



اوینیورسیتی تیکنیکل ملیسیا ملاک

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

**FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY**

**SEMESTER 1 2019/20**

**BITU3923 - WORKSHOP II**

**BITC & BITZ**

**FINAL REPORT**

**GROUP NUMBER: 14**

**PREPARED BY:**

NAME	MATRIC NO
MOHAMAD FAKHRI ANAS BIN ABDULLAH	B031710393
MOHD FARID WAJDI BIN MOHD MARZUKI	B031710278
SITI NORASHIKIN BINTI HASSAN	B031820127
NUR DAYANA MUNIRAH BINTI ZAINAL ABIDIN	B031820073
MARGARET MOSES	B031710058
UKASYAH BIN MOHD AZLAN	B031710337
NURHASEENA BINTI MOHAMMAD SALLEH	B031710230
WAN NURIN JAZMINA BINTI WAN OMAR	B031820016
NURUL AFIQAH BINTI MAT RIFIN	B031710253

## **ACKNOLEDGEMENTS**

First and foremost, we would like to thank our supervisors of this project, En, Mohammad Radzi bin Motsidi 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 him for showing us some examples that are related to the services in our project which helped us understand our project better. This helped us to complete our project on time. We would also like to thank our evaluator for this workshop, En Suhaimi 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 University of Technical Malaysia Melaka (UTeM) for providing us with good environment and facilities to complete this project. Finally, an honorable 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**

The main objectives for this Workshop 2 are designing a secured network infrastructure by using the available equipment, implementing designated secured network services and configuration into the network infrastructure, installing and integrating network infrastructure, services and configuration based on the requirement of secured network environment, and managing the secured network infrastructure, services and configuration. Our group consists of 9 students, 5 students from BITC and 4 students from BITZ. BITC students are required to install 18 designated network infrastructures includes DNS (IPv4 & IPv6), DHCP (IPv4 & IPv6), Inter VLAN and VLSM addressing, Routing and NAT, Active Directory (AD), Proxy Server, Samba, Network Management System, Server Virtualization, AAA (Authentication, Authorization and Accounting) using Radius, Access Control List (ACL), Secured FTP (with authentication and encryption), Web, SSL & Virtual Hosting, Linux Email Server, IPv6 Web with IPv6 Tunneling (testing IPv6 Web from remote site), Media Streaming Server and Cloud Server. Meanwhile for BITZ students, a security policy should be designed, 12 security services and configuration required to be implemented. The 12 security services and configuration are Router Security (router hardening and remote login using SSH), Server Hardening (Linux server1 hardening and Windows server hardening), Security Service (Authentication user by integrating AD with Linux, Wireless user authentication using Radius server, IDS with port mirror, IPsec VPN for remote employees (between server and user) and Samba security services) and LAN Security (Port security and VLAN security). We have been provided with the equipment which are three (3) servers, one (1) Cisco 1900 router (2 Fast Ethernet), one (1) Cisco 2960 manageable switch, 15 meters UTP cable, 12 pieces RJ-45, NIC card, Access Point (AP) and one set crimping tool. The operating system used in servers are Windows Server 2019, Debian and Ubuntu. After setting up all the network configuration, infrastructure and services, several tests will be done to ensure they are working properly. At the end of workshop II, we are required to demonstrate our work to supervisors and evaluator. We are also required to produce poster and video for exhibition based on our title which is Instrusion Detection System (IDS).

## **ABSTRAK**

Objektif utama Bengkel 2 ini adalah untuk mereka bentuk infrastruktur rangkaian yang selamat dengan menggunakan peralatan yang disediakan, mengaplikasikan servis rangkaian yang ditetapkan dan konfigurasi yang ditetapkan ke dalam infrastruktur rangkaian, memasang dan mengintegrasikan infrastruktur rangkaian, servis dan konfigurasi berdasarkan keperluan persekitaran rangkaian terjamin, dan menguruskan infrastruktur rangkaian, servis dan konfigurasi rangkaian yang dijamin. Kumpulan kami terdiri daripada 9 pelajar, 5 pelajar dari BITC dan 4 pelajar dari BITZ. Pelajar BITC perlu memasang 18 prasarana rangkaian yang ditetapkan termasuk *DNS (IPV4 & IPV6), DHCP (IPV4 & IPV6), InterVLAN dan VLSM, Routing dan NAT, Active Directory (AD), Proxy Server, Samba, Network Management System, Server Virtualization, AAA (Authentication, Authorization and Accounting) using Radius, Access Control List (ACL), Secured FTP (with authentication and encryption), Web, SSL \$ Virtual Hosting, Linux Email Server, IPv6 Web with IPv6 Tunnelling (testing IPv6 Web from remote site), Media Streaming Server and Cloud Server.* Selain itu, untuk pelajar BITZ, satu polisi keselamatan perlu direka, 12 servis keselamatan dan konfigurasi yang perlu dilaksanakan. 12 servis dan konfigurasi adalah *Router Security (router hardening and remote login using SSH), Server Hardening (Linux server1 hardening and Windows Server Hardening), Security Service (Authentication user by integrating AD with Linux, Wireless user authentication using Radius server, IDS with port mirror, IPsec VPN for remote employees (between server and user) and Samba security services) and LAN Security (Port security and VLAN Security).* Kami telah dilengkapi dengan peralatan yang terdiri daripada tiga (3) server, satu (1) Cisco 1900 router (2 Fast Ethernet), satu (1) Cisco 2960 manageable switch, 15 meters UTP cable, 12 pieces RJ-45, NIC card, Access Point (AP) dan satu set crimping tool. Sistem operasi yang digunakan dalam server adalah Windows Server 2019, Debian dan Ubuntu. Selepas melaraskan semua konfigurasi rangkaian, infrastruktur dan servis, beberapa ujian akan dilakukan untuk memastikan ia berfungsi dengan baik. Pada akhir bengkel II, kami dikehendaki menunjukkan kerja kami kepada penyelia dan penilai. Kami juga dikehendaki menghasilkan poster dan video untuk pameran berdasarkan tajuk kami iaitu Instrusion Detection System (IDS).

## Table of Contents

ACKNOLEDGEMENTS .....	2
ABSTRACT .....	3
ABSTRAK .....	4
CHAPTER 1: INTRODUCTION .....	22
1.0 Introduction.....	22
1.1 Objectives.....	23
1.2 Project Planning / Schedule .....	23
1.3 Conclusion .....	25
CHAPTER 2: PROJECT REQUIREMENT .....	26
2.1 Introduction.....	26
2.2 Types of Operating System use in the project .....	26
2.3 Operating system background.....	27
2.3.1 Window Server 2019.....	27
2.3.2 Linux Ubuntu 18.04.3 .....	27
2.3.3 Linux Debian 10.....	28
2.4 Operating system justification .....	28
2.4.1 Window Server 2019 R2.....	28
2.4.2 Linux Ubuntu 18.04.3 .....	29
2.4.3 Linux Debian 10.....	29
2.5 Hardware Requirement .....	30
2.6 Hardware Justification .....	30
2.6.1 Windows Server .....	30
2.6.2 Ubuntu Server .....	30
2.6.3 Debian Server.....	32
2.6.4 Router .....	32
2.6.5 Switch.....	34
2.6.6 UTP cable.....	34
2.6.7 RJ45 .....	35
2.6.8 Crimping Tool.....	35
CHAPTER 3 DESIGN.....	36
3.1 Introduction.....	36

3.2 Security Policy .....	36
3.2.1 General .....	36
3.2.2 Password Creation.....	36
3.2.3 Password Protection .....	36
3.2.4 Network Security .....	37
3.2.5 Application Security.....	38
3.3 Physical Design.....	45
3.4 Logical Design .....	46
3.5 VLAN and VLSM Addressing .....	47
3.6 Conclusion .....	47
<b>CHAPTER 4: SERVICES .....</b>	<b>48</b>
<b>4.1 INTRODUCTION .....</b>	<b>48</b>
<b>4.2 TYPE OF SOFTWARE .....</b>	<b>48</b>
4.2.1 LIST OF OPERATING SYSTEMS .....	48
4.2.2 LIST OF SERVICES .....	48
<b>4.3 BRIEF OVERVIEW OF SERVICES .....</b>	<b>49</b>
4.3.1 Windows Server 2012 .....	49
4.3.2 Ubuntu Server .....	50
4.3.3 Debian Server.....	50
4.3.4 Cloud Server .....	51
4.3.5 DHCP (IPv4 & IPv6) .....	51
4.3.6 Dynamic Routing and NAT .....	51
4.3.7 IPsec site-to-site tunnelling .....	51
4.3.8 Access Control List (ACL) .....	51
4.3.9 DNS (IPv4 & IPv6).....	52
4.3.10 Server Virtualization .....	52
4.3.11 Active Directory.....	52
4.3.12 Wireless user authentication using Radius server.....	52
4.3.13 Linux Email Server .....	52
4.3.14 Web, SSL & Virtual Hosting .....	53
4.3.15 IPv6 Web with IPv6 Tunnelling .....	53
4.3.16 Network Management System .....	53

4.3.17	Proxy server .....	54
4.3.18	Secure FTP .....	54
4.3.19	AAA (Authentication, Authorization and Accounting) using Radius. ....	54
4.3.20	VLAN and Port Security.....	55
4.3.21	Web Hardening .....	55
4.3.22	IDS with port mirror .....	55
4.3.23	Samba and Samba security services.....	55
4.3.24	Linux Server Hardening.....	55
4.3.25	IPsec VPN server for remote employees .....	56
4.3.26	User authentication by integrating AD with Linux.....	56
4.3.27	Windows Server Hardening .....	56
4.3.28	Remote login using SSH .....	56
4.3.29	Media Server .....	56
4.3.30	Router Hardening .....	56
4.3.31	Security Policy .....	57
4.3.32	Inter VLAN .....	57
4.3.33	VLSM addressing .....	57
CHAPTER 5: INSTALLATION AND CONFIGURATION.....		58
5.1	INTRODUCTION .....	58
5.2	SERVICES AND CORRESPONDING PERSON IN CHARGE.....	58
5.3	SERVICE INSTALLATION AND CONFIGURATION .....	61
5.3.1	Cloud Server .....	61
5.3.2	Dynamic Host Configuration Protocol (DHCP) IPV4.....	64
5.3.3	DYNAMIC ROUTING & NAT .....	73
5.3.3.1	DYNAMIC ROUTING.....	73
5.3.3.2	NETWORK ADDRESS TRANSLATING (NAT).....	74
5.3.4	IPSEC SITE TO SITE TUNNELLING .....	75
5.3.5	ACCESS CONTROL LIST .....	76
5.3.6	DOMAIN NAME SYSTEM.....	77
5.3.6.1	FORWARD LOOKUP ZONE (PRIMARY DNS).....	77
5.3.6.2	REVERSE LOOKUP ZONE (IPV4).....	80
5.3.7	SERVER VIRTUALIZATION.....	85

5.3.8 ACTIVE DIRECTORY .....	100
5.3.10 LINUX MAIL SERVER.....	114
5.3.11.1 CONFIGURING COURIER.....	115
5.3.11.2 INSTALLING AND CONFIGURING DOVECOT IMAP SERVER ....	120
5.3.11.3 CONFIGURING MAILBOX LOCATION .....	121
5.3.11.4 CONFIGURING AUTHENTICATION MECHANISM .....	122
5.3.11.5 CONFIGURING SSL/TLS ENCRYPTION.....	123
5.3.11.6 SASL AUTHENTICATION BETWEEN POSTFIX AND DOVECOT	124
5.3.11 WEB, SSL & VIRTUAL HOSTING.....	132
5.3.12 IPV6 WEB & IPV6 TUNNELING.....	138
5.3.12.1 TUNNELLING CONFIGURATION .....	140
5.3.13 NETWORK MANAGEMENT SYSTEM .....	143
5.3.13.1 Install JDK .....	149
5.3.13.2 Install OpenNMS Repository .....	152
5.3.13.3 Post Installation.....	154
5.3.13.4 Install bandwidthd.....	156
5.3.14 PROXY SERVER.....	158
5.3.15 SECURED FTP.....	160
5.3.17 VLAN AND PORT SECURITY .....	174
5.3.17.1 VLAN SECURITY .....	174
5.3.17.2 PORT SECURITY .....	175
5.3.18 WEB HARDENING .....	176
5.3.18.1 WINDOWS AUTHENTICATION.....	176
5.3.18.2 BASIC AUTHENTICATION.....	178
5.3.18.3 URL AUTHORIZATION .....	179
5.3.18.4 IP AND DOMAIN RESTRICTION .....	181
5.3.18.6 LOGGING .....	183
5.3.19 IDS WITH PORT MIRROR.....	184
5.3.19.1 Intrusion Detection System.....	184
5.3.19.2 Snort Installation .....	187
5.3.20 SAMBA AND SAMBA SECURITY DEVICES .....	190
5.3.21 LINUX SERVER HARDENING .....	192

5.3.22 IPSEC VPN SERVER FOR REMOTE EMPLOYEE .....	196
5.3.22.1 VPN SERVER .....	196
5.3.22.2 VPN CLIENT .....	205
5.3.23 USER AUTHENTICATION BY INTEGRATING AD WITH LINUX .....	208
5.3.24 WINDOWS SERVER HARDENING .....	213
5.3.25 REMOTE LOGIN USING SSH .....	221
5.3.25.1 Configuration SSH in Router .....	221
5.3.25.2 Configuration SSH in Ubuntu.....	222
5.3.25.3 Configuration SSH in Debian .....	222
5.3.26 MEDIA SERVER .....	225
5.3.27 ROUTER HARDENING .....	227
5.3.25.5 Enable configuration change notification and logging .....	229
5.2.29 Configure Intervlan in Vlan 10,20, and 30. ....	230
CHAPTER 6 – TESTING .....	232
6.1 INTRODUCTION .....	232
6.2 SERVICES TESTING .....	232
6.2.1 CLOUD SERVER.....	232
6.2.2 DHCP IPv4 & IPv6.....	234
6.2.3 DYNAMIC ROUTING & NAT .....	236
6.2.4 IPSEC SITE TO SITE TUNNELING .....	236
6.2.6 ACCESS CONTROL LIST .....	238
6.2.6 DOMAIN NAME SYSTEM.....	241
6.2.7 SERVER VIRTUALIZATION.....	242
6.2.8 ACTIVE DIRECTORY .....	245
6.2.9 WIRELESS USER AUTHENTICATION USING RADIUS SERVER .....	248
6.2.10 LINUX EMAIL SERVER .....	252
6.2.11 WEB, SSL & VIRTUAL HOSTING.....	257
6.2.12 IPV6 WEB WITH IPV6 TUNNELLING .....	259
6.2.13 NETWORK MANAGEMENT SYSTEM .....	261
6.2.14 PROXY SERVER.....	270
6.2.15 SECURE FTP .....	271
6.2.16 AAA (AUTHENTICATION, AUTHORIZATION, AND ACCOUNTING) USING RADIUS.....	274

6.2.17 VLAN AND PORT SECURITY .....	274
6.2.18 WEB HARDENING .....	275
6.2.19 IDS WITH PORT MIRROR.....	281
6.2.20 SAMBA AND SAMBA SECURITY SERVICES .....	283
6.2.21 LINUX SERVER HARDENING .....	285
6.2.22 IPSEC VPN SERVER FOR REMOTE EMPLOYEES .....	286
6.2.23 USER AUTHENTICATION BY INTEGRATING AD WITH LINUX ....	288
6.2.24 WINDOWS SERVER HARDENING .....	288
6.2.25 REMOTE LOGIN USING SSH .....	289
6.2.26 MEDIA SERVER .....	291
6.2.27 ROUTER HARDENING.....	294
6.2.28 INTER VLAN .....	297
<b>CHAPTER 7 CONCLUSION .....</b>	<b>299</b>
<b>7.0 CONCLUSION .....</b>	<b>299</b>
7.1 Introduction .....	299
7.2 Project Advantages.....	299
7.3 Project Disadvantages .....	300
7.4 Project Limitation.....	300
7.5 Conclusion .....	302
<b>BIBLIOGRAPHY .....</b>	<b>303</b>
<b>APPENDIX .....</b>	<b>304</b>

## LIST OF FIGURES

Figure Chapter 3	45
Figure 3.3.1: Physical Design	45
Figure 3.4.1: Logical Design	46
Figure Chapter 4	
Figure 5. 1 : Apache and MariaDB installation	61
Figure 5. 2 : Enable Apache and MariaDB	61
Figure 5. 3 : Installation PHP	61
Figure 5. 4 : Add password	62
Figure 5. 5 : Flush Priveleges	62
Figure 5. 6 : Install and configure Nextcloud	63
Figure 5. 7 : VH Cloudserver	63
Figure 5. 8 : Navigate URL	63
Figure 5. 9 : Server Roles	64
Figure 5. 10 : DHCP page	64
Figure 5. 11 : Name of the scope	65
Figure 5. 12 : IP address range of the scope	65
Figure 5. 13 : Router IP (Default Getaway)	66
Figure 5. 14 : Domain Name and DNS	66
Figure 5. 15 : Lease Duration	67
Figure 5. 16 : WINS Servers	67
Figure 5. 17 : Configure DHCP Options	68
Figure 5. 18 : Page of DHCP	68
Figure 5. 19 : IP helper command	69
Figure 5. 20 : Scope name IPV6	69
Figure 5. 21 : Scope Prefix IPV6	70
Figure 5. 22 : Add Exclusions for IPV6	70
Figure 5. 23 : Scope Lease IPV6	71
Figure 5. 24 : Configure DHCP Options	71
Figure 5. 25 : Page of DHCP	72
Figure 5. 26 : Scope Options	72
Figure 5. 27 : Scope options in IPV6	73
Figure 5. 28 : Router Eigrp and Router-ID	73
Figure 5. 29 : Network address	73
Figure 5. 30 : IP NAT Outside	74
Figure 5. 31 : Set Static NAT public IP	74
Figure 5. 32 : IP NAT INSIDE	74
Figure 5. 33 : Create ISAKMP phase 1 policy	75
Figure 5. 34 : Create the transform set	75
Figure 5. 35 : Define a pre shared key and create an access-list	75
Figure 5. 36 : Apply the crypto map to the outgoing interface	75
Figure 5. 37 : Deny the port	76
Figure 5. 38 : Assign the access-group in to specific port	76
Figure 5. 39 : Creating a new zone wizard	77
Figure 5. 40 : Selecting zone type	77
Figure 5. 41 : Selecting new zone data replicated	78

Figure 5. 42 : Create a new zone name	78
Figure 5. 43 : Select type of dynamic updates	79
Figure 5. 44 : Completing setup for new wizard zone	79
Figure 5. 45 : Create new ipv4 reverse lookup	80
Figure 5. 46 : Server ip	80
Figure 5. 47 : Select update type for new zone wizard	81
Figure 5. 48 : Completing setup for new wizard zone 2	81
Figure 5. 49 : Enter the Host IP Address	82
Figure 5. 50 : New Host (A or AAAA)	82
Figure 5. 51 : New Host IPv4	83
Figure 5. 52 : Ipv6 reverse lookup	83
Figure 5. 53 : Ipv6 reverse ip	84
Figure 5. 54 : Finish setup for reverse ip	84
Figure 5. 55 : Browse the host name from Forward zone	85
Figure 5. 56 : Add Features required Hyper-V	86
Figure 5. 57 : Select Server Roles	86
Figure 5. 58 : Create Virtual Switches	87
Figure 5. 59 : Virtual Machine Migration	87
Figure 5. 60 : Default Stores	88
Figure 5. 61 : Confirm Installation Selections	88
Figure 5. 62 : Hyper-V Manager	89
Figure 5. 63 : Specify Name And Location	89
Figure 5. 64 : Configure Networking	90
Figure 5. 65 : Connect Virtual Hard Disk	90
Figure 5. 66 : Installation Option	91
Figure 5. 67 : Hyper-V Manager	91
Figure 5. 68 : Virtual Switch Manager for PC-GROUP14	92
Figure 5. 69 : Virtual Switch Manager for PC-GROUP14	92
Figure 5. 70 : Hyper-V Manager	93
Figure 5. 71 : Setting For Group14SV on PC-GROUP14	93
Figure 5. 72 : Hyper-V Manager	94
Figure 5. 73 : Group14SV Virtual Machine	94
Figure 5. 74 : Select Server Roles	95
Figure 5. 75 : Select Role Services	95
Figure 5. 76 : Confirm Installation Selections	96
Figure 5. 77 : Server Manager	96
Figure 5. 78 : Internet Information Services (IIS) Manager	97
Figure 5. 79 : FTP Authentication	97
Figure 5. 80 : WIN-RBMEPARQR68 Home	98
Figure 5. 81 : FTP Authorization Rules	98
Figure 5. 82 : Sites	98
Figure 5. 83 : Binding and SSL Setting	99
Figure 5. 84 : Authentication and Authorization Information	99
Figure 5. 85 : Add Roles and Features Wizard	100
Figure 5. 86 : Select Server Roles	100
Figure 5. 87 : Active Directory Domain Services	101
Figure 5. 88 : Deployment Configuration	101

Figure 5. 89 : Domain Controller Options	102
Figure 5. 90 : Active Directory Users and Computers	103
Figure 5. 91 : New Object – User	103
Figure 5. 92 : Password and Confirm Password	104
Figure 5. 93 : Information Before Created	104
Figure 5. 94 : Add To a Group	105
Figure 5. 95 : Select Groups	105
Figure 5. 96 : ADDS message	105
Figure 5. 97 : Group Policy Management	106
Figure 5. 98 : Group Policy Management Editor	106
Figure 5. 99 : Policy Created	107
Figure 5. 100 : gpupdate Force	107
Figure 5. 101 : Active Directory Users and Computers	108
Figure 5. 102 : Wireless_Group14 properties	108
Figure 5. 103 : Network Policy Server	109
Figure 5. 104 : Select 802.1x Connection Type	109
Figure 5. 105 : New Radius Client	110
Figure 5. 106 : Configuration an Authentication Method	110
Figure 5. 107 : Specify User Group	111
Figure 5. 108 : Configuration Traffic Controls	111
Figure 5. 109 : Successful configure the Radius Client	112
Figure 5. 110 : Radius Client	112
Figure 5. 111 : Linksys Smart Wi-Fi Interface	113
Figure 5. 112 : create host	114
Figure 5. 113 : System Update	114
Figure 5. 114 : Installing Postfix	115
Figure 5. 115 : Directories Web Based	115
Figure 5. 116 : Directories Web Based II	116
Figure 5. 117 : Installation apache2 and php	116
Figure 5. 118 : Checking version apache2 and php	117
Figure 5. 119 : Set Information	117
Figure 5. 120 : Edit master.cf	118
Figure 5. 121 : Edit main.cf	119
Figure 5. 122 : Edit main.cf II	119
Figure 5. 123 : Restarting postfix	120
Figure 5. 124 : Installing Devecot	120
Figure 5. 125 : Edit dovecot.conf	121
Figure 5. 126 : Edit 10-mail.conf	121
Figure 5. 127 : Edit 10-auth.conf	122
Figure 5. 128 : Edit 10-ssl.conf	124
Figure 5. 129 : Edit 10-master.conf	125
Figure 5. 130 : Status	125
Figure 5. 131 : Directory Rainloop and Install Curl	126
Figure 5. 132 : Install Php-Curl	127
Figure 5. 133 : Install Php-Xml	127
Figure 5. 134 : Download Rainloop	128
Figure 5. 135 : Move Directory	128

Figure 5. 136 : Virtual Host	129
Figure 5. 137 : Create User Anas	130
Figure 5. 138 : Create User Farid	130
Figure 5. 139 : Enable Virtual Host	131
Figure 5. 140 : Edit Domain	132
Figure 5. 141 : Add Roles and Features wizard	133
Figure 5. 142 : verify installation succeeds	134
Figure 5. 143 : Server Manager Properties	134
Figure 5. 144 : Enter site name, bindings, and host name then press ok.	135
Figure 5. 145 : Create new host	135
Figure 5. 146 : Key Bindings	136
Figure 5. 147 : Add Website	136
Figure 5. 148 : Enter site name, bindings, and host name then press ok	137
Figure 5. 149 : Create new virtual host	138
Figure 5. 150 : Server Manager Properties	138
Figure 5. 151 : Enter site name, bindings, and host name then press ok	139
Figure 5. 152 : Create new host	140
Figure 5. 153 : ipv6 static	140
Figure 5. 154 : ipv6 tunneling configuration	141
Figure 5. 155 : ipv6 eigrp interface	141
Figure 5. 156 : ipv6 eigrp neighbors	141
Figure 5. 157 : ipv6 eigrp topology	142
Figure 5. 158 : Update Ubuntu	143
Figure 5. 159 : Done Update Ubuntu	143
Figure 5. 160 : Install PostgreSQL	144
Figure 5. 161 : PostgreSQL command	144
Figure 5. 162 : Configure PostgreSQL	145
Figure 5. 163 : Install phpPgAdmin	146
Figure 5. 164 : Edit /etc/apache2/conf.d/phpgadmin	146
Figure 5. 165 : Restart services	147
Figure 5. 166 : Edit /etc/phppgadmin/config.inc.php	147
Figure 5. 167 : Restart services	148
Figure 5. 168 : Create new user	148
Figure 5. 169 : Open phpPgAdmin website	148
Figure 5. 170 : Login done	149
Figure 5. 171 : Step to install JDK	149
Figure 5. 172 : Update	149
Figure 5. 173 : Install default JRE	150
Figure 5. 174 : Install Java 13	150
Figure 5. 175 : OK	151
Figure 5. 176 : Click Yes	151
Figure 5. 177 : Add the OpenNMS APT repository	152
Figure 5. 178 : Create a file	152
Figure 5. 179 : Add OpenNMS key	152
Figure 5. 180 : Install OpenNMS	153
Figure 5. 181 : Click OK	153
Figure 5. 182 : Click OK	154

Figure 5. 183 : Inform OpenNMS on version of Java	154
Figure 5. 184 : Create a database for OpenNMS	155
Figure 5. 185 : Edit a file in OpenNMS	155
Figure 5. 186 : Editing file	155
Figure 5. 187 : Restart and Check status OpenNMS	156
Figure 5. 188 : Install bandwidth	156
Figure 5. 189 : Interface to running in Bandwidthd choose any	157
Figure 5. 190 : Insert IP address and subnet mask	157
Figure 5. 191 : Install squid package	158
Figure 5. 192 : Checking squid status	158
Figure 5. 193 : Configure the proxy file	158
Figure 5. 194 : Setup proxy on browser	159
Figure 5. 195 : Install vsftpd	160
Figure 5. 196 : Open systemctl start vsftpd	160
Figure 5. 197 : Open vsftpd config file	160
Figure 5. 198 : Allow anonymous FTP	160
Figure 5. 199 : Uncomment write_enable=YES	161
Figure 5. 200 : FTP server log	161
Figure 5. 201 : Adding comment to the end	161
Figure 5. 202 : Add new user	161
Figure 5. 203 : Restart vsftpd	161
Figure 5. 204 : Add Roles	162
Figure 5. 205 : Create a new group	162
Figure 5. 206 : Create new user	163
Figure 5. 207 : Input password for the user	163
Figure 5. 208 : Create AAA in DNS Manager	164
Figure 5. 209 : Set a new host	164
Figure 5. 210 : Register server to Active Directory	165
Figure 5. 211 : Set the friendly name and Shared secret	165
Figure 5. 212 : Verify the Address	166
Figure 5. 213 : Change the vendor name	166
Figure 5. 214 : Creating new policy	167
Figure 5. 215 : Set policy name	167
Figure 5. 216 : Set a specify conditions (user group)	168
Figure 5. 217 : Select the access granted permission	168
Figure 5. 218 : Choose the authentication methods	169
Figure 5. 219 : Change the value of service-type	169
Figure 5. 220 : Choose the others attribute and set it to login	170
Figure 5. 221 : Add the vendor	170
Figure 5. 222 : Add the attribute value	171
Figure 5. 223 : Configure new accounting	171
Figure 5. 224 : Select Accounting options	172
Figure 5. 225 : Configure Local File	172
Figure 5. 226 : Configuration for local user	173
Figure 5. 227 : Configuration for the AAA	173
Figure 5. 228 : Create VLAN60	174
Figure 5. 229 : Put unused port into VLAN60	174

Figure 5. 230 : Assign all usable ports into trunk	174
Figure 5. 231 : Change native vlan into 3	174
Figure 5. 232 : Command for violation	175
Figure 5. 233 : Command for WIndows Server	175
Figure 5. 234 : Command for Ubuntu Server	175
Figure 5. 235 : Command for Debian Server	175
Figure 5. 236 : Add Roles and Features	176
Figure 5. 237 : Choose Windows Authentication	176
Figure 5. 238 : Install Windows Authentication	177
Figure 5. 239 : Disable anonymous authentication	177
Figure 5. 240 : Choose basic authentication	178
Figure 5. 241 : Install basic authentication features	178
Figure 5. 242 : Enable the basic authentication	179
Figure 5. 243 : Add URL Authorization features	179
Figure 5. 244 : Remove the existing rule	180
Figure 5. 245 : Specific users for the authorization rule	180
Figure 5. 246 : Insert the IP Address to restrict from access the websites	181
Figure 5. 247 : Change the settings	181
Figure 5. 248 : The website that contains.png picture	182
Figure 5. 249 : Deny the .png file extension	182
Figure 5. 250 : Configure the place to save the log files.	183
Figure 5. 251 : Command line	184
Figure 5. 252 : Command line	184
Figure 5. 253 : Command line	185
Figure 5. 254 : Download daq 2.0.6	185
Figure 5. 255 : List of daq	186
Figure 5. 256 : Configure and make install daq	186
Figure 5. 257 : Install Snort 2.9.15	187
Figure 5. 258 : Enable sourcefire and install	187
Figure 5. 259 : Update shared library	188
Figure 5. 260 : Create a symlink	188
Figure 5. 261 : Creating user	188
Figure 5. 262 : Create files and permissions	188
Figure 5. 263 : Create files in rules	188
Figure 5. 264 : Copy configuration	189
Figure 5. 265 : Install community rules	189
Figure 5. 266 : Extract the downloaded community rules	189
Figure 5. 267 : Installation	190
Figure 5. 268 : Server running	190
Figure 5. 269 : Create backup	191
Figure 5. 270 : Directory	191
Figure 5. 271 : Set group	191
Figure 5. 272 : Restart	191
Figure 5. 273 : Password information	192
Figure 5. 274 : Install library for minimum password	192
Figure 5. 275 : Configuration file for minimum password	193
Figure 5. 276 : Installing nmap	193

Figure 5. 277 : List of port in Ubuntu server	194
Figure 5. 278 : Backup interface	195
Figure 5. 279 : Install the VPN	196
Figure 5. 280 : Select Softether VPN Server	196
Figure 5. 281 : User to the License Agreement	197
Figure 5. 282 : Confirm install	197
Figure 5. 283 : Progress installation	198
Figure 5. 284 : Finish the installation.	198
Figure 5. 285 : Run the Softether	199
Figure 5. 286 : Setting name	199
Figure 5. 287 : Setting	200
Figure 5. 288 : Remote access	200
Figure 5. 289 : Set default	201
Figure 5. 290 : DNS hostname	201
Figure 5. 291 : Enable L2TP	202
Figure 5. 292 : Manage Virtual Hub	202
Figure 5. 293 : Create Client	203
Figure 5. 294 : Create Cert	203
Figure 5. 295 : Save Cert	204
Figure 5. 296 : Ipsec VPN	204
Figure 5. 297 : install the Softether	205
Figure 5. 298 : Choose Sofether VPN Client	205
Figure 5. 299 : Finish Installation	206
Figure 5. 300 : Configure VPN Client Manager	206
Figure 5. 301 : VPN Server	207
Figure 5. 302 : Navigate Directory	208
Figure 5. 303 : Install the PBIS	208
Figure 5.304: Direct to /etc/hosts	209
Figure 5. 305 : Edit /etc/hosts	209
Figure 5. 306 : Direct to /etc/resolv.conf	209
Figure 5. 307 : Edit /etc/resolv.conf	210
Figure 5. 308 : Setup AD settings	210
Figure 5. 309 : Direct to pam.d/common-session	210
Figure 5. 310 : Edit pam.d/common-session	211
Figure 5. 311 : Edit lightdm	211
Figure 5. 312 : Lightdm configuration	211
Figure 5. 313 : Integrate with Active Directory	212
Figure 5. 314 : Configuring Group Policy Management	213
Figure 5. 315 : Edit the GPO for Domain	213
Figure 5. 316 : Edit the Audit Policy	214
Figure 5. 317 : Change the properties of the service	214
Figure 5. 318 : Select Success	215
Figure 5. 319 : The policy setting changed	215
Figure 5. 320 : Execute the changes	216
Figure 5. 321 : Windows Firewall Setting	216
Figure 5. 322 : Turn on the Windows Firewall	217
Figure 5. 323 : The green indicates the firewall is turned on	217

