FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY

SEMESTER 2 2018/2019

BITU3923 - WORKSHOP II

BITC

FINAL REPORT: DOMAIN NAME SYSTEM (DNS)

GROUP NUMBER: 3

PREPARED BY:

NAME	MATRIC NO
HONG MIN KE	B031710043
SATTISH KUMARAN A/L TAYVANTRIAN	B031810086
MOHD RIDZUAN BIN MOHD AMIN	B031710052
MOHAMAD FIQHREEL EIZIQ BIN ISMAIL	B031710064
MUHAMMAD FARID ZAKWAN BIN SYAFRISAL	B031810084

PREPARED FOR: DR. NAZRULAZHAR BIN BAHAMAN

ACKNOWLEDGEMENTS

First and foremost, we would like to thank our supervisor of this project, Dr. NAZRULAZHAR BIN BAHAMAN for his valuable guidance and advice. He inspired us greatly to work in this project.His willingness to motivate us contributed tremendously to our project. We also would like to thank our seniors for showing us some examples that are related to the services in our project which helped us a lot to understand our project. This helped us to complete our project on time. We would also like to thank our evaluator for this workshop, TS ARIFF BIN IDRIS for taking the time to evaluate us. This evaluation gave us deeper understanding of our services and network infrastructure.

Besides, we would like to thank the authority of Universiti Teknikal Malaysia Melaka (UTeM) for providing us with 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 Server R2 in server 1 (Window), Ubuntu in server 2 and Debian in server 3. We choose this server operating system because it has many benefits. Our group also was assigned to set up 15 services listed. The 15 services listed are File Transfer Protocol (FTP), Authentication, Authorization and Accounting, Access Control List, Web SSL, Virtual Hosting, Linux email server, IPv6 Web and IPv6 Tunneling, Network Translation Address, Proxy Server, Network Management System, Domain Name System, Dynamic Host Configuration Protocol, Active Directory and Wireless User Authentication.

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, kita perlu menentukan, melaksanakan dan mengurus tugas-tugas yang bermula dari memilih pemimpin untuk memimpin projek ini dari awal hingga akhir projek ini sehingga dapat membina satu infrastuktur rangkain. Beberapa tugas telah diberikan kepada setiap ahli dan kami membuat jadual tugas untuk menyelesaikannya tepat pada waktu. Adalah sangat penting untuk mengurus dan melaksanakan setiap tugas untuk mengelakkan sebarang masalah dan kesilapan di penhujung projek..

Objektif utama kami dalam Bengkel II ini adalah untuk, berjaya dan dapat mengatasi halangan dan cabaran yang dihadapi ketika menyelesaikan tugas yang diberikan. Kami bersyukur kerana dapat diberi peluang untuk mengikuti Bengkel II ini kerana ia membantu kami menjadi lebih bersedia dalam latihan perindustrian kami.

Kumpulan kami telah memutuskan untuk menggunakan Windows Server R2 di pelayan 1 (Tetingkap), Ubuntu di pelayan 2 dan Debian dalam pelayan 3. Kami memilih sistem operasi pelayan ini kerana ia mempunyai banyak kegunaan. Kumpulan kami juga ditugaskan untuk menubuhkan 15 perkhidmatan yang disenaraikan. 15 perkhidmatan yang disenaraikan adalah Protokol Pemindahan Fail (FTP), Pengesahan, Kebenaran dan Perakaunan, Senarai Kawalan Akses, SSL Web, Hosting Virtual, pelayan e-mel Linux, IPv6 Web dan IPv6 Tunneling, Alamat Perangkaian Rangkaian, Server Proksi, Sistem Pengurusan Rangkaian, Domain Sistem Nama, Protokol Konfigurasi Hos Dinamik, Direktori Aktif dan Pengesahan Pengguna Tanpa Wayar.

Semasa Workshop II, kami menghadapi beberapa masalah tetapi masih dapat mengatasinya dan membuat projek ini berjaya.

TABLE OF CONTENT

TABLE OF FIGURES

CHAPTER 1: INTRODUCTION

1.1 Introduction

This company is expanding their department with approximately 100 current employees and 30 employees for the future. It will be divided into two departments which is IT department and HQ department; the server room will be the main sector where the main server is located with the other server. This main server is used to store the database of the employees and the client. The HQ department is connected with a simple point-to-point tunnels that can be used to carry IPv6 packets between the main department and other department. We have to setup the infrastructure for this company that covers all networking functions for internal and external IT communications, user management, port management, remote access to the network for telecommuters, network monitoring and a basic network security also applied in this project.

Other than that, the company also wants to provide several services for their employees, such as email, web services and file transfer service and much more. There are fifteen services that must be up and running to make sure the entire networking infrastructure working properly. Before we precede the installation, we have to develop a proper network design that includes physical and logical design. For the server operating system, we used the Window Server 2012, Ubuntu and Debian Operating System as a platform for our network implementation.

There are fifteen services that need to be install and configure such as, File Transfer Protocol (FTP), Authentication, Authorization and Accounting, Access Control List, Web SSL, Virtual Hosting, Linux email server, IPv6 Web and IPv6 Tunneling, Network Translation Address, Proxy Server, Network Management System, Domain Name System, Dynamic Host Configuration Protocol, Active Directory and Wireless User Authentication. Every group member is assigned with their own services.

1.2 Objective

The main objective of this project is to install a network service into a different operating system server that connected via LAN and WAN connection and also to develop an understanding of networking infrastructure, problem solving techniques and concept of network design. Other than that is to solve a particular problem of fifteen services in this network. Below is the list of objective that uses to develop this project.

1. To design a secure network infrastructure by using the given tools.
2. To provide a network access for every department.
3. To successfully provide a multiple network service into several servers which contains a different operating system.

1.3 Project Planning / Schedule

In week 1 and week 2, we will be assigned to the respective supervisor. After, we assigned in week 2 we gather together to divide our service tasks for every group members. After divided the tasks, we will start to do the proposal for our project to get approval from the supervisor. The proposal includes the details of the project like introduction, logical and physical network design to show the network topology, Gantt chart to show the project progress. We will submit the finalized proposal by the end of week 2 for approval. Then we will go to the lab to get the lab to collect the devices which needed for this project such as wireless router, switch and servers. Starting from week 3 to week 5 we will proceed to set up the services needed for this project. There are 8 services that we plan to install during this period. We will prepare the Progress Report 1 that will consist of the details of the setup and installation of the services. Then, we will submit the finalized Progress Report 1 that has been approved by the supervisor in end of week 5. From week 6 to week 10, we plan to proceed to set up the 10 other services. We will prepare the Progress Report 2 that will be consists of the setup details of the 10 services. Then, we will submit the finalized Progress Report 2 that has been approved by the supervisor in end of week 10. From week 11 to week 12, we will plan to complete the setup of the whole network and setup of all services required. At the same time, we will 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. Finally, the completed final report and individual log book will be submitted during study week (week 15).

Gantt chart

This Gantt chart were shown the whole task until week 15, for the first week we do project proposal that taking 2 weeks period, after that we taking 4 week on progress 1, 5 week for progress 2 and 3 week for the progress 3. Video and poster submission only take 1 week period to prepare and establish, same goes to exhibition and final report submission. All the data were shown on the table below.

	Week 1	Week 2	Week 3	Week 4	Week 5	Week 6	Week 7	Week 8	Week 9	Week 10	Week 11	Week 12	Week 13	Week 14	Week 15
Project Proposal															
Progress 1															
Progress 2															
Progress 3															
Video &Poster Submission															
Workshop 2 Exhibition															
Final Report & Peer Assesment report & Log Book Submission															

1.4 Conclusion

For the conclusion, we are able to apply knowledge and experience from the previous subject that we have learnt such as Computer Organization, Operating System, Local Area Network, Network Analysis and Design, Wide Area Network and Network Project Management into this project. We have practice the theory of the entire subject to solve the problem that we have been encountered during the development of this project. With every information security's role, protocols, architectures and technologies, systems and services can be secured. We should understand how security policies, standards and practice are developed. This course also is designed to cater all student knowledge needs from elementary networking concepts to intermediate network monitoring and security techniques.

Furthermore, we also can design the network infrastructure so that we can maintain and good network environment. Apart from that, we should recognize the need for contingency planning, able to describe the major component of contingency planning. Improving computer and networking security is a continuing process. This process requires close collaboration from all in order to form network design with secured connection and centralized protection.

CHAPTER 2: PROJECT REQUIREMENT

2.1 Introduction

The network to be developed will consist of three servers with combination of different platforms. This network will be used Windows Server 2012 R2, Ubuntu and Debian9. Besides, we need to apply 15 services and it will be divided among the three servers. It is very important to ensure the network system operate at the desired performance and the technologies used will be the best possible.

2.2 Types of Operating System Used in the Project

An operating system is used to manage the computer's memory, processes, software and hardware. In order to let the user able to gain a good experience when they are operating the computer, a high-quality operating system is needed to integrate network services infrastructure to suit the network environment. The operating systems uses in the project are:

1. Window Server 2012 R2
2. Ubuntu
3. Debian 9

2.3 Operating System Background

2.3.1 Windows Server 2012 R2

Windows Server 2012 is an operating system built by Microsoft and is the successor of Windows Server 2008 R2. Windows Server 2012 is the server-edition of Windows 8 and is available since September 2012. Its minor update (Windows Server 2012 R2) is available since October 2013. Various features were added or improved over Windows Server 2008 R2 such as an updated version of Hyper-V, an IP address management role, a new version of Windows Task Manager, and ReFS, a new file system.

Windows Server 2012 received generally good reviews in spite of having included the same controversial Metro-based user interface seen in Windows 8, which includes the "Charms Bar" for quick access to settings in the desktop environment.

2.3.2 Ubuntu

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.

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.

2.4 Operating System Justification

2.4.1 Windows Server 2012 R2

Windows Server 2012 is an operating system built by Microsoft and is the successor of Windows Server 2008 R2. Windows Server 2012 is the server-edition of Windows 8 and is available since September 2012. Its minor update (Windows Server 2012 R2) is available since October 2013. Various features were added or improved over Windows Server 2008 R2 such as an updated version of Hyper-V, an IP address management role, a new version of Windows Task Manager, and ReFS, a new file system.

2.4.2 Ubuntu 16.04

Ubuntu is a free and open-source Linux distribution based on Debian. 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".

2.4.3 Debian 9

Debian has access to online repositories that contain over 51,000 packages. Debian officially contains only free software, but non-free software can be downloaded and installed from the Debian repositories. Debian includes popular free programs such as LibreOffice, Firefox web browser, Evolution mail, K3b disc burner, VLC media player, GIMP image editor, and Evince document viewer. Debian is a popular choice for servers, for example as the operating system component of a LAMP stack.

2.5 Hardware Requirement

2.5.1 Windows Server 2012 R2

Windows Server 2012 R2 requires a 64-bit processor; Microsoft has discontinued 32-bit software with this release of Windows Server. Table 2-2 outlines the minimum and recommended hardware requirements for Windows Server 2012 R2 as provided by Microsoft:

Processor	1.4 GHz, x64
Memory	512 MB
Free disk space	32 GB (more if there is at least 16 GB of RAM)

2.5.2 Ubuntu

The Recommended Minimum System Requirements, here, should allow even someone fairly new to installing Ubuntu or Gnu & Linux to easily install a usable system with enough room to be comfortable. A good "rule of thumb" is that machines that could run XP, Vista, Windows 7 or x86 OS X will almost always be a lot faster with Ubuntu even if they are lower-spec than described below.

Processor	2 GHz dual core processor
Memory	2 GB RAM (system memory)
Free disk space	25 GB of hard-drive space

2.5.3 Debian 9

Following are the minimum system requirements for Debian 9 Installation

Processor	1GHz Pentium 4 processor
Memory	512 MB RAM
Free disk space	10 GB HDD

2.6 Hardware Justification

2.6.1 Servers

There are three desktop given. One of the servers will be installed with Windows Server 2012 R2 and the rest will be installed with Ubuntu and Debian 9. There are services to be installed into each server.

- Windows server r2
    1. Server Virtualization
    2. Domain Name System (DNS)
    3. The Dynamic Host Configuration Protocol (DHCP)
    4. Active Directory
    5. Web, SSL, Virtual Hosting
    6. Ipv6 Web and tunneling
    7. Wireless user authentication
- Ubuntu
    1. Proxy Server
    2. Network Management System
    3. Secure File transfer protocol
- Debian 9

    1. Linux Email Server

2.6.2 NIC (Network Interface Card)

A network interface card (NIC) is a hardware component, typically a circuit board or chip, which is installed on a computer so that it can connect to a network. Modern NICs provide functionality to computers such as support for I/O interrupt, direct memory access (DMA) interfaces, data transmission, network traffic engineering and partitioning.

2.6.3 UTP (Unshielded Twisted Pair) Cable

This project using about 15 meters long UTP cable. UTP cable is a 100ohm copper cable that consists of 2 to 1800 unshielded twisted pairs surrounded by an outer jacket. They have no metallic shield. This makes the cable small in diameter but unprotected against electrical interference. The twist helps to improve its immunity to electrical noise and EMI.

2.6.4 RJ-45 (Registered Jack-45) Connector

RJ45 is a type of connector, mainly used for Ethernet networking including connection with PC network cards, data switches, Wi-Fi access points, and routers. It is connected to each end of Ethernet cables and acts as the main source for transferring data. RJ stands for registered jack and ethernet cables are also known as RJ cables. The most common standard for RJ cables is known as CAT5 (Category 5). RJ connector comes with eight pins which indicate it can house eight wires inside. All these wires come in different colors i.e. four are in solid color while the remaining four are stripped. These wires are combined in twisted pairs that help in reducing the crosstalk and cancelling EMI.

2.6.5 Switch

A network switch is a computer networking device that connects devices on a computer network by using packet switching to receive, process, and forward data to the destination device. A network switch is a multiport network bridge that uses hardware addresses to process and forward data at the data link layer (layer 2) of the OSI model. Some switches can also process data at the network layer (layer 3) by additionally incorporating routing functionality. Such switches are commonly known as layer-3 switches or multilayer switches.

A switch is a device in a computer network that connects other devices together. Multiple data cables are plugged into a switch to enable communication between different networked devices. Switches manage the flow of data across a network by transmitting a received network packet only to the one or more devices for which the packet is intended.

2.6.6 Router

A router is a networking device that forwards data packets between computer networks. Routers perform the traffic directing functions on the Internet. Data sent through the internet, such as a web page or email, is in the form of data packets. A packet is typically forwarded from one router to another router through the networks that constitute an internetwork (e.g. the Internet) until it reaches its destination node. A router is connected to two or more data lines from different networks. When a data packet comes in on one of the lines, the router reads the network address information in the packet to determine the ultimate destination. Then, using information in its routing table or routing policy, it directs the packet to the next network on its journey. In this workshop II, we implement Routing and NAT, ACL,AAA and IPsec on this router.

2.7 Conclusion

In conclusion, with all the requirements for hardware and software for workshop II. We can continue the next process for our project. We do the research immediately about the hardware given and the operating system that we chose. The network can be up with the completeness of the requirements and the tools we have.

3.0 CHAPTER 3: DESIGN

3.1 Introduction

In this workshop II, we have to define, design, implement and manage the network services. Each group in Workshop II should be implementing their own network design. According to the requirements of Workshop II, we need to set up a LAN (Local Area Network) which consists of three servers, one router, on switch and one client based on network design that we did. As mentioned before, our group set up a network with three servers (1 Windows Server 2012 R2, 1 Linux Ubuntu 16.9 (Desktop Version) and 1 Debian 8 (Desktop Version)), one VM VirtualBox Machine (Windows Server 2012 R2), one Router Cisco 2800, one Switch Cisco Catalyst 2960, one AP (Access Point).

3.2 Physical Design

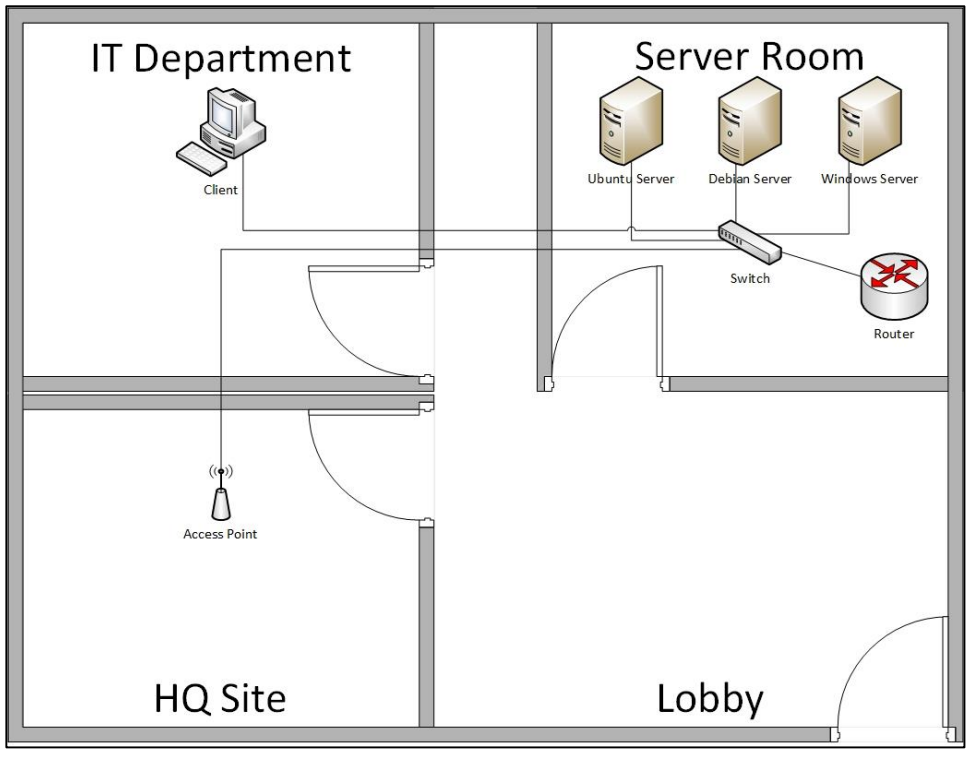


Figure 3.2 1 Physical Design

3.3 Logical Design

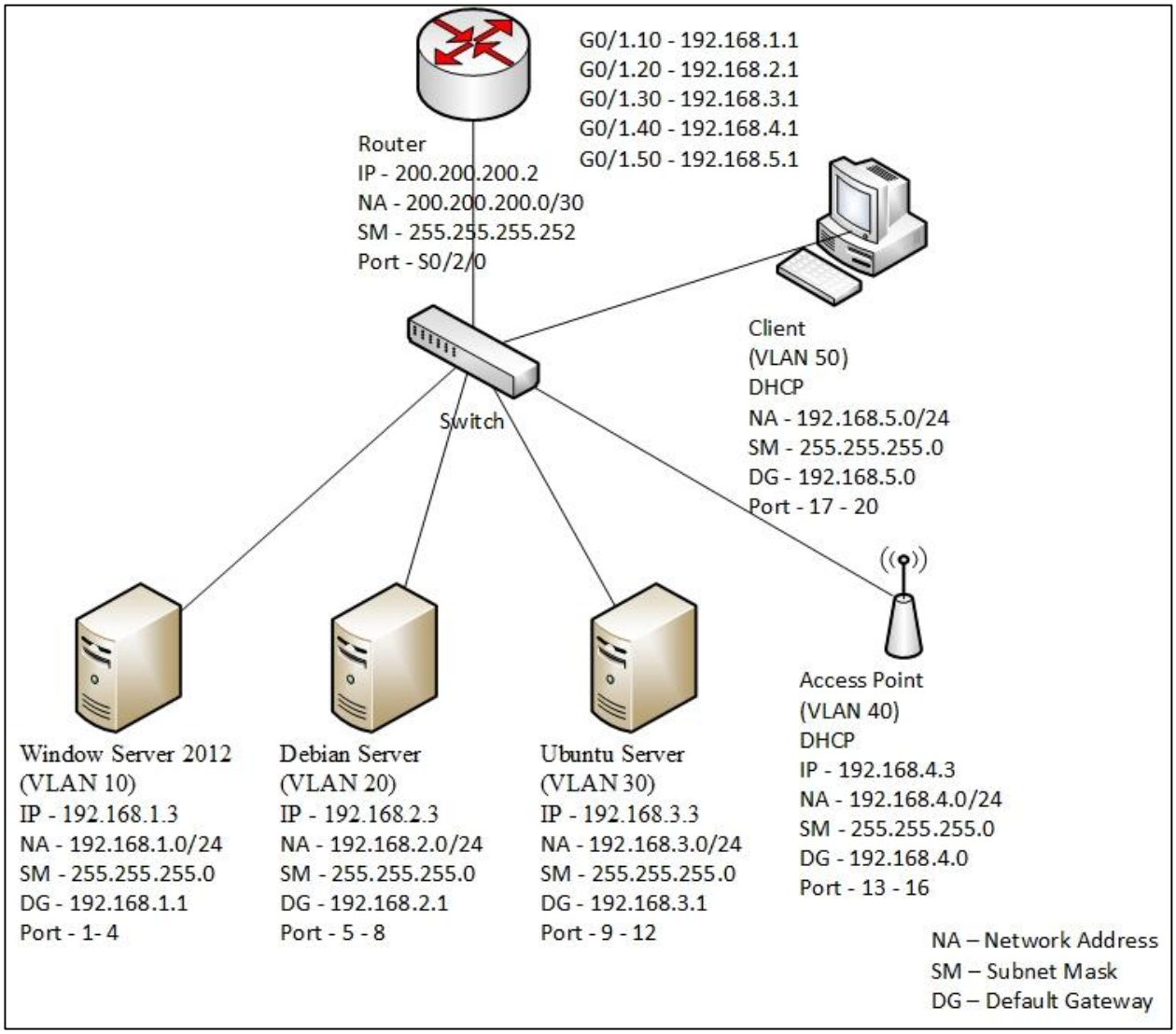


Figure 3.3 1 Logical Design

3.4 Conclusion

Network designing is an important part while creating a network. Without network design, there is no idea on how to begin the implementation of the network. There are few main factors that need to be considered while implementing network design that include, the planning of network complexity must be in line with the network administrator, redundancy, standards and maintenances factor. All of those factors are need to ensure the network can be implementing, expandable for future implementation and easy to maintain.

After considering on those factors, we had implemented network as designed physically and go through to the next level of implementing that is planning the implementation of network services.

4.0 CHAPTER 4: SERVICES

4.1 Introduction

In this chapter, we will provide a list of services that we are going to implement. We will briefly explain the overview for each service.

4.2 List of Services

Service for Networking

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

4.3 Brief Overview for Services

4.3.1 DNS

DNS known as Domain Names Server it's maintain a directory of domain names and translate them to Internet Protocol (IP) addresses. This is necessary because, although domain names are easy for people to remember, computers or machines, access websites based on IP addresses.

4.3.2 DHCP

DHCP stands for dynamic host configuration protocol and is a network protocol used on IP networks where a DHCP server automatically assigns an IP address and other information to each host on the network so they can communicate efficiently with other endpoints.

4.3.3 Wireless user authentication

Remote Authentication Dial-In User Service, an authentication and accounting system used by many Internet Service Providers (ISPs). Username and password information's will send to the RADIUS server which if the information is correct then authorize will send to the ISP.

4.3.4 Routing & NAT

Routing refers to establishing the routes that data packets take on their way to a particular destination and Network Address Translation (NAT) is the process where are a network device, usually a firewall, assigns a public address to a computer (or group of computers) inside a private network. The main use of NAT is to limit the number of public IP addresses an organization or company must use, for both economy and security purposes.

4.3.5 Active Directory

Active Directory (AD) is a Microsoft technology used to manage computers and other devices on a network. It is a primary feature of Windows Server, an operating system that runs both local and Internet-based servers. Active Directory allows network administrators to create and manage domains, users, and objects within a network.

4.3.6 Proxy Server

Proxy server is a computer that sits between a client computer and the Internet, and provide indirect network services to a client. It may reside on the user's local computer, or at various points between the user's computer and destination server on the Internet. All the information sent from that browser or app goes out via your ISP (internet service provider) then via the proxy server to the website or other server you want to access.

4.3.7 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. 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.

4.3.8 Network Management System

A network management system (NMS) is an application or set of applications that lets network engineers manage a network's independent components inside a bigger network management framework and performs several key functions. NMS may be used to monitor both software and hardware components in a network. It usually records data from a network's remote points to carry out central reporting to a system administrator.

4.3.9 Server Virtualization

Server virtualization is the process of using software on a physical server to create multiple partitions or virtual instances which consolidates multiple operating systems (OS) on a single server. Each virtual server runs multiple operating system instances at the same time. Server virtualization makes each virtual server look and act like a physical server, multiplying the capacity of every single physical machine.

4.3.10 Authentication, authorization, and accounting (AAA)

Authentication, authorization, and accounting (AAA) is a term for a framework for intelligently controlling access to computer resources, enforcing policies, auditing usage, and providing the information necessary to bill for services. System administrators monitor and add or delete authorized users from the system. Authorization refers to the process of adding or denying individual user access to a computer network and its resource. Accounting refers to the record-keeping and tracking of user activities on a computer network.

4.3.11 Access Control List (ACL)

An access control list (ACL) is a table that tells a computer operating system which access rights each user has to a particular system object, such as a file directory or individual file. ACLs provide a powerful way to control traffic into and go out of your network, this control can be as simple as permitting or denying network hosts or addresses.

4.3.12 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. 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.

4.3.13 Web, SSL & Virtual Hosting

Virtual hosting generally allows multiple IT appliances, such as websites and applications, to share a single Web server. SSL (Secure Sockets Layer) is the standard security technology for establishing an encrypted link between a web server and a browser. This link ensures that all data passed between the web server and browsers remain private and integral.

4.3.14 Linux Email Server

A mail server is an application that receives incoming e-mail from local users which people within the same domain and remote senders and forwards outgoing e-mail for delivery. The Linux mail server and SMTP protocol work together for send and receive emails.

4.3.15 IPv6 Web with IPv6 Tunneling

IP tunnels are solutions for sending IP packets over IP packets. This can be done within the same protocol family, which is often called VPNs. We use the same solution to tunnel IPv6 packets over IPv4 networks.

4.4 Conclusion

Through this chapter, we understand about the services we are going to implement. It allows us to get a clearer picture on each service. These services are common in industry. Thus, it will be helpful for us to have some basic knowledge and understanding before going to industrial training.

5.0 CHAPTER 5: INSTALLATION AND CONFIGURATION

5.1 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 or package.

5.2 Services and Corresponding Person-In-Charge

1. Server Virtualization **2. DNS (IPv4 & IPv6)** **3. DHCP (IPv4 & IPv6)**	MOHAMAD FIQHREEL EIZIQ BIN ISMAIL
1. Network Management System **2. Routing & NAT** **3. Proxy Server**	HONG MIN KE
1. AAA (Authentication, Authorization, and Accounting) **2. Secure FTP; with authentication and encryption** **3. Access Control List (ACL)**	MOHD RIDZUAN BIN MOHD AMIN
1. Linux Email Server **2. Web, SSL & Virtual Hosting** **3. IPv6 Web with IPv6 Tunneling**	SATTISH KUMARAN A/L TAYVANTRIAN
1. IPSec site-to-site tunneling **2. Active Directory** **3. Wireless user authentication using Radius server (AD user account/Mac Address)**	MUHAMMAD FARID ZAKWAN BIN SYAFRISAL

5.3 Service Installation and Configuration

5.3.1 Server Virtualization

Step 1: Click next on the Features screen. The management tools are on this screen and would have been selected by the popup on the previous screen.

Step 2: You will be presented with an informational page about Hyper-V. Click Next.

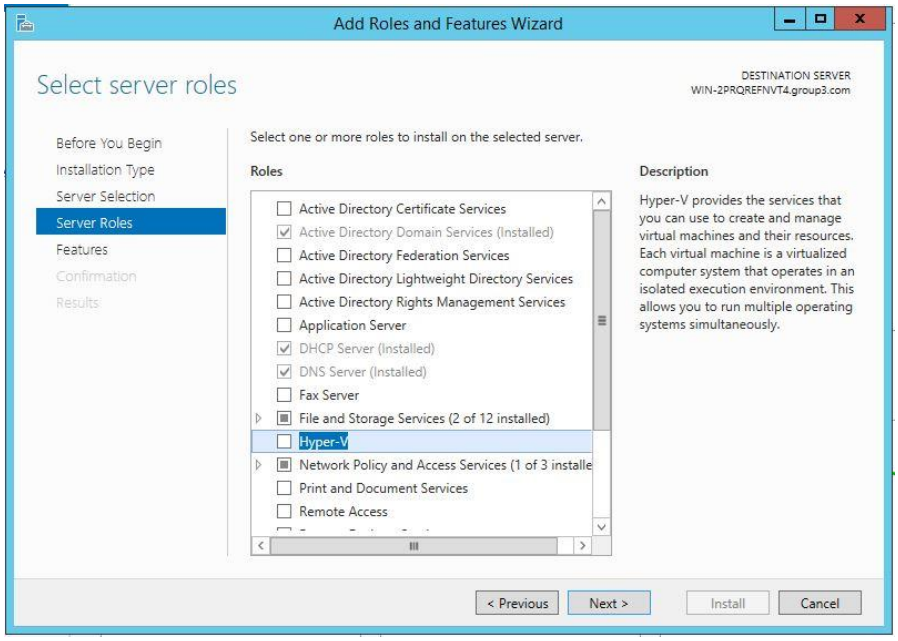


Figure 5.3.1 1 Hyper-v roles

Step 3: Click hyper-v box and click next

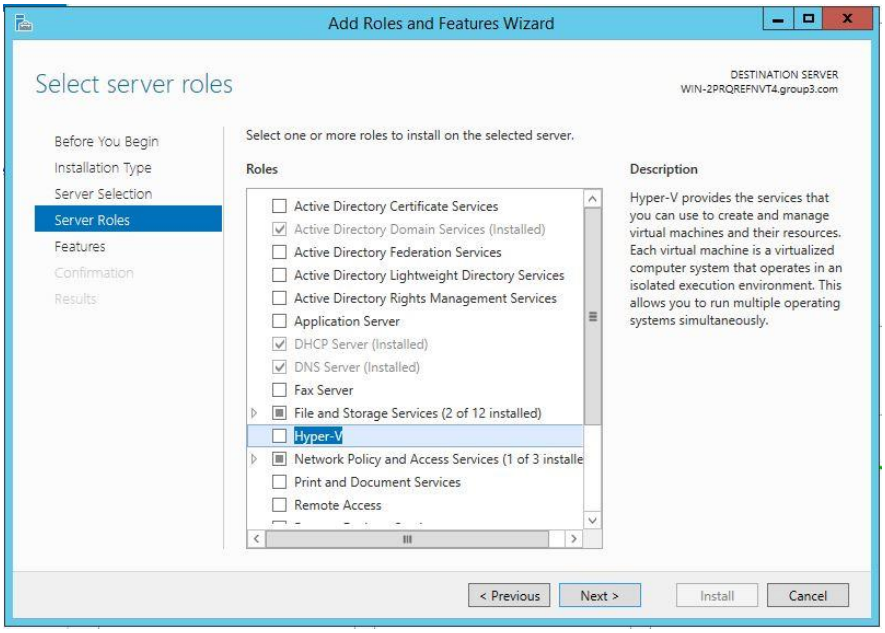


Figure 5.3.1 2 Hyper-v server roles installation

Step 4: Click add features for begin installation

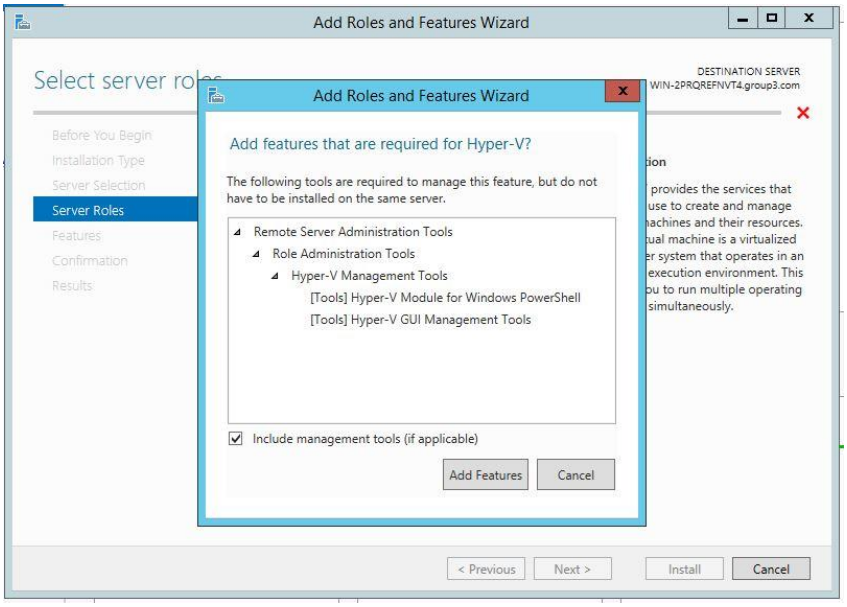


Figure 5.3.1 3 Hyper-v add features installation

Step 5: Click next on this step

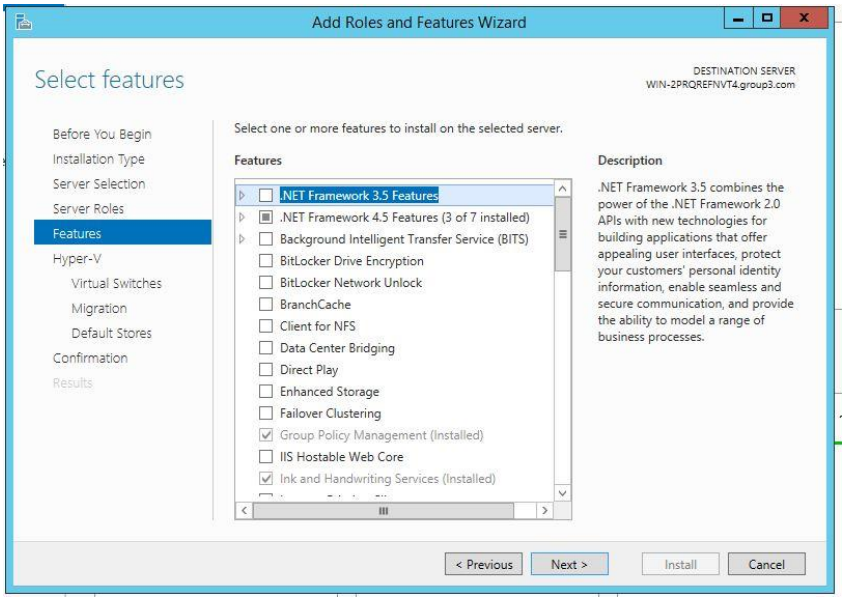


Figure 5.3.1 4 Hyper-v select features installation

Step 6: The Virtual Switches screen is next.

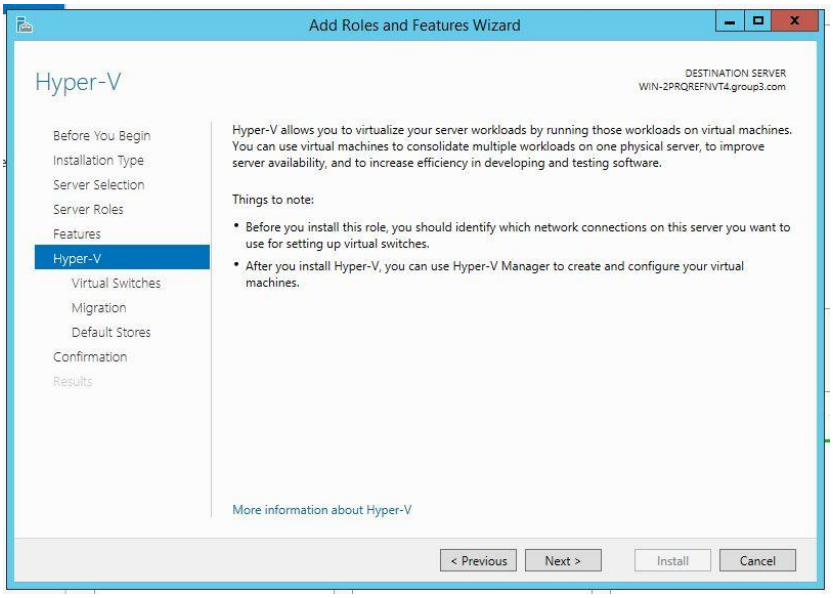


Figure 5.3.1 5 Hyper-v installation select next

Step 7: Select checkbox for network adapters and click next

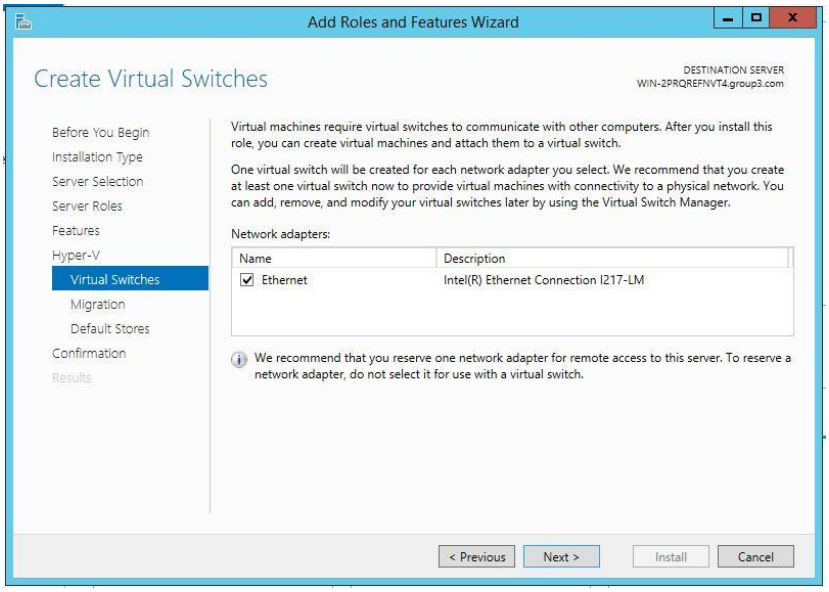


Figure 5.3.1 6 Hyper-v network editor selection

Step 8: Click next on the Live Migration screen. These options will be delved into later and are not necessary at this time.

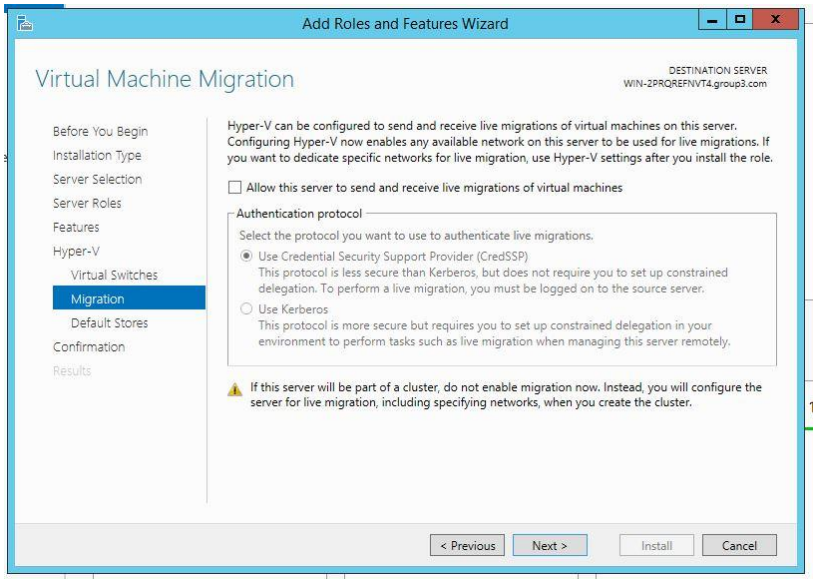


Figure 5.3.1 7 Migration setup

Step 9: Unless you intend to store virtual machines in their default location on the C: partition, change the settings here. They can be changed later, but it's helpful to do it now as it's easy to forget. It's perfectly acceptable to use SMB 3 paths here. Once both fields are set, click next.

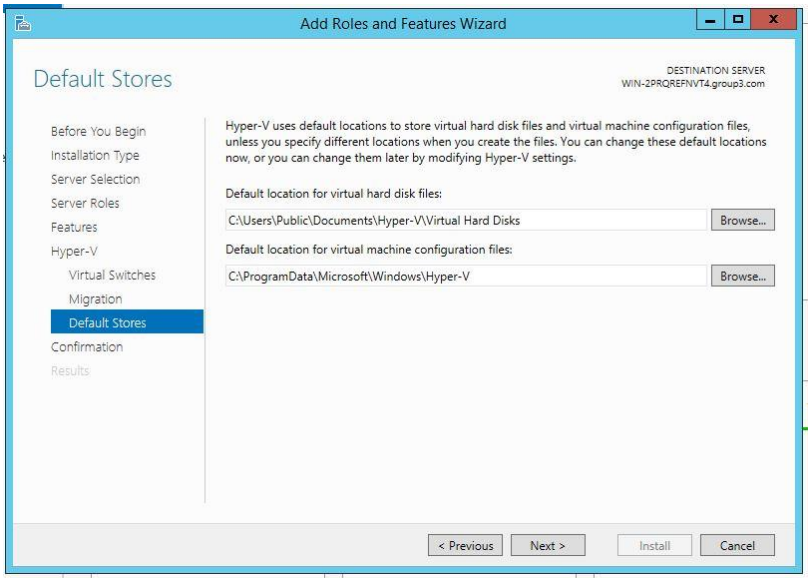


Figure 5.3.1 8 Hyper-v location setup

Step 10: Click install and waiting for finish installation

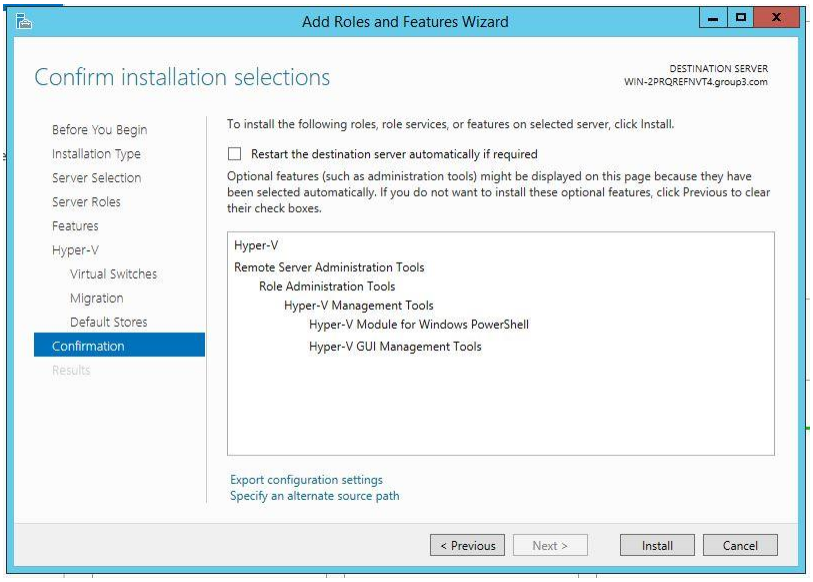


Figure 5.3.1 9 Hyper-v finish installation

Step 11: Click new and click Virtual machine to install new operating system

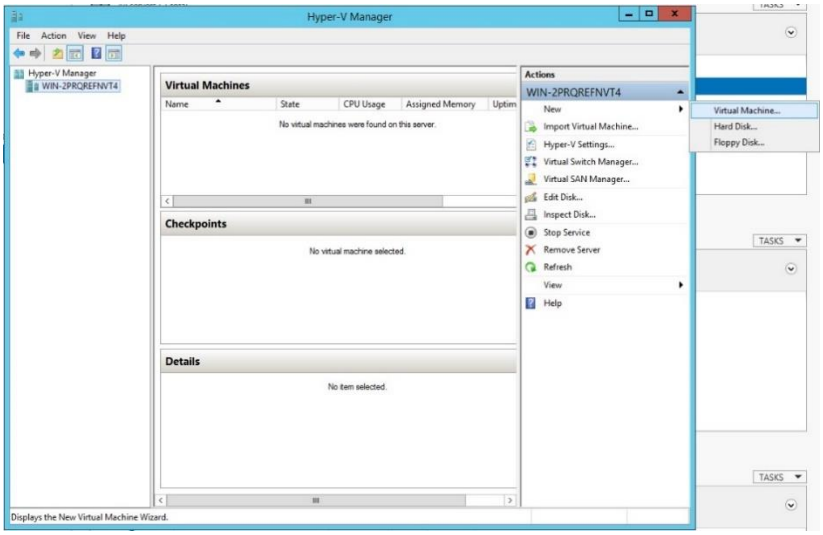


Figure 5.3.1 10 Hyper-v new operating system installation

Step 12: Click next on this step to begin installation

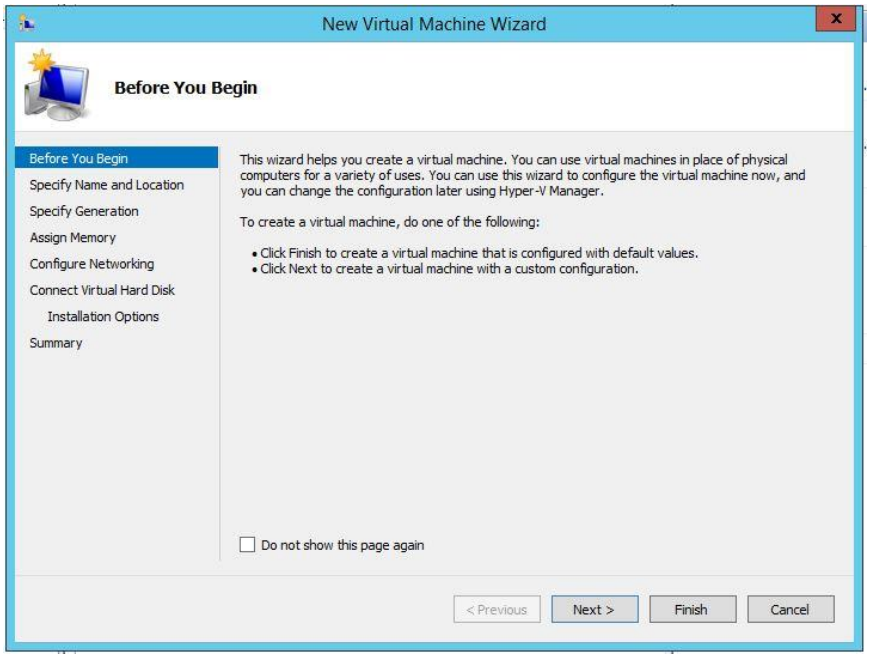


Figure 5.3.1 11 Hyper-v OS installation

Step 13: Choose the virtual machine generation and click next

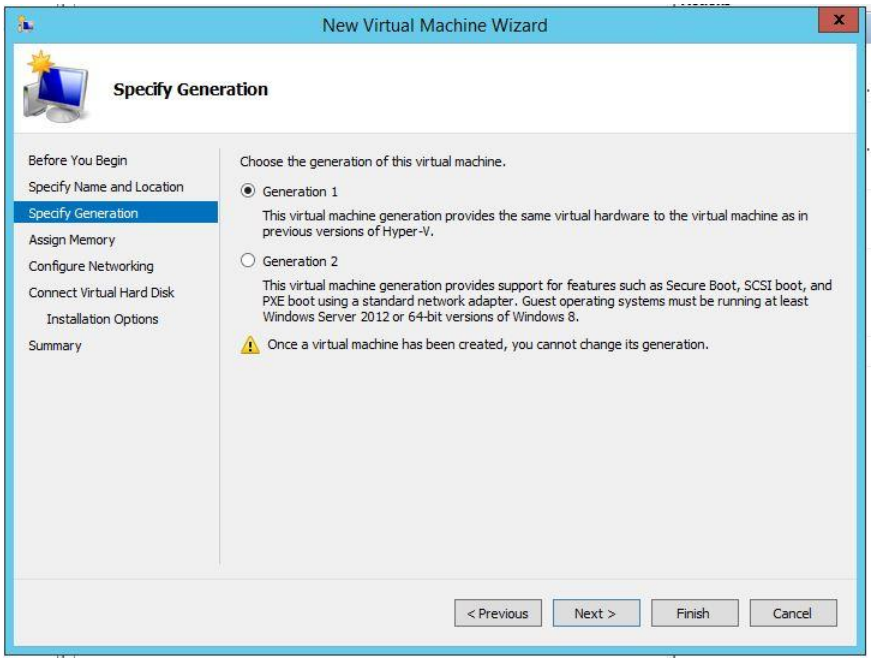


Figure 5.3.1 12 Hyper V virtual machine generation choose

Step 14: Insert memory for virtual machine and click next

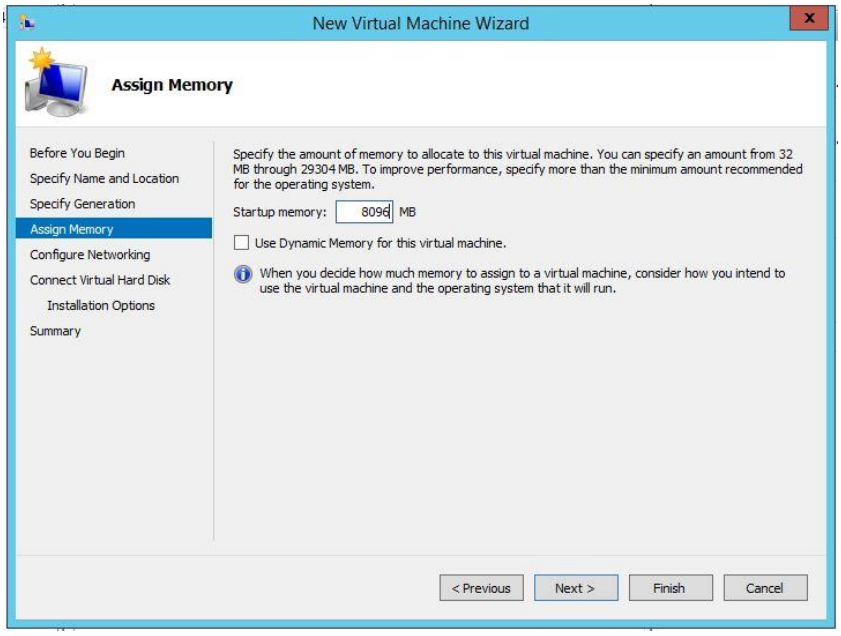


Figure 5.3.1 13 Hyper v memory setup

Step 15: Select connection for virtual machine and click next

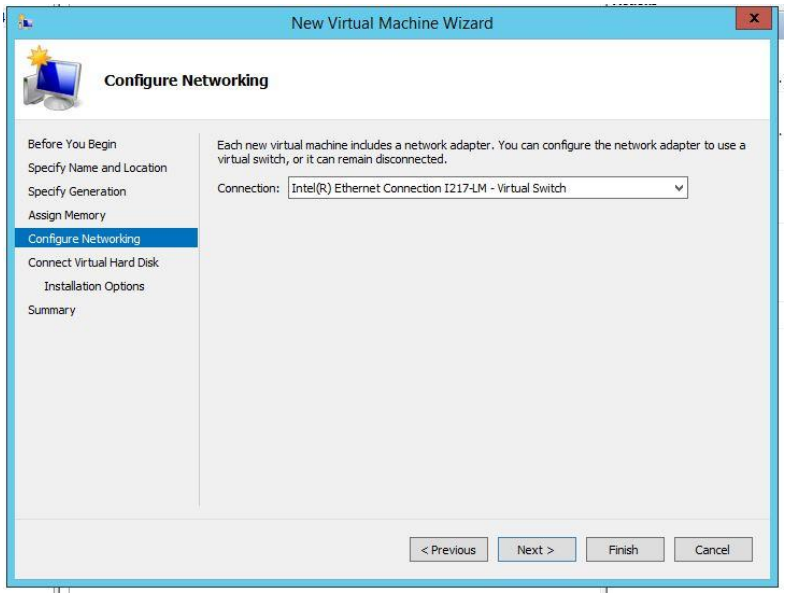


Figure 5.3.1 14 Hyper-v virtual machine connection

Step 16: Insert name for virtual machine and location for virtual machine

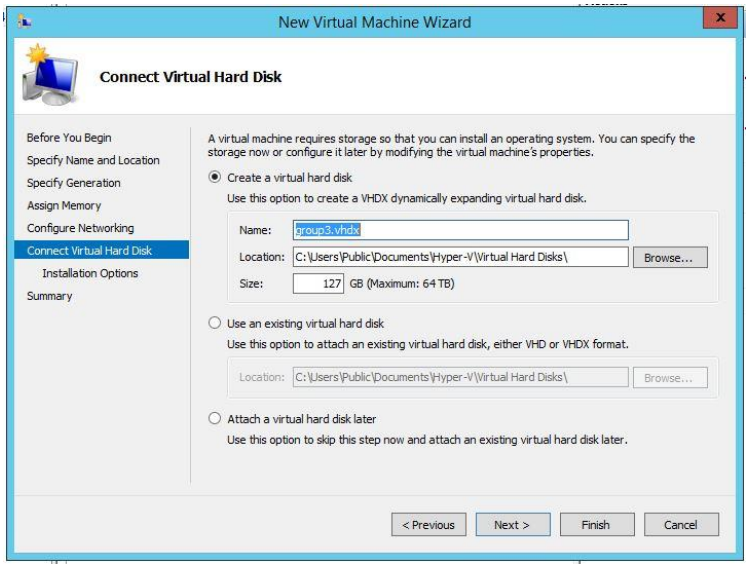


Figure 5.3.1 15 Hyper-v virtual name and location

Step 17: On this step select the iso for operating system and click next

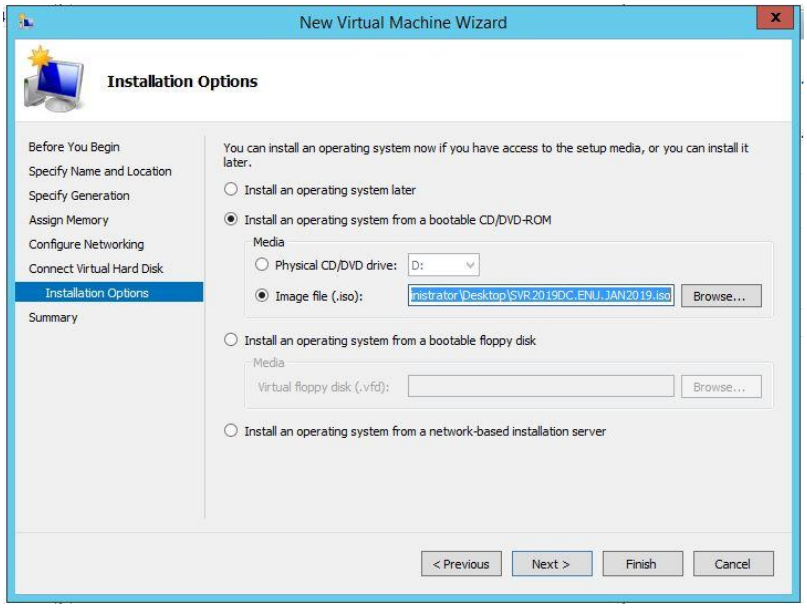


Figure 5.3.1 16 Hyper-v iso installation

Step 18: Click finish to complete virtual machine setup

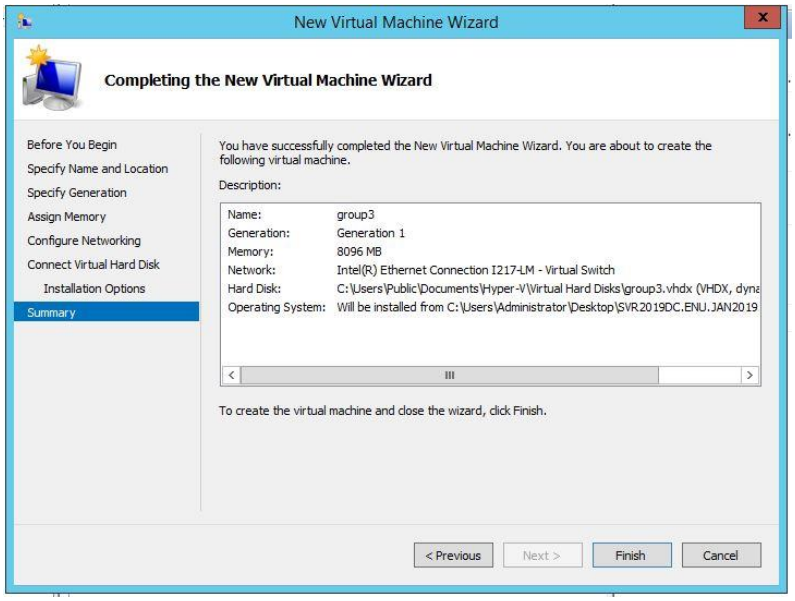


Figure 5.3.1 17 Hyper-v virtual machine finish installation

Step 19: Turn on the virtual machine to start the OS installation

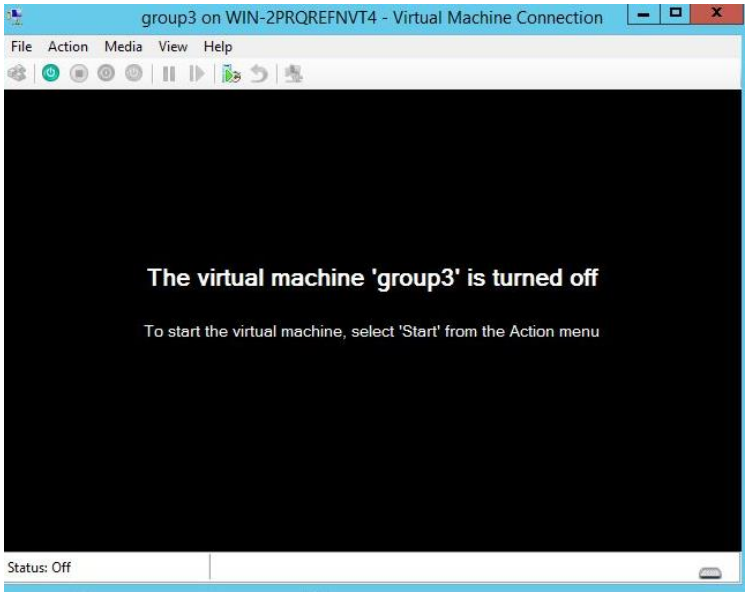


Figure 5.3.1 18 Hyper-v virtual machine start page

Step 20: Wait for windows starting the installation and install the windows server as usual setup

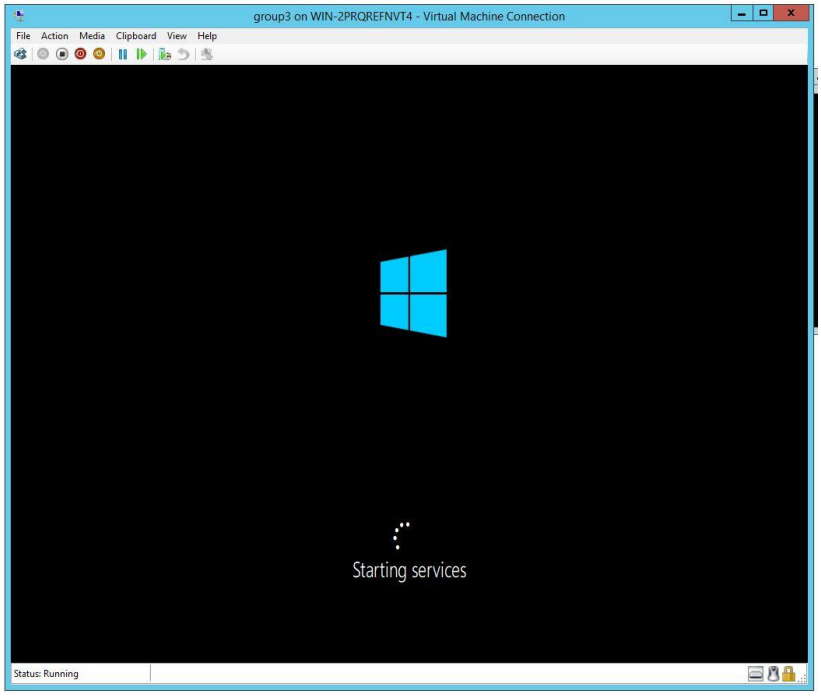


Figure 5.3.1 19 Hyper-v windows server installation

5.3.2 Domain Name System (Ipv4 & Ipv6)

Primary DNS

Step 1: Create new DNS server using wizard.

Figure 5.3.2 1 Creating a new zone wizard

Step 2: Then configure a DNS action by ticking a primary zone.

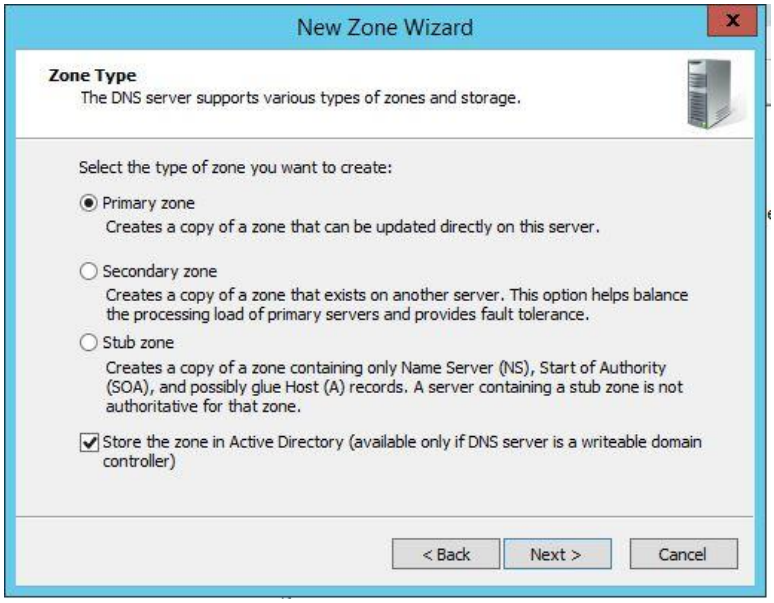


Figure 5.3.2 2 Selecting zone type

Step 3: Then select option to all DNS server running on domain controller.

Figure 5.3.2 3 Selecting new zone data replicated

Step 4: Then, enter the zone name (example; group3.com).

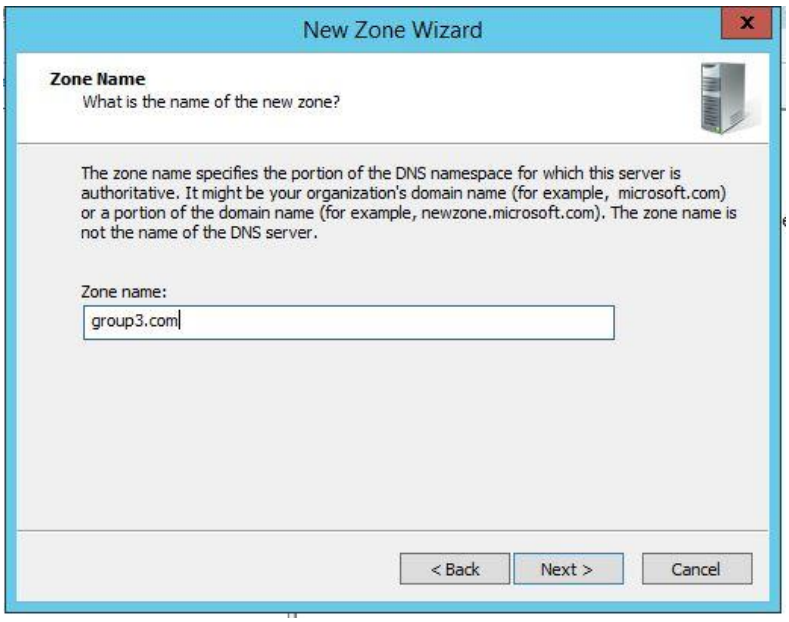


Figure 5.3.2 4 Create a new zone name

Step 5: For Dynamic Updates, select allow only secure dynamic updates. Then, click next

Figure 5.3.2 5 Select type of dynamic updates

Step 6: As a result of DNS configuration, it will show all the detail that you have enter.

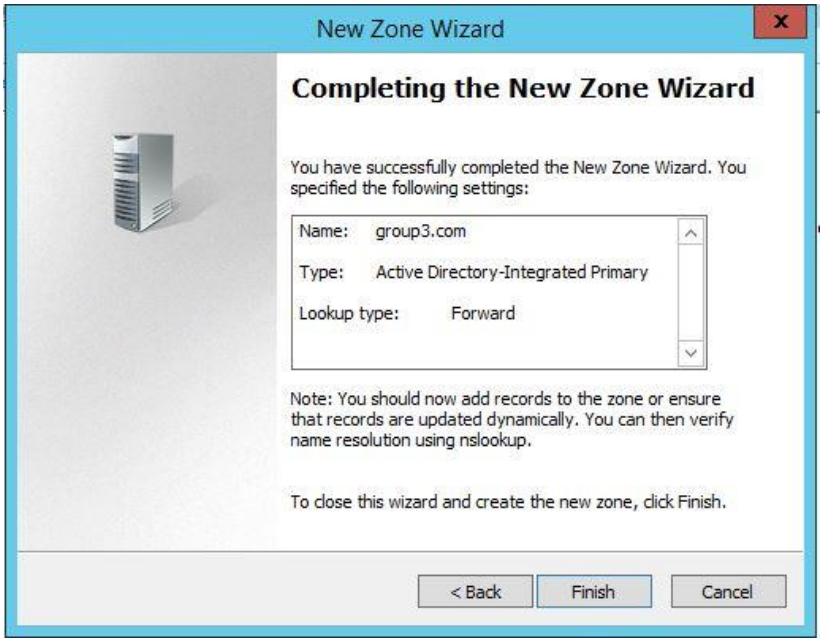


Figure 5.3.2 6 Completing setup for new wizard zone

Step 7: For Reverse Lookup Zone Name, select IPv4 Reverse Lookup Zone and click next.

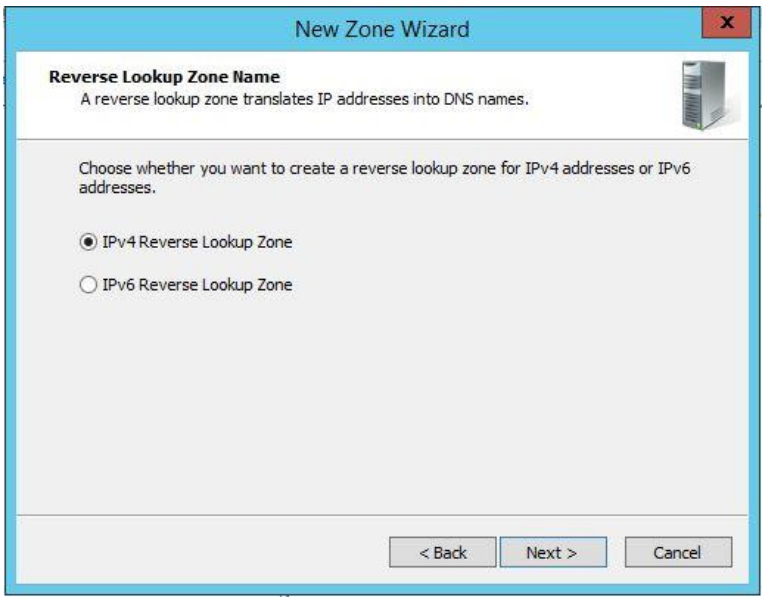


Figure 5.3.2 7 Create new ipv4 reverse lookup

Step 8: Enter Network ID for the zone and click Next button.

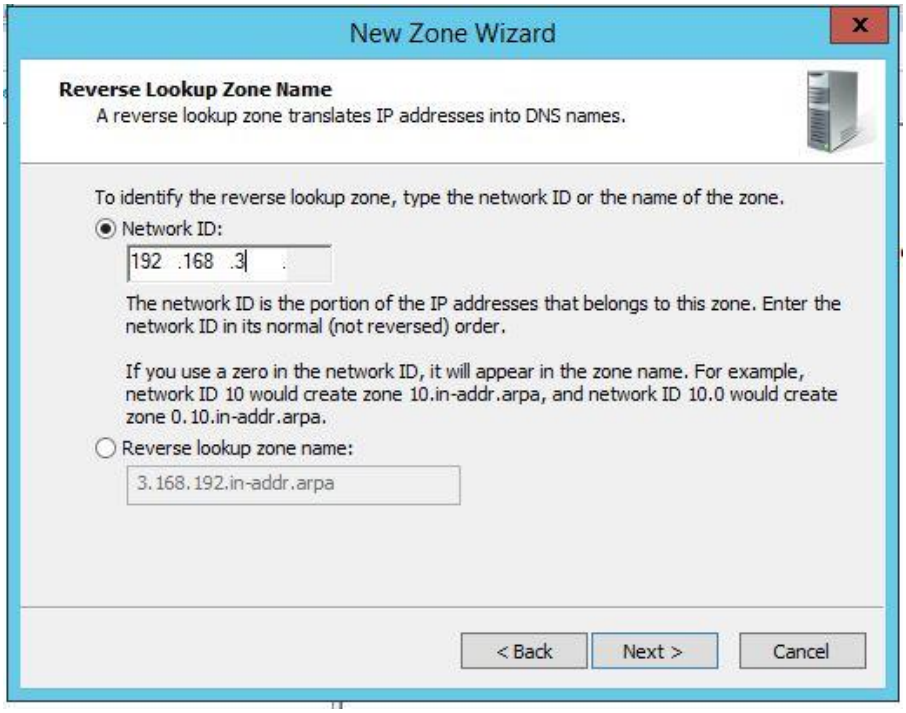


Figure 5.3.2 8 Server ip

Step 9: For Dynamic Updates, select allow only secure dynamic updates. Then, click Next.

Figure 5.3.2 9 Select update type for new zone wizard

Step 10: Upon completing the New Zone Wizard, it will show the specified settings that have been done. Then, click Finish to close.

