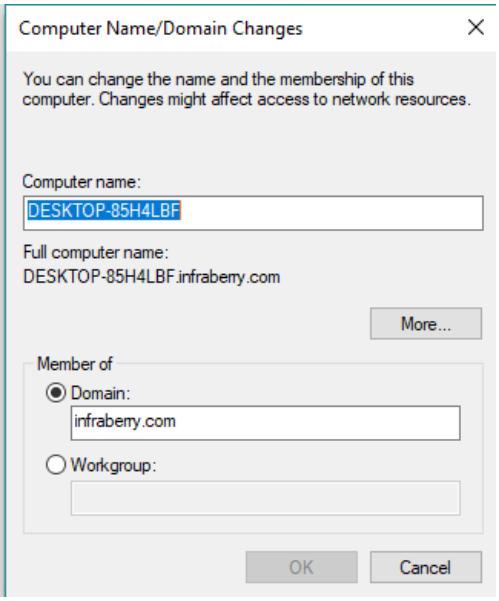


Figure 6-26: Join domain

Step 9: Login to the client PC using the username and password that already created.

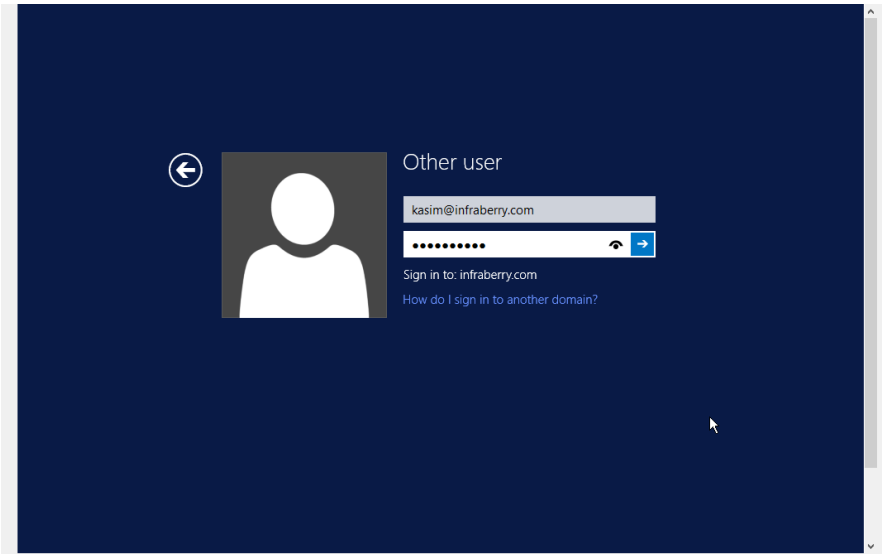


Figure 6-27: Login new user

Step 10: If successfully login, check the system. On the domain site it will show your domain name.

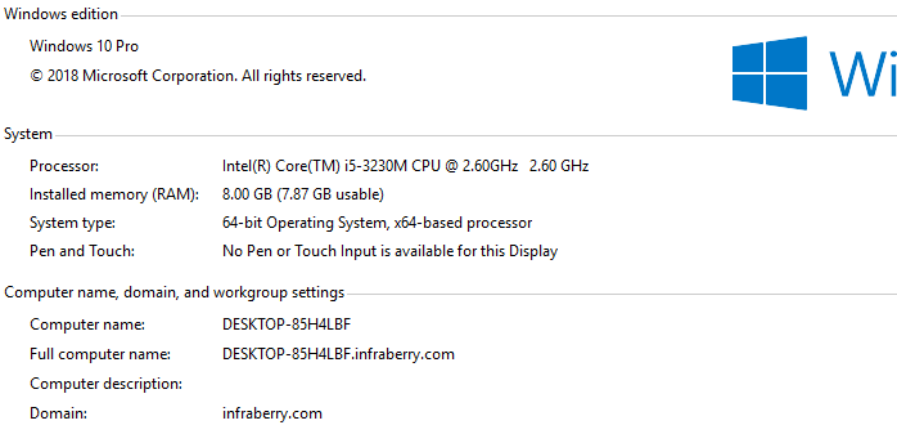


Figure 6-28: System details

6.2.8 Proxy Server

Scenario: Block a website page using Squid Proxy Server.

Step 1: Open squid.conf file for configuration.

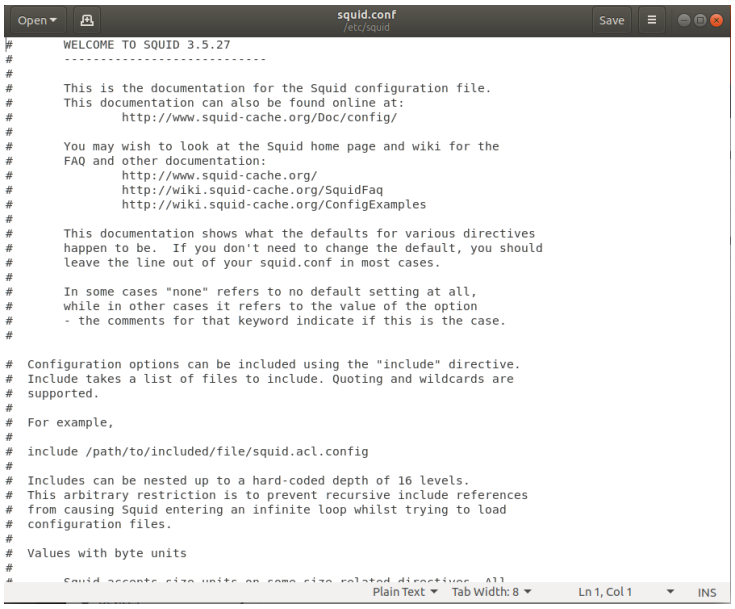


Figure 6-29: squid.conf file

Step 2: Add a new command in squid.conf file. Type http_access deny [variable name] and acl [variable name] dstdomain [your block website ex: .msn.com]. This command will block the website that you want. Save the file.

```
 988 acl Safe_ports port 280         # http-mgmt
 989 acl Safe_ports port 488         # gss-http
 990 acl Safe_ports port 591         # filemaker
 991 acl Safe_ports port 777         # multiling http
 992 acl CONNECT method CONNECT
 993
 994 acl block_websites dstdomain .msn.com .yahoo.com
 995 http_access deny block_websites
 996
 997 #  TAG: proxy_protocol_access
 998 #       Determine which client proxies can be trusted to provide correct
 999 #       information regarding real client IP address using PROXY protoco
1000 #
1001 #       Requests may pass through a chain of several other proxies
```

Figure 6-30: Add new command on squid.conf file

Step 3: Open browser and go to the blocked website. The website that has been blocked will show access denied.