Figure 5. 324 : Go to Services	218
Figure 5. 325 : Change the startup type	218
Figure 5. 326 : Change from Automatic to Disabled	219
Figure 5. 327 : Go to AD Users and Computers	219
Figure 5. 328 : Disable the unused account: Guest	220
Figure 5. 329 : Go to Windows Update	220
Figure 5. 330 : Automatically update	221
Figure 5. 331 : SSH configuration in router	221
Figure 5. 332 : SSH configuration in Ubuntu	222
Figure 5. 333 : Check the status of the SSH	222
Figure 5. 334 : Change user to root	223
Figure 5. 335 : SSH command to install	223
Figure 5. 336 : Start the SSH Service	223
Figure 5. 337 : Check the status of SSH service	224
Figure 5. 338 : Downloading of Plex media sever installer .	225
Figure 5. 339 : Installation of Plex media server.	225
Figure 5. 340 : Enable and start Plex media server.	225
Figure 5. 341 : Plex web interface.	226
Figure 5. 342 : Putty Login	227
Figure 5. 343 : Banner motd	227
Figure 5. 344 : System Log	228
Figure 5. 345 : Disable console and monitor logs	228
Figure 5. 346 : Enable syslog	229
Figure 5. 347 : Show Archive log config	229
Figure 5. 348 : Assign VLAN in switch	230
Figure 5. 349 : Assigns port in switch	230
Figure 5. 350 : Configure default getaway	231
Figure 5. 351 : Configure trunk	231
Figure Chapter 6	
Figure 6. 1 : Login to NextClouD	232
Figure 6. 2 : Homepage after login	233
Figure 6. 3 : Access NextCloud from Windows Server	233
Figure 6. 4 : IPV4 in Client's PC	234
Figure 6. 5 : Ping from Client to Server IPV4	234
Figure 6. 6 : Client connect to DNS	235
Figure 6. 7 : Ping from Client to Windows Server IPV	235
Figure 6. 8 : OSPF Neighbor	236
Figure 6. 9 : IP NAT translations	236
Figure 6. 10 : Ping IP Public Neighbor	236
Figure 6. 11 : Show crypto ipsec sa	237
Figure 6. 12 : Show crypto session	237
Figure 6. 13 : Ping 172.168.1.145 source 192.168.14.178	237
Figure 6. 14 : Show crypto ipsec sa	238
Figure 6. 15 : HTTPS testing	238
Figure 6. 16 : SFTP testing	239
Figure 6. 17 : PING testing	239
Figure 6. 18 : TELNET testing	240

Figure 6. 19 : Testing DNS	241
Figure 6. 20 : FileZilla Administrator	242
Figure 6. 21 : File Sharing	242
Figure 6. 22 : FTP file for file sharing	243
Figure 6. 23 : Create a text in Notepad	243
Figure 6. 24 : Share TXT.File from virtual machine to window server	244
Figure 6. 25 : TXT.file success sharing	244
Figure 6. 26 : Changes client to Domain	245
Figure 6. 27 : Windows Security	245
Figure 6. 28 : Computer Name/Domain Changes	246
Figure 6. 29 : Before The Policy is Enable	246
Figure 6. 30 : After The Policy is Enable	247
Figure 6. 31 : Linksys Smart Wi-Fi Ping Details	248
Figure 6. 32 : Command Prompt Window Server	248
Figure 6. 33 : group14 Wi-Fi	249
Figure 6. 34 : Certificate	249
Figure 6. 35 : Connected Group14 Wi-Fi	250
Figure 6. 36 : Connected at laptop	250
Figure 6. 37 : DHCP Manager	251
Figure 6. 38 : Sending Message	252
Figure 6. 39 : Sent item	253
Figure 6. 40 : Abu Inbox	253
Figure 6. 41 : Thunderbird Ali Login	254
Figure 6. 42 : Thunderbird Ali Sending a Message	255
Figure 6. 43 : Thunderbird Ali sent Item	255
Figure 6. 44 : Thunderbird Haikal Login	256
Figure 6. 45 : Thunderbird Abu Inbox.	256
Figure 6. 46 : Main website ( <a href="http://www.group14.com">http://www.group14.com</a> )	257
Figure 6. 47 : Main website ( <a href="https://www.group14.com">https://www.group14.com</a> )	257
Figure 6. 48 : Second webpage using virtual hosting ( <a href="http://website.group14.com">http://website.group14.com</a> )	258
Figure 6. 49 : ipv6 web	259
Figure 6. 50 : neighbour ipv6 web	259
Figure 6. 51 : neighbour ipv4 web	260
Figure 6. 52 : Browse OpenNMS Horizon website.	261
Figure 6. 53 : Login done.	261
Figure 6. 54 : Configure Notifications	262
Figure 6. 55 : Destination Path	262
Figure 6. 56 : Editing Path	263
Figure 6. 57 : Choose users and groups	263
Figure 6. 58 : Editing path: Email-Admin	263
Figure 6. 59 : Finish adding Email-Admin	264
Figure 6. 60 : Update Notification Status	264
Figure 6. 61 : Manually Add an Interface	264
Figure 6. 62 : Insert IP Address	265
Figure 6. 63 : Select perspective node	265
Figure 6. 64 : Turn OFF DNS service	266
Figure 6. 65 : DNS service down	266

Figure 6. 66 : Recent Event to view service up and down	267
Figure 6. 67 : Turn ON DNS service	267
Figure 6. 68 : DNS service up	268
Figure 6. 69 : View Charts	268
Figure 6. 70 : View graph by each service on 192.168.14.178	269
Figure 6. 71 : View graph on each node	269
Figure 6. 72 : Ulearn Blocked website	270
Figure 6. 73 : Group13 Blocked website	270
Figure 6. 74 : Successful Connected	271
Figure 6. 75 : Uploading a file	272
Figure 6. 76 : File Transfer Process	272
Figure 6. 77 : Captured FTP packets	273
Figure 6. 78 : Result when login into the router	274
Figure 6. 79 : Trunk setting in port	274
Figure 6. 80 : Show every VLAN	274
Figure 6. 81 : Check Port Security status	275
Figure 6. 82 : Authentication Testing successful	275
Figure 6. 83 : Unsuccessful authenticate	276
Figure 6. 84 : Log in using user anas	277
Figure 6. 85 : Error unauthorized	277
Figure 6. 86 : Successful URL Authorization	278
Figure 6. 87 : Access denied	278
Figure 6. 88 : Website that consists a picture	279
Figure 6. 89 : The picture has been filtered	279
Figure 6. 90 : Locate the log files	280
Figure 6. 91 : The log files	280
Figure 6. 92 : Check status snort service	281
Figure 6. 93 : Test snort	281
Figure 6. 94 : Test snort	282
Figure 6. 95 : Ubuntu ip address	283
Figure 6. 96 : Folder shared	283
Figure 6. 97 : Folder that is shared	284
Figure 6. 98 : Shared Folder	284
Figure 6. 99 : Display port that have been disabled	285
Figure 6. 100 : Display password information	285
Figure 6. 101 : Disabled Bluetooth	286
Figure 6. 102 : Setup the client of remote network	286
Figure 6. 103 : A VPN connection is created.	287
Figure 6. 104 : Success connection	287
Figure 6. 105 : Login successful	288
Figure 6. 106 : Start SSH	289
Figure 6. 107 : Login and create files	289
Figure 6. 108 : Check file at Debian.	289
Figure 6. 109 : Check file .txt in fiqa folder	290
Figure 6. 110 : start SSH	290
Figure 6. 111 : Login Ubuntu from Fedora	290
Figure 6. 112 : Create Ubuntu file from Fedora	290

Figure 6. 113 : Check existing file at Desktop	291
Figure 6. 114 : Plex WeB interface.	291
Figure 6. 115 : Add library for add media files	292
Figure 6. 116 : Choose media to upload	292
Figure 6. 117 : Browse media folder	293
Figure 6. 118 : Add themedia	293
Figure 6. 119 : Add Library	294
Figure 6. 120 : Successfully photo uploaded	294
Figure 6. 121 : Options controlling session logging	295
Figure 6. 122 : save log file name	295
Figure 6. 123 : Create log file in router	296
Figure 6. 124 : Location and save of log file	296
Figure 6. 125 : Show the configuration of log file	297
Figure 6. 126 : Ping from VLAN 20 to VLAN 10	297
Figure 6. 127 : Ping from VLAN 30 to VLAN 10	298

## **CHAPTER 1: INTRODUCTION**

### **1.0 Introduction**

This Workshop 2 (BITU 3923) is introduced to all third-year bachelor's degree students as a platform to prepare students before undergo their Final Year Project and Industrial Training. During Workshop 2 students will work in group and they are required to develop a project based on their majoring. Workshop 2 provides an opportunity to students to practice their knowledge and experience gained from previous subjects. Students also able to develop their understanding of problem-solving techniques to solve a particular problem based on their respective project.

One of the outcomes of the subject are student should be able to design the network infrastructure by using the available tools and be able to implement designated network services also to install and integrate network services infrastructure to suit the network environment while maintain and control the network services infrastructure

It will also train students to work in group and solve the problems that arise together like the actual environment in industry which emphasize on being a good team player and critical thinking. Each group will be provided with 3 servers (1 Windows and 2 Linux Distro), 2 network interface card (NIC), one Access Point, 1 router (2 FastEthernet), one Manageable Switch, one wireless router, one serial cable, UTP cable, 12 RJ-45 and 1 set of Crimping Tool.

Based on the above equipment, we are required to design, set up, maintain and monitor a network environment with basic server applications and fundamental services also the basic service that were built in this network environment. In total with 30 services will installed on the network to make sure it fulfil the question scenario requirements. We have to use three different operating system which is Microsoft Windows 2012 Server, Linux operating system that is Debian and UBUNTU.

Company Nexro sdn.bhd. is expanding with approximately 100 employees. This company provide server room where the main server is home and client connect to the remote site. The sites are connected with simple point to point that can be used to carry

IPv6 packets between the sites. We have setup the infrastructure for company Nexo that covers all the networking functions.

## **1.1 Objectives**

The main objective of this project is to setup and secure a network infrastructure using the available tools where at the same time able to improve the understanding of the concept of the network design. Next, to ensure the three servers with different platforms are suitable with each other is one of the objectives of this project. Other than that, this project is aimed for the students to be capable to install and integrate network services infrastructure to suit the network environment and the security policies that have been set.

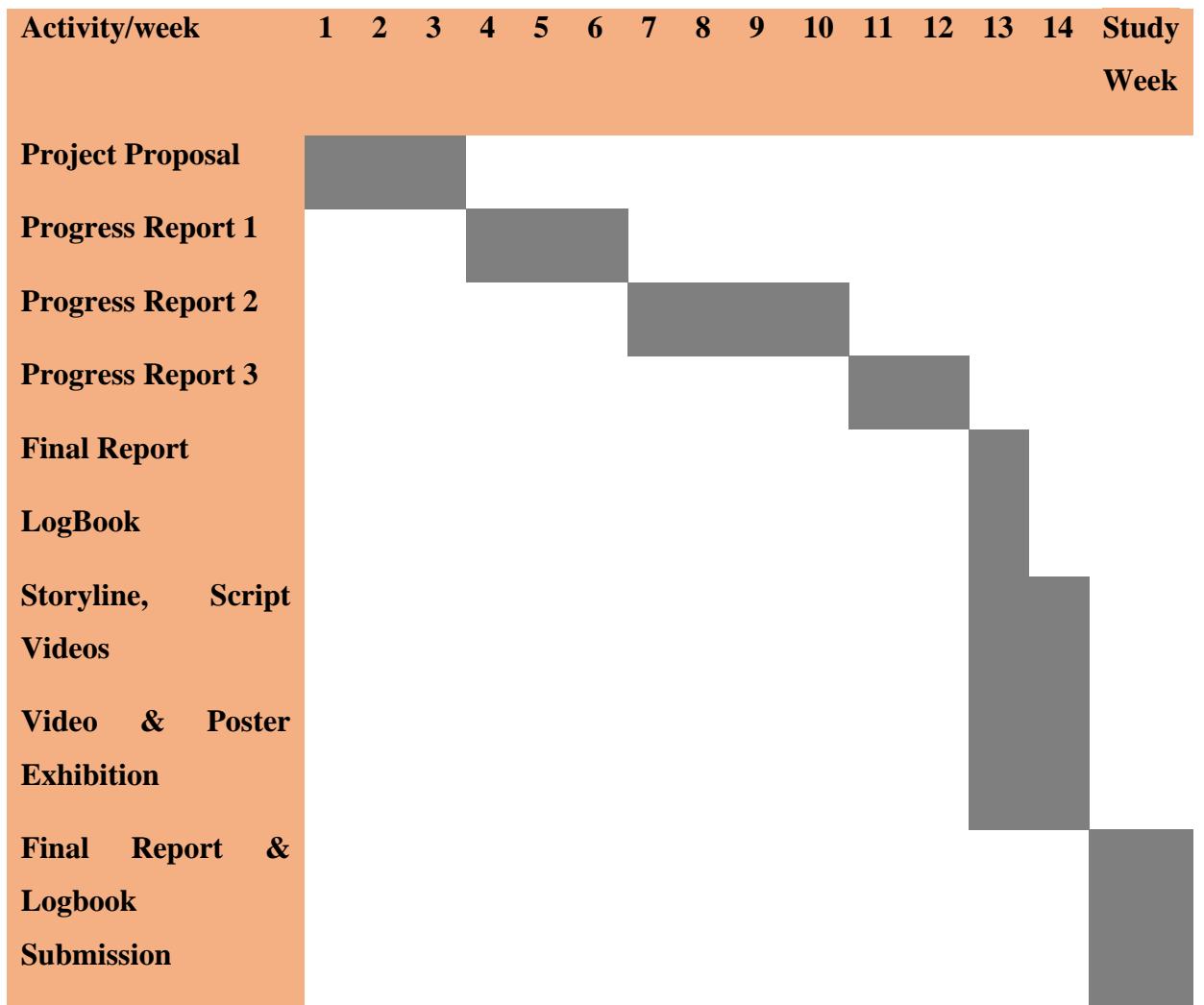
## **1.2 Project Planning / Schedule**

In week 1 and week 2, we will be assigned to the respective supervisors. After we assigned to supervisors, we gather together to separate the task for us to carry out during the following week. Then, we will prepare the project proposal that includes the details of the project like introduction, logical and physical network design to show the network topology, Gantt chart to show the timeline of the project and project distribution where the project manager will distribute the tasks to all the members accordingly. We will submit the finalized proposal by the end of week 2. Besides, we also going to the lab to borrow the equipment needed such as router, switch and servers from the faculty and then we will start to install operating system. In week 2 after the submission of the project proposal to week 5, we will proceed to set up the services needed for this project. There are 5 services that we plan to install during this period. The services include VLAN, IPv6, DNS, DHCP and the service for video. We will prepare the Progress Report 1 that will consists 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 end 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 consist of the setup details of the 10 other services. Then, we will submit the finalized Progress Report 2 that has been approved by the end of week 10. During week 11 to week 13, we will proceed towards completing 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 while the video and poster prepared will be presented during the project demonstration for the purpose of updates for the final exhibition at week 14. The finalized final report and individual logbook will be submitted during study week which is equivalent to week 15.

**Gantt Chart**



### **1.3 Conclusion**

By doing this project, we are able to apply every knowledge that we have learnt that can help us to solve all the problems that occur during the project implementation. Furthermore, we can gain more experience on how to manage and secure a network and it also helps us to enhance our skills on becoming better at networking and security field. The project was able to accomplish in time with the cooperation and toleration of all the team members.

## **CHAPTER 2: PROJECT REQUIREMENT**

### **2.1 Introduction**

The secure network infrastructure will be designed by using the available tools. The network to be developed will consist of three servers with combination of different platforms. Besides, we need to install and configure 30 services and they will be divided among the three servers. There are 18 services for computer networking and 12 services for network security. The servers will be using mainstream operating system to simulate the real environment and superior services for the users. It is very important to ensure the network system operate at the desired performance and the technologies used will be the best possible, depend on the allocated budget.

In this workshop two, we have been provided with the equipment which are three (3) servers, one (1) Cisco router (2 Fast Ethernet), one (1) Cisco manageable switch, 15 meters UTP cable and cables. By using the equipment listed, we are required to design, set up, maintain and monitor a network environment with basic server applications and fundamental services.

### **2.2 Types of Operating System use 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 and security policies that have been set. The operating systems uses in the project are:

1. Window Server 2019
2. Ubuntu 18.04.3 LTS (Linux-Based)
3. Debian 10 GNU (Buster)

## **2.3 Operating system background**

### **2.3.1 Window Server 2019**

Windows Server 2019 was announced on March 20, 2018, and the first Windows Insider preview version was released on the same day. It was released for general availability on October 2, 2018. On October 6, 2018, distribution of Windows version 1809 (build 17763) was paused while Microsoft investigated an issue with user data being deleted during an in-place upgrade. It affected systems where a user profile folder (e.g. Documents, Music or Pictures) had been moved to another location, but data was left in the original location. As Windows Server 2019 is based on the Windows version 1809 codebase, it too was removed from distribution at the time, but was re-released on November 13, 2018. The software product life cycle for Server 2019 was reset in accordance with the new release date.

Windows Server 2019 is built on the strong foundation of Windows Server 2016 and brings numerous innovations on four key themes: Hybrid Cloud, Security, Application Platform, and Hyper-Converged Infrastructure (HCI).

### **2.3.2 Linux Ubuntu 18.04.3**

Ubuntu is a Debian-based Linux operating system for personal computers, tablets and smartphones, where Ubuntu Touch edition is used, and runs network servers, usually with the Ubuntu Server edition, either on physical or virtual servers. Ubuntu server is an open source programming around the world and it can serve up websites, files sharing, and containers. Although Ubuntu itself is primarily a desktop Linux distribution, the brand also includes one of the powerful free server distribution around. Ubuntu Server boast a fast and frequent update cycle and come bundled with a useful 8

and divers set of package groups. The best features a unified package groups. The best feature in Ubuntu is that it features a unified package repository for all its different versions which makes it such a formidable choice. Ubuntu 18.04.3 runs on all major architecture – x86, x86-64, ARM v7, ARM64, POWER8 and IBM System mainframes via LinuxONE.

### **2.3.3 Linux Debian 10**

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 has been developed openly and distributed freely according to the principles of the GNU Project. Because of this, the Free Software Foundation sponsored the project from November 1994 to November 1995. The popular Linux operating system Ubuntu was also released based on Debian. When the sponsorship ended, the Debian Project formed the nonprofit Software in the Public Interest to continue financially supporting development.

## **2.4 Operating system justification**

### **2.4.1 Window Server 2019 R2**

In Workshop II, we decide to use Windows Server 2019. This is because Server Manager has been redesign with an emphasis on easing management of multiple servers. The operating system, like Windows 8, uses the Metro-based user interface unless installed in Server Core mode. Windows store is available in this version of Windows but is not installed by default. Windows PowerShell in this version has over 2300 commandlets. Moreover, unlike its processor, Windows Server 2019 can switch between “Server Core” and “Server with a GUI” installation options without a 9

full reinstallation. Server Core – an option with a command-line interface only – is now the recommended configuration. There is also a third installation option that allows some GUI elements such as MMC and Server Manager to run. But without the normal desktop, shell or default program like File Explorer.

The Active Directory Domain Services installation wizard has been replaced by a new section in Server Manager, and a GUI has been added to the Active Directory Recycle Bin. Multiple password policies can be set in the same domain. Active Directory in Windows Server 2019 is now aware of many changes resulting from virtualization, and virtualized domain controllers can be safely cloned. Active Directory Federation Services is no longer required to be downloaded when installed as a role, and claims which can be used by the Active Directory Federation Services have been introduced into Kerberos token. Windows PowerShell commands used by Active Directory Administrative Center can be viewed in a “PowerShell History Viewer”.

Finally, Window Server 2019 has an IP address management role for discovering, monitoring, auditing and managing the IP address space used on a corporate network. The IPAM is used for the management and monitoring of Domain Name System (DNS) and Dynamic Host Configuration Protocol (DHCP) servers. Both IPv4 and IPv6 are fully supported.

#### **2.4.2 Linux Ubuntu 18.04.3**

We have chosen Ubuntu 18.04.3 because it is the latest Ubuntu which is stable and long-term support provided. It uses Linux 4.4 kernel and system service manager. Another reason is, Ubuntu is supported by the great documentation, a very active community and plenty of online resource and Ubuntu came as a very stable operating system with professional appearance and easy to use.

#### **2.4.3 Linux Debian 10**

The Debian Project is an association of individuals who have made common cause to create a free operating system. An operating system is the set of basic programs and utilities that make your computer run. At the core of an operating system is the kernel.

The kernel is the most fundamental program 10 on the computer and does all the basic housekeeping and lets you start other programs.

## 2.5 Hardware Requirement

In this workshop, we have been provided with the equipment which are three servers, one Cisco 2811 router (2 Fast Ethernet), one Cisco 2960 manageable switch, 15 meters UTP cable, 12 pieces of RJ45 and one set crimping tool. These hardwares are required to complete the workshop. Because the equipments are not new, therefore several preparations have been taken before we start the configuration. For servers, we format the hard drive. Meanwhile for router and switch, we erase the configuration.

## 2.6 Hardware Justification

### 2.6.1 Windows Server

Brand	Dell Optiplex 7010
CPU	Intel Core i7-4790 @ 3.60 GHz
RAM	32GB 1600MHz DDR3 SDRAM
HDD	1TB 7200 rpm HDD
Display adapater	Intel HD Graphics 4000 Dynamic Video Memory Technology 5.0

**Table 2.6.1: Hardware Specification of Windows Server**

### 2.6.2 Ubuntu Server

Brand	Dell Optiplex 7010
CPU	Intel Core i7-4790 @ 3.60 GHz
RAM	32GB 1600MHz DDR3 SDRAM
HDD	1TB 7200 rpm HDD

Display adapter	Intel HD Graphics 4000 Dynamic Video Memory Technology 5.0
-----------------	---

**Table 2.6.2: Hardware Specification of Ubuntu Server**

### **2.6.3 Debian Server**

Brand	Dell Optiplex 7010
CPU	Intel Core i7-4790 @ 3.60 GHz
RAM	32GB 1600MHz DDR3 SDRAM
HDD	1TB 7200 rpm HDD
Display adapter	Intel HD Graphics 4000 Dynamic Video Memory Technology 5.0

**Table 2.6.2: Hardware Specification of Debian Server**

### **2.6.4 Router**

The router provided by university is Cisco 2811. The Cisco 2811 Integrated Services Router is part of the Cisco 2800 Integrated Services Router Series which complements the Integrated Services Router Portfolio. The Cisco 2811 Integrated Services Router provides the following support:

- Wire-speed performance for concurrent services such as security and voice, and advanced services to multiple T1/E1/xDSL WAN rates
- Enhanced investment protection through increased performance and modularity
- Increased density through High-Speed WAN Interface Card Slots (four)
- Enhanced Network Module Slot
- Support for over 90 existing and new modules
- Support for majority of existing AIMs, NMIs, WICs, VWICs, and VICs
- Two Integrated 10/100 Fast Ethernet ports
- Optional Layer 2 switching support with Power over Ethernet (PoE) (as an option)



Security:

- On-board encryption
- Support of up to 1500 VPN tunnels with the AIM-EPII-PLUS Module
- Antivirus defense support through Network Admission Control (NAC)
- Intrusion Prevention as well as stateful Cisco IOS Firewall support and many more essential security features

Voice:

- Analog and digital voice call support
- Optional voice mail support
- Optional support for Cisco CallManager Express (Cisco CME) for local call processing in stand alone business for up to 36 IP Phones
- Optional support for Survivable Remote Site Telephony support for local call processing in small enterprise branch offices for up to 36 IP phones

## **2.6.5 Switch**

Cisco Catalyst 2960 Series Intelligent Ethernet switches are a new family of fixed configuration standalone devices that provide desktop 10/100 Fast Ethernet and 10/100/1000 Gigabit Ethernet connectivity, enabling enhanced LAN services for entry-level enterprise, mid-market, and branch office networks. The Cisco Catalyst 2960 Series offers integrated security, including network admission control (NAC), advanced quality of service (QoS), and resiliency to deliver intelligent services for the network edge.

## **2.6.6 UTP cable**

15 meter of UTP cable is provided to allow us connect all the network peripherals. Some calculation should be made in order to estimate the length of each cable, and also to prevent insufficiency happens.

## **2.6.7 RJ45**

12 pieces of RJ45 is given in this workshop. RJ45 is an 8-pin plug commonly used to connect computers onto Ethernet-based local area networks (LAN).

## **2.6.8 Crimping Tool**

A crimping tool is a device used to affixing a connector to the end of a cable. When crimping the cable, we have to decide which cable type we should use: straight through or crossover. When the cable is used to connect two devices at different network layer e.g. switch to router, we should use straight through cable. When we connect two devices at same network layer, e.g. switch to switch, we should use crossover cable. A cable tester is also provided to ensure the cable is functional.

## **CHAPTER 3 DESIGN**

### **3.1 Introduction**

In this workshop II, we have to define, design, implement and manage network services. Every group need to implement their own network design which is needed to be applied in real device. Stated in the requirements, that need us to design the network that include three different servers, one CISCO router, one CISCO switch and a client host for the design. Our group already designs the networks that have three clients that are from internal and external. We have been supplied with RJ-45, UTP cable, console cable and a set of crimping tools. We also required using different operating system to set the network environment. The NOS we choose to install into HP platform is Window Server 2019 and Ubuntu 18.04.3 Another platform we use is Debian 10.

### **3.2 Security Policy**

#### **3.2.1 General**

##### i. Acceptable Encryption Policy

The purpose of this policy is to provide guidance that limits the use of encryption to those algorithms that have received substantial public review and have been proven to work effectively

##### ii. Password Protection Policy

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords and the frequency of change. IT Support Professional All system-level passwords (e.g., root, enable, admin, application administration accounts, etc.) must be changed every 90 days.

#### **3.2.2 Password Creation**

- i. Password MUST contain alphabet (lower or uppercase) and symbol or numbers.
- ii. Password must at least have minimum of 8 characters.

#### **3.2.3 Password Protection**

- i. Passwords MUST NOT be shared with anyone. All passwords are to be treated as sensitive, confidential group information. Corporate Information

- Security recognizes that legacy applications do not support proxy systems in place.
- ii. Passwords MUST NOT be inserted into email messages. Alliance cases or other forms of electronic communication.
  - iii. Passwords MUST NOT be revealed over the phone to anyone.
  - iv. DO NOT reveal a password on questionnaire or security forms.
  - v. DO NOT hint at the format of a password.
  - vi. DO NOT share group password with anyone, including administrative assistants, secretaries, managers, co-workers while on vacation or with family members.
  - vii. DO NOT write passwords down and store them anywhere in your office. Do not store passwords in a file on a computer system or mobile devices (phone, tablet) without encryption.
  - viii. DO NOT use the “Remember Password” feature of applications.

### **3.2.4 Network Security**

#### **3.2.4.1 Router and Switch Security Policy**

Every router must meet the following configuration standards:

- i. No local user accounts are configured on the router. Routers and switches must use TACACS+ for all user authentication (RADIUS)
- ii. The enable password on the router or switch must be kept in secure encrypted form. The router or switch must have the enable password set to the current production router/switch password from the device’s support organization
- iii. The following service must be configured:
  - Password-encryption
- iv. All routing updates shall be done using secure routing updates
- vi. Access control list must be used to limit source and type of traffic that can terminate on the device itself
- vii. Access control list for transiting the device are to be added as business needs arise

- viii. Each router and switch must have the following statement presented for all forms whether remote or local: "UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED. You must have explicit permission to access or configure this device. All activities performed on this device may be logged, and violations of this policy may result in disciplinary action and may be reported to law enforcement. There is no right to privacy on this device. Use of this system shall constitute consent to monitoring."
- ix. SSH may never be used across any network to manage a router, unless there is a secure tunnel protecting the entire communication path. SSH version 2 is the preferred management protocol
- x. Dynamic routing protocols must use authentication in routing updates sent to neighbours. Password hashing for the authentication string must be enabled when supported
- xi. The corporate router configuration standard will define the category of sensitive routing and switching devices, require additional services or configuration on sensitive devices including:
  - IP access list accounting
  - Device logging
  - Incoming packets at the router sourced with invalid addresses, such as the address that could be used to spoof network traffic shall be dropped.
  - Router console and modem access must be retrieved by additional security controls.

### **3.2.5 Application Security**

#### **3.2.5.1 IPv6 Web Policy**

IPv6 can run end-to-end encryption. While this technology was retrofitted into IPv4, it remains an optional extra that isn't universally used. The encryption and integrity-checking used in current VPNs is a standard component in IPv6, available for all connections and supported by all

compatible devices and systems. Widespread adoption of IPv6 will therefore make man-in-the-middle attacks significantly more difficult.

IPv6 also supports more-secure name resolution. The Secure Neighbour Discovery (SEND) protocol is capable of enabling cryptographic confirmation that a host is who it claims to be at connection time. This renders Address Resolution Protocol (ARP) poisoning and other naming-based attacks more difficult. And while not a replacement for application- or service-layer verification, it still offers an improved level of trust in connections. With IPv4 it's fairly easy for an attacker to redirect traffic between two legitimate hosts and manipulate the conversation or at least observe it. IPv6 makes this very hard.

### **3.2.5.2    Remote Login using SSH Policy**

Login remote by using SSH is a good way. The secure shell protocol uses modern cryptography methods to provide privacy and confidentiality, even over an unsecured, unsafe network, such as the Internet. However, its very availability also makes it an appealing target for attackers, so we should consider hardening its standard setup to provide more resilient, difficult-to-break-into connections. There are several methods to hardening the standard setup such extra protections, starting with simple configuration changes, then limiting access with PAM and finishing with restricted, public key certificates for password less restricted logins.

PAMs can be used for four security concerns. That are an account limitation (what the users are allowed to do), authorization (how the users identify themselves), passwords and sessions. PAM checks can be marked optional (may succeed or fail), required (must succeed), requisite (must succeed, and if it doesn't, stop immediately without trying any more checks) and sufficient (if it succeeds, don't run any more checks), so the policies can be varied.

### **3.2.5.3 Samba Policy**

There are three levels at which security principles must be observed in order to render a site at least moderately secure. They are the perimeter firewall, the configuration of the host server that is running Samba and Samba itself. Samba permits a most flexible approach to network security. As far as possible Samba implements the latest protocols to permit more secure MS Windows file and print operations. Samba can be secured from connections that originate from outside the local network. This can be done using host-based protection, using Samba's implementation of a technology known as "tcpwrappers," or it may be done by using interface-based exclusion, so samba will bind only to specifically permitted interfaces. It is also possible to set specific share- or resource-based exclusions, for example, on the [IPC\$] auto share. The [IPC\$] share is used for browsing purposes as well as to establish TCP/IP connections. Another method by which Samba may be secured is by setting Access Control Entries (ACEs) in an Access Control List (ACL) on the shares themselves.