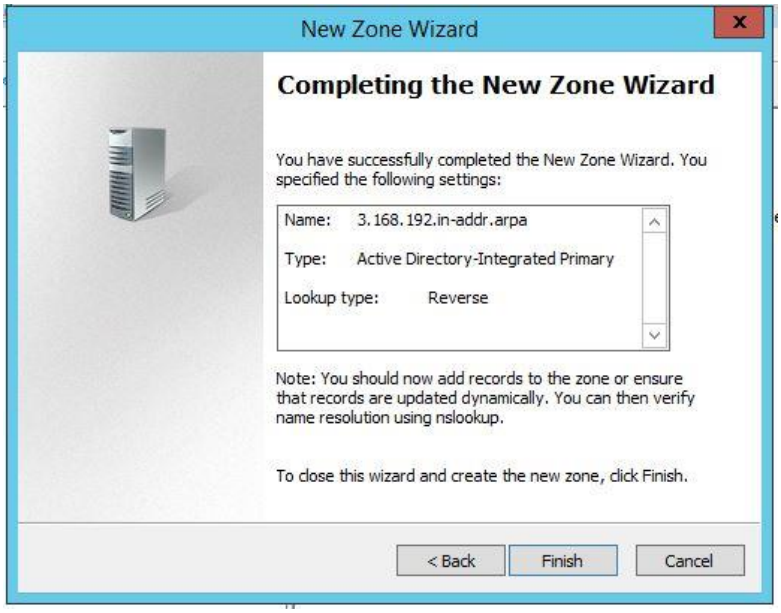


Figure 5.3.2 10 Completing setup for new wizard zone 2

Step 11: For Reverse Lookup Zone Name, select IPv6 Reverse Lookup Zone and click next.

Figure 5.3.2 11 Ipv6 reverse lookup

Step 12: Enter IPv6 Address Prefix and click next.

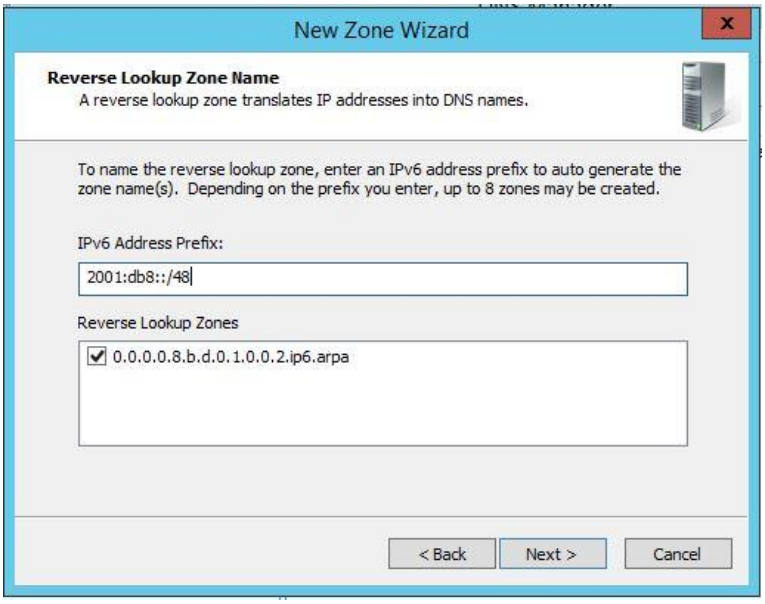


Figure 5.3.2 12 Ipv6 reverse ip

Step 13: Lastly, click finish.

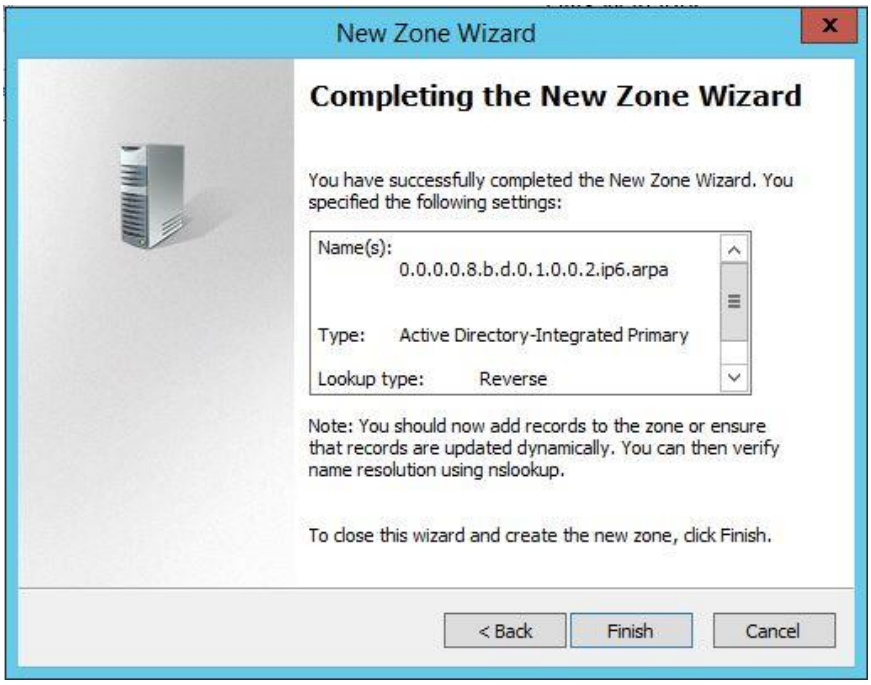


Figure 5.3.2 13 Finish setup for reverse ip

Step 14: Now create new pointer for ipv6.

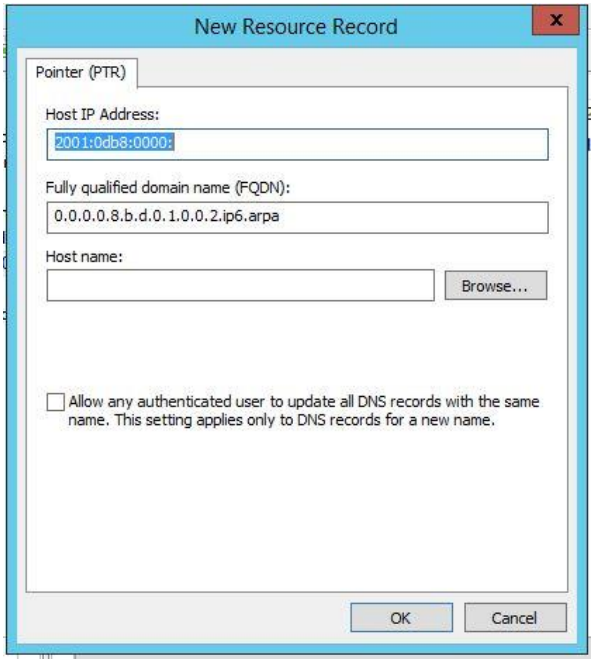


Figure 5.3.2 14 Create new pointer

Step 15: Click browser and find ipv6 host.

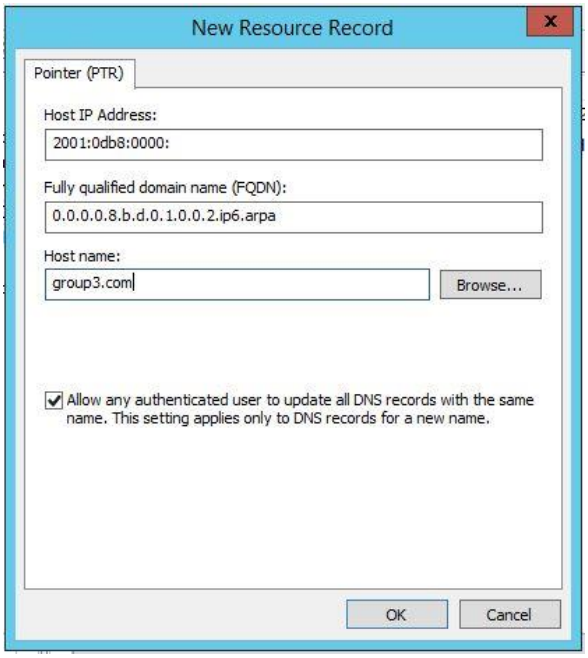


Figure 5.3.2 15 Create host name

Step 16: Select Ipv6 Host and click ok.

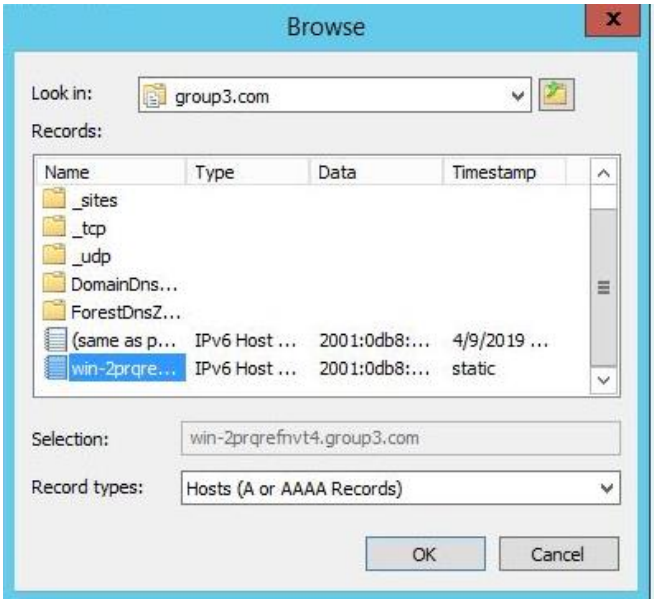


Figure 5.3.2 16 Ipv6 pointer

Step 17: Then, click allow any authentication user to update all DNS record with the same name.

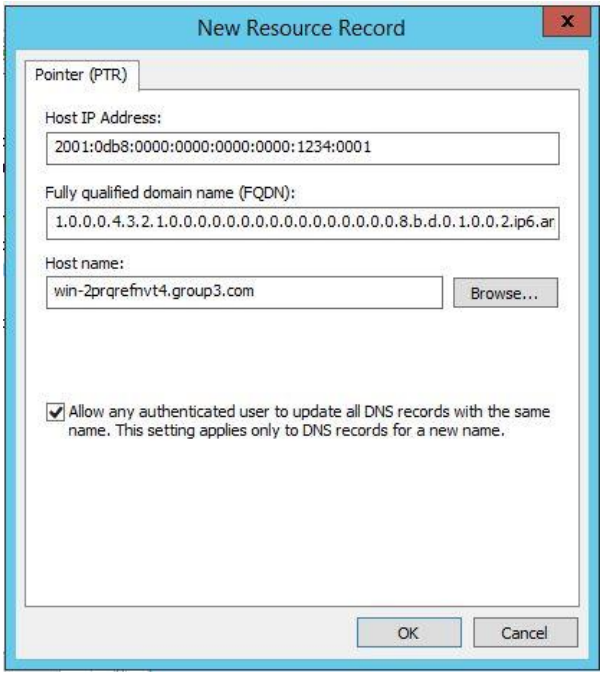


Figure 5.3.2 17 Finish setup pointer

5.3.3 DHCP

Step 1: Open Server Manager and click on Add Roles and Features Wizard.

Step 2: For Server Role, select the DHCP role and click Next button

Step 3: Then, tick or un-tick the desire checked box for Features and after that, click the Install button.

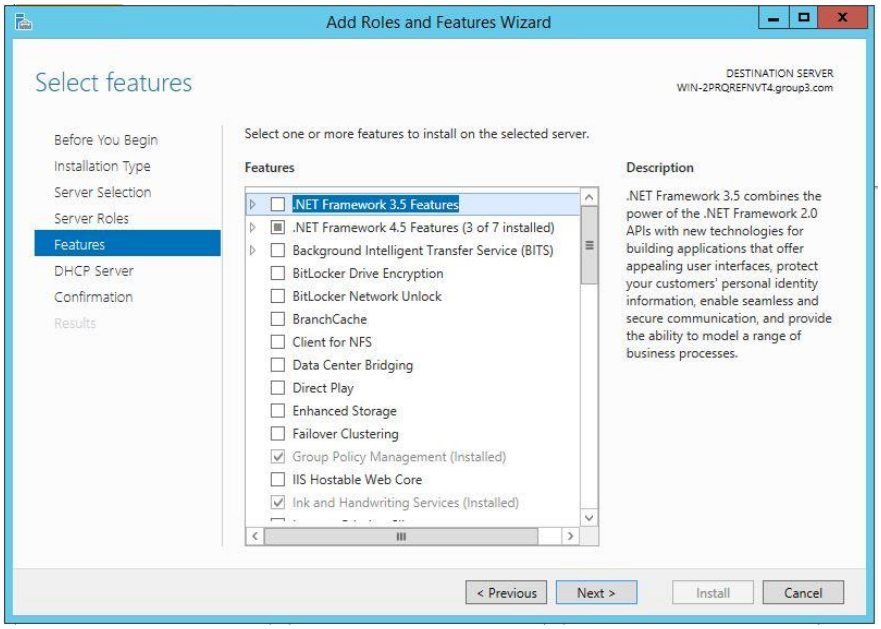


Figure 5.3.3 1 Installing new DHCP roles

Step 4: Then, wait until the installation completed.

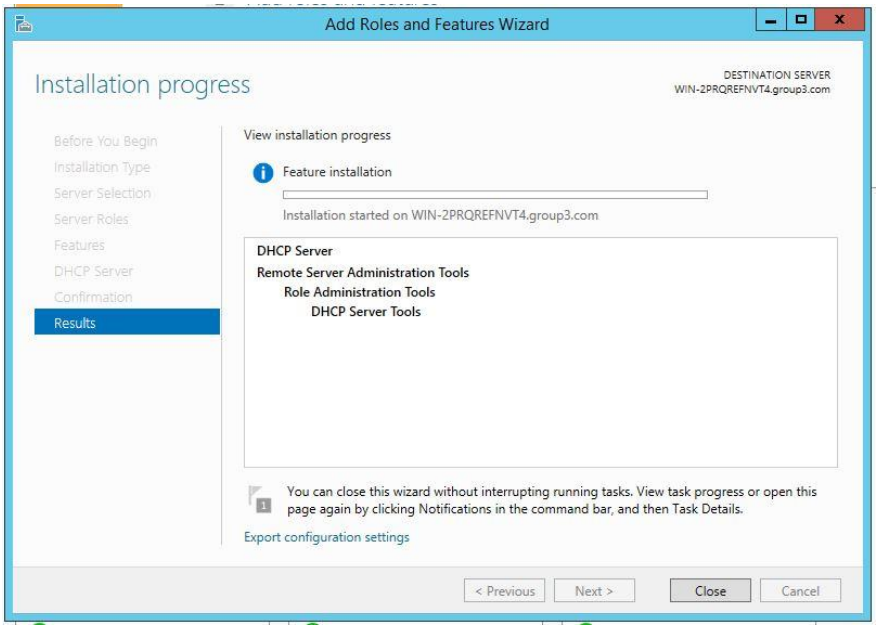


Figure 5.3.3 2 Finish setup DHCP roles

Step 5: After finishing the installation, open the DHCP configuration page.

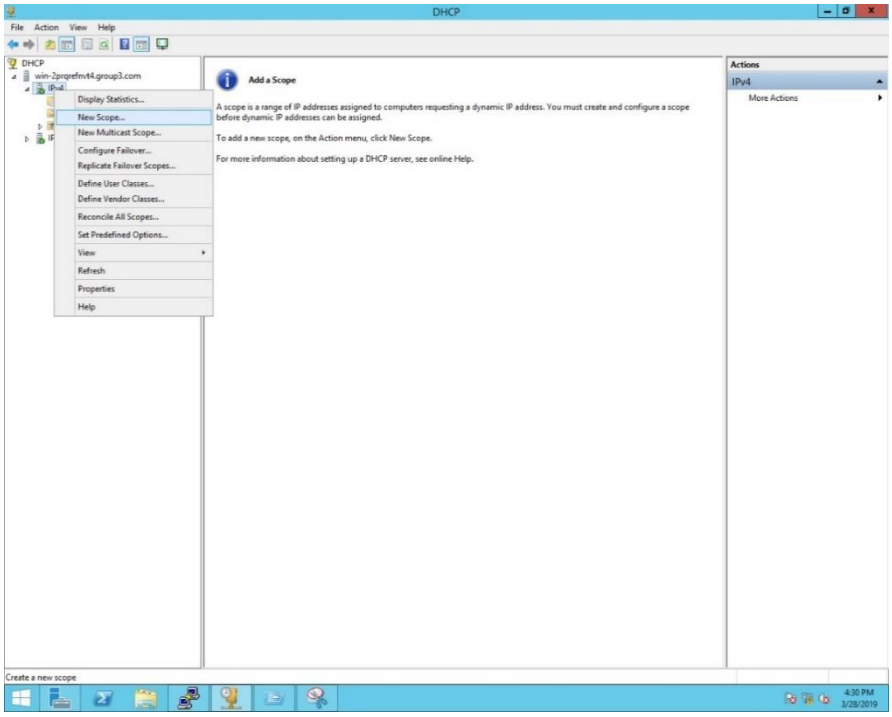


Figure 5.3.3 3 Creating new scope for DHCP

Figure 5.3.3 4 New zone setup for DHCP

Step 6: Then, create Scope Name for the New Scope Wizard and click next.

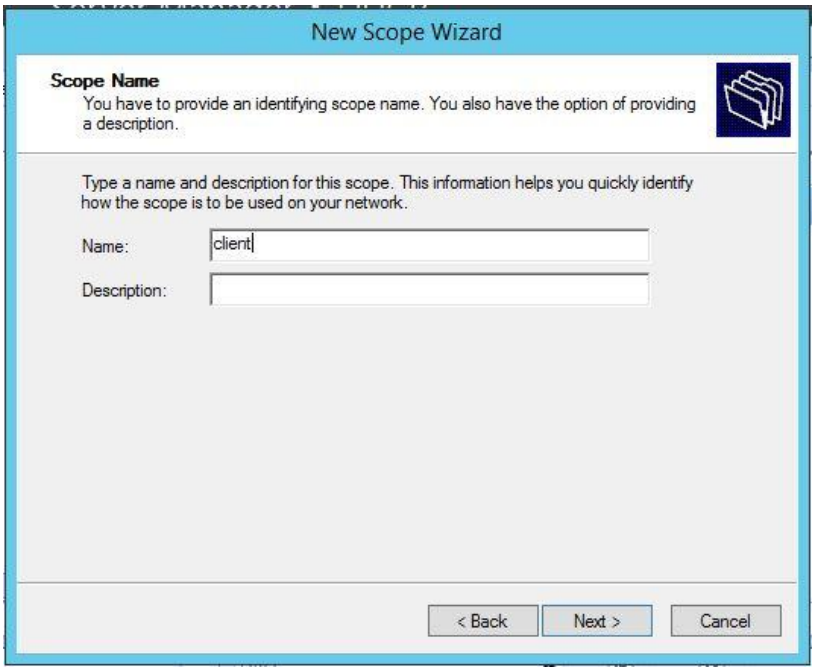


Figure 5.3.3 5 Create DHCP scope name

Step 7: Then, Insert ip address range for ipv4.

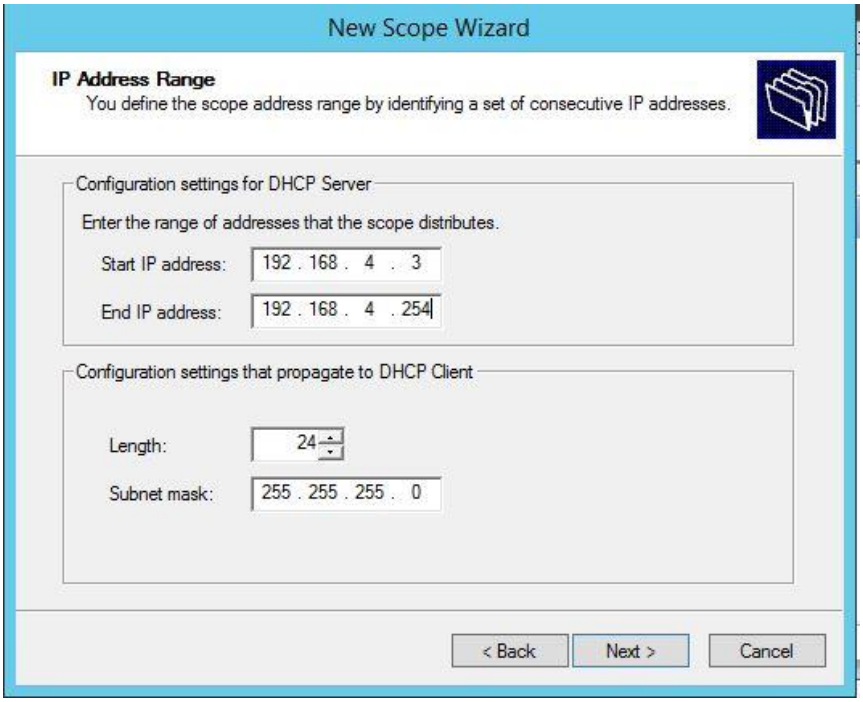


Figure 5.3.3 6 Setup DHCP ipv4 range

Step 8: Then insert default gateway for router.

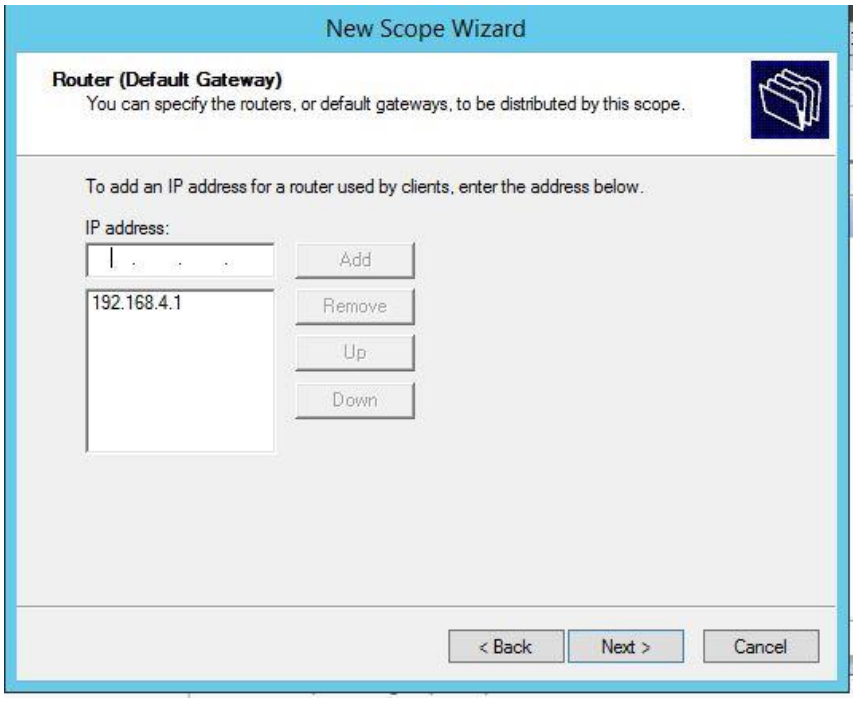


Figure 5.3.3 7 Insert DHCP gateway

Step 9: Select lease duration for DNS (example 8 days)

Figure 5.3.3 8 Select DHCP ip duration

Step 10: Then, select "Yes, I want to configure these option"

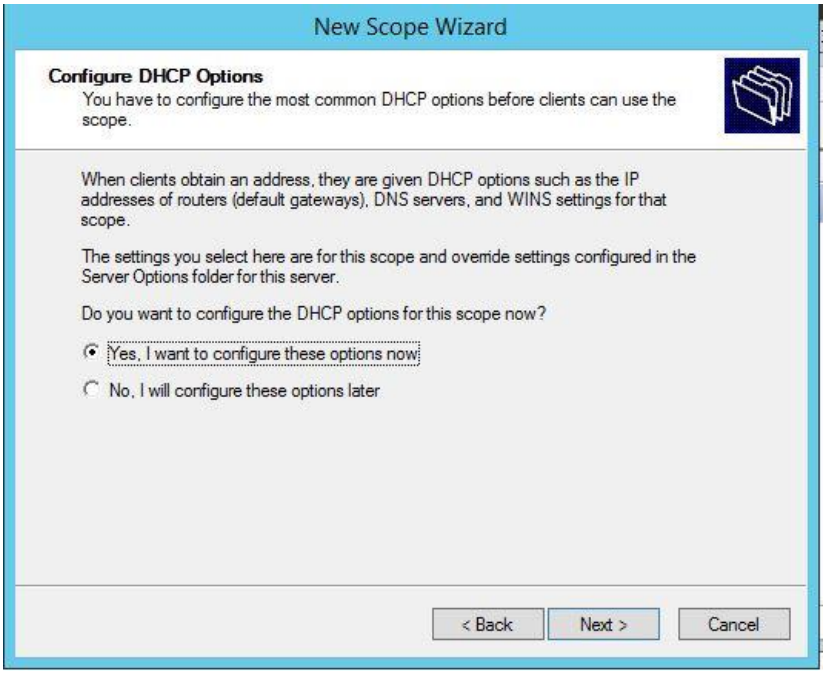


Figure 5.3.3 9 Finish configure scope for DHCP

Step 11: Click next this part.

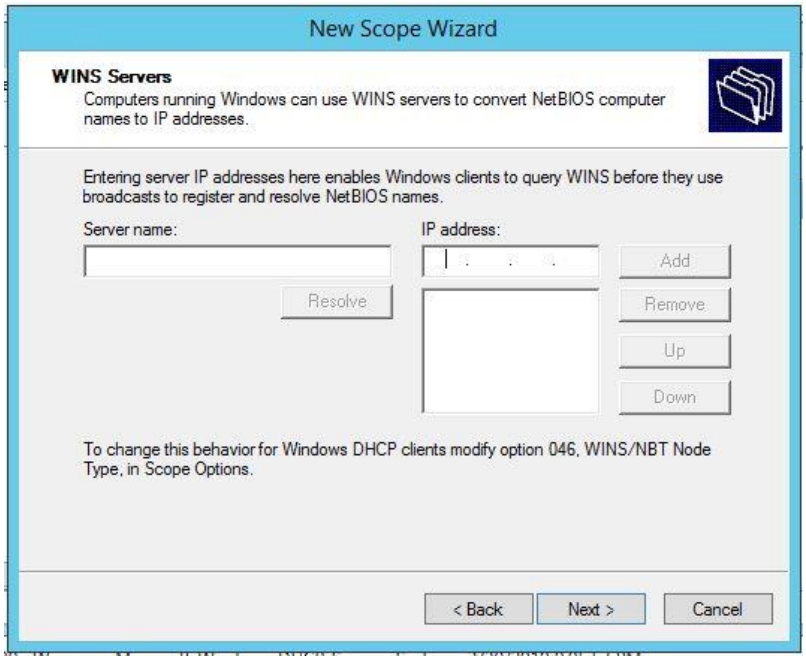


Figure 5.3.3 10 DHCP windows server client query setup

Step 12: Then click "Yes" and finish the setup for Ipv4.

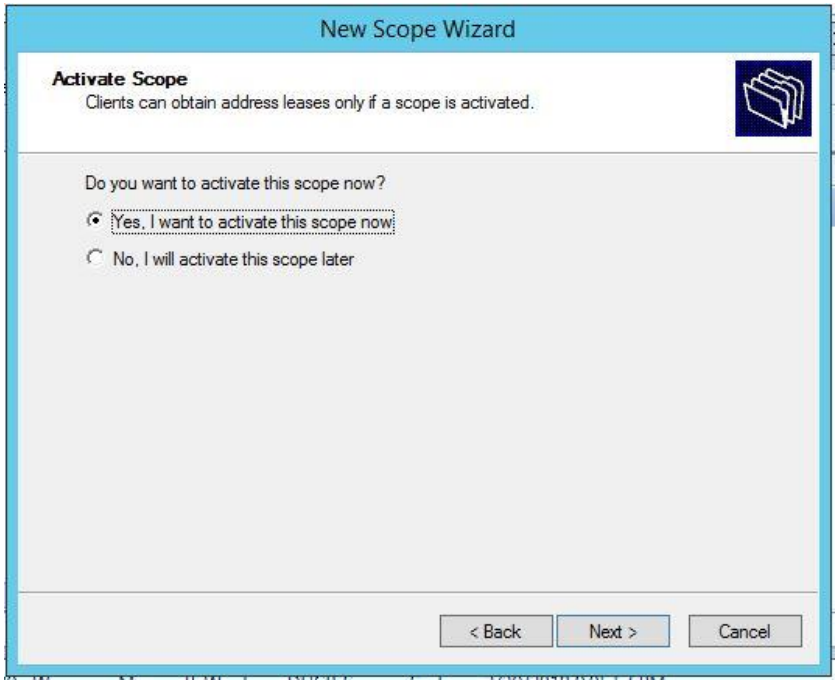


Figure 5.3.3 11 Finish DHCP setup

Figure 5.3.3 12 Successful DHCP setup

DHCP IPV6

Step 1: Now create new scope for ipv6

Step 2: Insert name as “client ipv6” then click next.

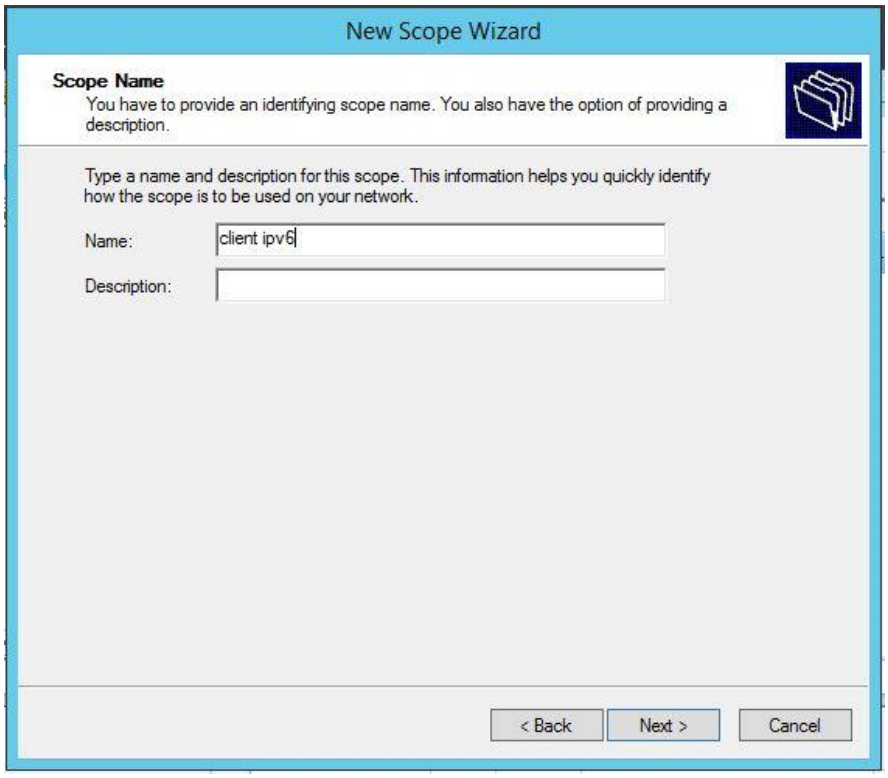


Figure 5.3.3 13 Insert ipv6 scope name

Step 3: Insert prefix with (2001:db8::1234:1/64). Then, click next until it finish.

Step 4: Just click next the next step and click finish.

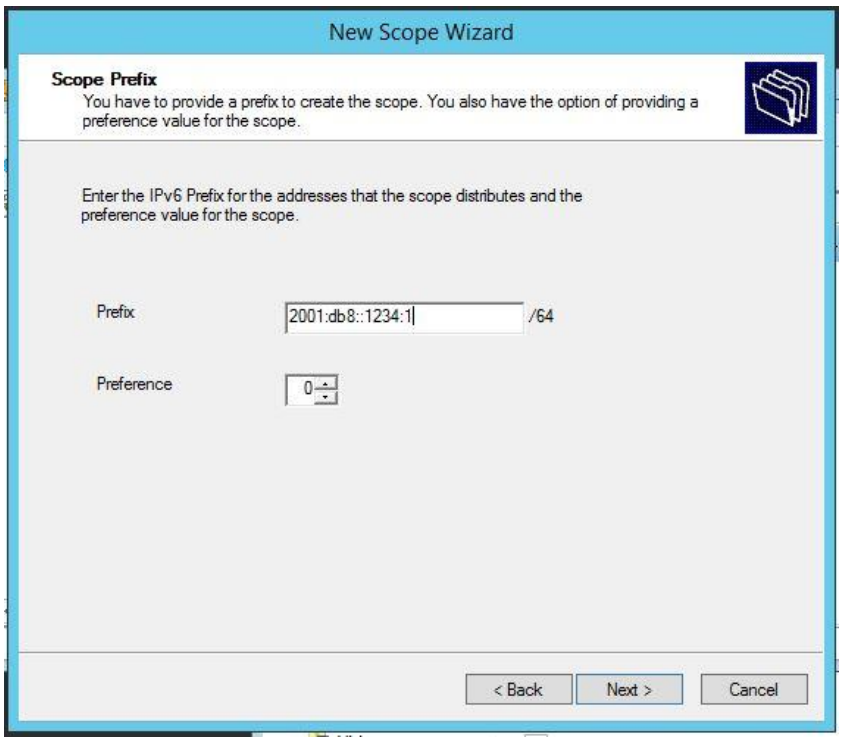


Figure 5.3.3 14 Ipv6 scope prefix

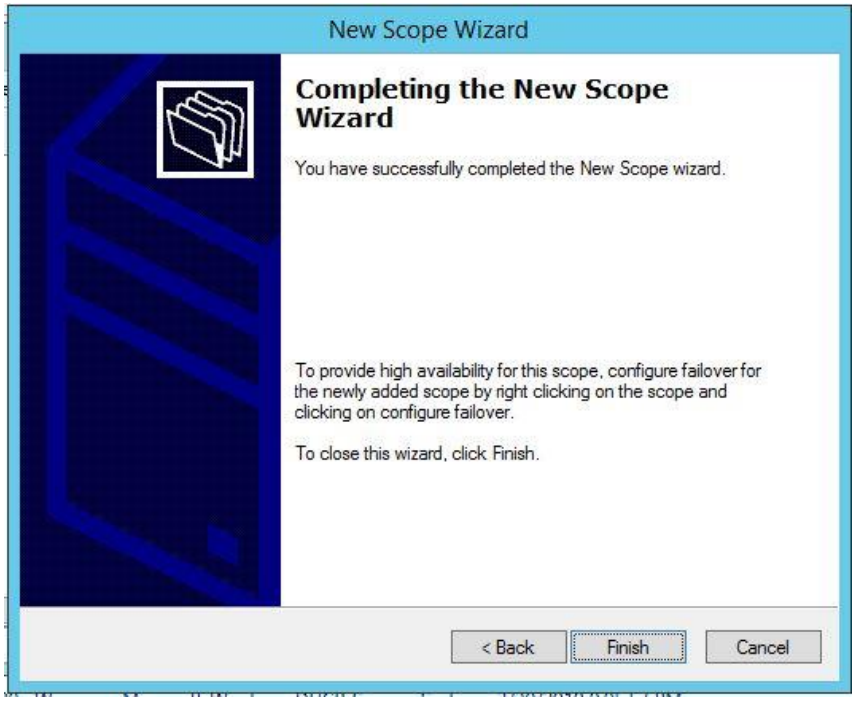


Figure 5.3.3 15 Ipv6 DHCP finish setup

5.3.4 Network Management System (NMS)

Step 1: Update the Ubuntu Server.

sudo apt-get update

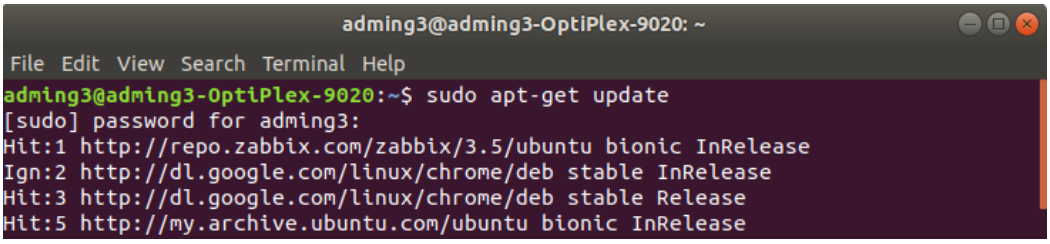


Figure 5.3.4 1 Update Ubuntu Server

Step 2: Upgrade the Ubuntu Server.

sudo apt-get upgrade

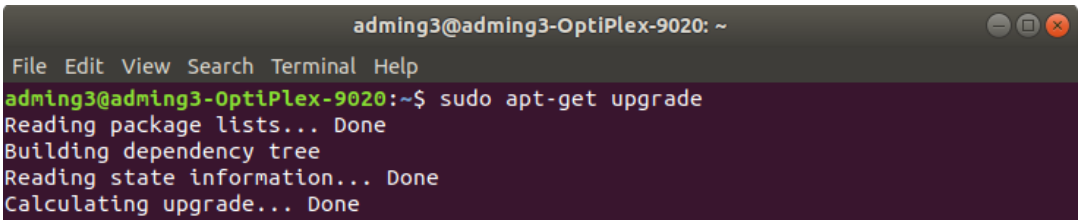


Figure 5.3.4 2 Upgrade Ubuntu Server

Step 3: Install apache web server.

sudo apt install apache2

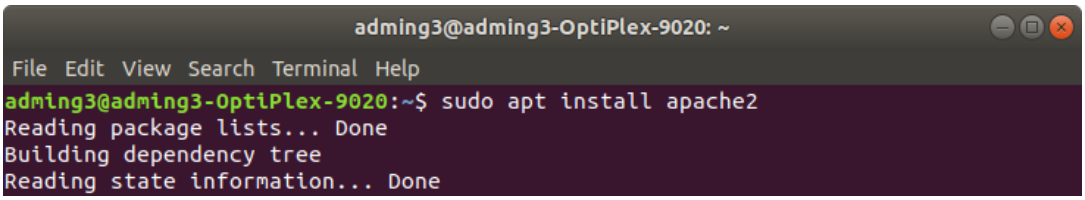


Figure 5.3.4 3 Install Apache

Step 4: Install mysql database.

sudo apt install mysql-server

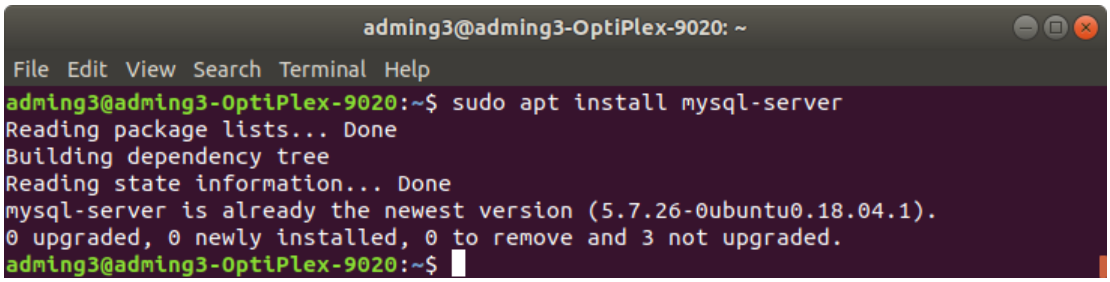


Figure 5.3.4 4 Install Mysql

Step 5: Install update version 7.2 needed for install Zabbix Server.

sudo apt install php php7.2-cli php7.2-mysql php7.2-common php7.2-curl php7.2-json php7.2-cgi libapache2-mod-php7.2 php7.2

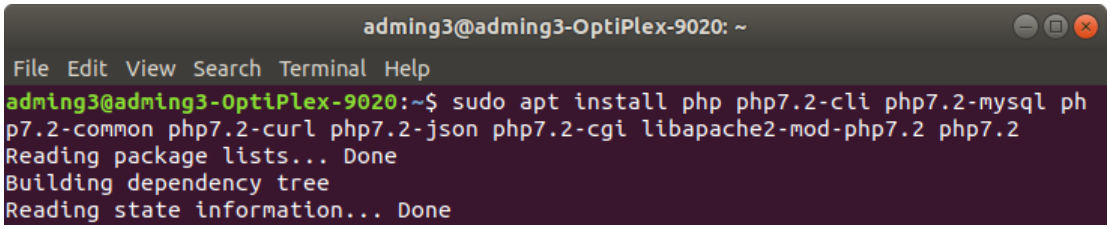


Figure 5.3.4 5 Install version 7.2

Step 6: Start Apache web server service.

sudo service apache2 start

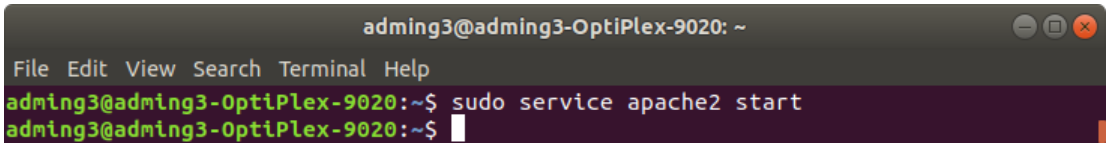


Figure 5.3.4 6 Start Apache service

Step 7: Download Zabbix deb file from the link.

sudo wget http://repo.zabbix.com/zabbix/3.5/ubuntu/pool/main/z/zabbix-release/zabbix-release_3.5-1%2Bbionic_all.deb

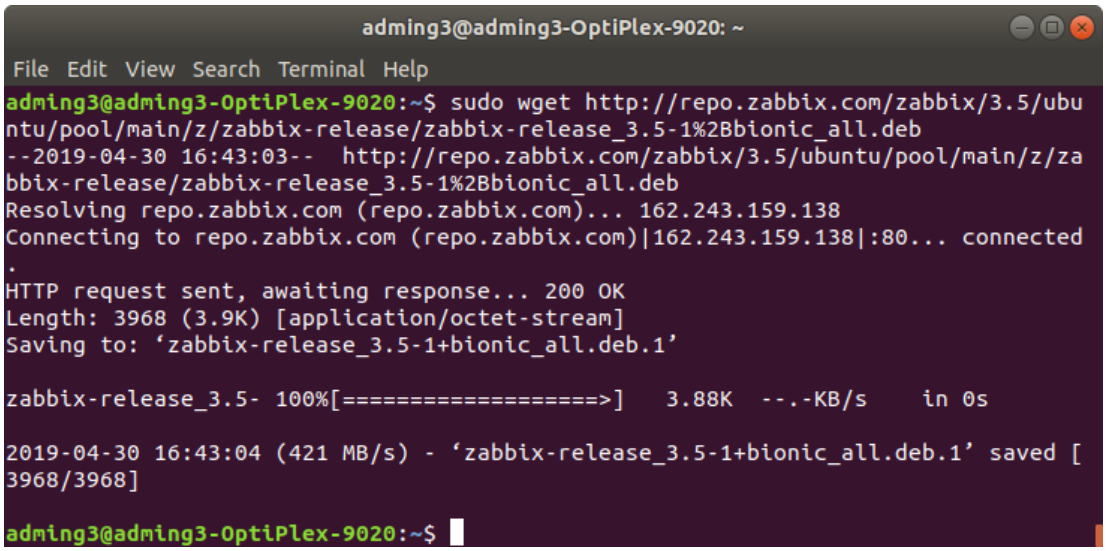


Figure 5.3.4 7 Download Zabbix

Step 8: Enable Zabbix repo for the server.

sudo dpkg -i zabbix-release_3.5-1+bionic_all.deb

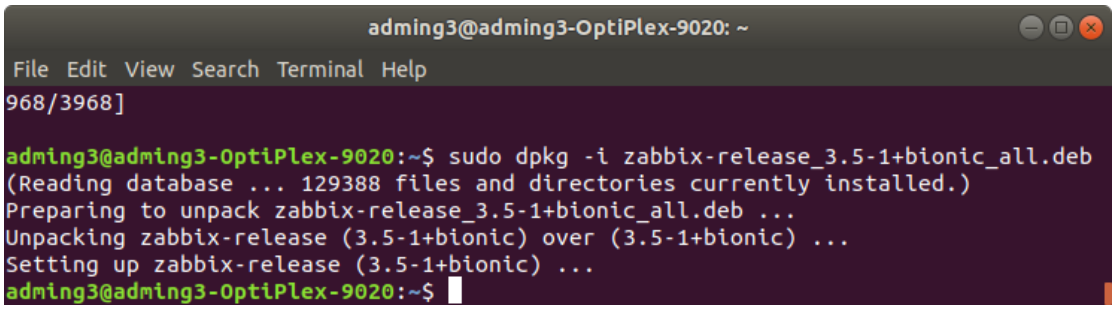


Figure 5.3.4 8 Enable Zabbix

Step 9: Update the newly released Zabbix Server.

sudo apt update

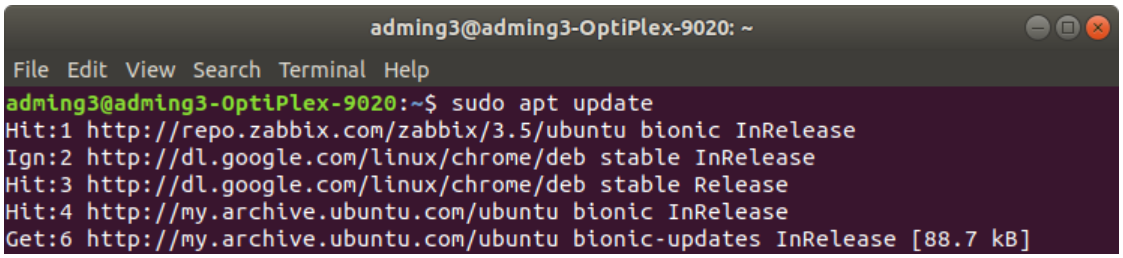


Figure 5.3.4 9 Update Zabbix Server

Step 10: Install Zabbix Server fronted mysql and php.

sudo apt install zabbix-server-mysql zabbix-frontend-php

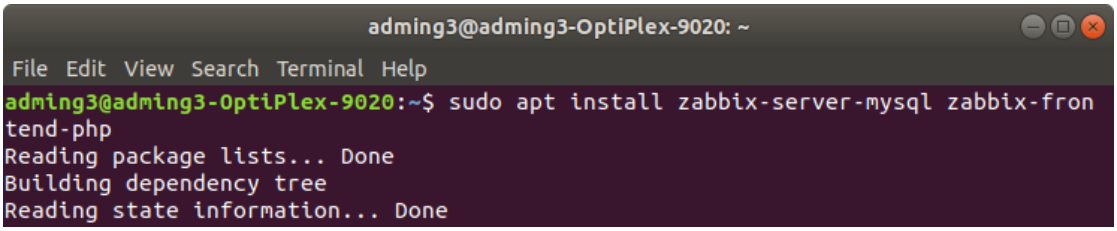


Figure 5.3.4 10 Install Zabbix Server

Step 11: Create Zabbix database and user from mysql terminal.

sudo mysql -u root –p

mysql > create database zabbix character set utf8 collate utf8_bin;

mysql > grant all privileges on zabbix.* to zabbix@localhost identified by 'passw0rd';

mysql > flush privileges;

mysql > cd database/mysql

mysql -uzabbix -ppassw0rd zabbix < schema.sql

mysql -uzabbix -ppassw0rd zabbix < images.sql

mysql -uzabbix -ppassw0rd zabbix < data.sql

\q

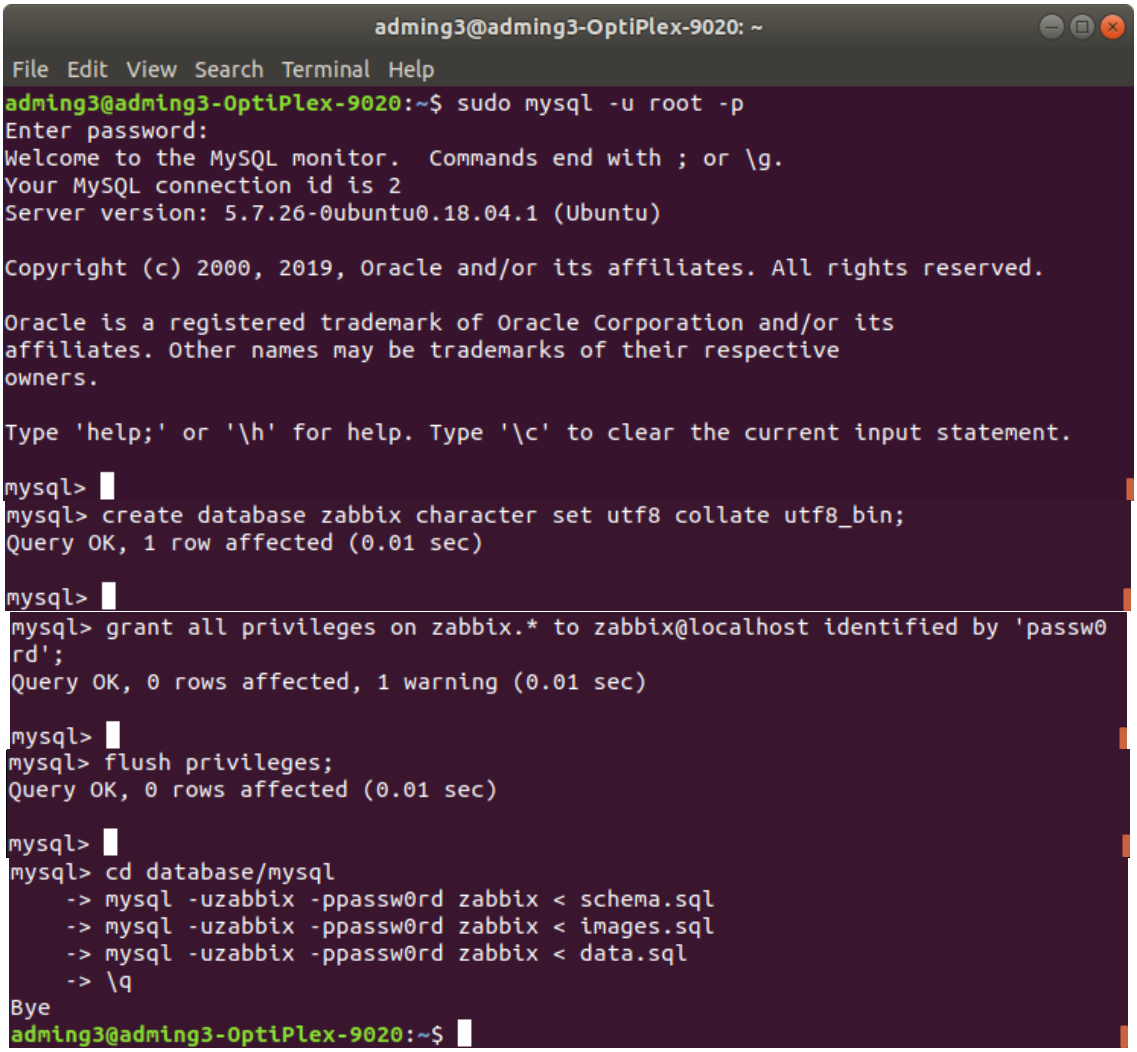


Figure 5.3.4 11 Create Zabbix database

Step 12: Create mysql table for store all data to the directory.

cd /usr/share/doc/zabbix-server-mysql/

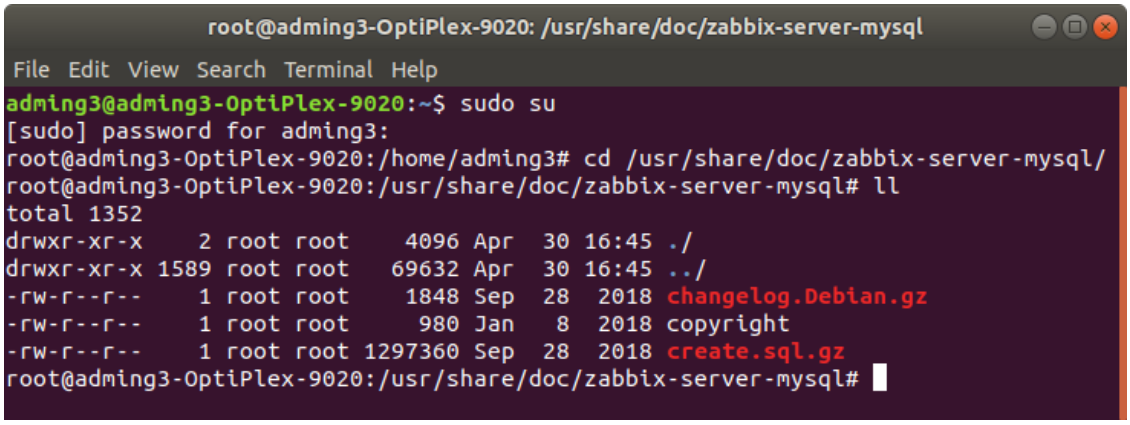


Figure 5.3.4 12 Create Mysql table

Step 13: Import all data into mysql database.

zcat create.sql.gz | mysql -uroot zabbix –p

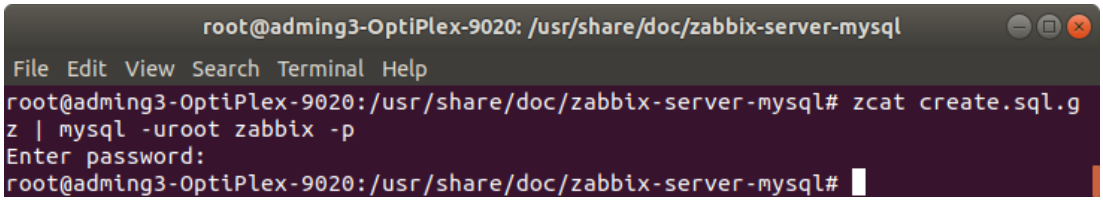


Figure 5.3.4 13 Import data to database

Step 14: Configure Zabbix Server conf file so open conf file.

nano /etc/zabbix/zabbix_server.conf

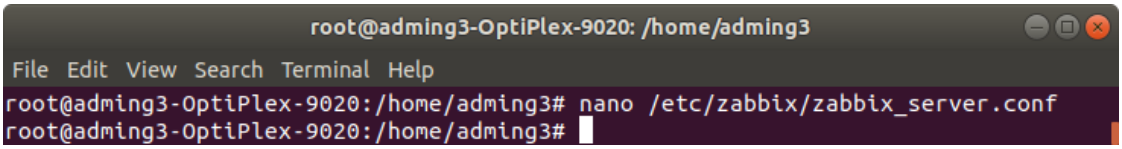


Figure 5.3.4 14 Configuration Zabbix Server conf file

Step 15: Change the config into zabbix_server.conf file.

DBHost=localhost

DBUser=zabbix

DBPassword=passw0rd

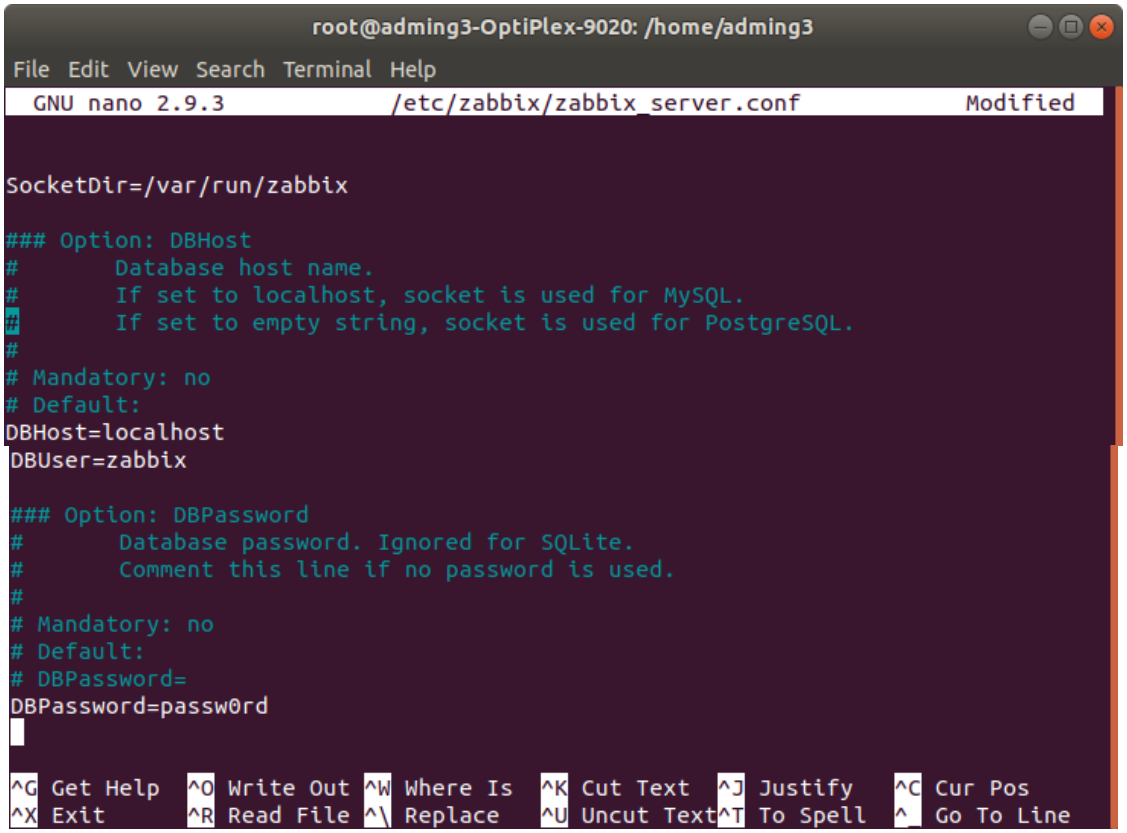


Figure 5.3.4 15 Change the config into zabbix.

Step 16: Edit php.ini file for time zone.

nano /etc/php/7.2/apache2/php.ini

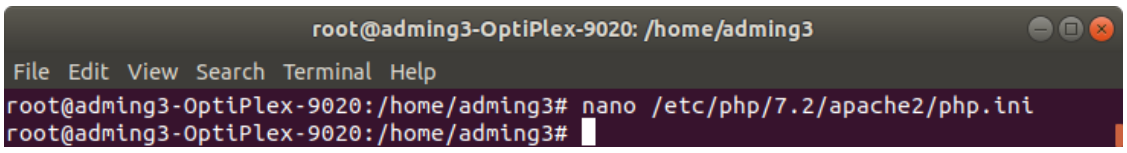


Figure 5.3.4 16 Edit time zone

Step 17: Update timezone in php configuration file

date.timezone = "Asia/Kuala_Lumpur"

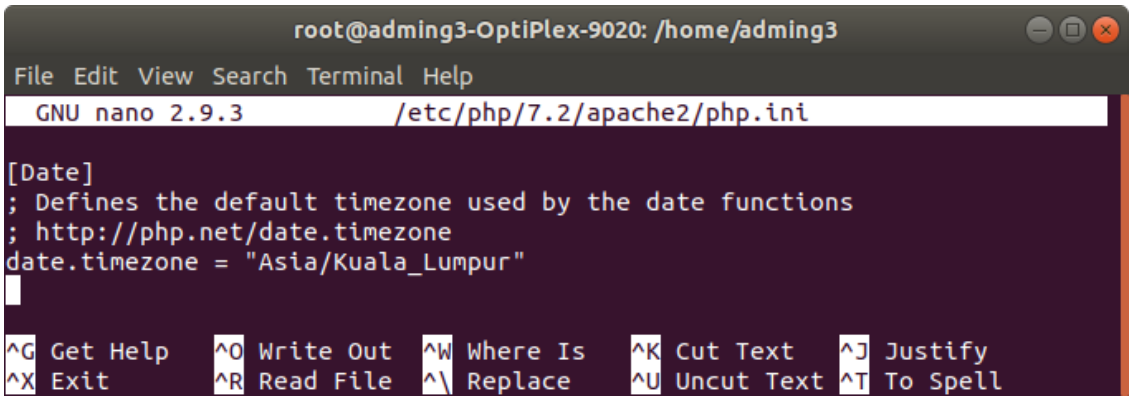


Figure 5.3.4 17 Update time zone

Step 18: Restart Apache web server service.

service apache2 restart

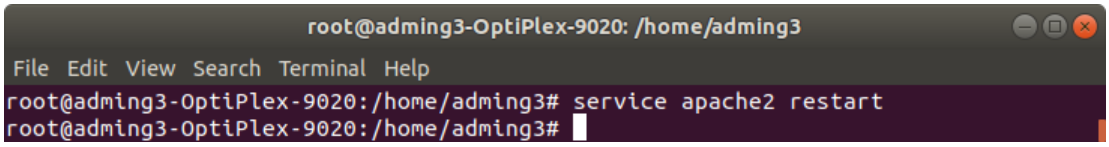


Figure 5.3.4 18 Restart Apache

Step 19: Start Zabbix Server.

service zabbix-server start

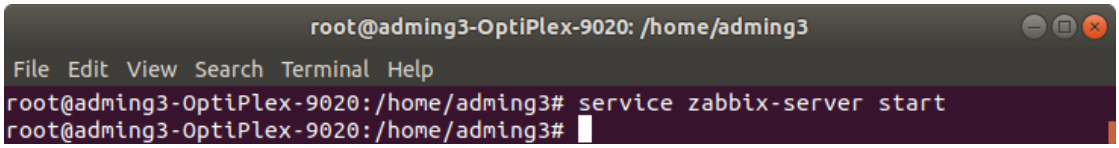


Figure 5.3.4 19 Start Zabbix Server

Setting up Zabbix Server

Step 1: Use the browser and type Server IP address. On Zabbix welcome page then click "Next step".

192.168.3.3/zabbix/setup.php

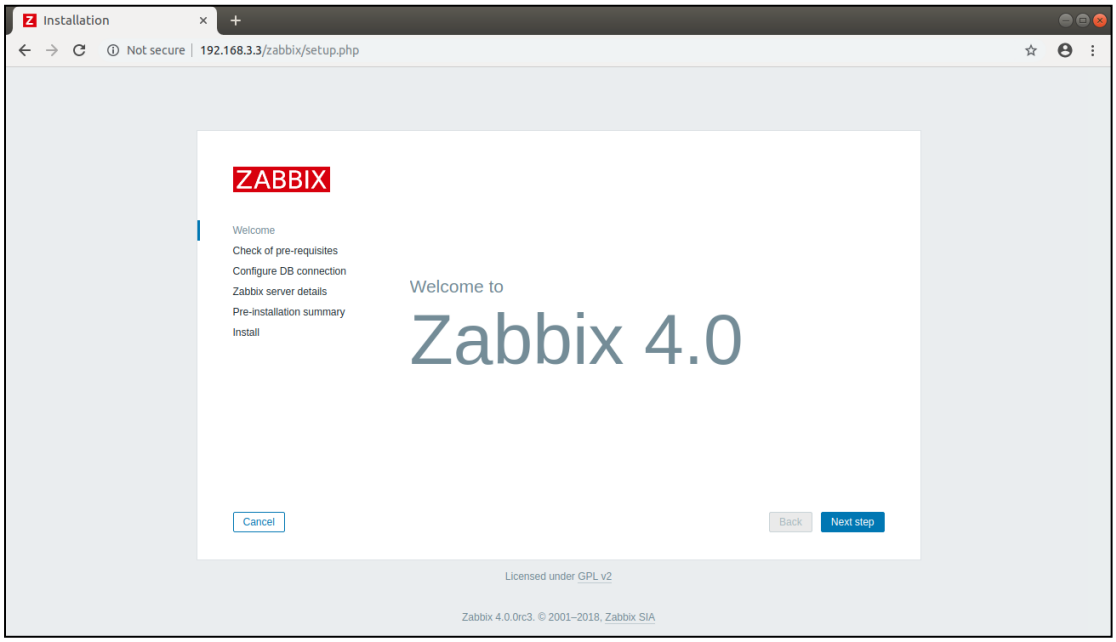


Figure 5.3.4 20 Zabbix welcome page

Step 2: Zabbix check of pre-requisites ensure that all of the dependencies are set up correctly. Then click “Next step”.

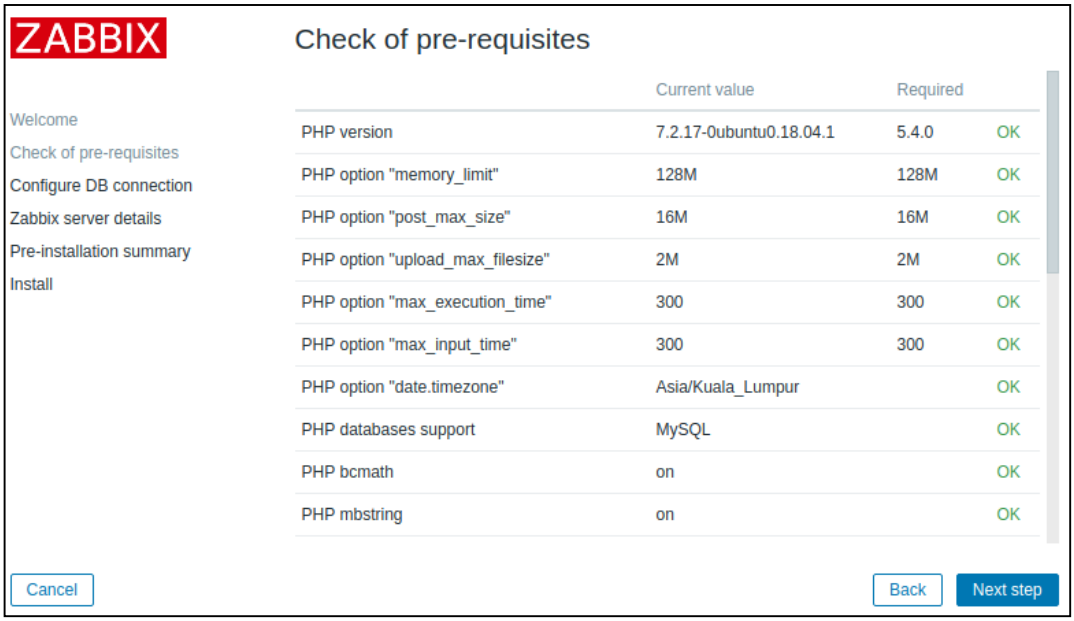


Figure 5.3.4 21 Zabbix check of pre-requisites page

Step 3: Zabbix Configure DB connection check all setting and select correct Database Engine you have installed during Zabbix Installation. In this case is MySQL is selected then click “Next step”.

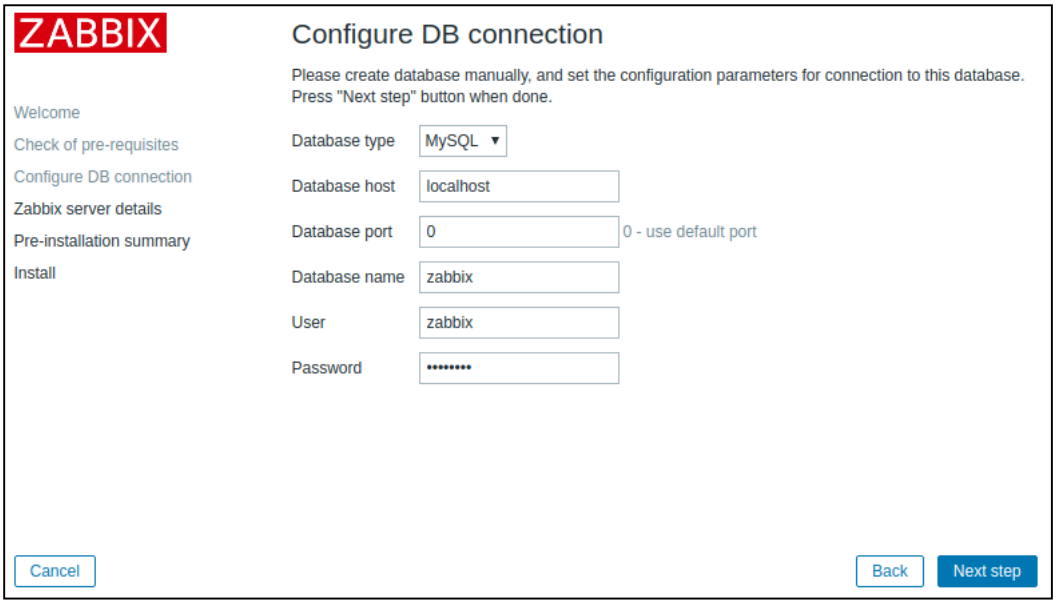


Figure 5.3.4 22 Zabbix configure DB connection page

Step 4: Check the hostname and port number on Zabbix Server details then click “Next step”.

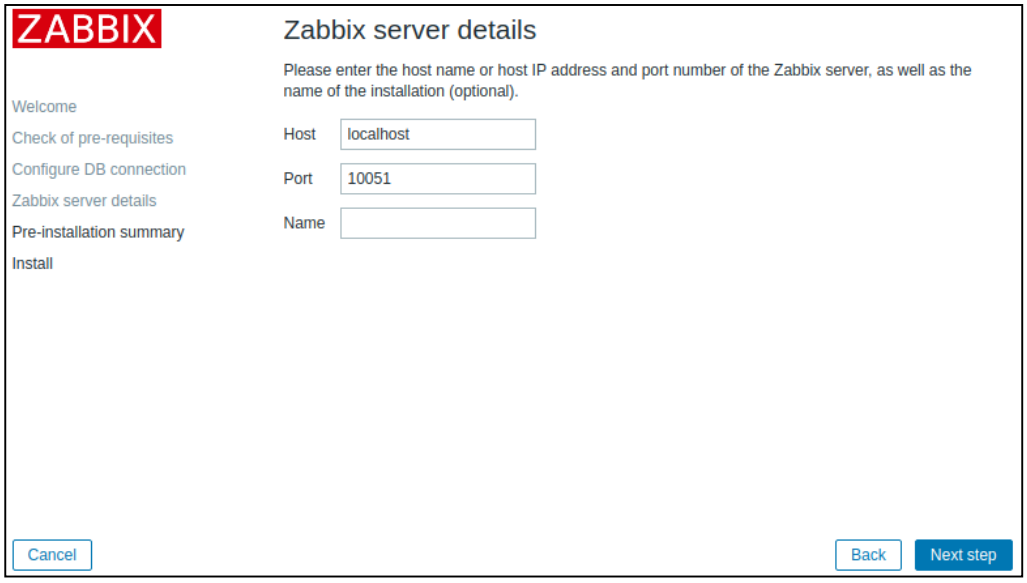


Figure 5.3.4 23 Zabbix server details page

Step 5: Check on Pre-installation summary and ensure that all settings are entered correctly then click “Next step”.