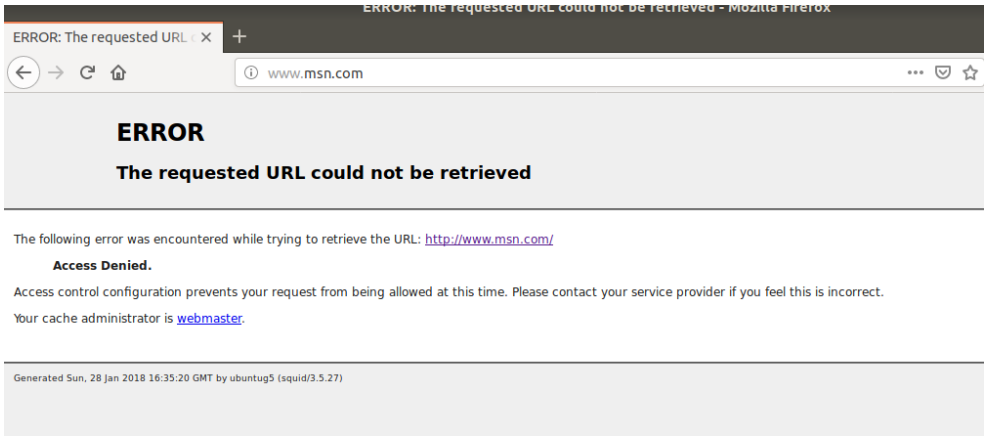


Figure 6-30: Blocked website

6.2.9 Network Management System (Nms)

Scenario: Monitor the Windows Server using Zabbix.

Step1: Go to zabbix.com website, go to Zabbix agent and find the windows.msi package.

Figure 6-31: Download Zabbix agent application for windows server

Step 2: After that, open the Zabbix-agent application and insert the details.

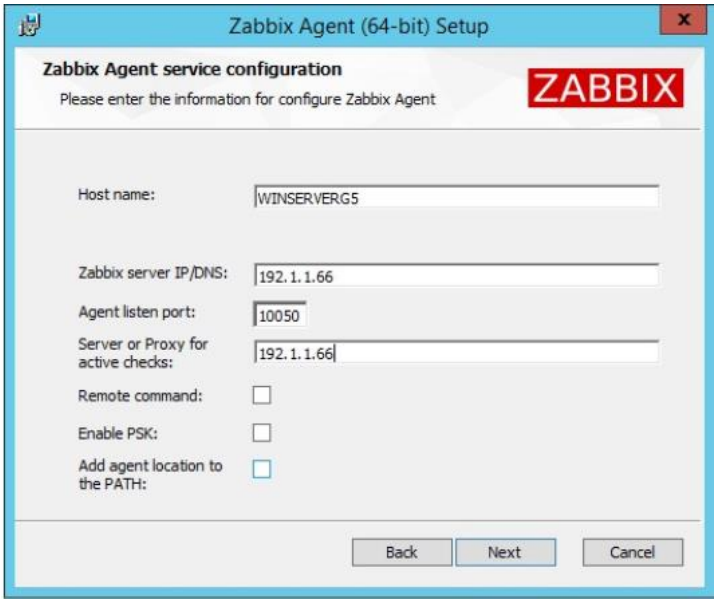


Figure 6-32: Insert details for Zabbix agent

Step 3: Wait for the Zabbix agent to finish installation.

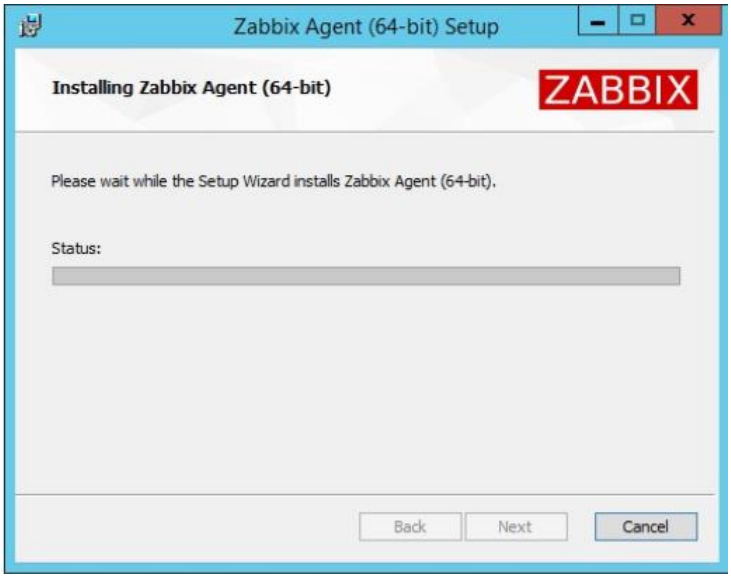


Figure 6-33: Installing Zabbix agent

Step 4: After finish installation, it will show the Zabbix agent is running on your system service.

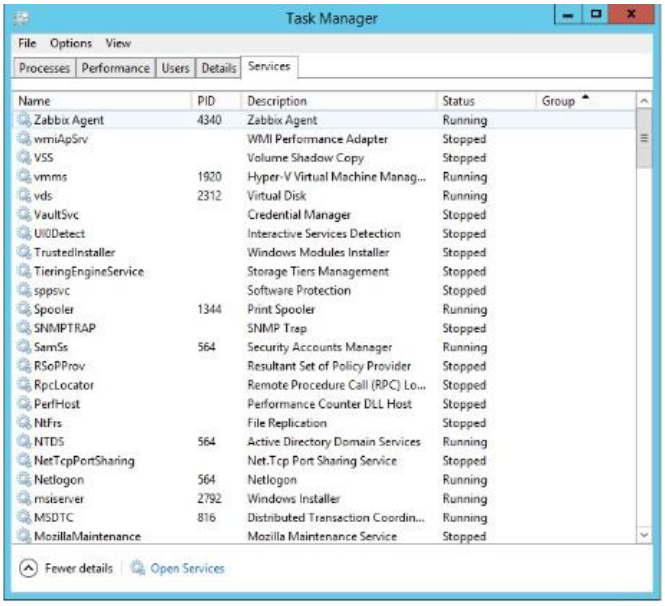


Figure 6-34: Zabbix agent is running on Windows Server services

Step 5: Login into Zabbix frontend and go to configuration then add new host. Fill the details for hostname, group and agent interface. On agent interface, insert your Windows Server IP address and leave the port as default.

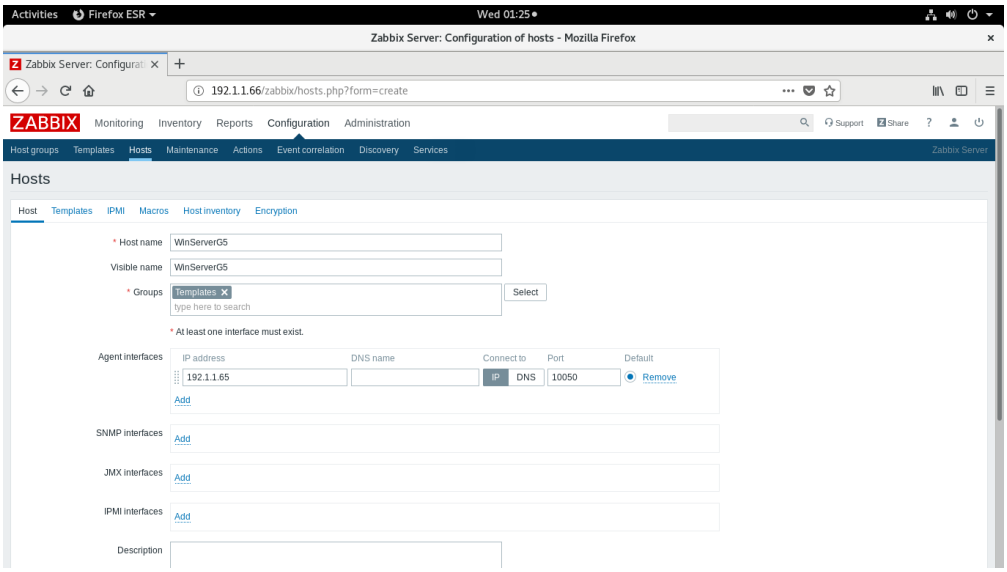


Figure 6-35: Adding new host on Zabbix frontend

Step 6: On template section, add Template OS Windows and click add button.