### **3.2.5.4 Hardening Services Policy**

Hardening is service that provide in every server that we have. So, our policy for hardening services is every server must have this requirement

#### **3.2.5.4.1 Access security**

- i. There a log of all access to the server (visitor book, card swipe, entry code records and video surveillance)
- ii. The server access governed by firewall appliances and/or software

#### **3.2.5.4.2 File system permissions**

- i. For Linux Servers, permissions are on key security files such as /etc/passwd or /etc/shadow set in accordance with best practice in harden.
- ii. Sudo being used, and are only root when members are allowed to use it.

- iii. For Windows Server, the key must executable, DLLs and drivers protected in the System32 and SysWOW64.

#### **3.2.5.4.3 User accounts and passwords**

- i. Default user account is the local Administrator will be protected via a password, a number of simple steps can be taken to multiply up the security defences in this area, simply by disabling the Guest account, and then renaming both the Guest and Administrator accounts.
- ii. The password policy set with ageing, complexity, length, retry, lockout and reuse settings in line with the best practice guidelines.

#### **3.2.5.4.4 Software and application image/ patching and updates**

- i. Secure Build Standard package and application must have included in this service.
- ii. A process to check latest versions and patches have been tested and applied.
- iii. Automated updates to packages disabled in favour of scheduled, planned updates deployed in conjunction with a Change Management process.

#### **3.2.5.4.5 LAN services policy**

Usually, when we have to do network segmentation using VLANs, we create the necessary networks either manually or automatically using protocols like Cisco VTP (VLAN Trunking Protocol). After that, we assign each one of the network devices to the different VLANs defined. This means that if we move tomorrow and change our laptop of network connection point, we will have to change the new network connection point, so it belongs to the original VLAN we had.

One solution to this problem is the use of the VTP protocol together with the Cisco VMPS (VLAN Management Policy Server) service, which provides a first approximation to a

solution of network access control such as the ones offered by manufacturers today. Among other features, VMPS allows to dynamically associate devices to VLANs based on MAC address (with the security issues this involves). This way, we can connect our laptop to any network point of the office and it will always belong to the same correct VLAN.

#### **3.2.5.4.6 Proxy server security**

Proxy server need to use Network Address Translation (NAT) to translate private internal IP addresses to one routable IP address assigned to an Internet-connected network adapter. Because Proxy Server directly connects to the Internet, Internet-based intruders see an opportunity to probe, hack, and attack. For our group, we are using proxy server to deny a few websites when we try to connect to the internet. The websites that we have blocked is [www.instagram.com](http://www.instagram.com).

#### **3.2.5.4.7 ACL policy**

An ACL policy is a set of rules, or permissions, that specify the conditions necessary to perform an operation on a protected object. An ACL policy identifies the operations permitted on a protected object and lists the identities such as users and groups that can protect object space and ACL policies are defined in the master authorization database. Each ACL policy has a unique name or label. Each ACL policy can be applied to one or more objects. An ACL policy consists of one or more entries that include user and group designations and their specific permissions.

#### **3.2.5.4.8 Hardening server policy**

All internal servers deployed at must be owned by an operational group that is responsible for system administration. Approved server configuration guides must be established and maintained by each operational group. Operational groups

should monitor configuration compliance and implement an exception policy tailored to their environment. Each operational group must establish a process for changing the configuration guides.

#### **3.2.5.4.9 Router policy**

- i. Every router must meet the following configuration standards:
- ii. No local user accounts are configured on the router. Only administrator can access to the router.
- iii. The enable secret password on the router must be kept in a secure encrypted form. The router must have the enable secret password to set to the current production router password from the Network Operations organization.
- iv. Disallow the following:
  - Incoming packets at the router sourced with invalid addresses such as RFC1918
  - TCP and UDP “small services”
  - All source routing d. All web services running on router
- v. Use corporate standardized SNMP community strings. Community strings “public” and “private” should never be used.
- vi. Every router should save system logging information to a local RAM buffer in addition to a secured “syslog” server.

#### **3.2.5.4.10 Physical Policy**

Physical security can often be overlooked by IT professionals. These policies discuss security measures that can be implemented using physical controls such as door locks, controlled room access, and procedures for adding or removing equipment from a machine room or office. Therefore, it controls:

- i. Computer
- ii. Media
- iii. Physical Access

### 3.3 Physical Design

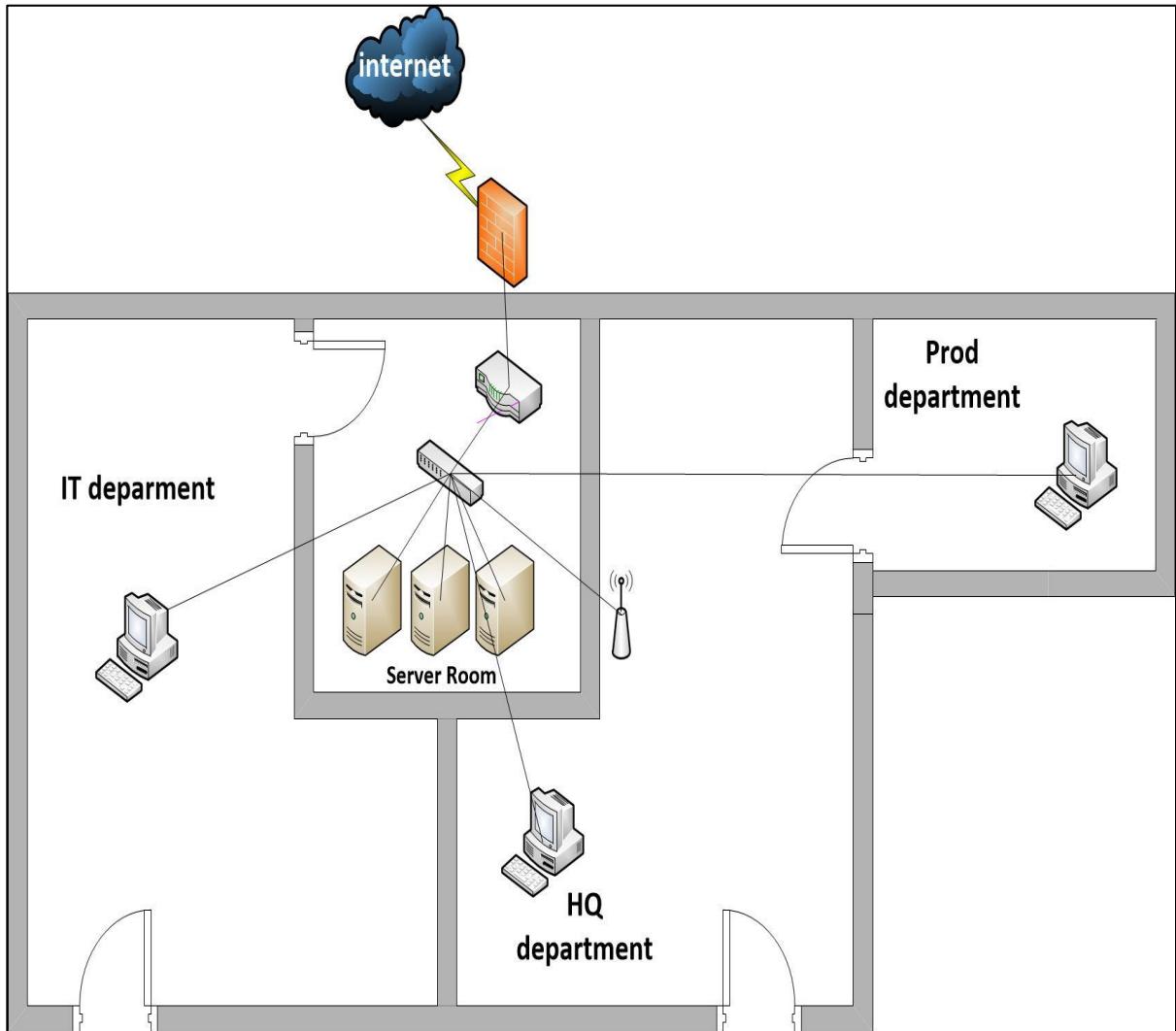


Figure 3.3.1: Physical Design

### 3.4 Logical Design

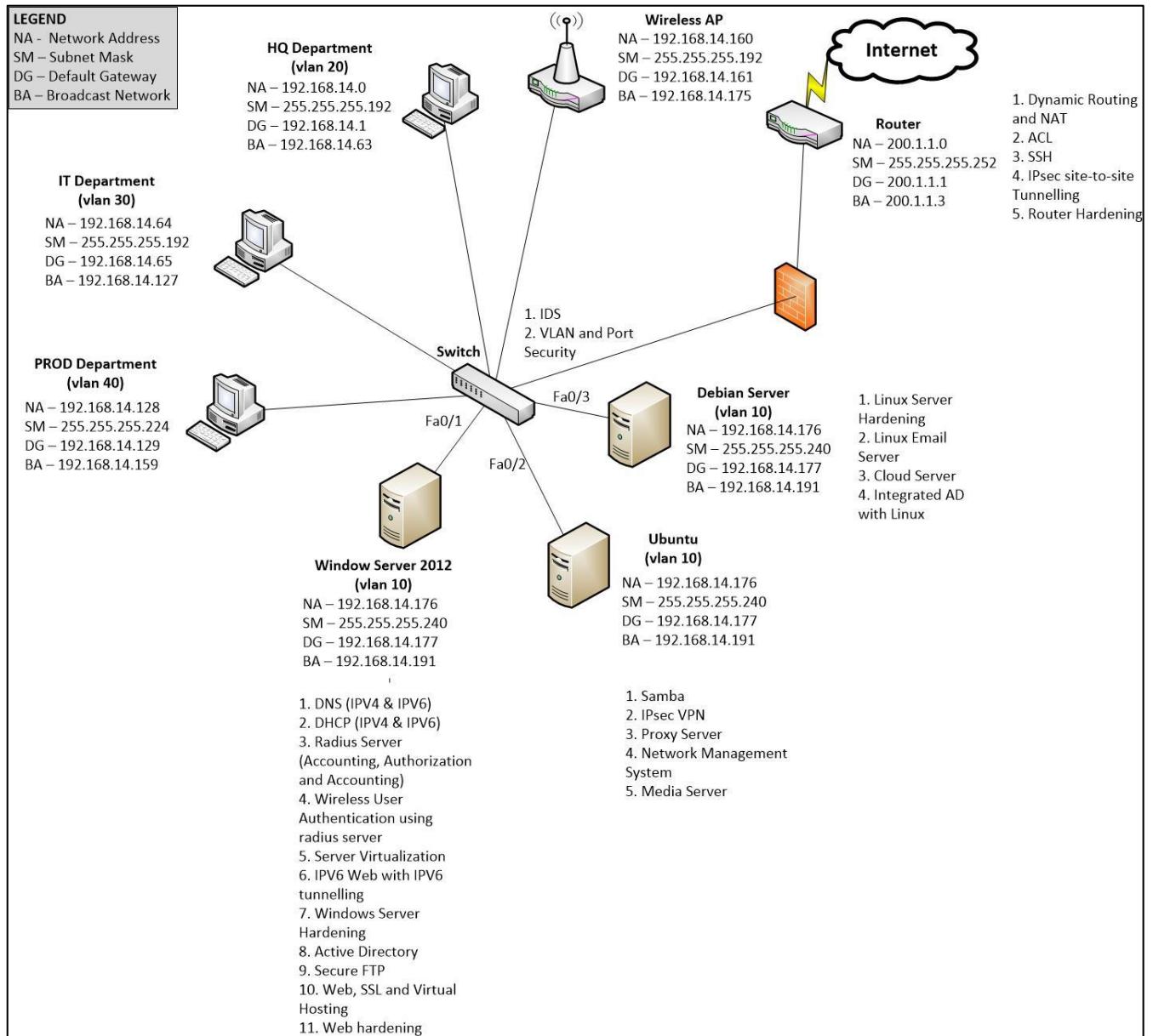


Figure 3.4.1: Logical Design

### 3.5 VLAN and VLSM Addressing

Subnet	Network address	CIDR	Subnet mask	Ranged	Broadcast address
Vlan 20	192.168.14.0	/26	255.255.255.192	192.168.14.1 - 192.168.14.62	192.168.14.63
Vlan 20	192.168.14.64	/26	255.255.255.192	192.168.14.65 - 192.168.14.126	192.168.14.127
Vlan 40	192.168.14.128	/27	255.255.255.224	192.168.14.129 - 192.168.14.158	192.168.14.159
Vlan 30	192.168.14.160	/28	255.255.255.240	192.168.14.161 - 192.168.14.174	192.168.14.175
Vlan 10	192.168.14.176	/28	255.255.255.240	192.168.144.177 - 192.168.1.190	192.168.14.191

Table 3: VLAN and VLSM Addressing

### 3.6 Conclusion

Designing a network is an integral part of creating a network. There is no idea how to start implementing the network without network design. There are few primary factors to consider when implementing network design that include, network complexity preparation must be consistent with network administrator, reliability, standards, and maintenance factor. All these considerations will ensure that the network can be enforced, expandable and easy to sustain for potential deployment. Upon considering these factors, we had implemented the network as physically built and continued to the next implementation stage that is preparing network services implementation.

## **CHAPTER 4: SERVICES**

### **4.1 INTRODUCTION**

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

### **4.2 TYPE OF SOFTWARE**

#### **4.2.1 LIST OF OPERATING SYSTEMS**

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

#### **4.2.2 LIST OF SERVICES**

1. Cloud Server
2. DHCP (IPv4 & IPv6)
3. Dynamic Routing and NAT
4. IPsec site-to-site tunnelling
5. Access Control List (ACL)
6. DNS (IPv4 & IPv6)
7. Server Virtualization
8. Active Directory
9. Wireless user authentication using Radius server
10. Linux Email Server
11. Web, SSL & Virtual Hosting
12. IPv6 Web with IPv6 Tunnelling
13. Network Management System
14. Proxy server
15. Secure FTP
16. AAA (Authentication, Authorization and Accounting) using Radius.
17. VLAN and Port Security
18. Web Hardening

19. IDS with port mirror
20. Samba and Samba security services
21. Linux Server Hardening
22. IPsec VPN server for remote employees
23. User authentication by integrating AD with Linux.
24. Windows Server Hardening
25. Remote login using SSH
26. Media Server
27. Router Hardening
28. Security Policy
29. Inter VLAN
30. VLSM addressing

## **4.3 BRIEF OVERVIEW OF SERVICES**

### **4.3.1 Windows Server 2012**

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

Following the fulfillment of this process, PowerShell scripts containing duplicates of command utilized in the process can help with the computerization of additional domain controllers, allowing for large-scale Active Directory deployments.

### 4.3.2 Ubuntu Server

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

`sudo snap install nextcloud`). Snaps can also be easily updated with a single command (`sudo snap refresh`), so there are fewer administrative tasks.

### 4.3.3 Debian Server

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

#### **4.3.4 Cloud Server**

Cloud server is known as a virtual server that can be accessed remotely which contain in a cloud computing environment to build, hosted and delivered via the Internet. Cloud server can function as independent as it has all the software that are required.

#### **4.3.5 DHCP (IPv4 & IPv6)**

DHCP is a network protocol that dynamically assigns an IP address. Computers that are connected to the DHCP server are able to request IP addresses automatically from the Internet Service Provider (ISP). It will simplifies the work for the network administrator as they do not have to manually assign IP addresses to all network devices.

#### **4.3.6 Dynamic Routing and NAT**

Dynamic routing is also known as adaptive routing that can enable the router to select the best route to forward data and put into the routing table. Dynamic routing will allows as many routes as possible to remain valid in response to the change. Network Address Translation (NAT) will assign a public address for the computer that consists inside the private network. It helps to make sure the security of outgoing on ingoing request.

#### **4.3.7 IPsec site-to-site tunnelling**

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 Access Control List (ACL)**

ACL is a set of rules used for packet filtering, controlling the network traffic that can permitted or denied any packets in or out of the network. It can also specifies which users or system process are granted access to object as well as what operations are allowed on given objects.

#### **4.3.9 DNS (IPv4 & IPv6)**

The Domain Name System (DNS) act as a phonebook of the Internet. DNS will translates domain names to IP addresses so browsers can load Internet resources. It will ease human's jobs as it is easier to remember the domain name rather than the IP addresses.

#### **4.3.10 Server Virtualization**

Server virtualization is the masking of server resources, including the number and identity of individual physical servers, processors, and operating systems, from server users. The server administrator uses a software application to divide one physical server into multiple isolated virtual environments. The virtual environments are sometimes called virtual private servers, but they are also known as guests, instances, containers or emulations.

#### **4.3.11 Active Directory**

Active Directory is a directory service that consists of authentication and authorization mechanism for all users and computers by enforcing security policies. it also uses to manage computer and other devices on the network.

#### **4.3.12 Wireless user authentication using Radius server**

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

#### **4.3.13 Linux Email Server**

Email server is capable for sending and receiving email across a network. Linux Email Server use Simple Mail Transport Protocol (SMTP) protocol and other related email protocol such as Post Office Protocol and Internet Message Access Protocol (IMAP).

#### **4.3.14 Web, SSL & Virtual Hosting**

Web is also known as World Wide Web which consists of web pages that can be accessed by using a web browser. Web pages are usually in Hypertext Markup Language (HTML). The Web uses HTTP protocol to allow transmission of data and sharing of information.

Secure Sockets Layer (SSL) is where a secure connection is being established between the web server and the user's web browser so that all the information transmitted through the network is secure. SSL Certificate also provides a pair of public and private key to establish an encrypted connection.

Virtual Hosting is a method where it can host multiple domain names on a single server where one server can share its resources, such as memory and processor cycles without requiring all services provided to use the same host name.

#### **4.3.15 IPv6 Web with IPv6 Tunnelling**

Internet Protocol version 6 (IPv6) is the most recent version of the IP which is a set of specifications from the Internet Engineering Task Force (IETF) that's essentially an upgrade of IP version 4 (IPv4). It is a communication protocol that provides an identification and location system for the computers on the networks and routers traffic across the Internet.

#### **4.3.16 Network Management System**

Network Management System (NMS) is a set of applications that allows administrators to manage such as monitor and maintain the individual components of a network within larger management framework. Moreover, NMS can identify, configure, monitor, update and troubleshoot network devices.

#### **4.3.17 Proxy server**

Proxy server is also known as application-level gateway where the computer will act as a gateway between local network and internet. Proxy server is secure because it will block direct access between two networks, so it will be more difficult for hacker to get internal addresses and details of a private network.

#### **4.3.18 Secure FTP**

Secure FTP is also known as SSH File Transfer Protocol as it uses SSH protocol. It refers to two different technologies that can encrypt both authentication information and data files in transit. Secure FTP will encrypt the file transfer process from start to finish with limited threat exposure for the user and proven secure method to transmit files.

#### **4.3.19 AAA (Authentication, Authorization and Accounting) using Radius.**

Authentication is where the system can identify the information from each user, such as username and password. The system will check the credentials and if the credentials match the user will gain access to the network. The authentication will fail if the credentials do not match and the user cannot access the network.

Authorization refers to the process of adding or denying individual user access to a computer network and its resources. Users may have different authorization levels so there will be a limit for them to access to the network and resources.

Accounting is where it will keep the record and will track every user activity while they are on the network. The information gathered can include the amount of system time used, the amount of data sent, or the quantity of data received by the user during a session.

#### **4.3.20 VLAN and Port Security**

VLAN is a virtual LAN that consists of a subnetwork which is a group of collections of devices on separate physical local area. Port security is to prevent any unknown devices from sending packets to secure the devices. By using port security, we can limit the number of MAC address on a given port.

#### **4.3.21 Web Hardening**

Web hardening is done by adding different layers of protection to reduce any attacks. Hardening often involves manual measures of adding code or making changes to the configuration. By doing a virtual hardening, it means that it allows Web Application Firewall (WAF) or any security plugin to automatically harden the website. Moreover, it also protects the web server and database from any threats.

#### **4.3.22 IDS with port mirror**

IDS is known as Intrusion Detection System, it is a device that will monitors and detect any malicious activity or policy violations. Any detection will be reported to administrator or collected using a security information and event management system. Port mirror is where the act of sending a copy of network packets seen on one switch port to another switchport.

#### **4.3.23 Samba and Samba security services**

Samba is a free software that is a re-implementation of the SMB networking protocol. Samba security modes consists of two types, which are share-level and userlevel. The share-level, it can only use in one way and the user-level can use in one of four different ways.

#### **4.3.24 Linux Server Hardening**

Linux Server Hardening is done for enhancing the security level of the system for Linux. It includes the principle of least privilege, segmentation and reduction.

#### **4.3.25 IPsec VPN server for remote employees**

IPsec VPNs is a method that provide a secure remote access from a company managed laptops. It offers more secure support for common remote user authentication methods like passwords and tokens.

#### **4.3.26 User authentication by integrating AD with Linux.**

Consolidate user accounts and groups into Active Directory and enforce separation of administrative duties. It will also eliminate multiple identities and ensure a “one user, one identity” framework that strengthens security

#### **4.3.27 Windows Server Hardening**

Server Hardening is done to secure the server so that it will be in much more secure server operating environment by reducing the risk of attackers compromising the critical system and data. It also identifies and remediating security vulnerabilities.

#### **4.3.28 Remote login using SSH**

SSH is a protocol which allows you to connect securely to a remote computer or a server by using command line interface (CLI). When a secure SSH connection is occur, a shell session will be started, and user can manipulate the server by typing commands within the client on the local computer.

#### **4.3.29 Media Server**

Media Server is a hardware or software that stores and shares media. A media server can be any device having network access and adequate bandwidth for sharing and saving media.

#### **4.3.30 Router Hardening**

Router Hardening is an act to secure the router from being attack. It can the make the router to be difficult to penetrate and give a maximum security by locking it down.

#### **4.3.31 Security Policy**

Security policy is a written documents that states how an organization can protect the organization's physical and information technology from threats and how to handle situations when they do occur.

#### **4.3.32 Inter VLAN**

Inter VLAN is where a network traffic is being forwarded from one VLAN to another VLAN using a router. The router interfaces can be connected to separate VLANs. The devices that are connected to the VLANs can communicate with each other via the router.

#### **4.3.33 VLSM addressing**

VLSM addressing is where an IP address space is divided into a hierarchy of subnets of different sizes so that subnets with very different host counts are created without wasting large numbers of addresses.

## CHAPTER 5: INSTALLATION AND CONFIGURATION

### 5.1 INTRODUCTION

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

### 5.2 SERVICES AND CORRESPONDING PERSON IN CHARGE

BITC		
NO	NAME	SERVICES
1	Mohd Farid Wajdi bin Mohd Marzuki	<input type="checkbox"/> <b>Server virtualization</b> <input type="checkbox"/> Active Directory <input type="checkbox"/> Wireless user authentication using Radius Server
2	Mohd Fakhri Anas bin Abdullah	<input type="checkbox"/> <b>Linux Email Server</b> <input type="checkbox"/> Web, SSL & Virtual Hosting <input type="checkbox"/> IPv6 Web with IPv6 Tunnelling
3	Siti Norashikin binti Hassan	<input type="checkbox"/> <b>IPSec site to site tunneling</b>

		<input type="checkbox"/> Access Control List (ACL) <input type="checkbox"/> DNS (IPv4 & IPv6)
4	Nur Dayana Munirah binti Zainal Abidin	<input type="checkbox"/> <b>Cloud Server</b> <input type="checkbox"/> DHCP (IPv4 & IPv6) <input type="checkbox"/> Dynamic Routing & NAT
5	Margaret Moses	<input type="checkbox"/> <b>Network Management System</b> <input type="checkbox"/> Proxy Server <input type="checkbox"/> Secure FTP

<b>BITZ</b>		
<b>NO</b>	<b>NAME</b>	<b>SERVICES</b>
1	‘Ukasyah bin Mohd Azlan	<input type="checkbox"/> <b>IDS</b> <input type="checkbox"/> Samba <input type="checkbox"/> Linux server hardening
2	Nurhaseena binti Mohamed Salleh	<input type="checkbox"/> <b>AAA</b> <input type="checkbox"/> VLAN & Port Security <input type="checkbox"/> Web Hardening
3	Wan Nurin Jazmina binti Wan Omar	<input type="checkbox"/> <b>IPSec Vpn Server for remote employees</b> <input type="checkbox"/> User authentication

		<input type="checkbox"/> Windows server hardening
4	Nurul Afiqah binti Mat Ripin	<input type="checkbox"/> <b>Remote login using SSH</b> <input type="checkbox"/> Media server. <input type="checkbox"/> Router hardening.

## 5.3 SERVICE INSTALLATION AND CONFIGURATION

### 5.3.1 Cloud Server

**STEP 1:** Install apache and MariaDB server.

```
147 apt install apache2 php7.0 libapache2-mod-php7.0
148 apache2 -v
149 php -v
150 openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/group14.key -out /etc/ssl/certs/group14.pem

364 apt-get install mariadb-server -y
365 mysql -v
366 systemctl start apache2
```

Figure 5. 1: Apache and MariaDB installation

**STEP 2:** Start Apache and MariaDB service and enable them to start on boot time.

```
root@group14:/home/group14# systemctl start apache2
root@group14:/home/group14# systemctl enable apache2
Synchronizing state of apache2.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable apache2
root@group14:/home/group14# systemctl start mariadb
```

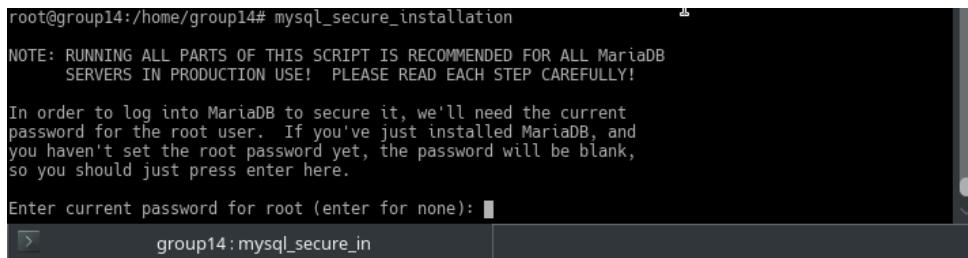
Figure 5. 2: Enable Apache and MariaDB

**STEP 3:** Install PHP and other required modules to system by installing a recent PHP 7.2 version from Ondrej Repository.

```
group14:bash — Konsole
File Edit View Bookmarks Settings Help
group14@group14:~$ su
Password:
su: Authentication failure
group14@group14:~$ su
Password:
root@group14:/home/group14# php -v
PHP 7.2.25-1+deb10u1 (20191128) 32-bit
Copyright (c) 1999-2018 Zend Technologies
    with Zend OPcache v7.2.25-1+deb10u1, Copyright (c) 1999-2018, by Zend Technologies
root@group14:/home/group14# apt-get install libapache2-mod-php php7.2 php7.2-xml php7.2-curl php7.2-gd php7.2-cgi php7.2-zip php7.2-mysql php7.2-mbstring wget unzip -y
Reading package lists... Done
Building dependency tree
Reading status information... Done
unzip is already the newest version (6.0-21+deb9u2).
unzip was previously uninstalled.
wget is already the newest version (1.19-5+deb9u3).
php7.2 is already the newest version (7.2.25-1+deb10u1).
php7.2-cgi is already the newest version (7.2.25-1+deb10u1).
php7.2-gd is already the newest version (7.2.25-1+deb10u1).
php7.2-xml is already the newest version (7.2.25-1+deb10u1).
The following packages were automatically installed and are no longer required:
courier-authdaemon courier-authlib courier-authlib-userdb courier-base expect liblcurvier-unicodel libtcl8.6 libtk8.6 tcl-expect tcl8.6 tk8.6
Use "apt autoremove" to remove them.
The following additional packages will be installed:
libapache2-mod-php7.3 libpcre2-8-0 libzip4 php7.3-common php7.3-json php7.3-opcache php7.3-readline
Suggested packages:
php-pear
The following NEW packages will be installed:
libapache2-mod-php libapache2-mod-php7.3 php7.2-cgi php7.2-curl php7.2-gd php7.2-mbstring php7.2-mysql php7.2-xml php7.2-zip php7.3-cli php7.3-common php7.3-json php7.3-opcache
php7.3-readline
The following packages will be upgraded:
libpcre2-8-0 libzip4
2 upgraded, 14 newly installed, 0 to remove and 18 not upgraded.
Need to get 5,874 kB of archives.
After this operation, 29.4 MB of additional disk space will be used.
Get:1 https://packages.sury.org/php stretch/main amd64 php7.3-common amd64 7.3.12-1+0-20191128.49+debian9-1.gbp24559b [563 kB]
Get:2 https://packages.sury.org/php stretch/main amd64 php7.3-json amd64 7.3.12-1+0-20191128.49+debian9-1.gbp24559b [18.2 kB]
Get:3 https://packages.sury.org/php stretch/main amd64 php7.3-opcache amd64 7.3.12-1+0-20191128.49+debian9-1.gbp24559b [178 kB]
Get:4 https://packages.sury.org/php stretch/main amd64 php7.3-readline amd64 7.3.12-1+0-20191128.49+debian9-1.gbp24559b [11.8 kB]
Get:5 https://packages.sury.org/php stretch/main amd64 libcurl4-openssl4 amd64 7.3.12-1+0-20190707.45+debian9-1.gbp24559b [33.1 kB]
Get:6 https://packages.sury.org/php stretch/main amd64 libpcre2-8-0 amd64 7.3.12-1+0-20191128.49+debian9-1.gbp24559b [1,374 kB]
Get:7 https://packages.sury.org/php stretch/main amd64 libapache2-mod-php7.3 amd64 7.3.12-1+0-20191128.49+debian9-1.gbp24559b [1,319 kB]
Get:8 https://packages.sury.org/php stretch/main amd64 libapache2-mod-php all 7.3.12-1+0-20191118.18+debian9-1.gbp66bed [6,294 B]
Get:9 https://packages.sury.org/php stretch/main amd64 libzip4 amd64 1.5.1-4+0-20190318173229.9+stretch-1.gbp333132 [51.1 kB]
Get:10 https://packages.sury.org/php stretch/main amd64 php7.2-cgi amd64 7.2.25-1+0-20191128.32+debian9-1.gbp108445 [1,354 kB]
```