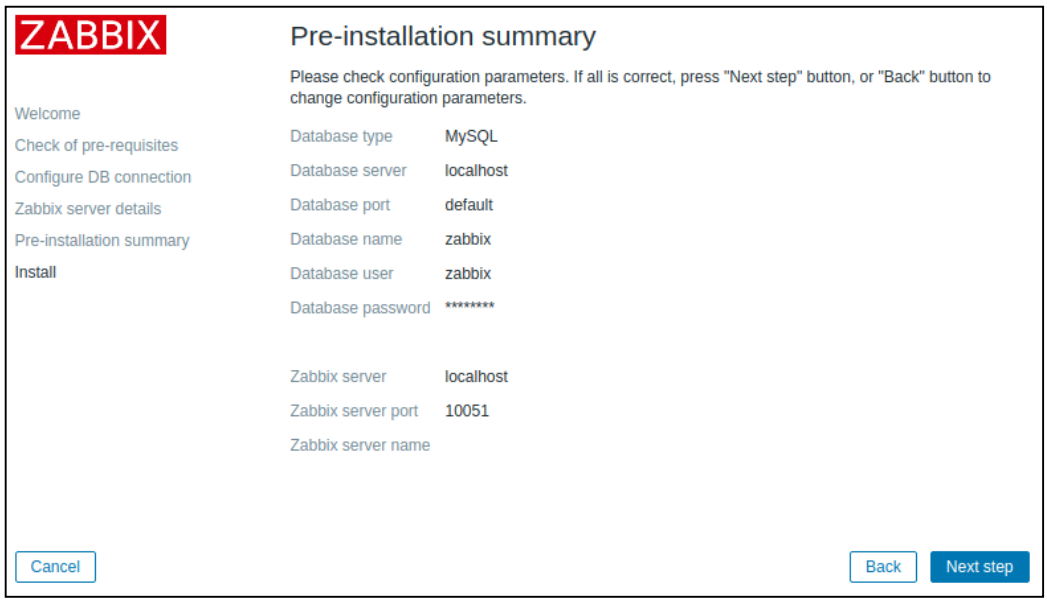


Figure 5.3.4 24 Zabbix pre-installation summary page

Step 6: When all configurations and installation are done, click “Finish” to finalize your installation.

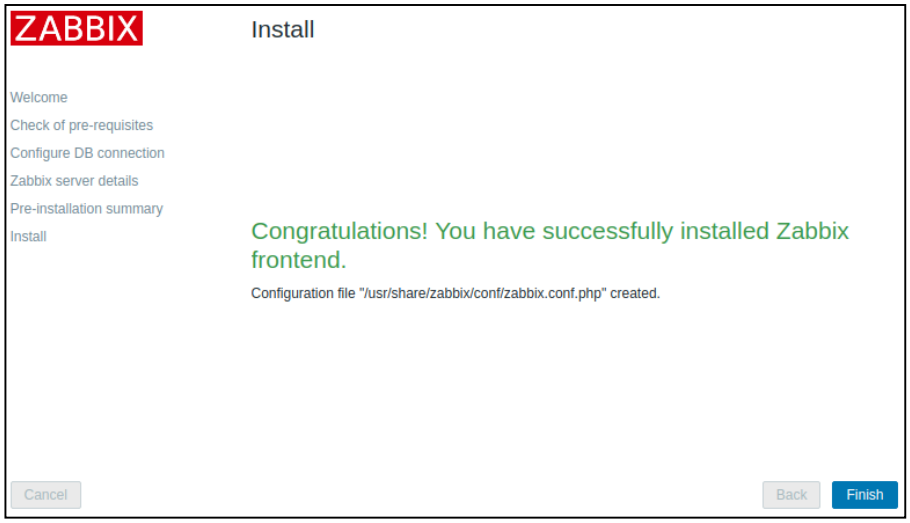


Figure 5.3.4 25 Zabbix install page

Step 7: After clicking finish, that will show the Login Page of Zabbix Server. Proceed to add your network hosts to the Zabbix Server.

Adding Network Hosts to Zabbix Server

Step 1: Log in to Zabbix Server by using default login account.

Username: Admin

Password: Zabbix

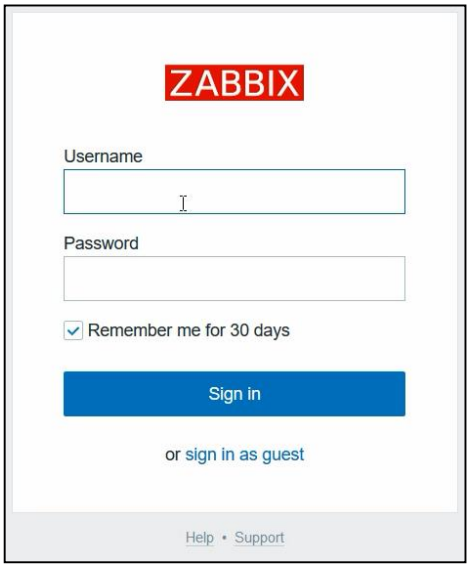


Figure 5.3.4 26 Zabbix login page display

Step 2: After login, that will show the Zabbix main page Dashboard.

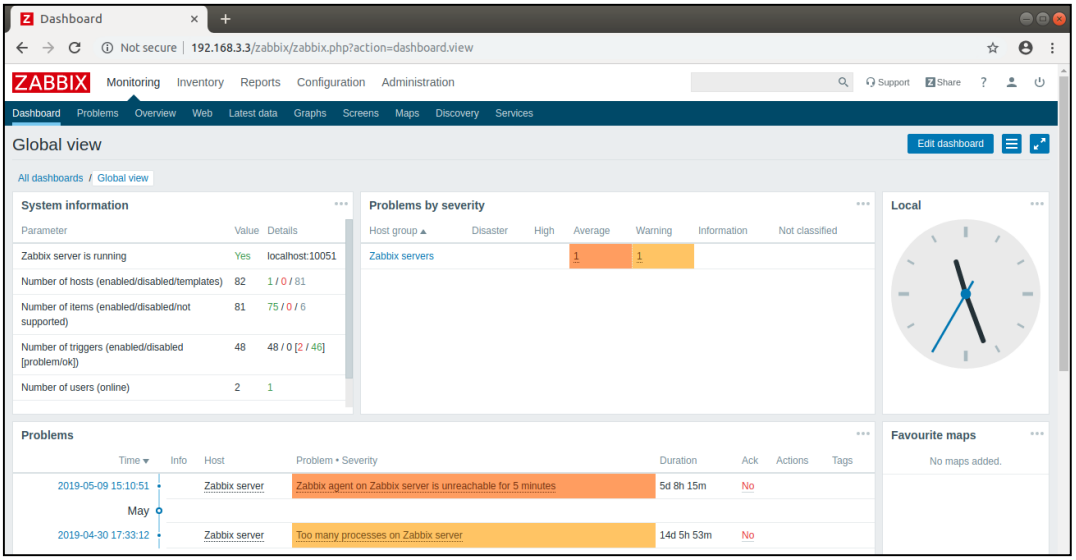


Figure 5.3.4 27 Zabbix main page

Step 3: To add new Network Hosts, first, click on “Configuration” tab, then, click on “Create host” button.

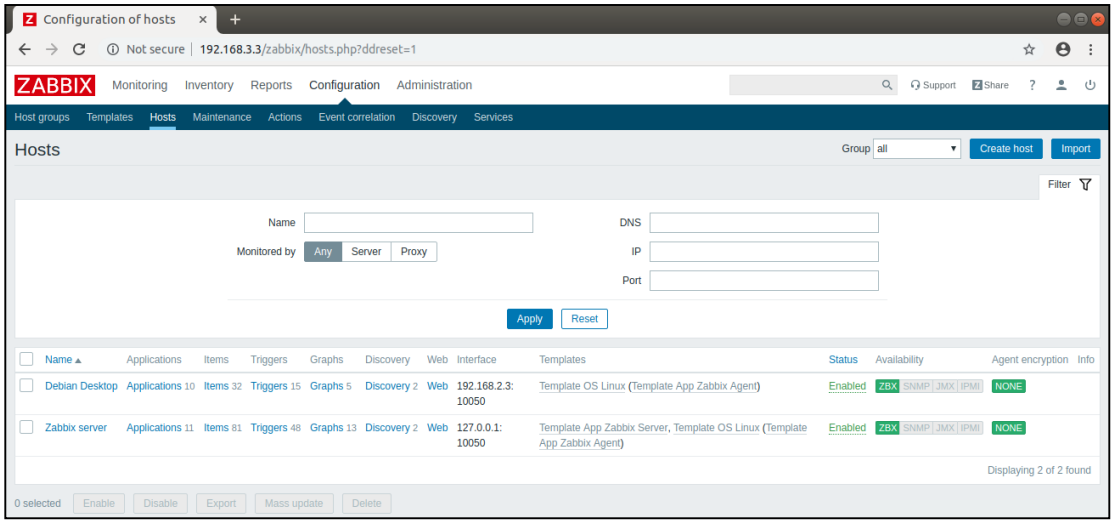


Figure 5.3.4 28 Zabbix hosts page

Step 4: Fill in the required forms for Zabbix Server to discover device on the network.

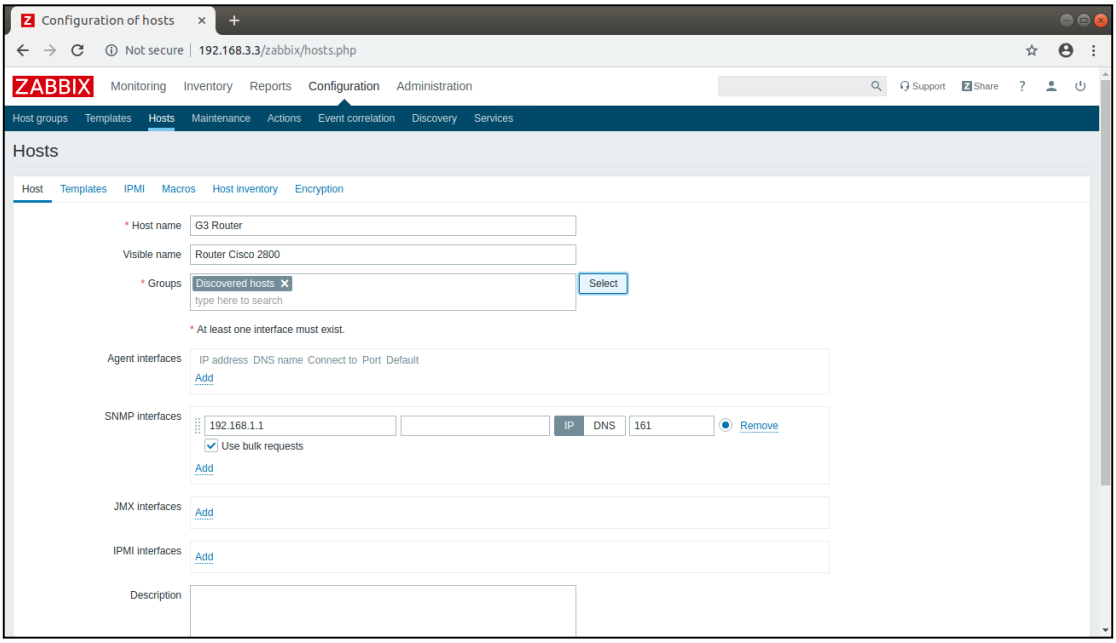


Figure 5.3.4 29 Zabbix add new hosts page

Step 5: Next, for Zabbix server to discover what service want to monitor, need to choose the preset templates. In this case, monitoring “Cisco’s Router”, need to choose “Template Net Cisco IOS SNMPv2”.

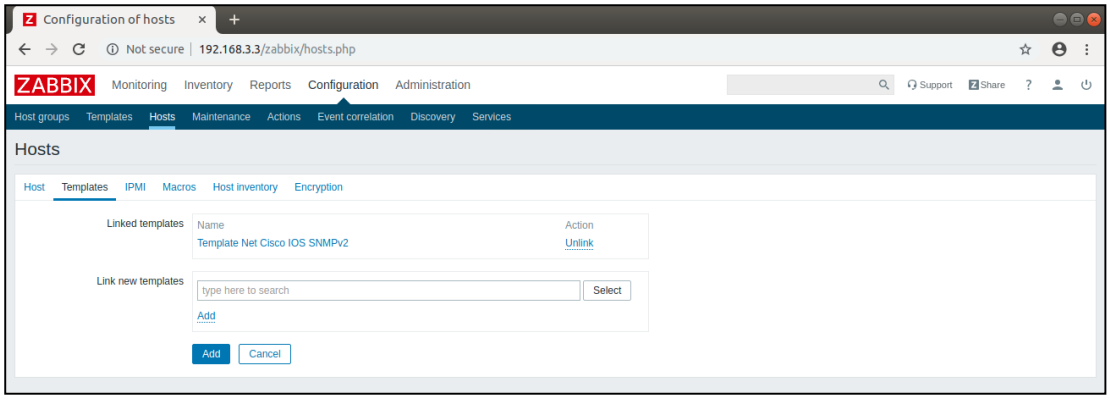


Figure 5.3.4 30 Zabbix host templates select page

Step 6: Install Zabbix Agent on Cisco devices, such as SNMP. Need to enable the Simple Network Management Protocol (SNMP) protocol.

snmp-server community G3 RW

Figure 5.3.4 31 Enable SNMP on Cisco Router

Step 7: Add macros for Zabbix Server can link with Zabbix Agent for SNMP.

{$SNMP_COMMUNITY}G3

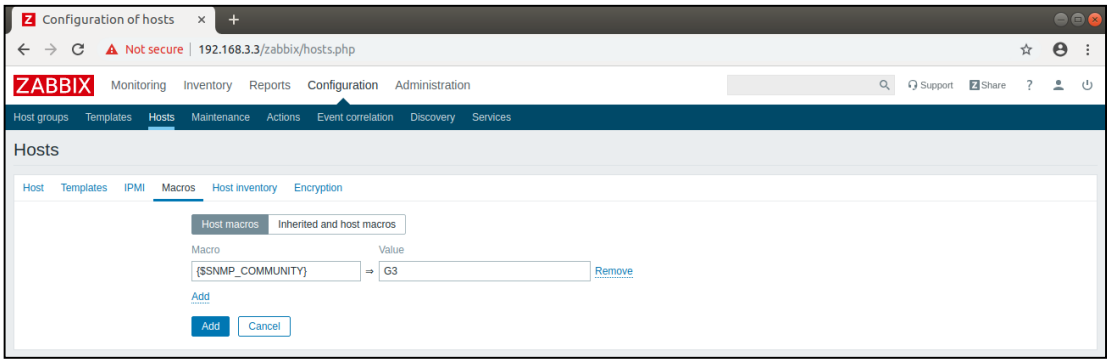


Figure 5.3.4 32 Zabbix host macros page

Step 8: When settings are setup correctly, all real time data of the devices as shown in the diagram below.

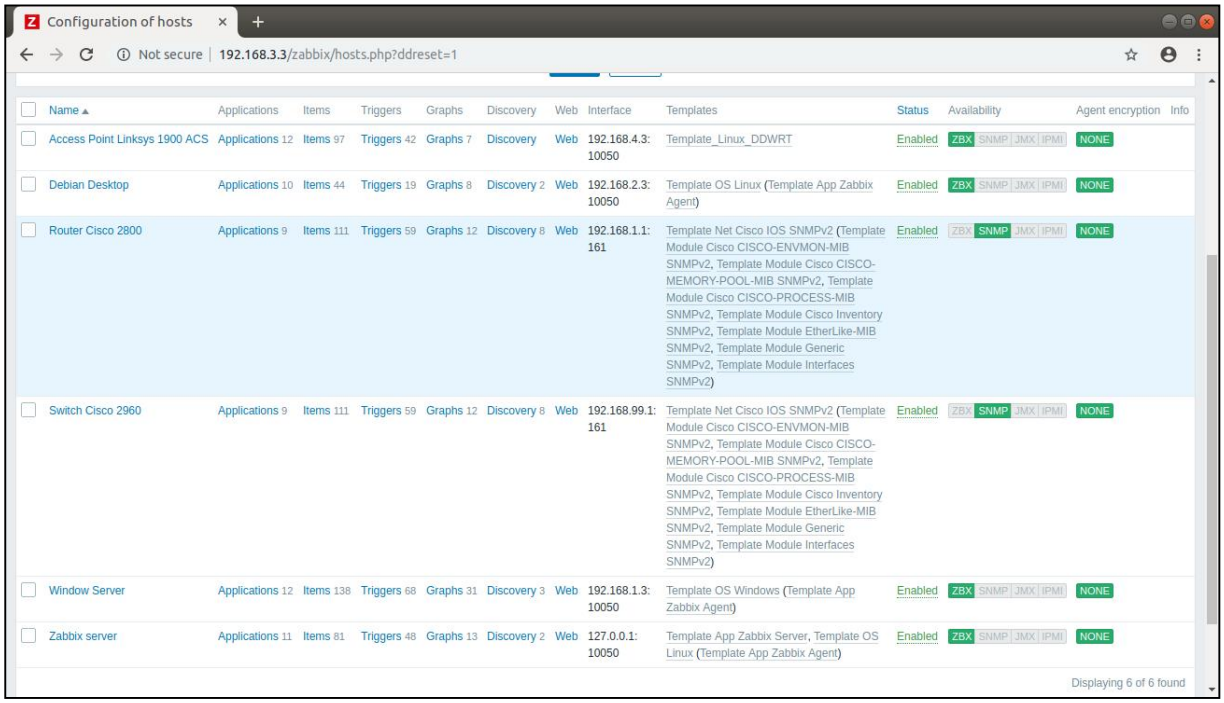


Figure 5.3.4 33 Zabbix hosts page

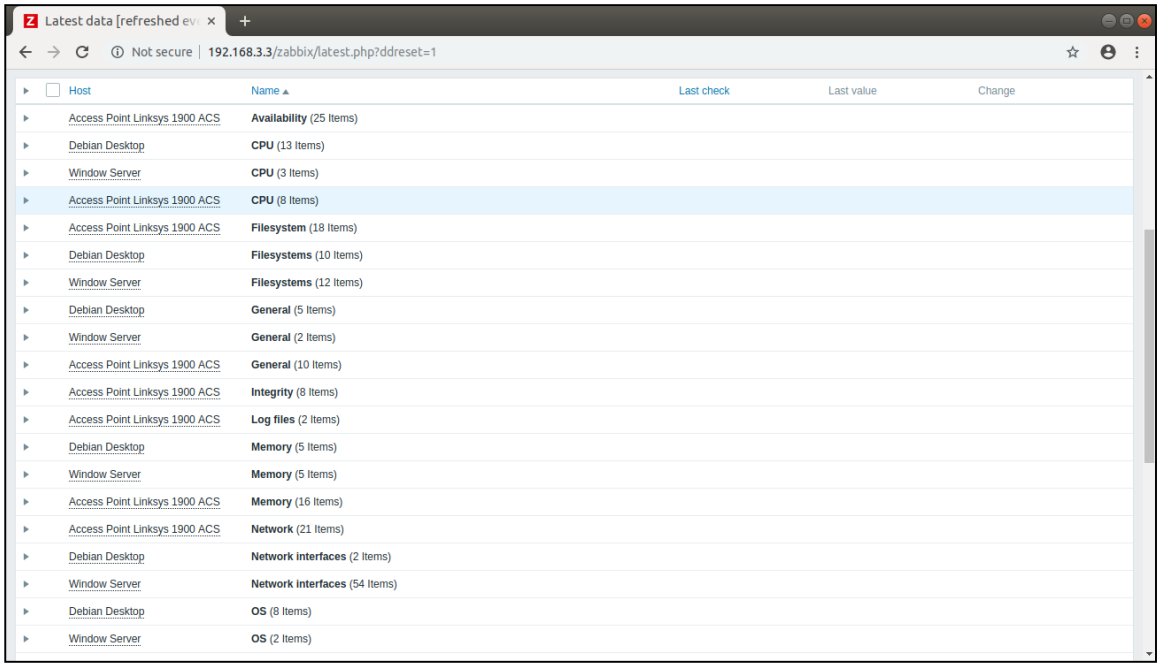


Figure 5.3.4 34 Zabbix device latest date page

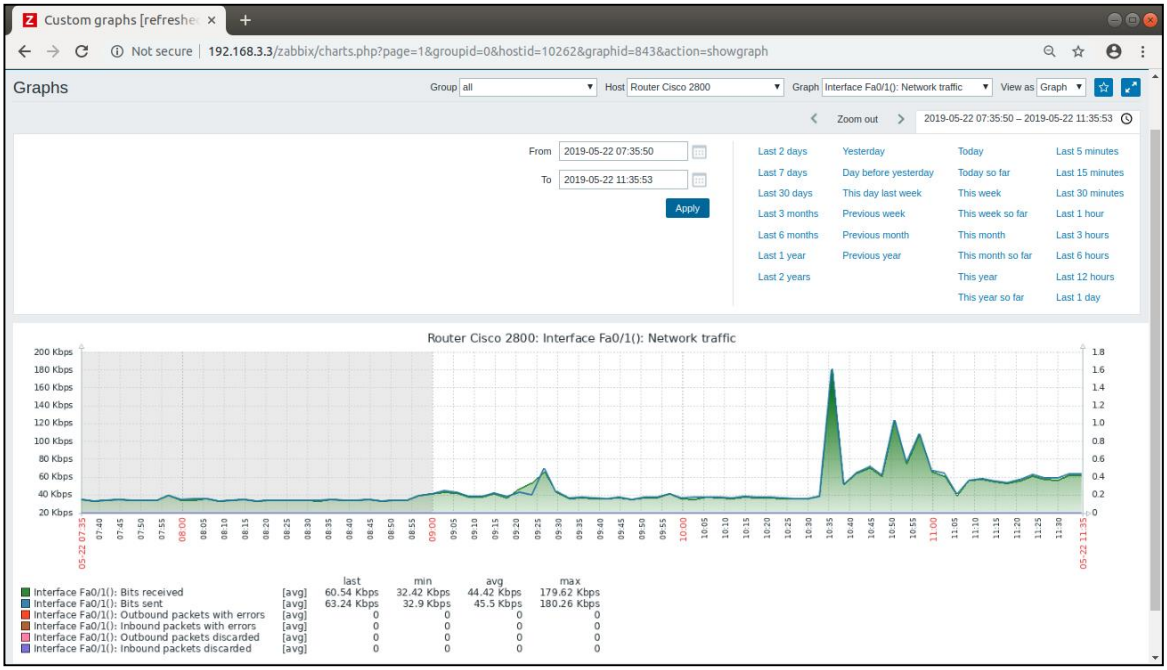


Figure 5.3.4 35 Zabbix graph page

Zabbix Agent Installation

Windows Server 2019 Zabbix Agent Installation

Step 1: Download latest Windows' Zabbix Agent installer from Zabbix's Official Website.

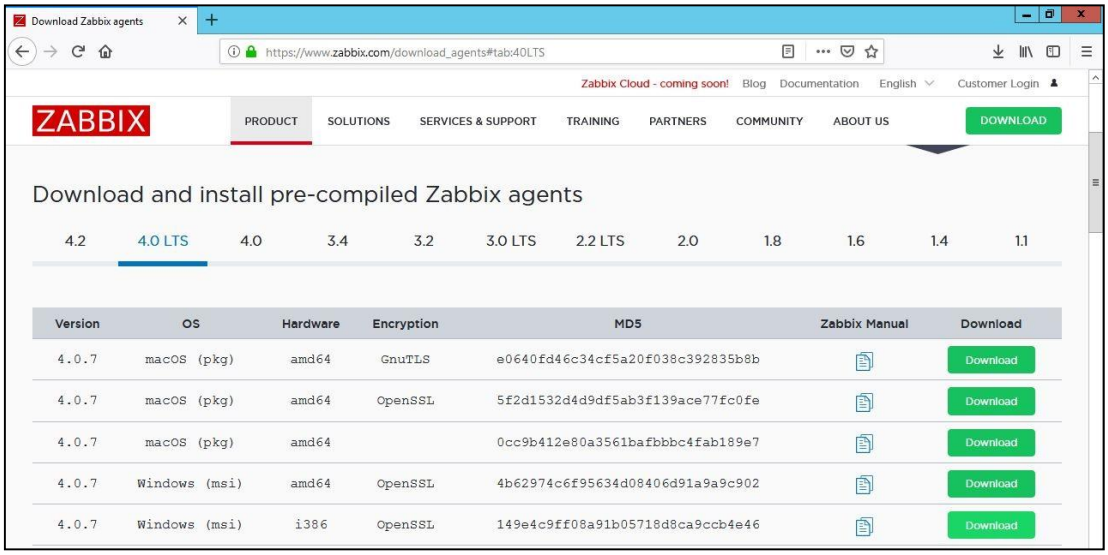


Figure 5.3.4 36 Zabbix Agent download page from Windows Server

Step 2: Open the Zabbix Agent (64-bit) Setup file then click "Next".

Figure 5.3.4 37 Zabbix Agent setup from Windows Server

Step 3: On End-User License Agreement tick the "I accept the terms in the License Agreement" then click "Next".

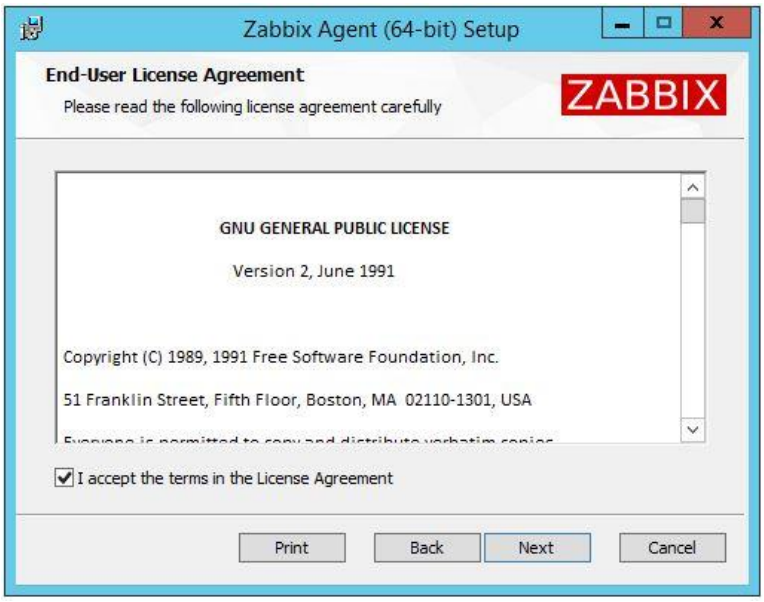


Figure 5.3.4 38 Zabbix Agent End-User License Agreement

Step 4: On Zabbix Agent service configuration change the hostname, Zabbix server IP/DNS, Agent listen port and Server or Proxy for active checks.

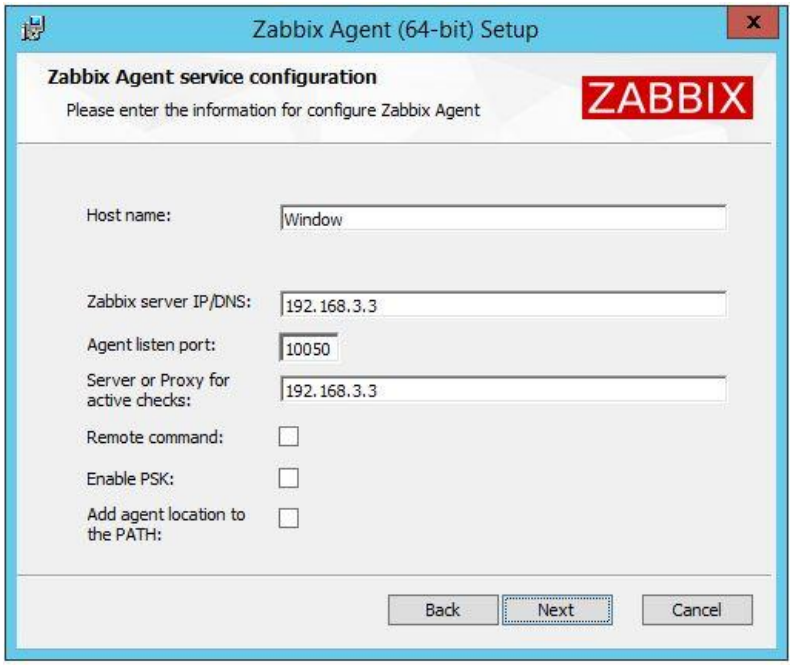


Figure 5.3.4 39 Zabbix Agent service configuration

Step 5: On Custom Setup select the Zabbix Agent (64-bit) then click “Next”.

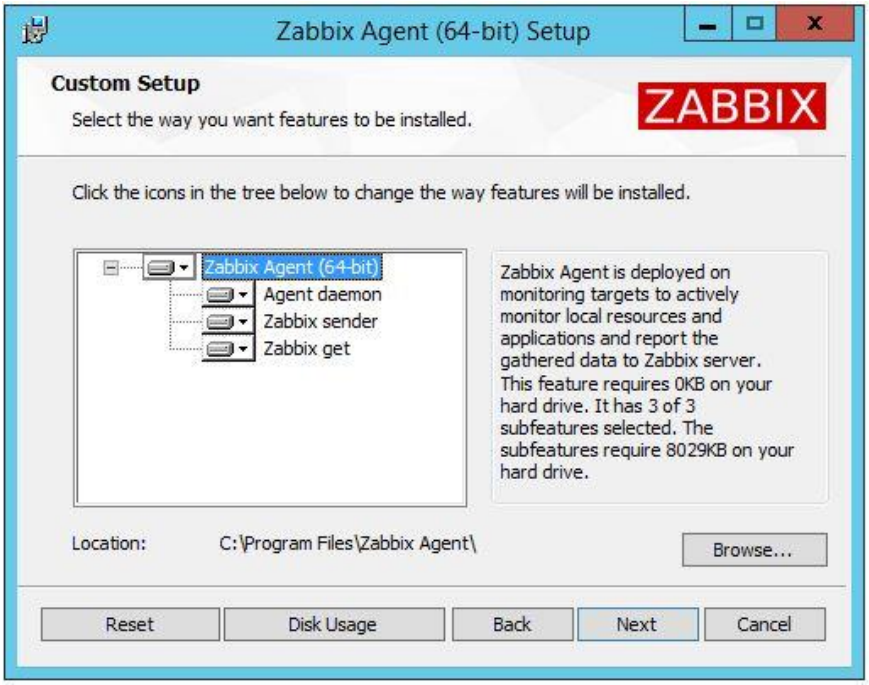


Figure 5.3.4 40 Zabbix Agent custom setup

Step 6: On Ready to install Zabbix Agent (64-bit) click “Install” to install the Zabbix Agent.

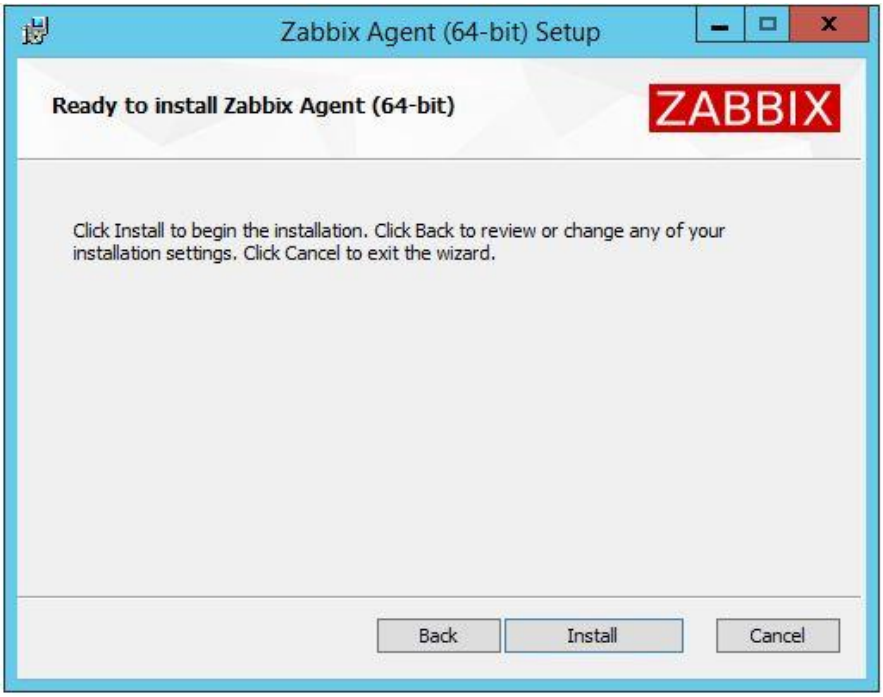


Figure 5.3.4 41 Zabbix Agent install

Step 7: After Completed the Zabbix Agent (64-bit) Setup Wizard then click “Finish” to finish the installation.

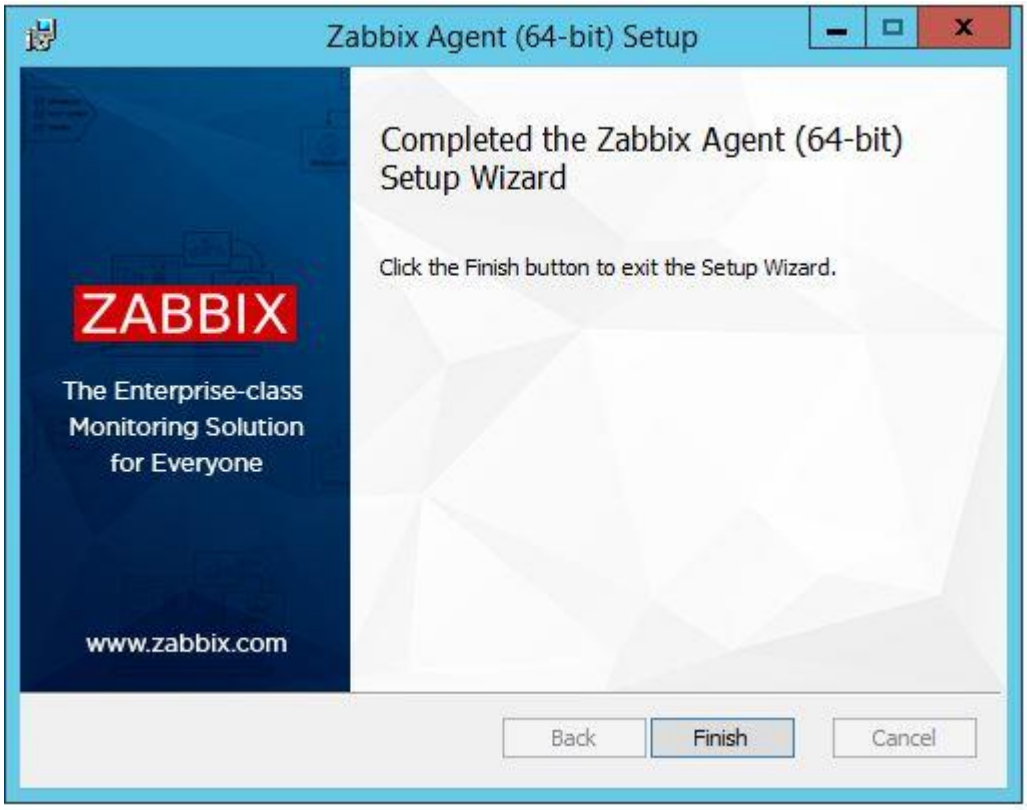


Figure 5.3.4 42 Zabbix Agent completed setup

Debian Zabbix Agent Installation

Step 1: Install Zabbix Agent.

apt install zabbix-agent

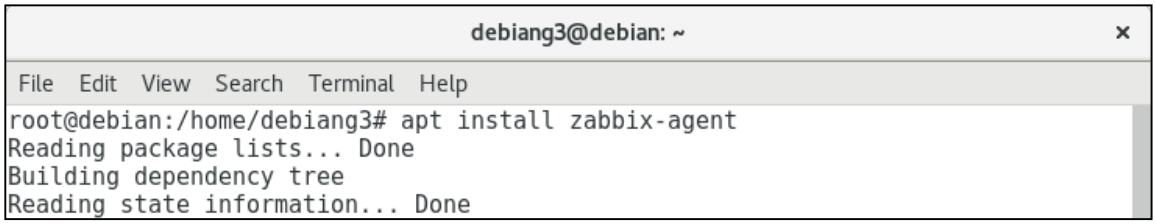


Figure 5.3.4 43 Install Zabbix Agent

Step 2: Configure zabbix agent file.

nano /etc/zabbix_agentd.conf

Figure 5.3.4 44 Configure Zabbix Agent file

Step 3: Change the config into zabbix_agentd.conf file.

Server=192.168.3.3

ServerActive=192.168.3.3

Hostname=Debian

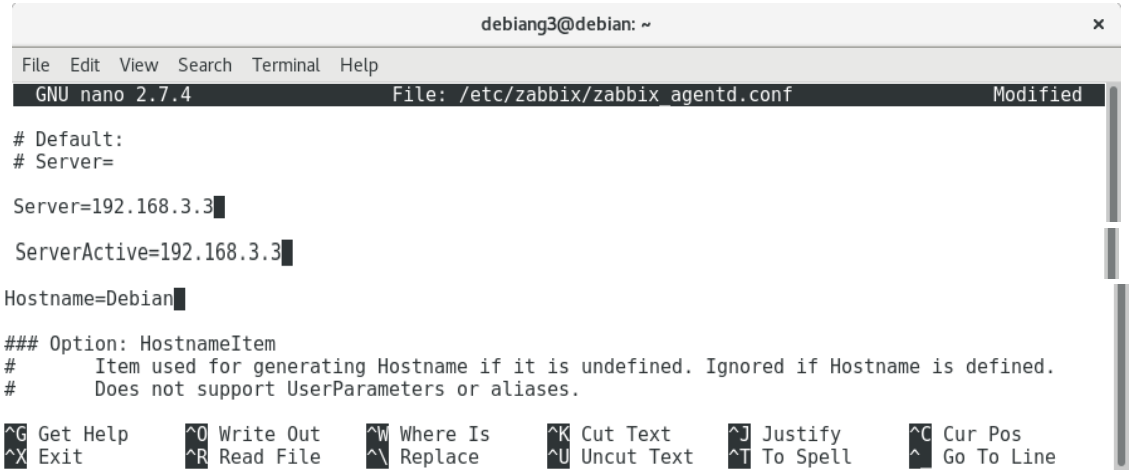


Figure 5.3.4 45 Configure Zabbix Agent file

Step 4: Restart Zabbix Agent service for the configuration file to be overwritten.

service zabbix-agent restart

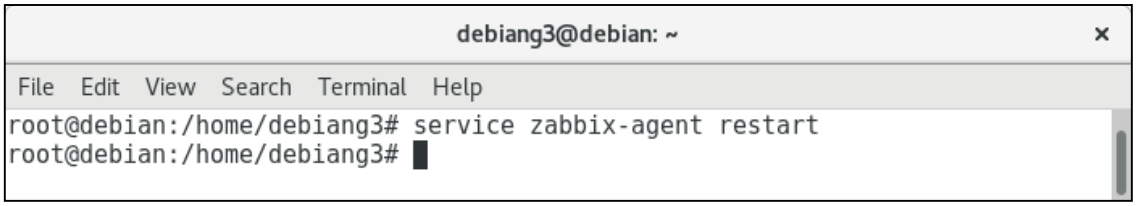


Figure 5.3.4 46 Restart Zabbix Agent

5.3.5 Routing & NAT

i. Routing

Step 1: Define an IP address in the Se0/2/0. Then create the default routing to route two network.

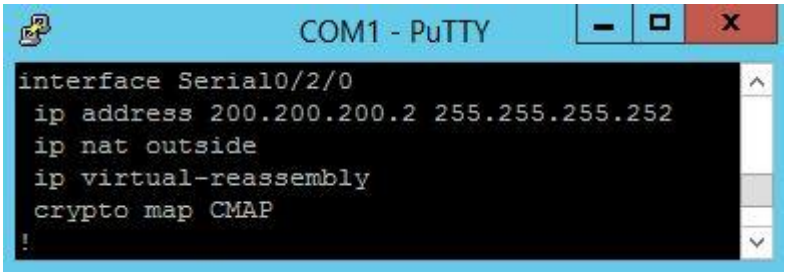


Figure 5.3.5 1 Default Route

ii. Network Address Translation (NAT)

Step 1: Setup s0/2/0 as NAT outside**.**

```
Group3Router(config-subif)#int s0/2/0
Group3Router(config-if)#ip nat outside
```

Figure 5.3.5 2 Set up NAT

Step 2: Used command below to configure static NAT for the three server.

```
ip nat inside source static 192.168.3.3 200.200.200.18
ip nat inside source static 192.168.1.3 200.200.200.21
ip nat inside source static 192.168.2.3 200.200.200.22
```

Figure 5.3.5 3 Set up static NAT

Step 3: Setup fa0/1 as NAT inside and all-sub interface as ***NAT inside***.

```
Group3Router(config)#int fa0/1.10
Group3Router(config-subif)#ip nat inside
Group3Router(config-subif)#int fa0/1.20
Group3Router(config-subif)#ip nat inside
Group3Router(config-subif)#int fa0/1.30
Group3Router(config-subif)#ip nat inside
Group3Router(config-subif)#int fa0/1.40
Group3Router(config-subif)#ip nat inside
```

Figure 5.3.5 4 Identify the inside interfaces

Step 4: Used command below to configure dynamic NAT to the client.

access-list 1 permit 192.168.4.0 0.0.0.255

ip nat pool G3 200.200.200.19 200.200.200.20 netmask 255.255.255.248

ip nat inside source list 1 pool G3

```
access-list 1 permit 192.168.4.0 0.0.0.255
```

Figure 5.3.5 5 Standard Access-List

```
ip nat pool G3 200.200.200.19 200.200.200.20 netmask 255.255.255.248
ip nat inside source list 1 pool G3
```

Figure 5.3.5 6 Configure dynamic NAT

5.3.6 Proxy Server

Step 1: Install the squid package.

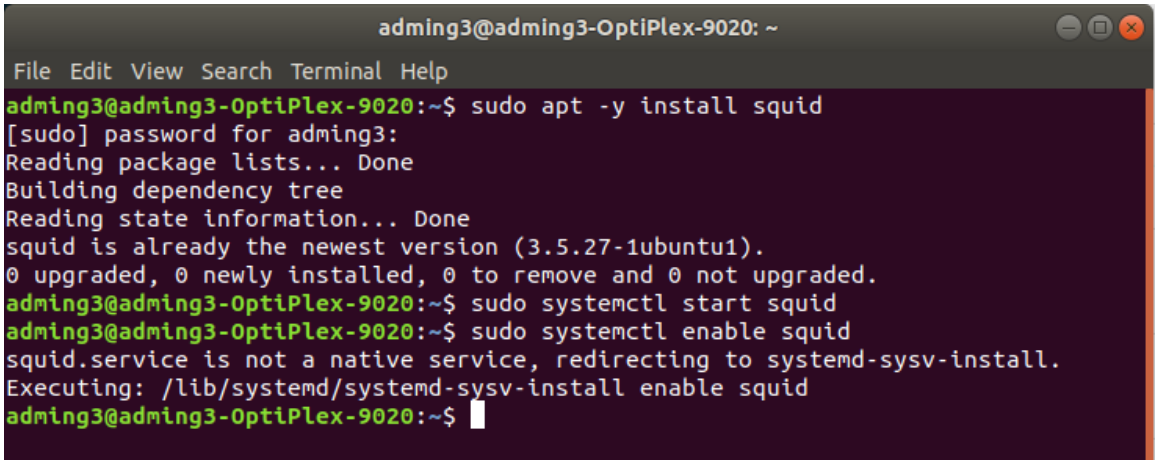


Figure 5.3.6 1 Install squid packages

Step 2: Check status the squid package.

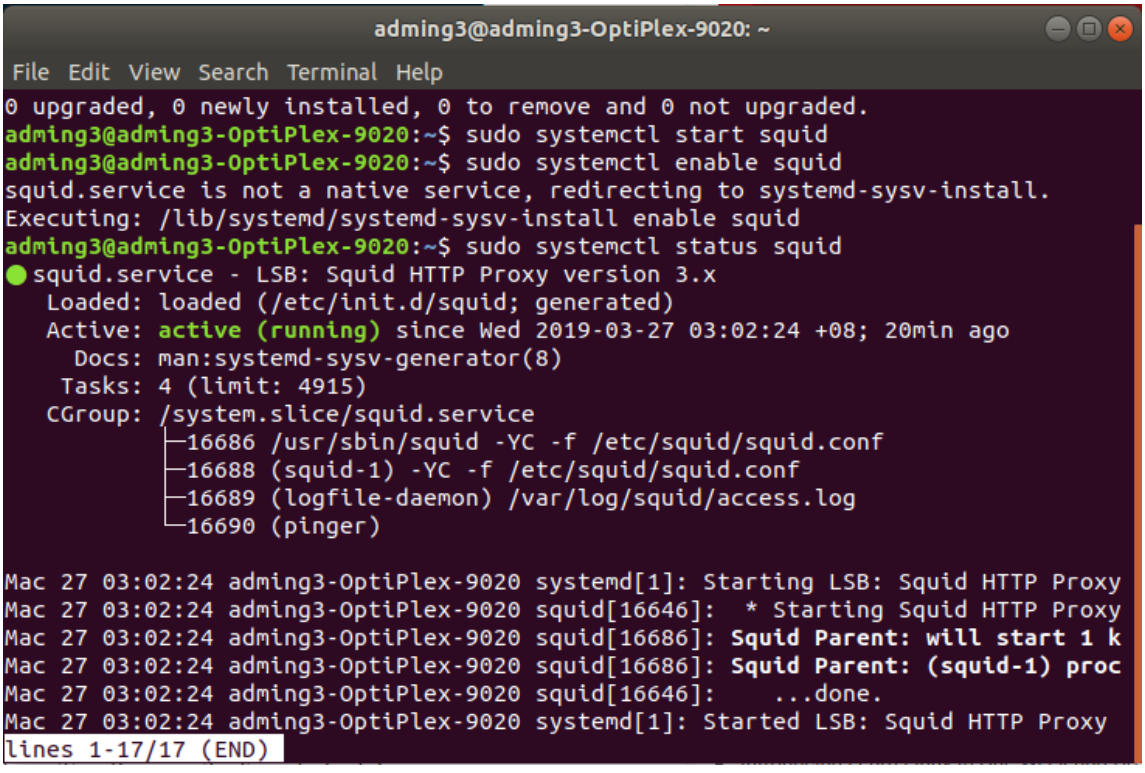


Figure 5.3.6 2 Check status the squid package

Step 3: Edit the configuration file of squid.

sudo gedit /etc/squid/squid.conf

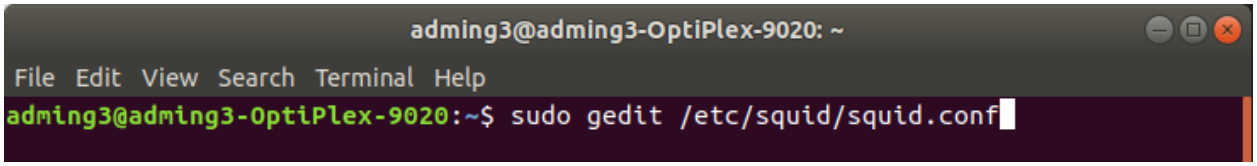


Figure 5.3.6 3 Edit ACL command on configuration file

Step 4: List all the website that will be block.

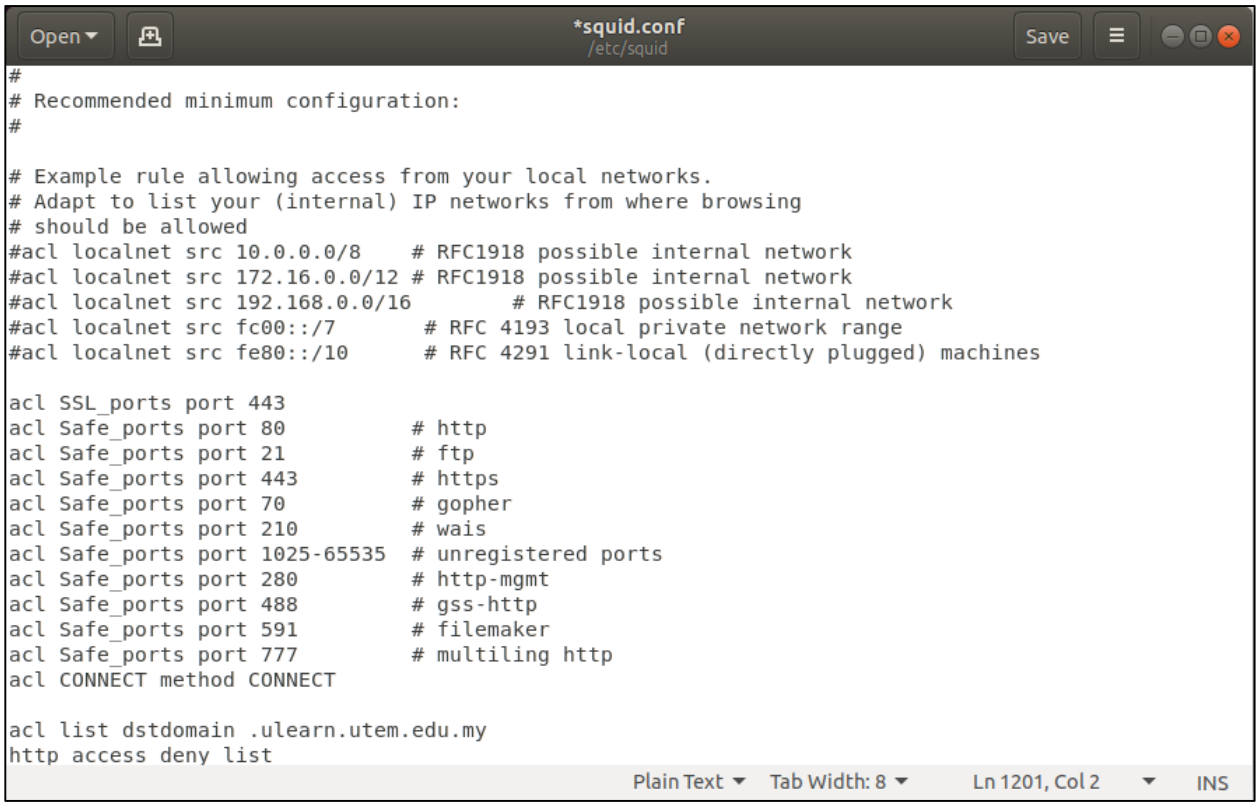


Figure 5.3.6 4 The list of blocking website

Step 5: Change ‘deny’ all to ‘allow’ all.

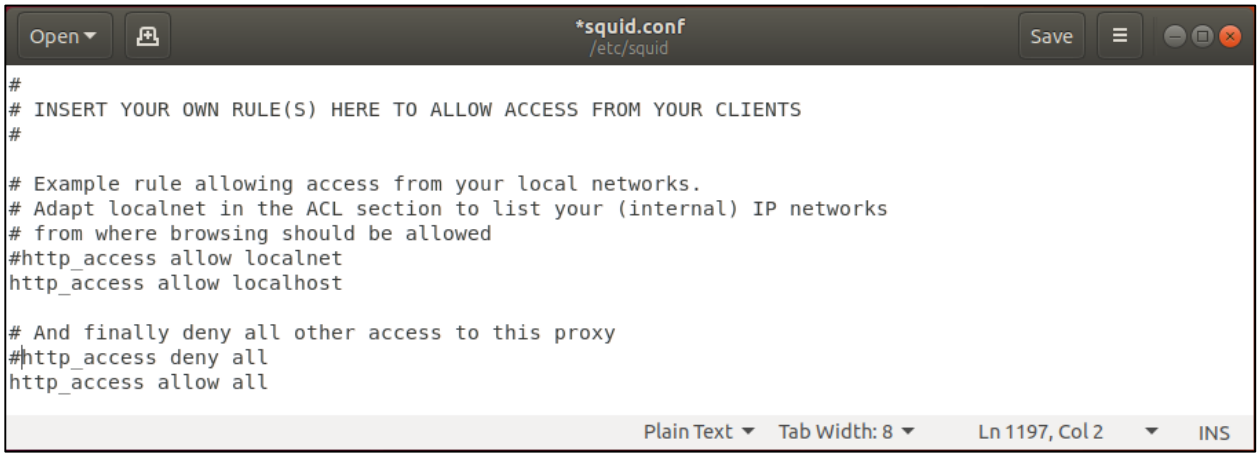


Figure 5.3.6 5 Change http_access

Step 6: restart the squid proxy.

sudo systemctl restart squid.

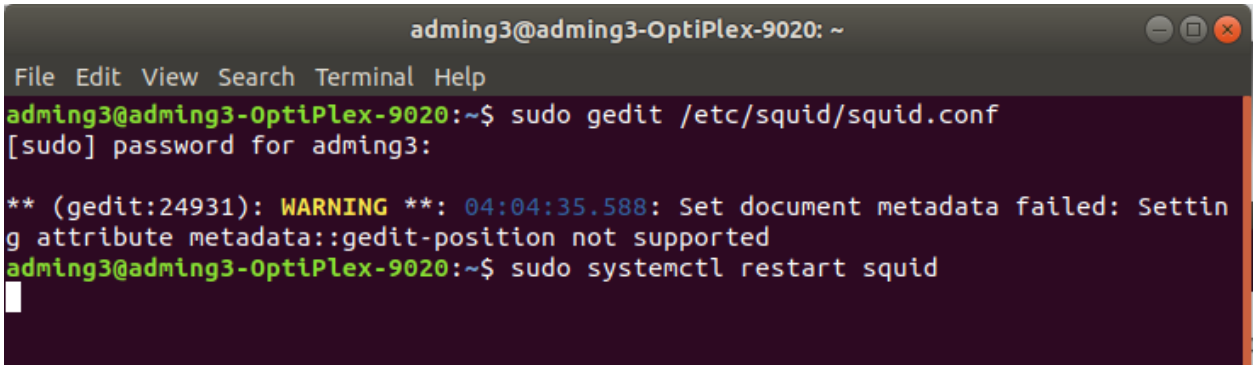


Figure 5.3.6 6 Restart service squid

Step 7: Open the Browser.

Step 8: At the top right bar, click and select “Preferences” option.

Step 9: Select “Advance” option, “Network” and “Setting” button.

Step 10: Select “Manual proxy configuration” and fill in as below.

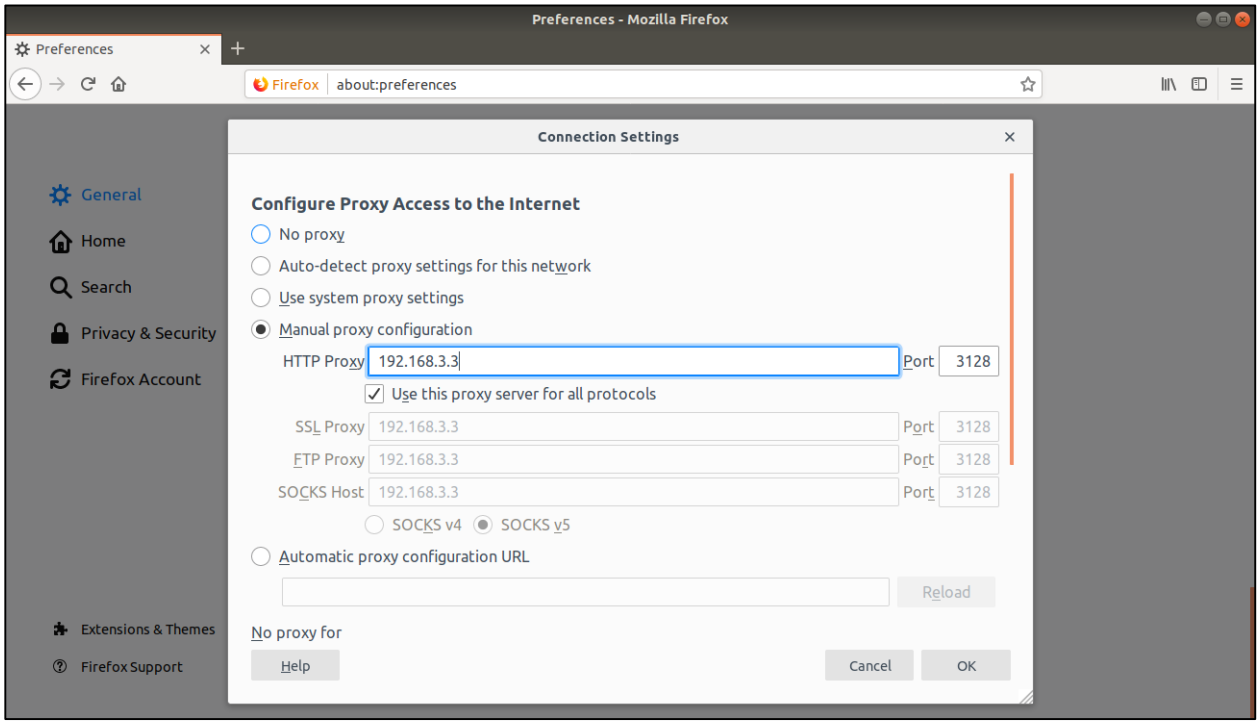


Figure 5.3.6 7 Setting IP proxy server at browser

5.3.7 Authentication, Authorization, Accounting (AAA)

In this case I'm using Windows Server 2012 R2

Step 1: open server manager, select "Roles" and click "Add Roles". Then go to Server Roles and click on "Network Policy and Access Services" and click "Next" to continue.

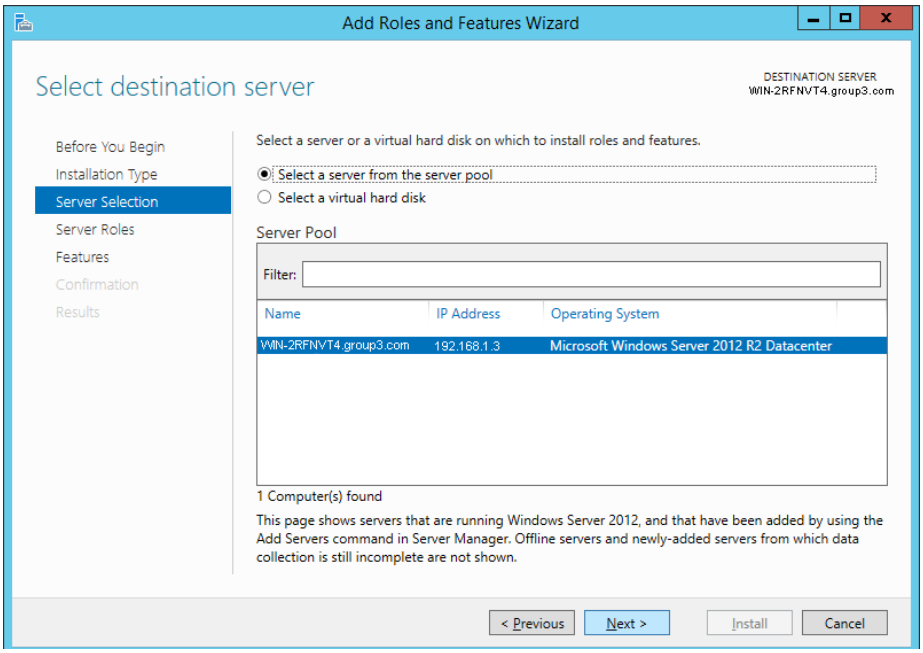


Figure 5.3.7 1 Select a server from the server pool

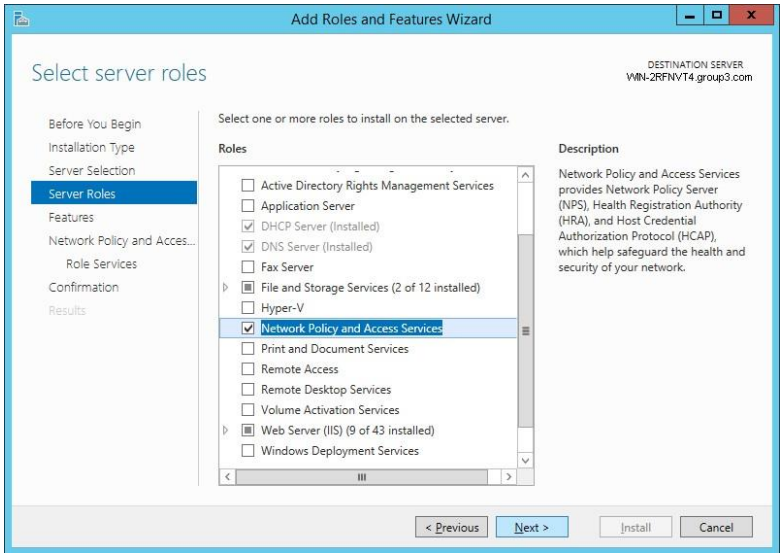


Figure 5.3.7 2 Add roles and features for AAA

Step 2: Go to Role Services and click "Network Policy Server" and "Routing and Remote Access Services" then click "Next".

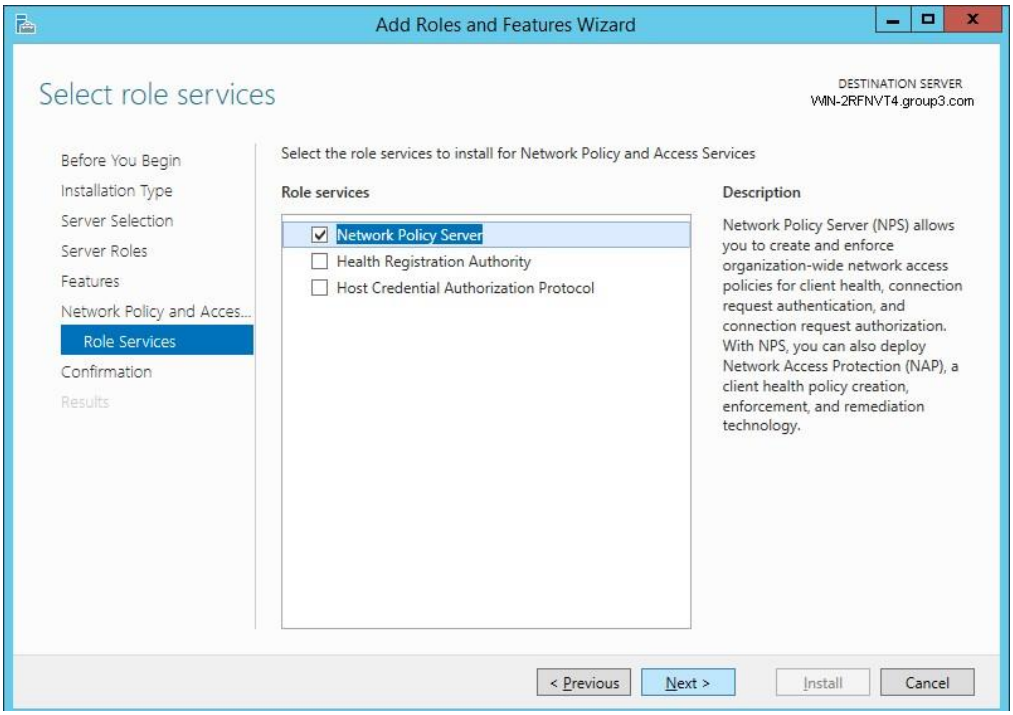


Figure 5.3.7 3 Add roles service NPS for AAA

Step 3: Confirm all the configure that done above and then click install. After that it will show a finish sign.

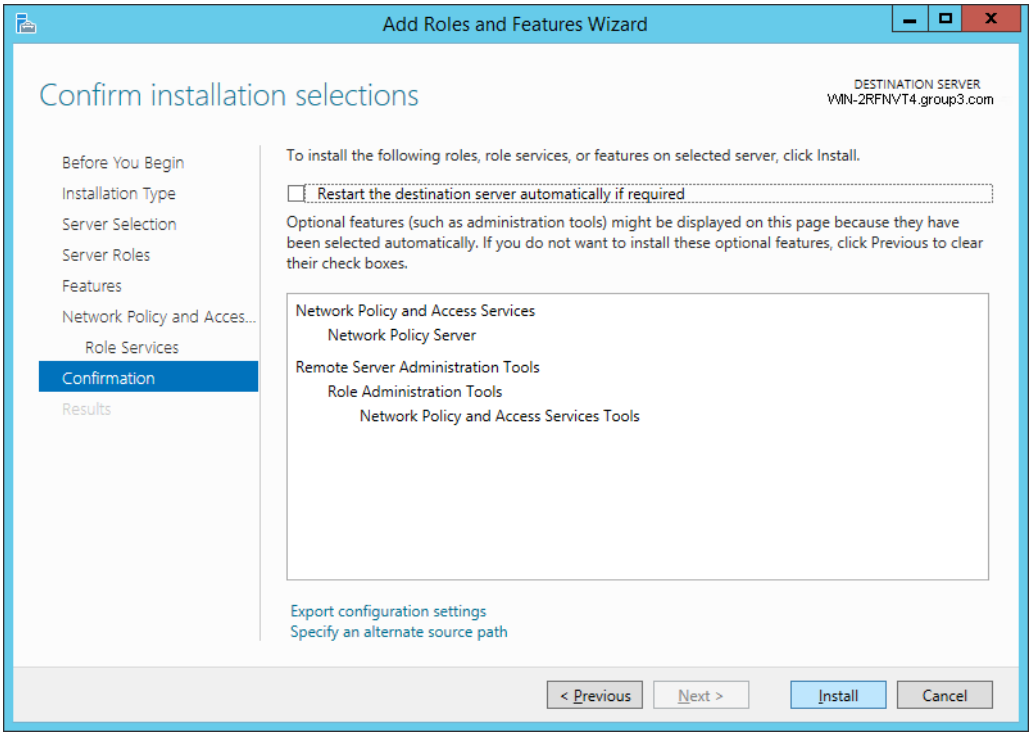


Figure 5.3.7 4 Confirm installation selections for AAA Roles

Step 4: Create a new group; in this case I'm using Radius Users as group name.

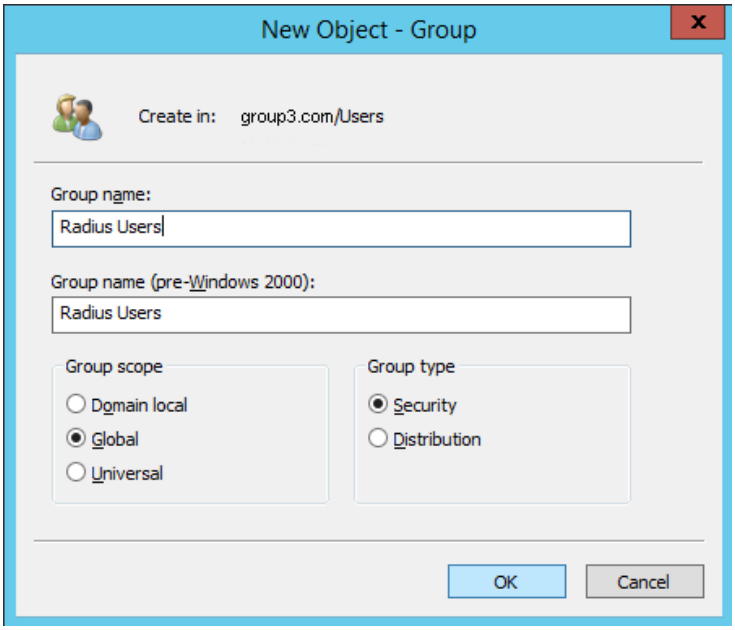


Figure 5.3.7 5 Creating a new group object for AAA

Step 5: Create a user's then we have to link to the group that we just created. In this installation I'm created radius user.

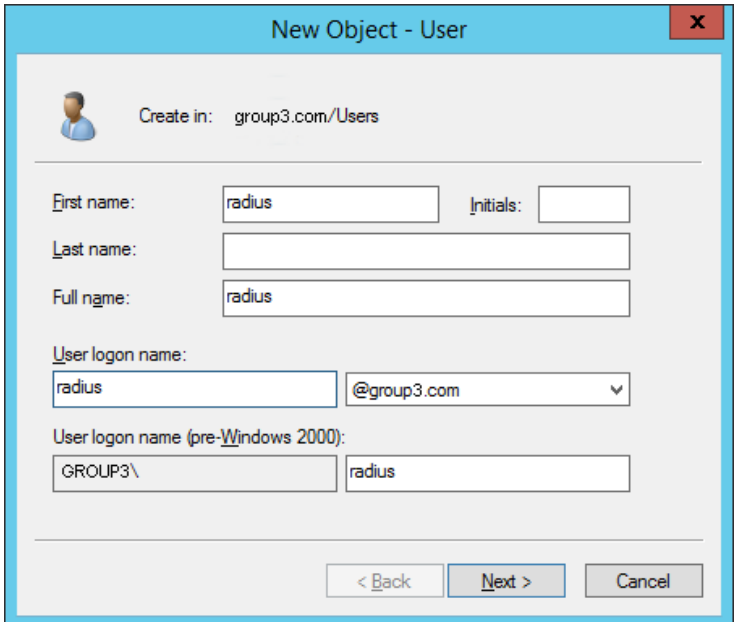


Figure 5.3.7 6 Creating new users for AAA

Step 6: Don't forget to input some password to those users.