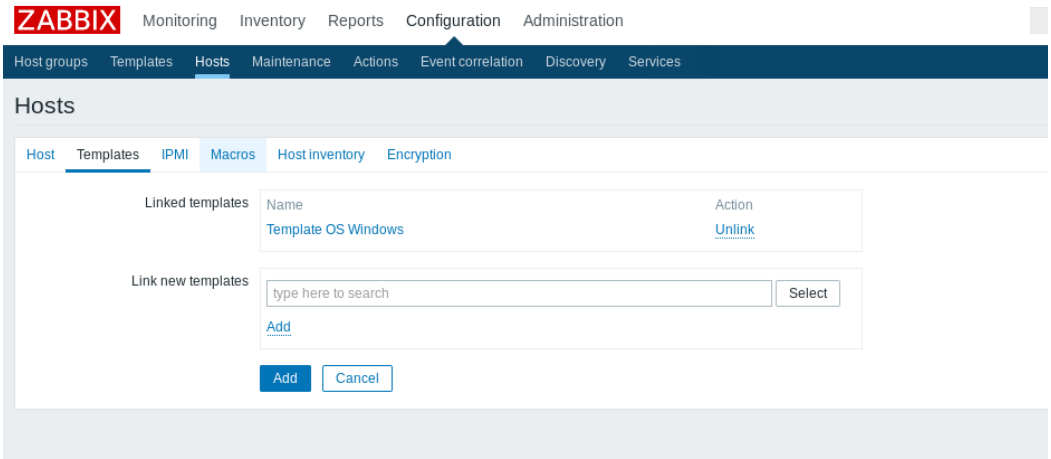


Figure 6-36: Add template

Step 7: Now the Zabbix can monitor the Windows Server. Choose what you want to monitor. The monitoring can be show by graph. Below picture is example for monitoring Windows Server CPU load by graph.

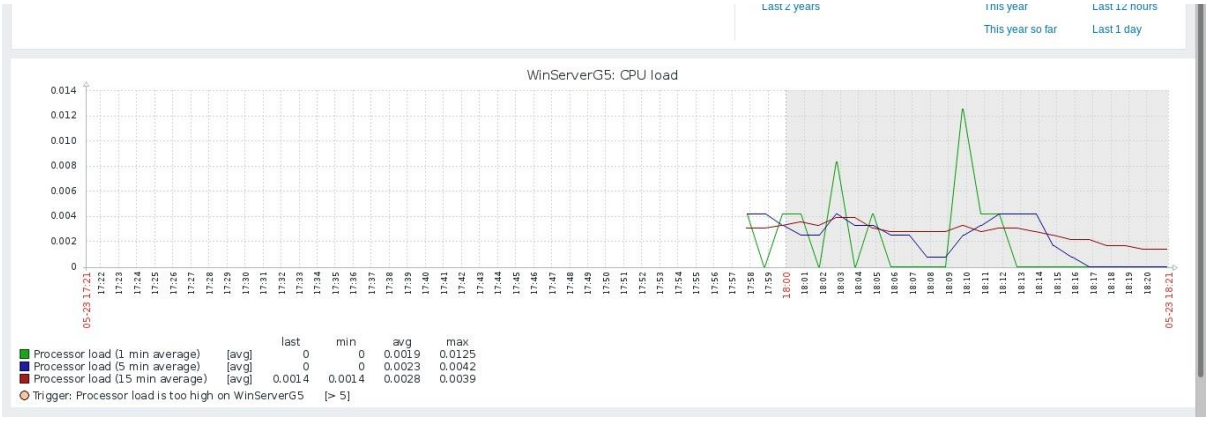


Figure 6-37: Monitor Windows Server CPU load by graph

6.2.10 Web, SSL & Virtual Hosting

Step 1: Click on ***Browse Website.***

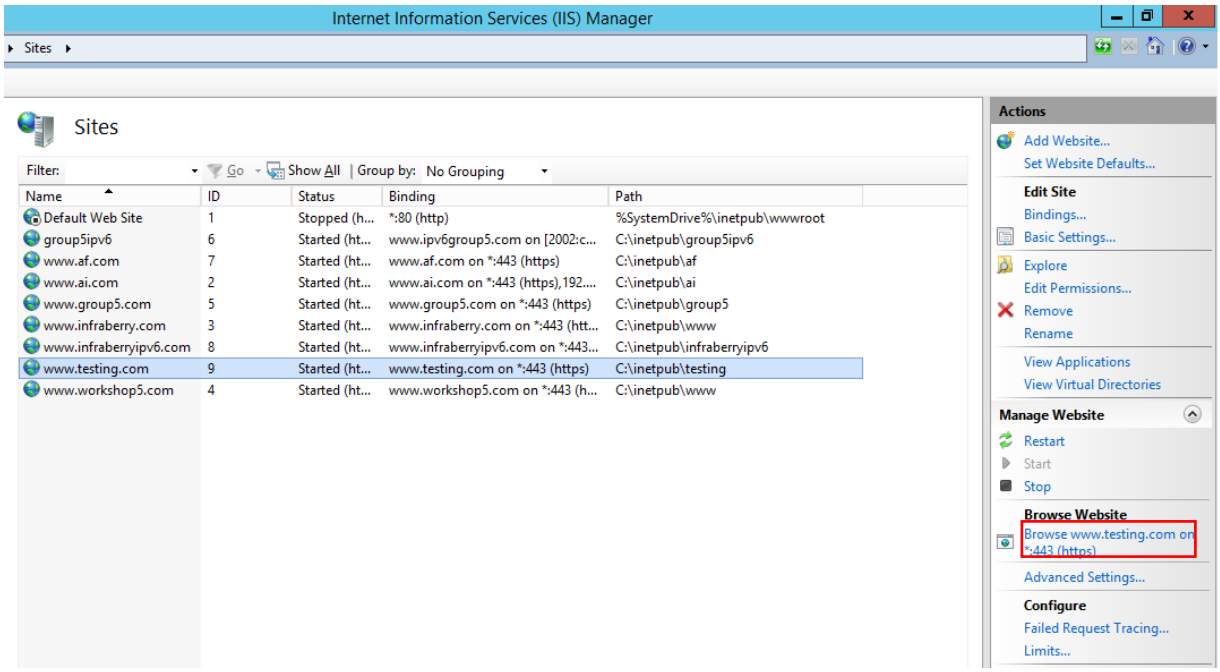


Figure 6-38: Sites

Step 2: Show secure website with certificate

No.	No Matric	Name
1.	B031810084	MUHAMMAD SHOLEHIN BIN RAHMAT
2.	B031810020	MUHAMMAD HELMI AQMAR BIN MAT RAWI
3.	B031810046	AMIRUL AZIM BIN ABDUL RASHID
4.	B031810068	AIMAN FIKRI BIN ASMADI
5.	B031810091	AHMAD FAISAL BIN MD JAMAL