Figure 5. 3: Installation PHP

**STEP 4:** Secure the MariaDB installation by adding password.



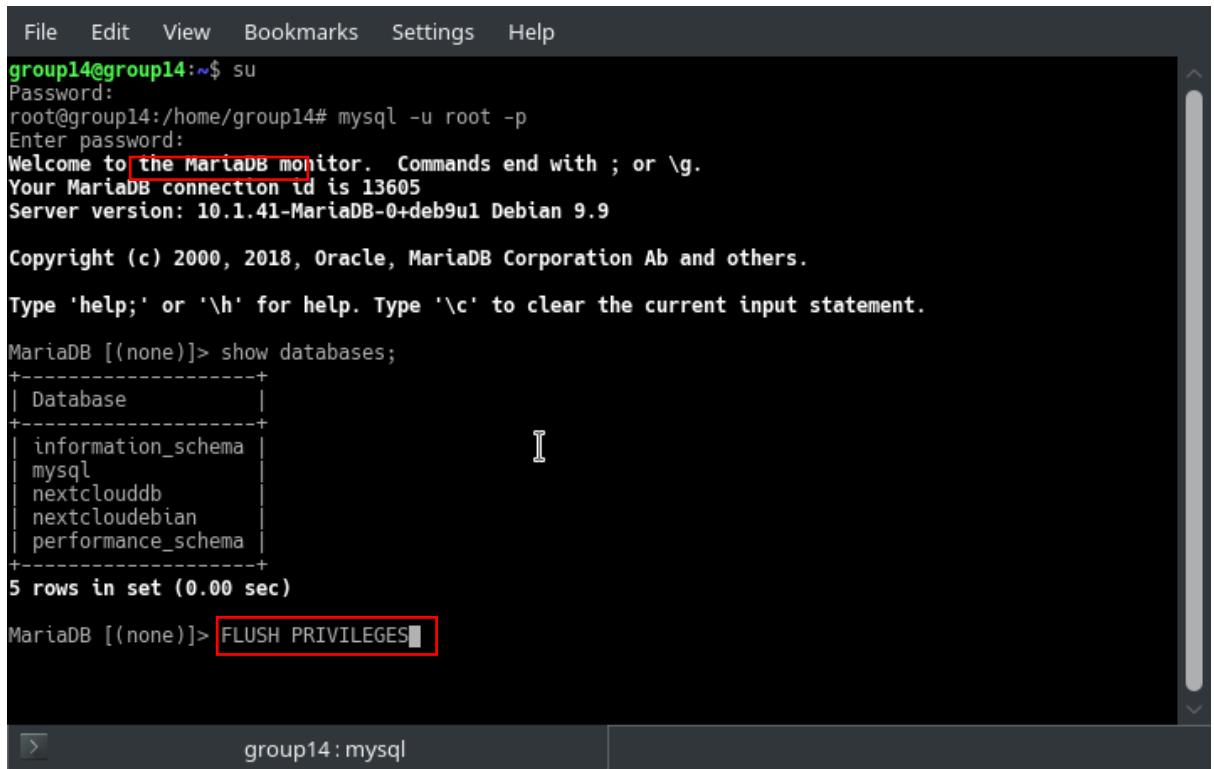
```
root@group14:/home/group14# mysql_secure_installation
NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MariaDB
      SERVERS IN PRODUCTION USE! PLEASE READ EACH STEP CAREFULLY!
In order to log into MariaDB to secure it, we'll need the current
password for the root user. If you've just installed MariaDB, and
you haven't set the root password yet, the password will be blank,
so you should just press enter here.

Enter current password for root (enter for none):
```

Figure 5. 4: Add password

**STEP 5:** Log in to MariaDB console and create database Nextcloud and admin user.

**STEP 6:** Run the FLUSH PRIVILEGES command so that the privileges table will be reloaded by MariaDB.



```
File Edit View Bookmarks Settings Help
group14@group14:~$ su
Password:
root@group14:/home/group14# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 13605
Server version: 10.1.41-MariaDB-0+deb9u1 Debian 9.9

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> show databases;
+-----+
| Database |
+-----+
| information_schema |
| mysql |
| nextclouddb |
| nextcloudebian |
| performance_schema |
+-----+
5 rows in set (0.00 sec)

MariaDB [(none)]> FLUSH PRIVILEGES;
```

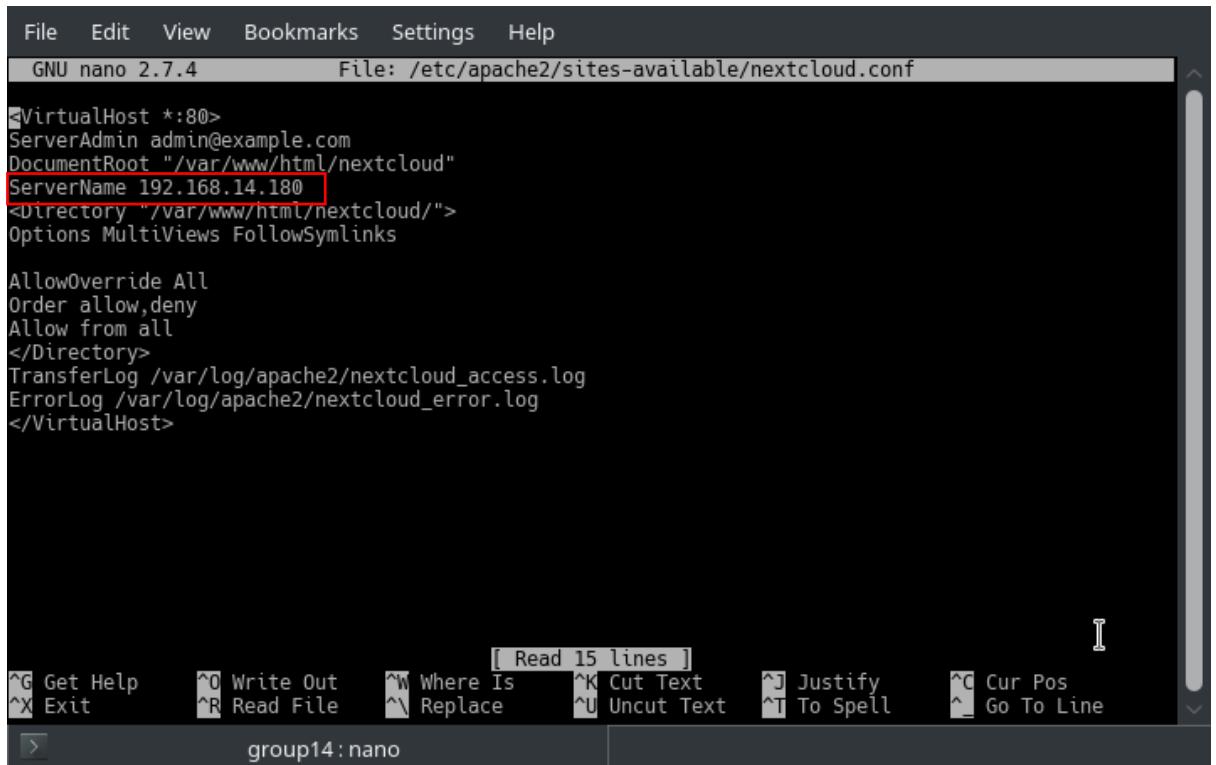
Figure 5. 5: Flush Priveleges

**STEP 7:** Install the Nextcloud and create a directory for the Nextcloud installation and a data directory where Nextcloud will store the uploaded files.

```
root@group14:/home/group14# mkdir /var/www/nextcloud/chown www-data:www-data /var/www/nextcloud chmod 750 var/www/nextcloud
group14:bash
```

*Figure 5. 6: Install and configure Nextcloud*

**STEP 8:** Next, create an apache virtual host file for NextCloud



```
File Edit View Bookmarks Settings Help
GNU nano 2.7.4 File: /etc/apache2/sites-available/nextcloud.conf

<VirtualHost *:80>
ServerAdmin admin@example.com
DocumentRoot "/var/www/html/nextcloud"
ServerName 192.168.14.180
<Directory "/var/www/html/nextcloud/">
Options MultiViews FollowSymlinks

AllowOverride All
Order allow,deny
Allow from all
</Directory>
TransferLog /var/log/apache2/nextcloud_access.log
ErrorLog /var/log/apache2/nextcloud_error.log
</VirtualHost>

[ Read 15 lines ]
^G Get Help      ^O Write Out     ^W Where Is      ^K Cut Text      ^J Justify      ^C Cur Pos
^X Exit          ^R Read File     ^\ Replace       ^U Uncut Text    ^T To Spell     ^_ Go To Line
group14:nano
```

*Figure 5. 7: VH Cloudserver*

**STEP 9:** Finally, restart apache and open web browser and navigate to URL

```
root@group14:/home/group14# systemctl restart apache2
group14:bash
```

*Figure 5. 8: Navigate URL*

### 5.3.2 Dynamic Host Configuration Protocol (DHCP) IPV4.

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

**STEP 2:** For Select installation Type just choose Role-based or feature-based installation.

**STEP 3:** For Server Role, select the DHCP role and click Next button and wait until the installation complete.

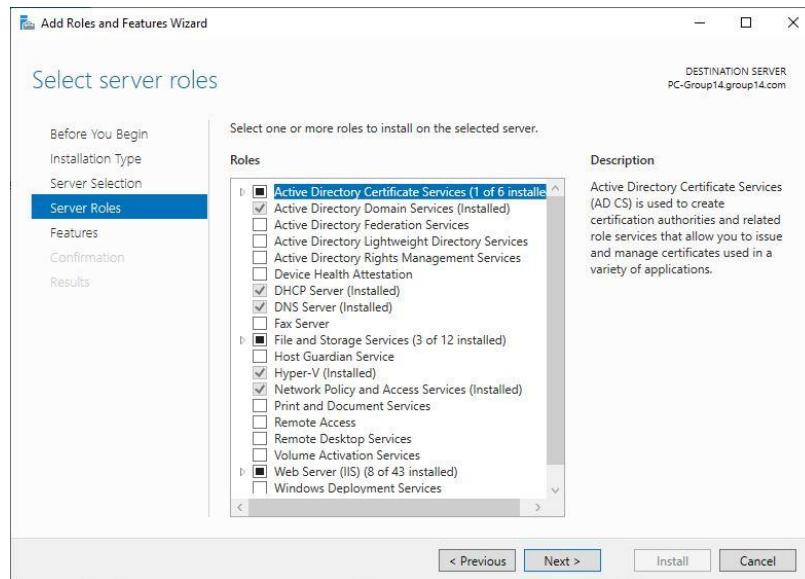


Figure 5.9 Server Roles

**STEP 4:** After finishing the installation, open the DHCP configuration page.

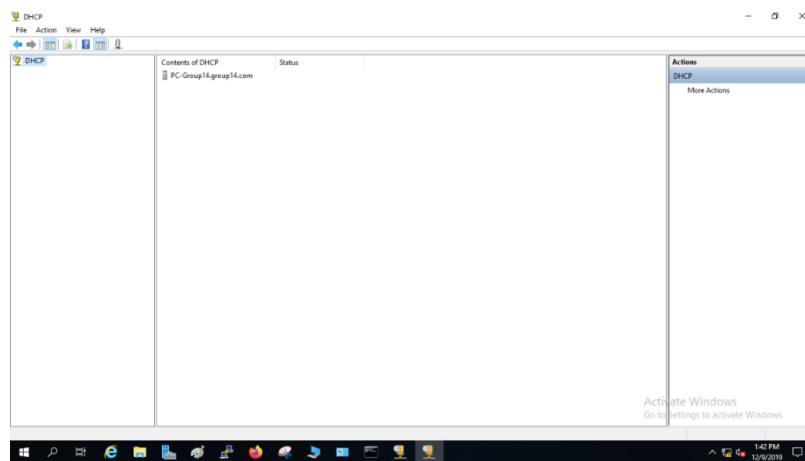


Figure 5.10 DHCP page

**STEP 5:** Just click at the IPV4 and add new scope.

**STEP 6:** In the new scope, write the Scope Name “ws14” and description as below. After that, click the Next button.

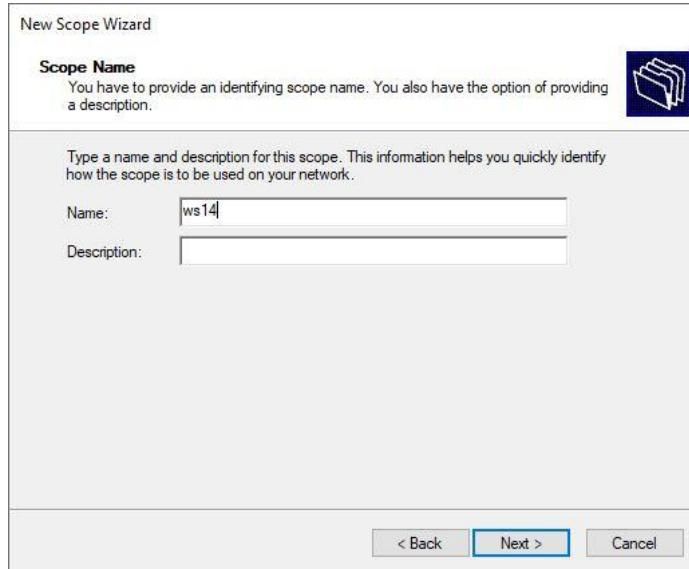


Figure 5.11 Name of the scope

**STEP 7:** Insert client’s IPV4 address starting from 192.168.14.2 until 192.168.14.126 and subnet its mask 255.255.255.192. After that, click Next button.

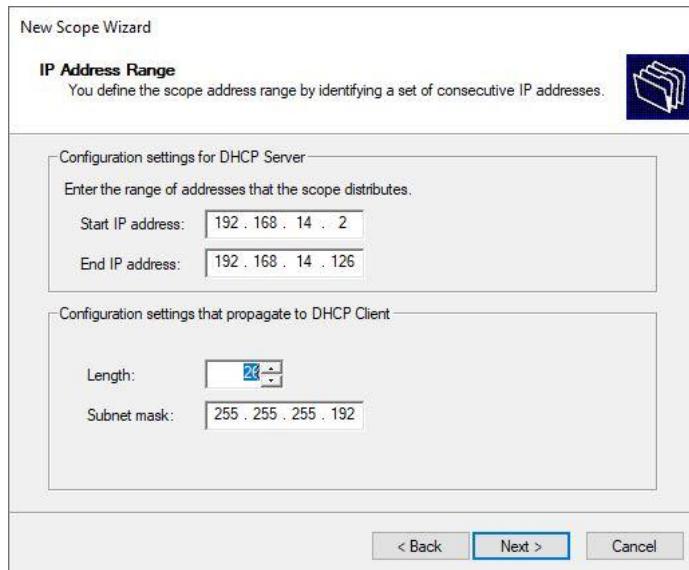


Figure 5.12 IP address range of the scope

**STEP 8:** Enter the 192.168.14.1 for getaway of the client's IPV4 and click Next.

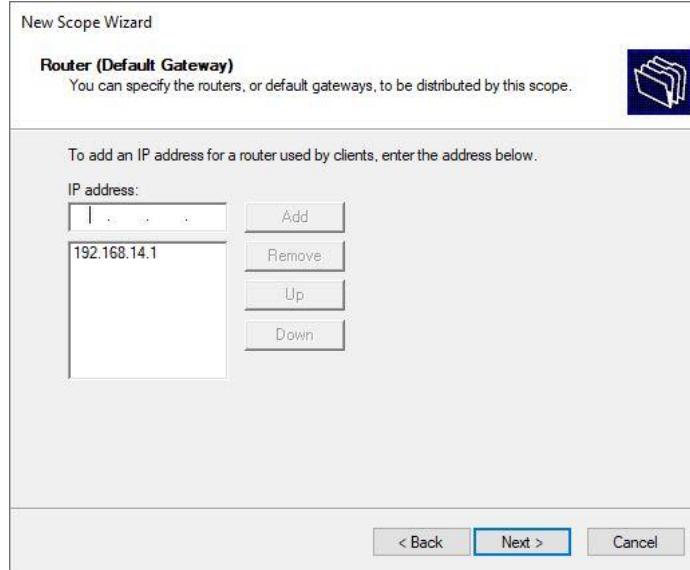


Figure 5.13 Router IP (Default Getaway)

**STEP 9:** For the Domain Name and DNS Servers, insert the DNS IP which is 192.168.14.178 and group14.com. Then, click Next button.

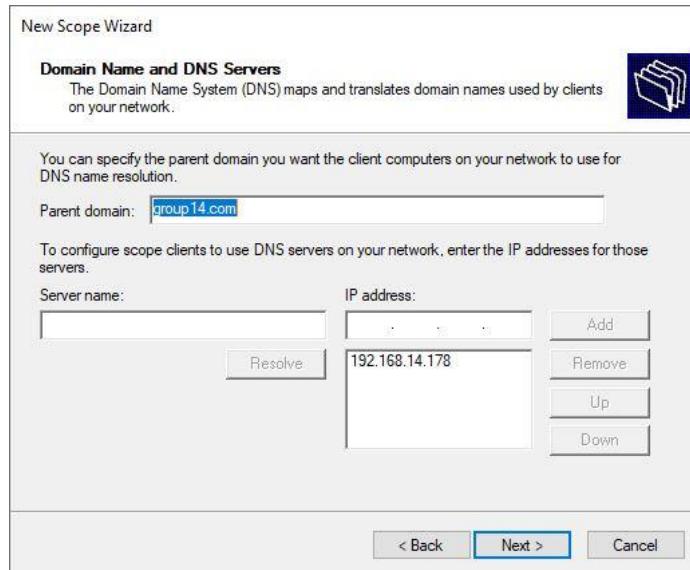


Figure 5.14 Domain Name and DNS

**STEP 10:** For Lease Duration page, just click Next button.

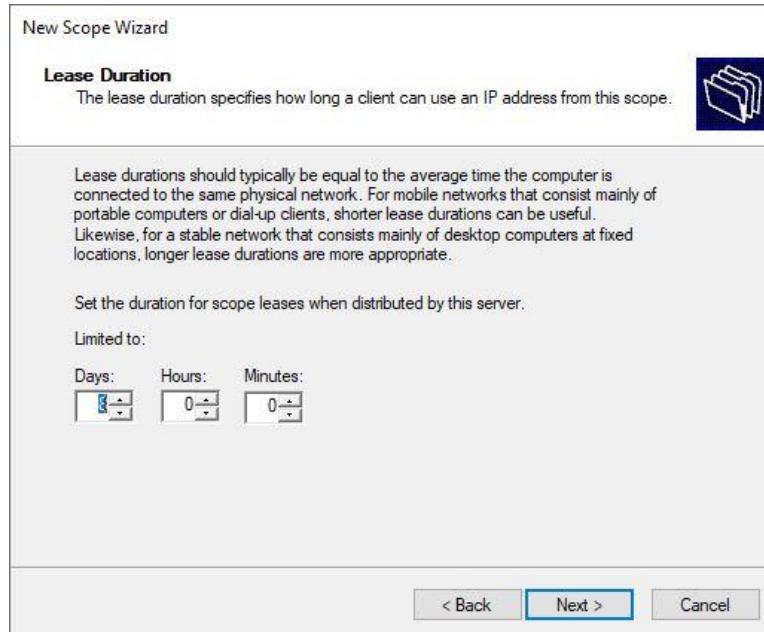


Figure 5. 15 Lease Duration

**STEP 11:** Next, for WINS Servers page, also just click Next button.

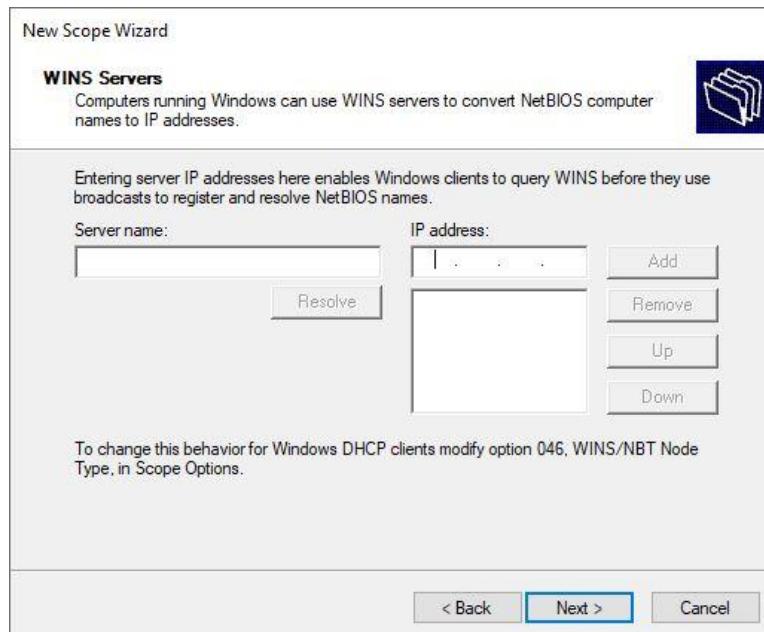


Figure 5. 16 WINS Servers

**STEP 12:** For the final step, just choose “Yes, I want to configure these options now” and click Next.

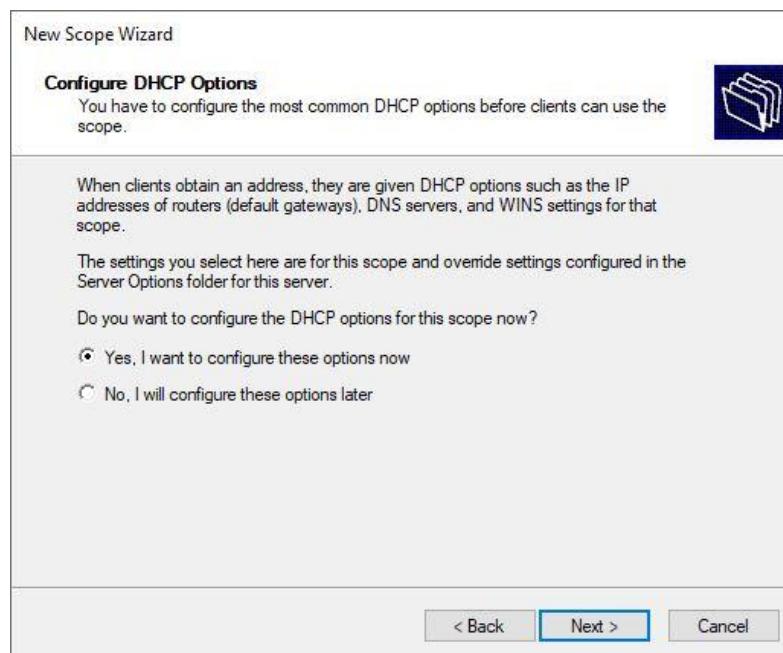


Figure 5.17 Configure DHCP Options

**STEP 13:** Just click finish to complete DHCP configuration.

**STEP 14:** After you complete the configuration, the new scope will appear at the DHCP page.

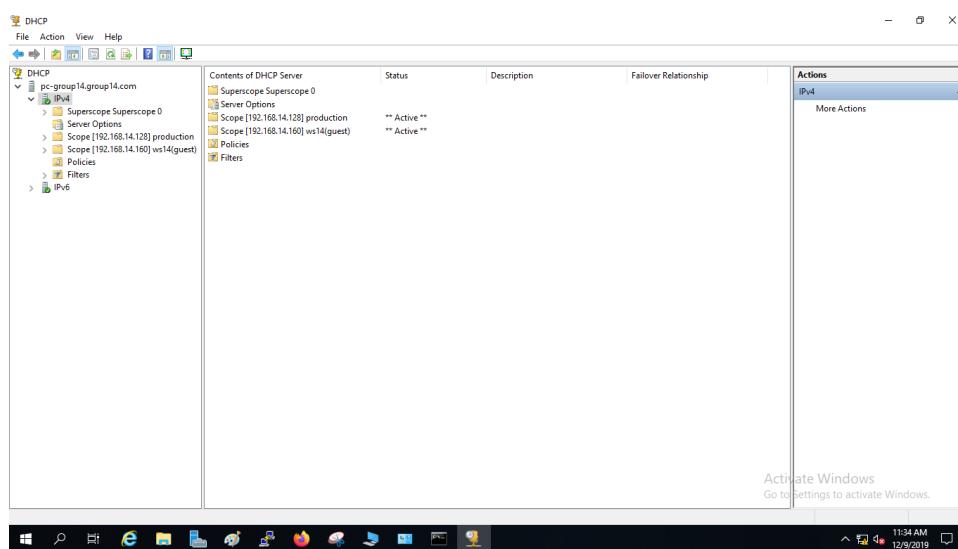
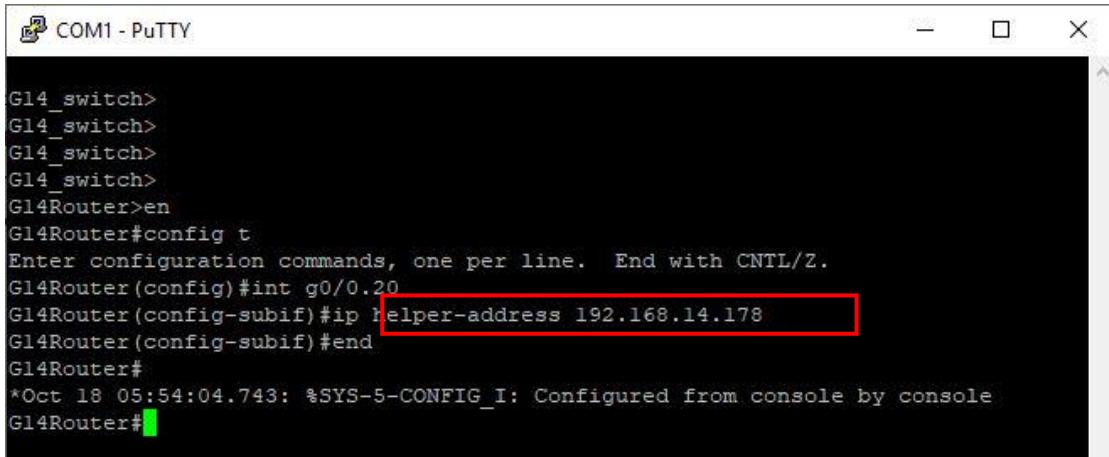


Figure 5. 18 Page of DHCP

**STEP 15:** Configure IP helper address in router.



```
COM1 - PuTTY
G14_switch>
G14_switch>
G14_switch>
G14_switch>
G14Router>en
G14Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
G14Router(config)#int g0/0.20
G14Router(config-subif)#ip helper-address 192.168.14.178
G14Router(config-subif)#end
G14Router#
*Oct 18 05:54:04.743: %SYS-5-CONFIG_I: Configured from console by console
G14Router#
```