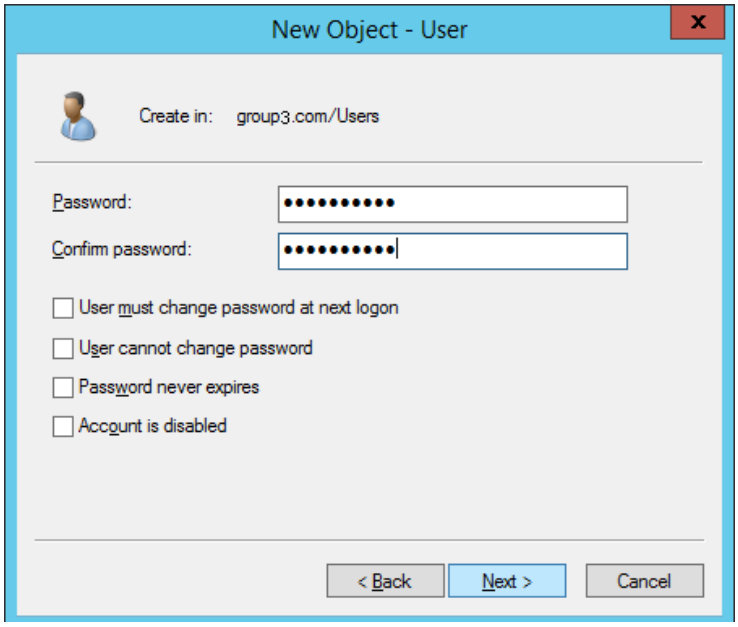


Figure 5.3.7 7 Insert a new password for the new user AAA

Step 7: After all the above process is done, it will prompt this dialog, click Finish.

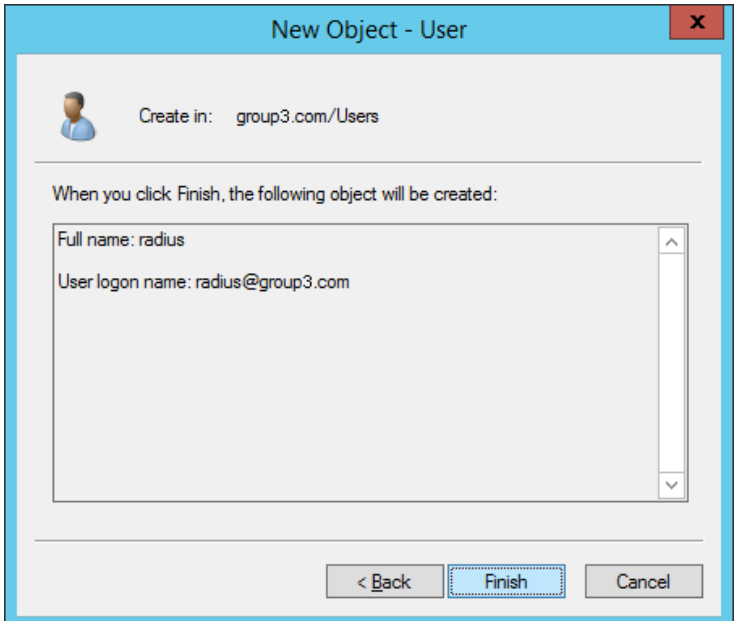


Figure 5.3.7 8 Adding new users finished for AAA

Step 8: After that create AAA in DNS Manager, click New Host (A or AAAA).

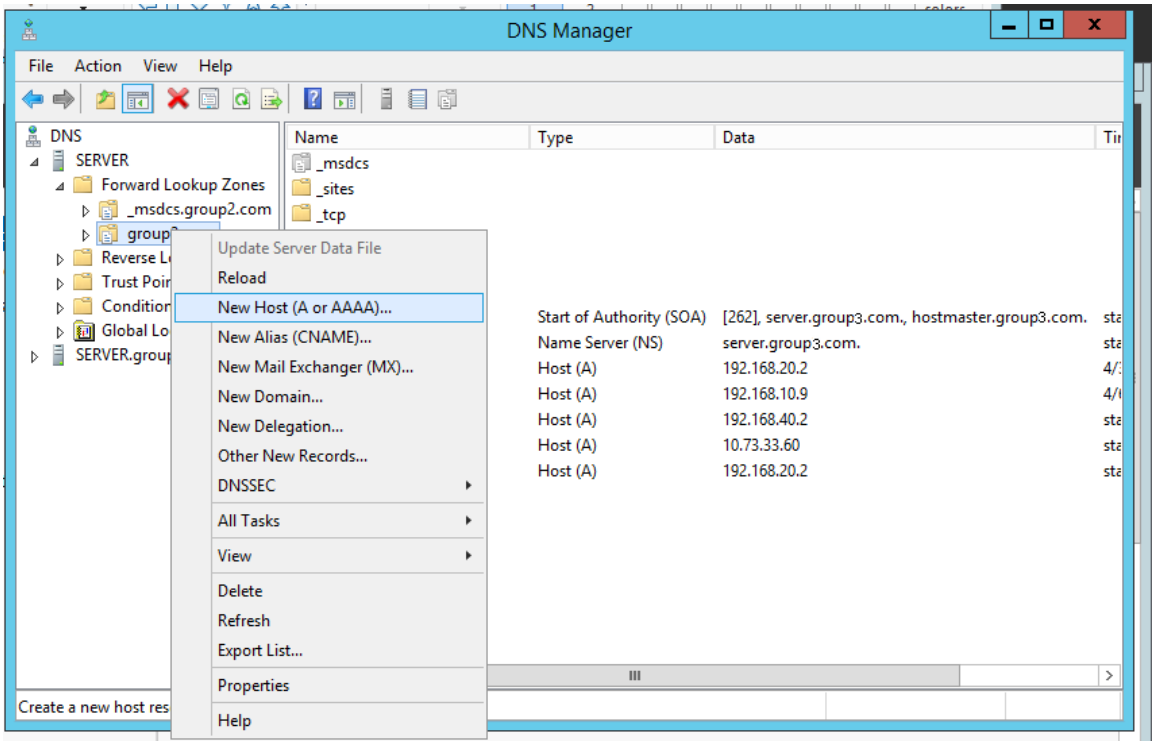


Figure 5.3.7 9 Creating new host for AAA

Step 9: Insert the router name along with its IP address, in this case, router name is Group3Router and its IP address is 192.168.1.1

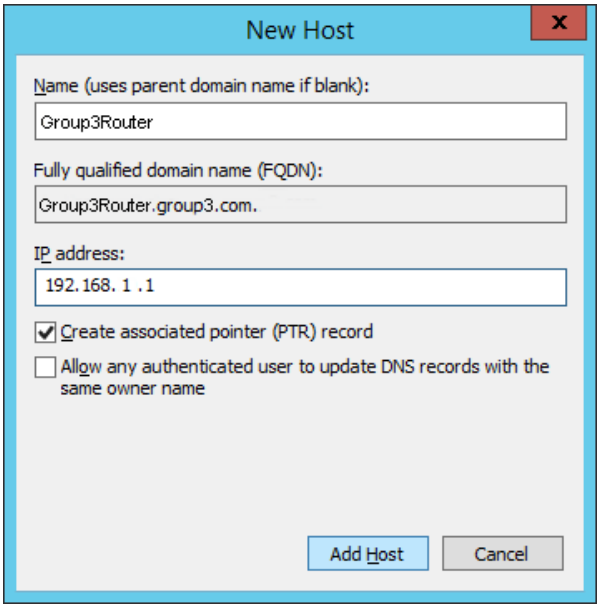


Figure 5.3.7 10 Insert router names and IP address for AAA

Step 10: After that, go to the Network Policy Server and right click the NPS (Local) and then click Register server in Active Directory.

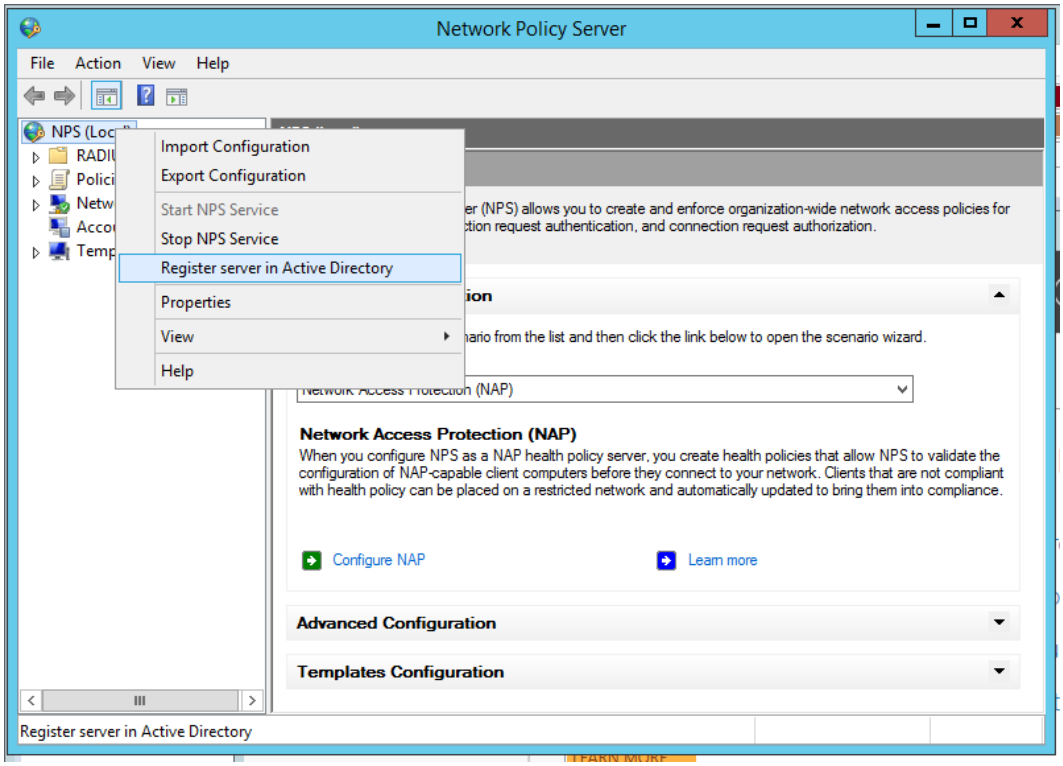


Figure 5.3.7 11 Register the NPS to the Active for AAA

Step 11: And then create a new Radius Client, right click to the Radius Client and click New.

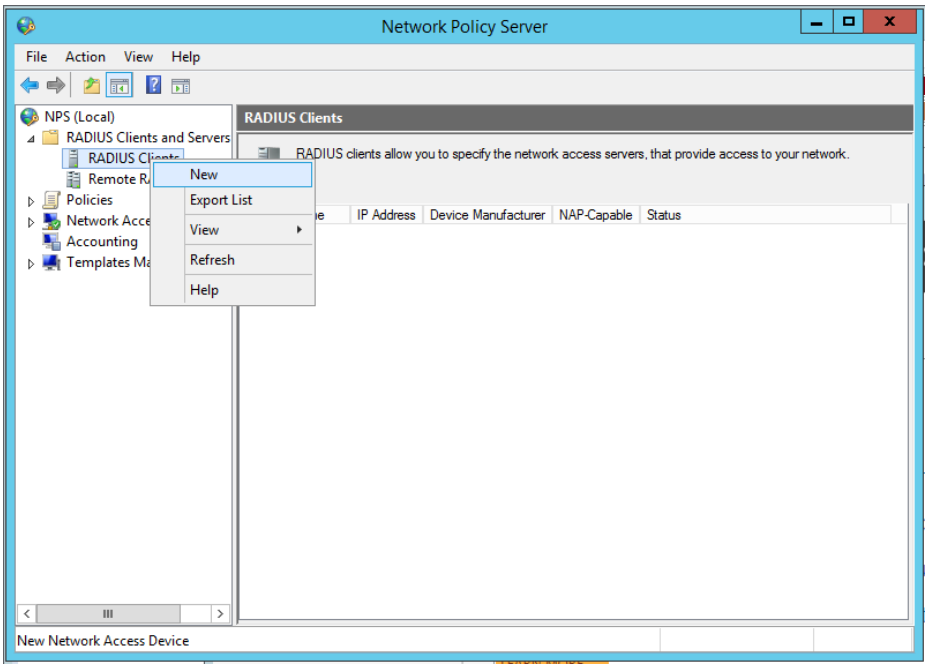


Figure 5.3.7 12 Create a new Radius client for AAA

Step 12: After that we have to insert some information about the client such as its name and password.

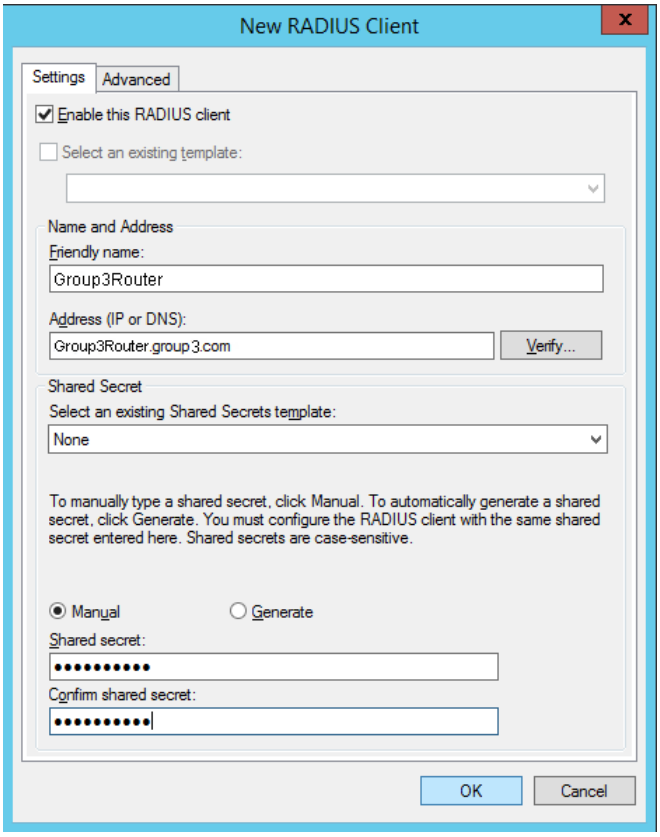


Figure 5.3.7 13 Insert router name and IP address for AAA

Step 13: Next click Verify to verify and solve the address that you inserted, it will show the IP address of the router.

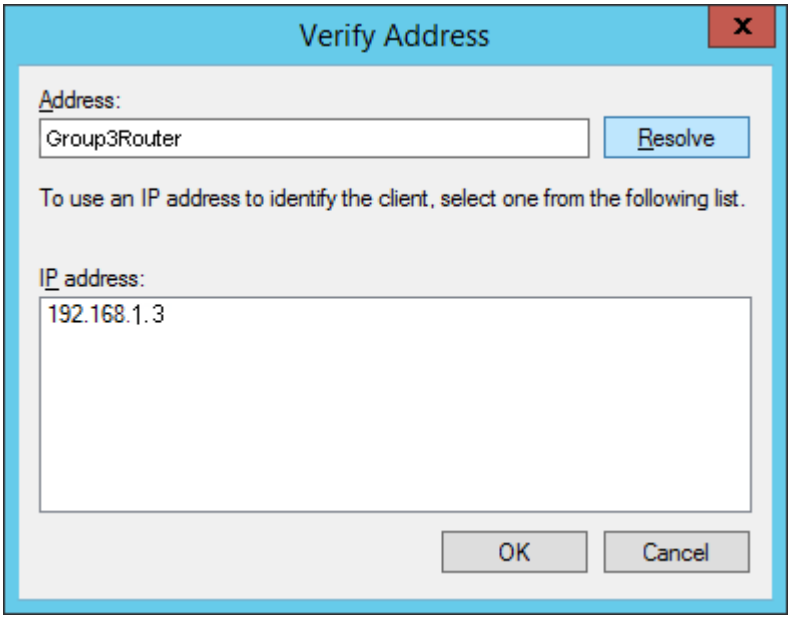


Figure 5.3.7 14 Resolve router name to get IP for AAA

Step 14: After finish all the configuration above, we can check our router name in radius client.

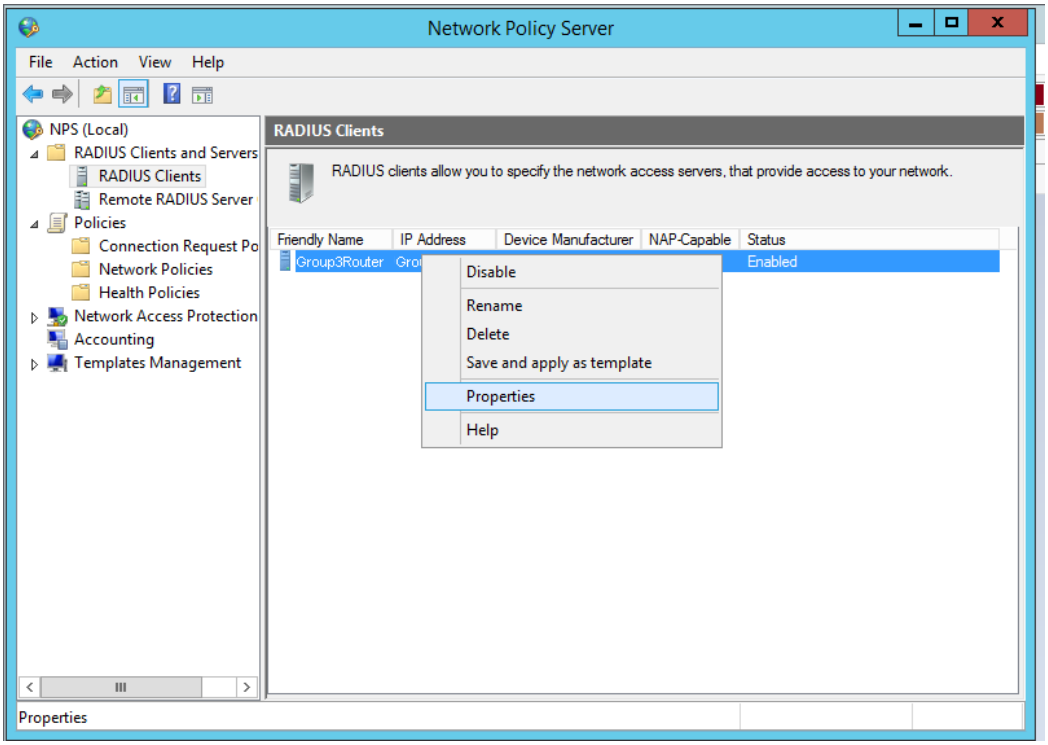


Figure 5.3.7 15 Setting the router name by clicking for AAA

Step 15: Right click on the router name in this case its named Group3Router, right click on it. It will show this dialog box, change the Vendor name from default to the Cisco, since we are using cisco router.

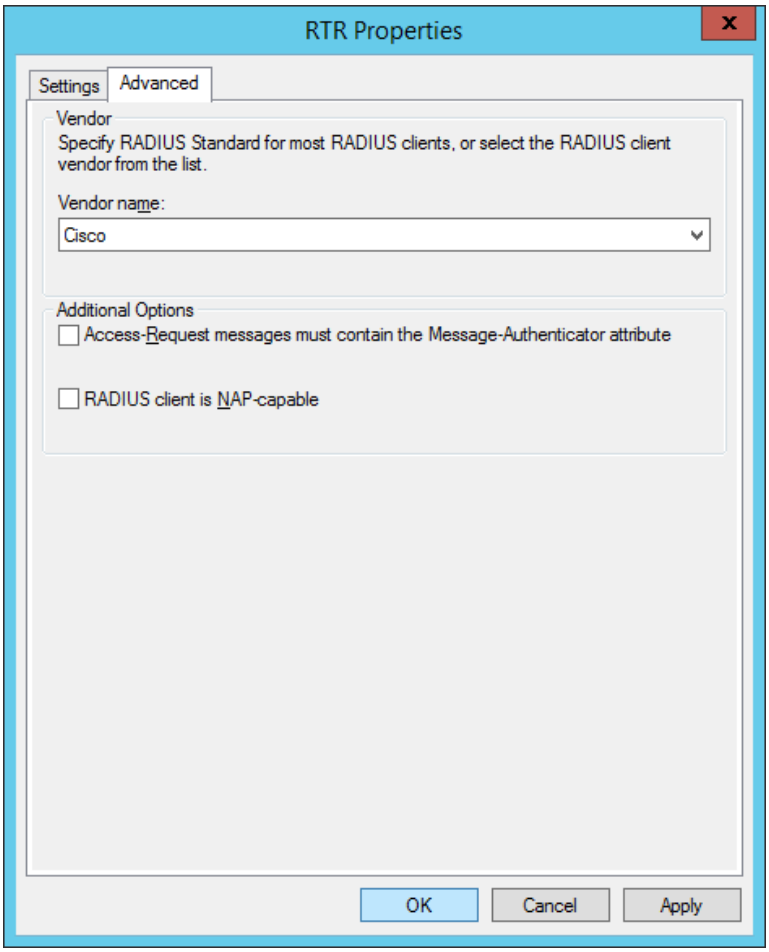


Figure 5.3.7 16 Choose vendor name, in this case I'm choosing

Step 16: Go to New Network Policy and click “Next”.

Click on the “Access granted”.

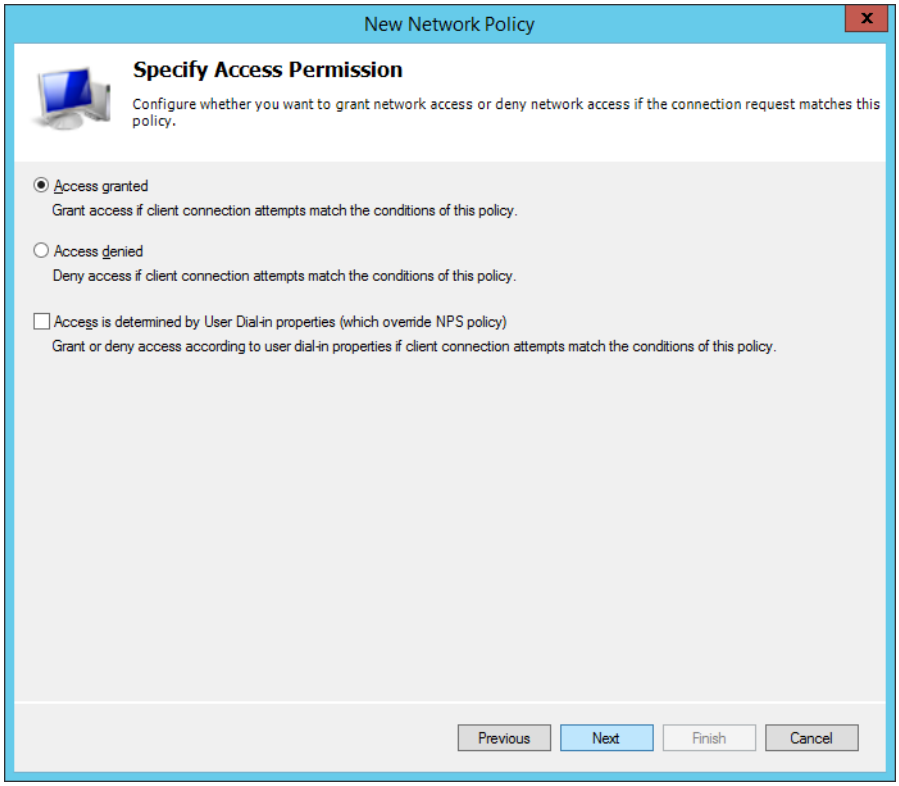


Figure 5.3.7 17 Specify the Access Permission

Step 17: Select “Unencrypted authentication (PAP, SPAP)”and click “Next”.

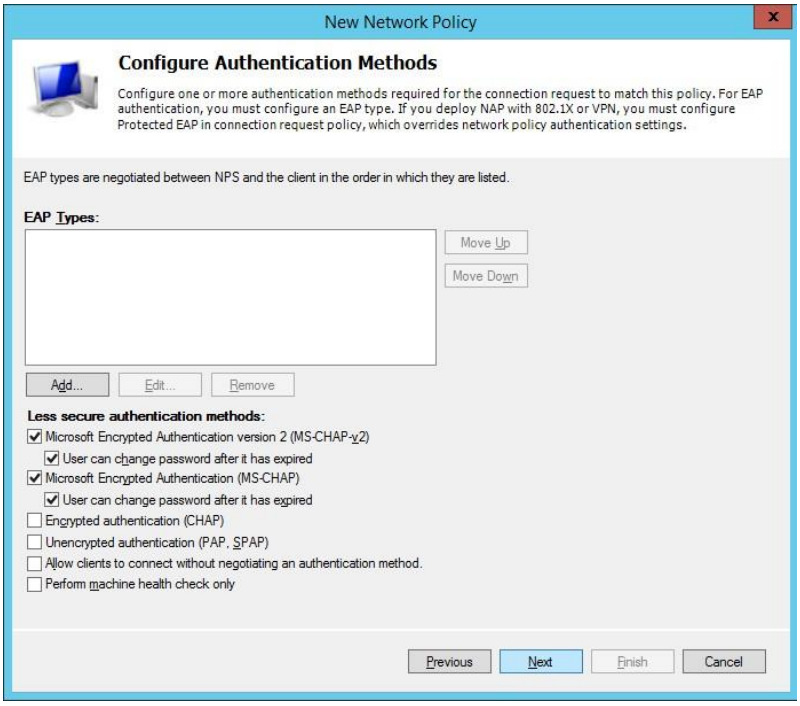


Figure 5.3.7 18 Configure Authentication for AAA

Step 18: It will go to Idle Timeout and click “Next”.

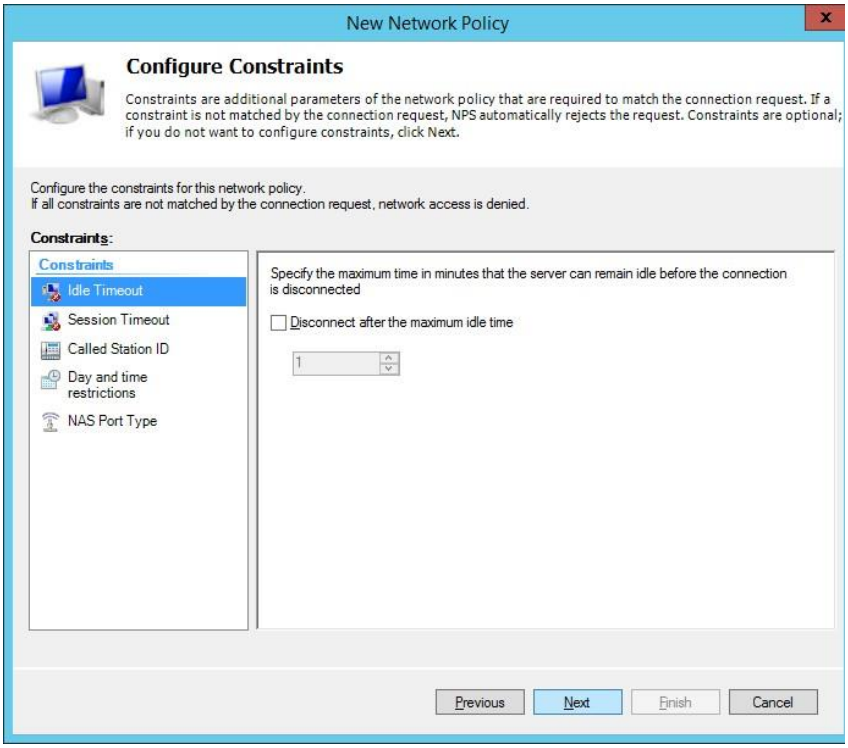


Figure 5.3.7 19 Configure Constraints for AAA

Step 19: The Radius Attributes Standard and click “Next”.

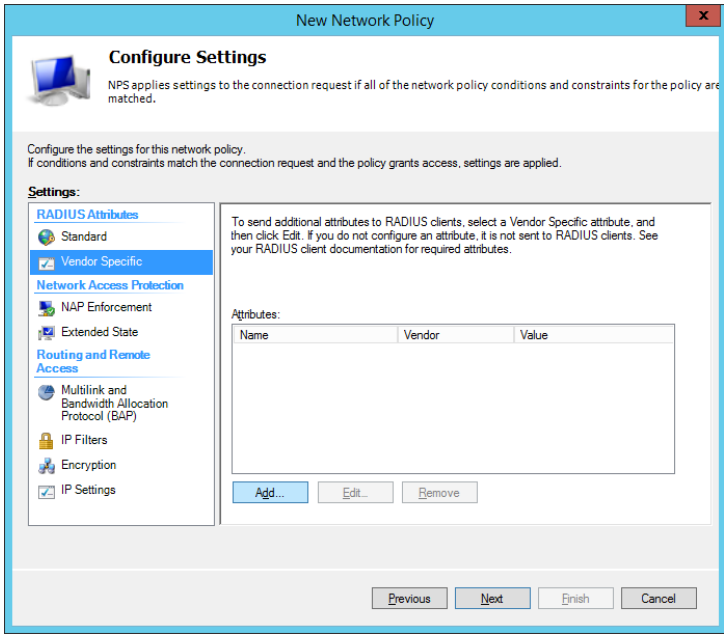


Figure 5.3.7 20 Configure Vendor Specific Settings for AAA

Step 20: To add a Vendor Specific Attribute, select vendor

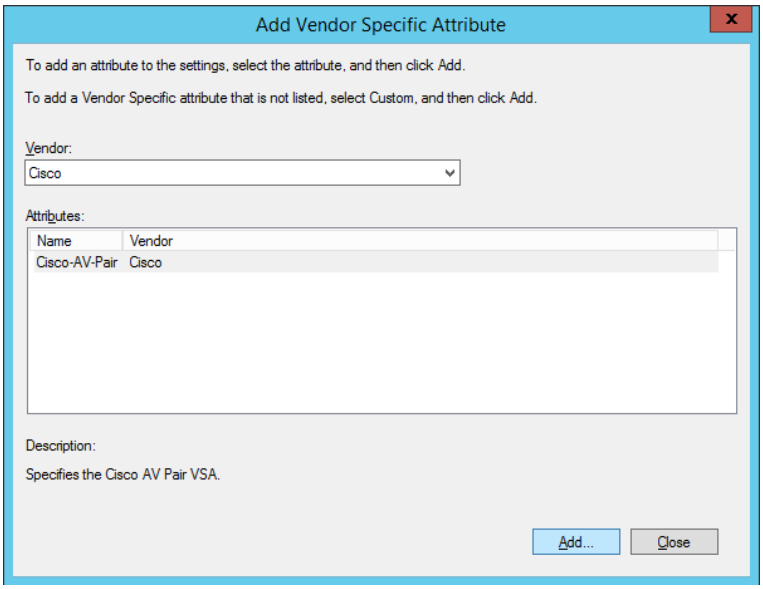


Figure 5.3.7 21 Add vendor specific Attribute for AAA

Step 21: Enter the Attribute value.

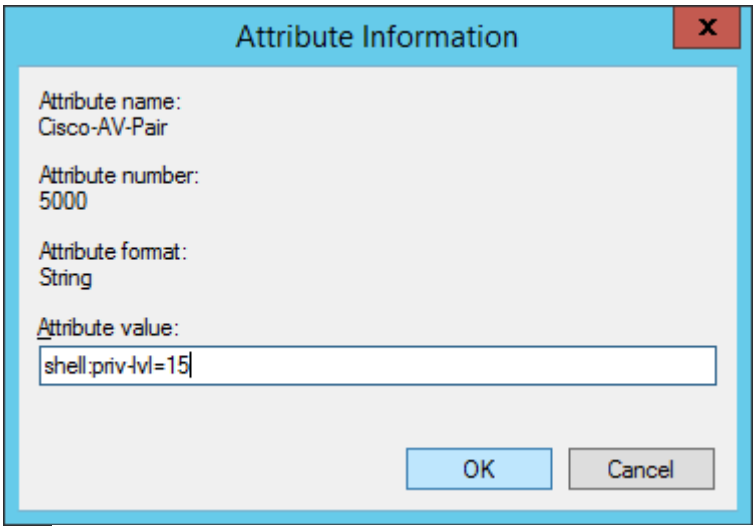


Figure 5.3.7 22 Add attributes information for AAA

Step 22: Successfully added.

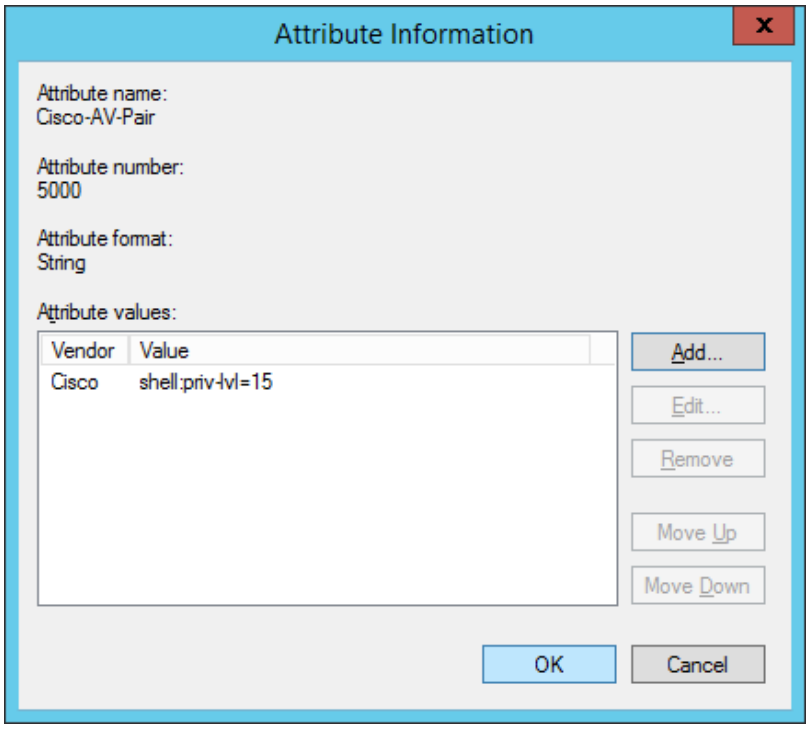


Figure 5.3.7 23 Attribute information display

Step 23: Successful added Vendor and click “Next”.

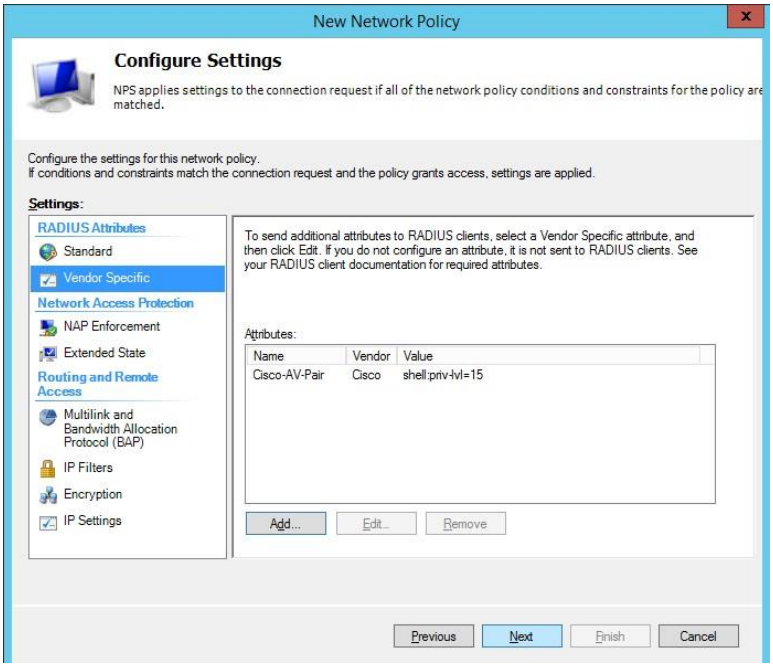


Figure 5.3.7 24 Display the added attribute for AAA

Step 24: The New Network Policy is completely created.

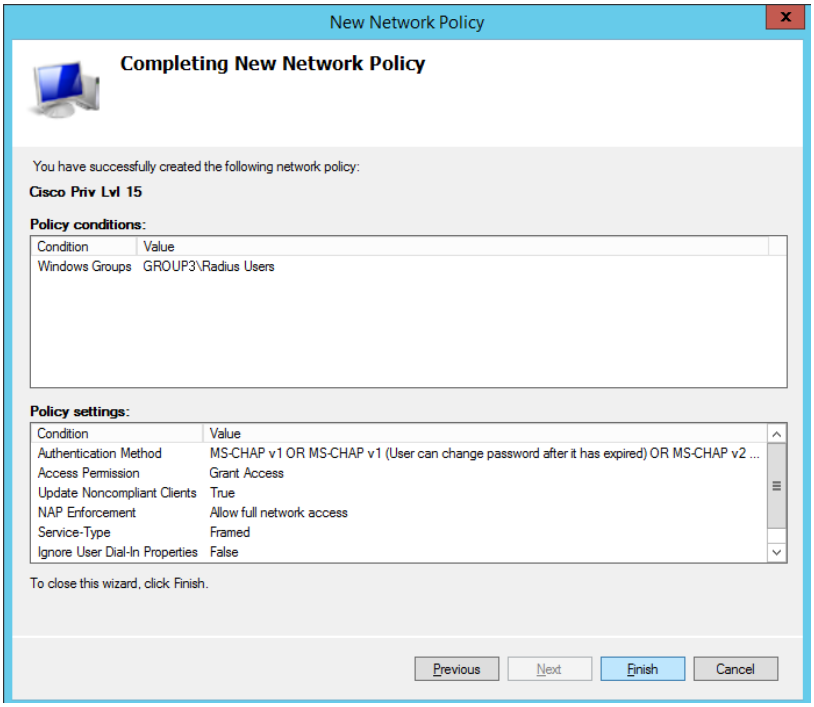


Figure 5.3.7 25 Configure vendor finishing installation for AAA

Step 25: Configure the AAA inside the router.

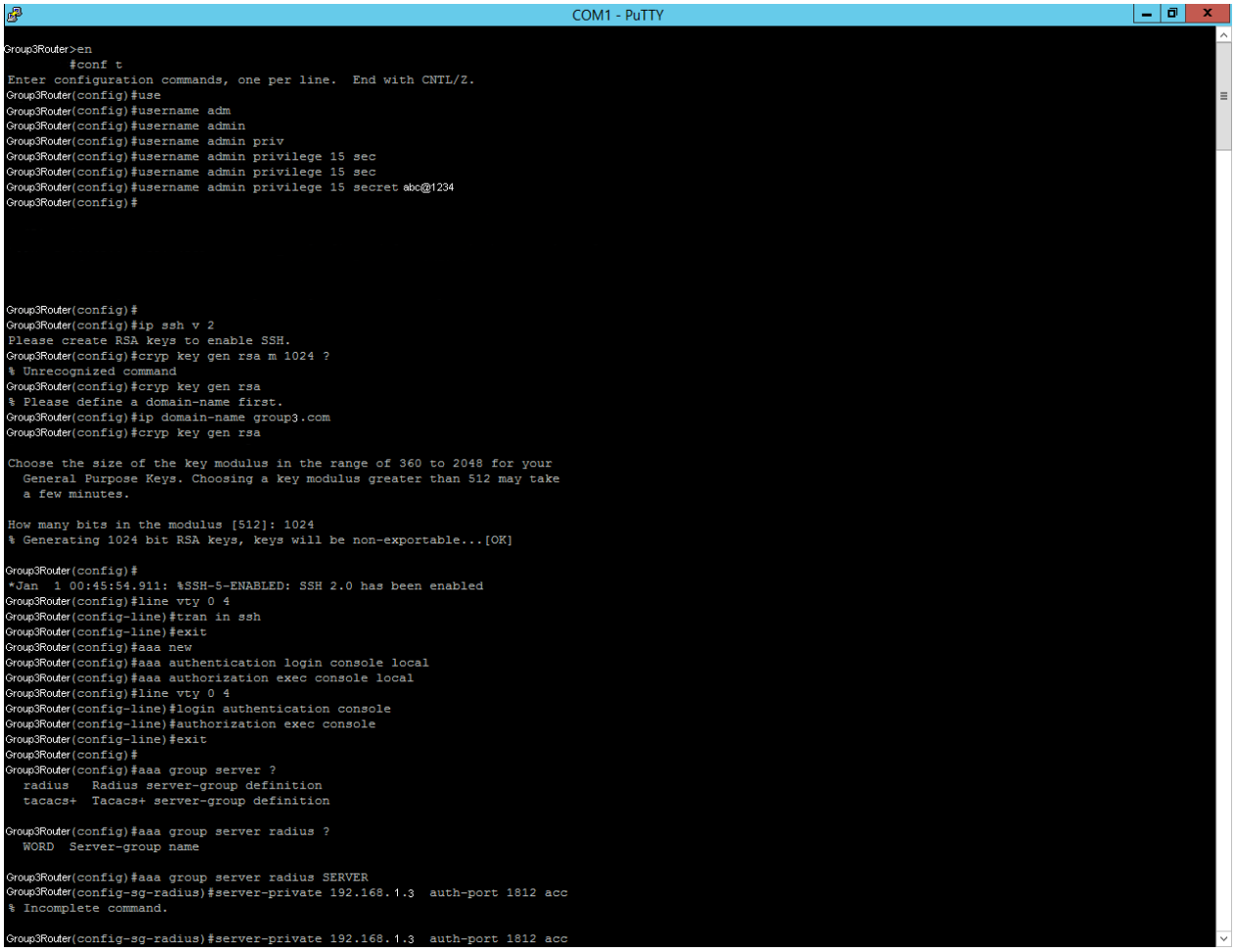


Figure 5.3.7 26 Creating a new AAA model

Step 26: Create the username of the router and password, in this case I'm using admin as username for admin user, and with the password abc@1234. After it's done, then it's time to install the AAA service, start with *AAA new model* and press enter.

```
aaa new-model
!
!
aaa authentication login default local
aaa authentication login aaa-server group radius local
aaa authorization exec default group radius if-authenticated
aaa authorization network default group radius
!
```

Figure 5.3.7 27 Creating a new authentication for AAA

Step 27: Configure the authentication and accounting port. For authentication we use 1812 port and for accounting we use 1813 port.

```
Group3Router(config)#$2.168.1.3 auth-port 1645 acct-port 1646 key cisco
Group3Router(config)#$2.168.1.3 auth-port 1812 acct-port 1813 key cisco
Group3Router(config)#exit
Group3Router#
```

Figure 5.3.7 28 Configure authentication port and accounting port for AAA

Step 28: After the entire configuration is done, restart the Putty to enter router again. This time we have to insert the username and password as authentication for the router. In this scenario I'm using admin login. The history of the login can be view in Event Viewer on Windows Server.

5.3.8 Secure File Transfer Protocol (SFTP)

Step 1: Installation process

Install update of this Ubuntu

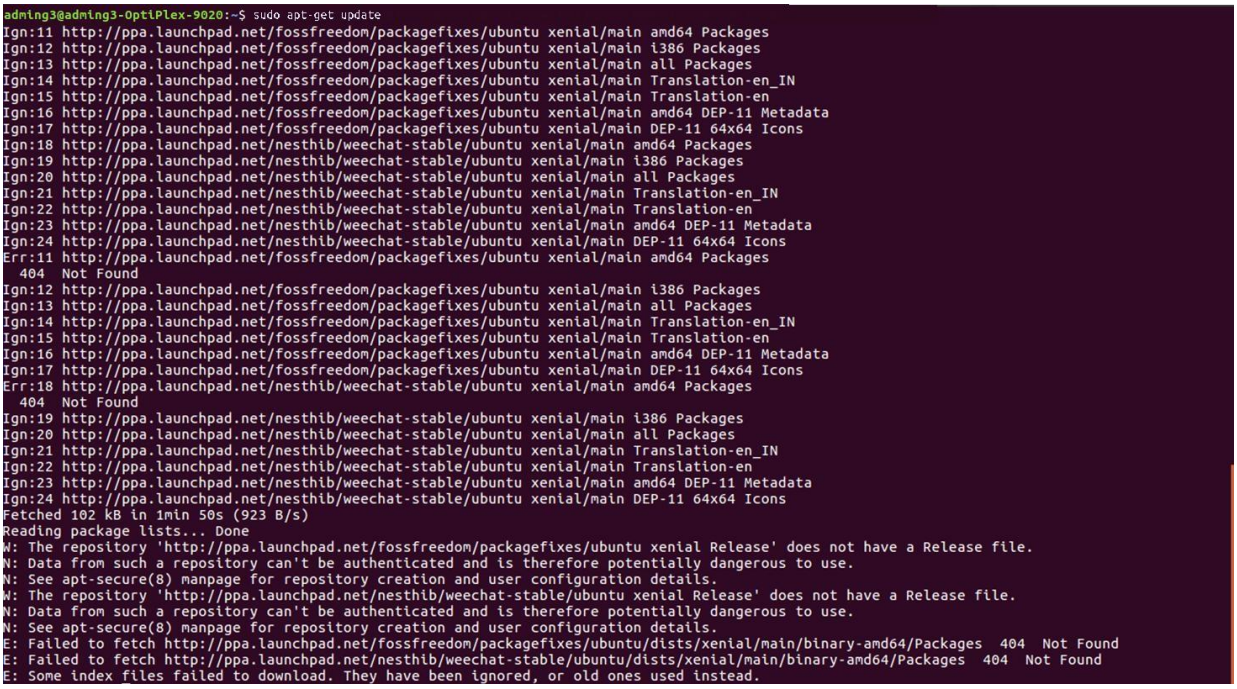


Figure 5.3.8 1 Install update for SFTP

Step 2: Install vsftpd by typing “sudo apt-get install vsftpd”

```
adming3@adming3-OptiPlex-9020:~$ apt-get -y install vsftpd
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  vsftpd
0 upgraded, 1 newly installed, 0 to remove and 214 not upgraded.
Need to get 111 kB of archives.
After this operation, 361 kB of additional disk space will be used.
Get:1 http://archive.ubuntu.com/ubuntu/ trusty-updates/main vsftpd amd64 3.0.2-1
ubuntu2.14.04.1 [111 kB]
Fetched 111 kB in 0s (147 kB/s)
Preconfiguring packages ...
Selecting previously unselected package vsftpd.
(Reading database ... 23985 files and directories currently installed.)
Preparing to unpack .../vsftpd_3.0.2-1ubuntu2.14.04.1_amd64.deb ...
Unpacking vsftpd (3.0.2-1ubuntu2.14.04.1) ...
Processing triggers for man-db (2.6.7.1-1) ...
Processing triggers for ureadahead (0.100.0-16) ...
ureadahead will be reprofiled on next reboot
Setting up vsftpd (3.0.2-1ubuntu2.14.04.1) ...
vsftpd start/running, process 1228
Processing triggers for ureadahead (0.100.0-16) ...
```

Figure 5.3.8 2 Install vsftpd package

Step 3: Type nano /etc/vsftpd.conf to configure the ftp policy

```
root@adming3-OptiPlex-9020:/home/adming3# nano etc/vsftpd.conf
root@adming3-OptiPlex-9020:/home/adming3# cd
root@adming3-OptiPlex-9020:~# cd /etc
root@adming3-OptiPlex-9020:/etc# nano etc/vsftpd.conf
root@adming3-OptiPlex-9020:/etc# gedit vsftpd.conf
^C
root@adming3-OptiPlex-9020:/etc# nano vsftpd.conf
root@adming3-OptiPlex-9020:/etc#
```

Figure 5.3.8 3 Enter the vsftpd configuration file

Step 4: Find the line “anonymous_enable” and change the value to “NO”

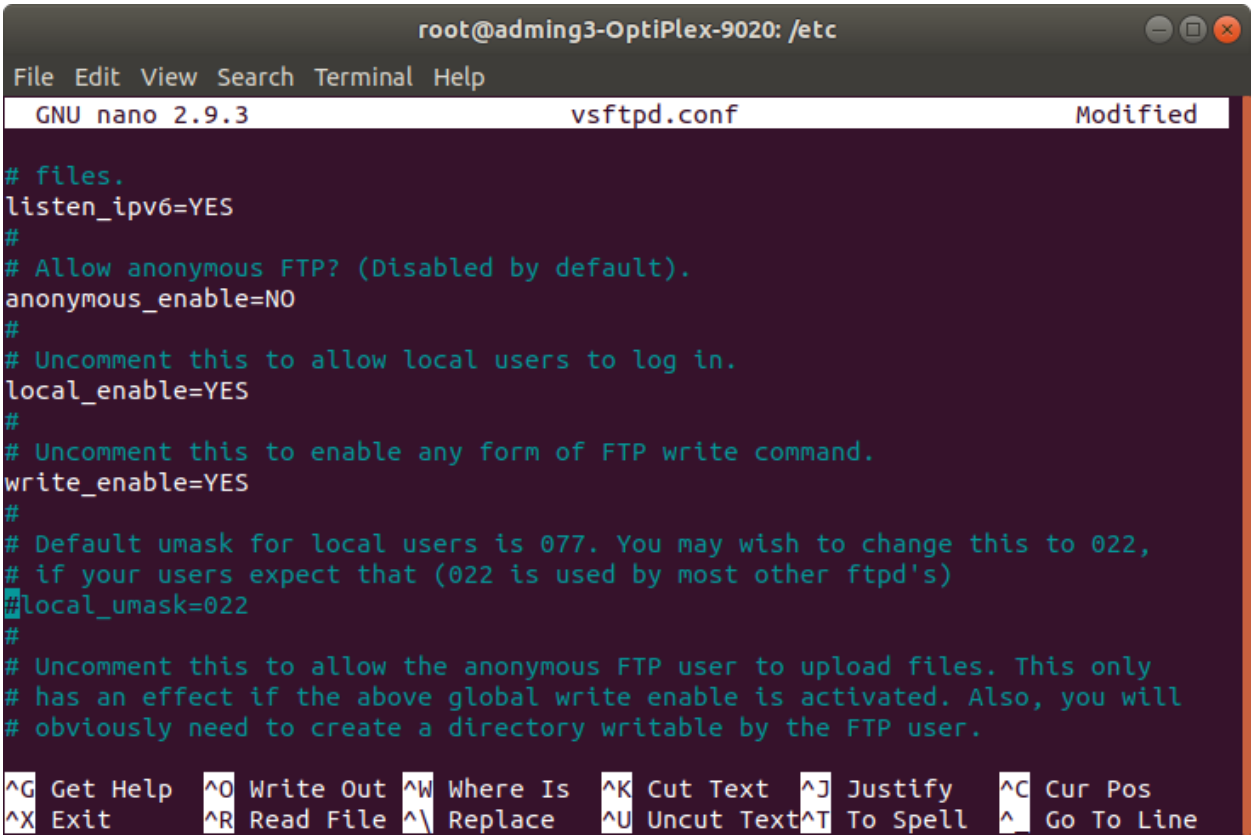


Figure 5.3.8 4 Editing the vsftpd configuration file

Step 5: Create a new user with password, to use the FTP service

```
root@adming3-OptiPlex-9020:/etc#
root@adming3-OptiPlex-9020:/etc# useradd -g ftp-users -d /home/adming3/ftp-files
 hong
root@adming3-OptiPlex-9020:/etc# passwd hong
```

Figure 5.3.8 5 Add new user and its password for SFTP

Step 6: Testing the FTP inside localhost in this case I'm using Ubuntu as a FTP server.

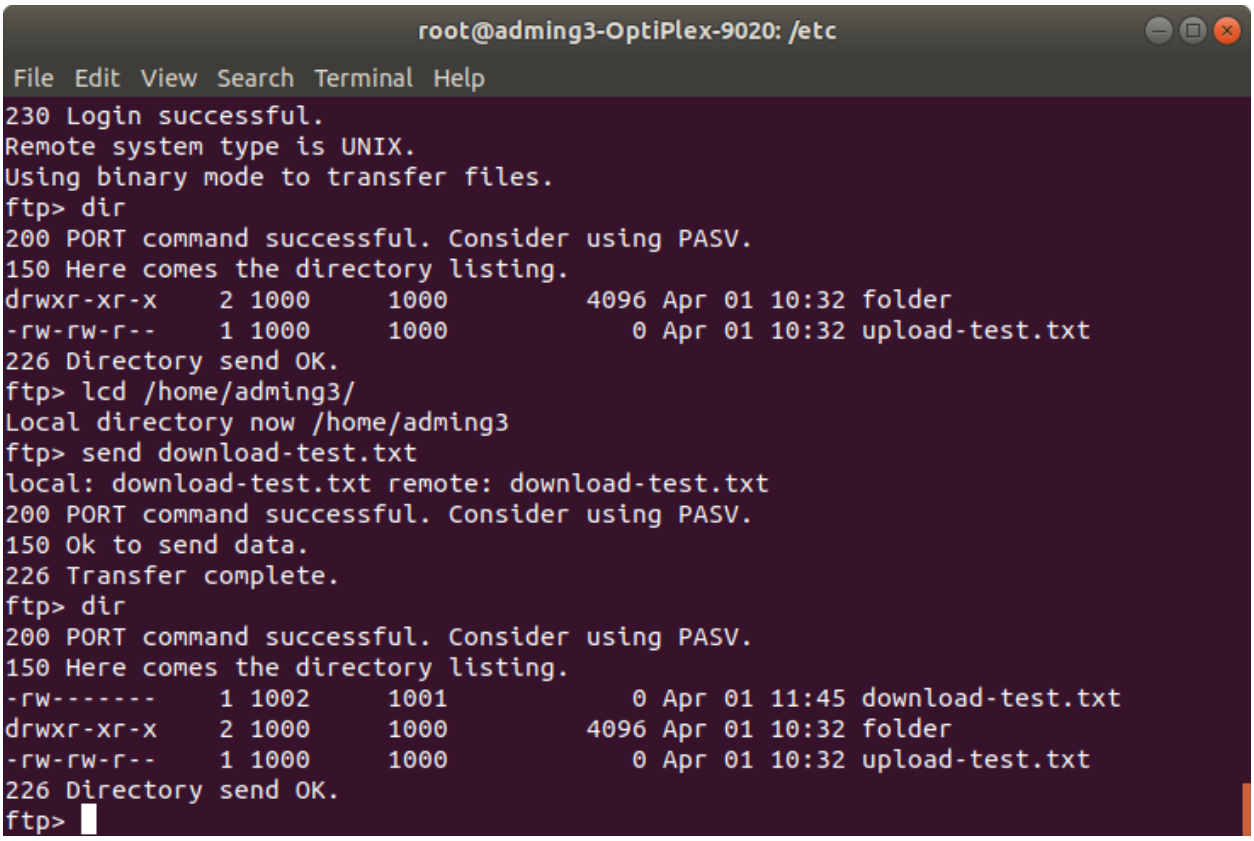


Figure 5.3.8 6 Testing run FTP in locahost

Step 7: Enable the Secure Shell (SSH)

Install the SSH by typing sudo apt install openssh-server

Figure 5.3.8 7 Install openssh-server

Step 8: Configure the sshd_config file by typing sudo nano /etc/ssh/sshd_config

After finish all the configuration, restart the vsftpd service by typing *sudo systemctl restart vsftpd* and restart the ssh by typing *sudo systemctl restart ssh.service*

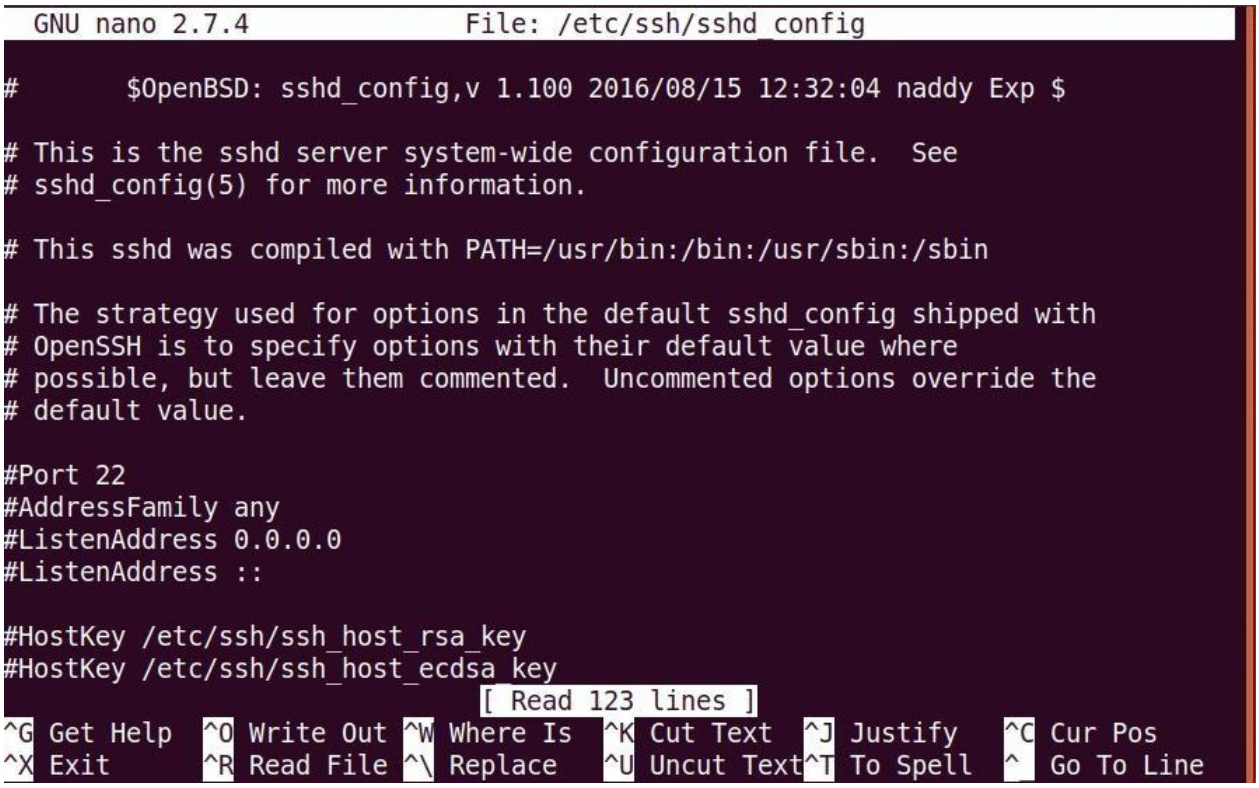


Figure 5.3.8 8 Setting and configure the router for SFTP

5.3.9 Access Control List (ACL)

The Access Control List (ACL) is used for filtering traffic based on a given filtering criteria on a router or switch interface. Based on the conditions supplied by the ACL, a packet is allowed or blocked from further movement. The filtering can be made through IP address and also TCP port. The usage of ACL allows only certain network traffic to get in or out of the network.

This ACL is applied into interface FastEthernet 0/1 and served as an internal firewall. It designs to deny a few services, like HTTP, HTTPS, EMAIL and FTP. But only permit ICMP function. This ACL are implemented on VLAN50 which is vlan for client.

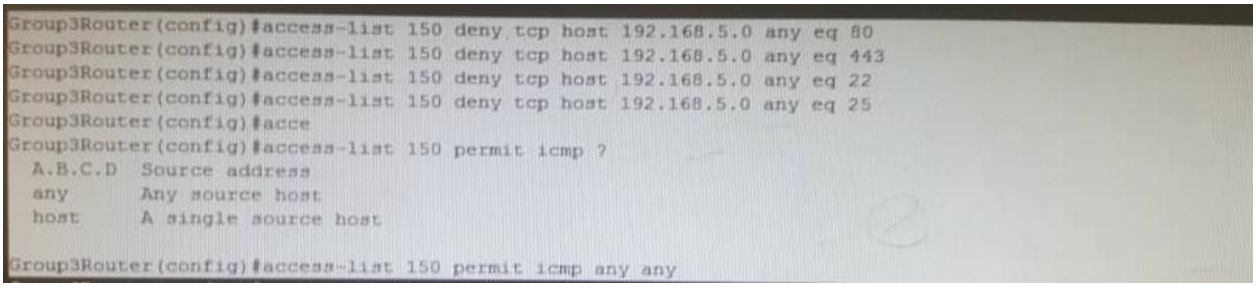


Figure 5.3.9 1 Deny and permit process

The screenshot above shows that, we deny a VLAN50 network using IP address 192.168.5.0, port 80 is for HTTP, port 443 is for HTTPS which is for secure web, port 22 is for SFTP and port 25 is for SMTP which is use for email service, I only permit ICMP function on this network. So, user in this network is only able to ping to the router and the server, but they can't use any service in this network.

5.3.10 Linux Email Server

Step 1: Install &Update apt

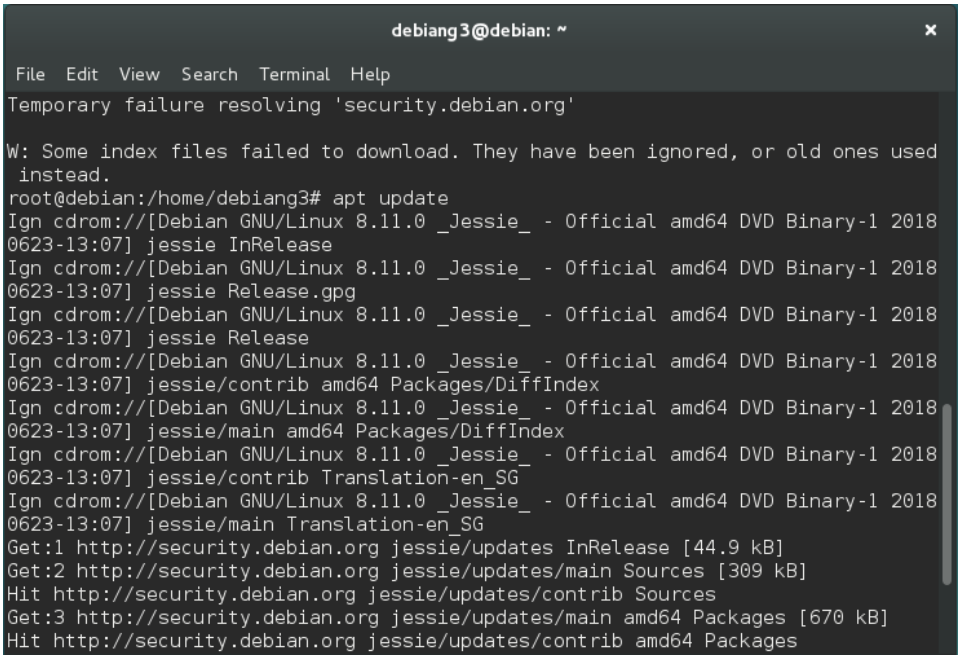


Figure 5.3.10 1 Updating apt

Step 2: Install Postfix Mail Server

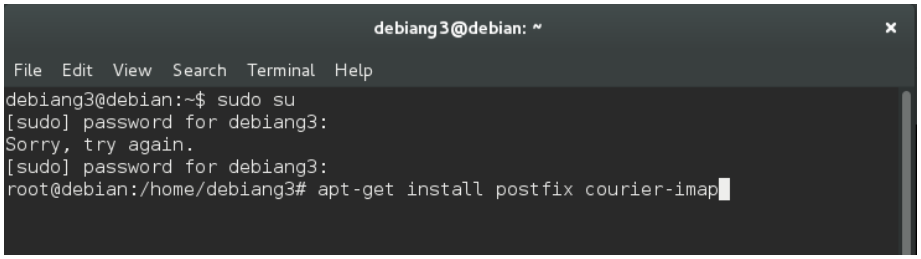


Figure 5.3.10 2: Installing Postfix

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

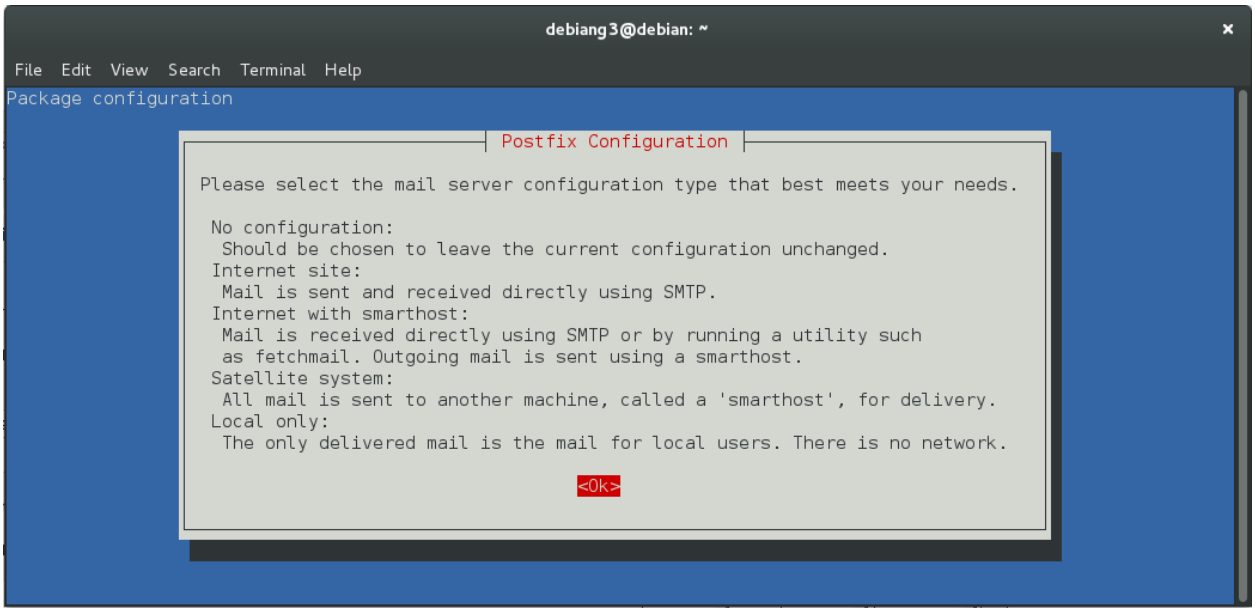


Figure 5.3.10 3 Postfix configuration

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

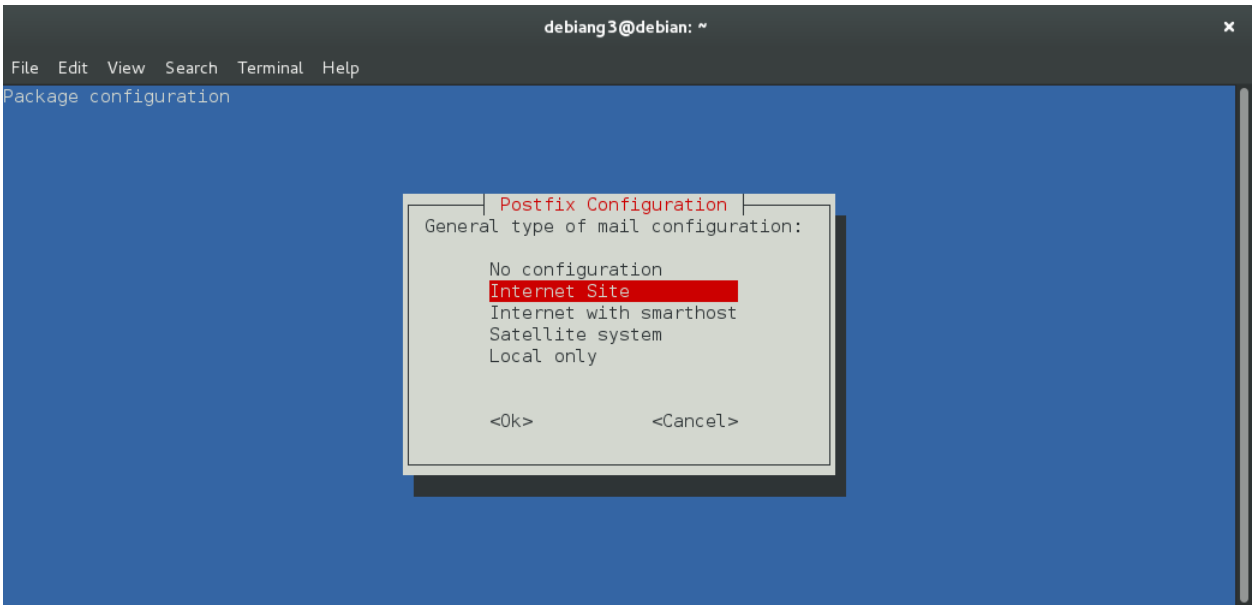


Figure 5.3.10 4 Choosing internet sit

Step 5: Now enter the fully qualified domain name that you want to use for send and receive mails. In this case, we use mail.group3.com