Figure 6-39: Secure Website

Step 3: Show certificate

No.	No Matric	Name
1.	B031810084	MUHAMMAD SHOLEHIN BIN RAHMAT
2.	B031810020	MUHAMMAD HELMI AQMAR BIN MAT RAWI
3.	B031810046	AMIRUL AZIM BIN ABDUL RASHID
4.	B031810068	AIMAN FIKRI BIN ASMADI
5.	B031810091	AHMAD FAISAL BIN MD JAMAL

Figure 6-40: Show certificate

6.2.11 Wireless User Authentication Using Radius Server

Step 1: Check network that are available

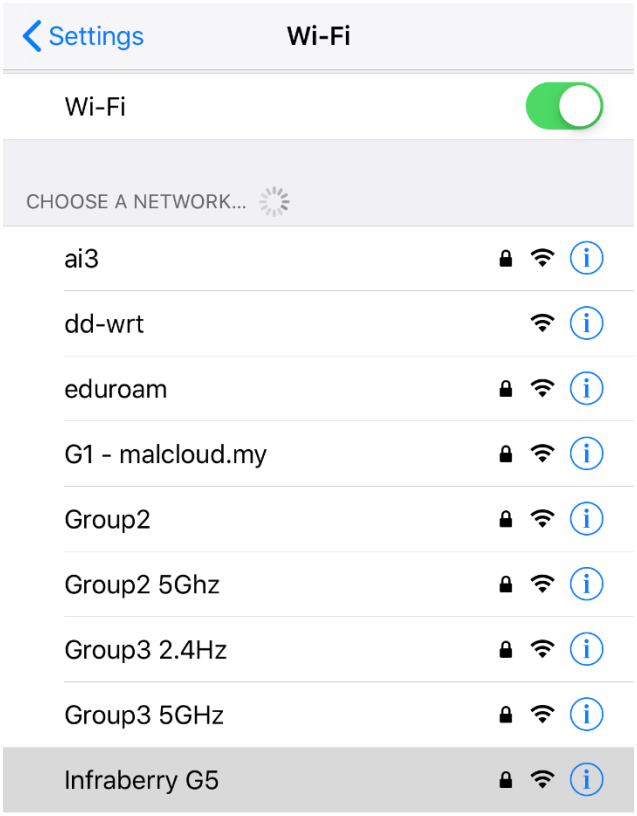


Figure 6-41: Choose a network

Step 2: Key in your username and password that has been create

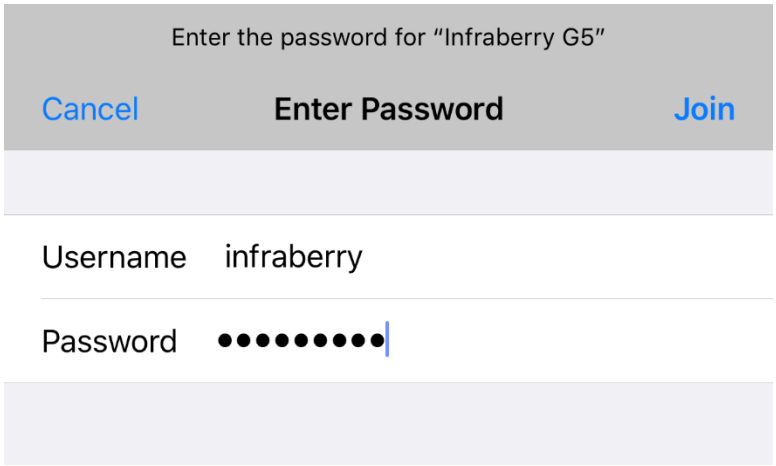


Figure 6-41: Key in username and password

Step 3: Trust the certificate

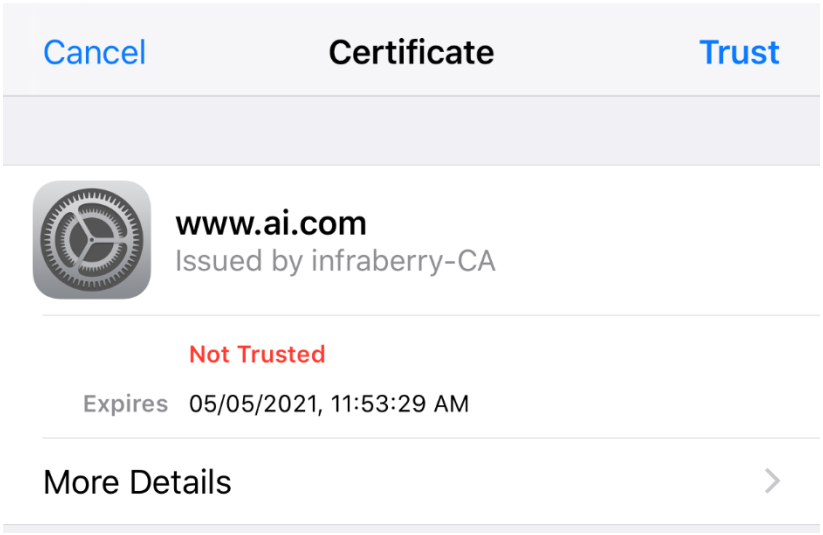


Figure 6-42: Trust the certificate

Step 4: Finally, user can connect to the Wi-Fi.

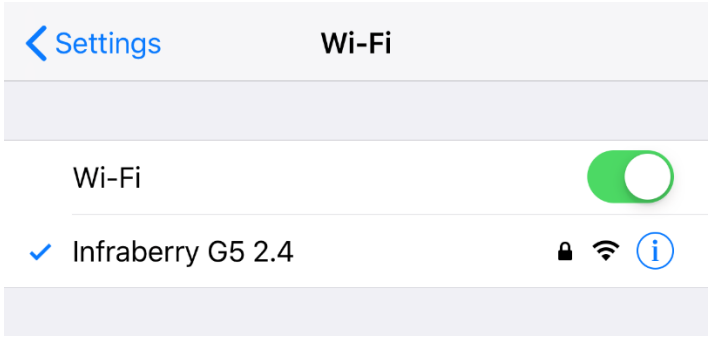


Figure 6-43: Wi-Fi connected

6.2.12 IPsec Site-To-Site Tunneling

Step 1: Show the settings used by IPsec security associations (SAs)