Figure 5.19 IP helper command

## CONFIGURE DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP) IPV6.

**STEP 1:** Open tool in Task Manager and choose DHCP.

**STEP 2:** Enter scope name as “ws14” and click Next button.

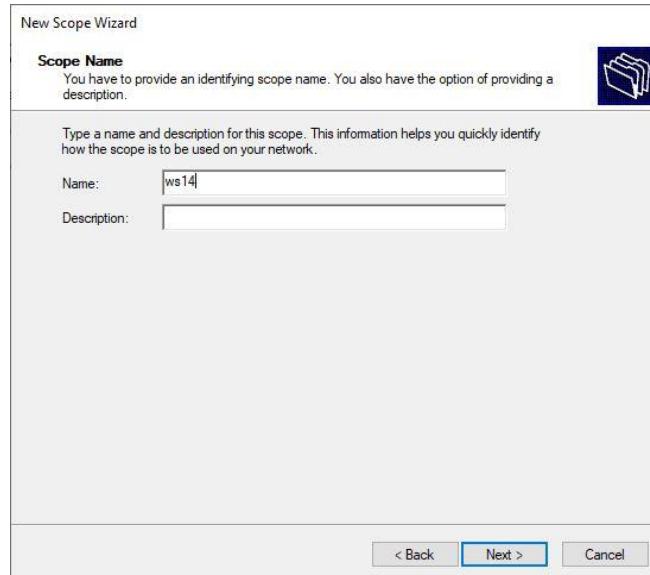


Figure 5. 20 Scope name IPV6

**STEP 3:** Enter scope prefix as below 2001:0DC0:0002:: for client's IPV6. Then, click Next button.

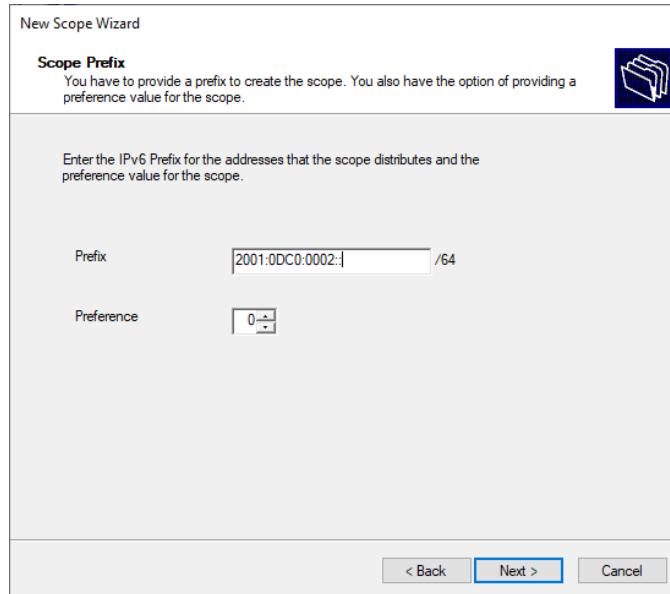


Figure 5.21 Scope Prefix IPV6

**STEP 4:** For Add Exclusions page, just enter the getaway of the IPV6 address, 2001:0DC0:0002::1

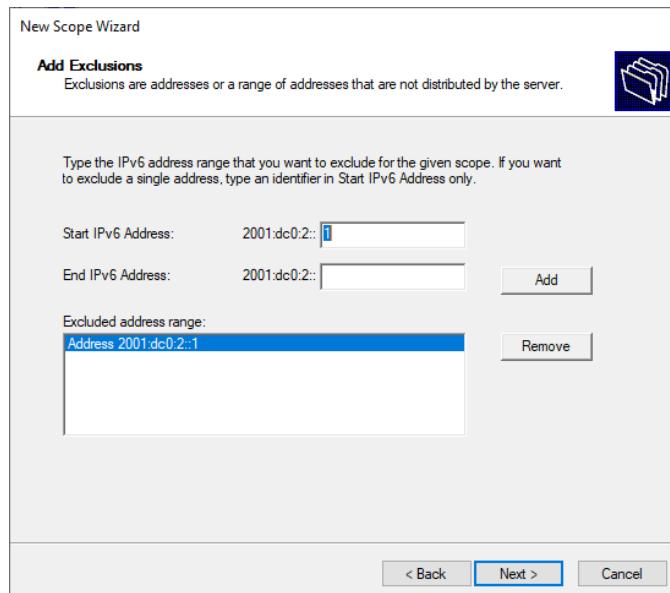


Figure 5. 22 Add Exclusions for IPV6

**STEP 5:** For the Scope Lease page, just click Next button.

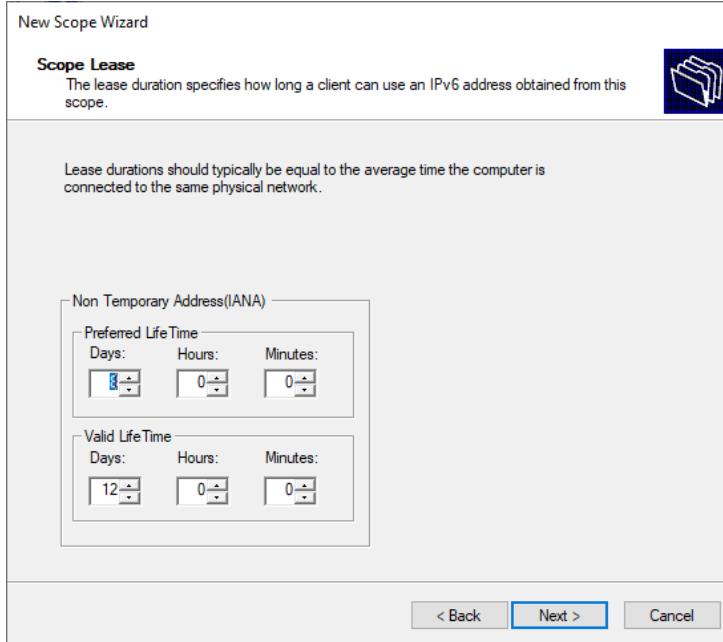


Figure 5.23 Scope Lease IPV6

**STEP 6:** For the final step, just choose “Yes, I want to configure these options now” and click Next.

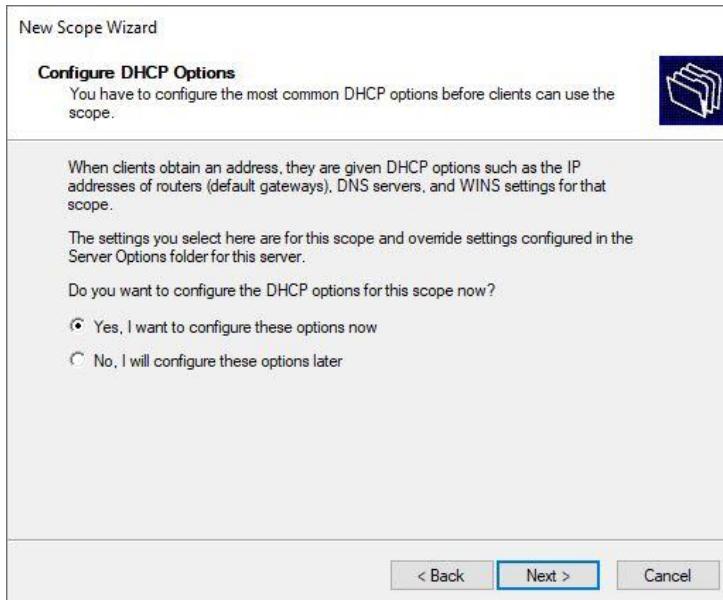


Figure 5.24 Configure DHCP Options

**STEP 7:** Just click Finish button.

**STEP 8:** After configuration, the DHCP IPV6 scope appear at the page of DHCP.

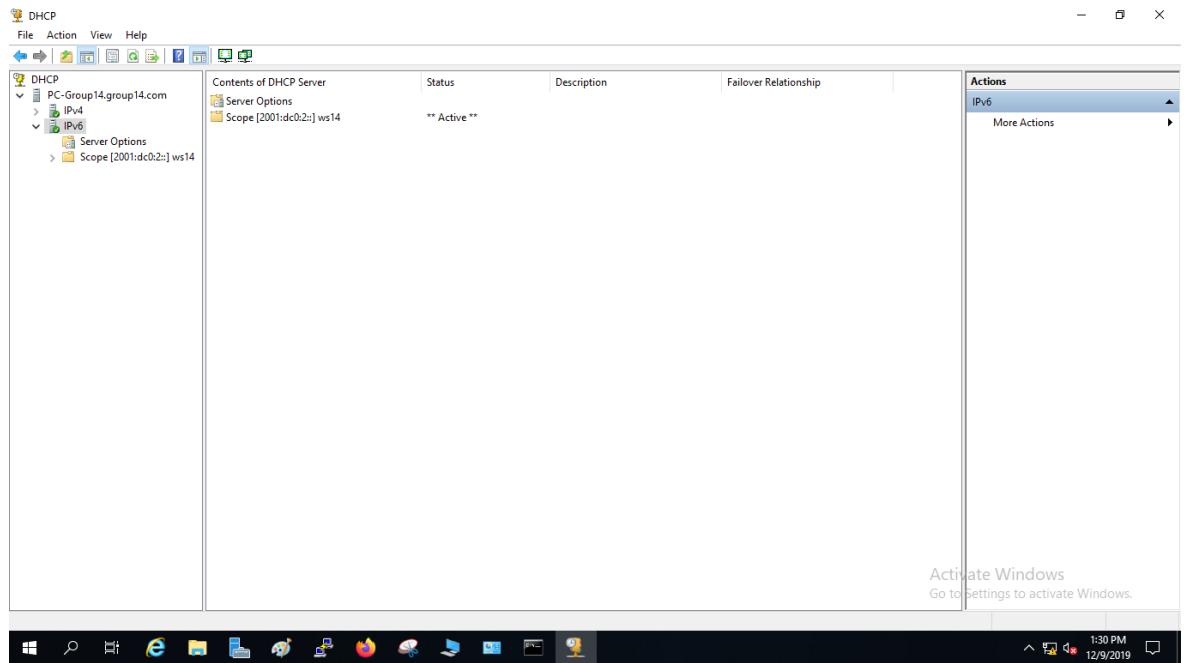


Figure 5.25 Page of DHCP

**STEP 9:** Click at the Scope Options to configure the DNS Recursive Name Server IPV6 Addresses.

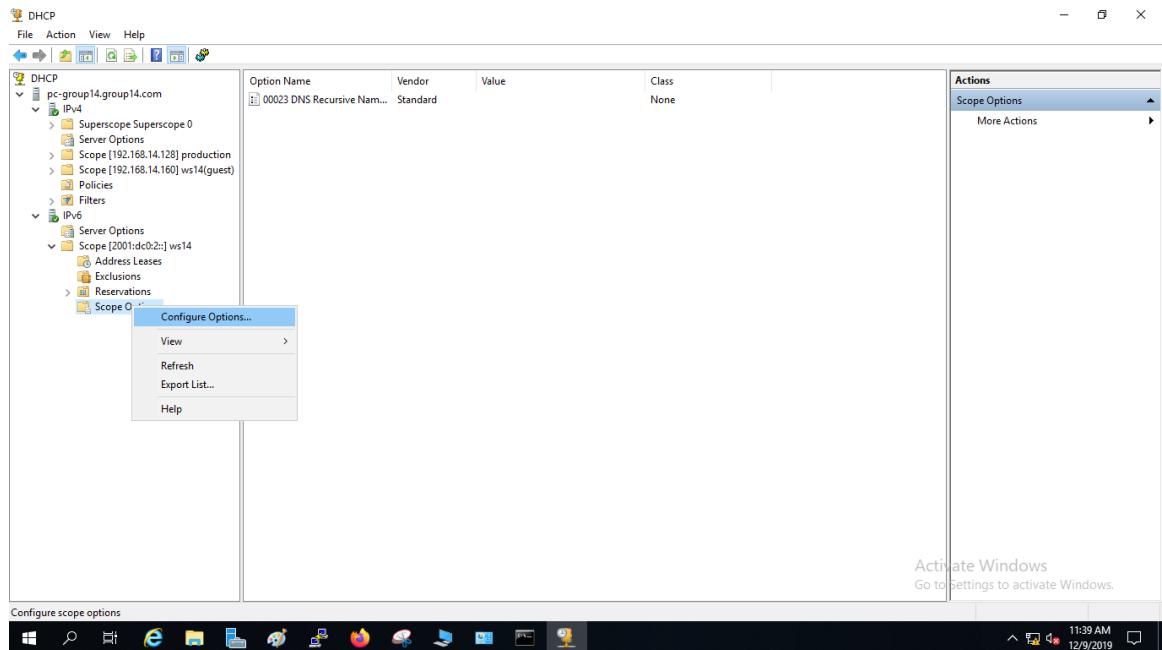


Figure 5. 26 Scope Options

**STEP 10:** Click the 0023 checkbox and enter 2001:0DC0:0001::3 for DNS IPv6.

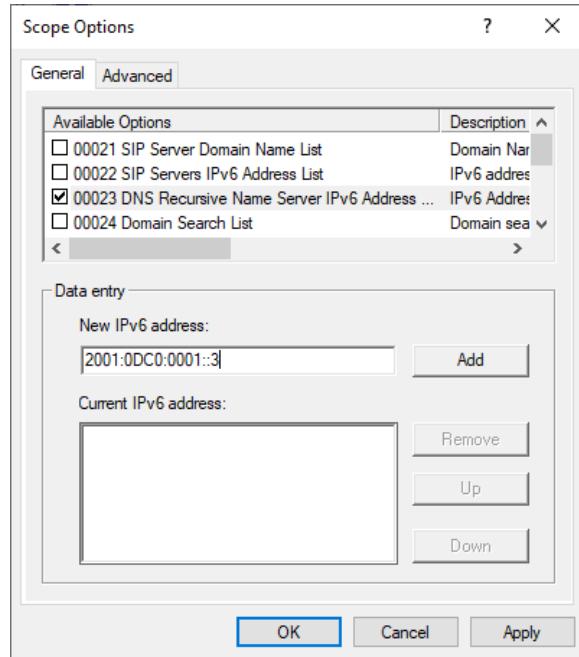


Figure 5. 27 Scope options in IPV6

### 5.3.3 DYNAMIC ROUTING & NAT

#### 5.3.3.1 DYNAMIC ROUTING

**STEP 1:** Configure router EIGRP 10 and router-id 1.1.1.1

```
G14Router(config)#router eigrp 10  
G14Router(config-router)#router-id 1.1.1.1  
G14Router(config-router)#exit
```

Figure 5.28 Router eigrp and Router-ID

**STEP 2:** Configure all the network addresses

```
G14Router(config-router)#network 192.168.14.0 0  
G14Router(config-router)#network 192.168.14.64 0  
G14Router(config-router)#network 192.168.14.128 0  
G14Router(config-router)#network 192.168.14.144 0
```

Figure 5.29 Network address

### 5.3.3.2 NETWORK ADDRESS TRANSLATING (NAT)

**STEP 1:** Set IP Address to the interface connected to neighbour router and set IP NAT Outside.

```
interface Serial0/0/0
ip address 200.200.200.2 255.255.255.248
ip nat outside
ip virtual-reassembly in
ipv6 enable
ipv6 ospf 1 area 0
crypto map CMAP
```

Figure 5. 30 IP NAT Outside

**STEP 2:** Set the serial0/0/0 overload and set the static NAT public IP to all servers.

```
ip nat inside source list 100 interface Serial0/0/0 overload
ip nat inside source static 192.168.14.178 200.200.200.4
ip nat inside source static 192.168.14.179 200.200.200.5
ip nat inside source static 192.168.14.180 200.200.200.6
ip route 192.168.1.144 255.255.255.240 200.200.200.1
```

Figure 5. 31 Set Static NAT public IP

**STEP 3:** Assign all VLANs under IP Nat Inside as below.

```
interface GigabitEthernet0/0.10
encapsulation dot1Q 10
ip address 192.168.14.177 255.255.255.240
ip nat inside
ip virtual-reassembly in
ipv6 address 2001:DC0:1::1/48
ipv6 enable
ipv6 ospf 1 area 0
!
interface GigabitEthernet0/0.20
encapsulation dot1Q 20
ip address 192.168.14.1 255.255.255.192
ip helper-address 192.168.14.178
ip nat inside
ip virtual-reassembly in
ipv6 address 2001:DC0:2::1/48
ipv6 dhcp relay destination 2001:DC0:1::3
!
interface GigabitEthernet0/0.30
encapsulation dot1Q 30
ip address 192.168.14.161 255.255.255.240
ip helper-address 192.168.14.178
ip nat inside
ip virtual-reassembly in
```

Figure 5. 32 IP NAT INSIDE

### 5.3.4 IPSEC SITE TO SITE TUNNELLING

**STEP 1:** Create an ISAKMP phase 1 policy and 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.

```
crypto isakmp policy 1
  encr 3des
  hash md5
  authentication pre-share
  group 2
crypto isakmp key group14 address 200.200.200.1
```

*Figure 5. 33 Create ISAKMP phase 1 policy*

**STEP 2:** Create the transform set used to protect our data. We've named this TS.

```
crypto ipsec transform-set TS esp-3des esp-md5-hmac
  mode tunnel
```

*Figure 5. 34 Create the transform set*

**STEP 3:** Create the pre share key authentication with our peer (Next group router) and Create an access-list and define the traffic we would like the router to pass through the VPN tunnel.

```
crypto map CMAP 10 ipsec-isakmp
  set peer 200.200.200.1
  set transform-set TS
  match address VPN-TRAFFIC
```

```
ip access-list extended VPN-TRAFFIC
  permit ip 192.168.14.176 0.0.0.15 192.168.1.144 0.0.0.15
```

*Figure 5. 35 Define a pre shared key and create an access-list*

**STEP 4:** Create the Crypto Map and connects the previously defined ISAKMP and Ipsec configuration together. We've named our crypto map CMAP. Apply the crypto map to the outgoing interface of the router to another router. Here, the outgoing interface is Serial 0/0/0.

```
interface Serial0/0/0
  crypto map CMAP
```

*Figure 5. 36 Apply the crypto map to the outgoing interface*

### 5.3.5 ACCESS CONTROL LIST

**STEP 1:** Configure ACL configuration. This extended access-list used to block specific port from client accessing to server network and certain services.

```
G14Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
G14Router(config)#access-list 120 deny tcp 192.168.14.0 0.0.0.63 any eq 443
G14Router(config)#access-list 120 deny tcp 192.168.14.0 0.0.0.63 any eq 25
G14Router(config)#access-list 120 deny tcp 192.168.14.0 0.0.0.63 any eq 22

G14Router(config)#access-list 110 permit icmp any any
G14Router(config)#access-list 110 deny    tcp 192.168.14.0 0.0.0.63 any eq 443

G14Router(config)#access-list 110 permit icmp any any
G14Router(config)#access-list 110 deny    tcp 192.168.14.0 0.0.0.63 any eq 443
```

Figure 5. 37 Deny the port

**STEP 2:** Configure the access-group in to the port

```
G14Router(config)#int g0/0.20
G14Router(config-subif)#acc
G14Router(config-subif)#acce
G14Router(config-subif)#ip acc
G14Router(config-subif)#ip acce
G14Router(config-subif)#ip access-group 110 in
```

Figure 5.38 Assign the access-group in to specific port

## 5.3.6 DOMAIN NAME SYSTEM

### 5.3.6.1 FORWARD LOOKUP ZONE (PRIMARY DNS)

**STEP 1:** Create new DNS using wizard

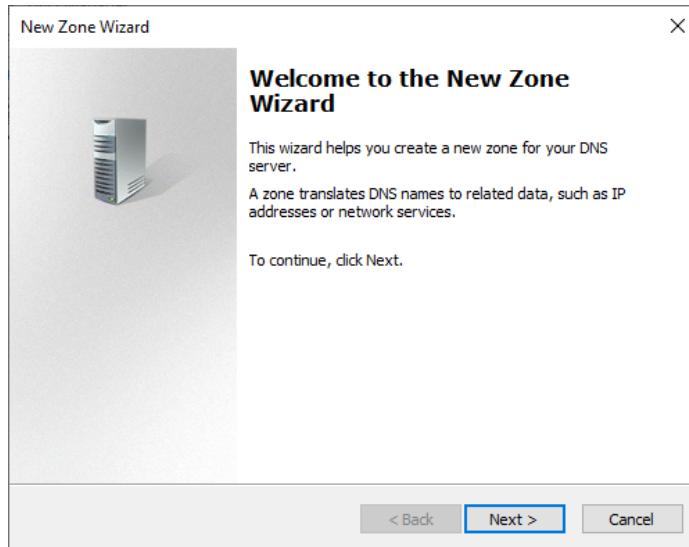


Figure 5. 39 Creating a new zone wizard

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

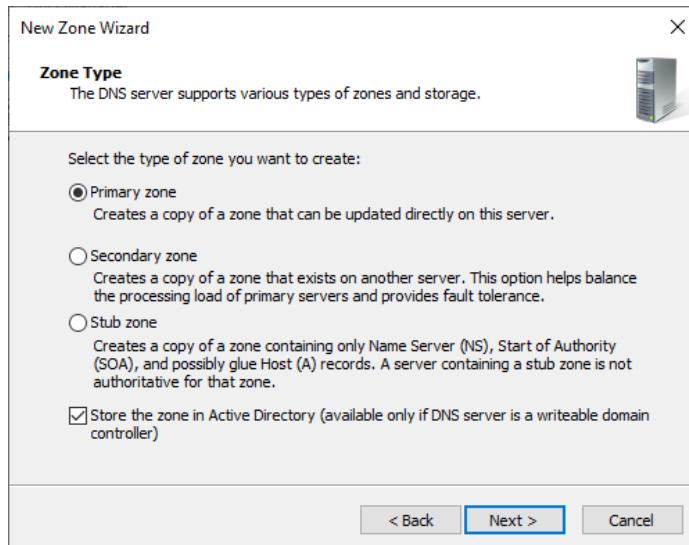


Figure 5. 40 Selecting zone type

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

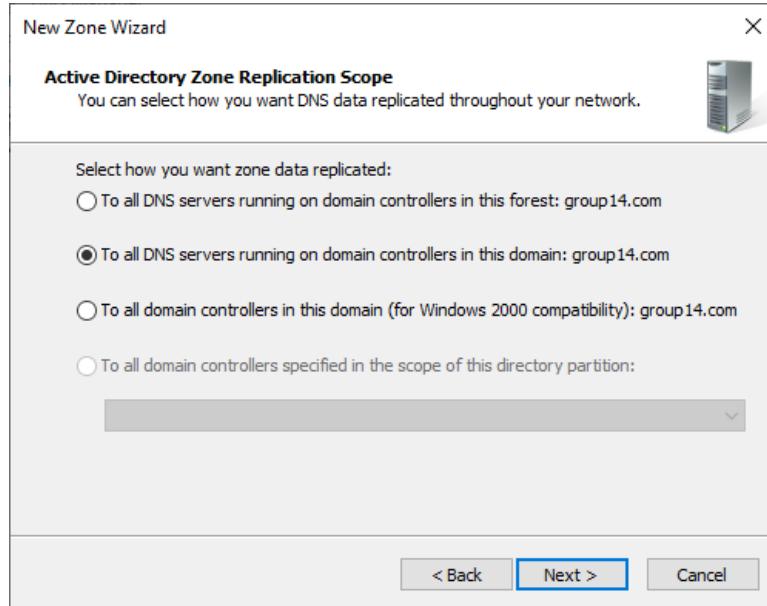


Figure 5. 41 Selecting new zone data replicated

**STEP 4:** Then, enter the zone name (example; group14.com)

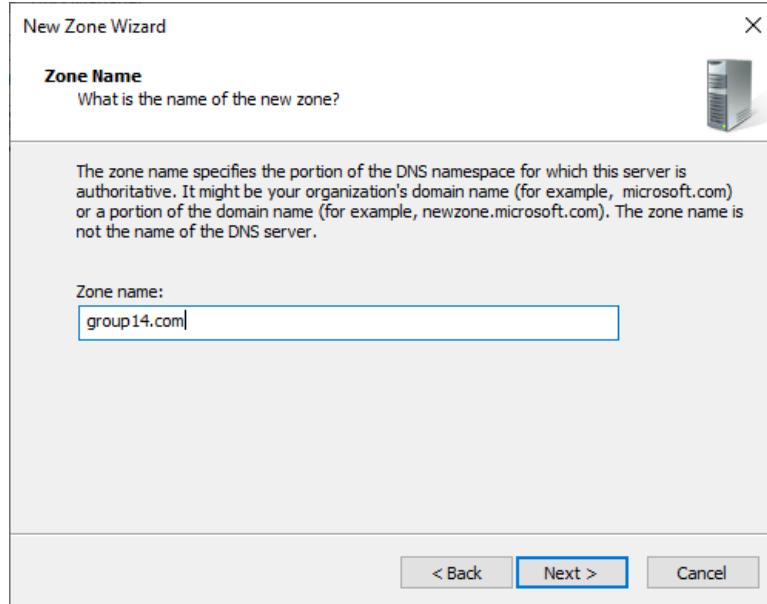


Figure 5. 42 Create a new zone name

**STEP 5:** For Dynamic Updates, select allow both non-secure and secure dynamic updates.  
Then, click next

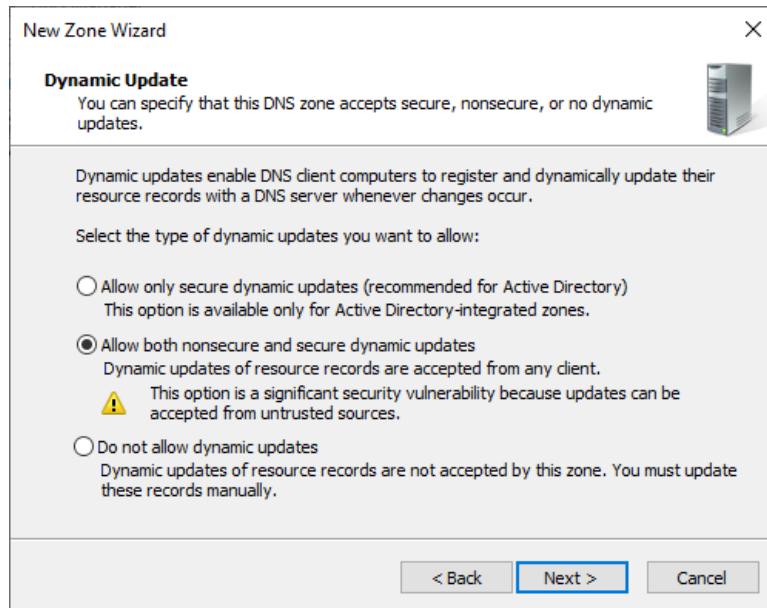


Figure 5. 43 Select type of dynamic updates

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

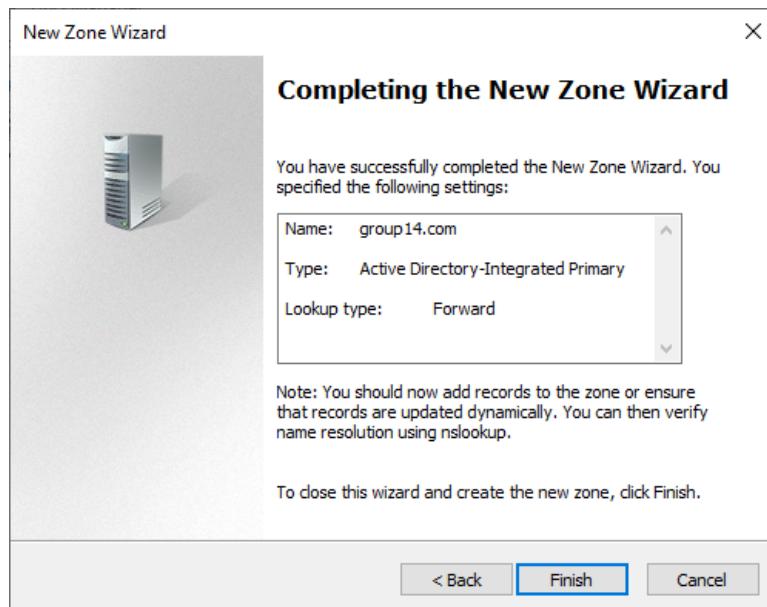


Figure 5. 44 Completing setup for new wizard zone

### 5.3.6.2 REVERSE LOOKUP ZONE (IPV4)

**STEP 1:** For Reverse Lookup Zone Name, select IPv4 Reverse Lookup Zone and click next.

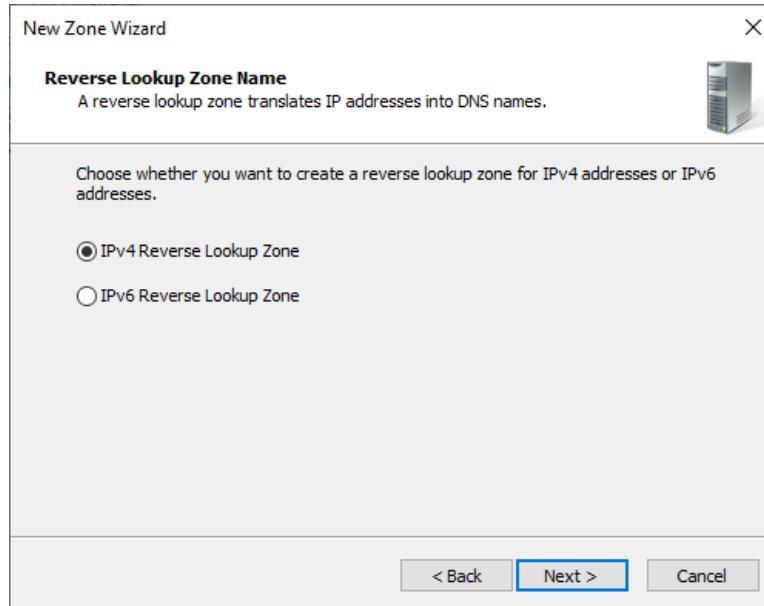


Figure 5. 45 Create new ipv4 reverse lookup

**STEP 2:** Enter Network ID for the zone and click Next button

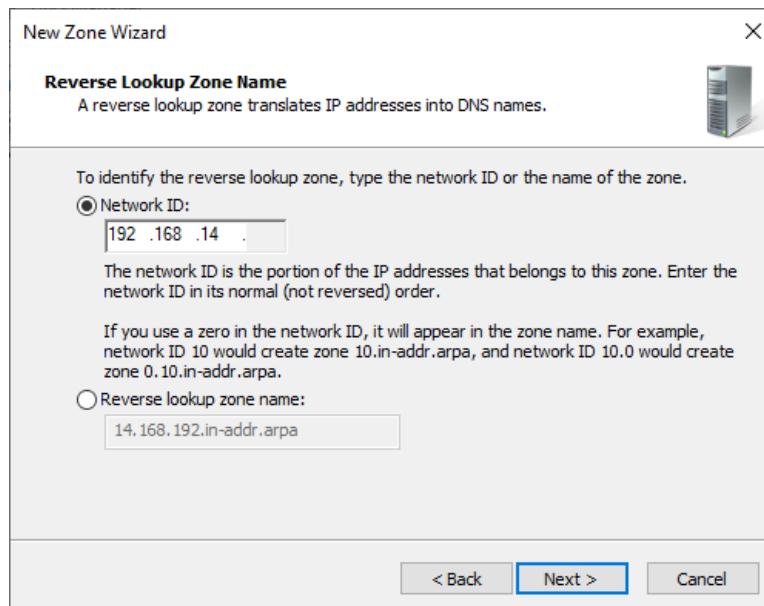


Figure 5. 46 Server ip

**STEP 3:** For Dynamic Updates, select allow both non-secure and secure dynamic updates.

Then, click next

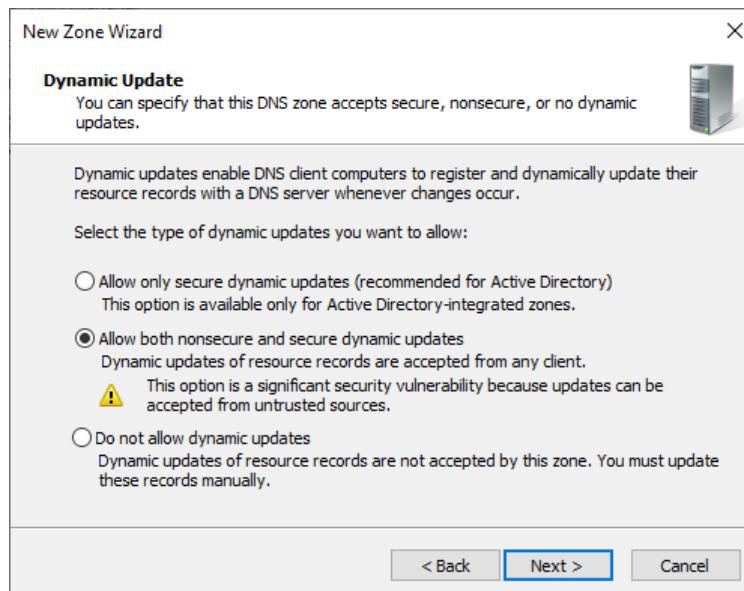


Figure 5. 47 Select update type for new zone wizard

**STEP 4:** Upon completing the New Zone Wizard, it will show the specified settings that have been done. Then, click Finish to close.

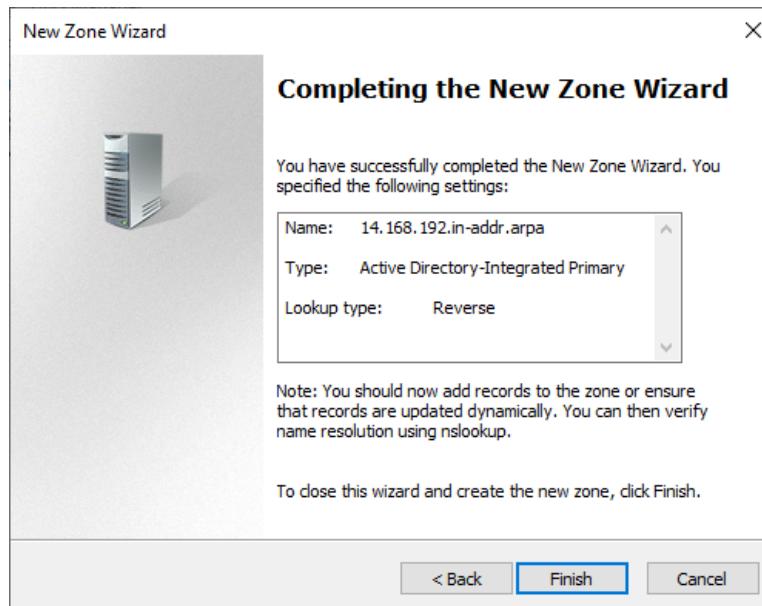


Figure 5. 48 Completing setup for new wizard zone 2

**STEP 5:** Create new pointer for reverse lookup IPV4 and enter the Host IP Address and host name. Then click OK.

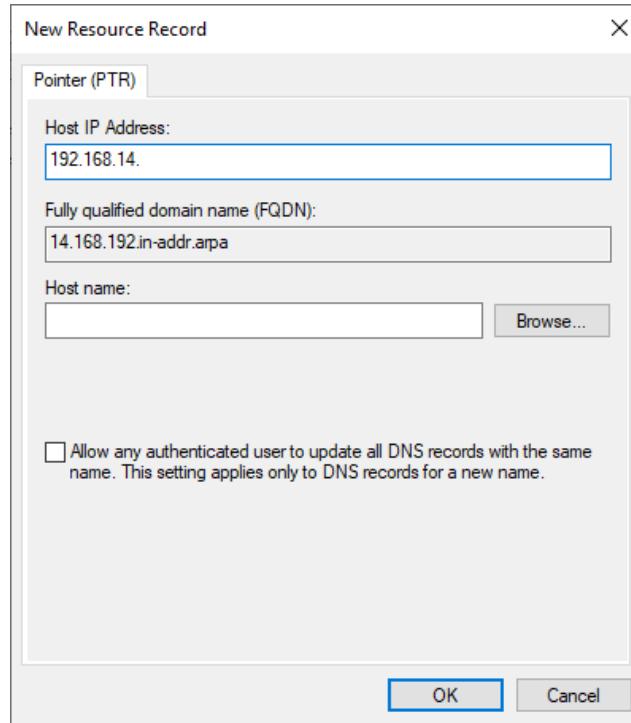


Figure 5. 49 Enter the Host IP Address

**STEP 6:** Click on group14.com and right click then click on New Host (A or AAAA).

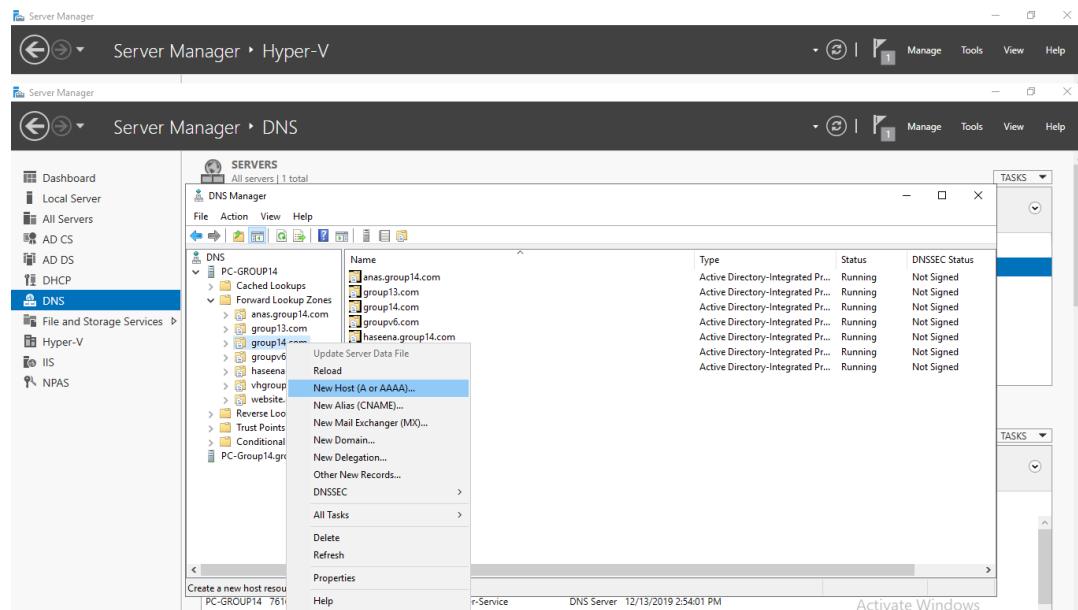


Figure 5. 50 New Host (A or AAAA)