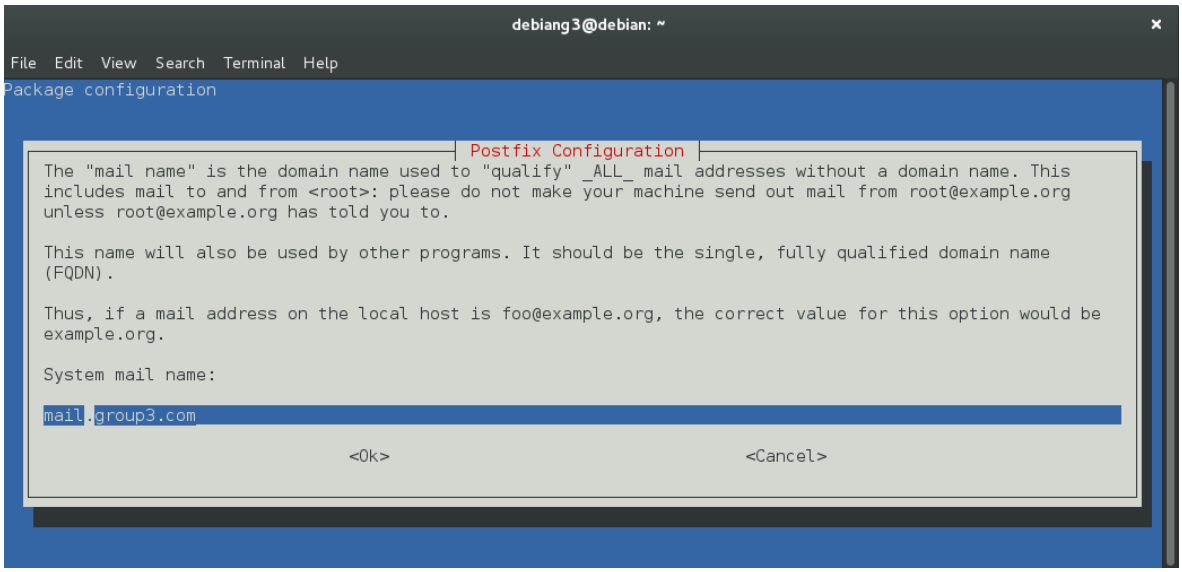


Figure 5.3.10 5 Adding domain for mail ,mail.group3.com

Step 6: click yes for create web based administration

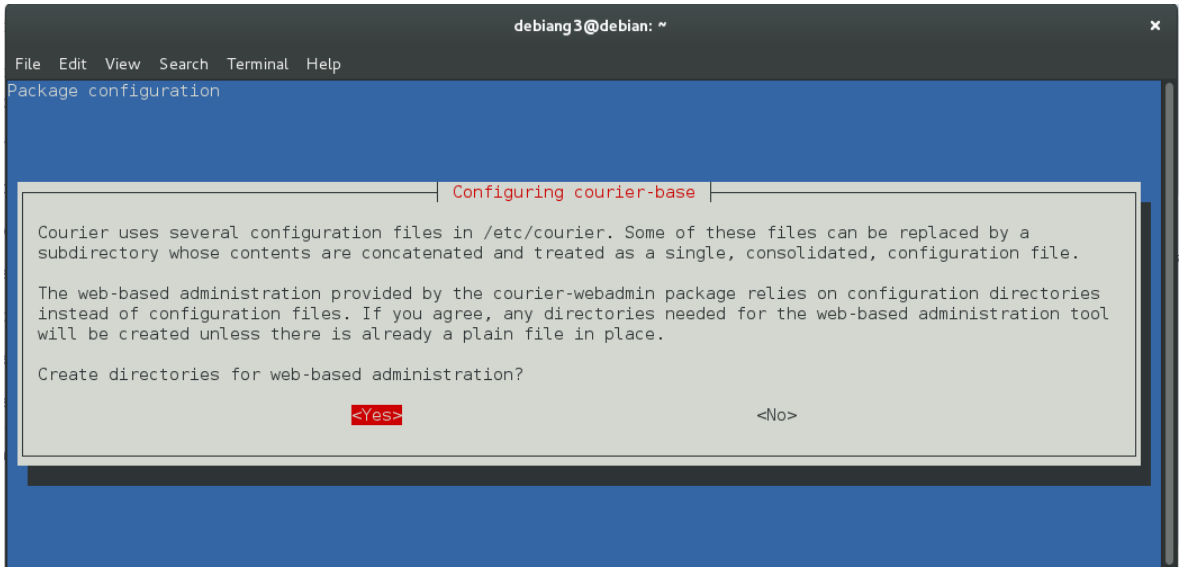


Figure 5.3.10 6 Configuring courier-base

Step 7: Click ok for ssl certificate

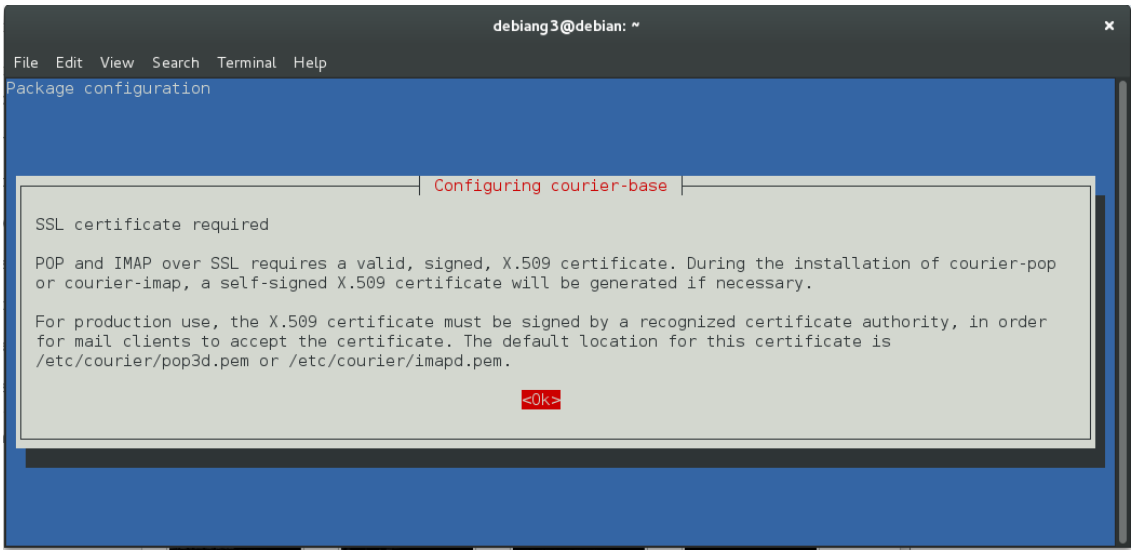


Figure 5.3.10 7 SSL certificate required

Step 8: Install both Apache2 & PHP7.0 packages

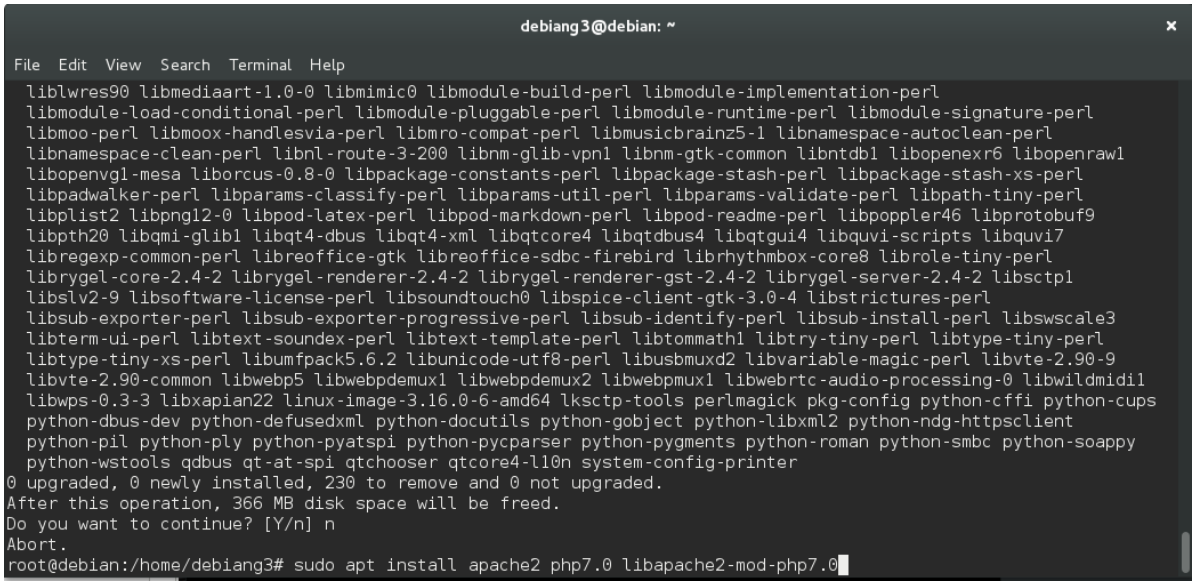


Figure 5.3.10 8 Installing Apache2 & PHP7.0

Step 9: Installing Apache2 & PHP7.0 packages

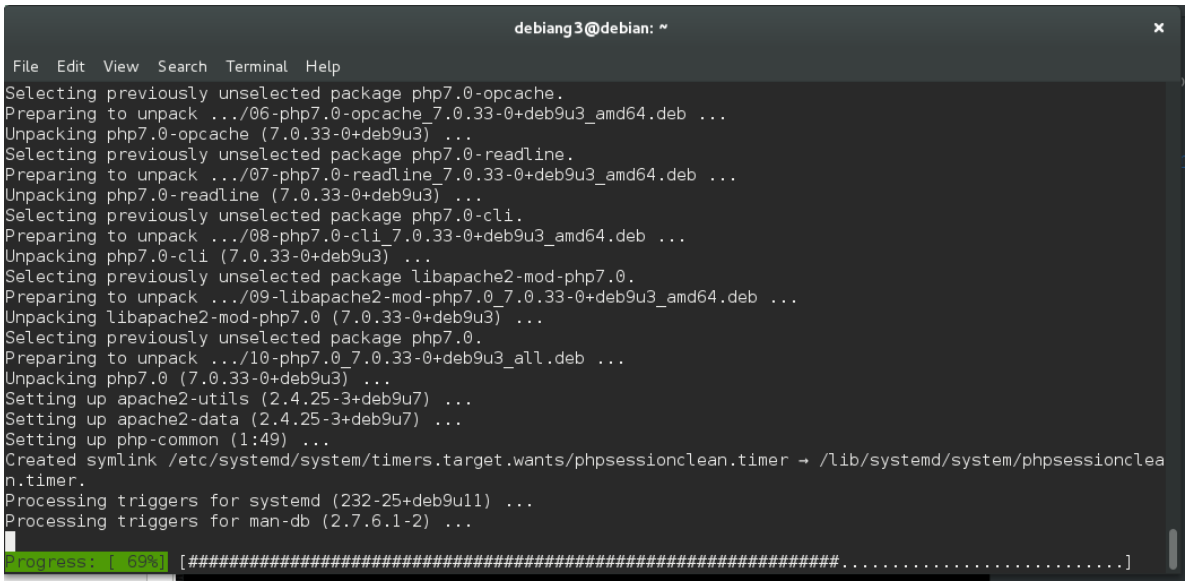


Figure 5.3.10 9 Installing apache and php7.0 packages

Step 10: After installation enter country name,state & email address

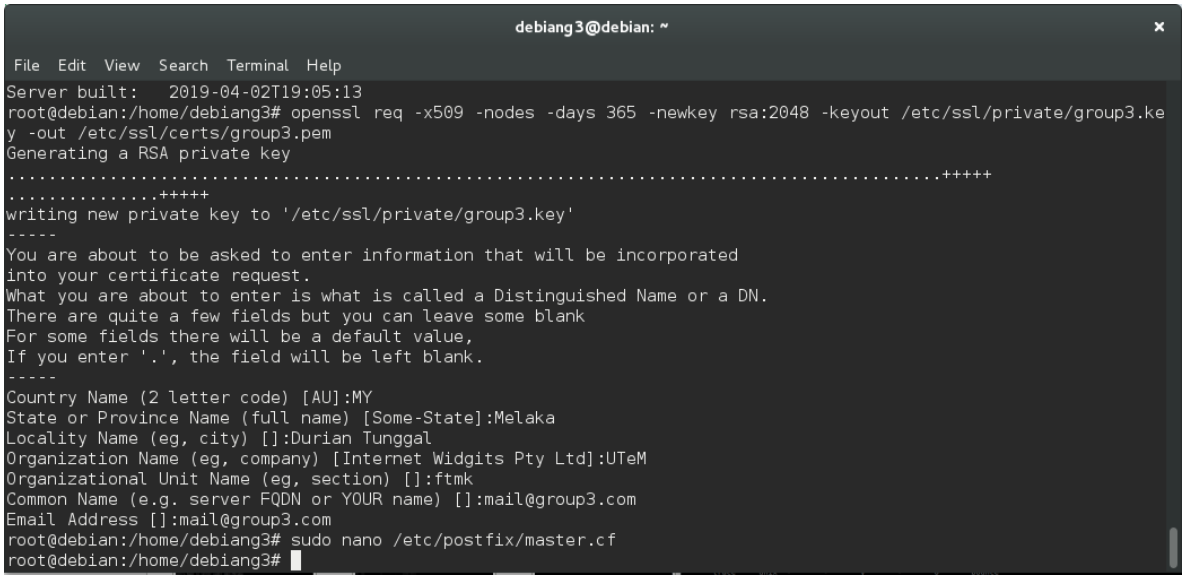


Figure 5.3.10 10 Entering country name and email address

Step 11: Dovecot is a mail delivery agent (MDA), it delivers the emails from/to the mail server, to install it, run the following command.

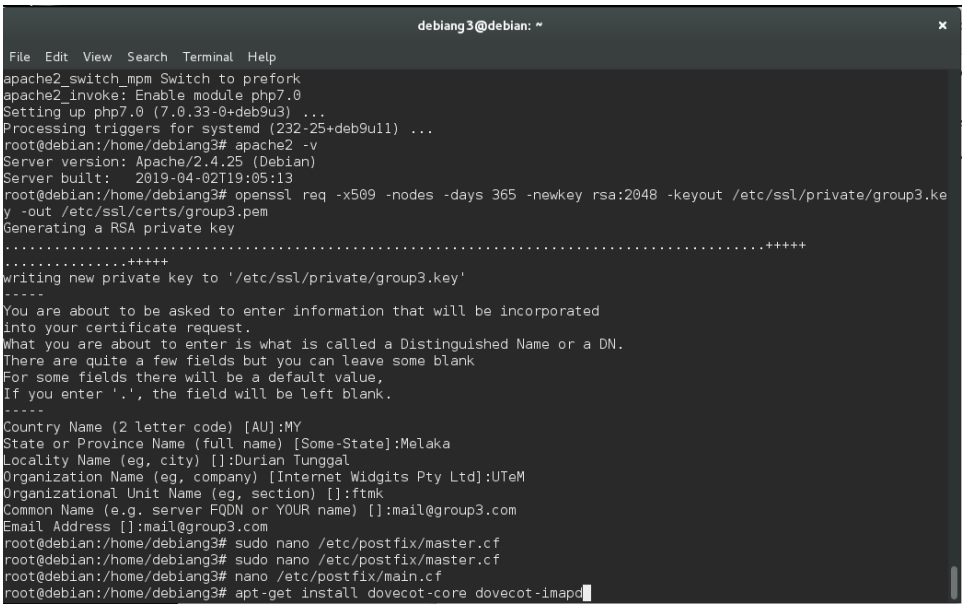


Figure 5.3.10 11 Installing dovecot-imapd

Step 12: Start configuring Dovecot by edit main config file. Run the command and add the following line to enable IMAP protocol.

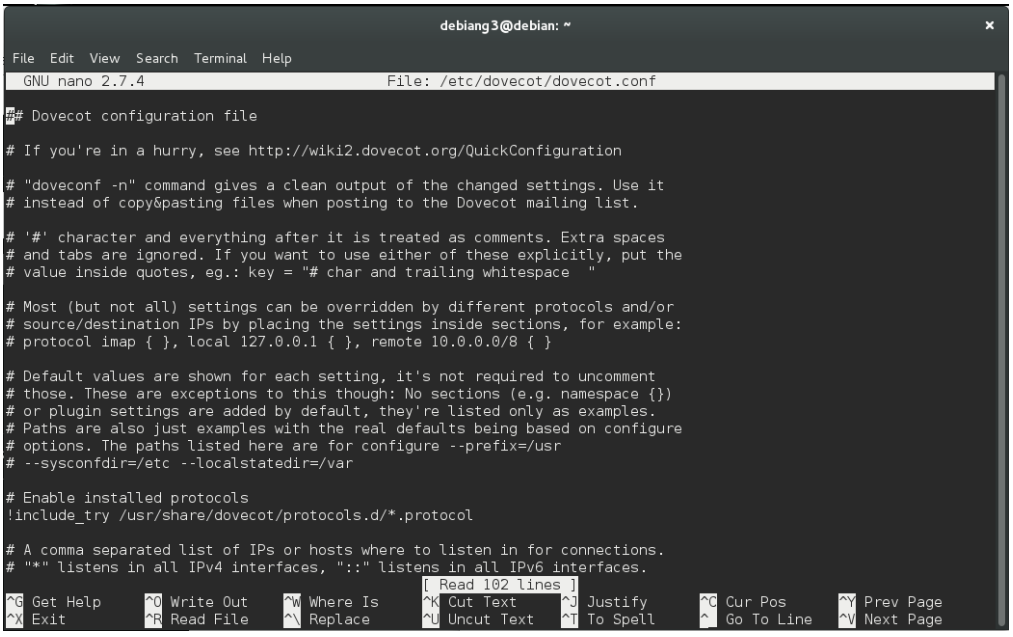


Figure 5.3.10 12 Configuring dovecot part 1

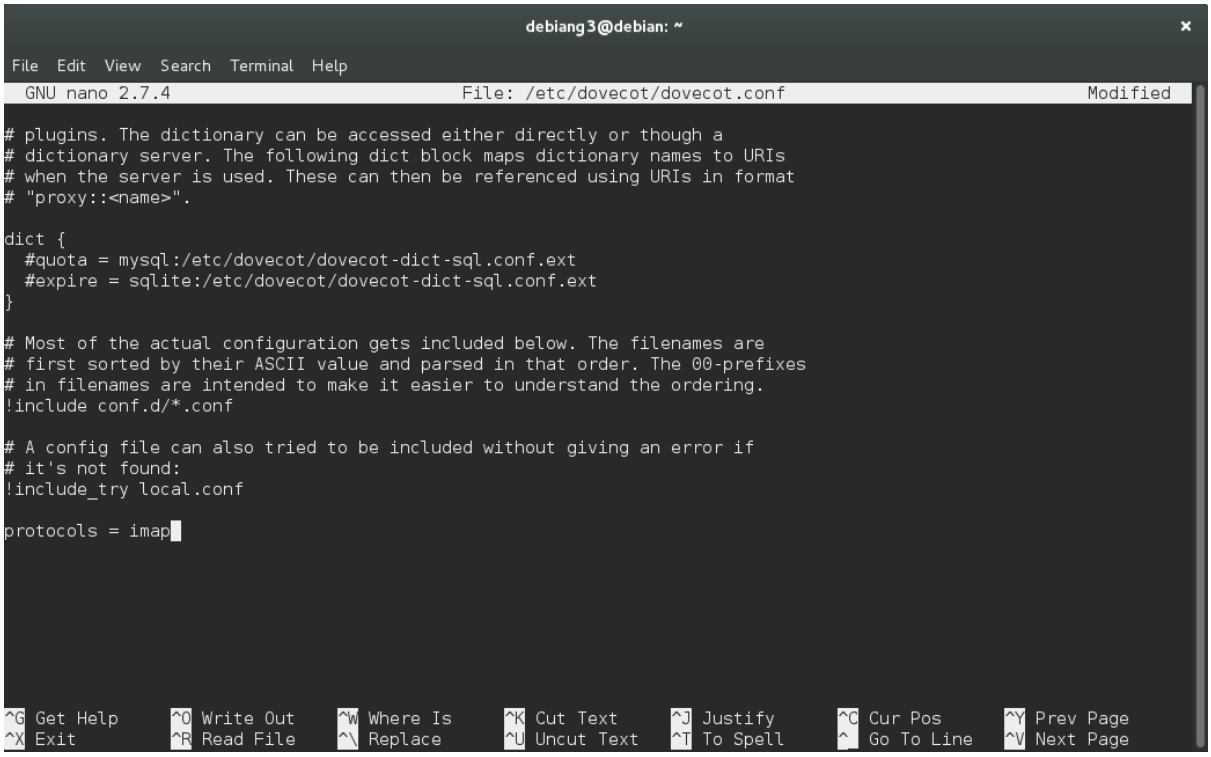


Figure 5.3.10 13 Configuring dovecot part 2

Step 13: Edit SSL/TLS config file nd change **ssl= no to ssl= required.**

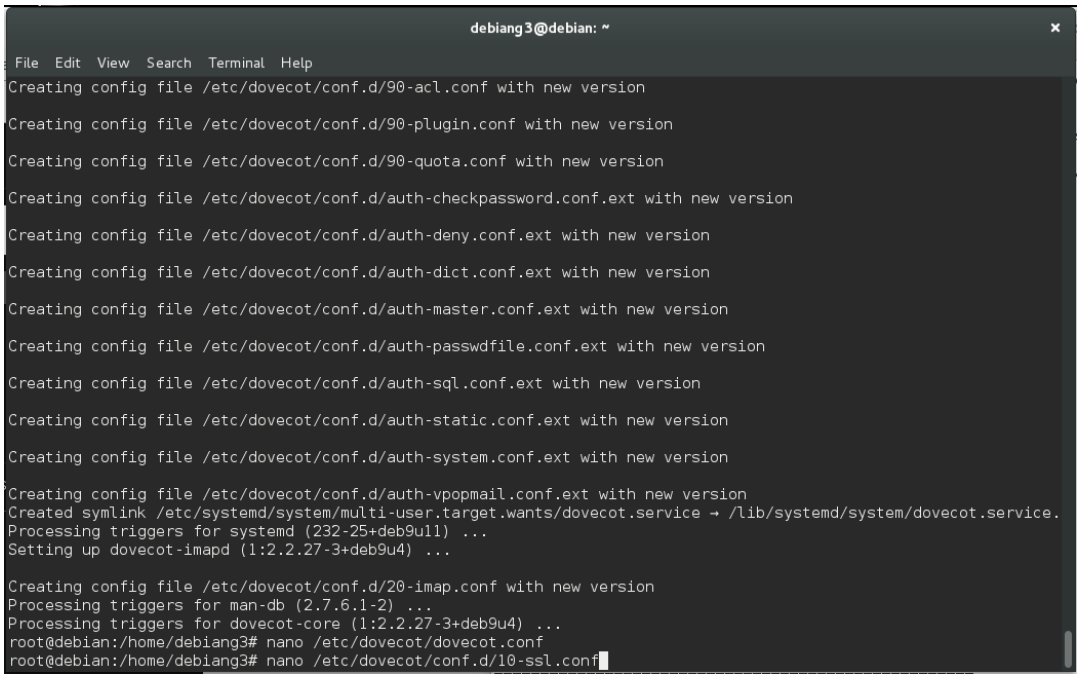


Figure 5.3.10 14 Edit SSL required part 1

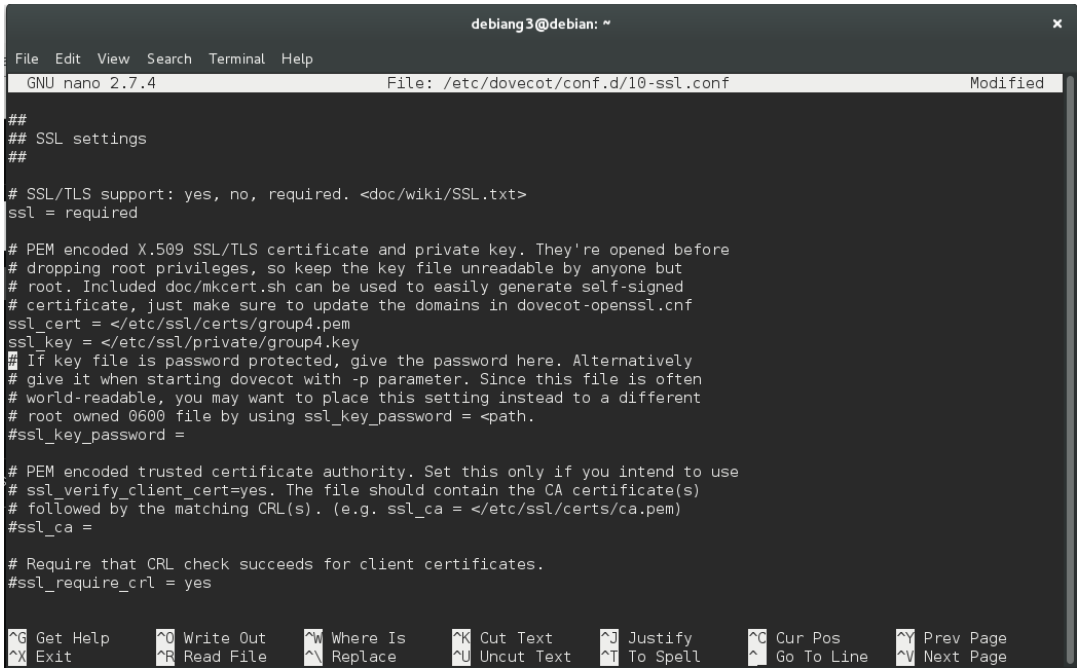


Figure 5.3.10 15 Edit SSL required part 2

Step 14: Edit the following file. Then change the auth section to the following so that postfix can find the dovecot authentication server.

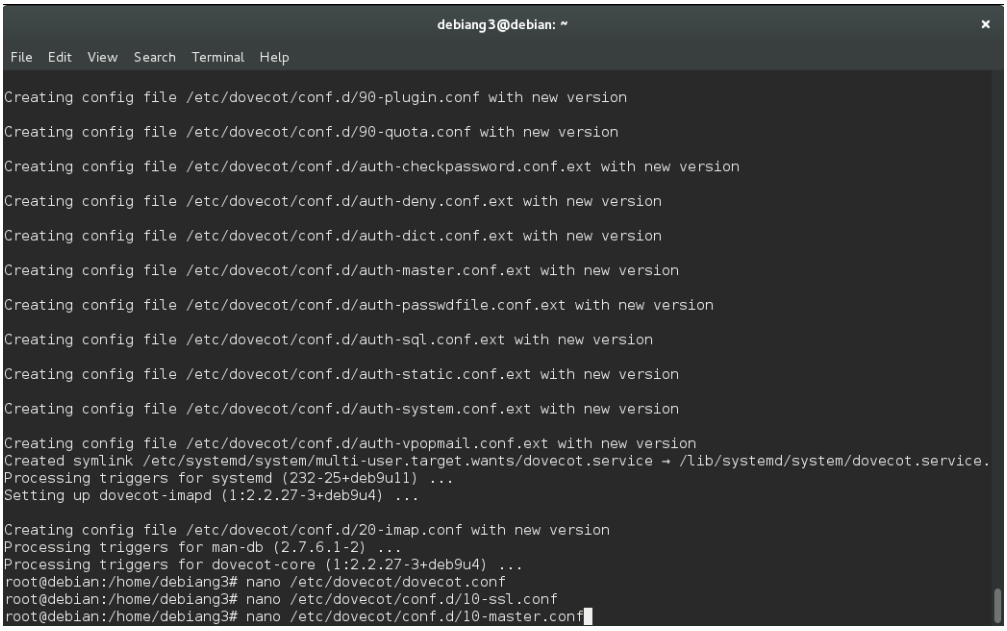


Figure 5.3.10 16 Enter command nano/etc/dovecot/conf./10-master.conf

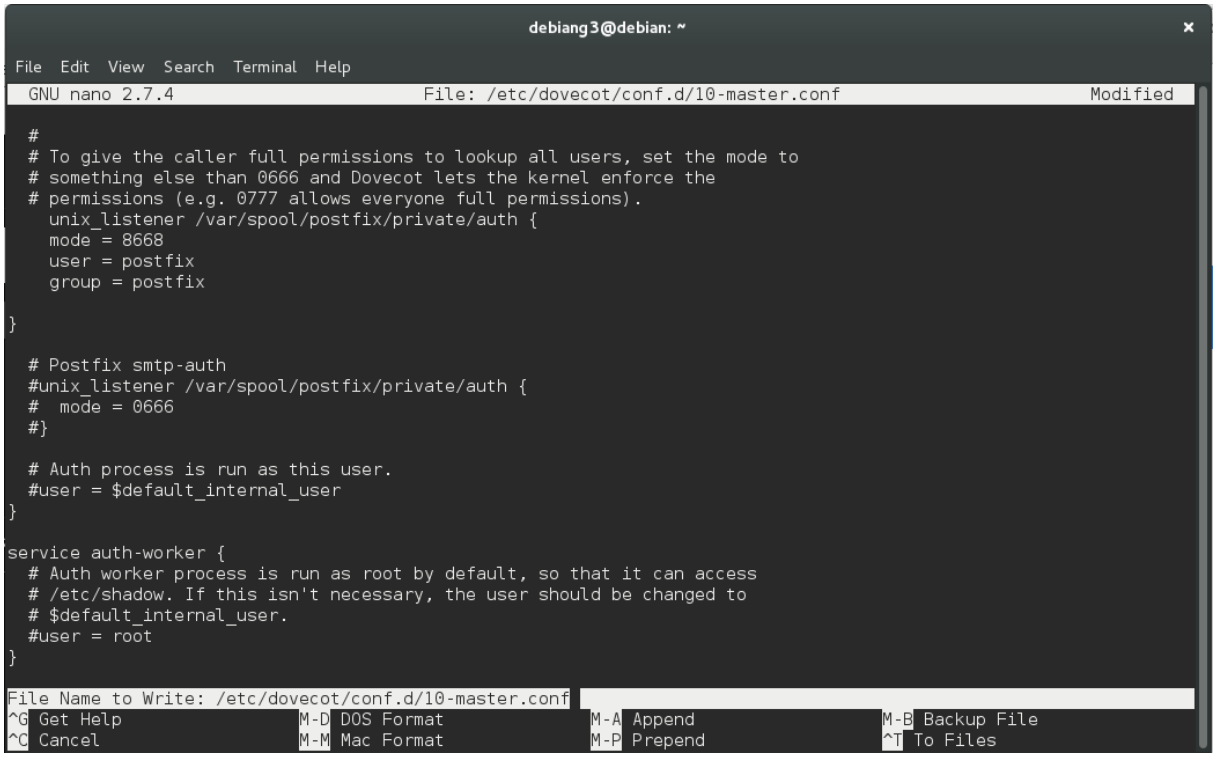


Figure 5.3.10 17 Edit Mode = 8668, user = postfix, group = postfix.

Step 15: Install Rainloop for webmail access.

```
~# mkdir rainloop
```

Figure 5.3.10 18 Installing command for rainloop

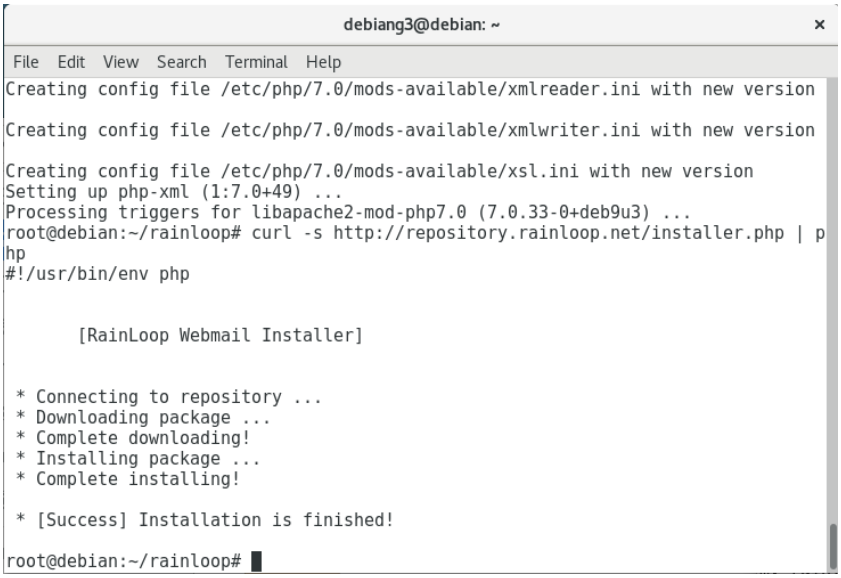


Figure 5.3.10 19 Rainloop successfully installed

5.3.11 WEB, SSL and Virtual Hosting

Step 1: In IIS need to click default website and need to choose default document

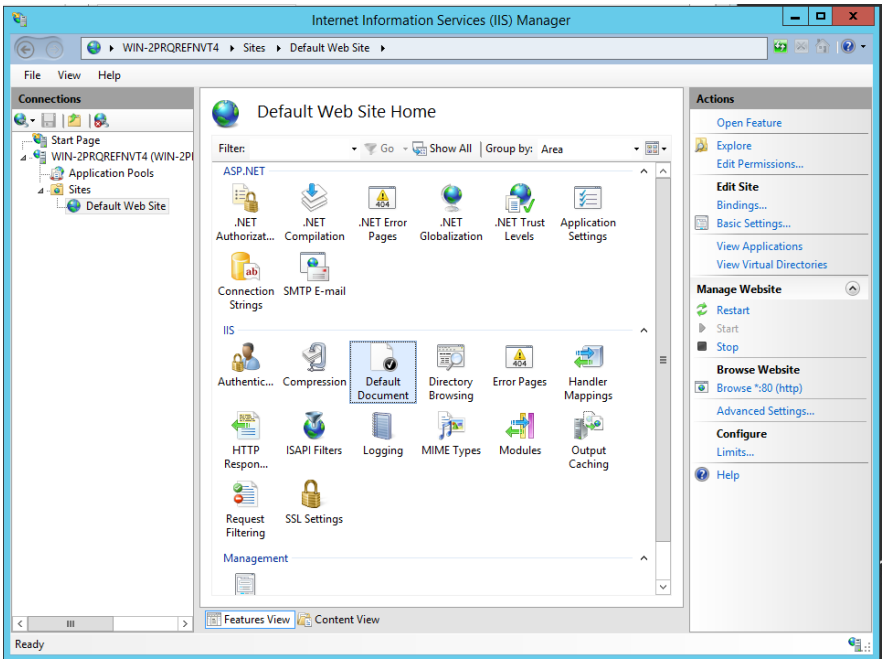


Figure 5.3.11 1 Choosing default document

Step 2: Add new default document

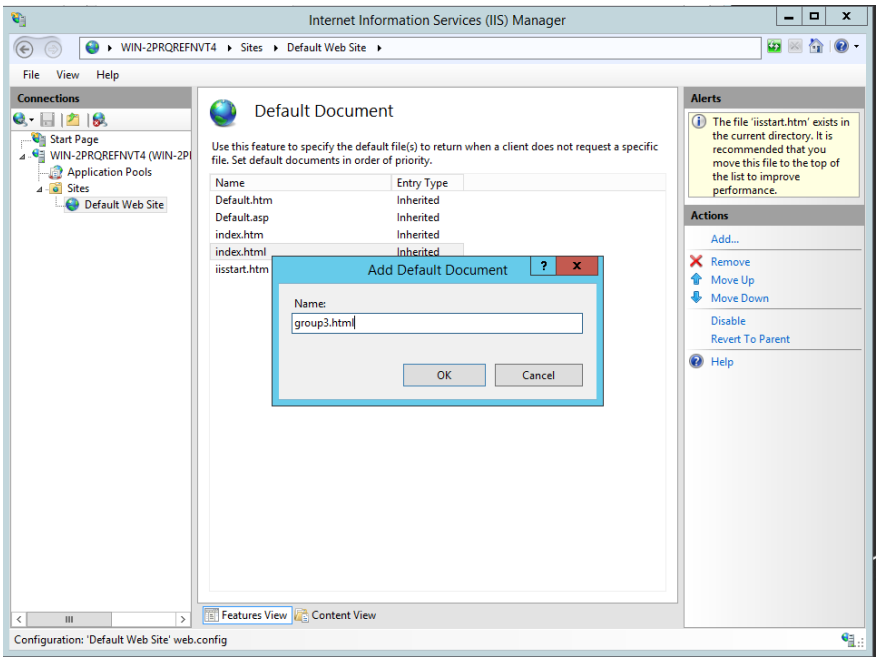


Figure 5.3.11 2 Adding new default document

Step 3: default website created

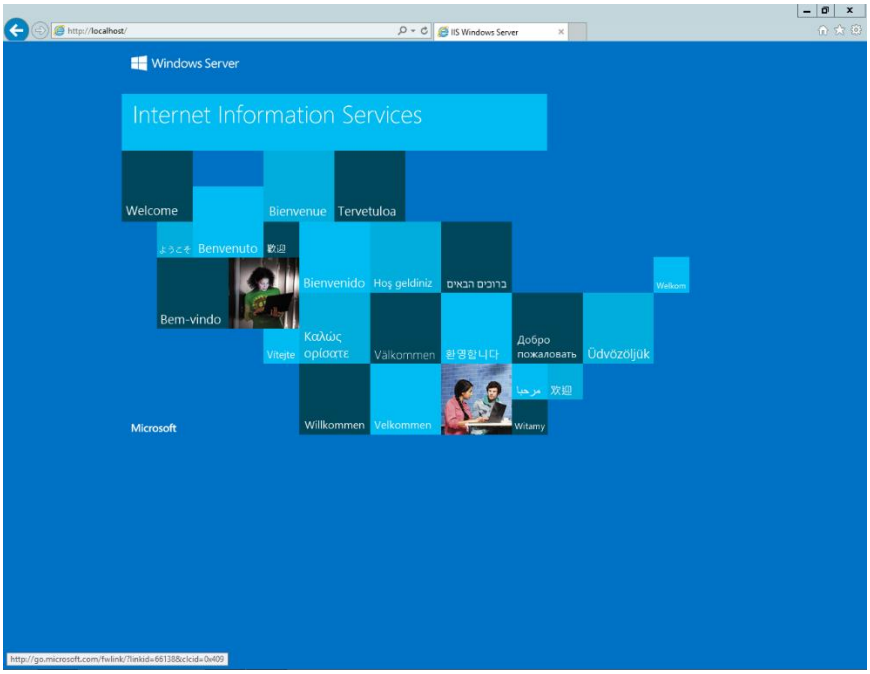


Figure 5.3.11 3 Default website

WEB

Step 4: Add new website

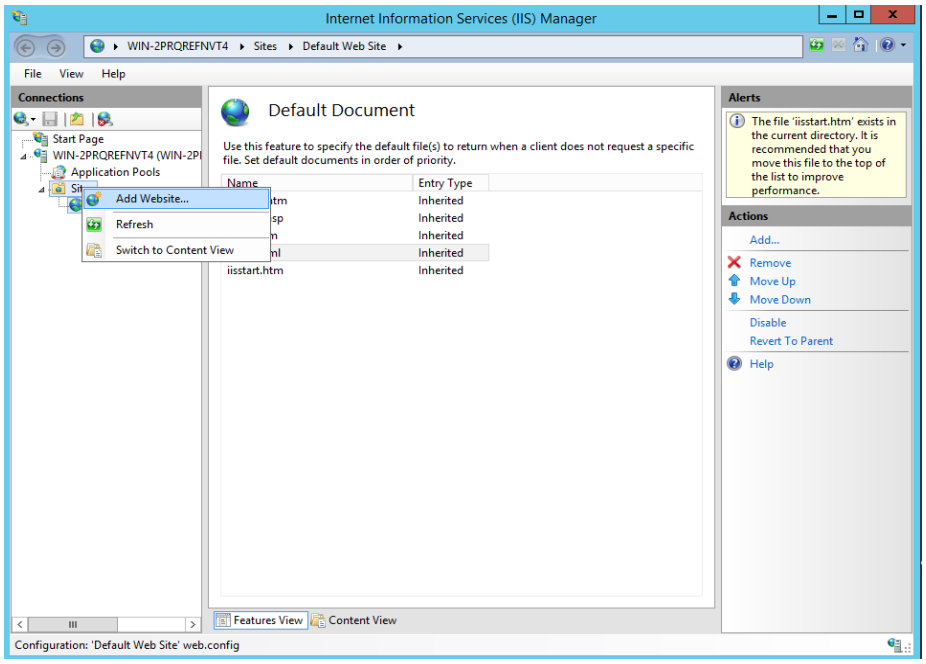


Figure 5.3.11 4 Adding new website

Step 5: Add new website details

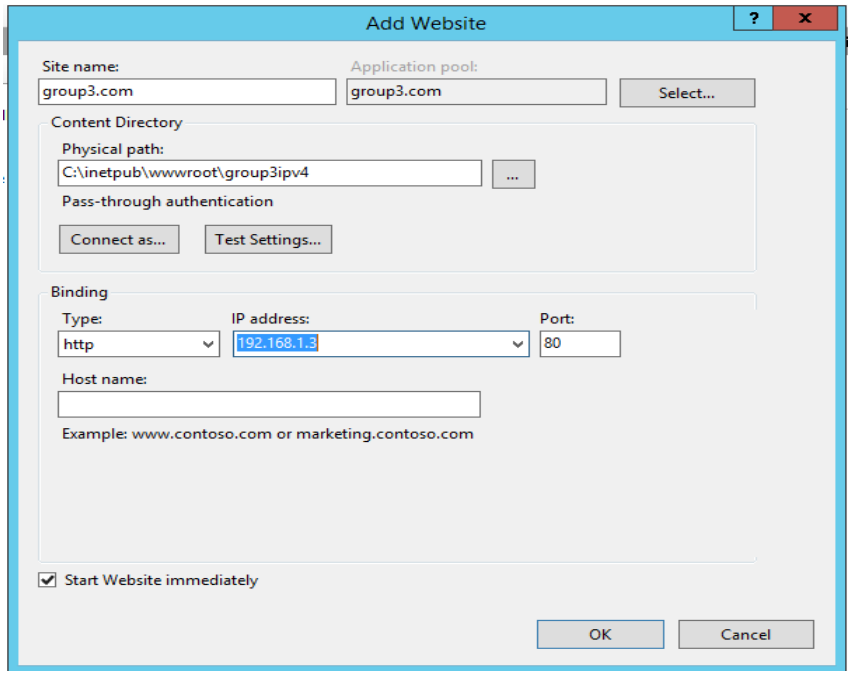


Figure 5.3.11 5 Adding website details

Step 6: Choose default document in group 3.com

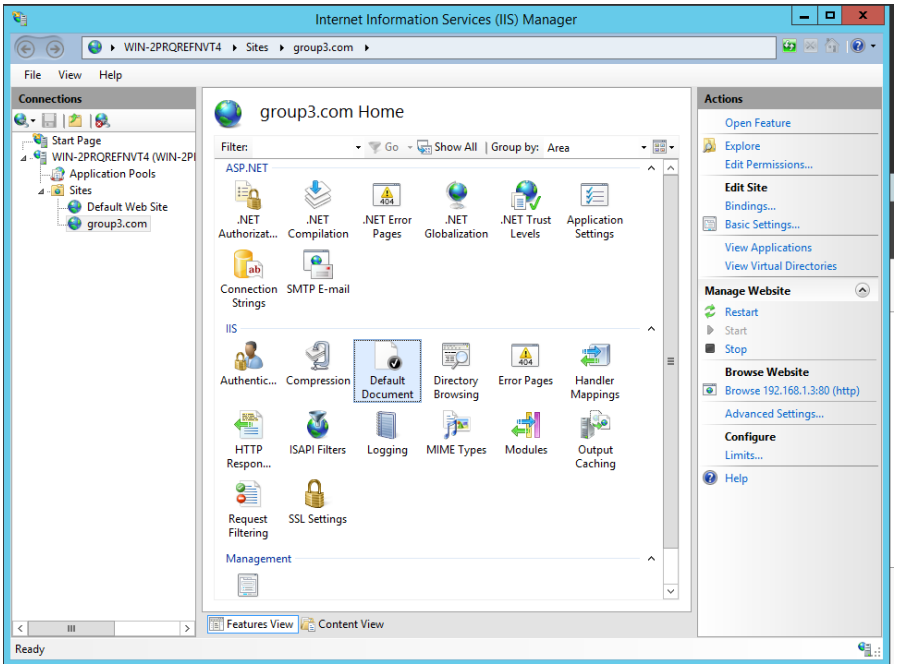


Figure 5.3.11 6 Choosing default document

Step 7: Create new default document group3ipv4

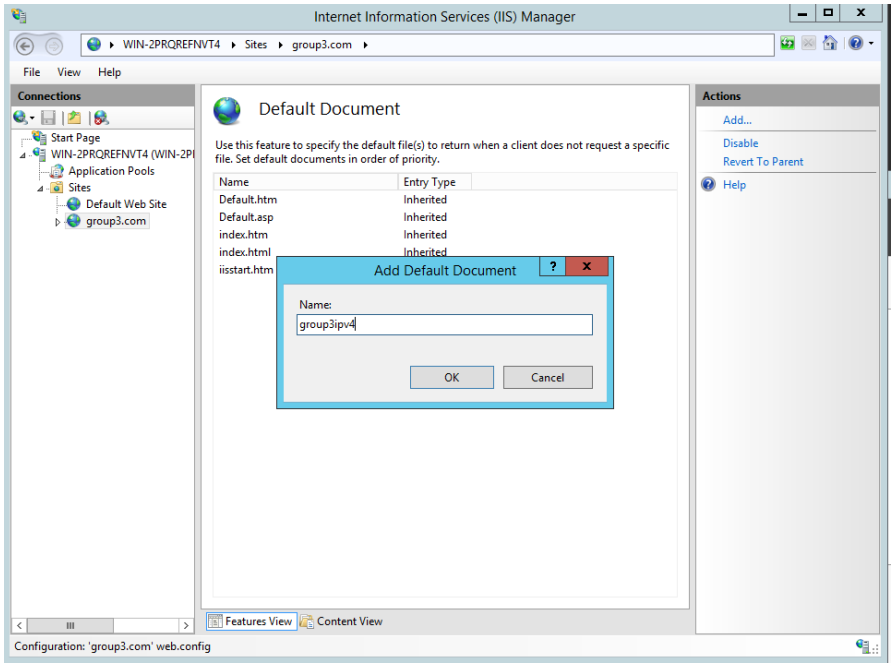


Figure 5.3.11 7 Creating default document

SSL

Step 1: Choose server certificate in IIS

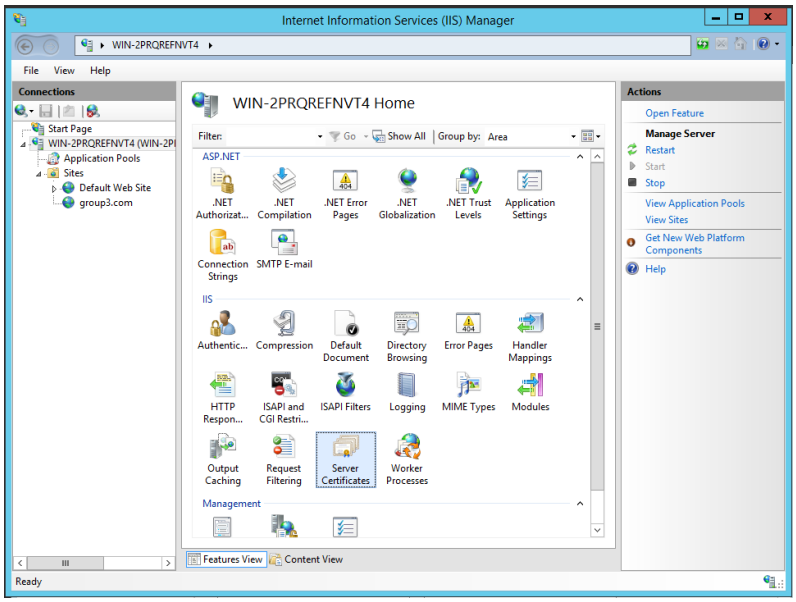


Figure 5.3.11 8 Clicking server certificates

Step 2: Create domain certificate (group3secured.com)

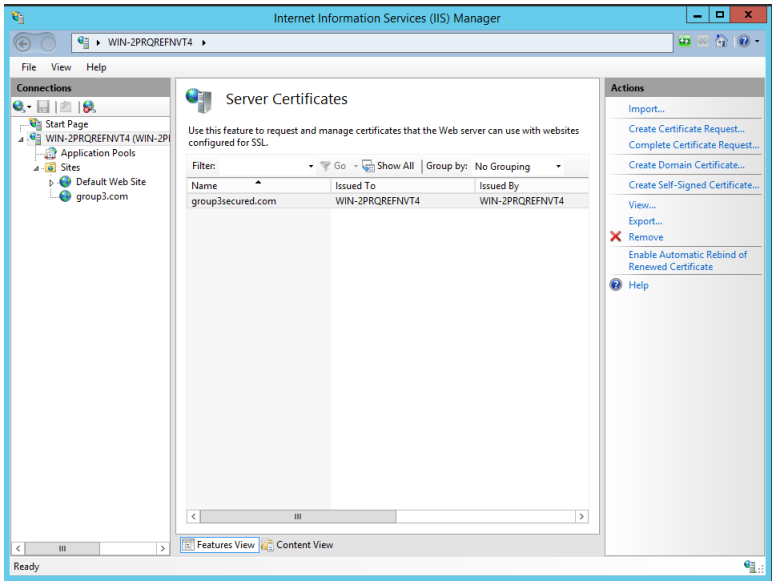


Figure 5.3.11 9 Creating certificate

Step 3: Add new website

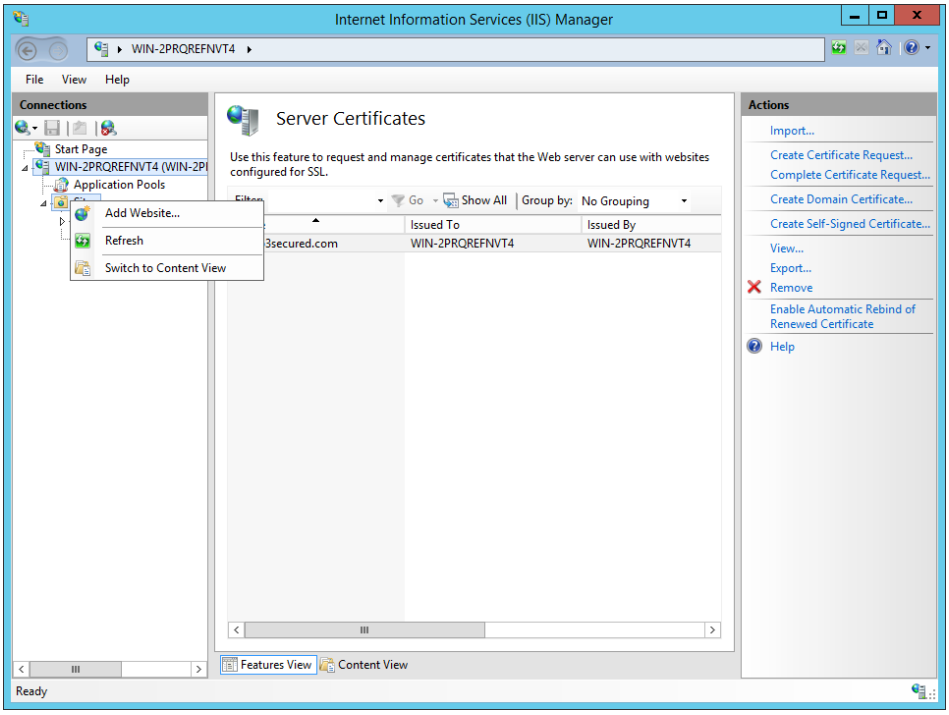


Figure 5.3.11 10 Adding new website

Step 4: Choose ssl certificate

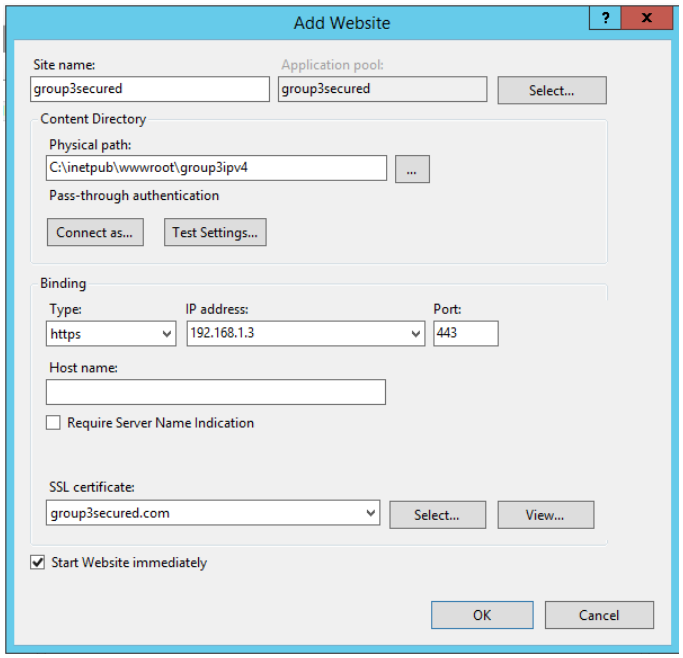


Figure 5.3.11 11 Adding ssl certificate for website

Step 5: Choose ssl settings

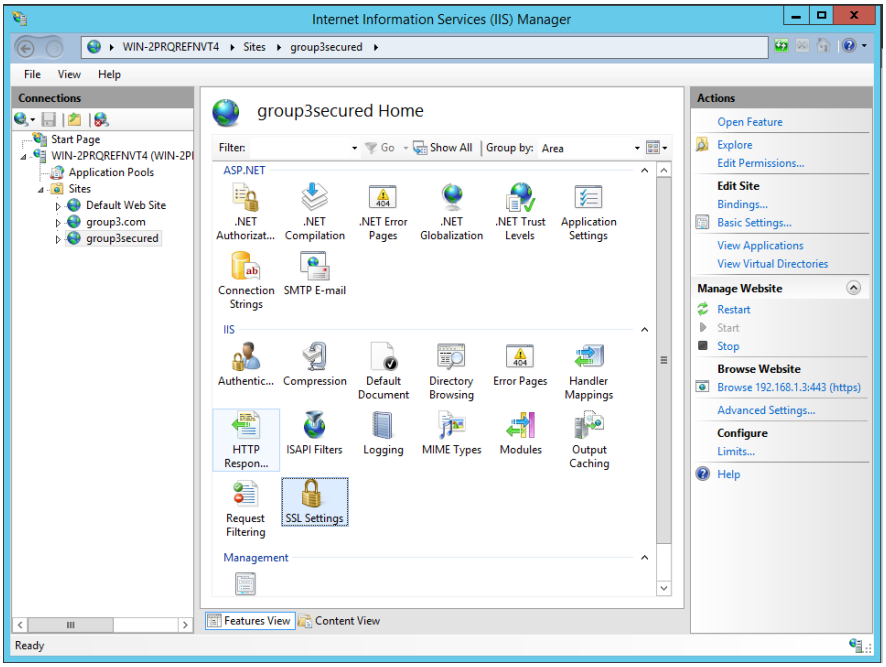


Figure 5.3.11 12 Selecting ssl cerificate

Step 6: In ssl settings click require ssl and click ignore

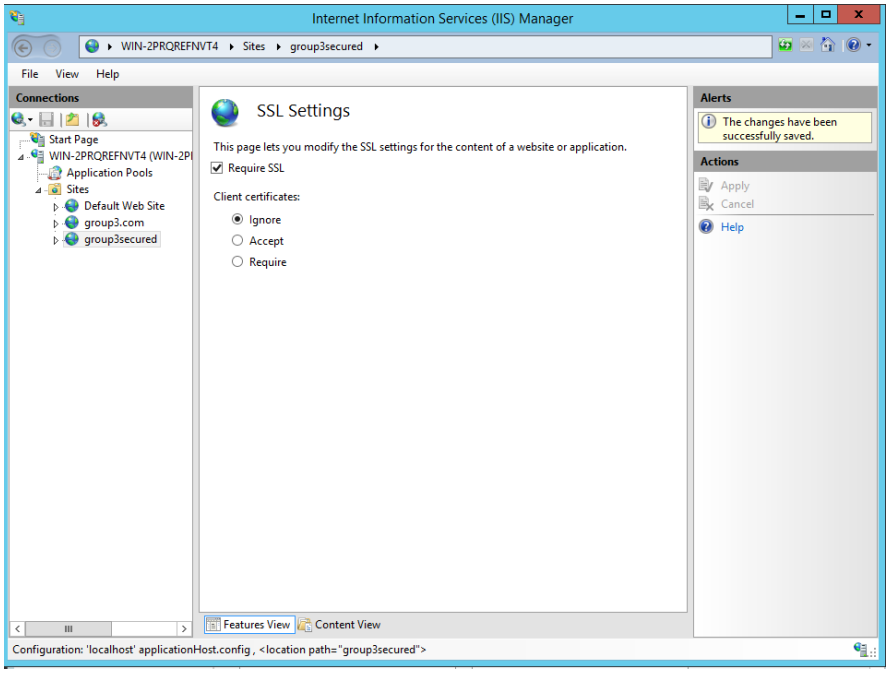


Figure 5.3.11 13 Click require ssl

VIRTUAL HOSTING

Step 1: Create new zone in forward lockup zones in DNS manager

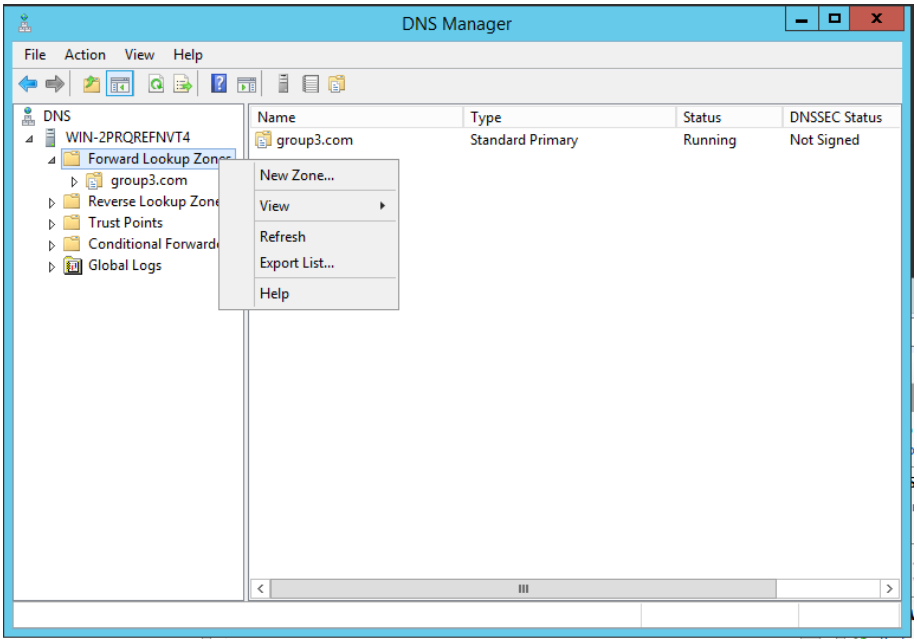


Figure 5.3.11 14 Creating new zone

Step 2: Click next

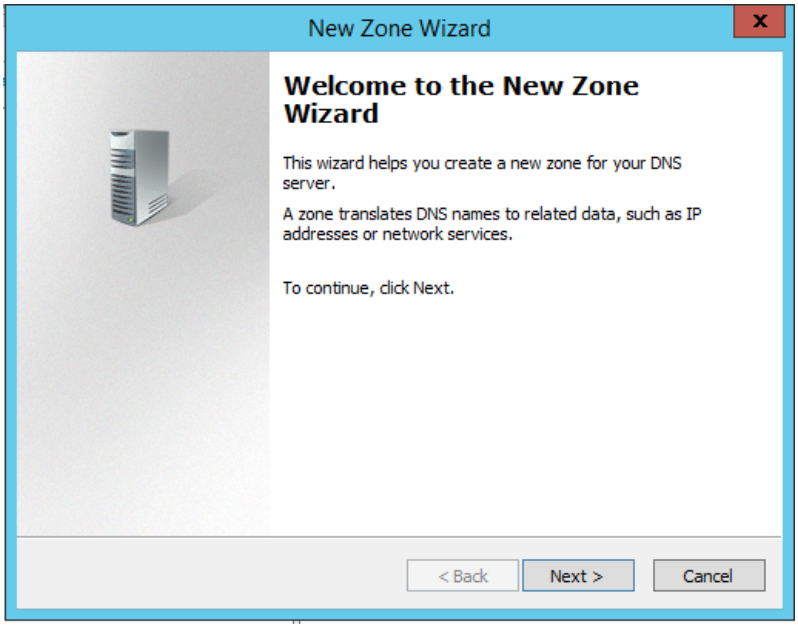


Figure 5.3.11 15 Create new zone in forward lockup zones in DNS manager

Step 3: Choose primary zone and click store zone in active directory. Then click next.

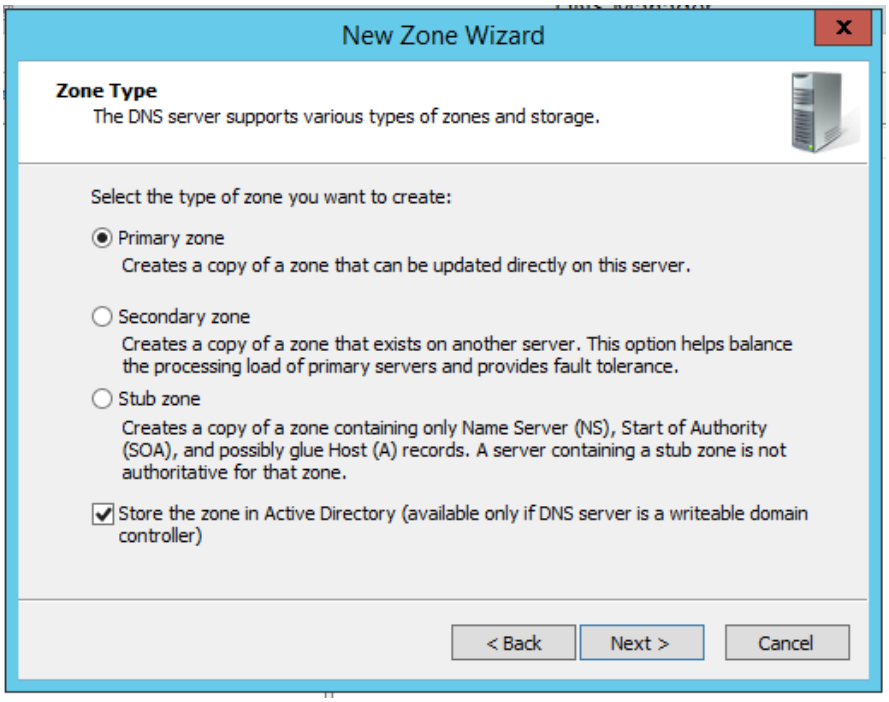


Figure 5.3.11 16 Choosing primary zone

Step 4: Choose domain: group3.com

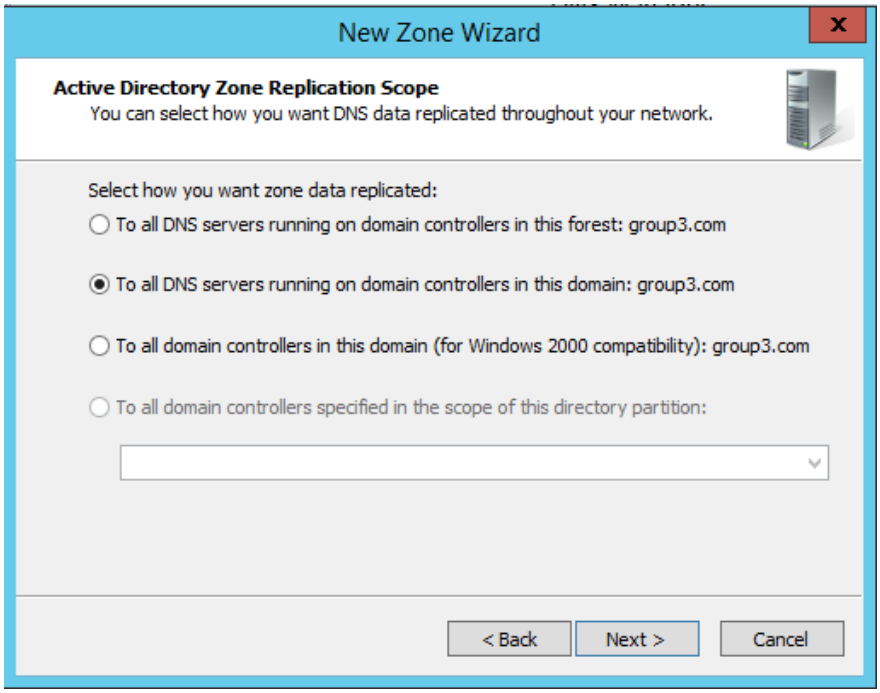


Figure 5.3.11 17 Choosing zone in wizard for Web

Step 5: Create new zone name

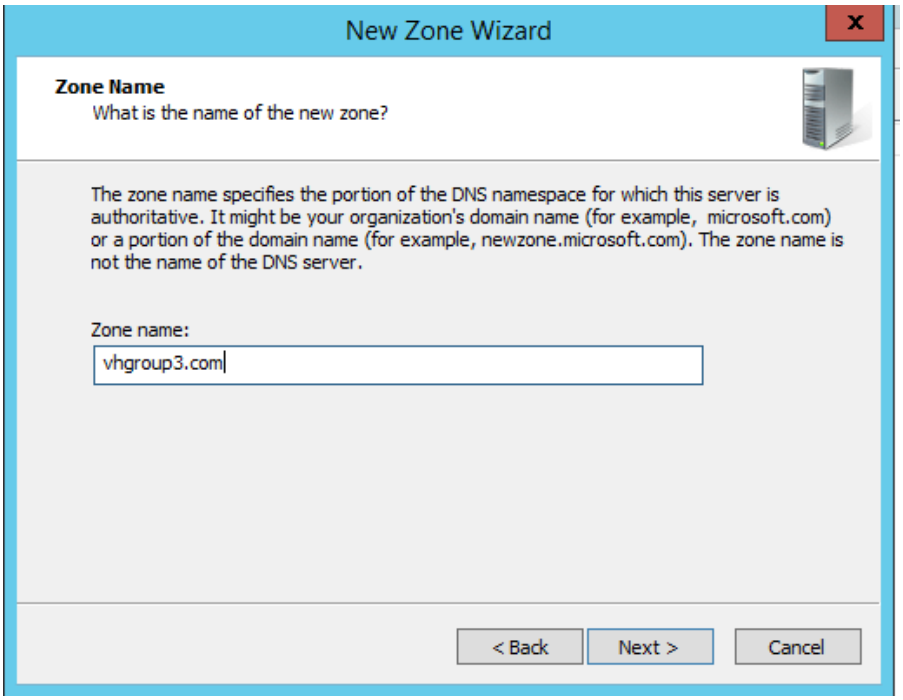


Figure 5.3.11 18 Creating new zone name

Step 6: Choose type of dynamic updates

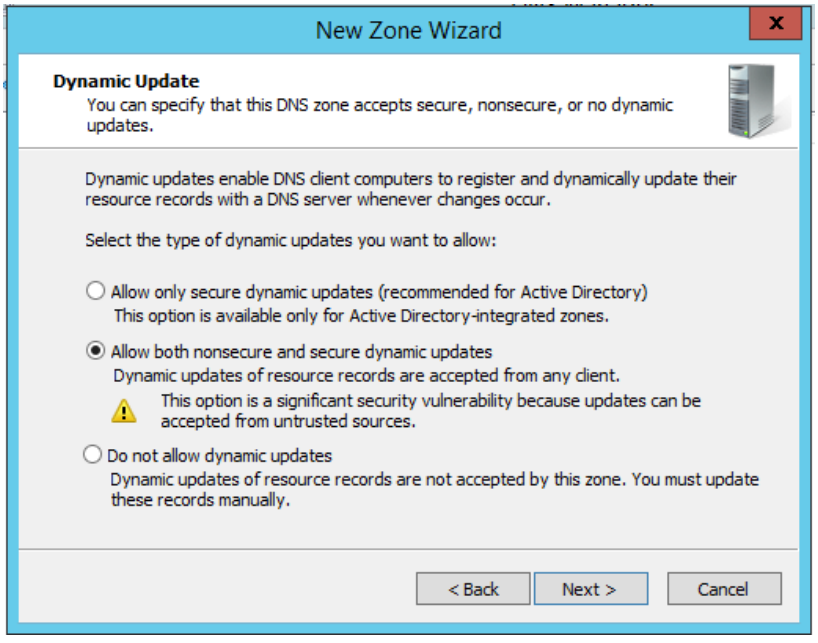


Figure 5.3.11 19 Choosing dynamic update

Step 7: New zone wizard created succesfully

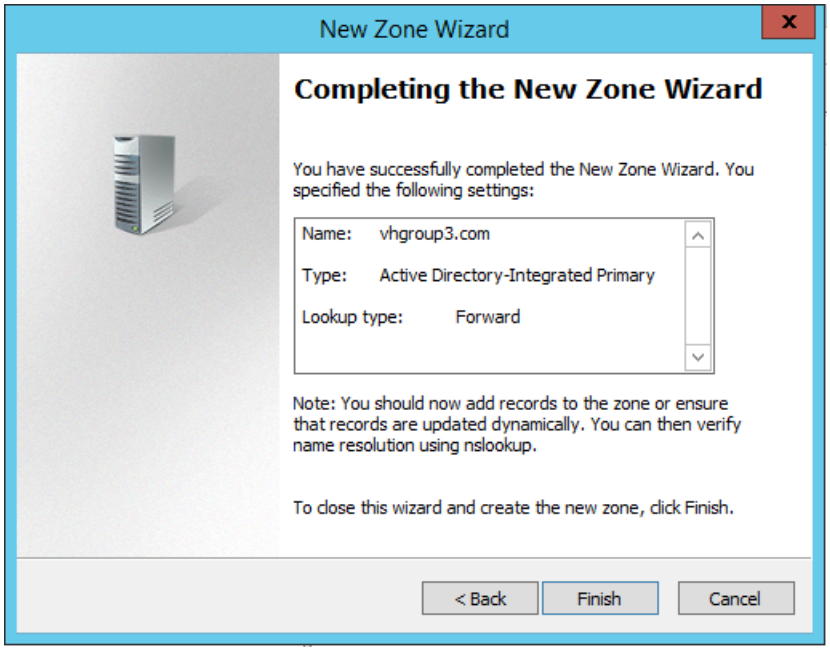


Figure 5.3.11 20 Created new zone vhgroup3.com

Step 8: Create new host by right –click the website and select the **New host (A Or AAA).**