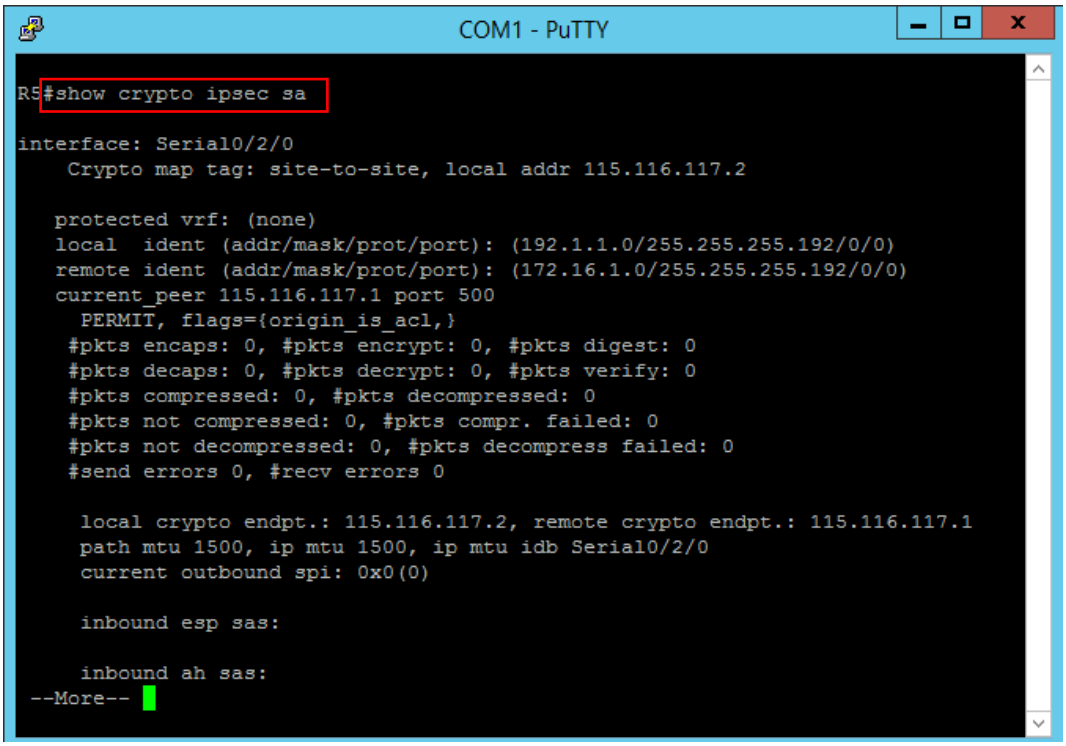


Figure 6-44: Show crypto ipsec sa

Step 2: Show detailed information about the session

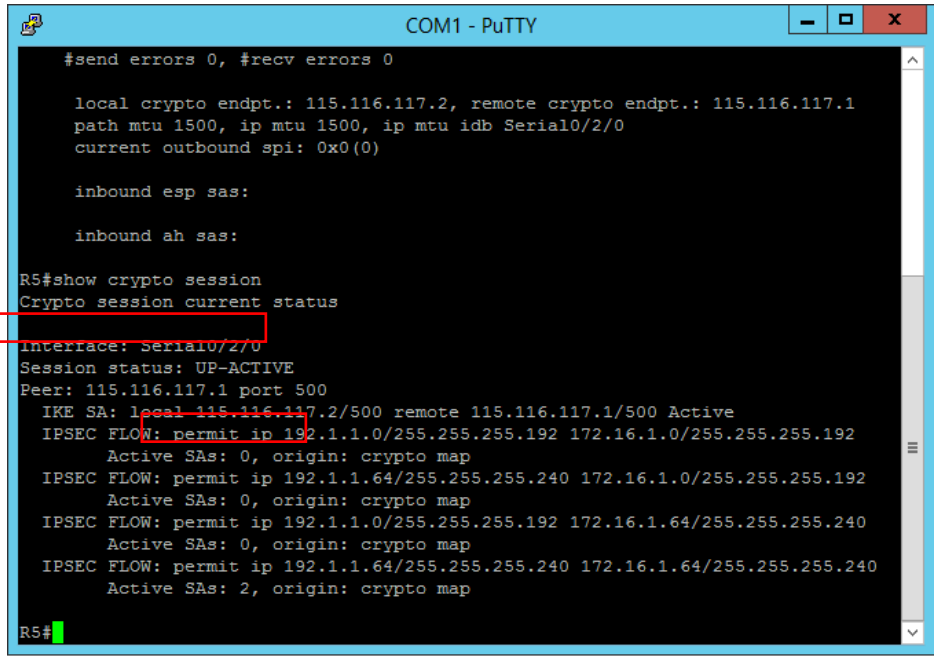


Figure 6-45: Show crypto session

Step 3: Ping to beside group router to our router.

```
R5#ping 172.16.1.78 source 192.1.1.78

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.78, timeout is 2 seconds:
Packet sent with a source address of 192.1.1.78
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms
R5#
```

Figure 6-46: Ping 172.16.1.78 source 192.1.1.78

Step 4: Show that packets has been encrypt.

```
protected vrf: (none)
local  ident (addr/mask/prot/port): (192.1.1.64/255.255.255.240/0/0)
remote ident (addr/mask/prot/port): (172.16.1.0/255.255.255.192/0/0)
current_peer 115.116.117.1 port 500
  PERMIT, flags={origin_is_acl,}
 #pkts encaps: 31, #pkts encrypt: 31, #pkts digest: 31
 #pkts decaps: 40, #pkts decrypt: 40, #pkts verify: 40
 #pkts compressed: 0, #pkts decompressed: 0
 #pkts not compressed: 0, #pkts compr. failed: 0
 #pkts not decompressed: 0, #pkts decompress failed: 0
 #send errors 0, #recv errors 0

  local crypto endpt.: 115.116.117.2, remote crypto endpt.: 115.116.117.1
  path mtu 1500, ip mtu 1500, ip mtu idb Serial0/2/0
  current outbound spi: 0x0(0)

  inbound esp sas:

  inbound ah sas:

  inbound pcp sas:

  outbound esp sas:

  outbound ah sas:

  outbound pcp sas:

protected vrf: (none)
local  ident (addr/mask/prot/port): (192.1.1.0/255.255.255.192/0/0)
remote ident (addr/mask/prot/port): (172.16.1.64/255.255.255.240/0/0)
current_peer 115.116.117.1 port 500
  PERMIT, flags={origin_is_acl,}
 #pkts encaps: 27, #pkts encrypt: 27, #pkts digest: 27
 #pkts decaps: 27, #pkts decrypt: 27, #pkts verify: 27
 #pkts compressed: 0, #pkts decompressed: 0
 #pkts not compressed: 0, #pkts compr. failed: 0
 #pkts not decompressed: 0, #pkts decompress failed: 0
 #send errors 1, #recv errors 0

  local crypto endpt.: 115.116.117.2, remote crypto endpt.: 115.116.117.1
  path mtu 1500, ip mtu 1500, ip mtu idb Serial0/2/0
  current outbound spi: 0x0(0)

  inbound esp sas:

  inbound ah sas:

  inbound pcp sas:

  outbound esp sas:

  outbound ah sas:

  outbound pcp sas:

protected vrf: (none)
local  ident (addr/mask/prot/port): (192.1.1.64/255.255.255.240/0/0)
remote ident (addr/mask/prot/port): (172.16.1.64/255.255.255.240/0/0)
```