**STEP 7:** Enter the Name winsrv and IP address 192.168.1.10. Then click Add Host.

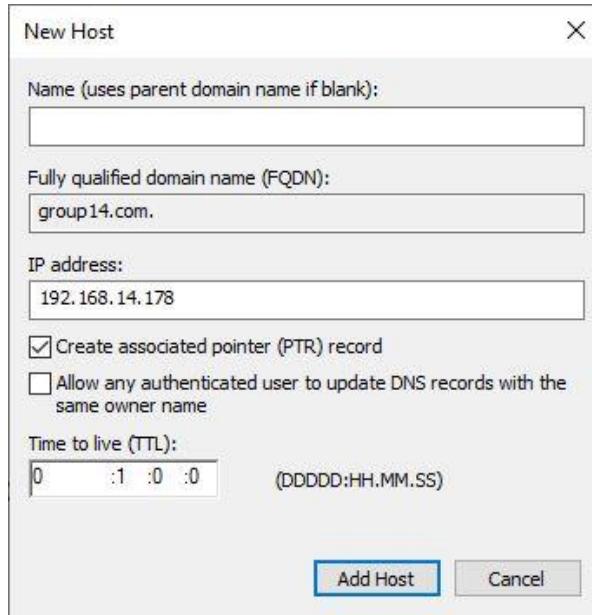


Figure 5. 51 New Host IPv4

### 5.3.6.3 FORWARD LOOKUP ZONE (IPV6)

**STEP 1:** For Reverse Lookup Zone Name, select IPv6 Reverse Lookup Zone and click next.

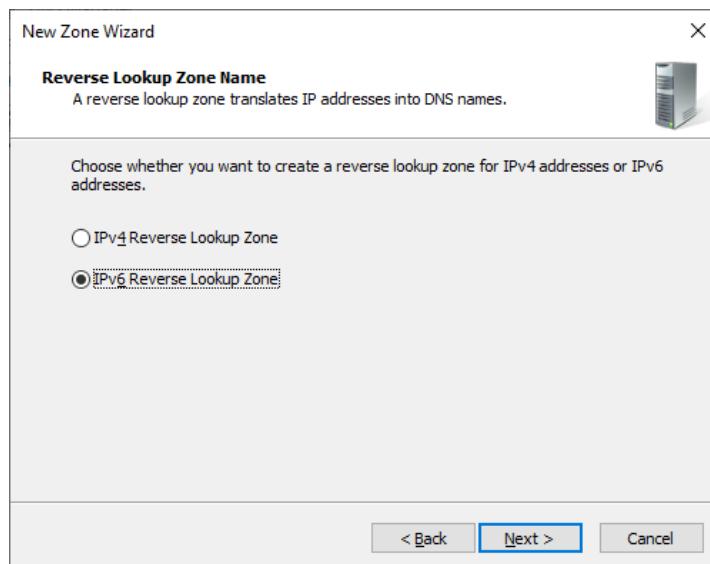


Figure 5. 52 Ipv6 reverse lookup

**STEP 2:** Enter IPv6 Address Prefix and click next.

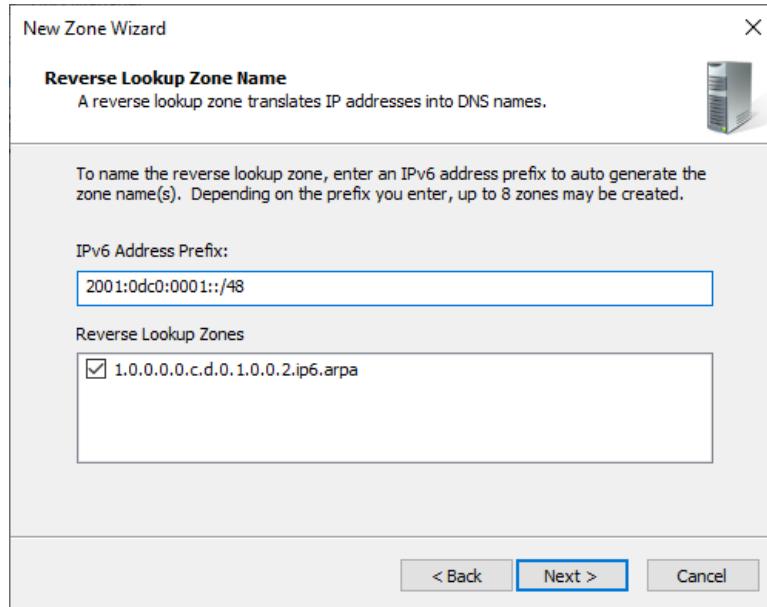


Figure 5. 53 Ipv6 reverse ip

**STEP 3:** Lastly, click finish.

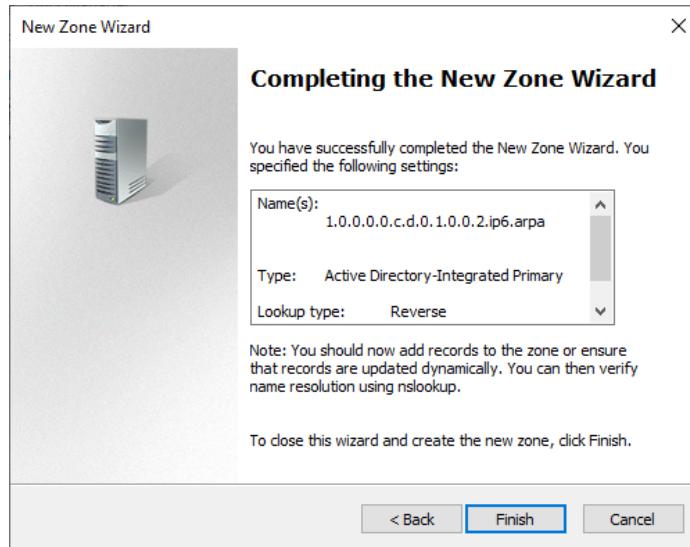
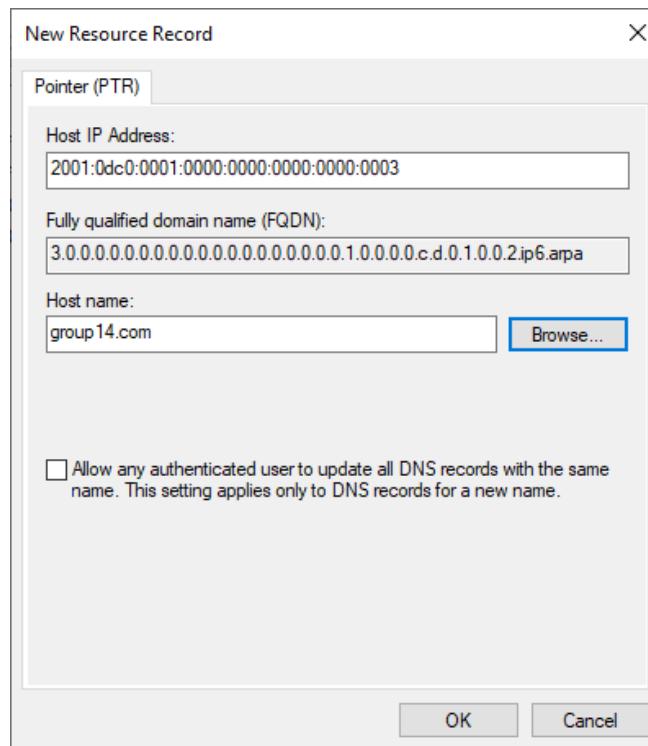


Figure 5. 54 Finish setup for reverse ip

**STEP 4:** Create new pointer for reverse lookup IPV6 and browse the Host IP Address and host name from. Then click OK.



*Figure 5. 55 Browse the host name from Forward zone*

### 5.3.7 SERVER VIRTUALIZATION

**STEP 1 :** Select add roles and features wizard to begin the install Hyper-V server.

**STEP 2 :** Select role-based or feature-based installation.

**STEP 3 :** Select destination server from the server pool.

#### STEP 4 : Click Add Features

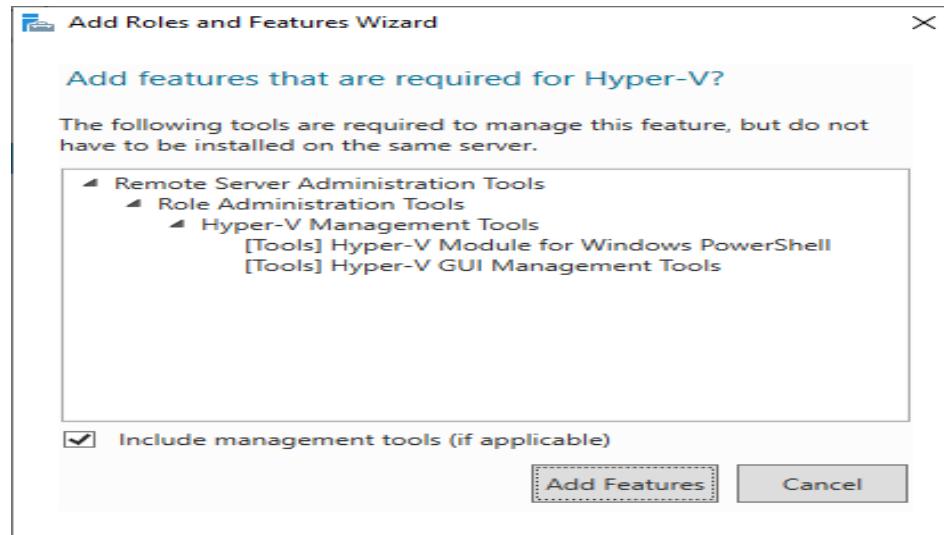


Figure 5. 56 : Add Features required Hyper-V

#### STEP 5 : Add server roles by tick the hyper-v and click next.

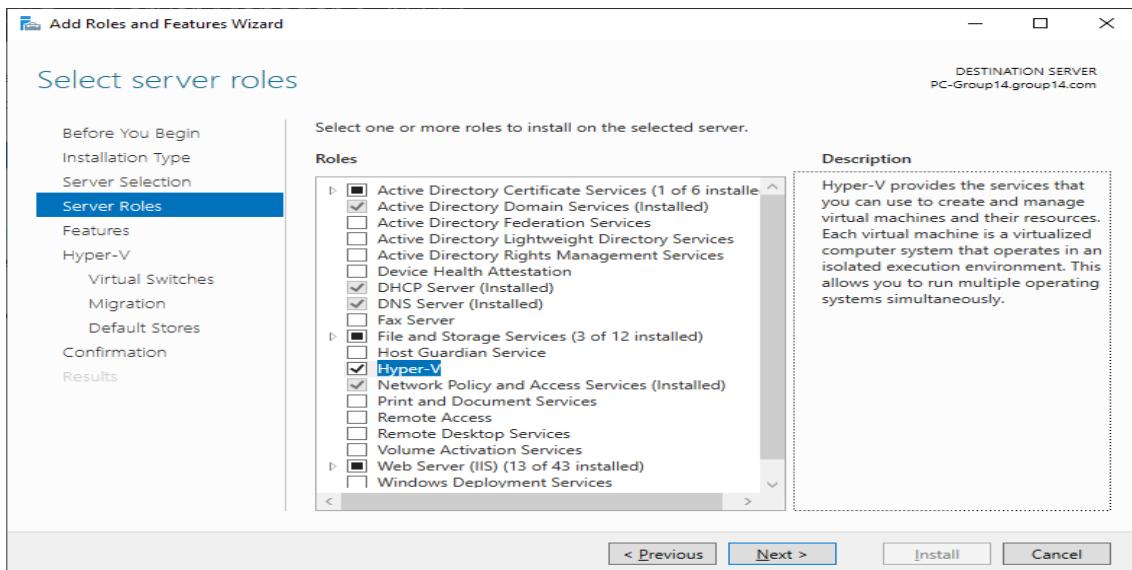


Figure 5. 57 : Select Server Roles

**STEP 6** : Click next

**STEP 7** : Select the network adapters by tick the ethernet and click next.

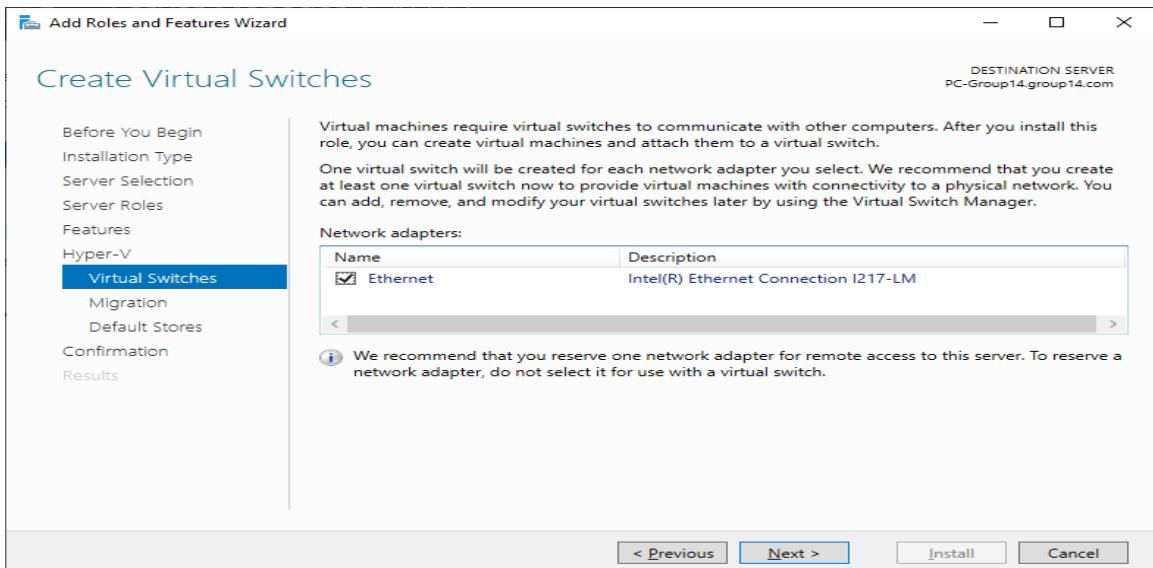


Figure 5. 58 : Create Virtual Switches

**STEP 8** : Tick “Allow this server to send and receive live migrations of virtual machines”.

Then click next.

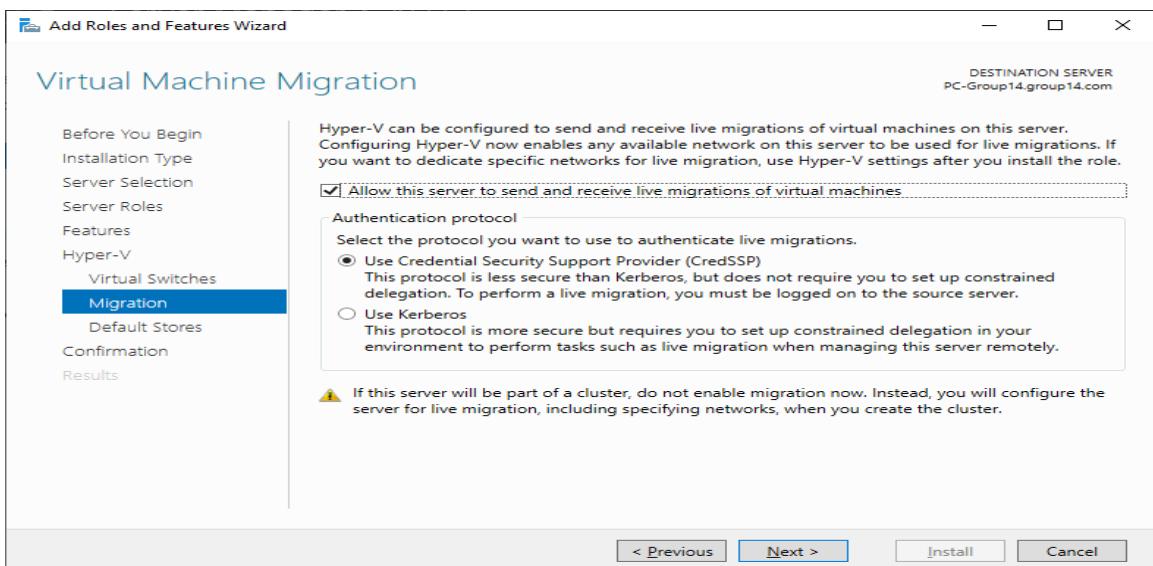


Figure 5. 59 : Virtual Machine Migration

**STEP 9 :** Browse the location where to put the file of the hyper-v. Then click next.

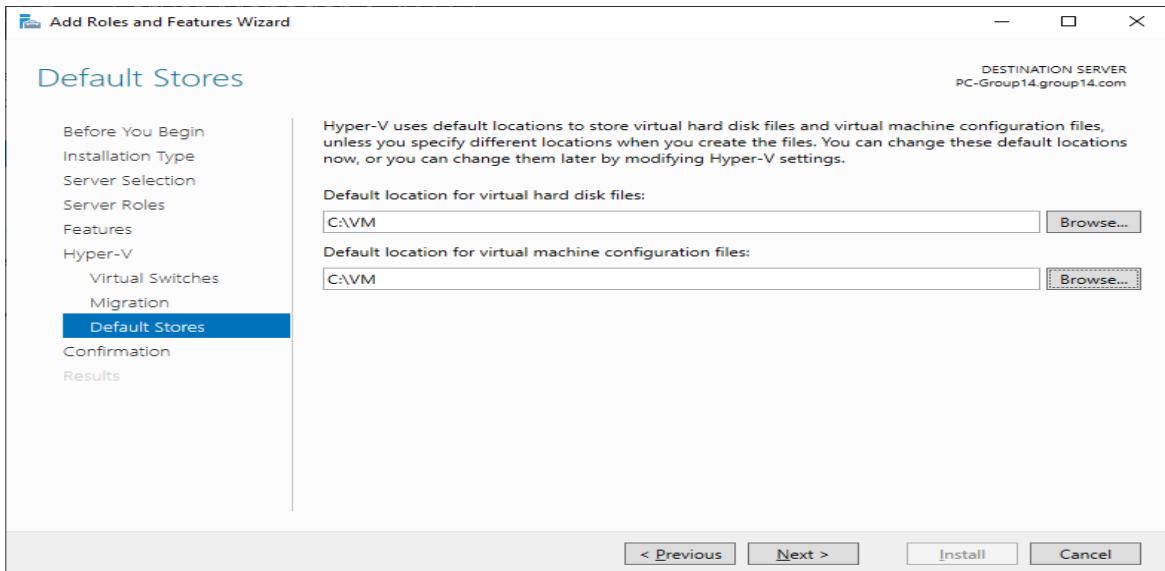


Figure 5. 60: Default Stores

**STEP 10 :** Install the service by click the install button.

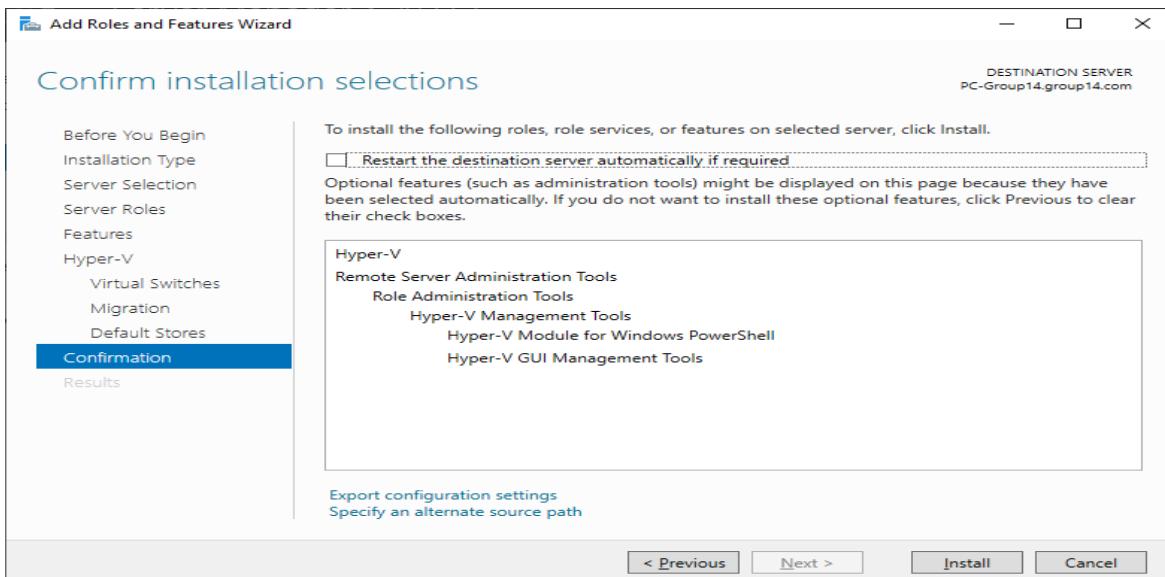


Figure 5. 61 : Confirm Installation Selections

**STEP 11 :** Restart the window server

**STEP 12 :** Open the hyper-v manager and click new > new virtual machines.

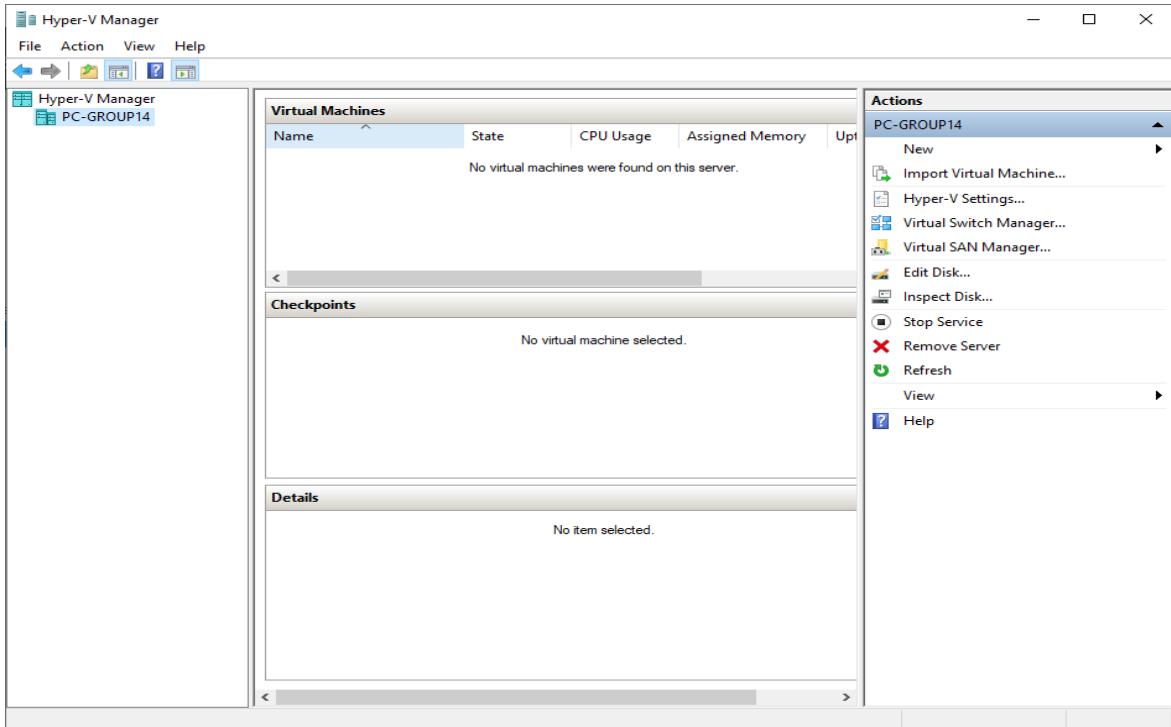


Figure 5. 62 : Hyper-V Manager

**STEP 13 :** Set a name for the new virtual machines and click next.

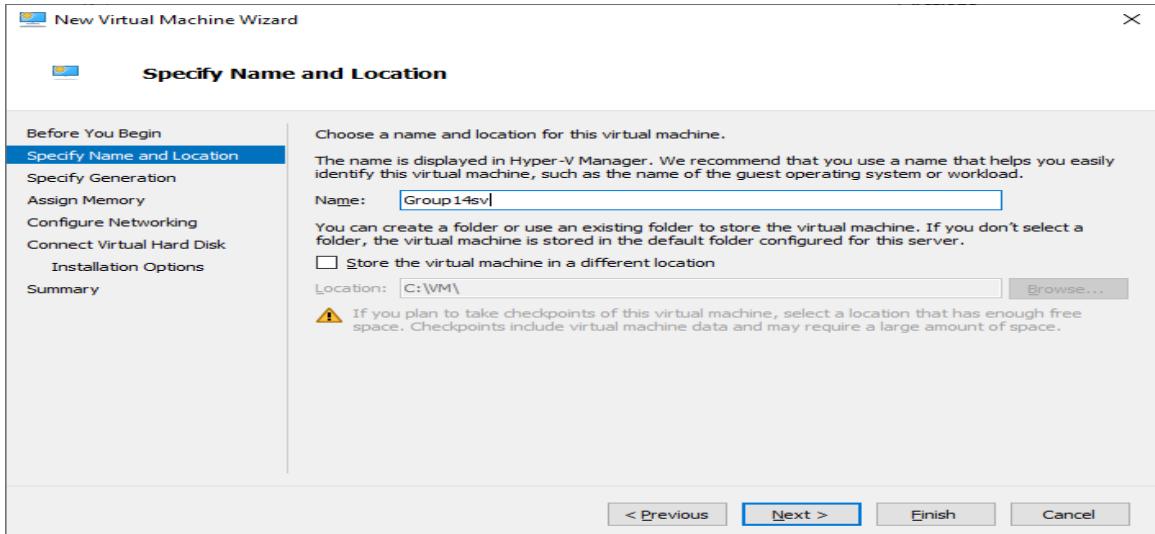


Figure 5. 63 : Specify Name And Location

**STEP 14 :** Choose generation 1 and click next.

**STEP 15 :** Set up a startup memory 8094mb and click next.

**STEP 16 :** Choose the network connection for the virtual switch.

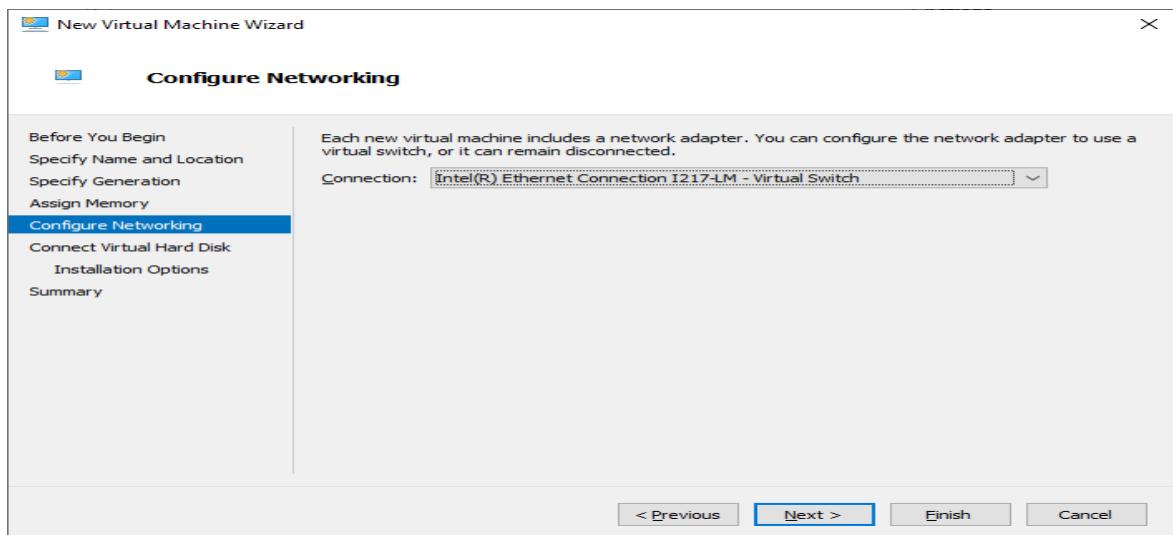


Figure 5. 64: Configure Networking

**STEP 17 :** Create a new virtual machine hard disk. Name as Group14sv.vdhx and size 127GB. Then click next.

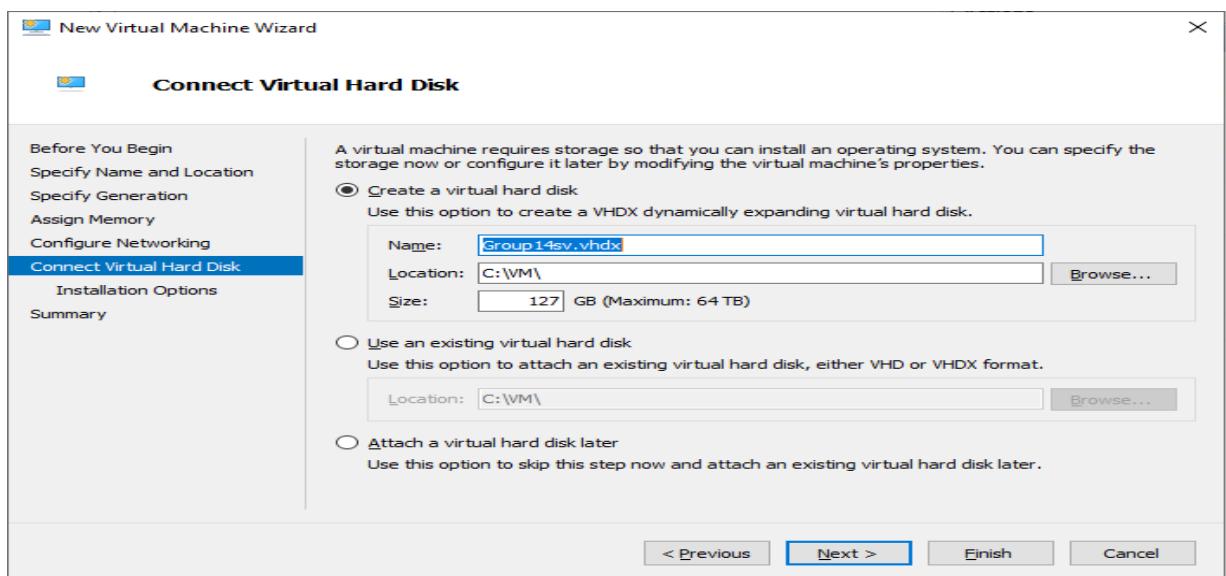


Figure 5. 65 : Connect Virtual Hard Disk

**STEP 18 :** Choose “Install an operation system from a bootable CD/DVD-ROM”. Select image file and browse to the location of the ISO.file. Then click next.