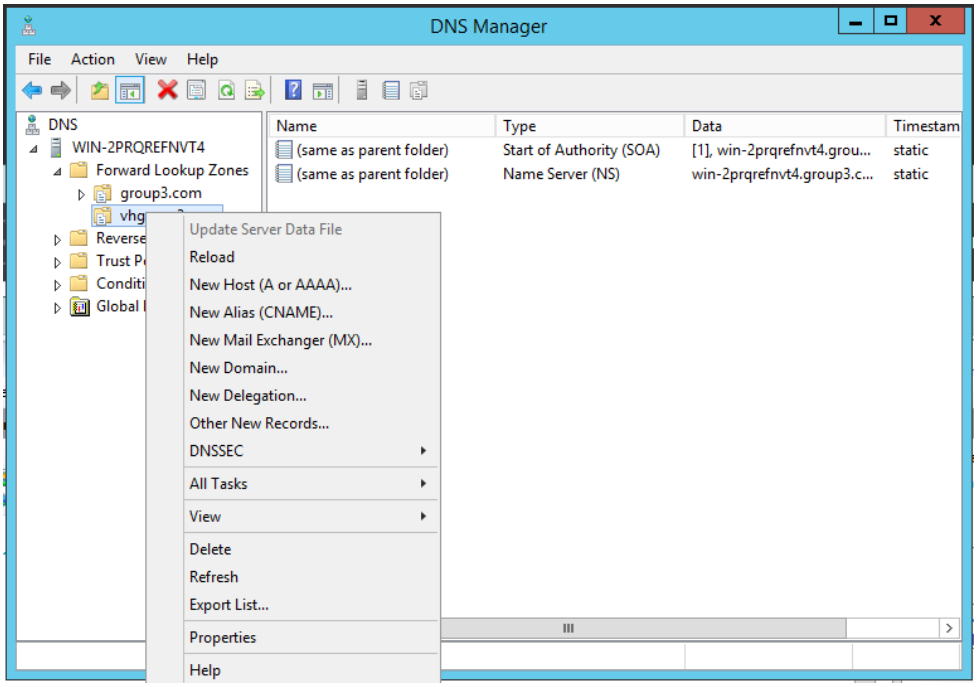


Figure 5.3.11 21 Adding host

Step 9: Type the ip address **192.168.1.3** and click the **add host**

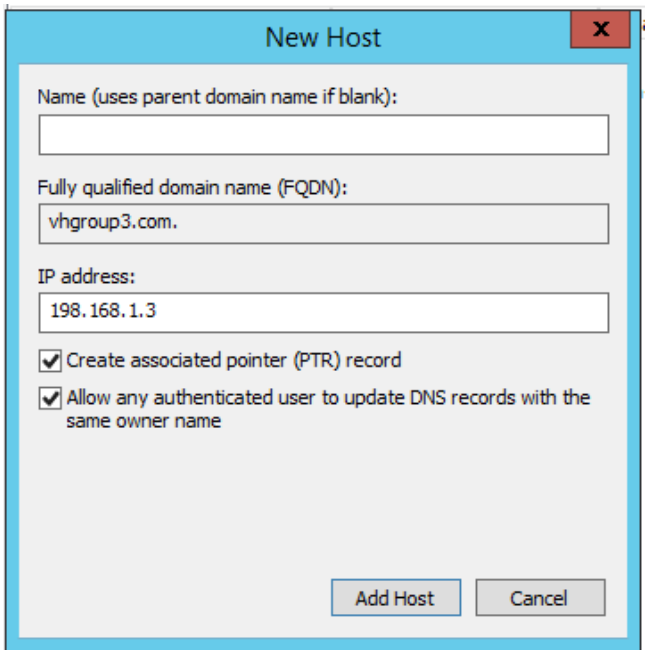


Figure 5.3.11 22 Entering ip address in new host

Step 10: Host created

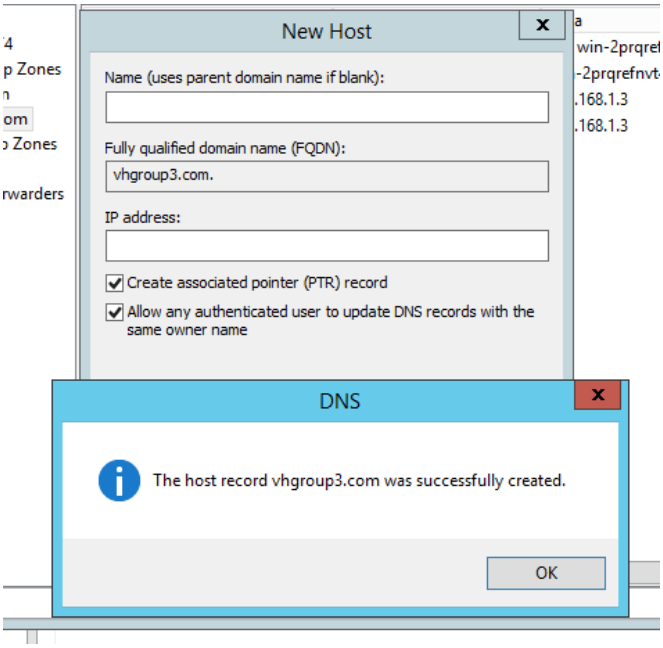


Figure 5.3.11 23 Host created

5.3.12 IPv6 Web with IPv6 Tunneling

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

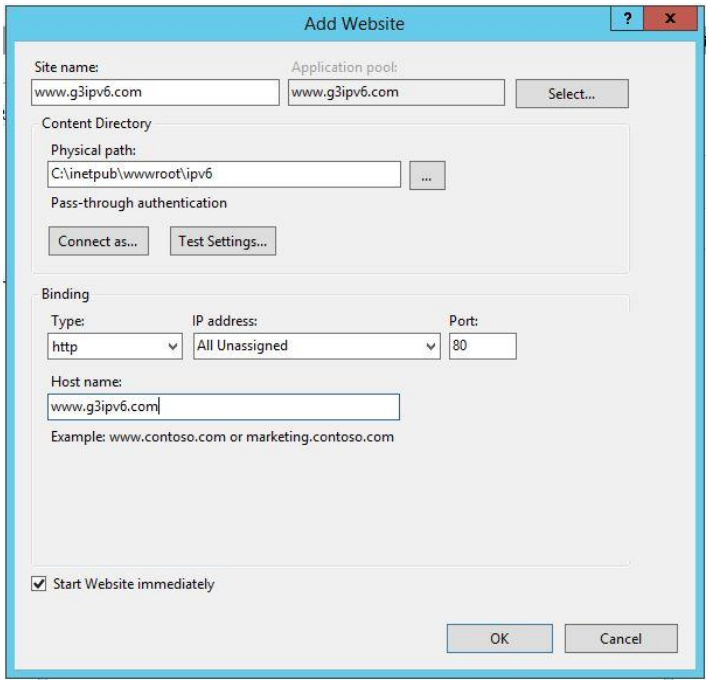


Figure 5.3.12 1 Adding new ipv6 website

Step 3: After finish new website has been created with name www.g3ipv6.com

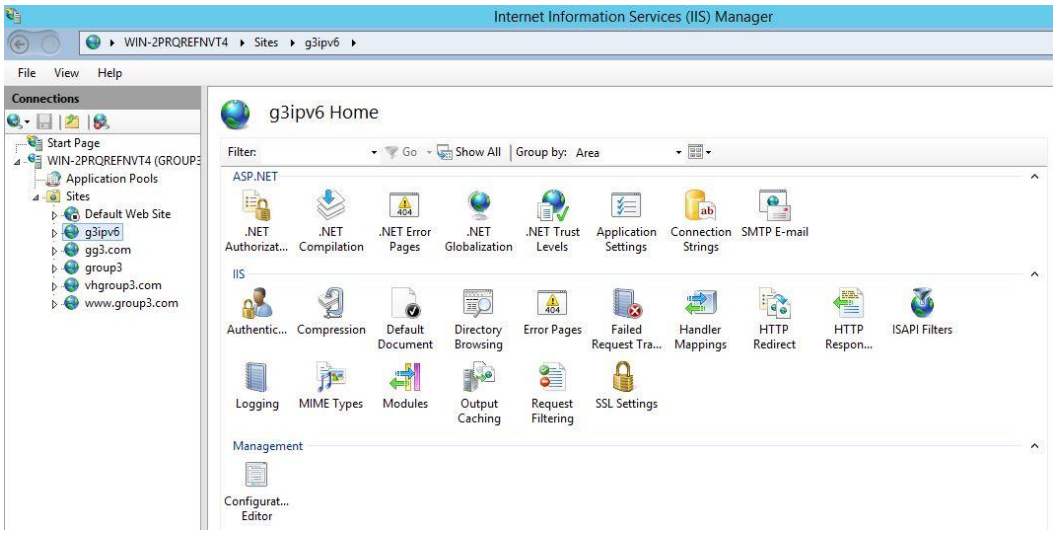


Figure 5.3.12 2 Successfully created ipv6 website

Step 4: Edit Bindings

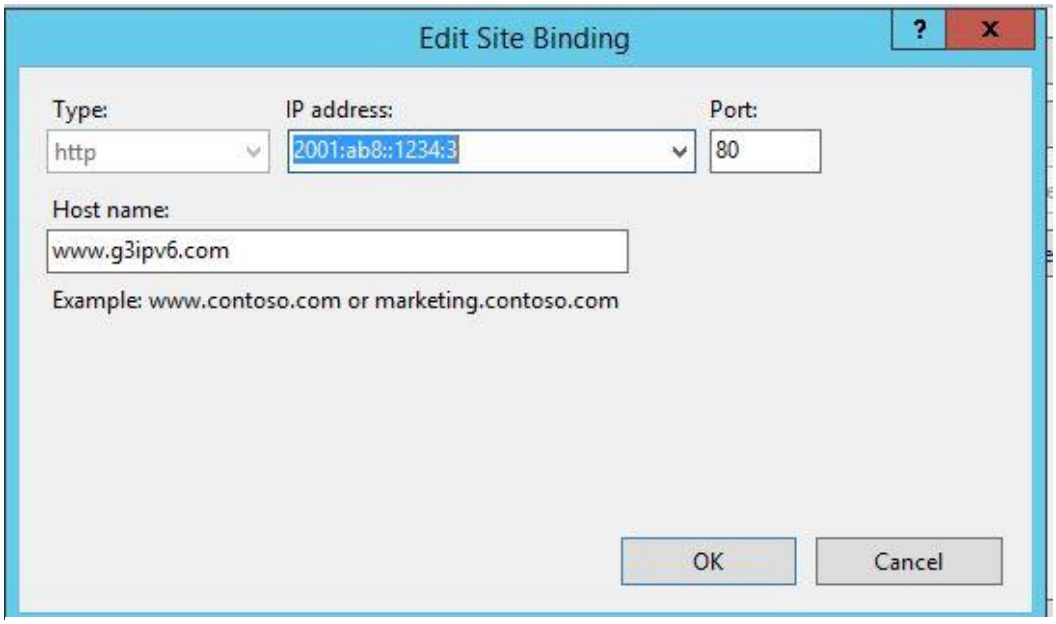


Figure 5.3.12 3 Binding ipv6 address

Step 5: In DNS, insert zone name www.g3ipv6.com

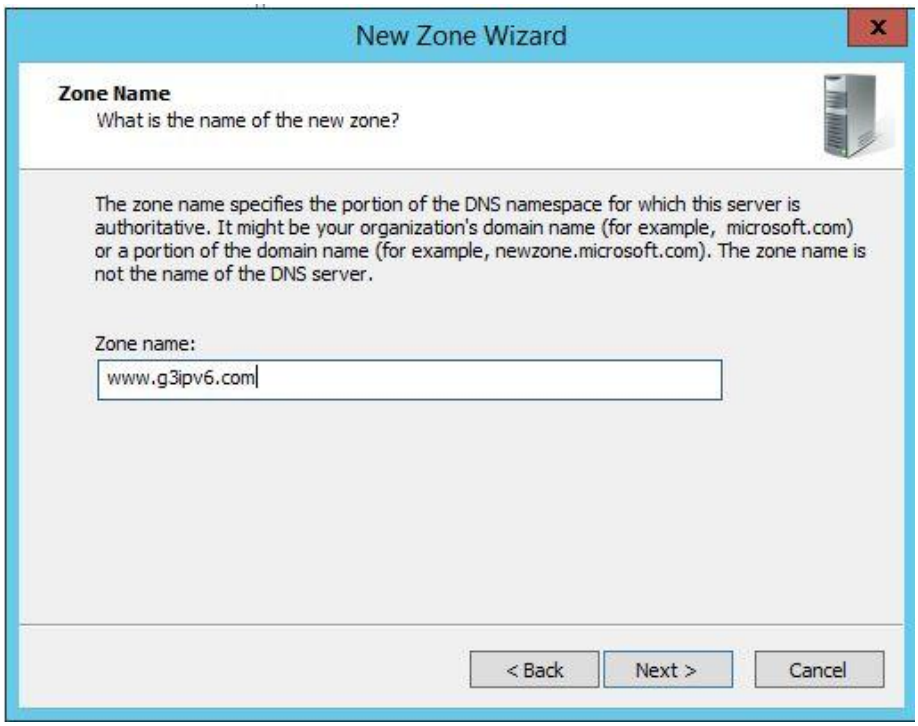


Figure 5.3.12 4 Creating new zone name for 1pv6

Step 6: Create a new zone at Forward Lookup Zones > g3ipv6.com

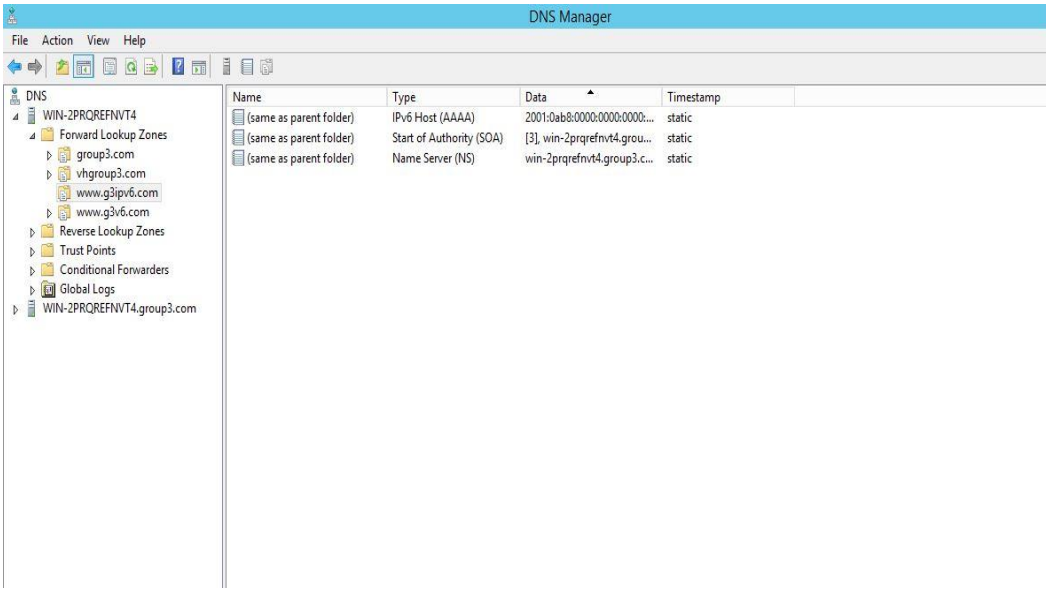


Figure 5.3.12 5 Create a new zone at Forward Lookup Zones

Step 7: After insert zone, Right click > Set the Host

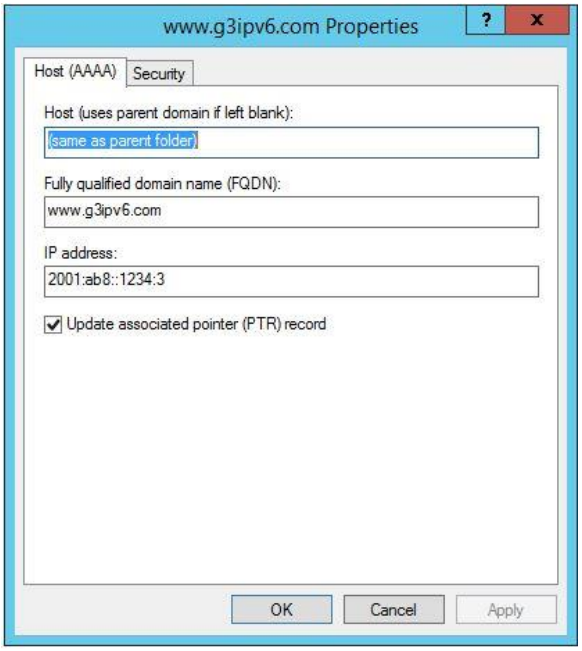


Figure 5.3.12 6 Set the Host

IPv6 Tunneling

To configure 6to4 tunneling, 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.

Step 1: Open PuTTY and fill all requirement needed and click open.

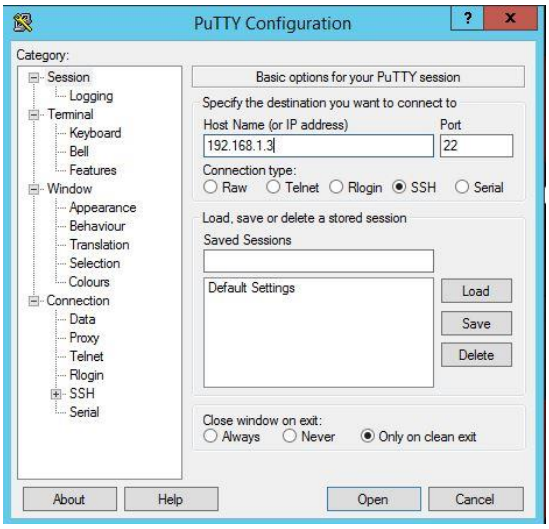


Figure 5.3.12 7 Open putty

Step 2: Login as authorized user and enter password to start configuration.

Figure 5.3.12 8 Login into putty

Step 3: Enter the command for IPv6 tunneling as show below and save the config.

Figure 5.3.12.9: IPv6 tunneling configuration

```
crypto map CMAP 10 ipsec-isakmp
 set peer 200.200.200.1
 set transform-set TS
 match address VPN-TRAFFIC
!
!
!
!
interface Tunnel2
 no ip address
 ipv6 address 2008:A0A8:800::9/123
 ipv6 enable
 ipv6 ospf 10 area 0
 tunnel source Serial0/2/0
 tunnel destination 200.200.200.1
 tunnel mode ipv6ip
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet0/0.10
!
interface FastEthernet0/0.40
!
interface FastEthernet0/0.50
 shutdown
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/1.10
 encapsulation dot1Q 10
 ip address 192.168.1.1 255.255.255.0
 ip helper-address 192.168.1.3
 no snmp trap link-status
 ipv6 address 2001:AB8::1234:1/64
 ipv6 ospf 10 area 0
 crypto map CMAP
!
interface FastEthernet0/1.20
 encapsulation dot1Q 20
 ip address 192.168.2.1 255.255.255.0
 ip helper-address 192.168.1.3
 no snmp trap link-status
 ipv6 address 2001:BB8::1234:1/64
 ipv6 ospf 10 area 0
!
interface FastEthernet0/1.30
 encapsulation dot1Q 30
 ip address 192.168.3.1 255.255.255.0
 ip helper-address 192.168.1.3
 no snmp trap link-status
 ipv6 address 2001:CB8::1234:1/64
```

Figure 5.3.12 9 Enter the command for IPv6 tunneling

5.3.13 IPSec Site-To-Site Tunneling

Step 1 : Create an ISAKMP phase 1 policy.

Figure 5.3.13 1 Create ISAKMP phase 1 policy

Step 2 : Create an encryption method to be used for Phase 1. This encryption method is to secure and encrypt our packet and connection between the tunnel.

Figure 5.3.13 2 Create an encryption method

Step 3: Create an hashing algorithm to be used for Phase 1.

Figure 5.3.13 3 Create hashing algorithm

Step 4 : Configure Pre-Shared key as the authentication method and the session key lifetime, Expressed in either kilobytes (after x-amount of traffic, change the key) or seconds. Value set is the default value.

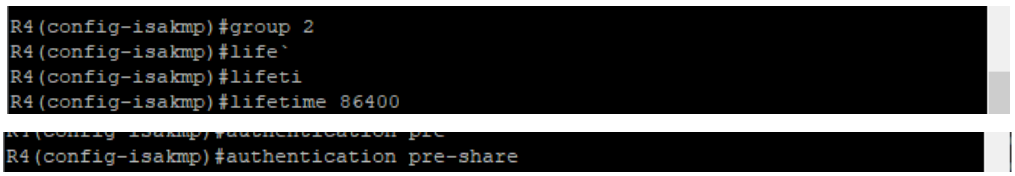


Figure 5.3.13 4 Configure Pre Shared Key

Step 5 : Create the pre share key authentication with our peer (Next group router). The peer's pre shared ker is set to Group4 and its public IP address is 1.1.1.2. Every time the router try to establish a tunnel with the other group router (1.1.1.2), this pre shared key will be used.

```
R4(config)#crypto isa
R4(config)#crypto isakmp key Group4 address 1.1.1.2
```

Figure 5.3.13 5 Define a pre shared key

Step 6 : Create an access-list and define the traffic we would like the router to pass through the VPN tunnel. In this configuration it would be traffic from one network to the other, 192.168.1.0/30 to 192.168.6.0/30.

```
R4(config)#ip access-list extended VPN-TRAFFIC
R4(config-ext-nacl)#permit ip 192.168.6.0 0.0.0.3 192.168.1.0 0.0.0.3
```

Figure 5.3.13 6 Create an access-list

Step 7 : Create the transform set used to protect our data. We've named this TS.

```
R4(config)#crypto ipsec transform-set TS esp-3des es
R4(config)#crypto ipsec transform-set TS esp-3des esp-md
R4(config)#crypto ipsec transform-set TS esp-3des esp-md5-hmac
R4(cfg-crypto-trans)#
```

Figure 5.3.13 7 Create the transform set

Step 8 : Create the Crypto Map and connects the previously defined ISAKMP and Ipsec configuration together. We've named our crypto map CMAP. The ipsec-isakmp tag tells the router that this crypto map is an Ipsec crypto map.

```
R4(config)#crypto map CMAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
R4(config-crypto-map)#set p
R4(config-crypto-map)#set p
R4(config-crypto-map)#set
R4(config-crypto-map)#set peer 1.1.1.2
R4(config-crypto-map)#set tra
R4(config-crypto-map)#set transform-set TS
R4(config-crypto-map)#matc
R4(config-crypto-map)#match add
R4(config-crypto-map)#match address VPN-TRAFFIC
```