Figure 6-47: Show crypto ipsec sa

6.2.13: AAA With Radius

Step 1: log in into putty using serial port and insert username and password

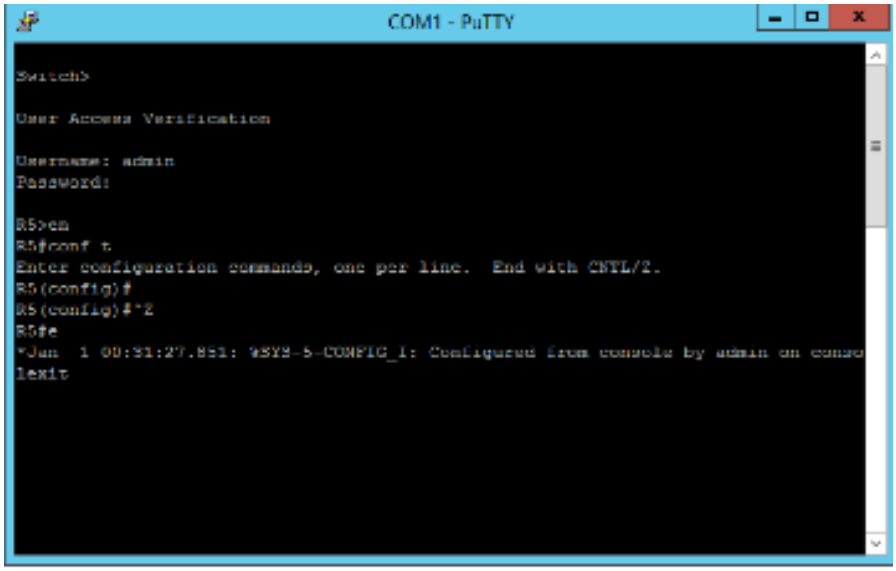


Figure 6.48 :login in putty

Step 2: Login putty using SSH port use ip router

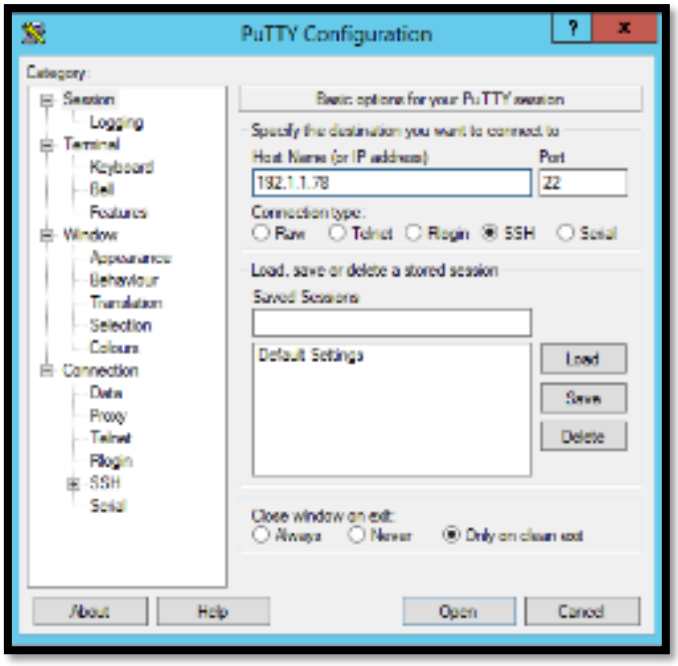


Figure 6.49:login in using SSH

Step 3: Login using username and password

Figure 6.50:login in using SSH

6.2.14: Secure FTP

Step 1: Open third party to transfer file

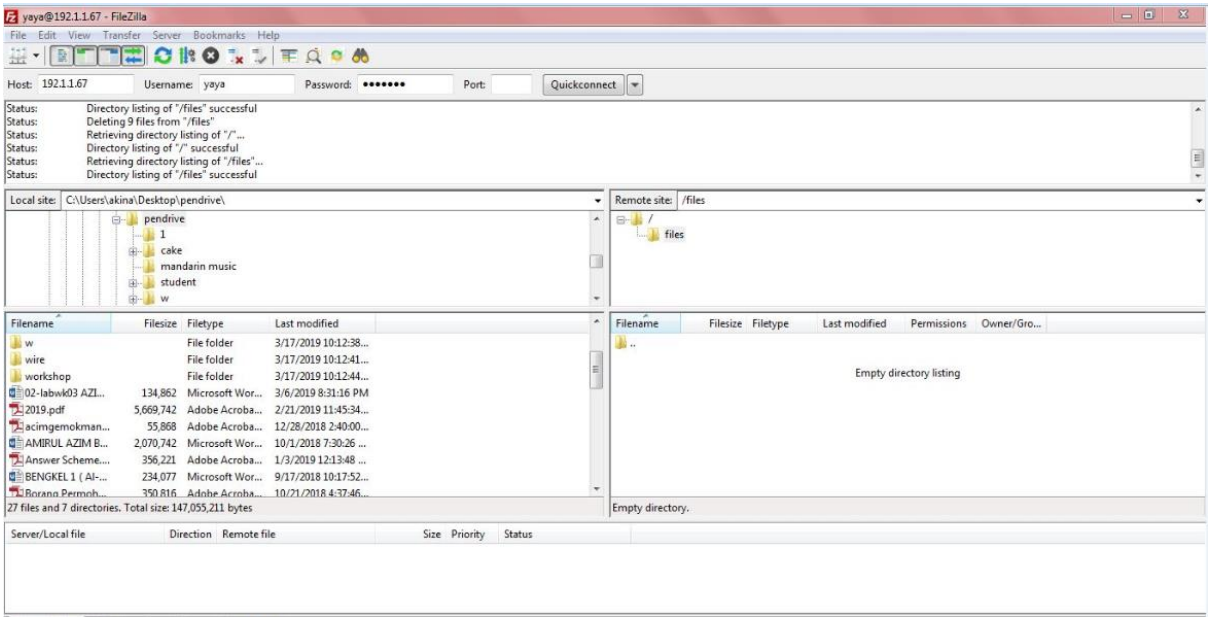


Figure 6.51: Transfer file using FileZilla

Step 2: Proceed with transfer file

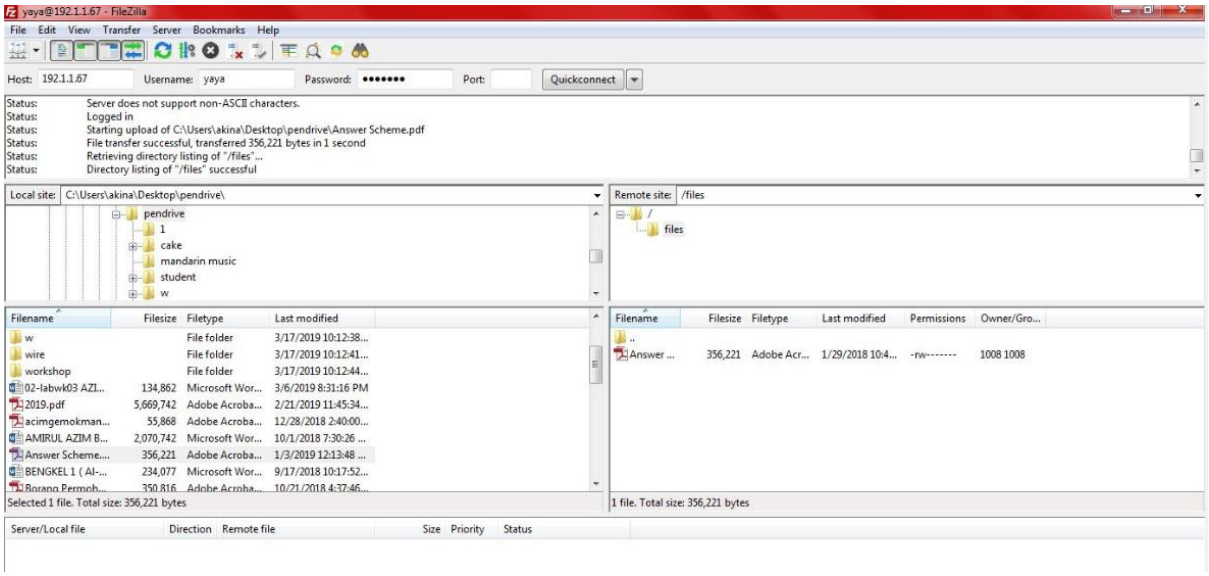


Figure 6.52: Transfer file using FileZilla to server

6.2.15: Access Control List

Step 1: Test the HTTP and HTTPS using browser, it can't be opened the web server.