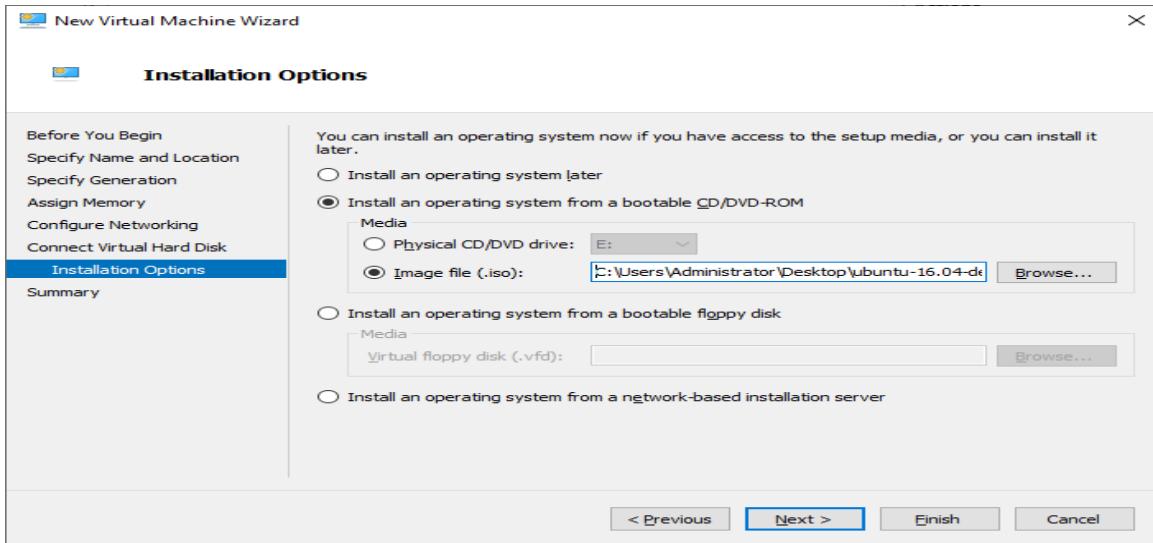


Figure 5. 66: Installation Option

**STEP 19 :** Click finish button to complete that new virtual machine.

**STEP 20 :** Go to virtual switch manager

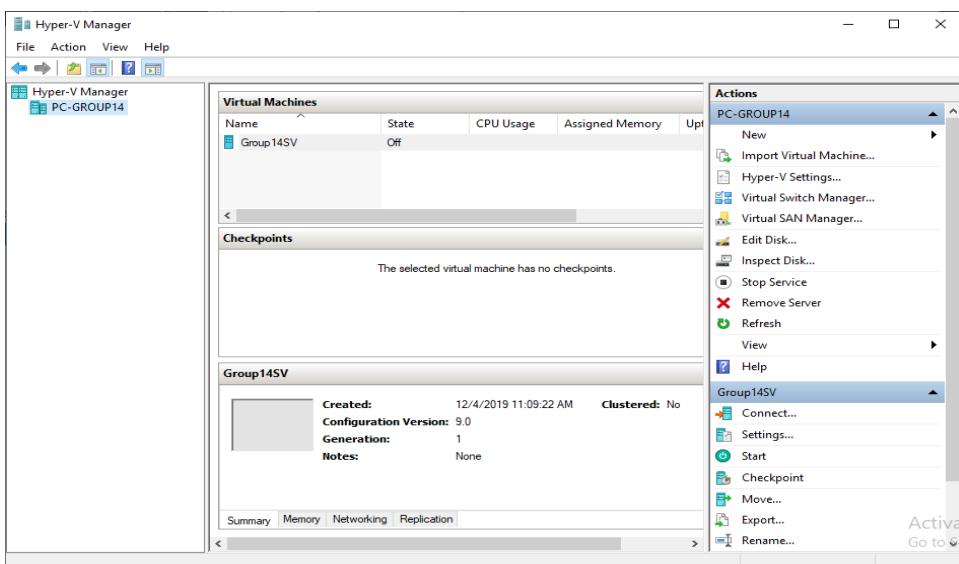


Figure 5. 67 : Hyper-V Manager

**STEP 21 :** Choose external and click create virtual switch

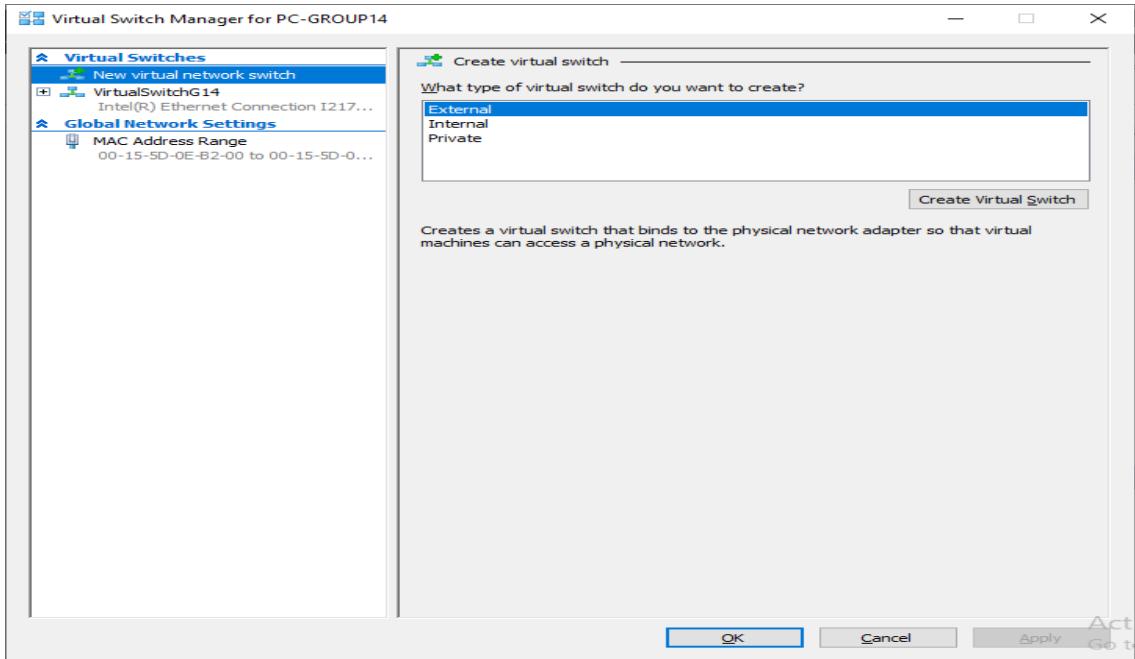


Figure 5. 68 : Virtual Switch Manager for PC-GROUP14

**STEP 22 :** Name the virtual switch as VirtualSwitchG14. Choose the external network and click Ok button.

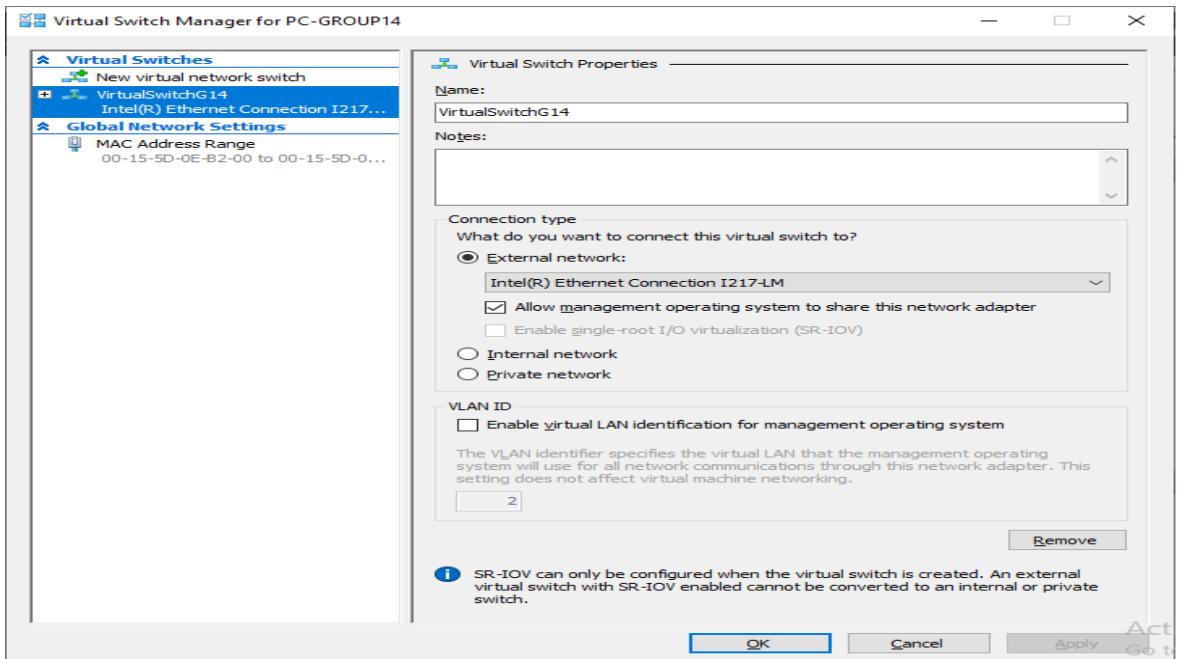


Figure 5. 69 : Virtual Switch Manager for PC-GROUP14

**STEP 23 :** At the Hyper-V manager, right click the Group14SV and click setting.

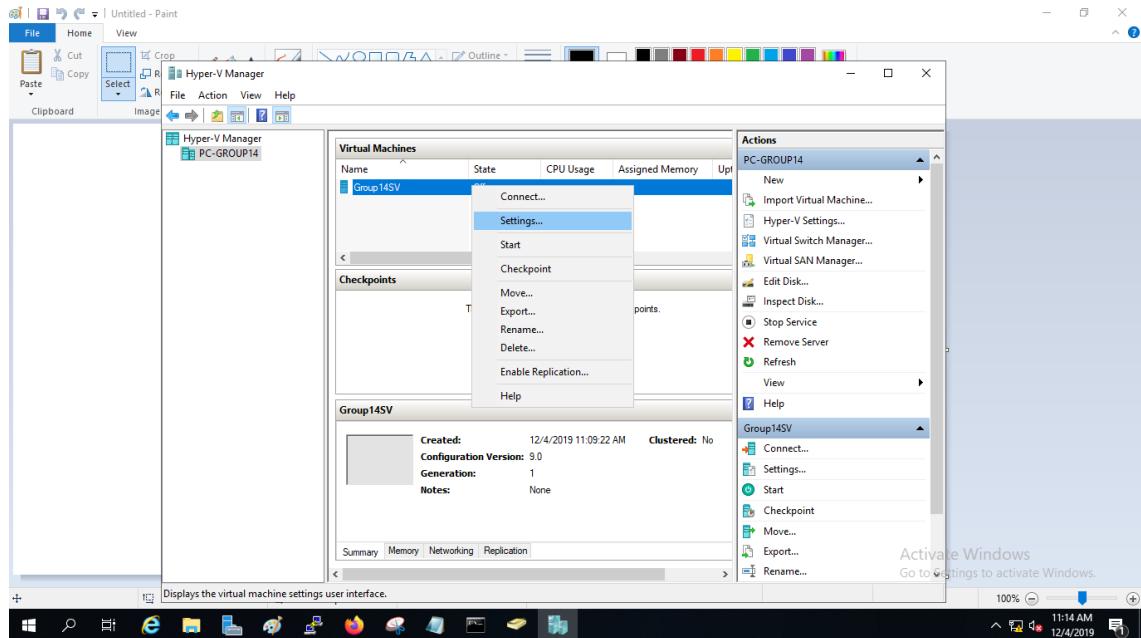


Figure 5. 70 : Hyper-V Manager

**STEP 24 :** At the network adapter virtual switch G14, change it to VirtualSwitchG14.  
Next, click Ok.

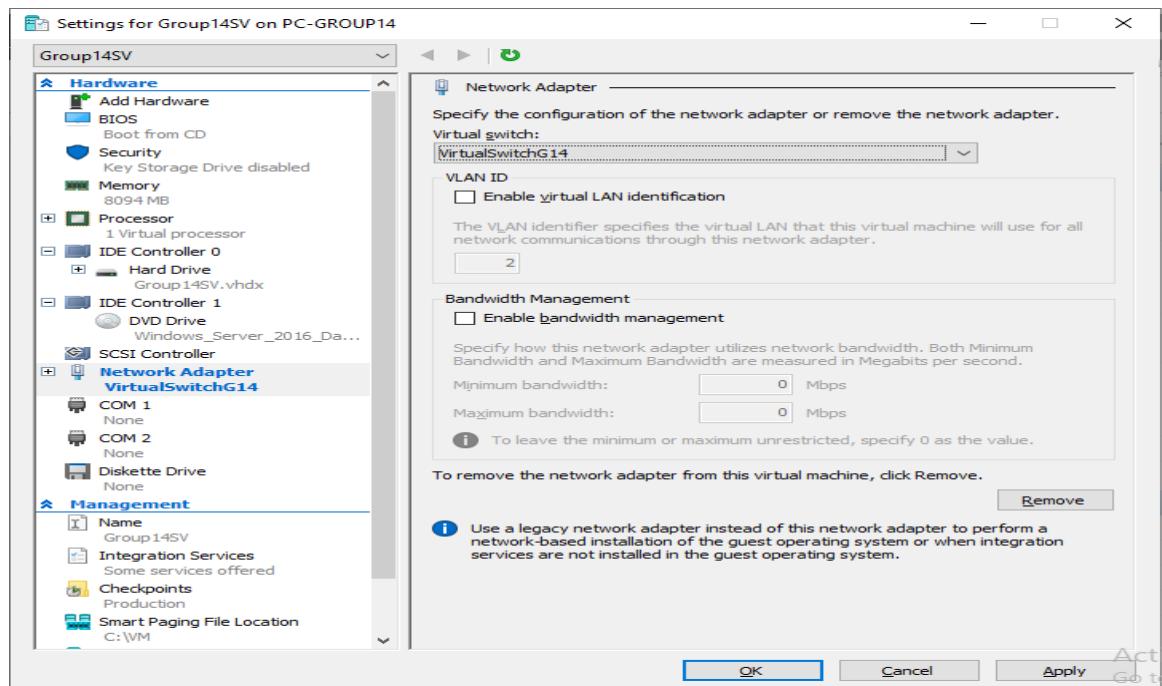


Figure 5. 71 : Setting For Group14SV on PC-GROUP14

**STEP 25 :** Start the new virtual machines.

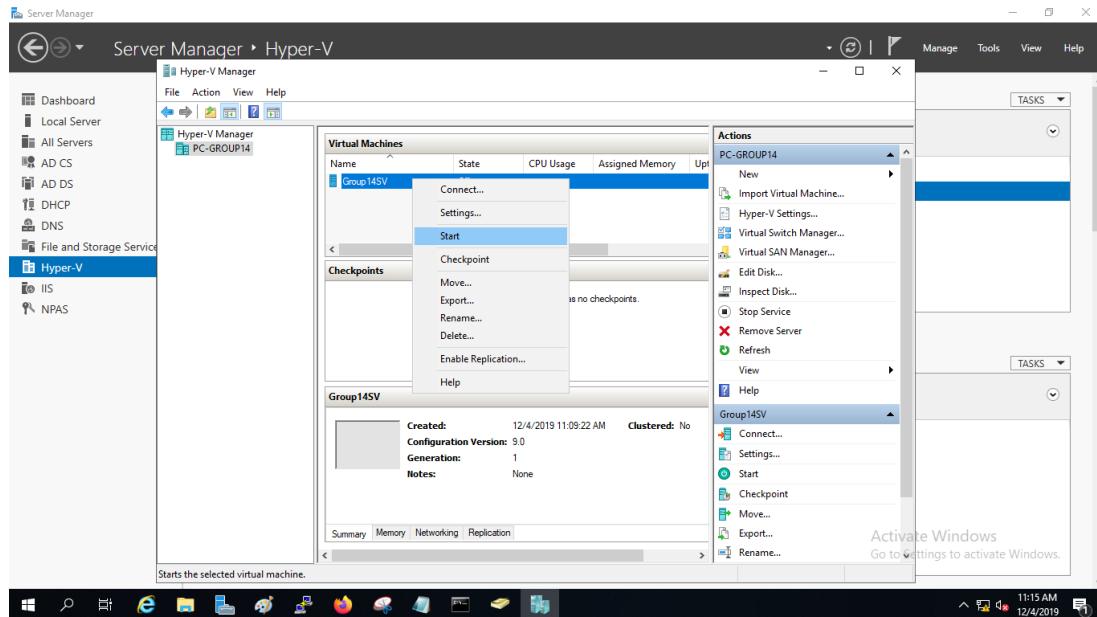


Figure 5. 72 : Hyper-V Manager

**STEP 26 :** Install the window server as usual

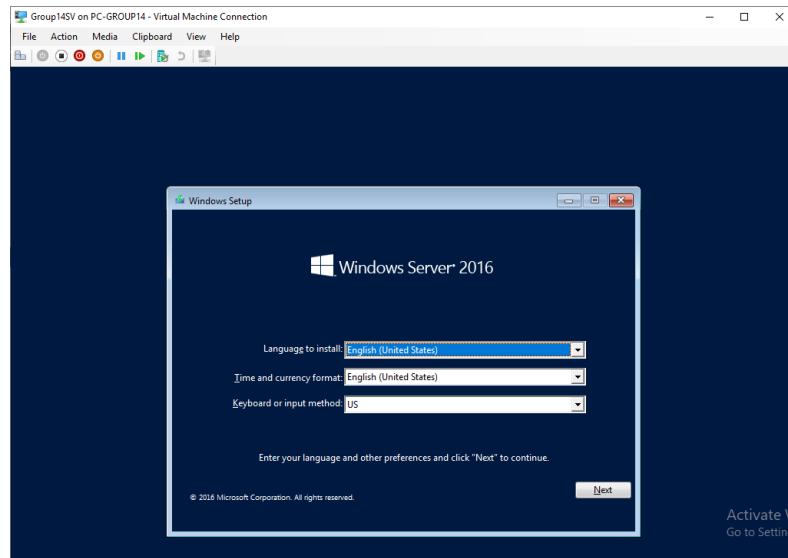


Figure 5. 73 : Group14SV Virtual Machine

**STEP 27 :** Open the Server Manager in the virtual machine and add roles. Then click next.

**STEP 28 :** Select Web Server(IIS) and add features. Then click next.

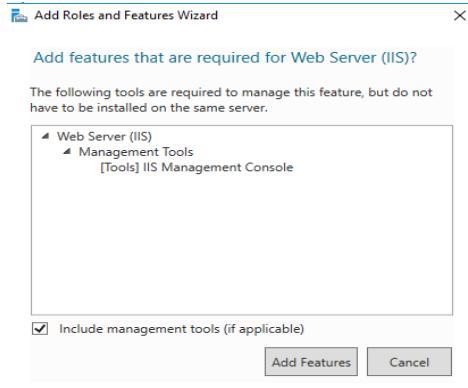


Figure 5. 74: Select Server Roles

**STEP 29 :** Select FTP server and click next.

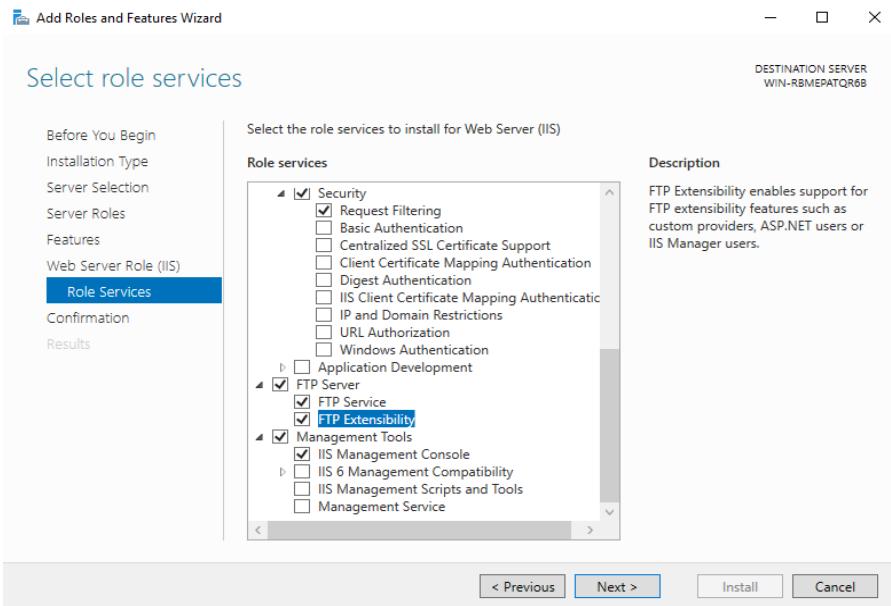


Figure 5. 75 : Select Role Services

**STEP 30 :** Click the install button to install the selection that have been made.

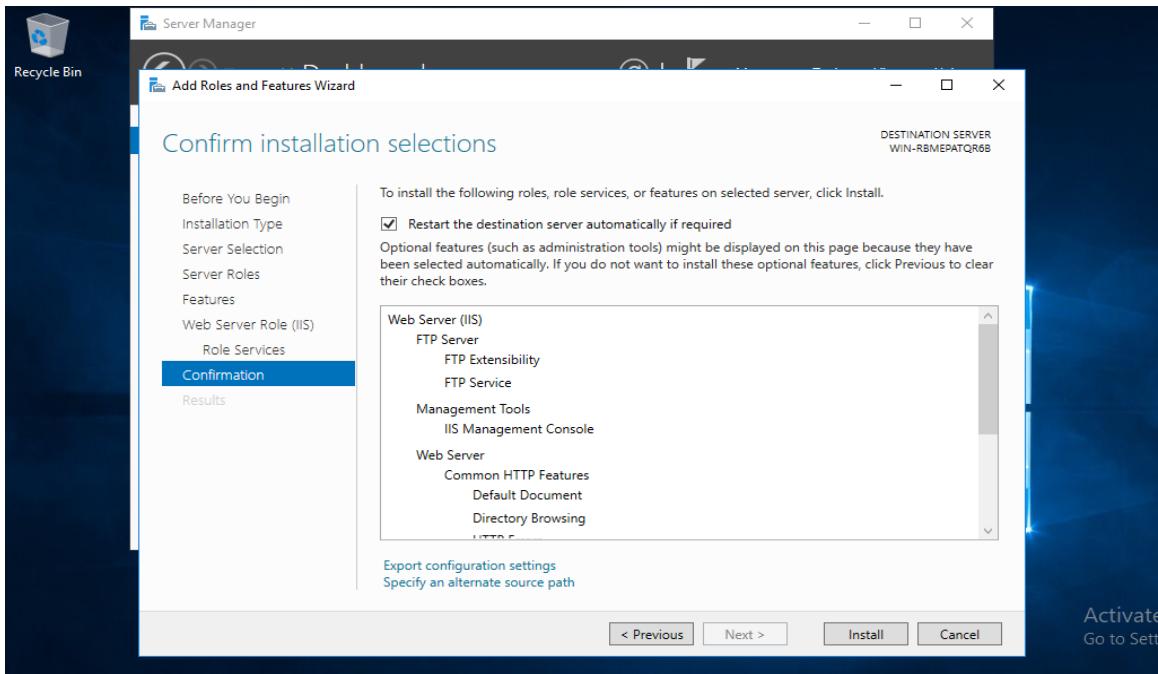


Figure 5. 76 : Confirm Installation Selections

**STEP 31 :** Go to tools and click Internet Information Services (IIS) Manager

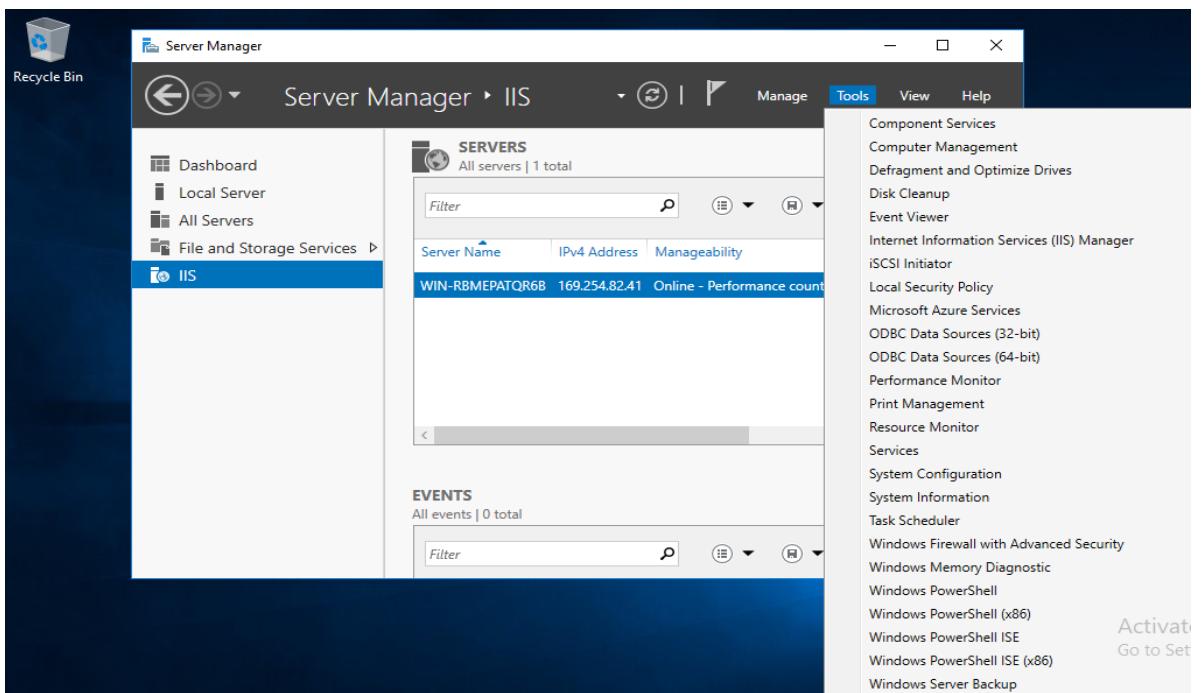


Figure 5. 77 : Server Manager

**STEP 32 : Click FTP authentication**

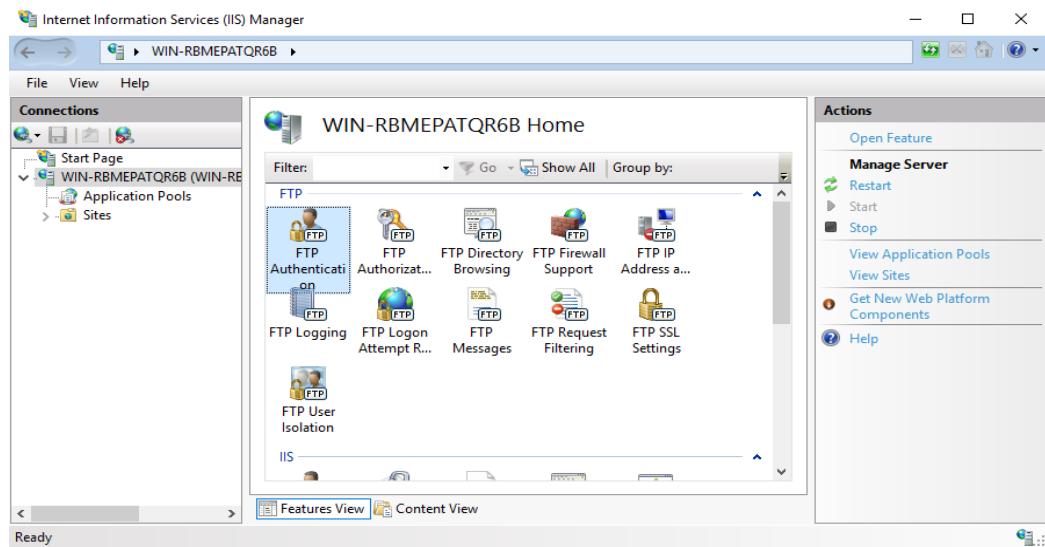


Figure 5. 78 : Internet Information Services (IIS) Manager

**STEP 33 : Enable the basic authentication**

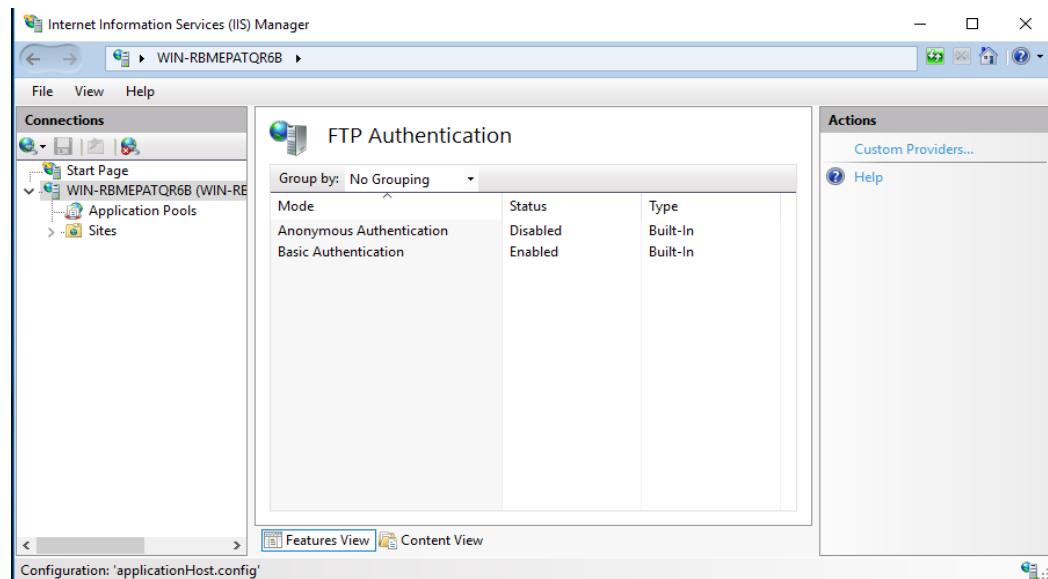


Figure 5. 79 : FTP Authentication

**STEP 34 :** Click FTP authorization rules

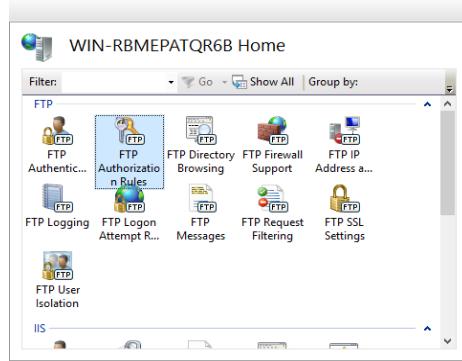


Figure 5. 80 : WIN-RBMEPARQR68 Home

**STEP 35 :** Add a new rule and choose specified users. Tick the read and write for the permission. Then click ok.

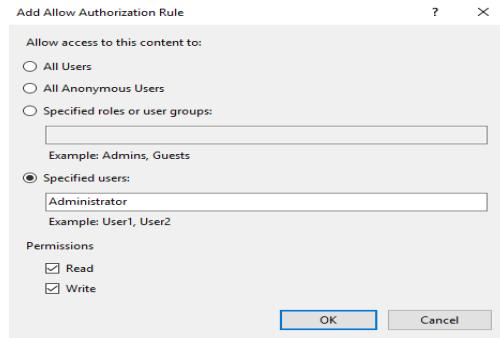


Figure 5. 81 : FTP Authorization Rules

**STEP 36 :** Go to sites, click add FTP site.

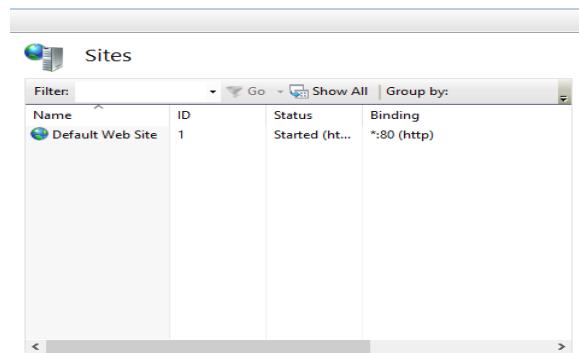


Figure 5. 82 : Sites

**STEP 37** : Set up the site information by entering the site name and physical path. Then click next.

**STEP 38** : Setting the site by set the ip address as all unassigned and port 21. for the SSL, tick No SSL. Then click next.