Figure 5.3.13 8 Create the Crypto Map

Step 9 : Apply the crypto map to the outgoing interface of the router to another router. Here, the outgoing interface is Serial 0/2/0.

```
R4(config)#int s0/2/0
R4(config-if)#cry
R4(config-if)#crypto map CMAP
R4(config-if)#
*Jan  1 04:28:45.422: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

Figure 5.3.13 9 Apply the crypto map to the outgoing interface

5.3.14 Active Directory

Step 1: Open Server Manager and select Add roles and features. This will launch the Roles and Features.

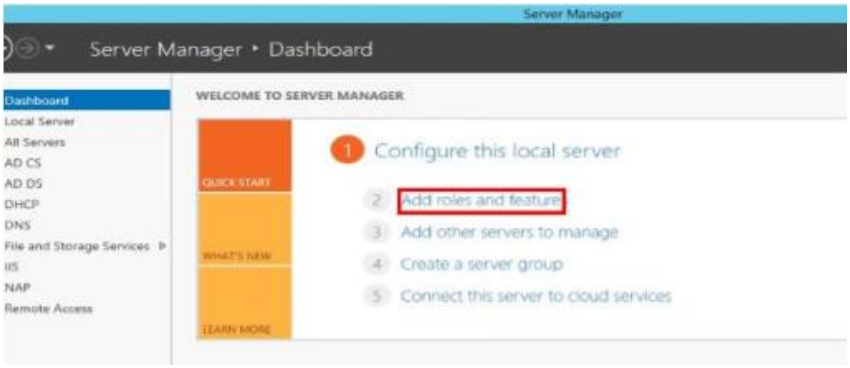


Figure 5.3.14 1 Add roles and features for Active Directory

Step 2: Select Role-based or features-based installation from the Installation Type screen and click Next.

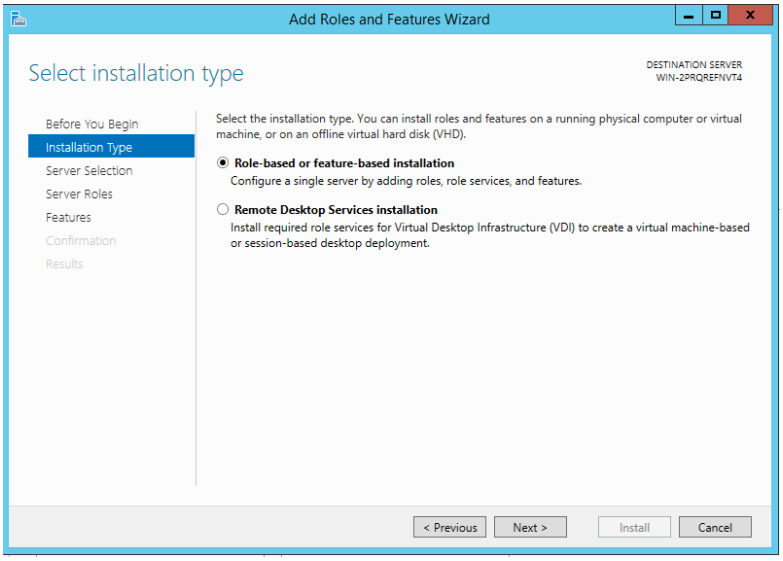


Figure 5.3.14 2 Select installation type for Active Directory

Step 3: Review and select optional features to install during the AD DS installation by placing a check in the box next to any desired features, and then click Next.

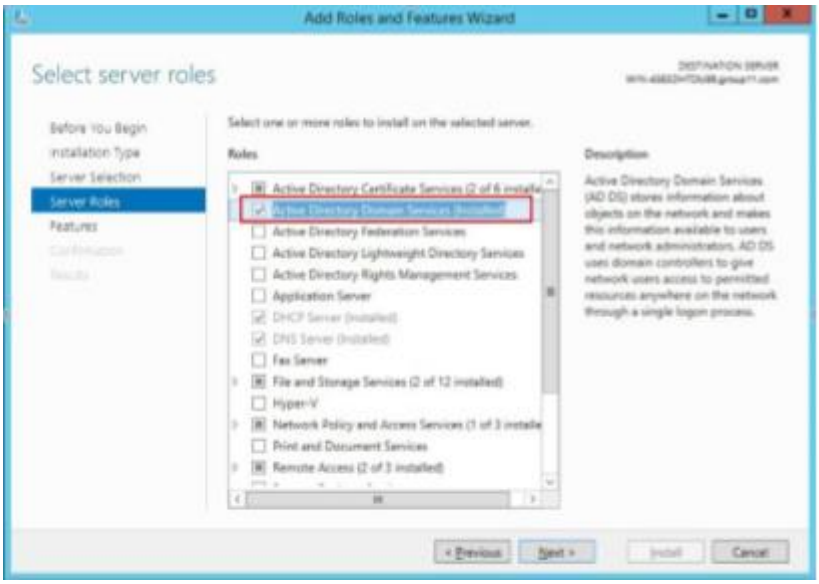


Figure 5.3.14 3 Select server roles for Active Directory

Step 4: Review the information on the AD DS tab and click Next. On the confirm installation selections screen, review the installation and then click Install.

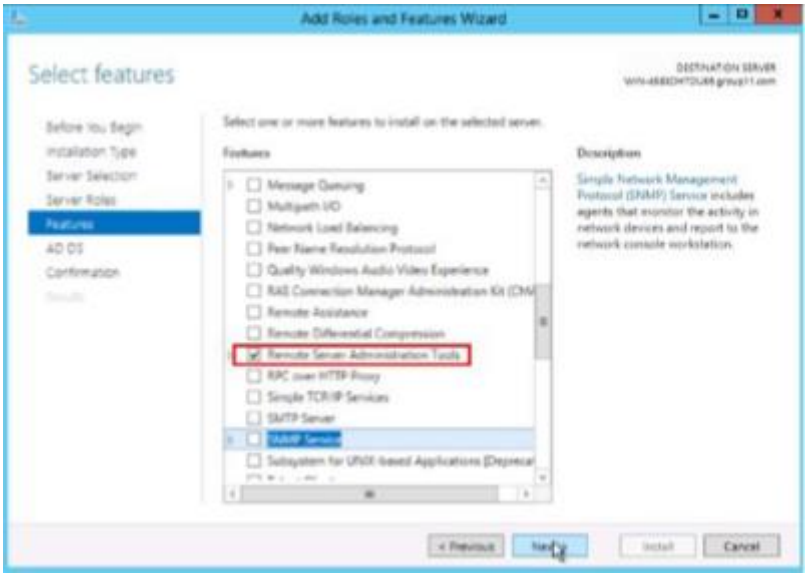


Figure 5.3.14 4 Select features for Active Directory

Step 5: On the Server Manager, go to Tools > Active Directory Users and Computers to configure.

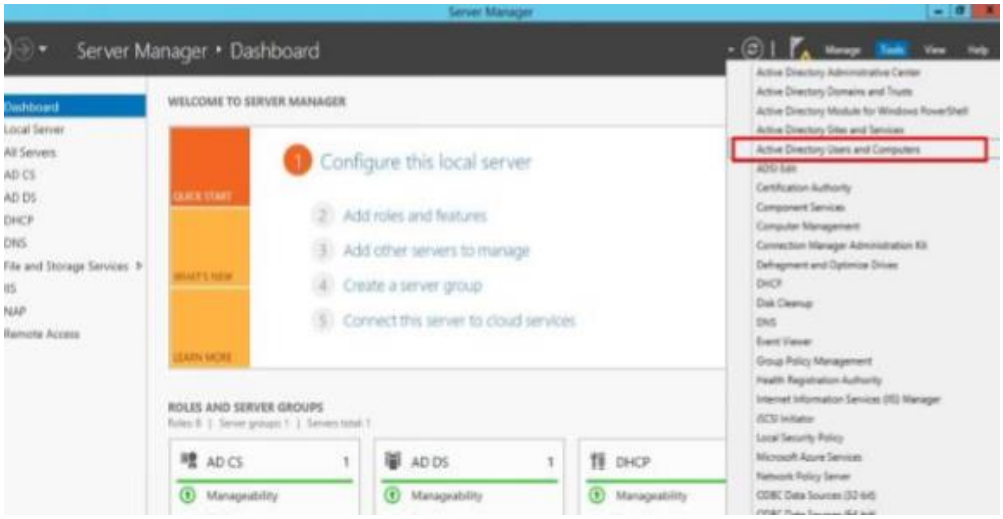


Figure 5.3.14 5 Choose Active Directory Users and Computers

Step 6: Right click on Users and select New > User in order to add a new user for AD.

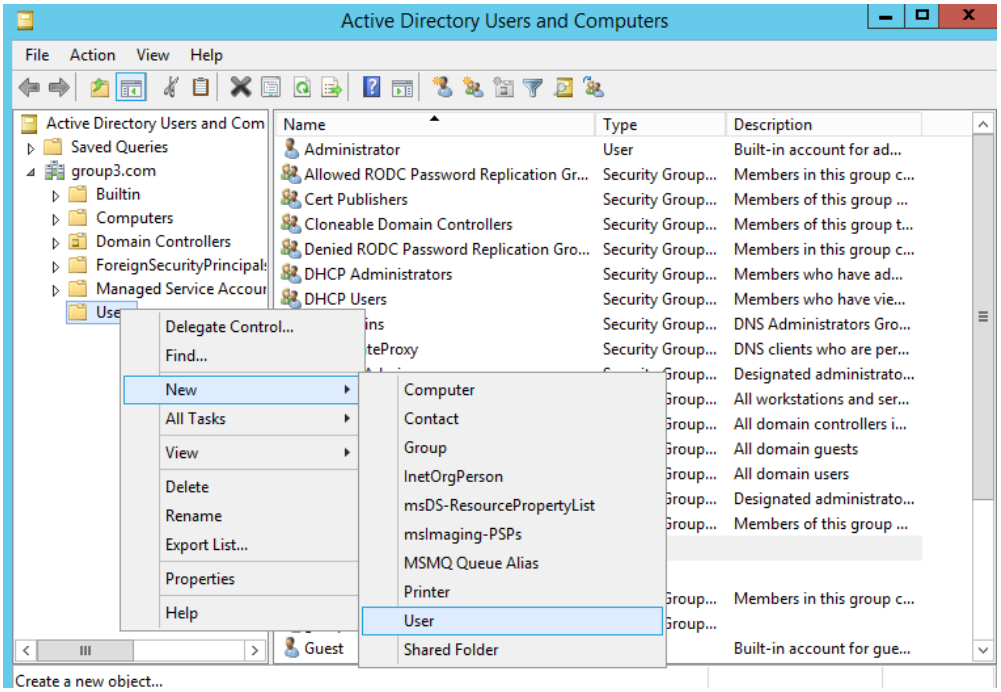


Figure 5.3.14 6 Create a user for Active Directory

Step 7: Configure the new user by entering the First name and Full name, and also User login name of the user, click Next when done.

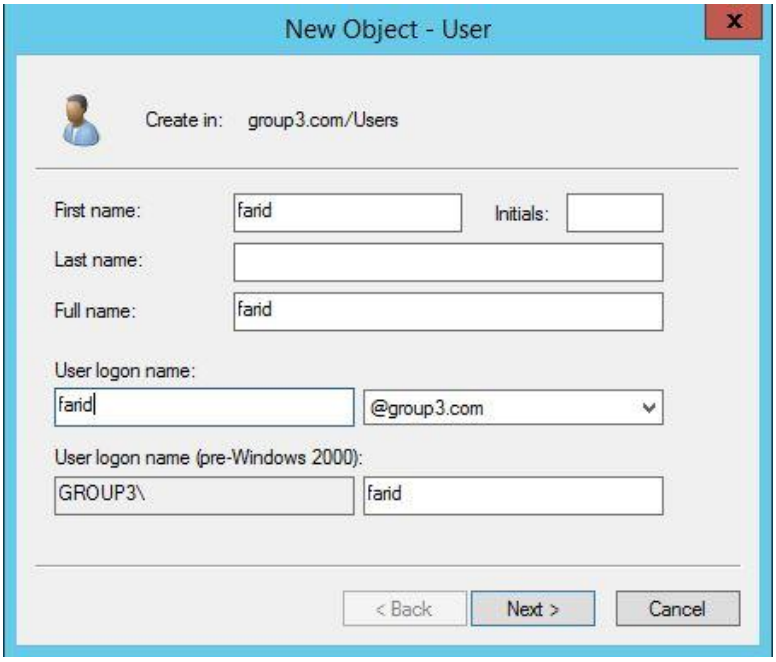


Figure 5.3.14 7 Create name for user Active Directory

Step 8: Set the password for user and set password never expires.

Figure 5.3.14 8 Create password user for Active Directory

Step 9: Review the new user and then click finish to create the user.

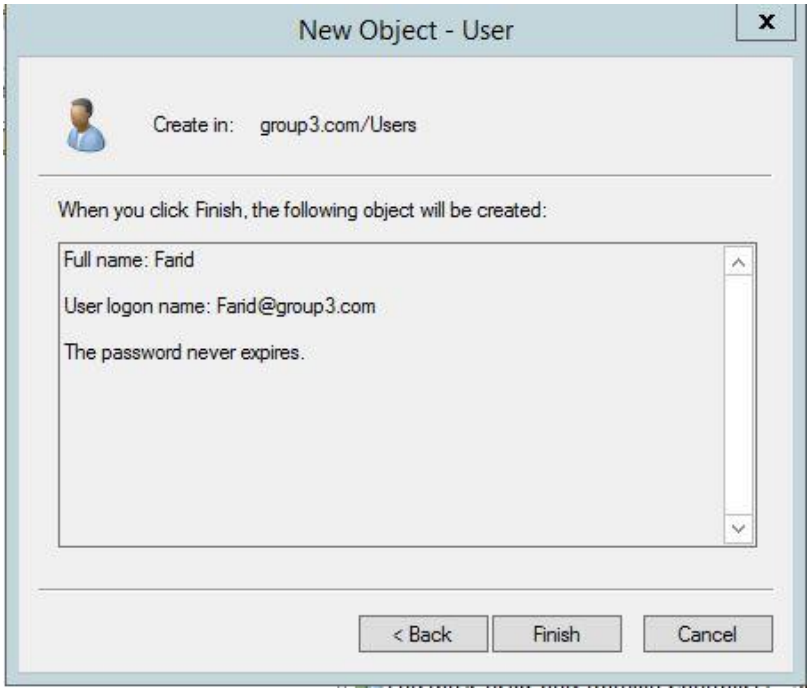


Figure 5.3.14 9 Complete create user for Active Directory

Step 10: Create new group by right-clicking at the user.

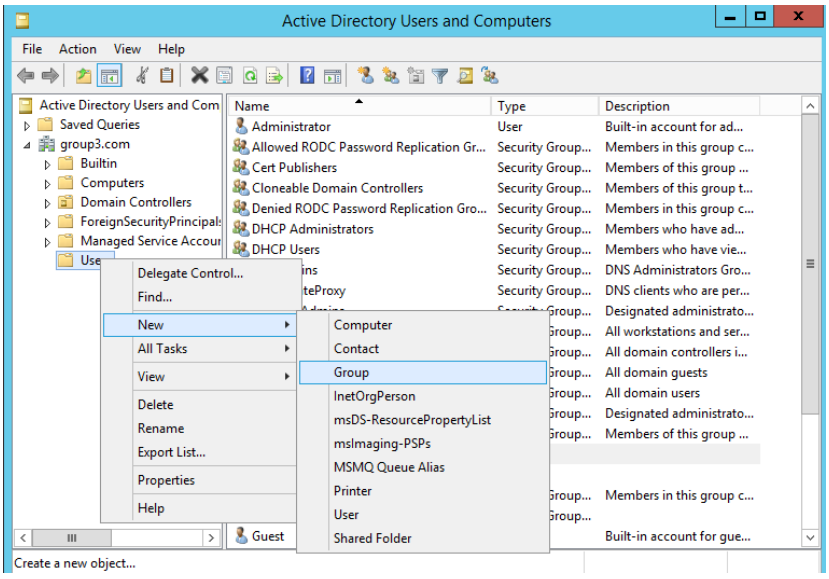


Figure 5.3.14 10 Create group for Active Directory

Step 11: Configure the new group by entering the group name (as what it is created for) and then click OK. This group is created for IT department in the organization.

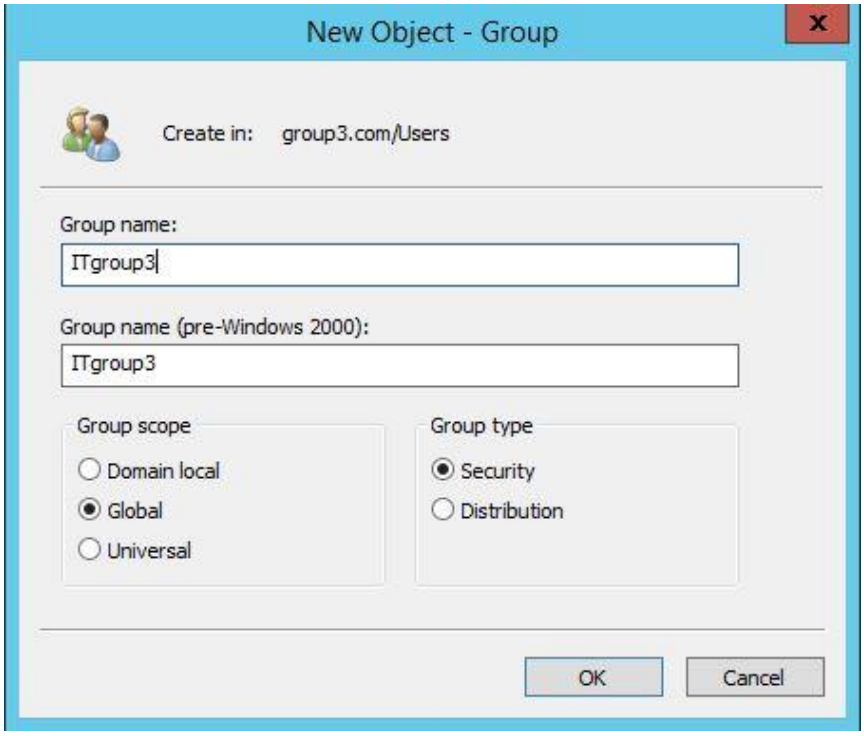


Figure 5.3.14 11 Create group name for Active Directory

Step 12: Configure users to add to a group by selecting "add to a group" and then choose the desired group as in this case is ITgroup3 and then click OK.

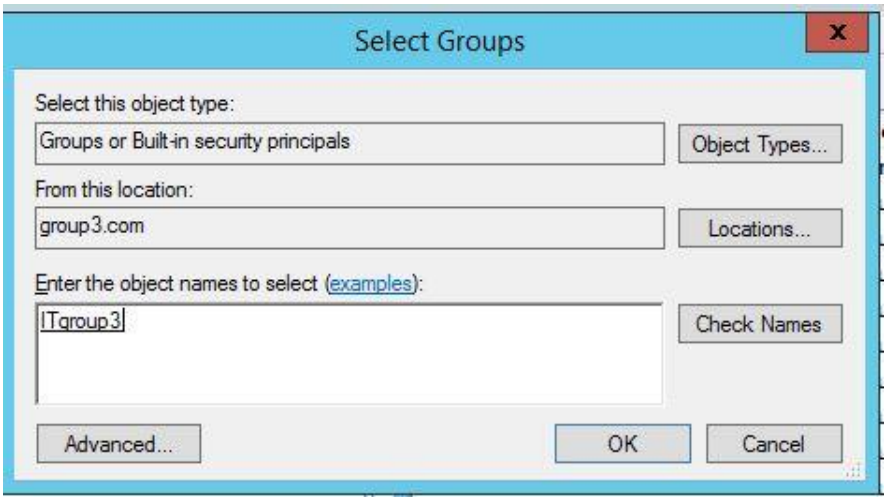


Figure 5.3.14 12 Add to a group for Active Directory

Figure 5.3.14 13 Complete create group for Active Directory

Step 13: Configure user to add to a group and right click the user, and select "Add to a group". Type "Dom" and click check names.

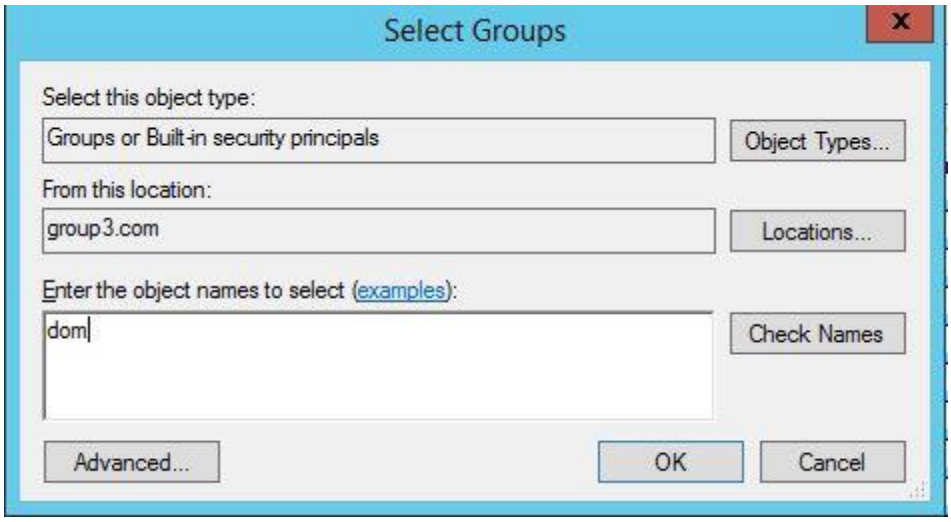


Figure 5.3.14 14 Add Active Directory user for group

Step 14: Add the users to desired domain users group and then click OK.

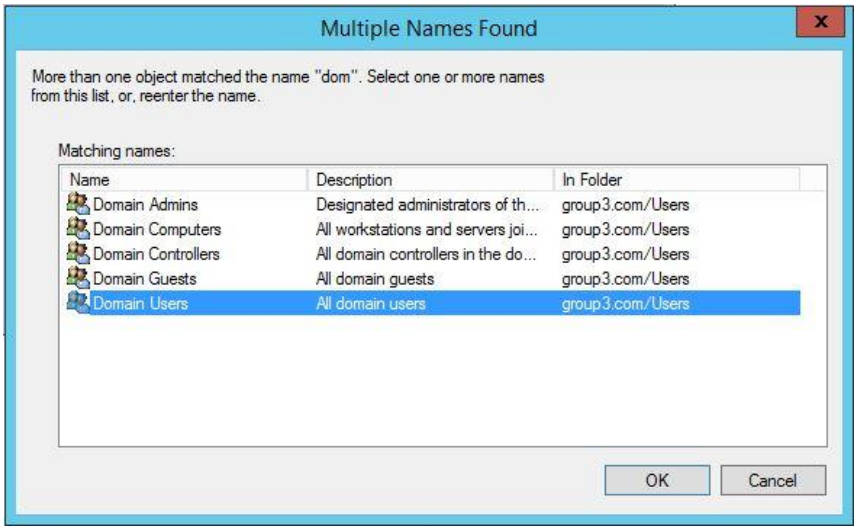


Figure 5.3.14 15 Add users to desired domain users group for Active Directory

Step 15: To check the user successfully to the group, click on the Domain Admins Group and then click on the members tab to show.

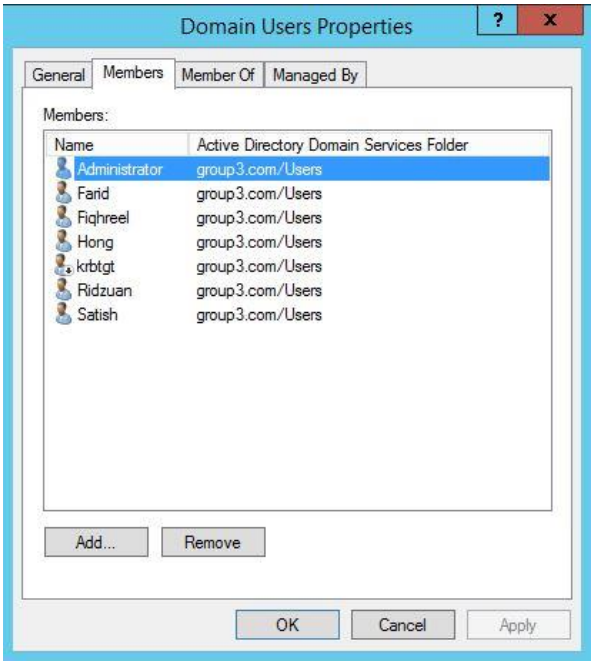


Figure 5.3.14 16 Show user members for Active Directory

Step 16: Repeat the step from 6-13 for other users and in order to add users to a group; Hong, Satish, Ridzuan and Fiqhril.

Step 17: In the local security policy setting, set the account lockout policy.

Account lockout duration: 1 minutes

Account lockout threshold: 3 invalid logon attempts

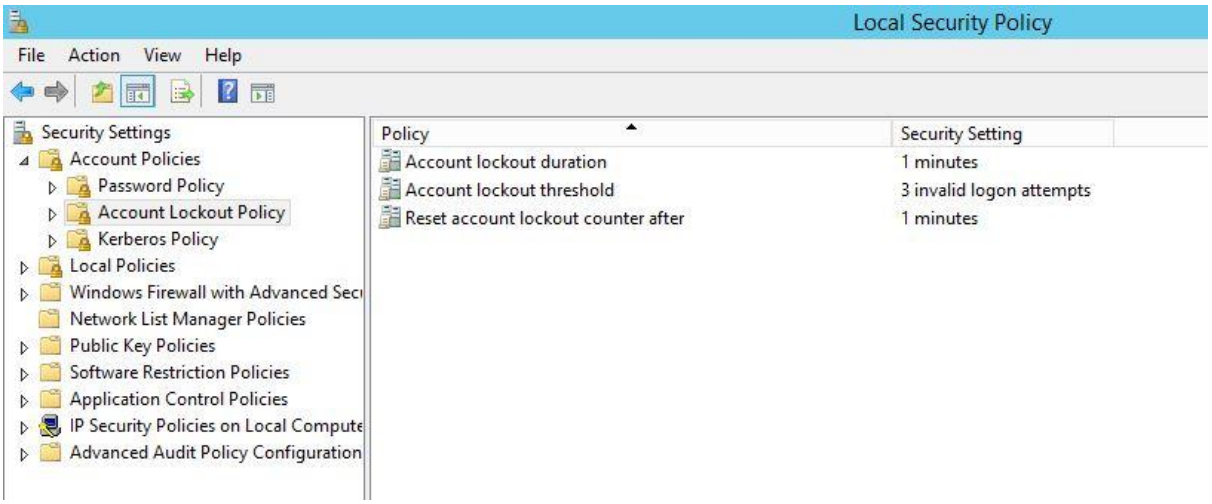


Figure 5.3.14 17 Set account lockout policy for Active Directory

5.3.15 Wireless User Authentication Using Radius Server

Step 1: Connect your wireless access point with your computer.

Step 2: Use web browser to access the access point web management on “192.168.1.1”.

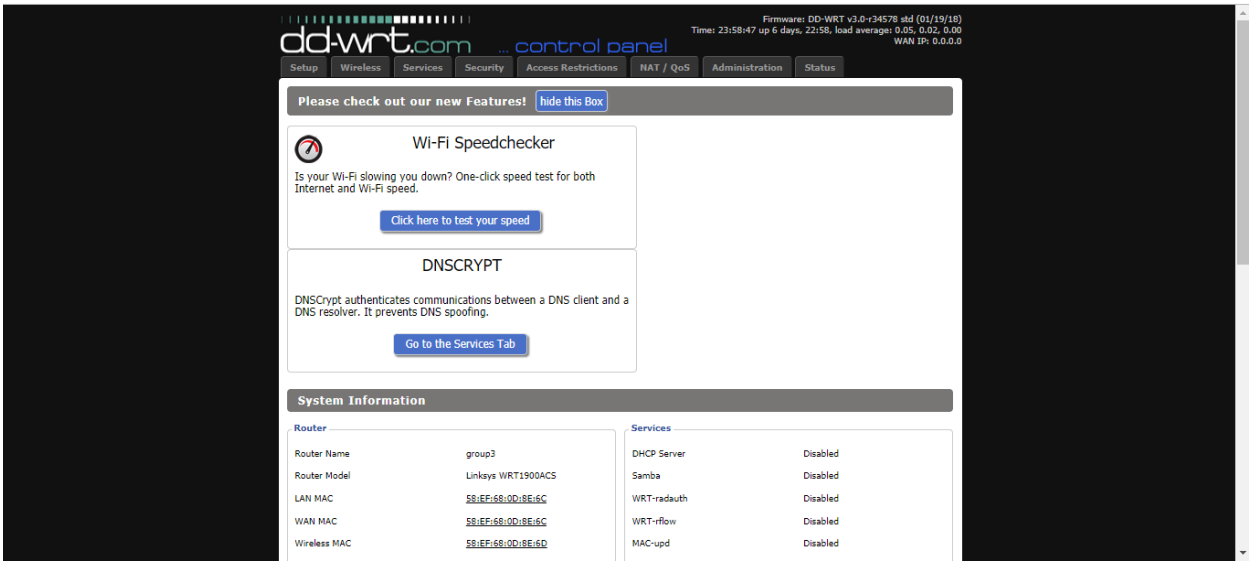


Figure 5.3.15 1 Main page for access point web management

Step 3: Change the basic settings of your access point such as hostname, IP address and etc.

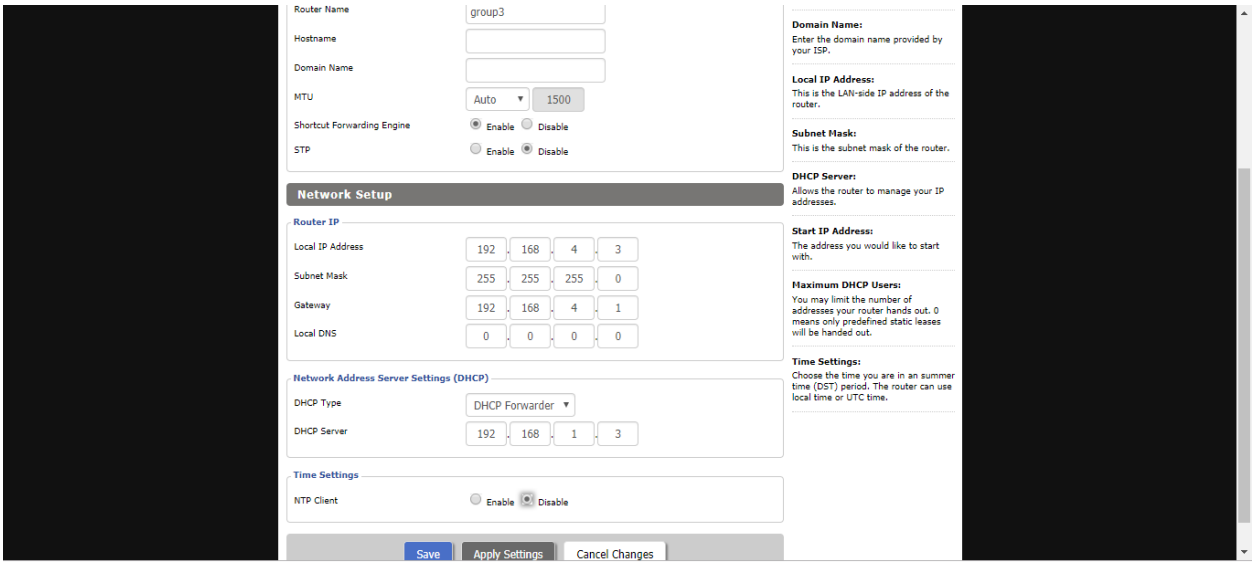


Figure 5.3.15 2 Configure basic setting

Step 4: Set the DHCP server for wireless access point to forward DHCP client request.

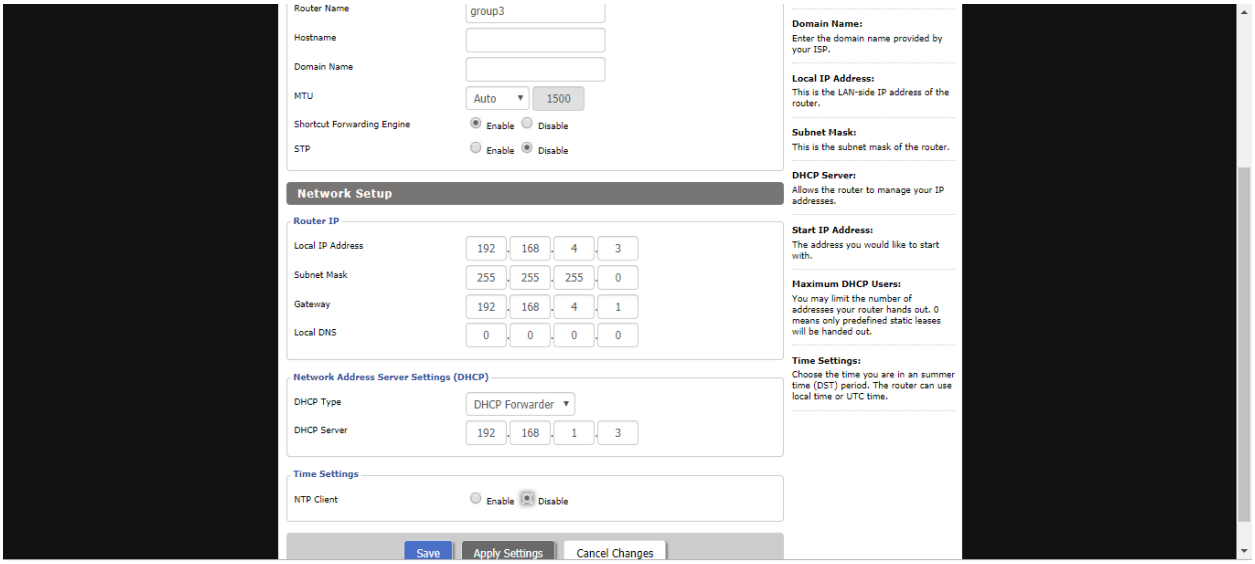


Figure 5.3.15 3 Configured DHCP forwarder

Step 5: Setup your SSID for 2.4 and 5 Ghz frequency

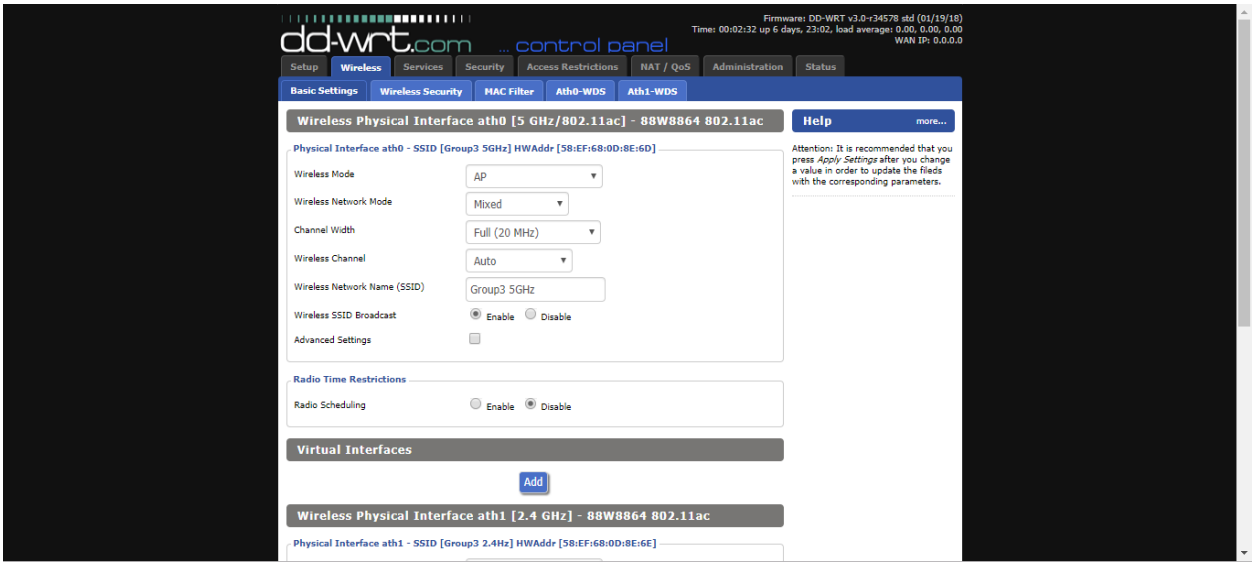


Figure 5.3.15 4 Setting up your SSID for both frequencies.

Step 6: Connect the access point to the VLAN 40.

Step 7: Install Network Policy and Access Service in Windows Server using add and role features.

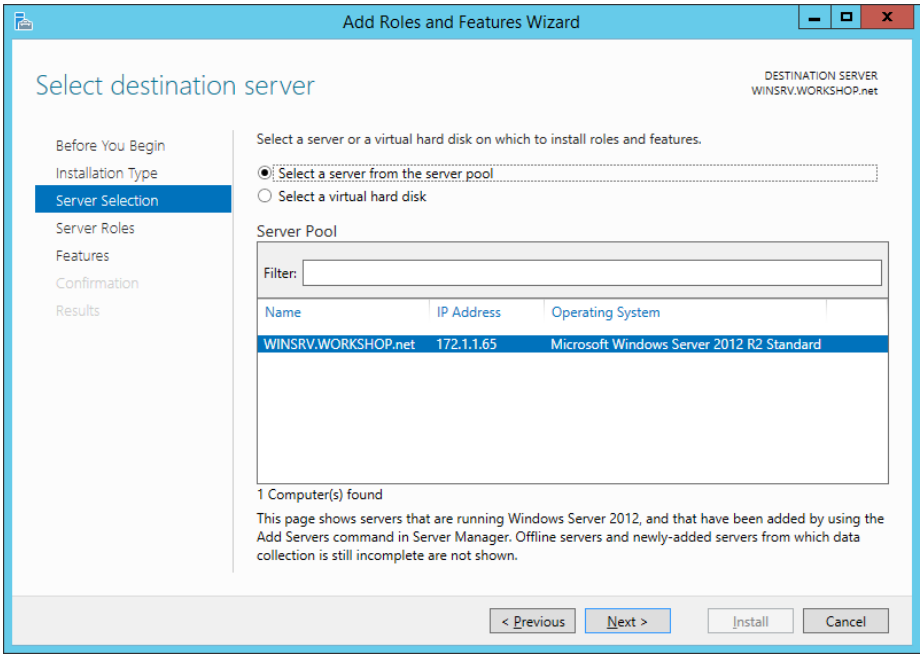


Figure 5.3.15 5 Select the window server for install the service.

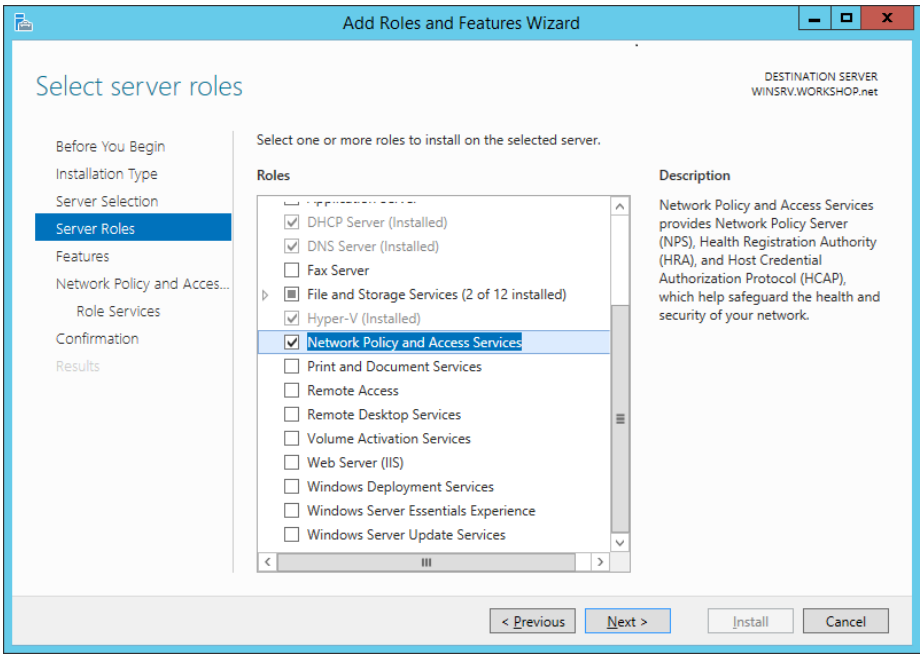


Figure 5.3.15 6 Select Network Policy and Access Services.

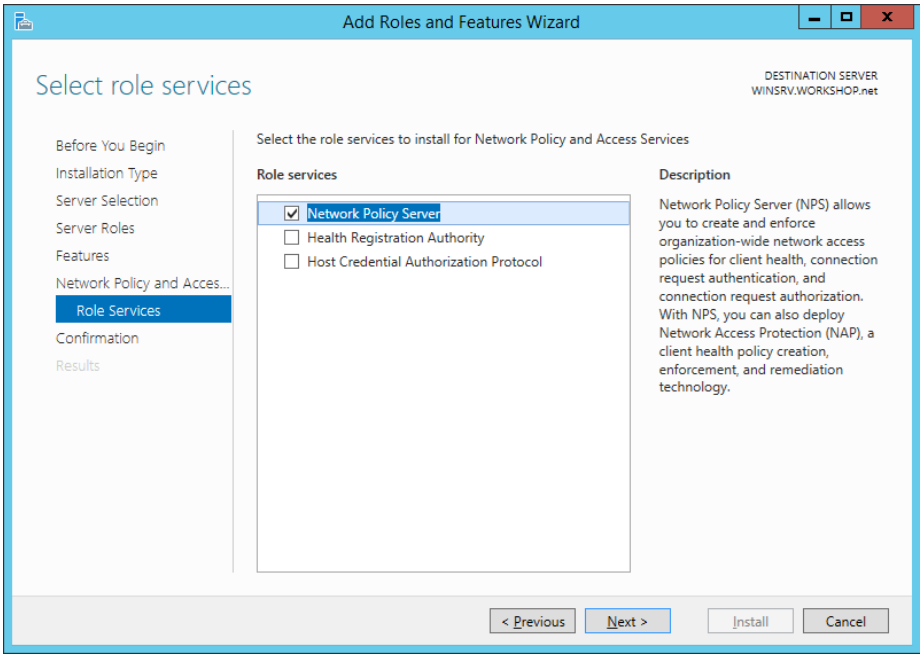


Figure 5.3.15 7 Include Network Policy Server

Step 8: Create new group for wireless user and add all domain user into the group.

Step 9: Open Network Policy Server management console and authorize the server into group3.com domain.

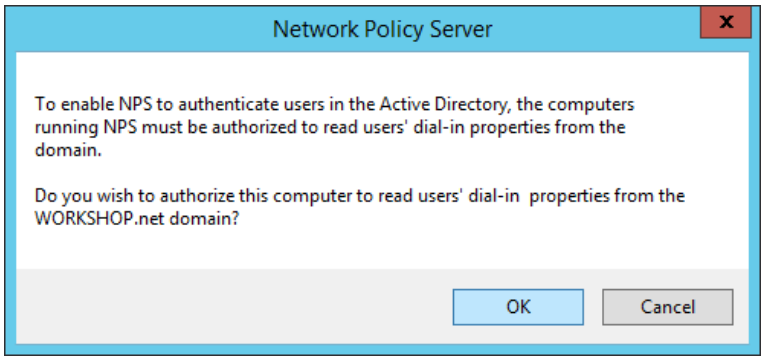


Figure 5.3.15 8 Authorize the server to use the domain resources

Step 10: Add new radius client in the server.

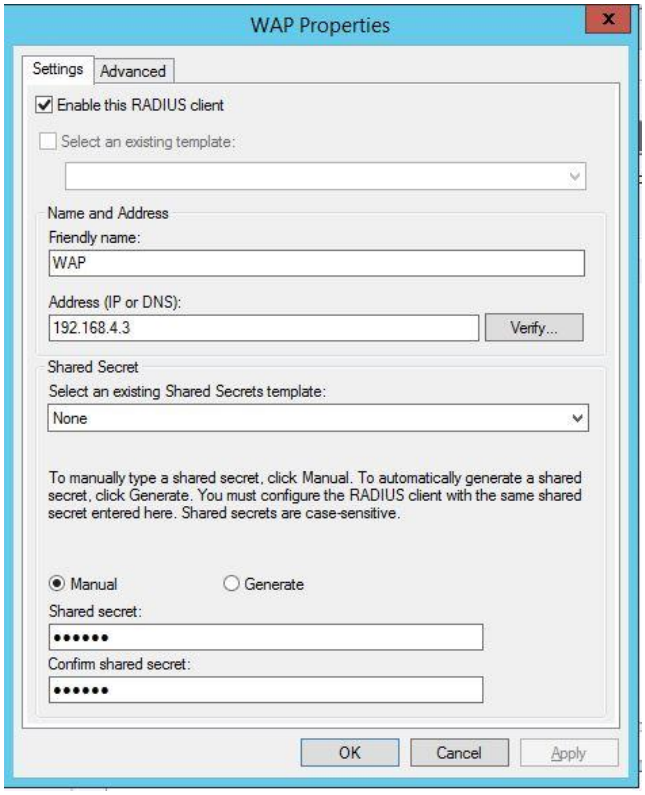


Figure 5.3.15 9 New radius client template

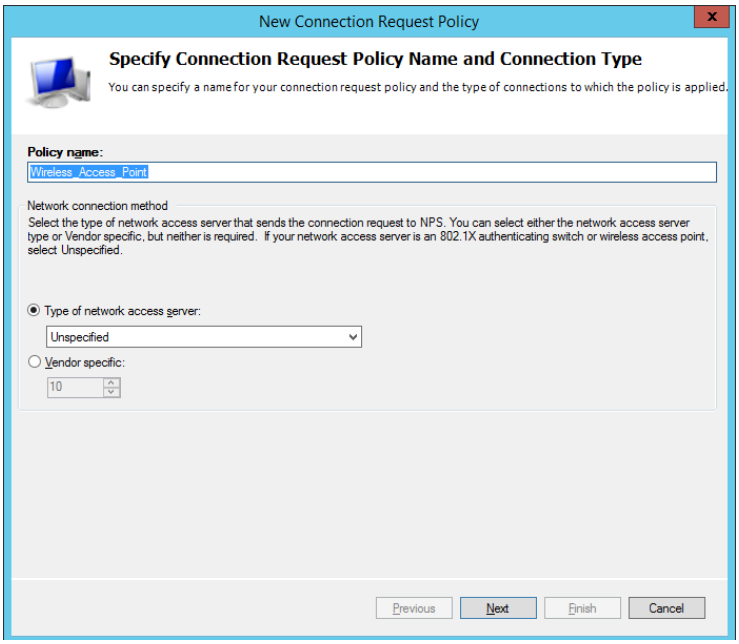


Figure 5.3.15 10 Add new connection request for radius client

Step 11: Create new connection policy to allow radius connection from the device in radius client template.

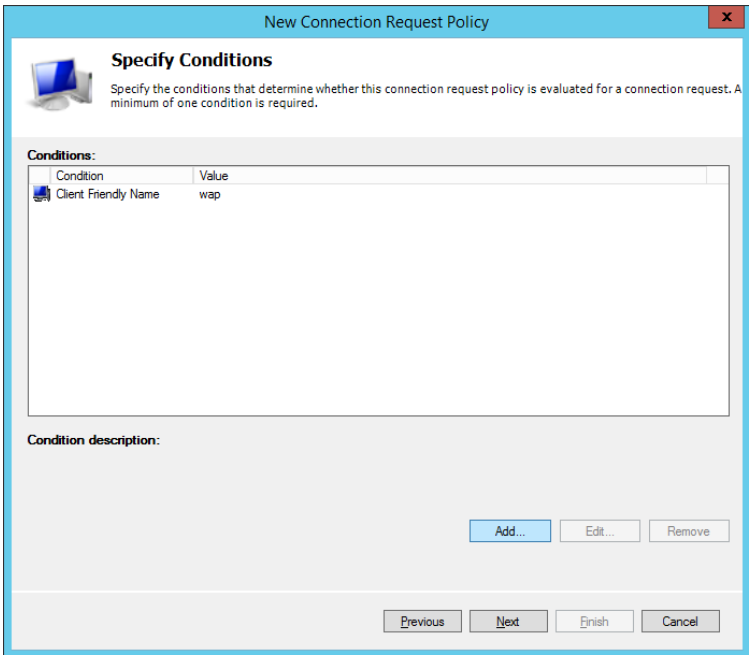


Figure 5.3.15 11 Map the policy to the client friendly name created

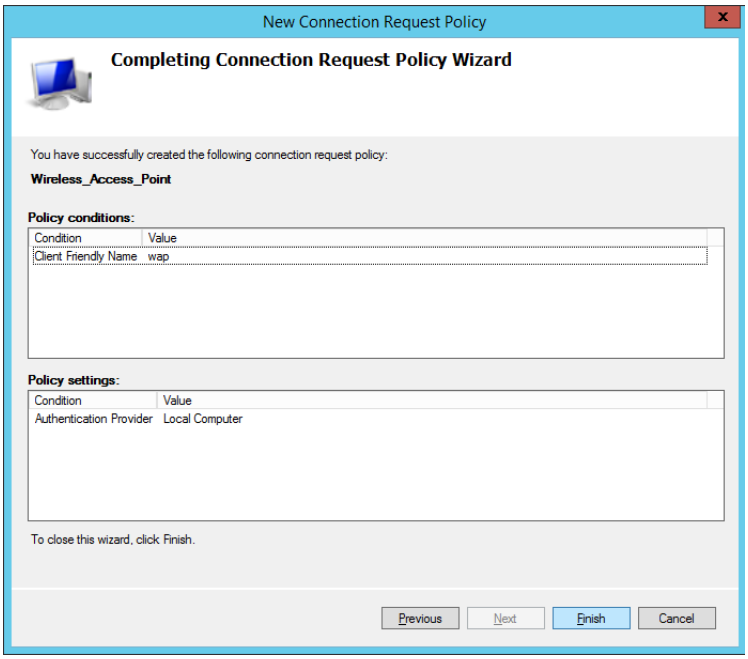


Figure 5.3.15 12 Finish the connection policy configuration

Step 12: Create an Active Directory group and add all user into the group.

Step 13: Create new network policy to allow radius client to user Active Directory user database.

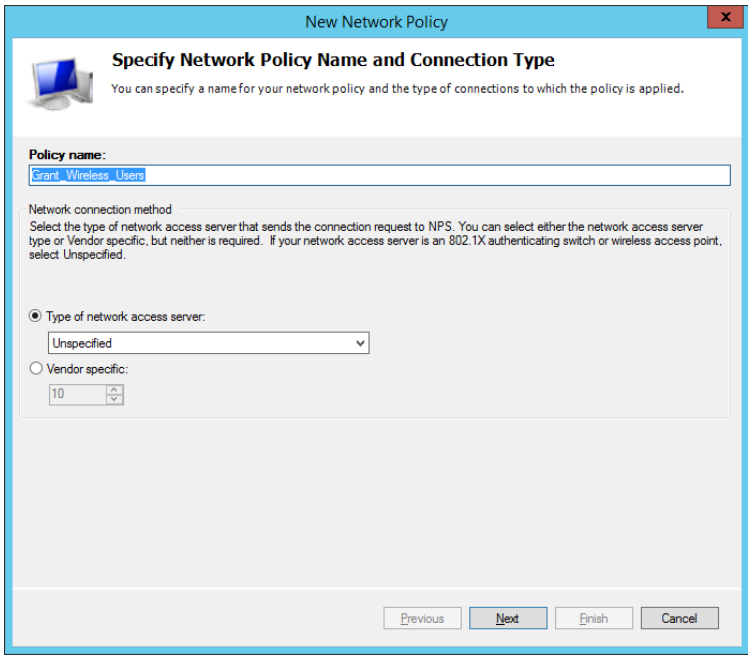


Figure 5.3.15 13 New network policy

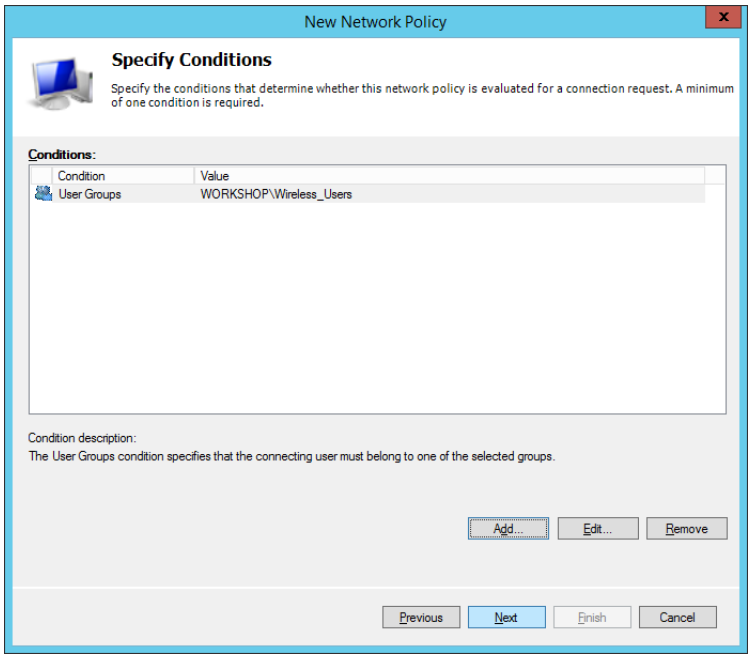


Figure 5.3.15 14 Map all the user that will use radius authentication

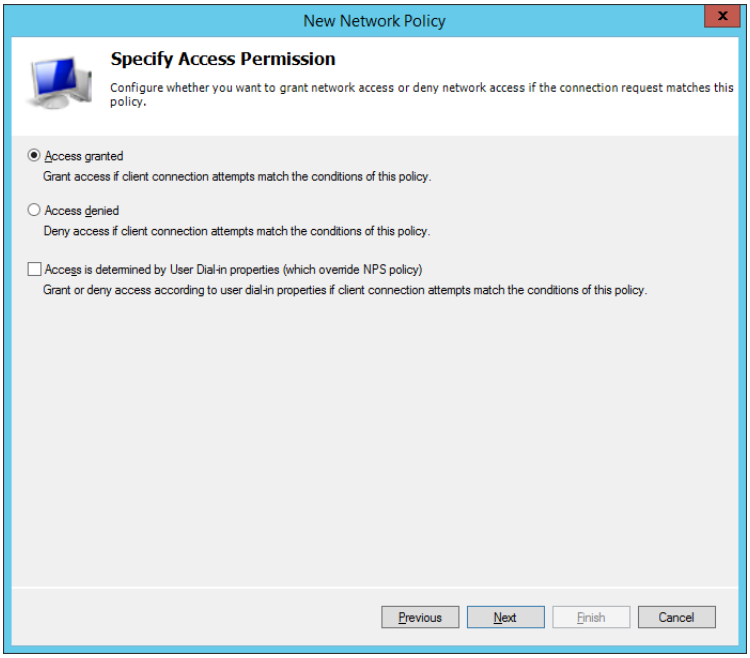


Figure 5.3.15 15 Set permission to allow access for the users

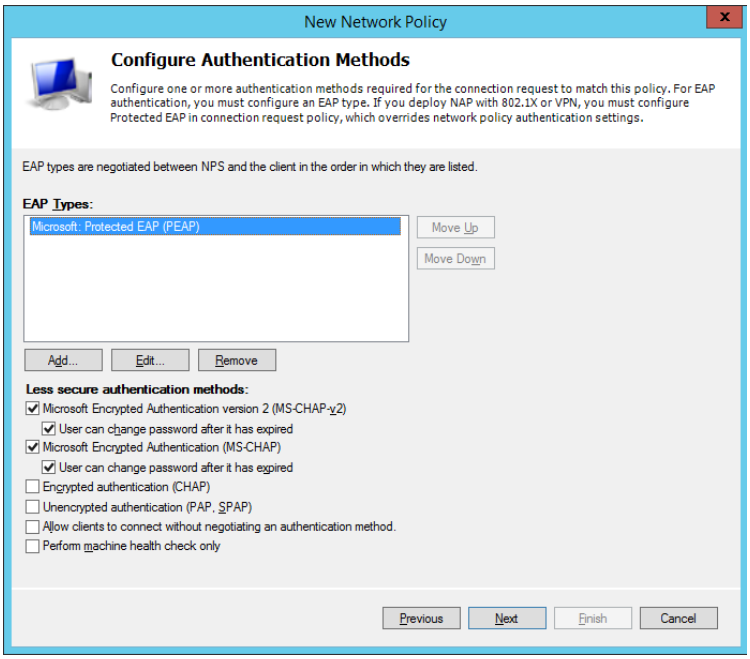


Figure 5.3.15 16 User PEAP as the authentication methods

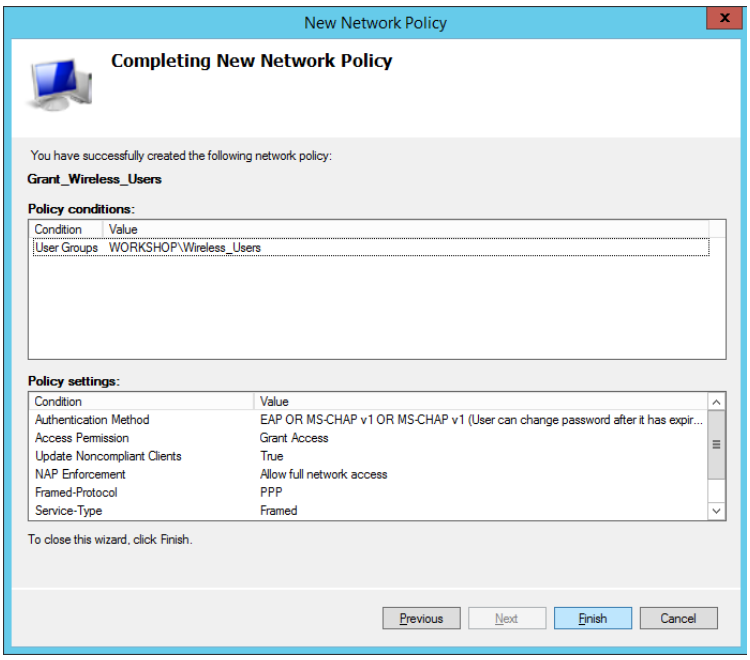


Figure 5.3.15 17 Finish the configuration

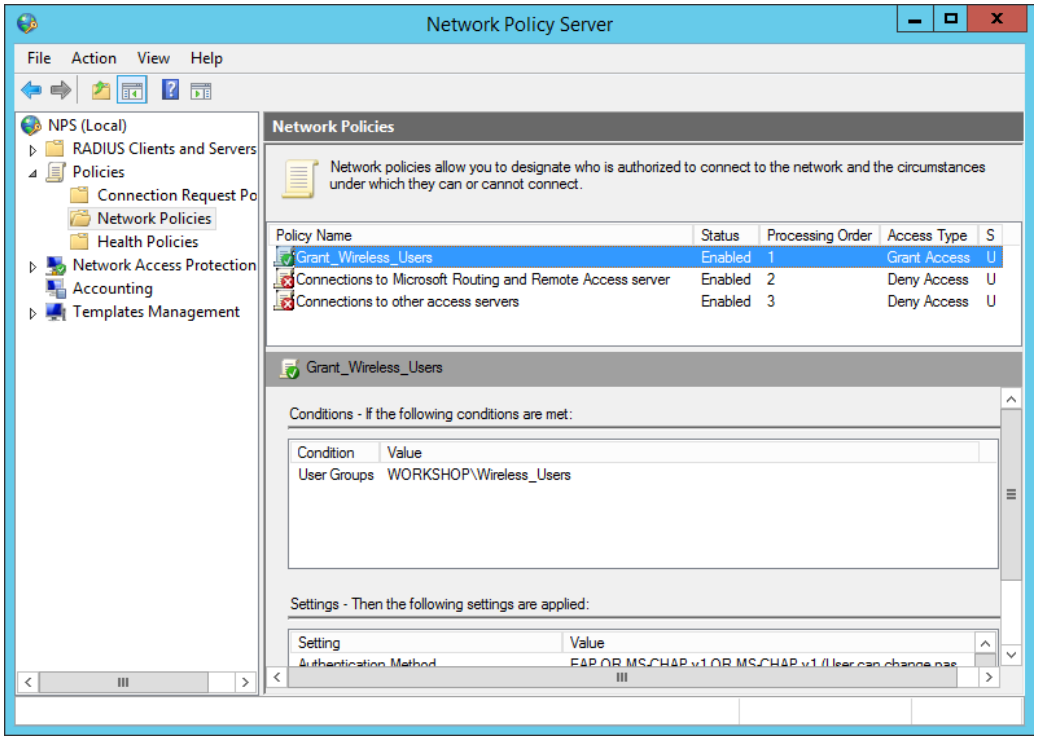


Figure 5.3.15 18 Move newly created policy on the first order

Step 14: Set the Radius server IP address on the access point configuration both for 5Ghz and 2.4Ghz.

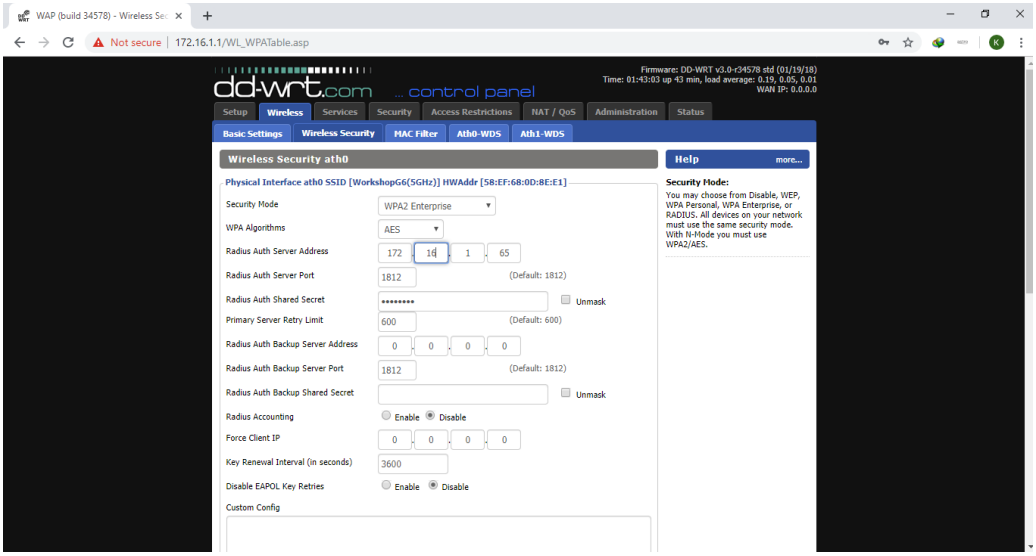


Figure 5.3.15 19 Radius server IP address setup on wireless access point

5.4 Conclusion

Installation and configuration are important procedure to be done before testing the services. Installation of a program is the act of putting the program onto a computer system so that it can be executed. Because the requisite process varies for each program and each computer, many programs come with a general-purpose or dedicated installer (a specialized program which automates most of the work required for their installation). This stage must be done carefully to make sure the service can be run efficiently during the testing part. The installation guide will help you get up and running in no time.

6.0 CHAPTER 6: TESTING

6.1 Introduction

There are different methods and several ways that have been done in testing all the services process. This section will show the ways to test all the services that have been setup and configured. Testing is importance to isolate the services and shows the individual parts are correct. Moreover, testing are also enable to show us the functioning of the services are successfully up and running. A good testing the services is when the errors is occurred and detected so, we will find the solutions to modify the errors and make some improvement to produce the best performance.

6.2 Services Testing

6.2.1 Server Virtualization

User from virtual machine can access and sharing file from the windows server.

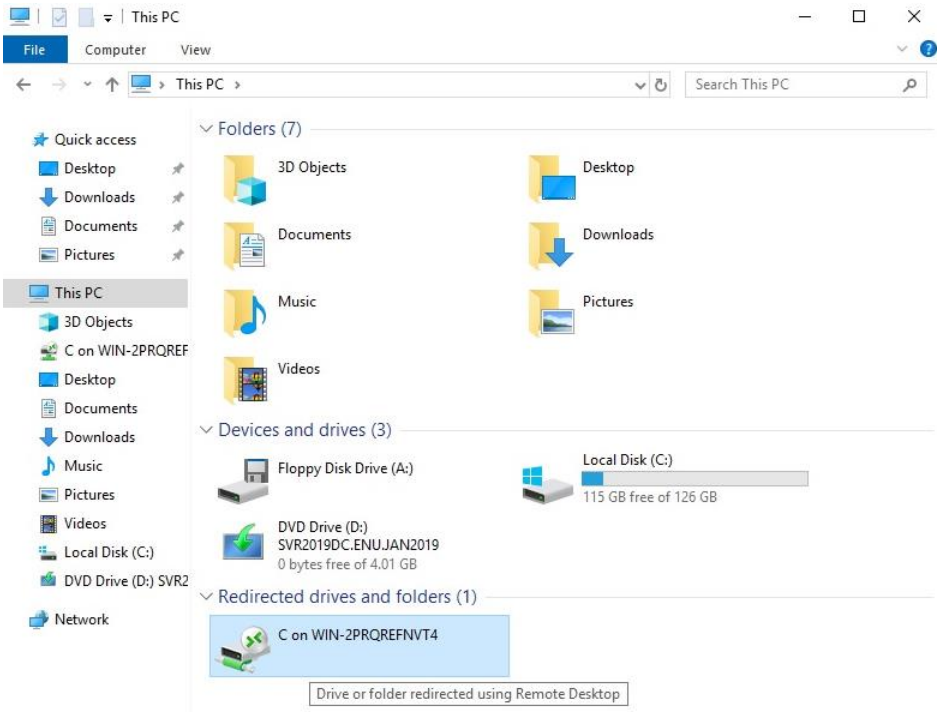


Figure 6.2.1 1 C path from windows server

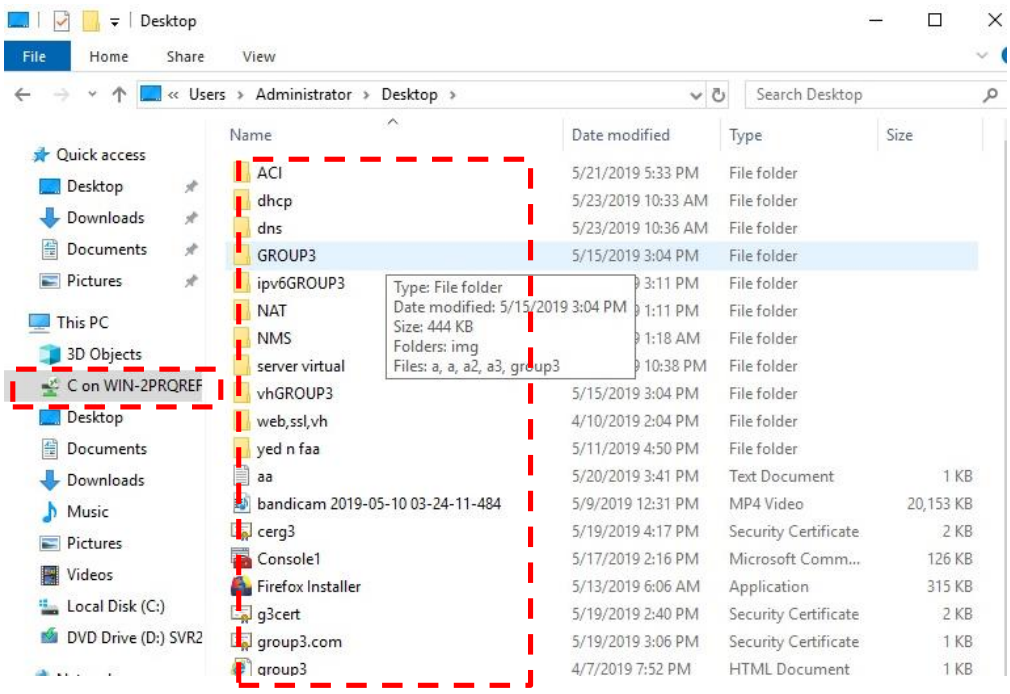


Figure 6.2.1 2 File sharing from windows server

6.2.2 DNS

Step 1: Click start and then open Command Prompt

Figure 6.2.2 1 Open Command prompt

Step 2: Type nslookup, and then press enter. There will be shown list of servers with their own DNS.

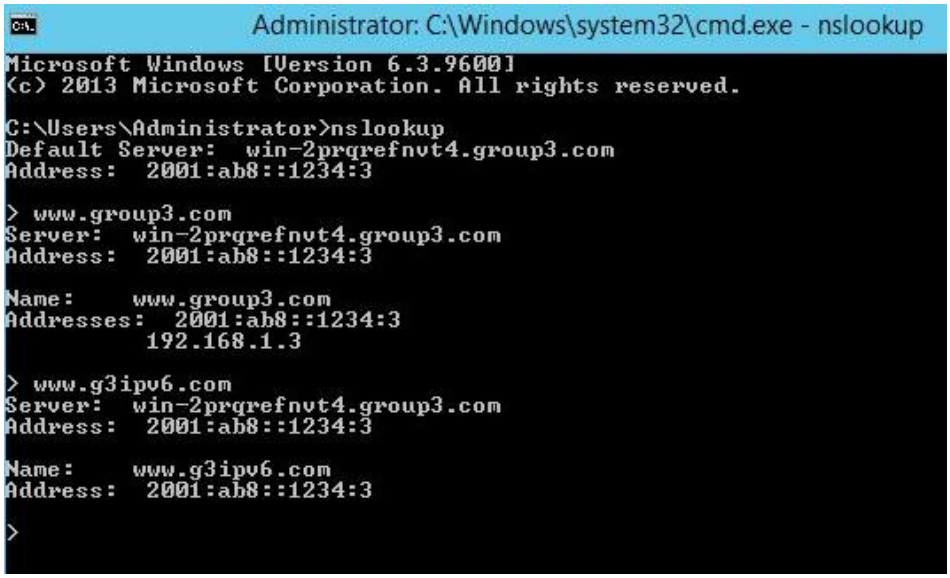


Figure 6.2.2 2 nslookup for group3.com

6.2.3 DHCP IPv4 and IPv6

Testing requirement.

• Hardware: Windows Server Workstation and Client Workstation

• Software: Windows Server 2019 and Windows 10

IPv4 Testing

Step 1: Open command prompt at the client and type ipconfig and check for client either get the ipv4 automatically form the DHCP server.

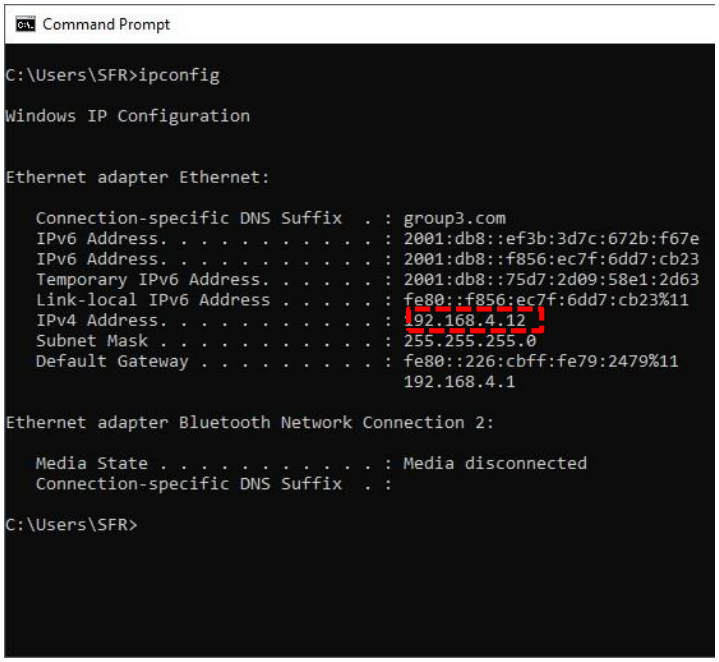
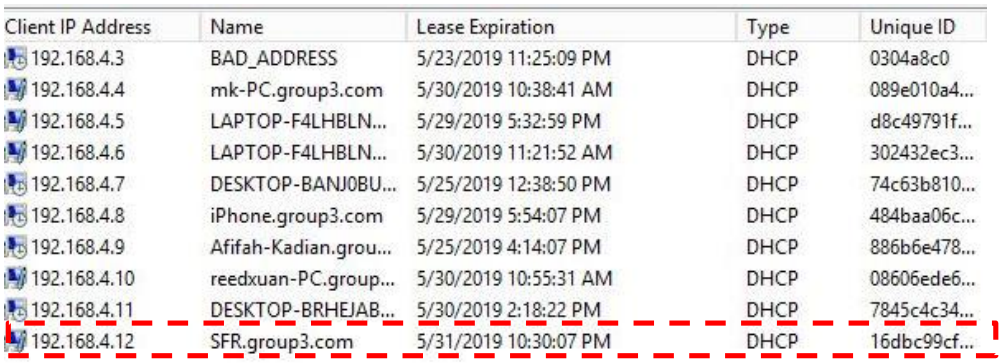


Figure 6.2.3 1 ipconfig IPv4

Open the Windows Server and open the DHCP services. Find IPv4>Scope>Scope Lease. Check the list for ipv4 match with client ip address.



Client IP Address	Name	Lease Expiration	Type	Unique ID
192.168.4.3	BAD_ADDRESS	5/23/2019 11:25:09 PM	DHCP	0304a8c0
192.168.4.4	mk-PC.group3.com	5/30/2019 10:38:41 AM	DHCP	089e010a4...
192.168.4.5	LAPTOP-F4LHBLN...	5/29/2019 5:32:59 PM	DHCP	d8c49791f...
192.168.4.6	LAPTOP-F4LHBLN...	5/30/2019 11:21:52 AM	DHCP	302432ec3...
192.168.4.7	DESKTOP-BANJ0BU...	5/25/2019 12:38:50 PM	DHCP	74c63b810...
192.168.4.8	iPhone.group3.com	5/29/2019 5:54:07 PM	DHCP	484baa06c...
192.168.4.9	Afifah-Kadian.grou...	5/25/2019 4:14:07 PM	DHCP	886b6e478...
192.168.4.10	reedxuan-PC.group...	5/30/2019 10:55:31 AM	DHCP	08606ede6...
192.168.4.11	DESKTOP-BRHEJAB...	5/30/2019 2:18:22 PM	DHCP	7845c4c34...
192.168.4.12	SFR.group3.com	5/31/2019 10:30:07 PM	DHCP	16dbc99cf...

Figure 6.2.3 2 Address Lease IPv4

IPv6 Testing

Step 1: Open command prompt at the client and type ipconfig and check for client either get the ipv6 automatically form the DHCP server.

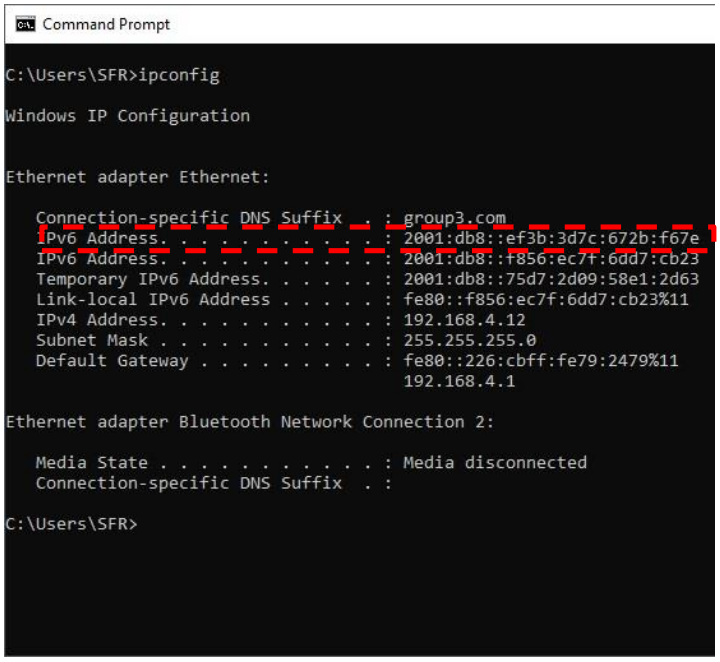
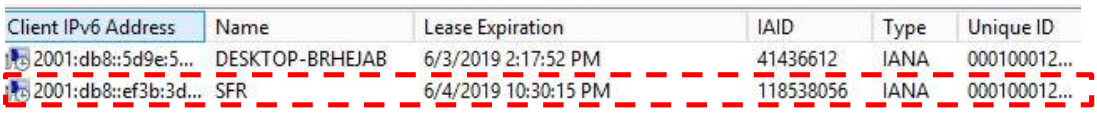


Figure 6.2.3 3 ipconfig IPv6

Step 2: Open the Windows Server and open the DHCP services. Find IPv6>Scope>Scope Lease. Check the list for ipv6 match with client ip address.



Client IPv6 Address	Name	Lease Expiration	IAID	Type	Unique ID
2001:db8::5d9e:5...	DESKTOP-BRHEJAB	6/3/2019 2:17:52 PM	41436612	IANA	000100012...
2001:db8::ef3b:3d...	SFR	6/4/2019 10:30:15 PM	118538056	IANA	000100012...

Figure 6.2.3 4 Address Lease IPv6

6.2.4 Network Management System

Step 1 : Turn off any service that have selected in server's template, Zabbix's Dashboard will show that which service needs attention.

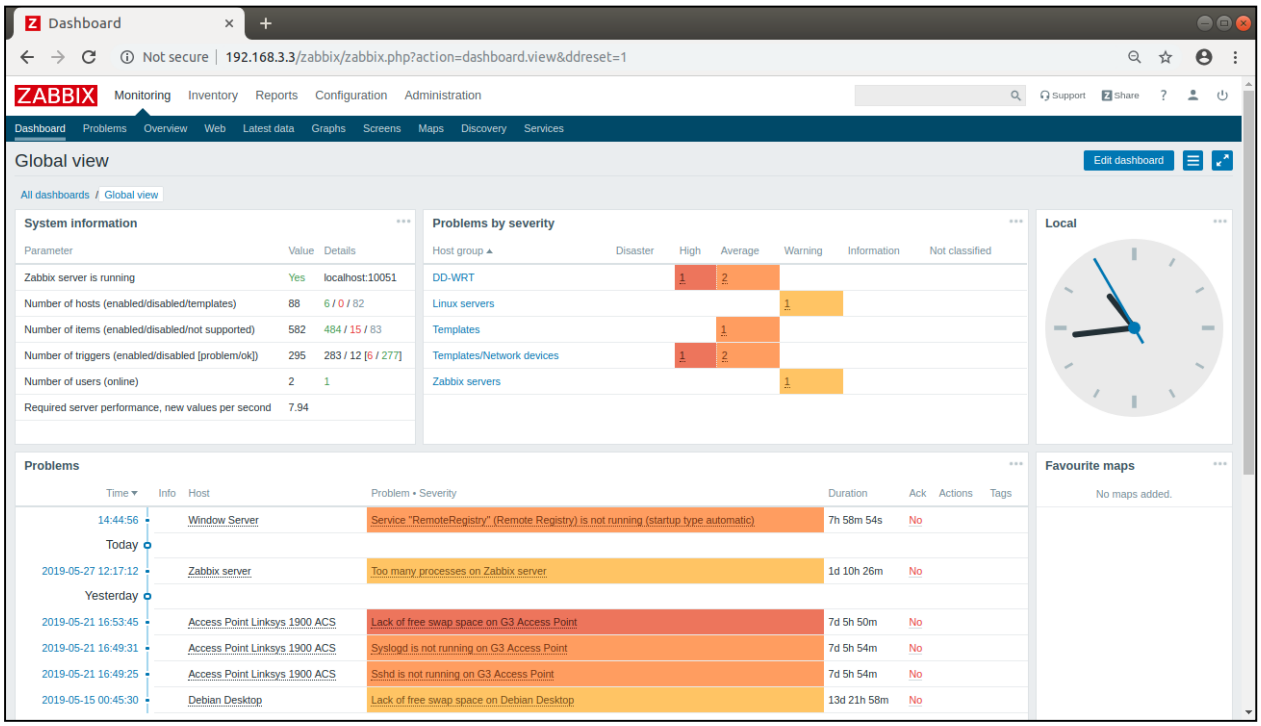


Figure 6.2.4 1 Zabbix Server Dashboard

Step 2 : Other testing and graph show.

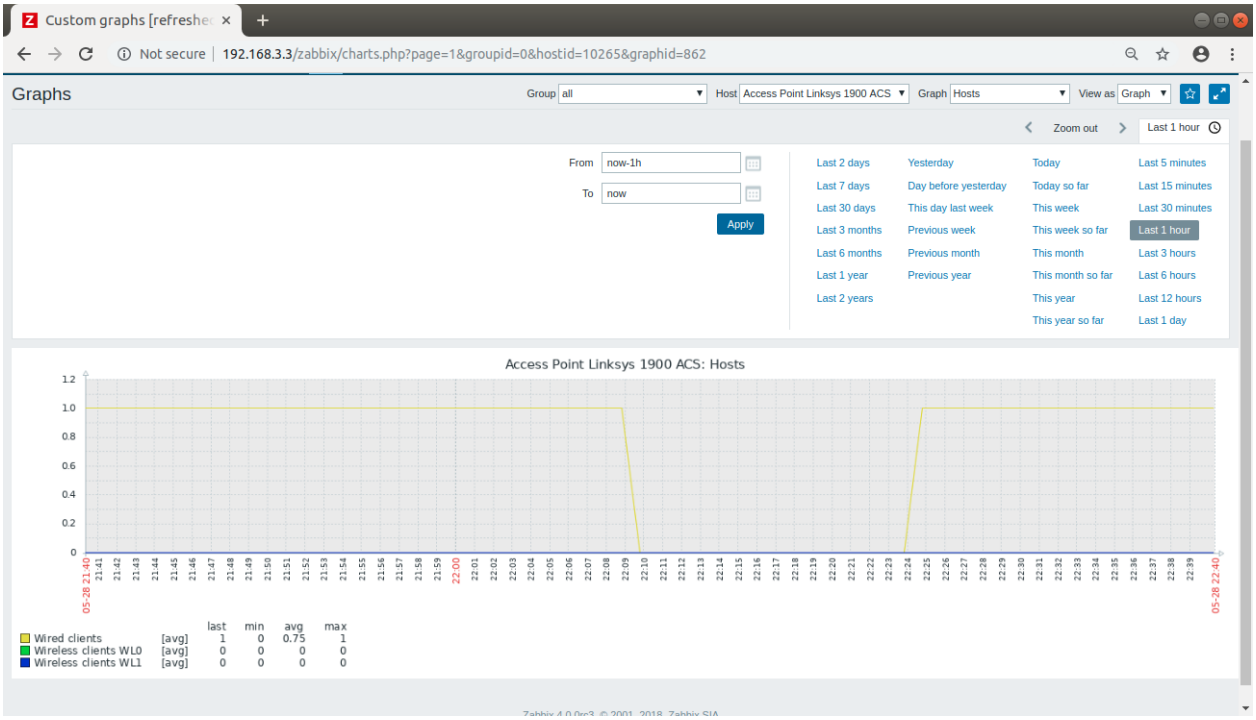


Figure 6.2.4 2 Access Point graph

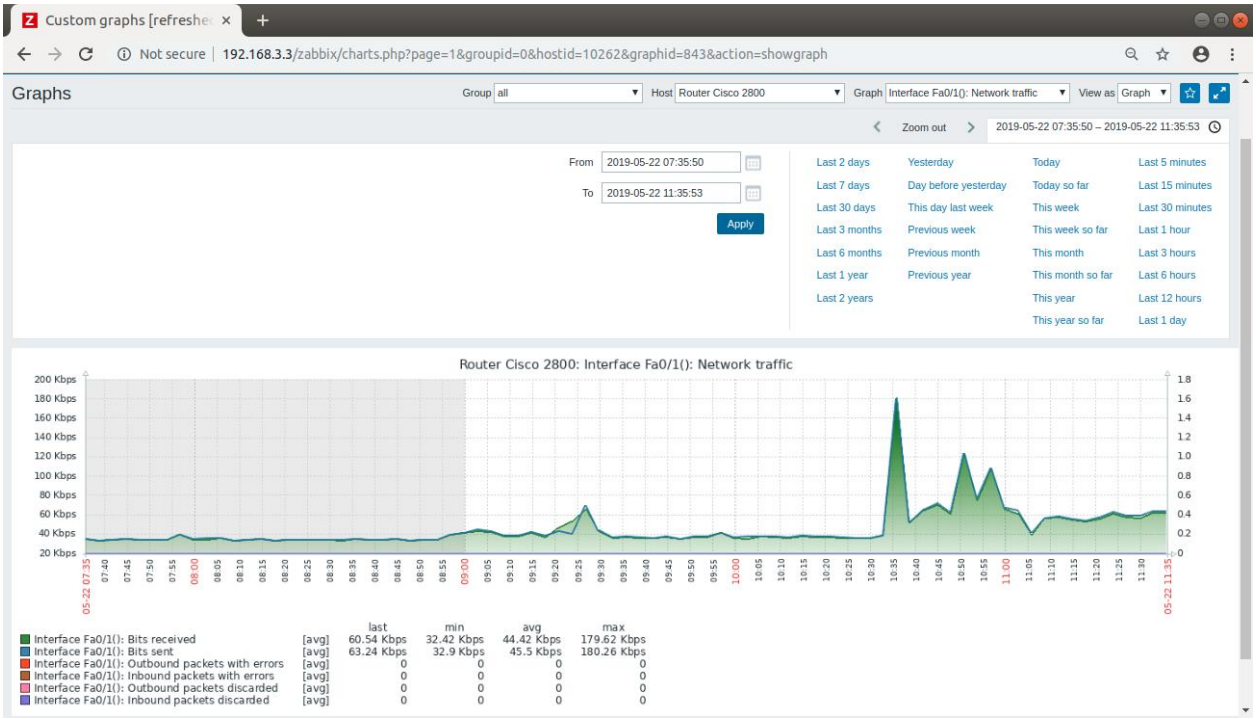


Figure 6.2.4 3 Cisco Router graph

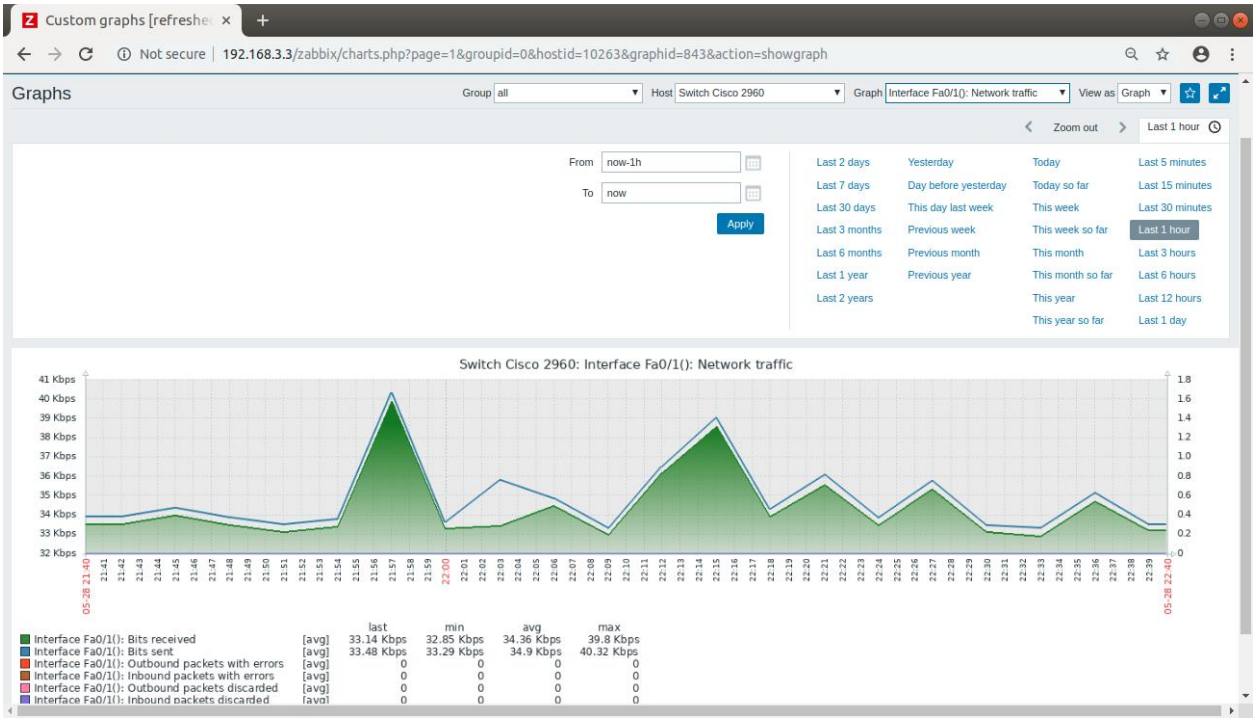


Figure 6.2.4 4 Cisco Switch graph

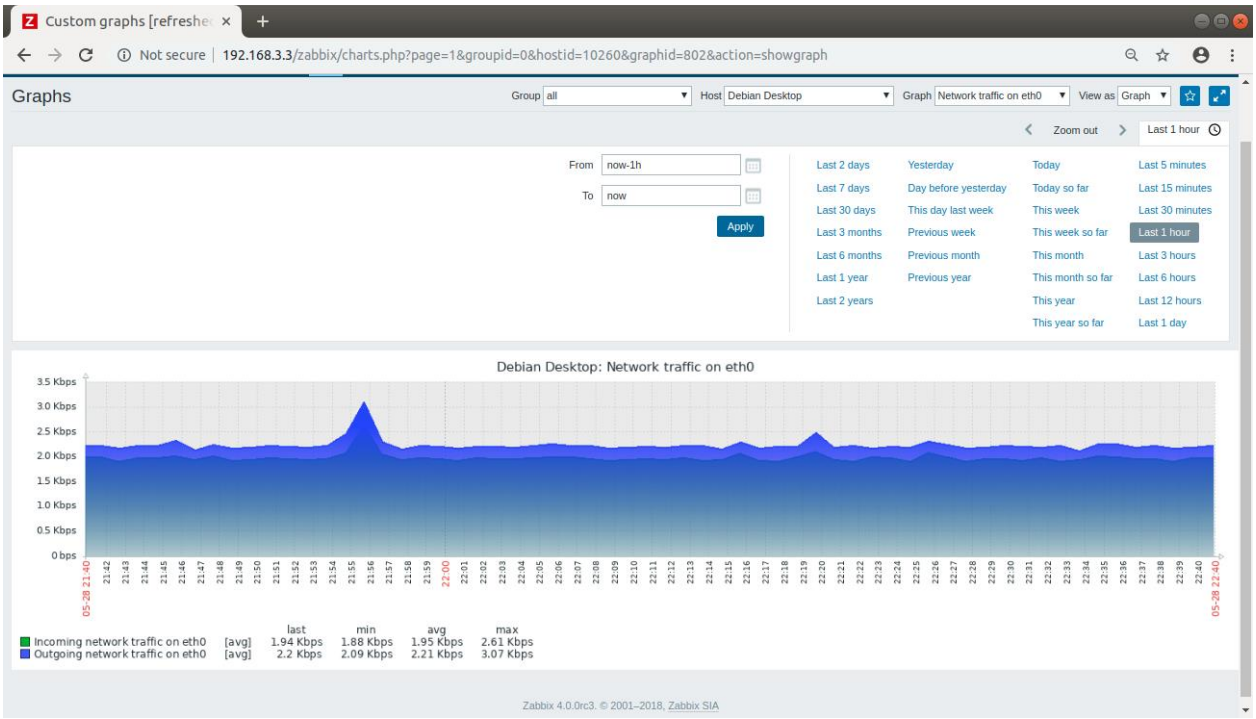


Figure 6.2.4 5 Debian Server Desktop graph

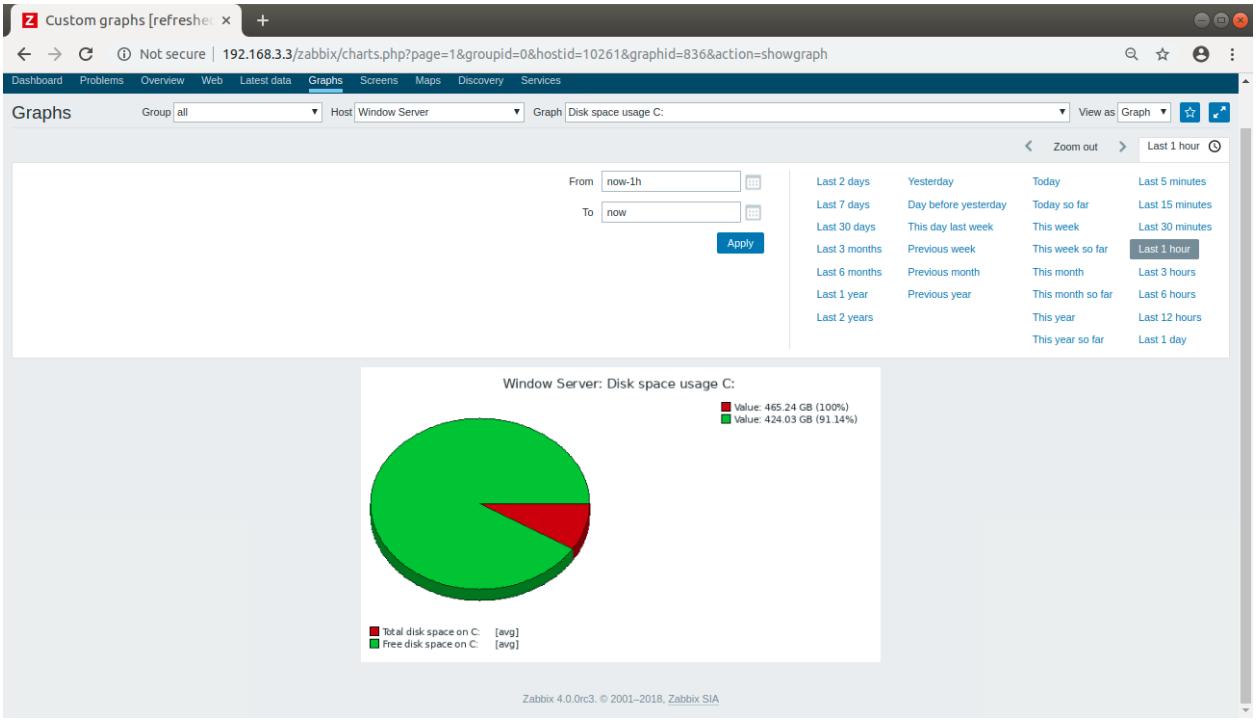


Figure 6.2.4 6 Windows Server Desktop graph

6.2.5 Testing Routing & NAT

Network Address Translation (NAT)

Step 1 : Used command "***show run***" to show the NAT inside and outside interface.

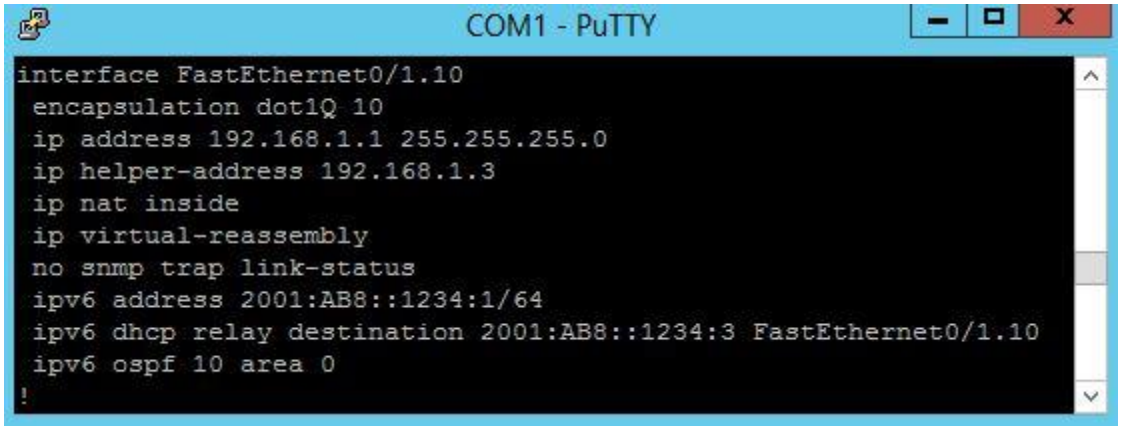


Figure 6.2.5 1 : IP NAT inside (int f0/1.10)

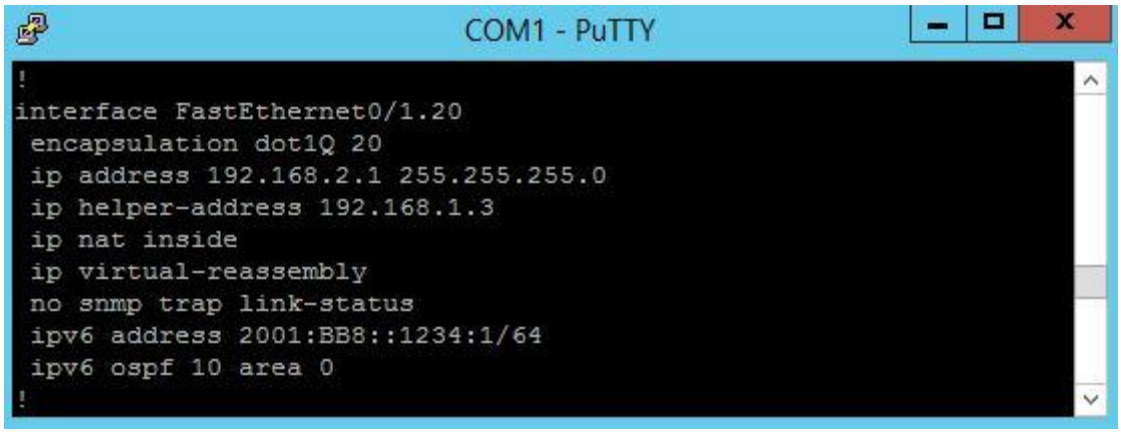


Figure 6.2.5 2 IP NAT inside (int f0/1.20)

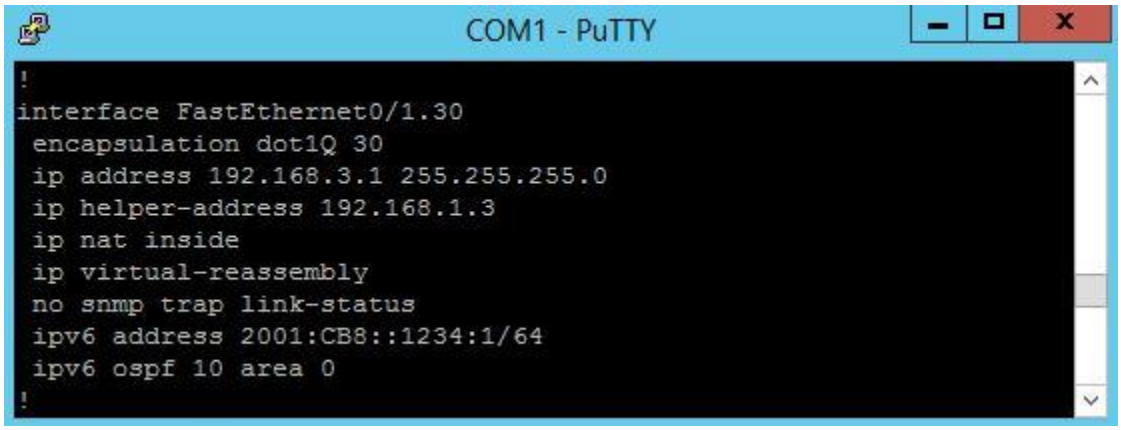


Figure 6.2.5 3 IP NAT inside (int f0/1.30)

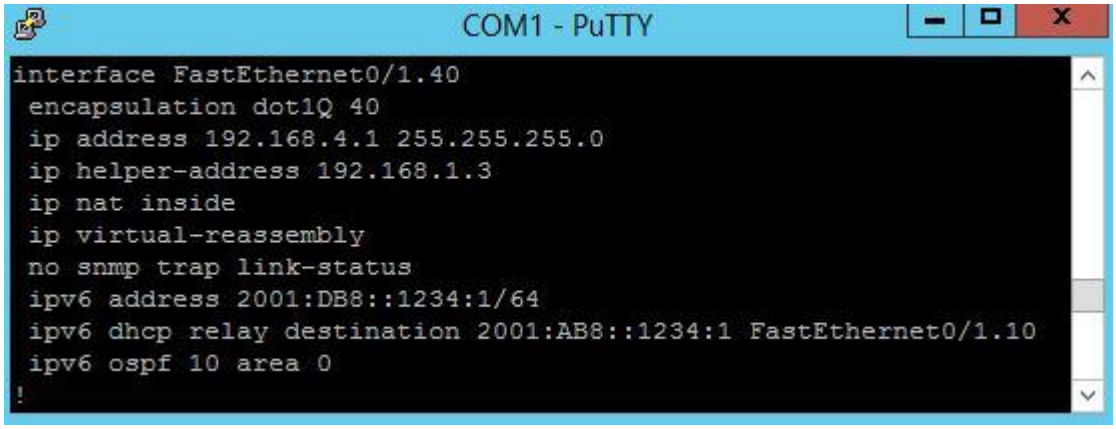


Figure 6.2.5 4 IP NAT inside (int f0/1.40)

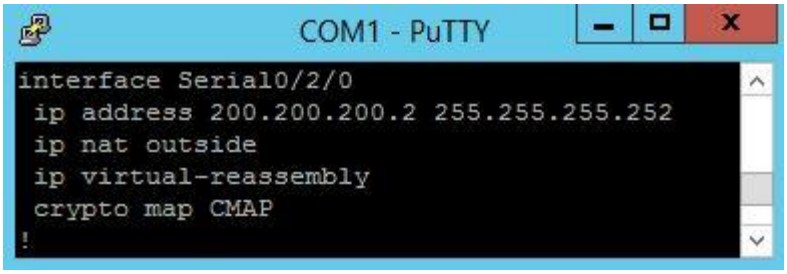


Figure 6.2.5 5 IP NAT outside (int s0/2/0)

Step 2 : Show configuration of static NAT and dynamic NAT.

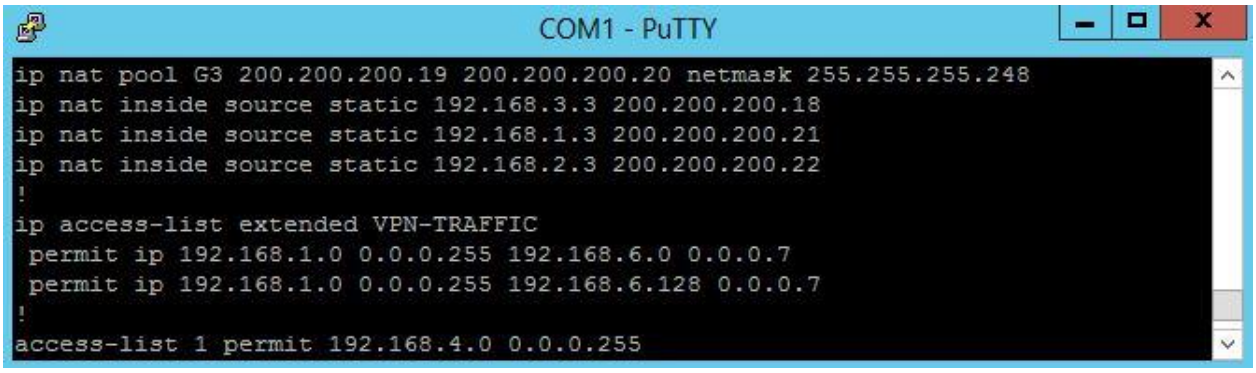


Figure 6.2.5 6 Configuration of static NAT and dynamic NAT

Step 3 : Ping from pc windows server (group 3) to pc group 4 using public IP.

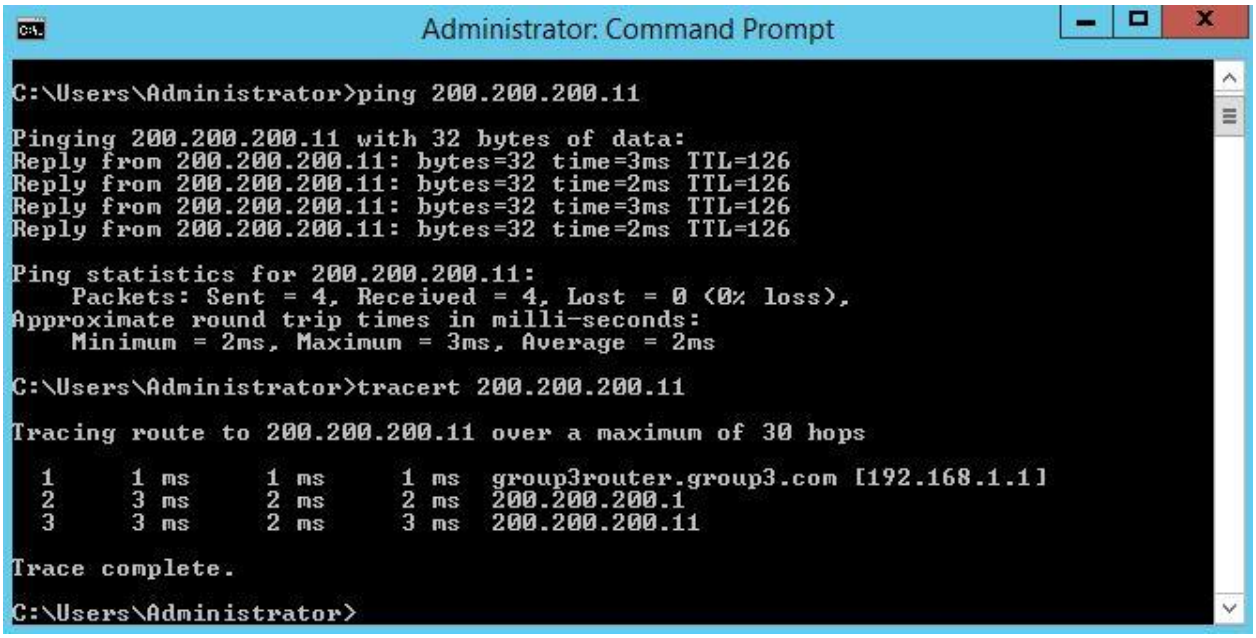


Figure 6.2.5 7 Ping IP 200.200.200.11

Step 4: Show IP NAT translation

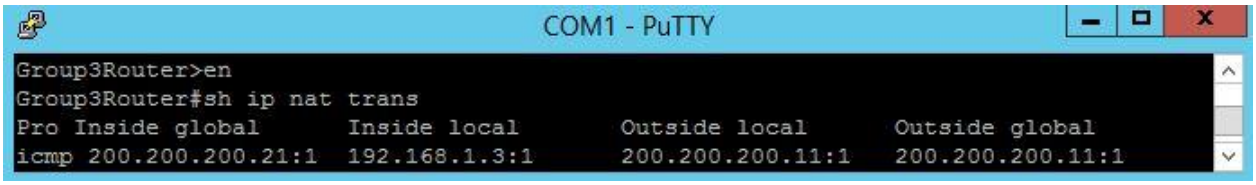


Figure 6.2.5 8 Result IP NAT translation

Step 5 : Ping from pc windows server (group 4) to pc group 3 using public IP.

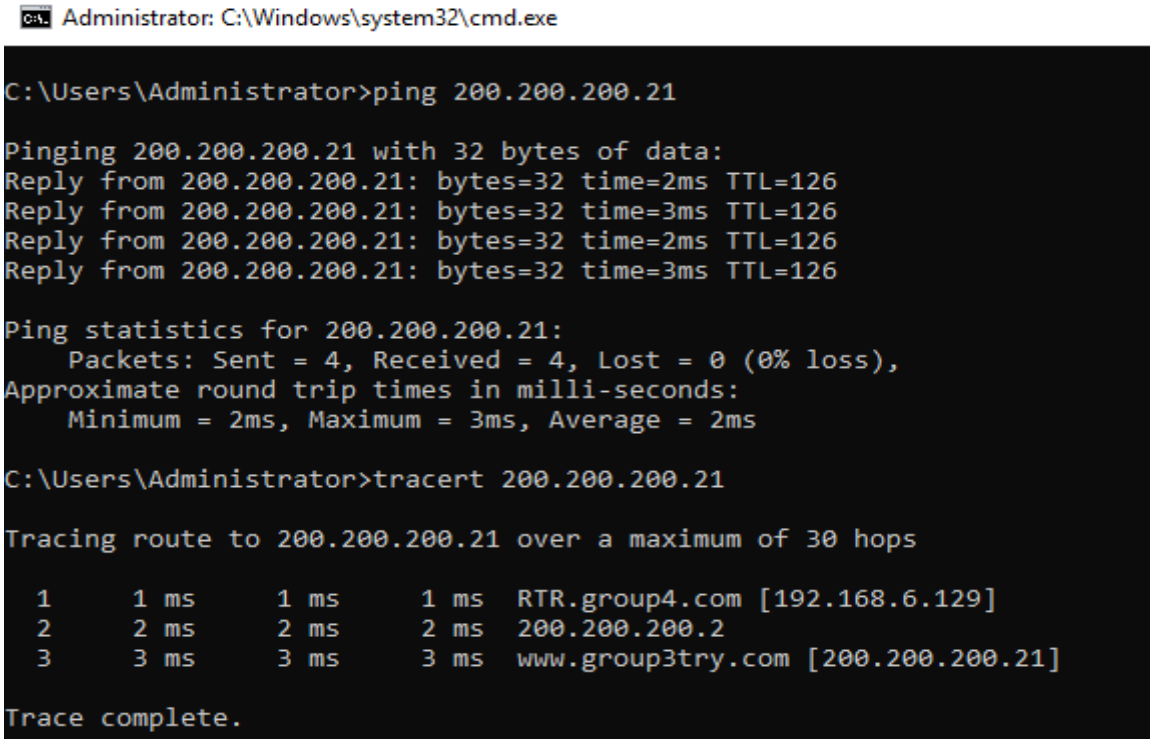


Figure 6.2.5 9 Ping IP 200.200.200.21

6.2.6 Proxy Server

Step 1 : Set IP address in Connection Settings.

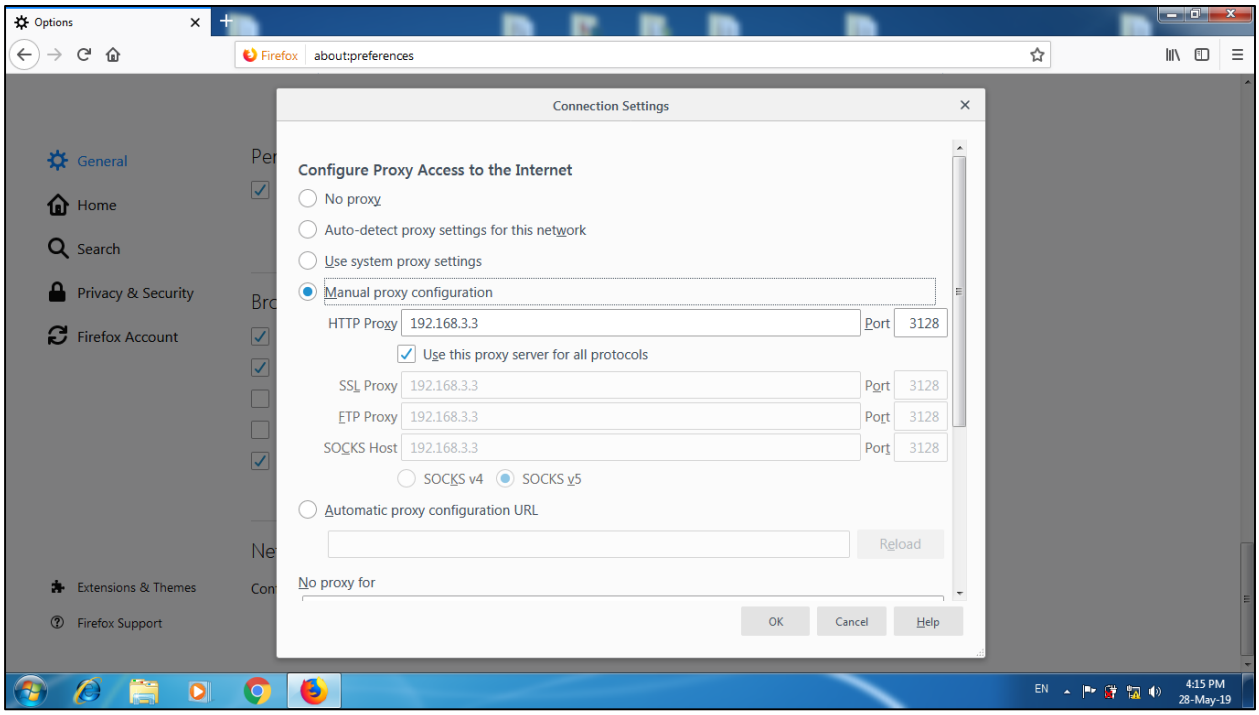


Figure 6.2.6 1 Set IP address on client Windows

Step 2 : Test from client on Windows.

ulearn.utem.edu.my

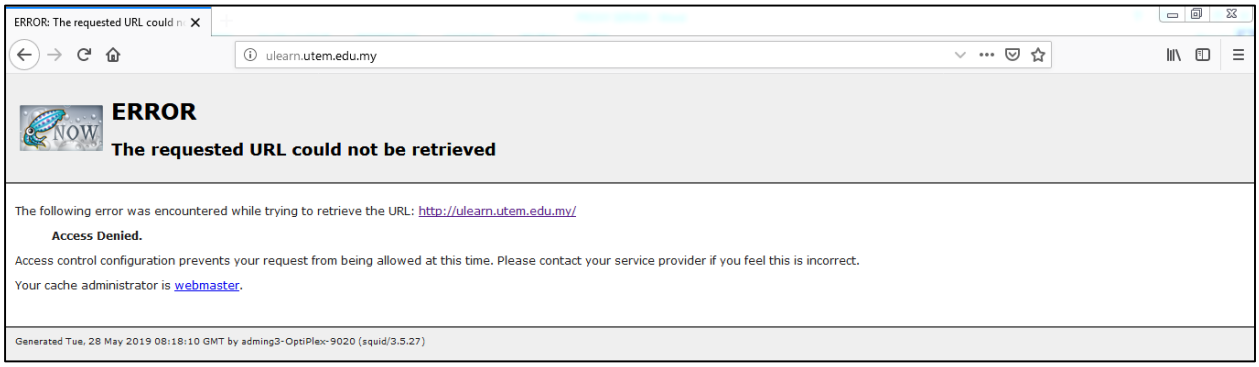


Figure 6.2.6 2 Error message when search "ulearn.utem.edu.my"

Step 3 : Test from client on Ubuntu.

ulearn.utem.edu.my

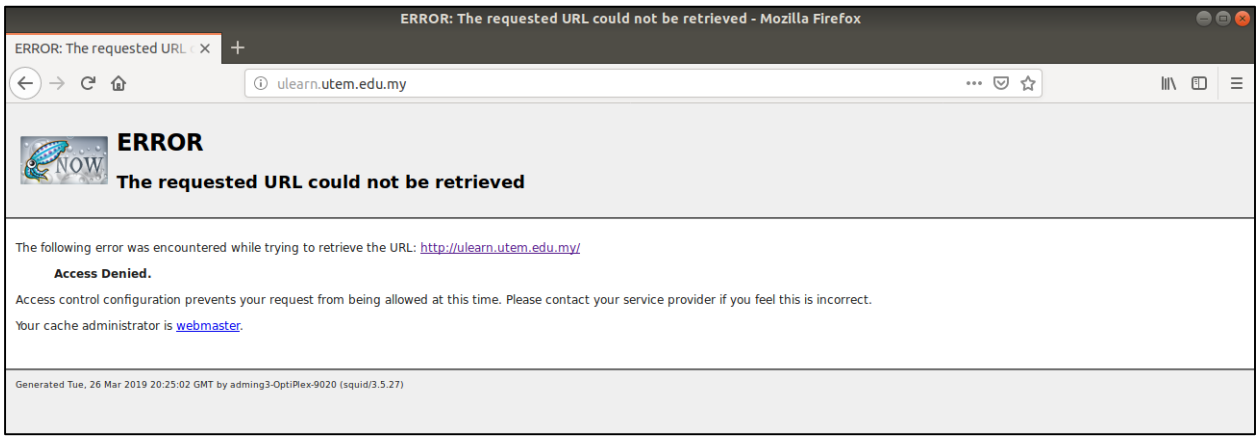


Figure 6.2.6 3 Error message when search "ulearn.utem.edu.my" Ubuntu

6.2.7 Authentication, Authorization, Accounting (AAA)

In this process we have to create the username of the router and password, in this case I'm using admin as username for admin user, and with the password abc@1234. After it's done, then it's time to install the AAA service, start with *AAA new model* and press enter.

```
aaa new-model
!
!
aaa authentication login default local
aaa authentication login aaa-server group radius local
aaa authorization exec default group radius if-authenticated
aaa authorization network default group radius
!
```

Figure 6.2.7 1 Creating a new authentication AAA

Next, we have to configure the authentication and accounting port. For authentication we use 1812 port and for accounting we use 1813 port.