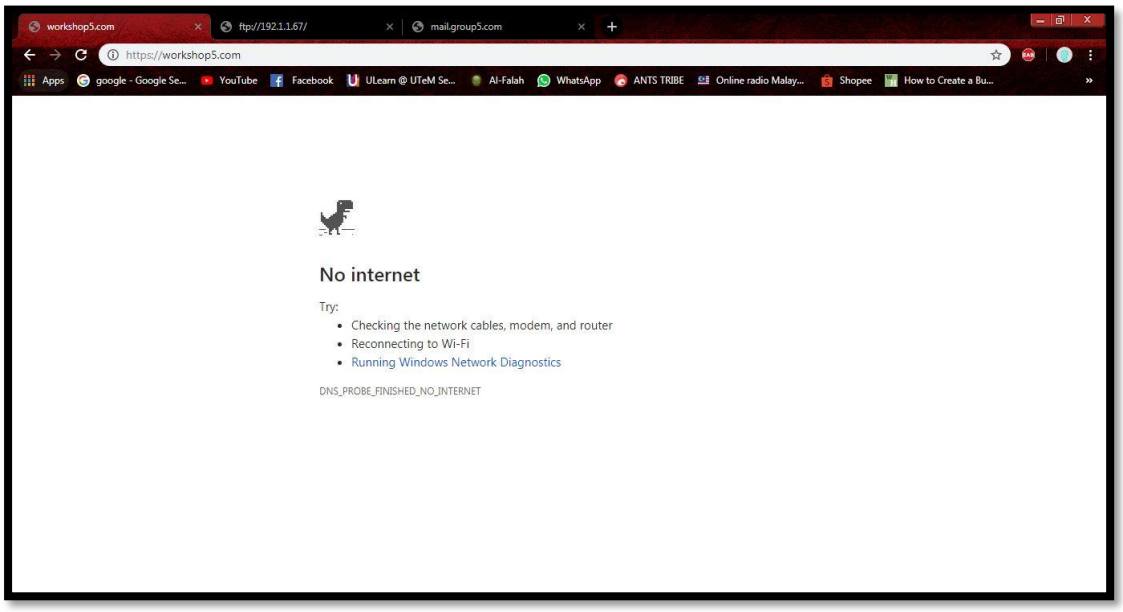


Figure 6.53: HTTP and HTTPS testing

Step 2: Test the FTP using browser, it can't be login into Ubuntu Server

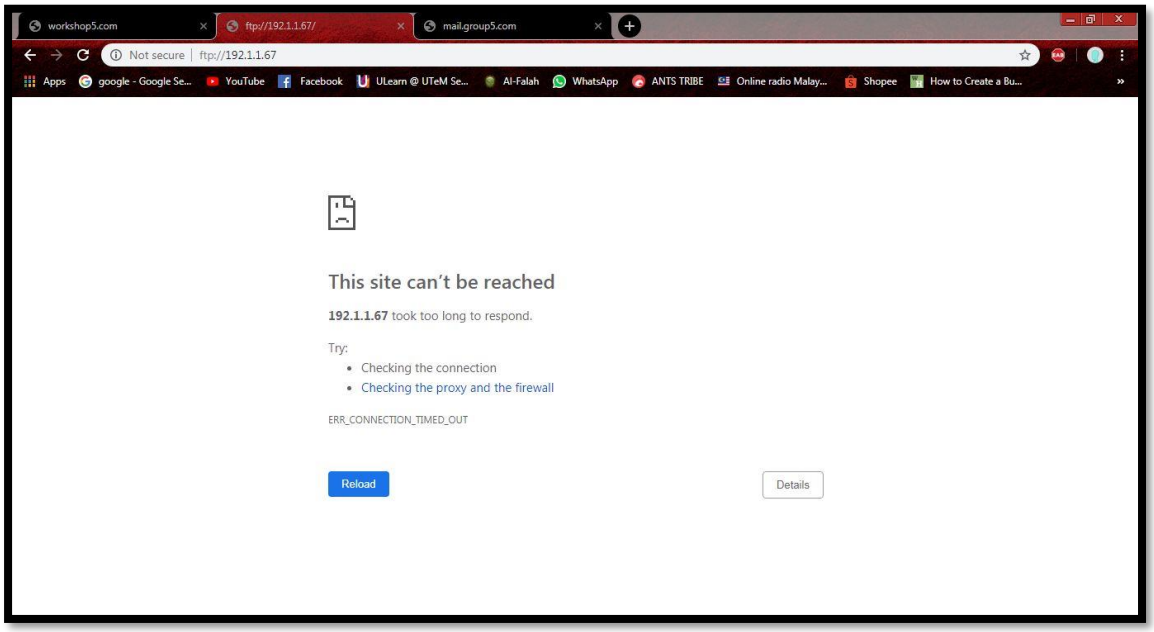


Figure6.54: FTP testing

Step 3: Test the mail server using browser, it can't be access into mail server

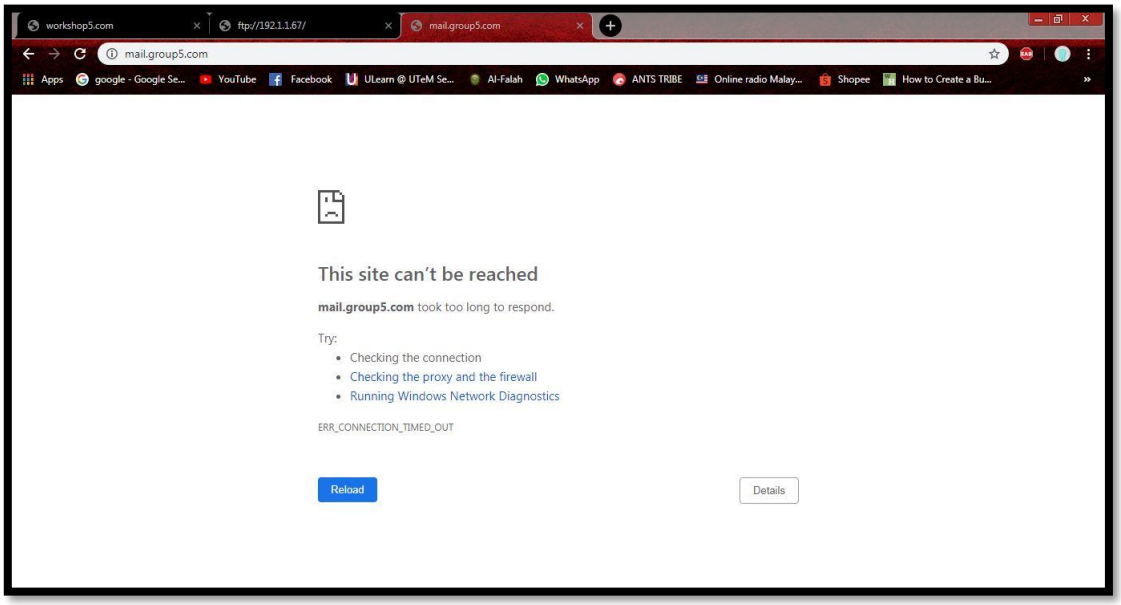


Figure 6.55: mail server testing

CHAPTER 7: CONCLUSION

7.1 Introduction

Through these various weeks, a great deal of things has been concentrated, for example, technique to setup, arrange, keep up, and investigate and the majority of the essential of the administrations in this Workshop 2. The majority of the exercises gained from this Workshop 2 is the prerequisite for industrial training.

To characterize, execute and deal with this Workshop beginning from choosing a pioneer to lead this undertaking from the earliest starting point until the finish of the venture. The general execution of this workshop is adequate. Our gathering has effectively done the majority of the administrations before the due date. Errands have been disseminated similarly to every part and a timetable has been made to deal with its progression. This is significant in overseeing and sorting out each assignment so as to keep the blunder from happening before the due date.

This system is the blend of system and system security. This system is truly reasonable for Small and Medium Enterprise Business since it is anything but difficult to oversee and actualize. In this system, the majority of the essential administrations and security administrations are incorporated to keep up and control the system administrations framework. We are appreciative to increase the majority of the learning and encounters by achieving this undertaking as to set up all of us for the mechanical preparing.

7.2 Project Advantages

There are a lot of advantages to implement this project. The most important of this project is providing an experience during the working environment on computer networking and security. Besides that, this project also provides others advantages which are:

1. To design the network infrastructure for this project.
2. To implement designated network services.
3. To integrate network services infrastructure to suit the network environment.
4. To maintain and control the network services infrastructure.
5. To increase the communication between network student and security student in developing a good network environment.

6. To troubleshoot and overcome any problems during setting up the services.
7. To learn configuration and installation of the services in a server.
8. To build team work between network student and security student in a group.
9. Other important advantages are to experience working in a group and to tolerate between group members and also with different groups to ensure that the network works.

7.3 Project Disadvantages

Even through, this project also gives disadvantages to us to achieve the successful. The project disadvantages which are:

1. We lack of knowledge about some of the services.
2. The servers that were provided were old and caused many problems during the progress of Workshop 2.
3. Some of the network equipment's are not in a good condition, it may not work as well as expected.
4. The lab environment during the night time is very humid because the air condition is turned off and all of the servers are running causing the servers to heat up.

7.4 Project Limitation

There was some project limitation that was caused and we had to adapt and work harder to succeed in this project. These limitations were:

1. The network was only implemented in wired environment.
2. The network was not implemented in larger environment.
3. The equipment that was provided to each group is not in good condition.
4. The network for the projects only involved 3 servers.
5. The wireless technology was not implemented in this project due to the problem in the wireless device.

7.5 Conclusion

As an end from this Workshop 2, there are a great deal of things that have been adapted, for example, setting up, configuring, maintaining and troubleshooting the issue. Workshop 2 gives a ton of experience to experience the system and security condition. Prior to Workshop 2, we have just learned and knew the hypothesis part, however after Workshop 2 we picked up a great deal of information and saw increasingly about the system.

In Workshop 2, we were required to install and configuring 15 computer networking services. At long last, we have taken in and comprehended the administrations from our supervisor. We are extremely thankful and we value supervisor for guiding us to an effective workshop finish.

BIBILIOGRAPHY

REFERENCE

Book

i. Windows Server 2012:
- William R. Stanek (2013). Windows Server 2012 Inside Out, Microsoft Press; 1 edition.
- Mitch Tulloch (2012). Introducing Windows Server 2012, Microsoft Press.
- Nick Rushton (2014). Windows Server 2012 R2 Essentials Installation Guide Small Businesses, CTACS; 10 edition.

ii. Linux Ubuntu 14.04 :
- Jan Just Keijser (2011). OpenVPN 2 Cookbook. Packt Publishing Ltd.
- Carl Taylor, Alistair McDonald (2005). Linux Email: Setup and Run a Small Office Email Server Using Postfix, Courier, Procmail, Squirrelmail, Clamav and Spamassassin. Packt Publishing.
- Barth, Wolfgang; (2008) Nagios: System And Network Monitoring, 2nd edition.

Web link

i. Linux Ubuntu 14.04

- Linode (March 24th, 2014) Troubleshooting Problems with Postfix, Dovecot, and MySQL from https://www.linode.com/docs/email/postfix/troubleshootingproblems with-postfix-dovecot-and-mysql#dovecot.
- Web Mail System from http://www.server-world.info/en/note?os=Ubuntu_14.04&p=mail&f=1
- Ubuntu 14.04 – Install / Configure Postfix from https://www.linux.com/learn/tutorials/308917-install-and-configure- a-postfix-mail-server

ii. Network

- Interface and Hardware Component Configuration Guide, Cisco IOS XE Release 3S. Retrieved from http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/configuration/xe-3s/ir-xe-3s-book/ip6-man-tunls- xe.html
- Cisco IOS IPv6 Configuration Guide (2009, March 5th). Retrieved from http://www.cisco.com/c/en/us/td/docs/ios/ipv6/configuration/guide/12_4t/ipv6_12_4t_book/ip6-tunnel.html
- Cisco IOS Security Configuration Guide (2006). Retrieved from http://www.cisco.com/c/en/us/td/docs/ios/12_2/security/configuration/guide/fsecur_c/scfids.html

APPENDEIX

VLSM Adressing and IP Table

Network	Broadcast	Subnet Mask	VLAN
192.1.1.64	192.1.1.79	255.255.255.240	20
192.1.1.0	192.1.1.63	255.255.255.192	40
192.1.2.0	192.1.2.63	255.255.255.192	60
125.126.127.0	125.126.127.7	255.255.255.248	-
125.126.127.8	125.126.127.15	255.255.255.248	-

Device	Interface	IP Address	Subnet Mask	Default Gateway	VLAN
R5	Se0/0	125.126.127.1	255.255.255.248	-	-
	Fa0/0	125.126.127.14	255.255.255.248	-	-
	Tun0	2340:1212:ABCD:3::1	/64	-	-
	Fa0/1.20	192.1.1.78	255.255.255.240	-	20
		2340:1212:ABCD:1::FFFE	/64	-	20
	Fa0/1.40	192.1.1.62	255.255.255.192	-	40
		2340:1212:ABCD:2::FFFE	/64	-	40
SW	Vlan20	192.1.1.77	255.255.255.240	-	20
		2340:1212:ABCD:1:FFFD	/64	-	
WINDSRVR	Eth0	192.1.1.65	255.255.255.240	192.1.1.78	20
		2340:1212:ABCD:1::1	/64	2340:1212:ABCD:1::FFFE	
DEBIAN	Eth0	192.1.1.66	255.255.255.240	192.1.1.78	20
		2340:1212:ABCD:1::2	/64	2340:1212:ABCD:1::FFFE	
UBUNTU	Eth0	192.1.1.67	255.255.255.240	192.1.1.78	20
		2340:1212:ABCD:1::3	/64	2340:1212:ABCD:1::FFFE	
WAP	Eth0	192.1.1.1	255.255.255.192		40
		2340:1212:ABCD:2::1	/64		
CLNT1	Eth0	DHCP	255.255.255.192	192.1.178	40
CLNT2	Eth0	125.126.127.9	255.255.255.248	123.124.125.14	

Activity / week	1	2	3	4	5	6	7	8	9	10	11	12	13	14	Study Week
Project Proposal															
Progress Report 1															
Progress Report 2															
Progress Report 3															
Final Report															
Log Book															
Video & Poster Exhibition															
Final Report & Log Book Submission															