```
Group3Router(config)#$2.168.1.3 auth-port 1645 acct-port 1646 key cisco
Group3Router(config)#$2.168.1.3 auth-port 1812 acct-port 1813 key cisco
Group3Router(config)#exit
Group3Router#
```

Figure 6.2.7 2 Configure authentication port and accounting port

This is the final step, after the entire configuration is done, restart the Putty to enter router again. This time we have to insert the username and password as authentication for the router. In this scenario I'm using admin login. The history of the login can be view in Event Viewer on Windows Server.

Figure 6.2.7 3 Result shows the attempt to enter the router by admin

6.2.8 Secure File Transfer Protocol (SFTP)

In this scenario I'm using third party software called FileZilla

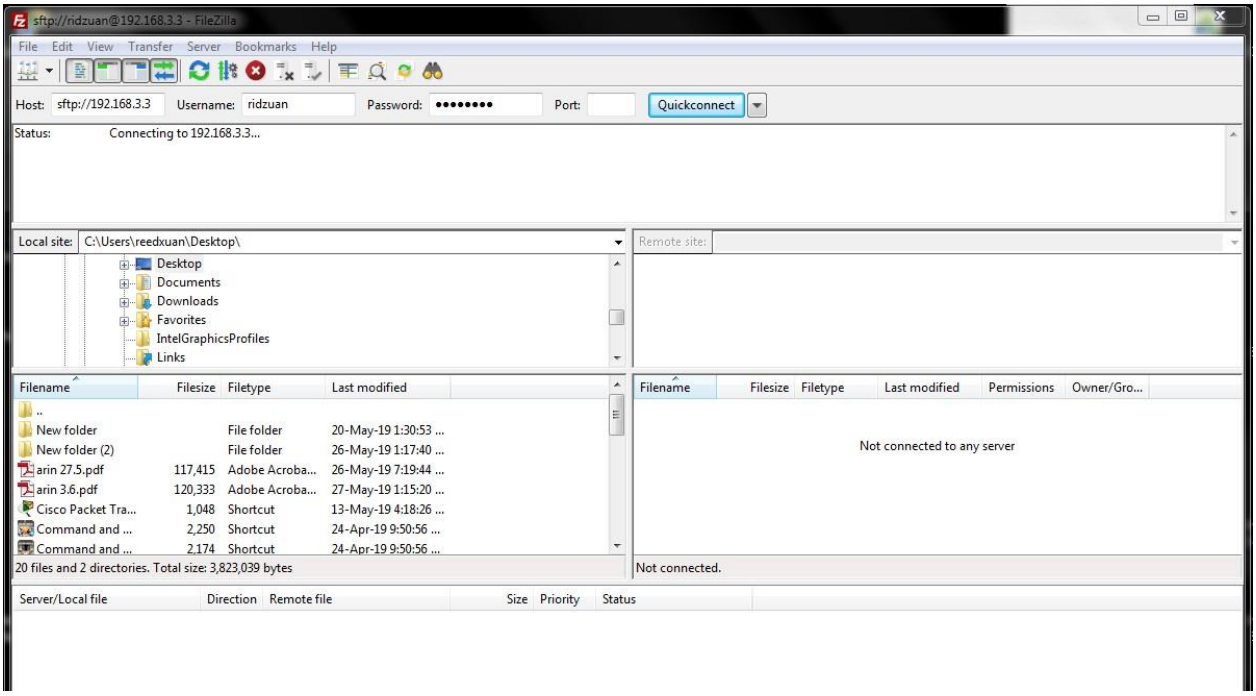


Figure 6.2.8 1 FTP tested in FileZilla

Insert the host by the IP address of the server in this case 192.168.3.3, and then insert the username that have been created before along with the password and don't forget to using port 22 as the connecting port otherwise it will not secure the transfer process. After that click "OK".

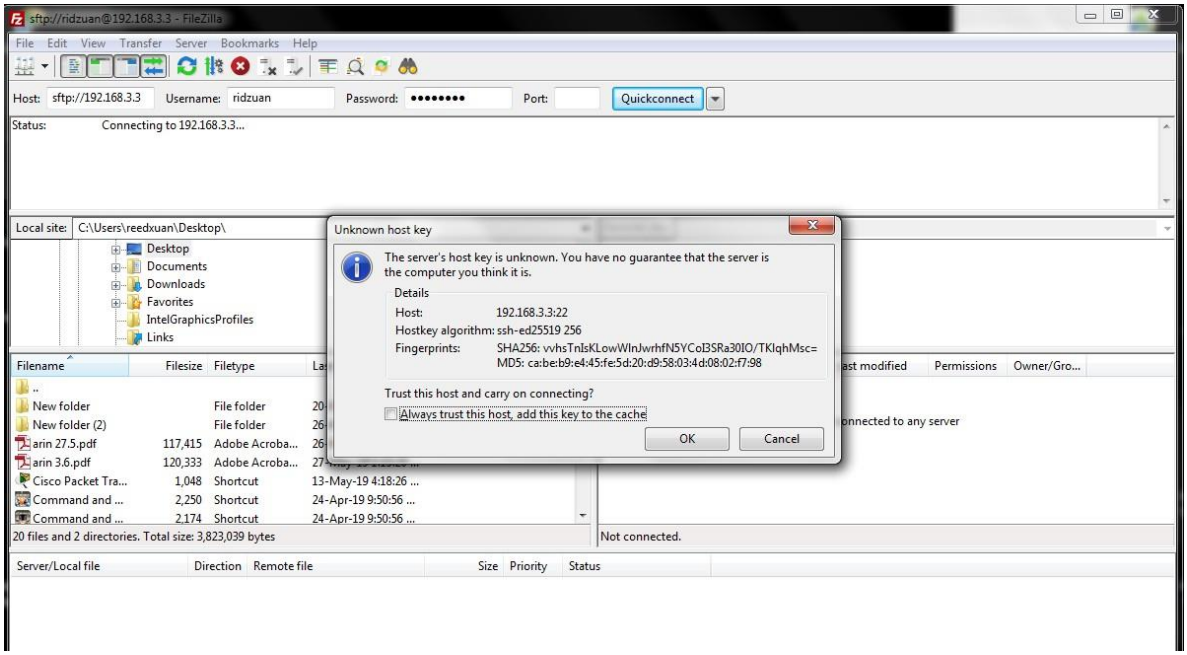


Figure 6.2.8 2 Insert Host/IP address, username and password

If we insert the correct IP address and correct username/password, it will be success like shown below. Now registered user can access the server, without going physically to the server.

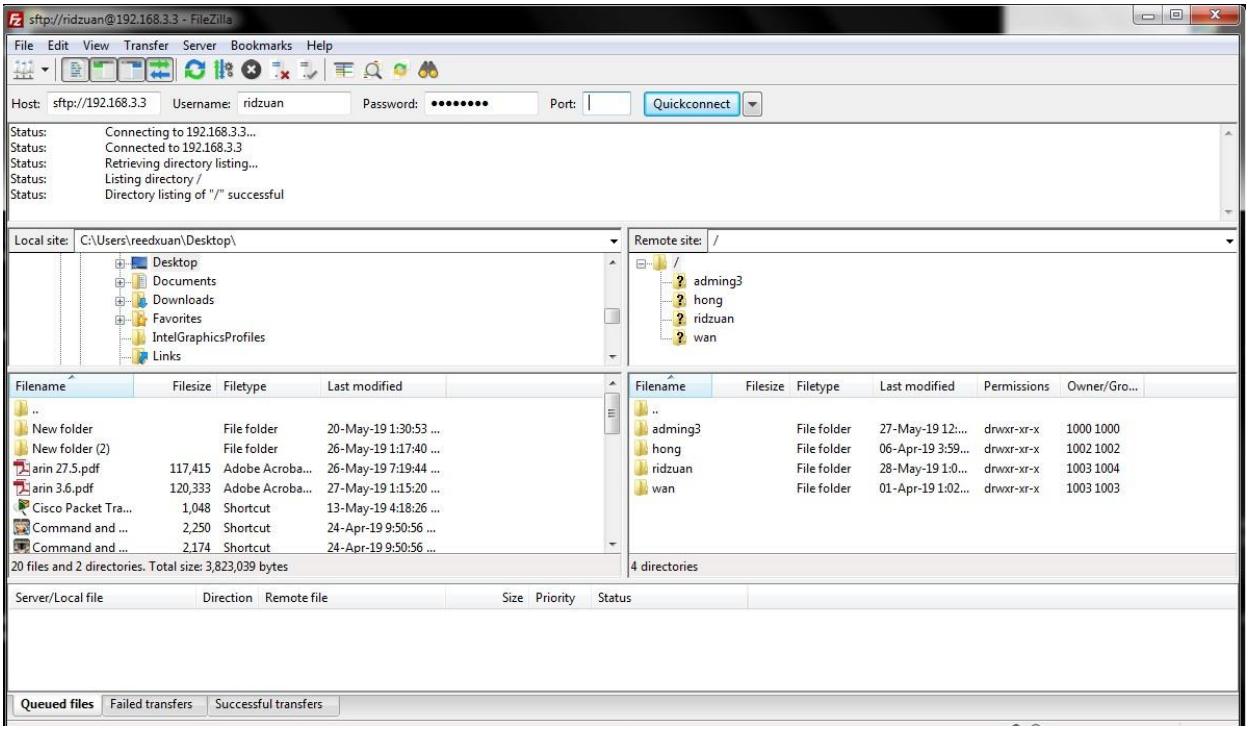


Figure 6.2.8 3 FTP tested in FileZilla successful using port 22

6.2.9 Access Control List (ACL)

Diagram below show the result of the ACL implementation, this is port 25 which is for mail services. It shows that the page cannot be reach.

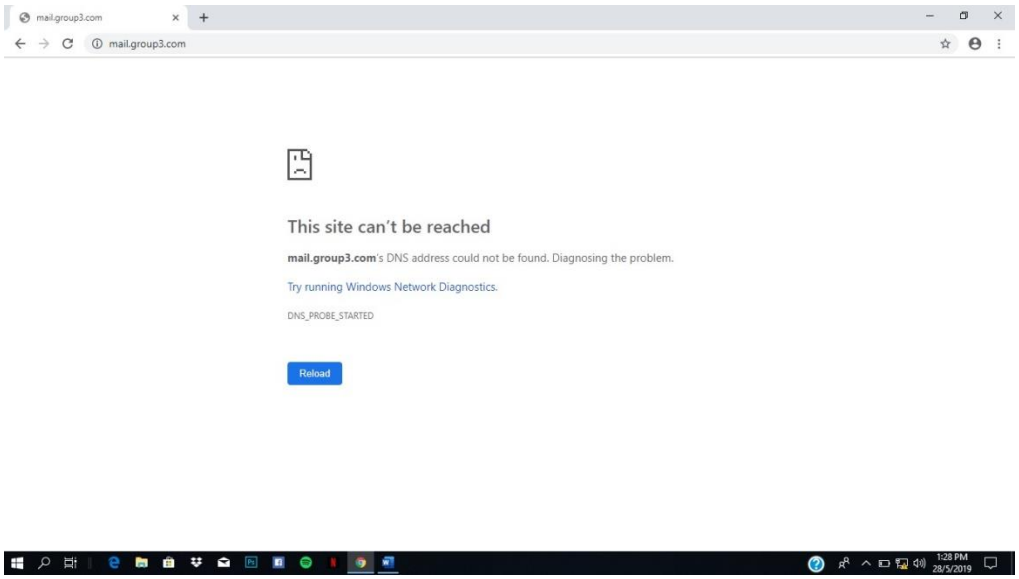


Figure 6.2.9 1 Testing result for SMTP port

Diagram below show the result of deny the port 443 which is for HTTPS web.

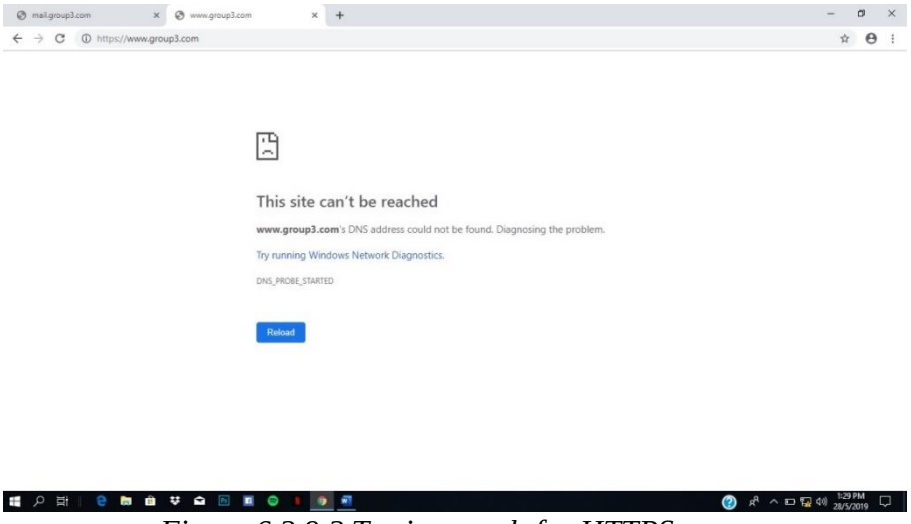


Figure 6.2.9 2 Testing result for HTTPS port

Next is, we deny the 80 port which is for HTTP web. The result is shown as below.

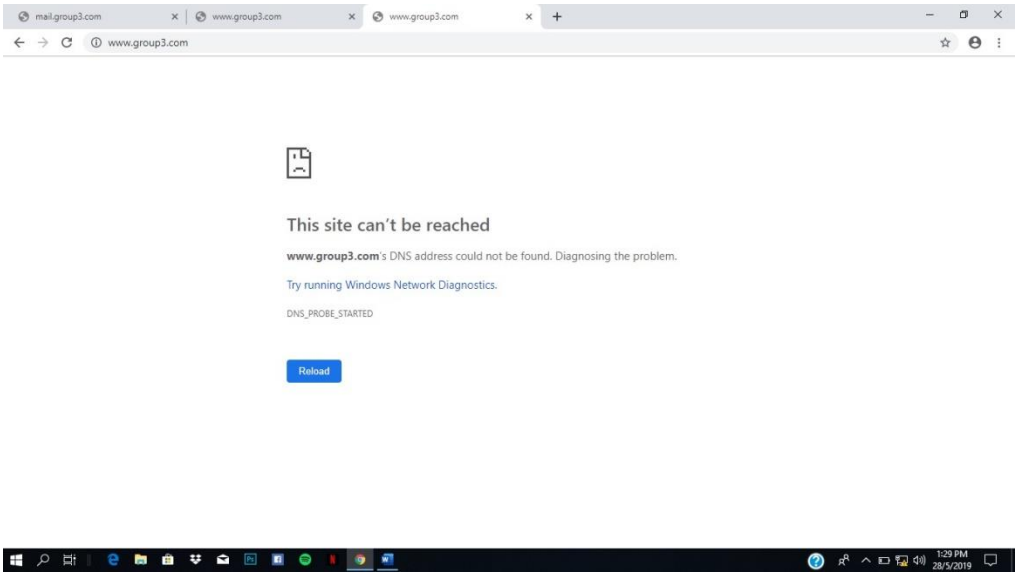


Figure 6.2.9 3 Testing result for HTTP port

Lastly, for the port 22 which is for the FTP service. The result shown as below,(*ftp: connect :connection timed out.*)

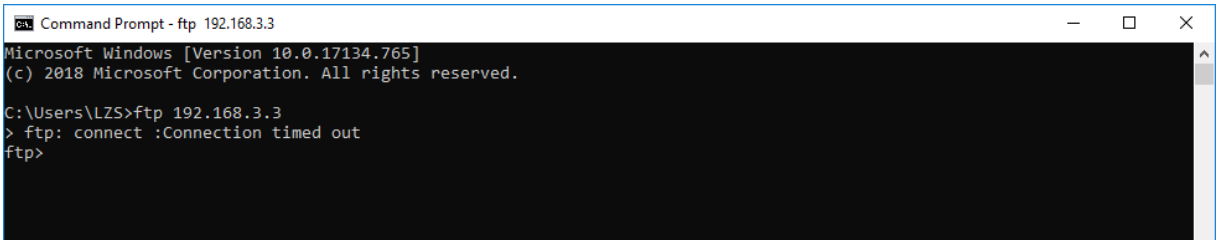


Figure 6.2.9 4 Testing result for FTP port

The client in VLAN50 that used IP address 192.168.5.0 was only able to use ICMP function. The result is tested to ping both server (192.168.1.3) and router (192.168.1.1). Both are successfully ping.

Windows Server 192.168.1.3

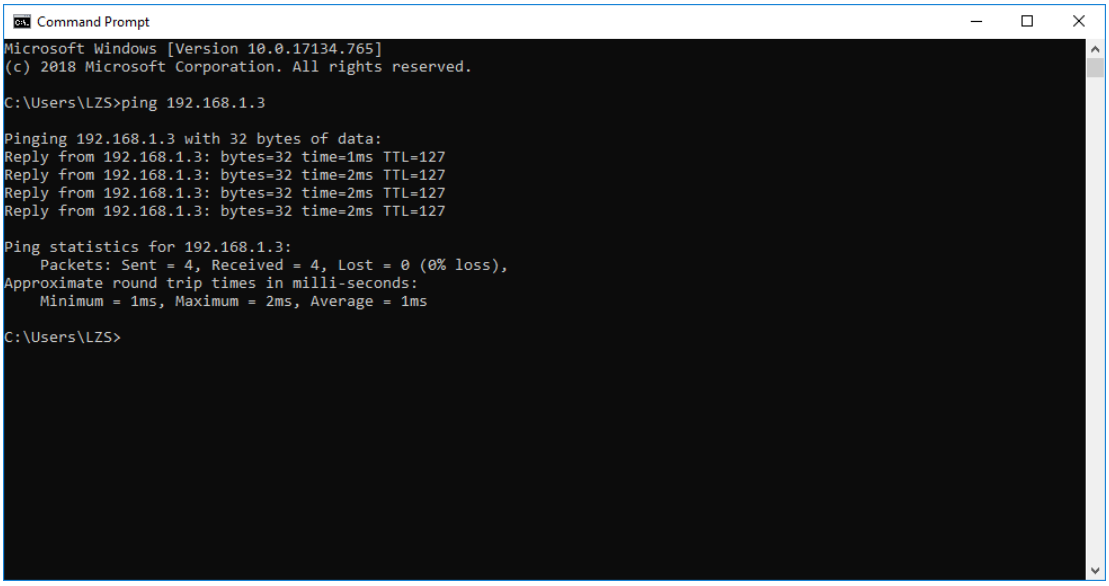


Figure 6.2.9 5 Testing result for ICMP in Windows Server

Router 192.168.1.1

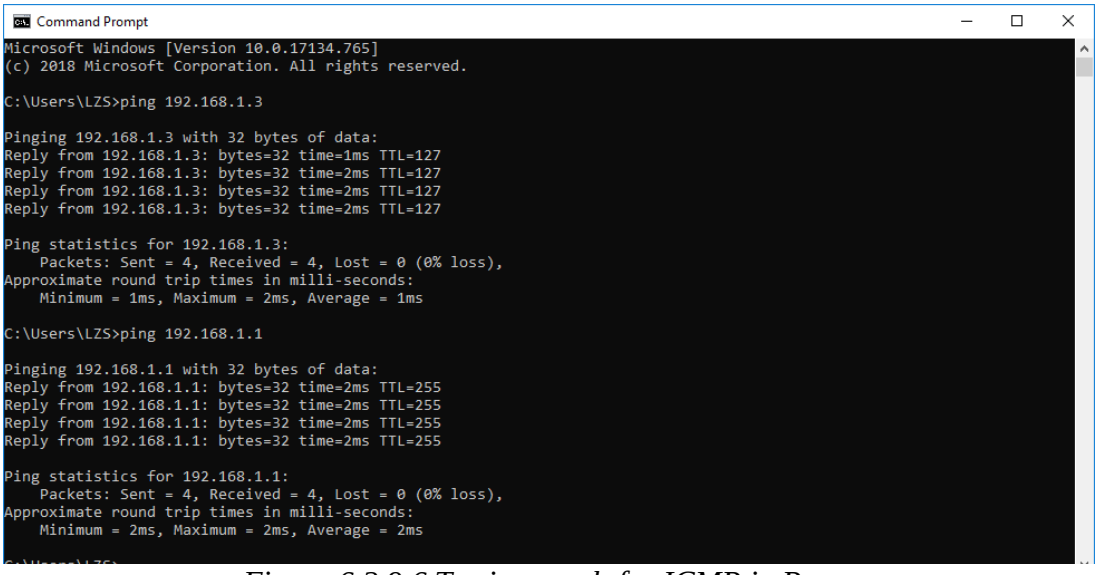


Figure 6.2.9 6 Testing result for ICMP in Router

6.2.10 Linux Email Server

Output of email server after configuration. Browse http://mail.group3.com to open the output.

Step 1: login with username

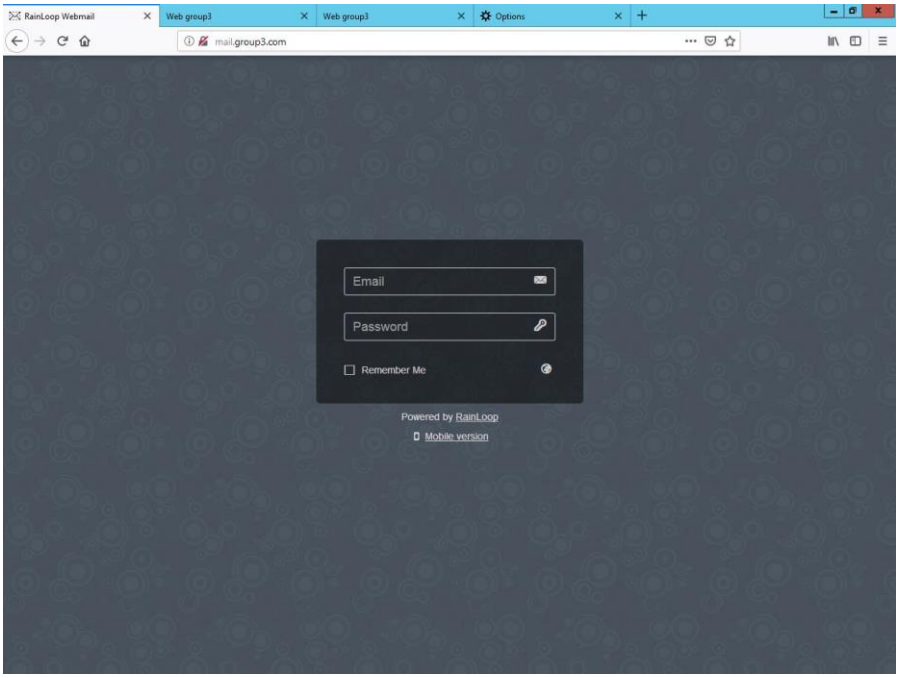


Figure 6.2.10 1 Email login

Step 2: Sent email to other user by clicking new. Email sent to user2@group3.com

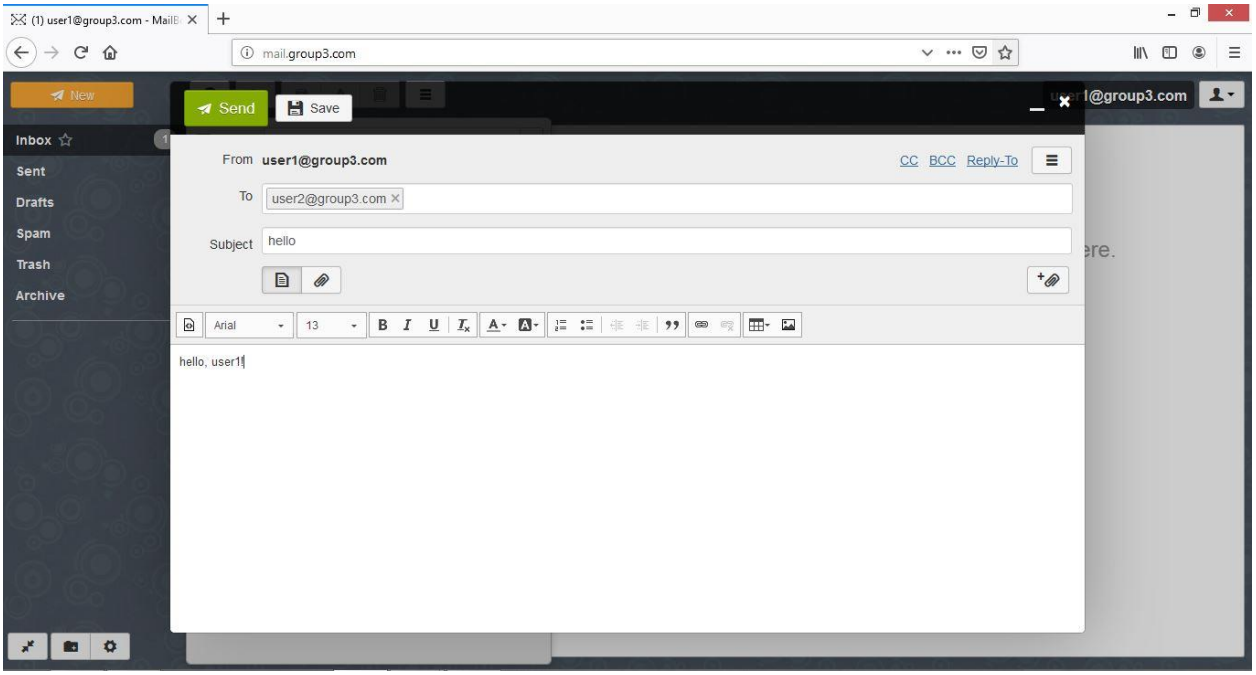


Figure 6.2.10 2 Login as user

Step 3: Open new mail using other user (user2@group3.com)

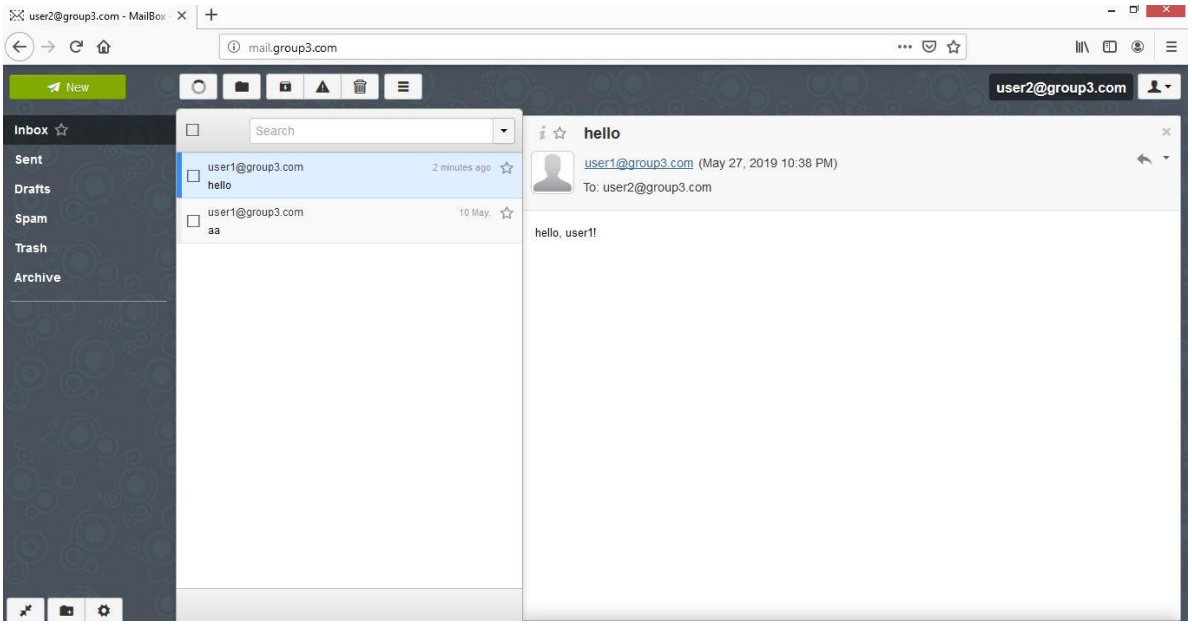


Figure 6.2.10 3 User 2 email receiver

6.2.11 WEB, SSL & Virtual Hosting

TESTING WEB

Step 1: Open the output of web using http://www.group3.com

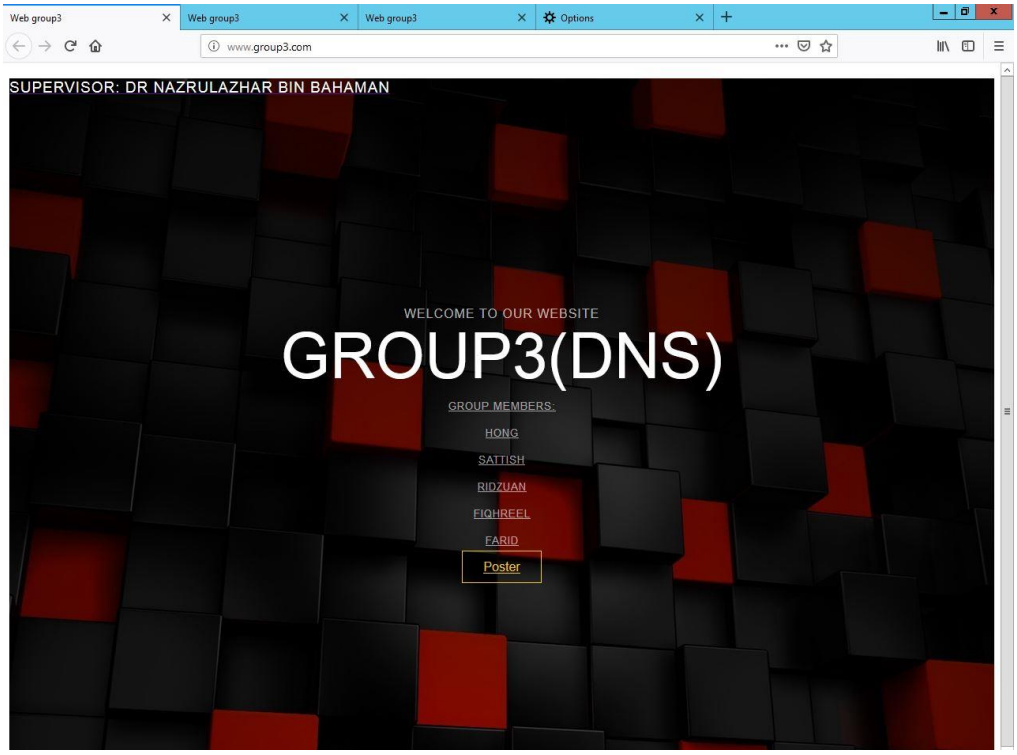


Figure 6.2.11 1 Group website

TESTING SSL

Step 1: Open the output of ssl web using https://www.group3.com

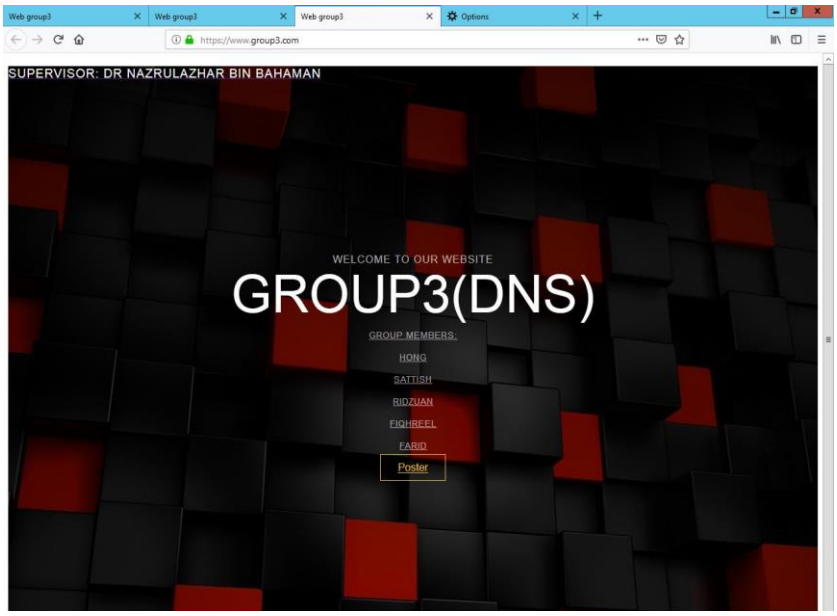


Figure 6.2.11 2 SSL Website

TESTING VIRTUAL HOSTING

Step 1: Open the output of virtual host web using http://www.vhgroup3.com

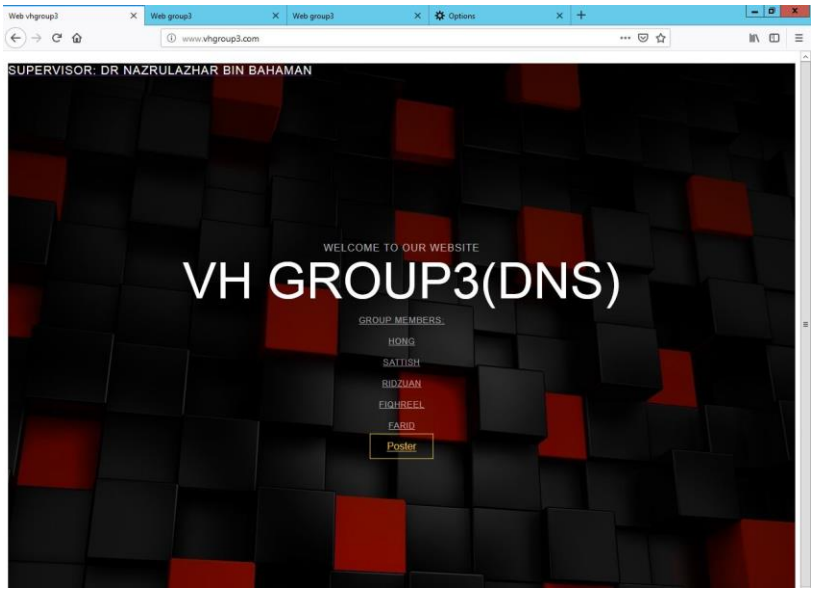


Figure 6.2.11 3 Virtual hosting website

6.2.12 IPV6 Web &Tunneling

IPv6 Web Testing

The website http://www.g3ipv6.com and http://[2001:ab8::1234:3] was tested successfully on three servers which Debian, Windows Server, Ubuntu and Client.

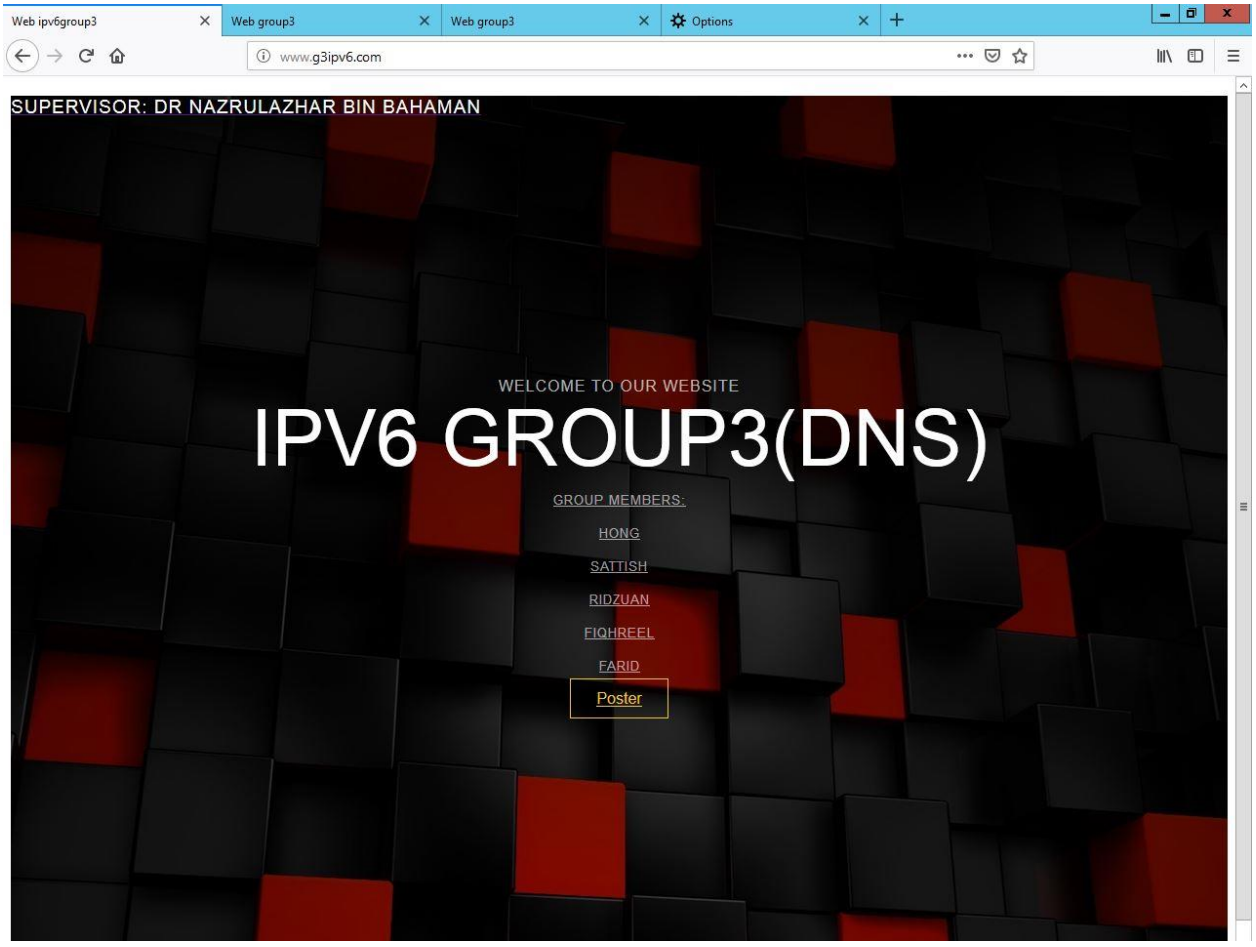


Figure 6.2.12 1 IPv6 website

IPv6 Tunneling Testing

Type the neighbor's website which is http://www.groupv6.com in the web browser. The group 4 website already popup in the browser after insert the website URL, and the tunneling process is successfully completed.

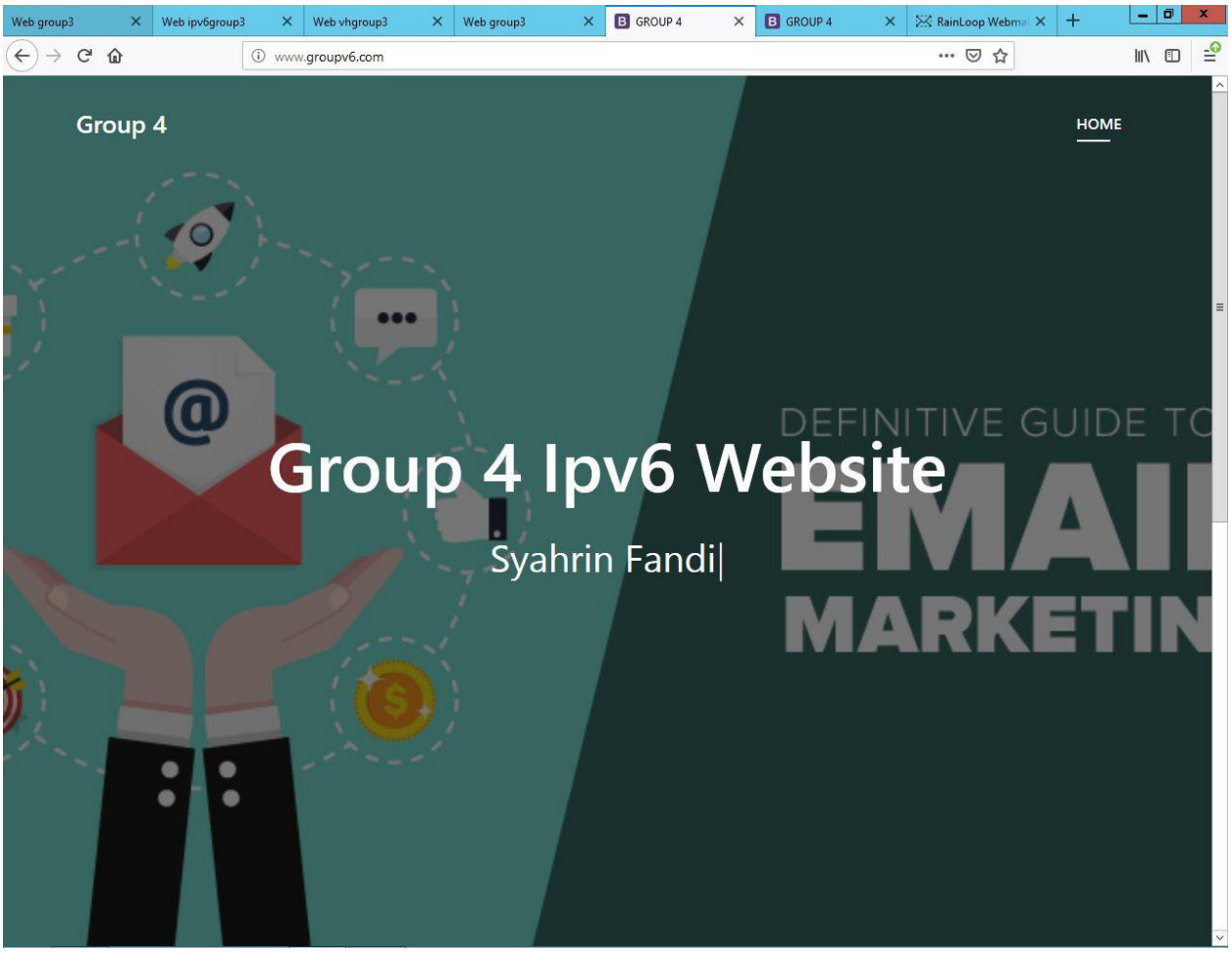


Figure 6.2.12 2 Neighbour group website

6.2.13 IPSec Site-To-Site Tunneling

Step 1 : Test the connection by ping the private ip address of the neigbour using command “ping <neighbour ip_address> source <router ip_address>”

```
Group3Router#ping 192.168.6.1 source 192.168.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.6.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.1.1
```

Figure 6.2.13 1 Ping ip address neighbor from router

Step 2 : Test the connection by ping the public ip address of the neigbour using command “ping <neighbour ip_address> source <router ip_address>”

```
Group3Router#ping 200.200.200.1 source 200.200.200.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 200.200.200.1, timeout is 2 seconds:
Packet sent with a source address of 200.200.200.2
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Figure 6.2.13 2 Ipsec mapping table part 1

Step 3 : Show the ipsec mapping by using command "show crypto session” .

```
Group3Router#sh crypto session
Crypto session current status

Interface: Serial0/2/0
Session status: UP-ACTIVE
Peer: 200.200.200.1 port 500
  IKE SA: local 200.200.200.2/500 remote 200.200.200.1/500 Active
  IPSEC FLOW: permit ip 192.168.1.0/255.255.255.0 192.168.6.128/255.255.255.248
        Active SAs: 0, origin: crypto map
  IPSEC FLOW: permit ip 192.168.1.0/255.255.255.0 192.168.6.0/255.255.255.248
        Active SAs: 2, origin: crypto map
```

Figure 6.2.13 3 Ipsec mapping table part 2

6.2.14 Active Directory

Step 1: Use laptop as client to login the active directory user. Go to the control panel > system and security > system

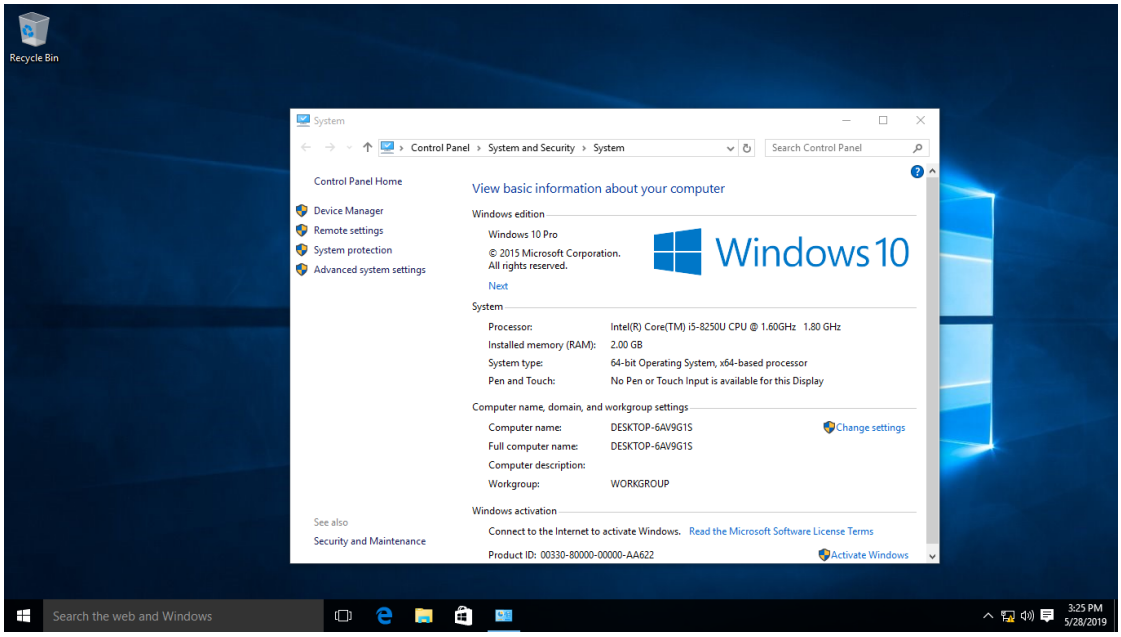


Figure 6.2.14 1 Select my computer for Active Directory Testing

Step 2: Change domain name to group3.com. Go to system properties > change.

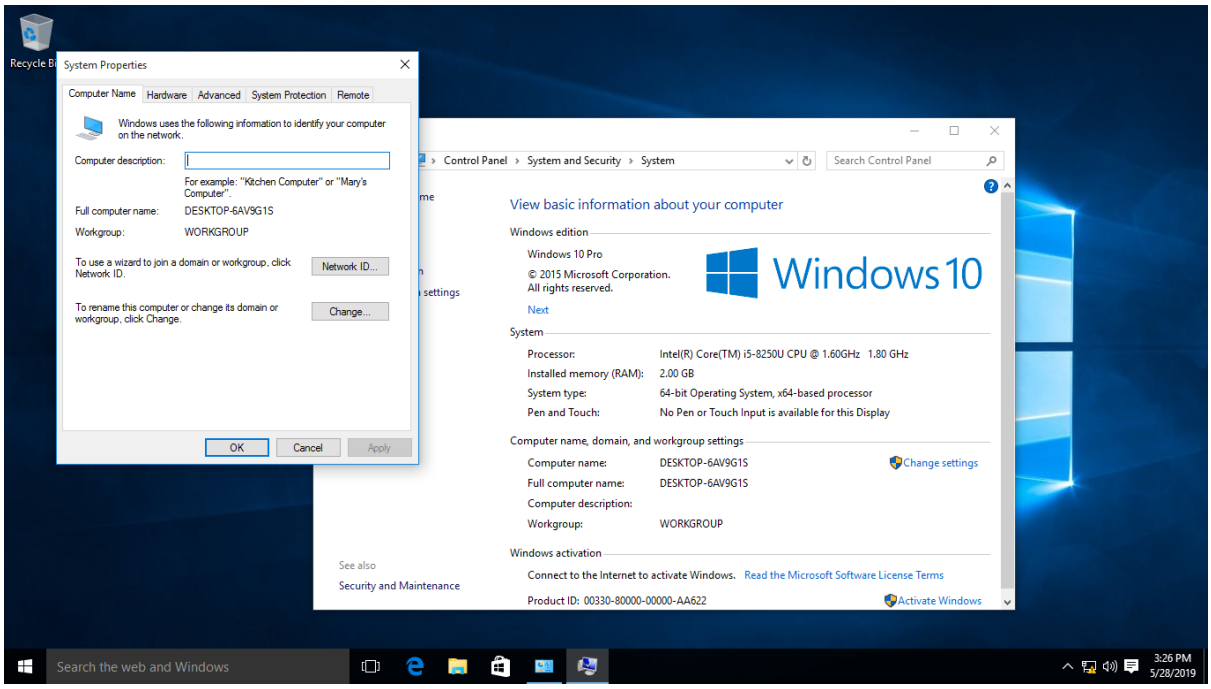


Figure 6.2.14 2 Change domain for Active Directory Testing

Step 3: Choose domain and type group3.com (domain name).

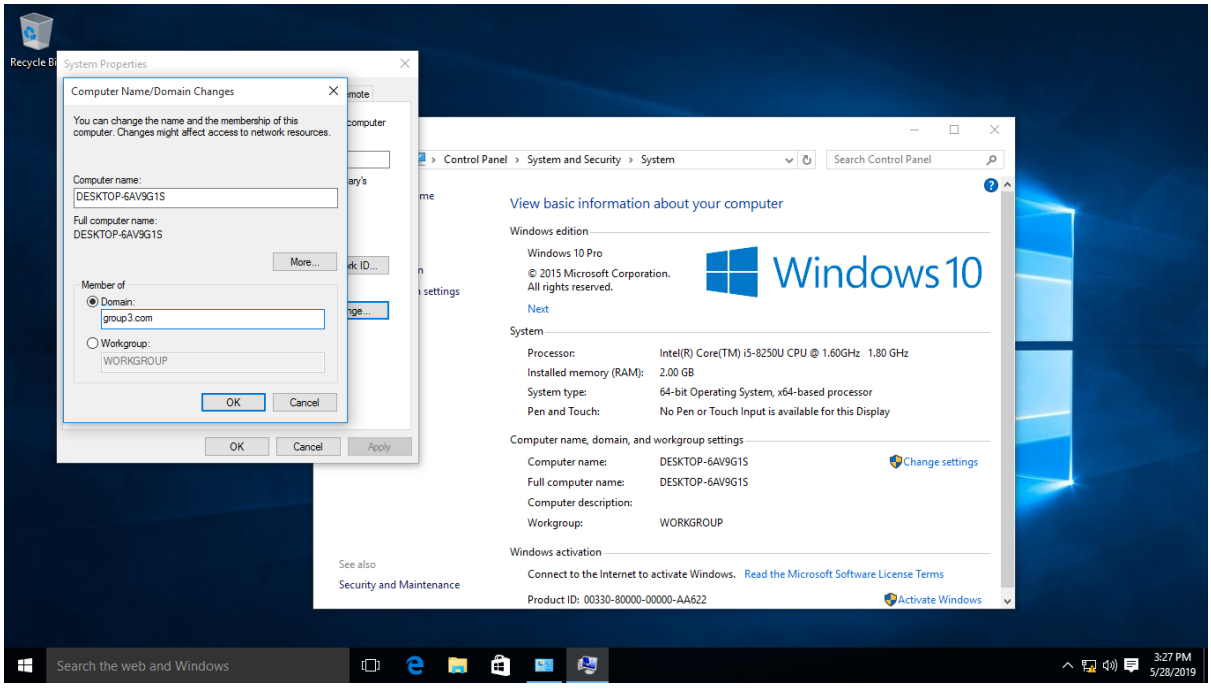


Figure 6.2.14 3 Choose domain for Active Directory Testing

Step 4: Type any AD that created in domain: group3.com.

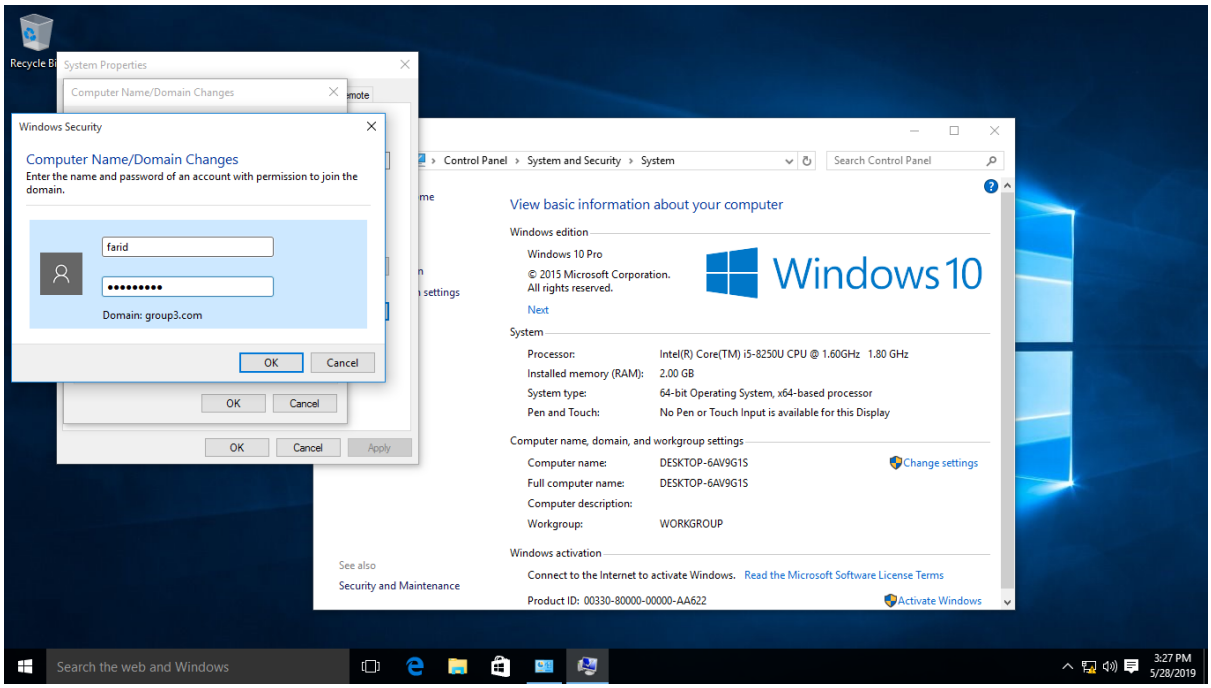


Figure 6.2.14 4 Adding user AD for Active Directory Testing

Step 5: Restart client in order to implement the domain changed to access users of AD that created in the Windows Server.

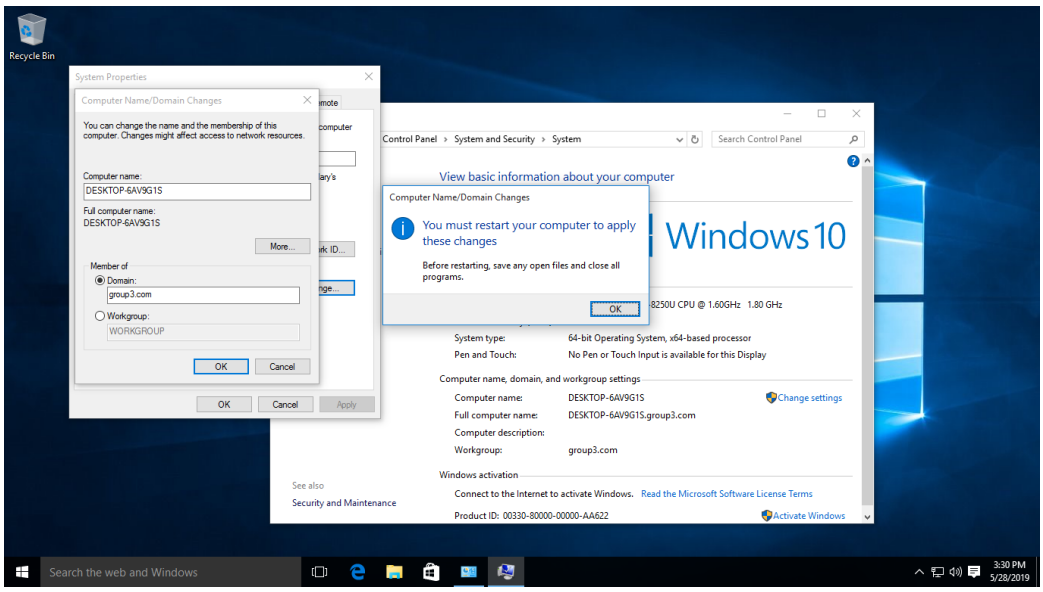


Figure 6.2.14 5 Apply setting for Active Directory Testing

Step 6: User AD can login at client computer.

Figure 6.2.14 6 Login as AD user for Active Directory Testing

Step 7: Show that the account lockout policy has been applied correctly by typing in wrong password for more than 3 times.

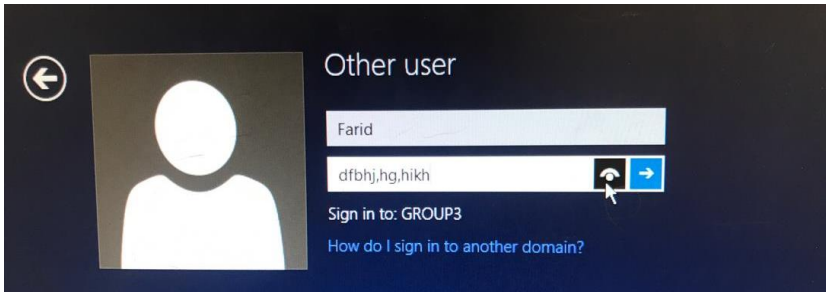


Figure 6.2.14 7 First Wrong Attempt

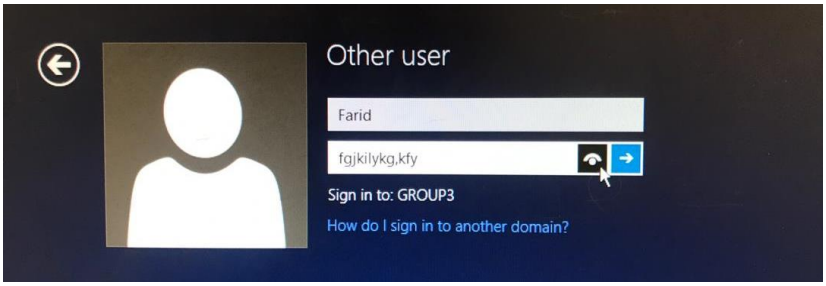


Figure 6.2.14 8 Second Wrong Attempt

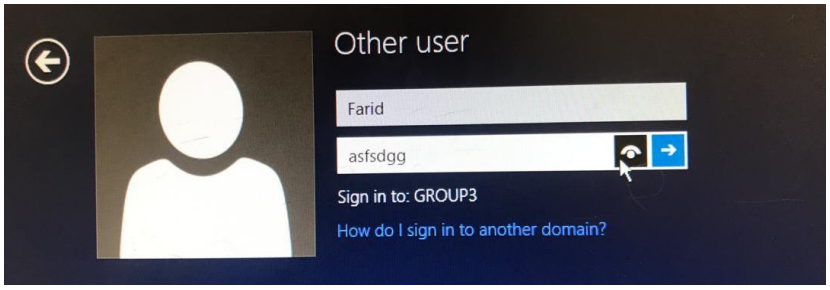


Figure 6.2.14 9 Third Wrong Attempt

Step 8: All the wrong attempts results in computer prompting error login message.

Figure 6.2.14 10 Computer Prompt Message

Step 9: *Try logging in using wrong password for the fourth time.*

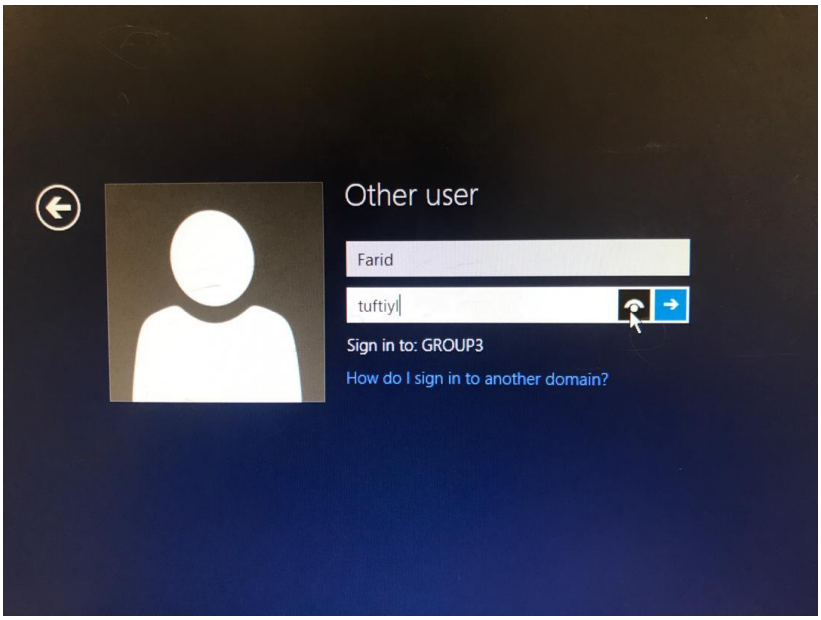


Figure 6.2.14 11 Fourth Wrong Attempt

Step 10: After the fourth attempt, the computer will prompt message that the user account has been locked. This shows that the group policy (security policy) is successfully applied.

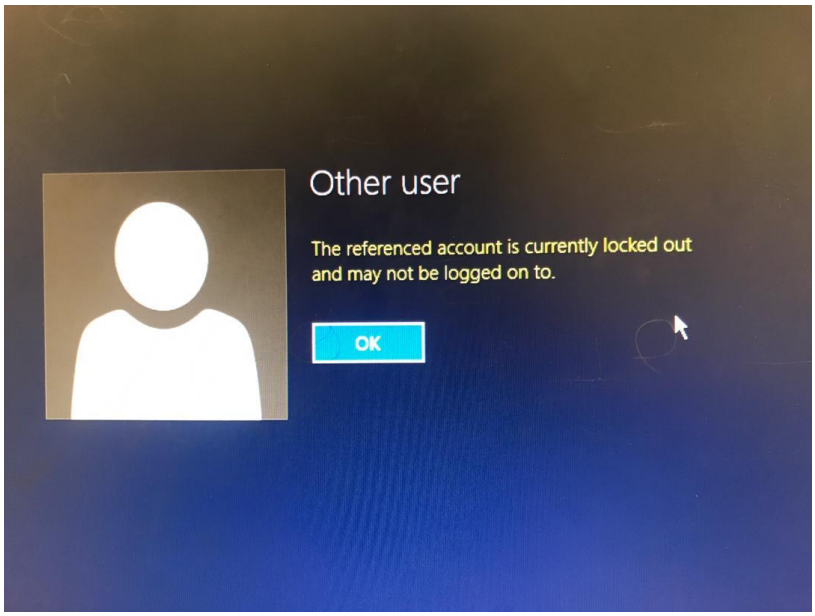


Figure 6.2.14 12 User Account Has Been Locked

6.2.15 Wireless User Authentication Using Radius Server

Step 1: Select available wireless as seen (Group 3 5GHz)

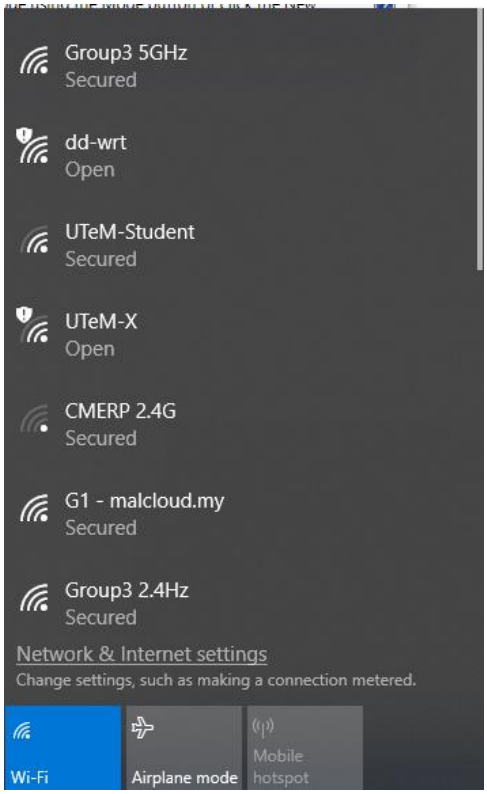


Figure 6.2.15 1 Select available wifi for Wireless Authentication Testing

Step 2: Click and enter user username and password

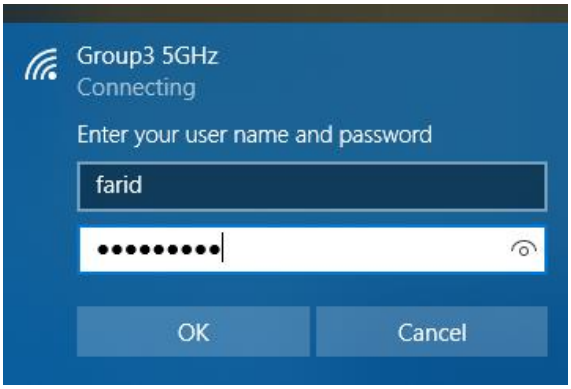


Figure 6.2.15 2 Enter username and password for Wireless Authentication Testing

Step 3: Click connect for a connection with Group 3 wireless.

Figure 6.2.15 3 Connect wifi Wireless Authentication Testing

Step 4 : Check connection log at event viewer if already successful.

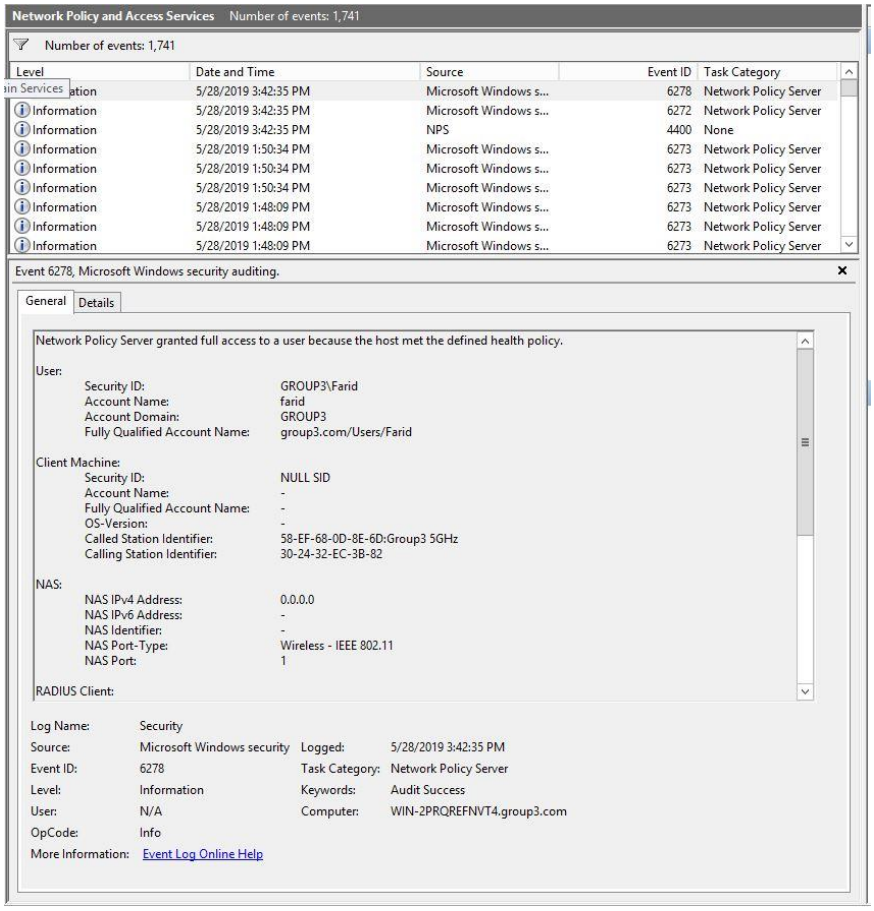


Figure 6.2.15 4 Check connection for Wireless Authentication Testing

6.3 Conclusion

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 needed for risk assessment. A good testing program will allow administrator to determine errors and carry out modification for the best performance. Therefore, all of the services shall be carried out testing.

7.0 CHAPTER 7: CONCLUSION

7.1 Introduction

In this Workshop 2, there are many things have been learnt such as network setup, service configuration, troubleshooting, problem solving throughout the whole semester. Workshop 2 acts as a platform for students to prepare for final year project and industrial training in the future. Through this Workshop 2, students from different majors are worked together as a group to complete all tasks. It is a good platform for students to experience real work environment, practice, apply knowledge from previous learnt subjects into it and so on. Students also able to gain knowledge from mistakes and learn to solve problems.

Starting from planning, implementation, management, a group leader is selected to lead the group. Tasks have been given equally for every member to make sure everyone of it involve. A schedule is arranged to ensure the flow runs smoothly and prevent clashing. So, planning and management is important to ensure tasks given can be completed within given time and reduce the risk of problem occurs. The overall performance of this Workshop 2 was acceptable and running smoothly. Although there are some problems occur during this period still everything is done successfully within the period.

Network environment set up in this Workshop 2 is suitable for small or medium Enterprise Business as it is easy to manage and implement. Moreover, it includes most of the basic network services such as email server, SFTP, DNS, DHCP and others which are the essential elements in running a business. In a nutshell, we are feeling grateful to learn and gain knowledge from this subject which help in future.

7.2 Project Advantage

There are some advantages when implementing this project. The most helpful part of this project is to provide us a real working environment experience on computer networking and security. Besides, it also provides other advantages like: -

i. Learn on designing network design for this project
ii. Learn on how to setup a real network environment
iii. Learn on service installation and configuration
iv. Learn to set up services using different operating systems
v. Learn to troubleshoot and solve problems during the process
vi. Learn to maintain and control network
vii. Learn to build teamwork and tolerance between group members

7.3 Project Disadvantage

Besides advantages, there are disadvantages which are: -

i. Lack of knowledge about certain services
ii. Some equipment provided are old in condition and not functioning well
iii. Time spent on this Workshop is more than expected time
iv. Air-conditioner environment is not provided all the time especially during night time

7.4 Project Limitation

These limitations prevent us from implementing to larger coverage area. We have to adapt and work hard to succeed in this project due to some limitation which are: -

i. The network can only be implemented in wired environment
ii. Not suitable to implement a larger and complex network environment
iii. Equipment provided is not the updated version
iv. This project only involves 3 servers

7.5 Conclusion

Upon the completion of Workshop 2, students are expected to know on how to setup, install, configure, test, maintain, monitor and solve own network environment based on different condition. Workshop 2 has provided a good platform for students to experience real work environment, real hands on activities which couldn't be learnt during class. Through this, more knowledge about network is gained.

Besides, design, installation, configuration, monitoring, problem solving as well as maintenance are required to complete the project using available tools. From this, subjects that have been taken before like Local Area Network (LAN), Wide Area Network (WAN), Operating system (OS) and others are given this opportunity to apply in this Workshop. There are total of 15 network services respectively have been installed in the workstation.

In conclusion, this workshop has been completed successfully on time with the cooperation from each member in the group and also guidance from supervisor.

BIBLIOGRAPHY

How IPSec VPN Site-to-Site Tunnels Work?. (2013, May 28) Retrieved from https://co mmunity.spiceworks.com/topic/341044-how-ipsec-vpn-site-to-site-tunnels-work

Squid - Proxy Server. (n.d.). Retrieved from https://help.ubuntu.com/lts/serverguide/squid.html.en

Understanding VPN IPSec Tunnel Mode and IPSec Transport Mode - What's The Difference. (n.d.). Retrieved from http://www.firewall.cx/networking-topics/protocols/870-ipsec-modes.html

ACL configuration from https://docs.oracle.com/cd/E19859-01/820-3252-11/FP44ucgACL.html

Xiao Guo An (July 12, 2018). How to install RainLoop Webmail on Ubuntu16.04 from https://www.linuxbabe.com/mail-server/install-rainloop- webmail-ubuntu-16-04

APPENDIX

	Week 1	Week 2	Week 3	Week 4	Week 5	Week 6	Week 7	Week 8	Week 9	Week 10	Week 11	Week 12	Week 13	Week 14	Week 15
Project Proposal															
Progress 1															
Progress 2															
Progress 3															
Video &Poster Submission															
Workshop 2 Exhibition															
Final Report & Peer Assesment report & Log Book Submission															