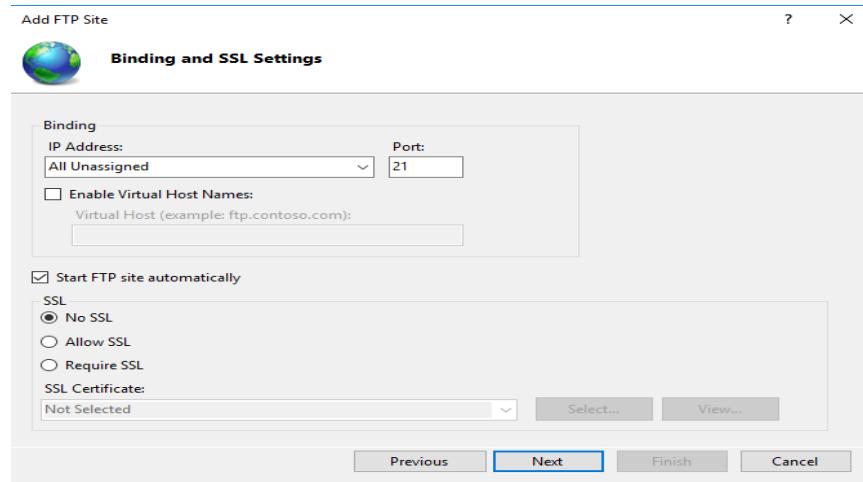


Figure 5. 83 : Binding and SSL Setting

**STEP 39** : For authentication, choose the basic one. For the authorization, choose specified users and tick both read and write for the permissions. Then click Finish.

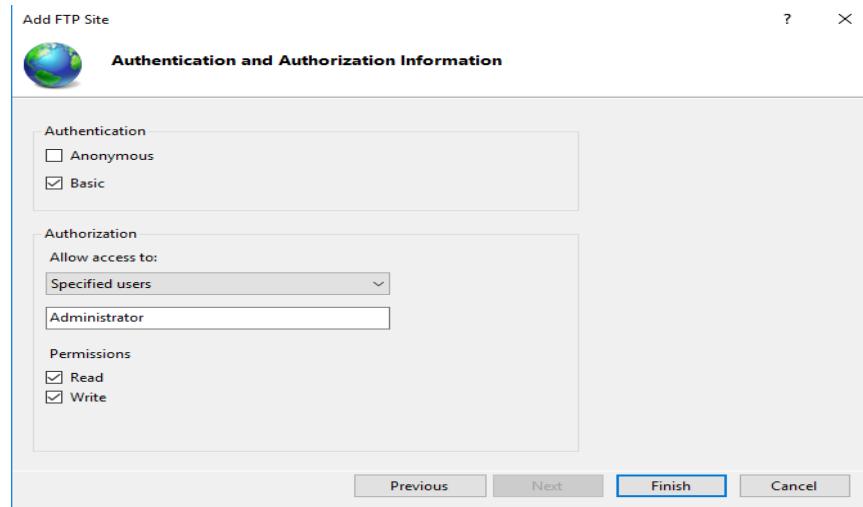


Figure 5. 84 : Authentication and Authorization Information

### 5.3.8 ACTIVE DIRECTORY

**STEP 1 :** Open the server manager and click manage. Then click add role and features to install ADDS server.

**STEP 2 :** Choose Active Directory and click add features.

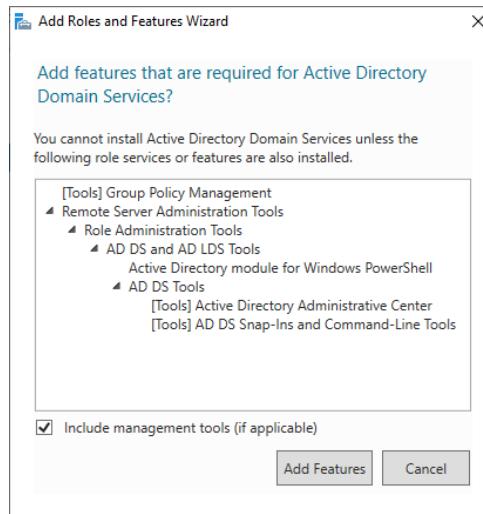


Figure 5. 85 : Add Roles and Features Wizard

**STEP 3 :** Make sure the active directory Domain services have been choose and click next.

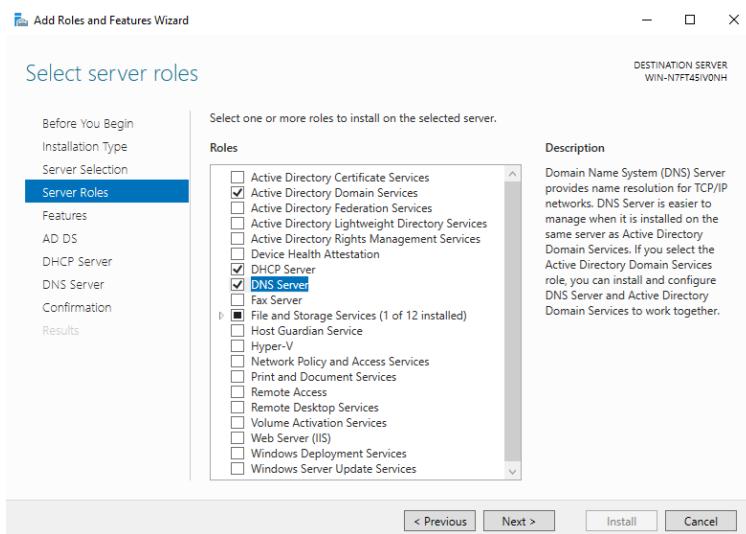
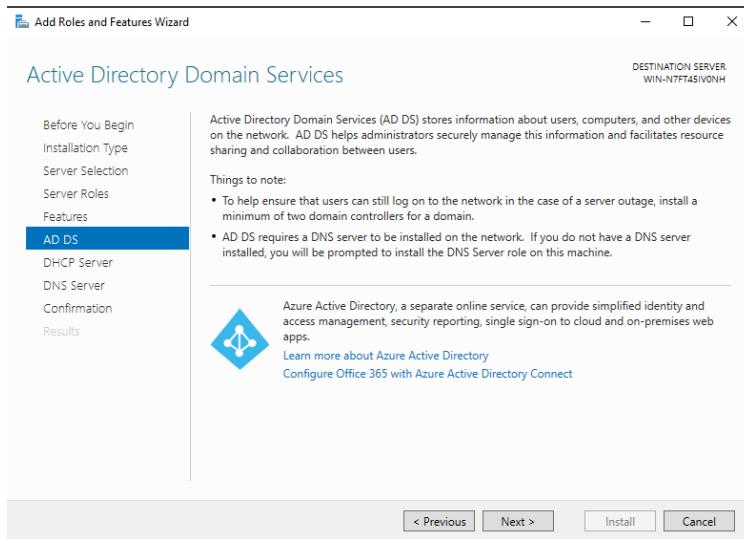


Figure 5. 86 : Select Server Roles

**STEP 4** : Then, click next until confirmation to install the server.

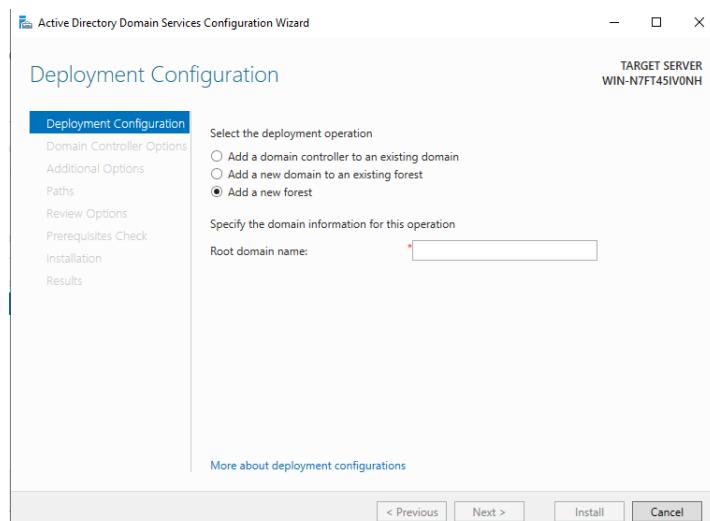


*Figure 5. 87 : Active Directory Domain Services*

**STEP 5** : Then, click install to install the server.

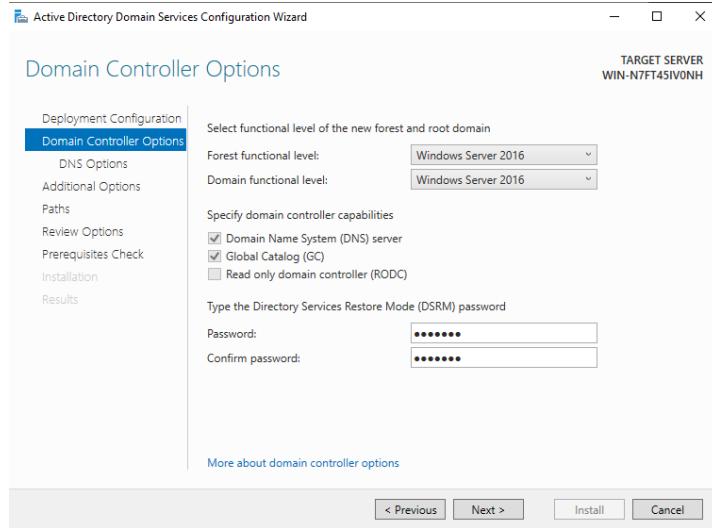
**STEP 6** : The installation is success.

**STEP 7** : After that, a ADDS Configuration Wizard will appear. Choose “Add a new forest” and insert the Root Domain Name. Then, click next.



*Figure 5. 88 : Deployment Configuration*

**STEP 8 :** In the domain controller options, insert a password and confirm password. Specify domain controller by tick the domain name system and global catalog. After that, click next.



*Figure 5. 89 : Domain Controller Options*

**STEP 9 :** In DNS options, just click next.

**STEP 10 :** After that, click install.

**STEP 11 :** After finish install, click close. Restart the system to complete the installation.

**STEP 12 :** After restart the system, open tools and click the active directory users and computers.

**STEP 13 :** Go to user, right click and choose “New > User”.

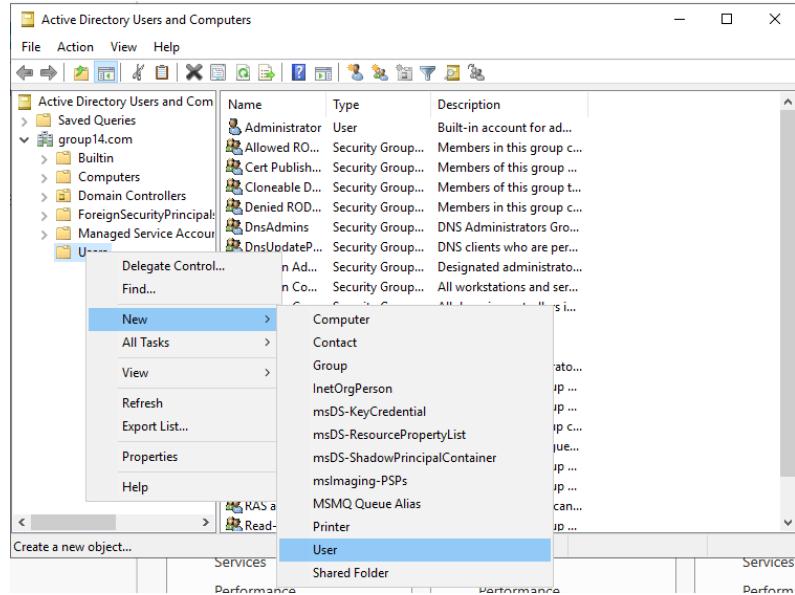


Figure 5. 90 : Active Directory Users and Computers

**STEP 14 :** After that, insert the first name, and the user logon name. Then click next.

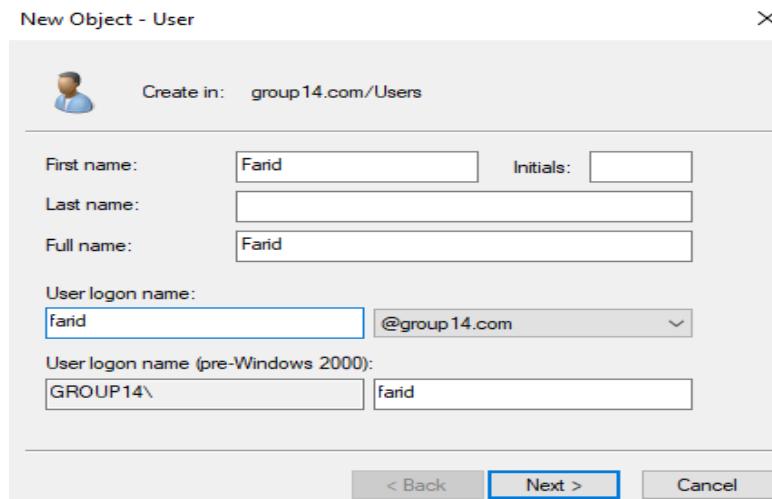


Figure 5. 91 : New Object - User

**STEP 15 :** Next, insert the password for the user. Pick password never expires and click next.

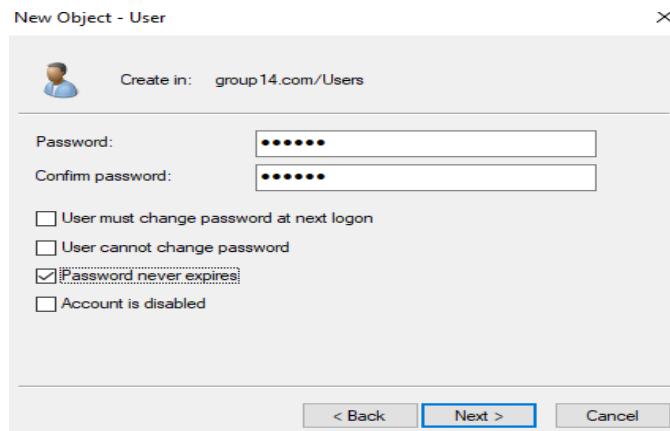


Figure 5. 92 : Password and Confirm Password

**STEP 16 :** Before created the object, check whether the information that were inserted are right. Then click finish.

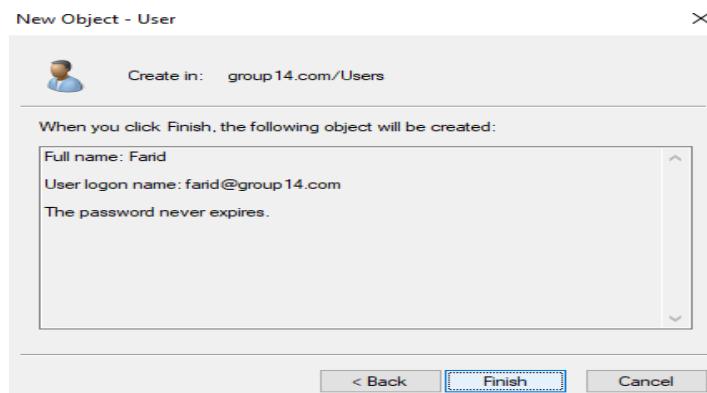


Figure 5. 93 : Information Before Created

**STEP 17 :** Right click at the user that has been created, choose add to group

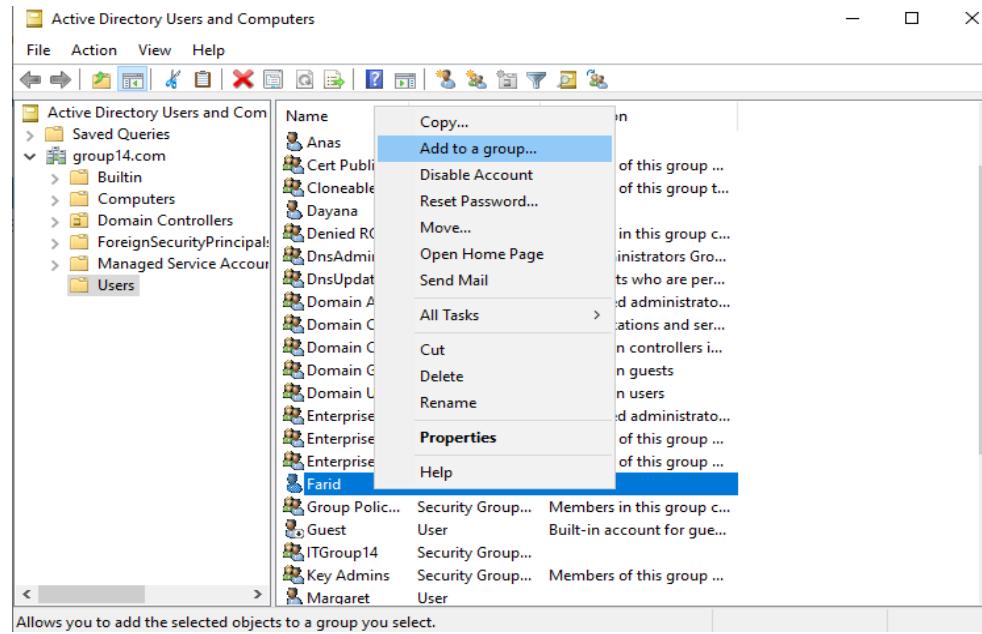


Figure 5. 94 : Add To a Group

**STEP 18 :** Insert the group that have been created and click check name. Then click ok.

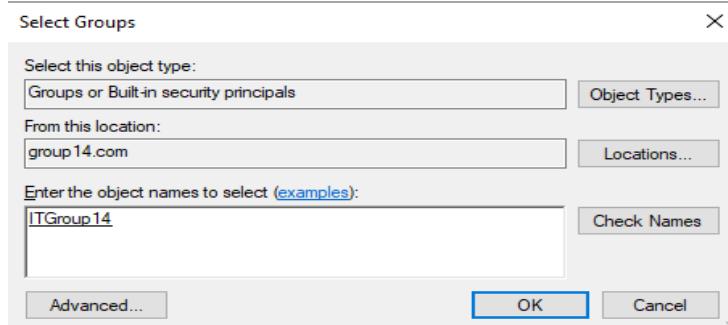


Figure 5. 95 : Select Groups

**STEP 19 :** A message will appear. Then click ok.



Figure 5. 96 : ADDS message

## Group Policy Object :

**STEP 1 :** Open the Group Policy Management in Server Manager. Then, go to Group Policy Management Editor.

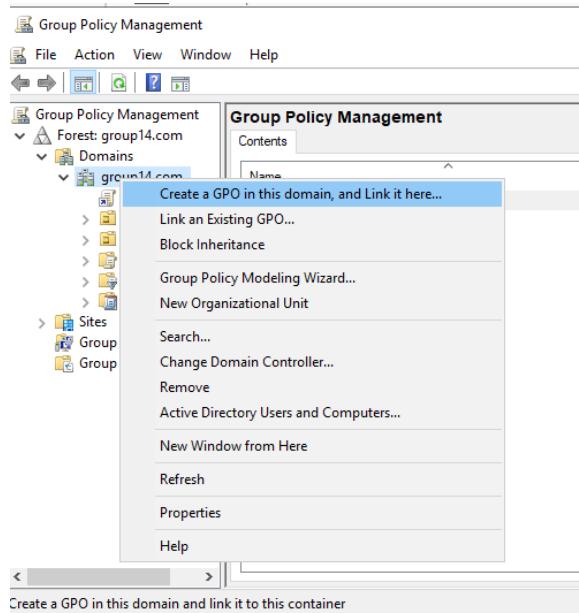


Figure 5. 97 : Group Policy Management

**STEP 2 :** Click the User Configuration > Policies > Administrator Templates : Policies > Desktop. Pick any policy to be edit. For example “Remove Recycle Bin Icon from desktop”. Click enable, apply and OK.

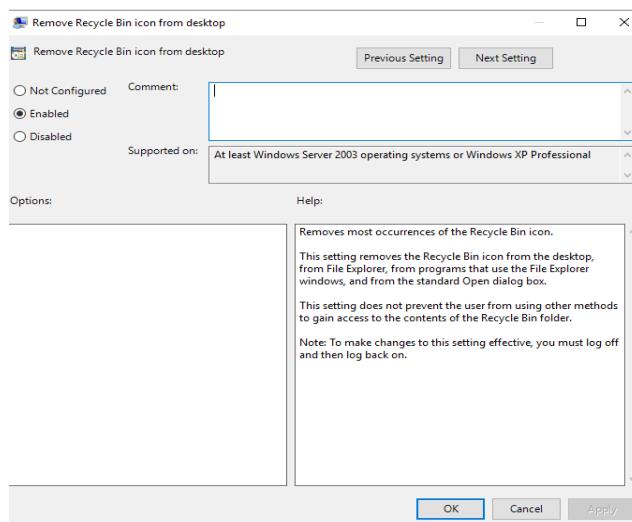


Figure 5. 98 : Group Policy Management Editor

**STEP 3 :** After enable the policy that have been made, go to Group Policy Management, Click Group Policy Object and click the group GPO that have created. From that, we can see the policy have been enabled.

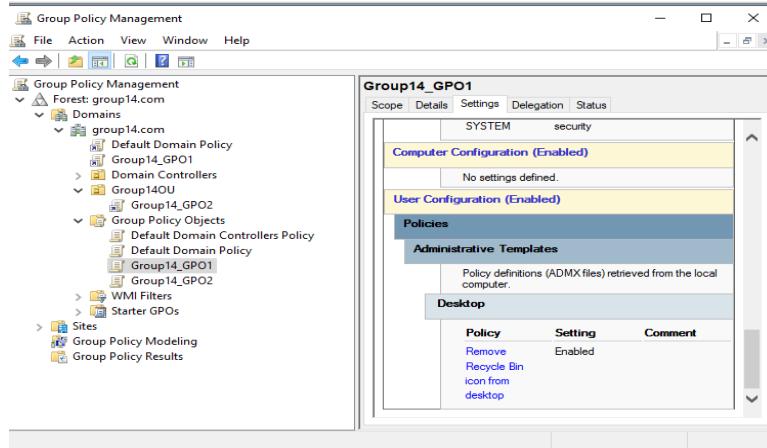


Figure 5. 99 : Policy Created

**STEP 4 :** Open command prompt and insert command line “gpupdate.exe /force /boot /logoff to finish the setting. This command need to be used to update the group policy management editor.

```

Administrator: Command Prompt
Sync
Causes the next foreground policy application to
be done synchronously. Foreground policy
applications occur at computer start up and user
logon. You can specify this for the user,
computer or both using the /target parameter.
The /Force and /Wait parameters will be ignored
if specified.

C:\Users\Administrator>gpupdate.exe /force /boot /logoff
Updating policy...
Computer Policy update has completed successfully.
User Policy update has completed successfully.

C:\Users\Administrator>

```

Figure 5. 100 : gpupdate Force

### 5.3.9 WIRELESS USER AUTHENTICATION USING RADIUS SERVER

**STEP 1 :** create a new group for the wireless user which is Wireless\_Group14. Set group scope as global. Set the group type as security. Then click ok.

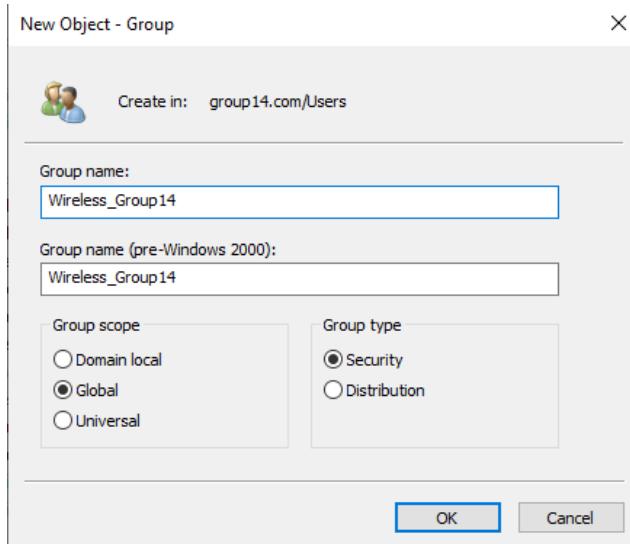


Figure 5. 101 : Active Directory Users and Computers

**STEP 2 :** assign all the user that have been created into the wireless group. Click ok.

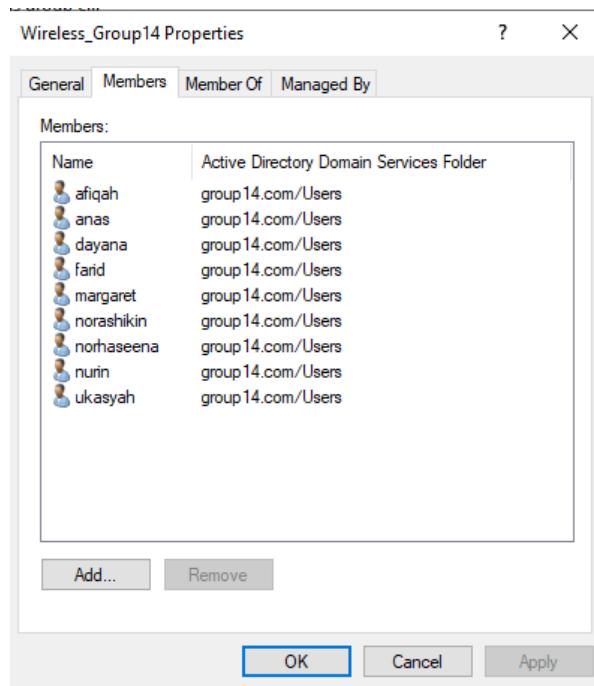


Figure 5. 102 : Wireless\_Group14 properties

**STEP 3 :** configure the network policy server. Select the configuration scenario as radius server for 802.1x wireless or wired connections. Then click configure 802.1x.

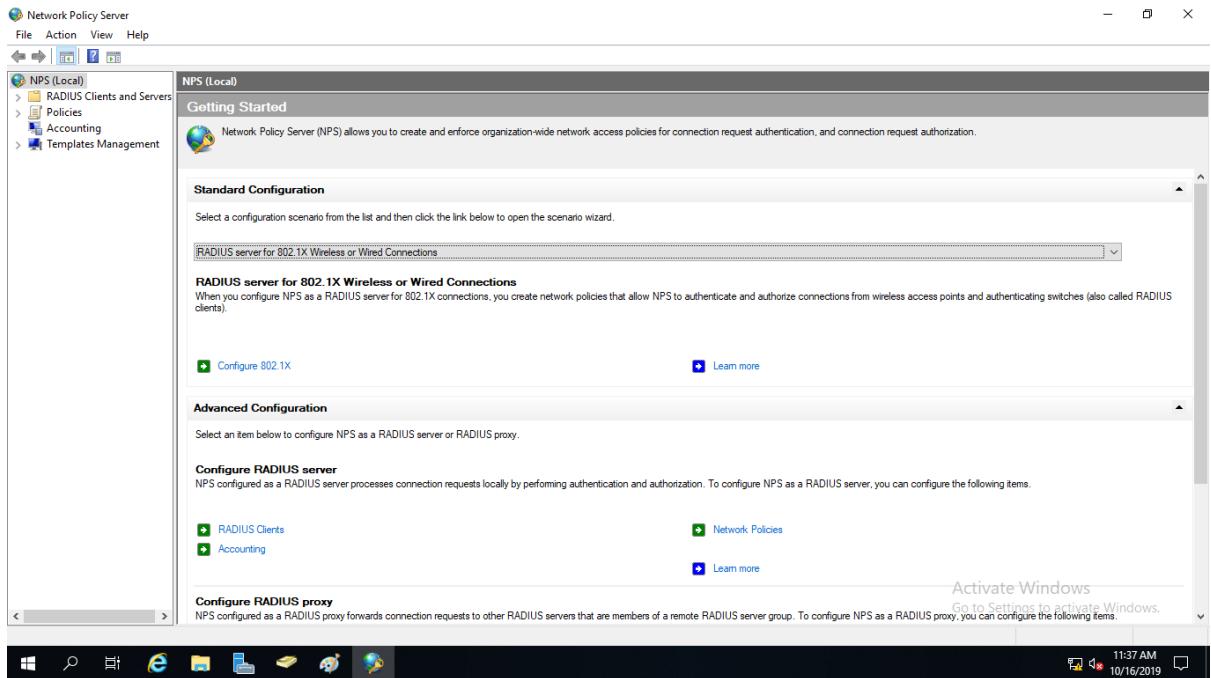


Figure 5. 103 : Network Policy Server

**STEP 4 :** select the type of 802.1x connections as secure wireless connections. Then click next.

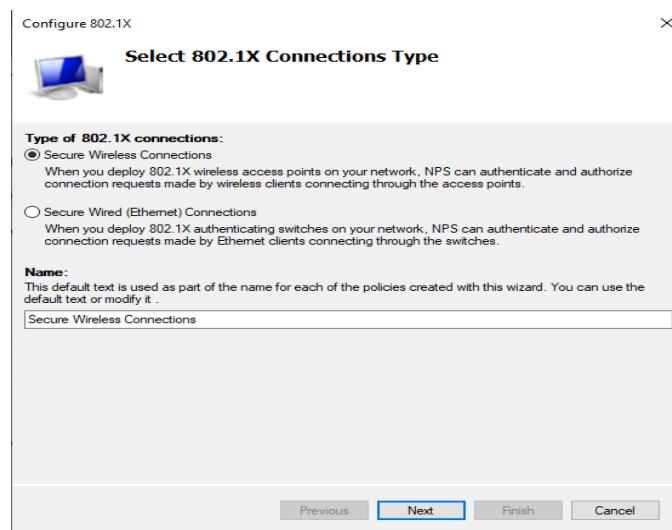


Figure 5. 104 : Select 802.1x Connection Type

**STEP 5** : create new radius client and click ok.

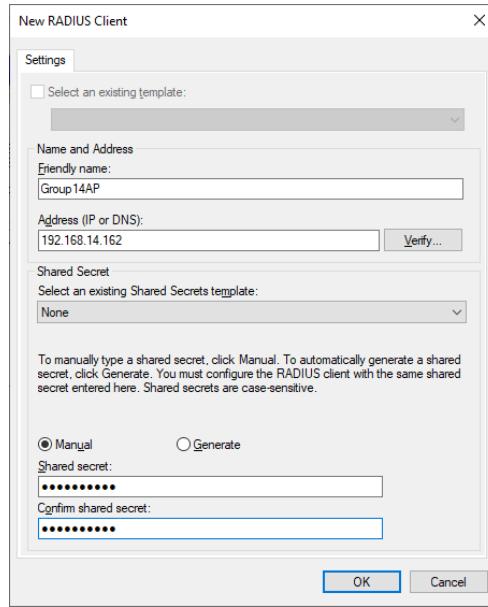


Figure 5. 105 : New Radius Client

**STEP 6** : set the configure authentication method as Microsoft protected EAP (PEAP).

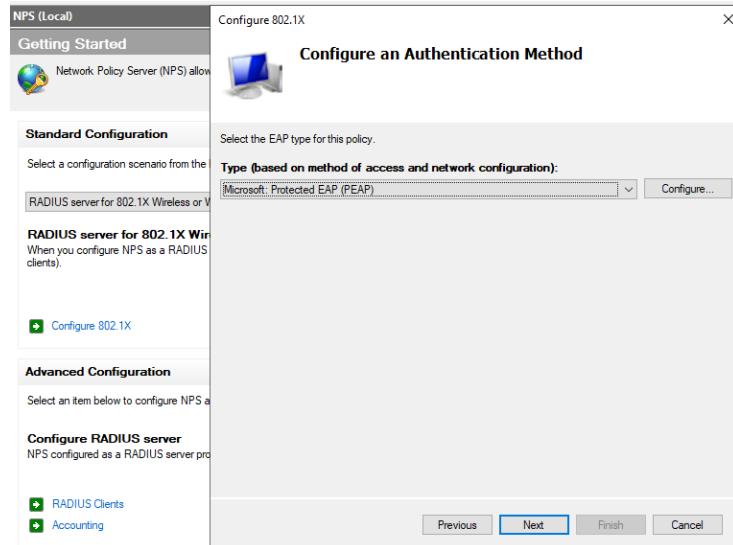
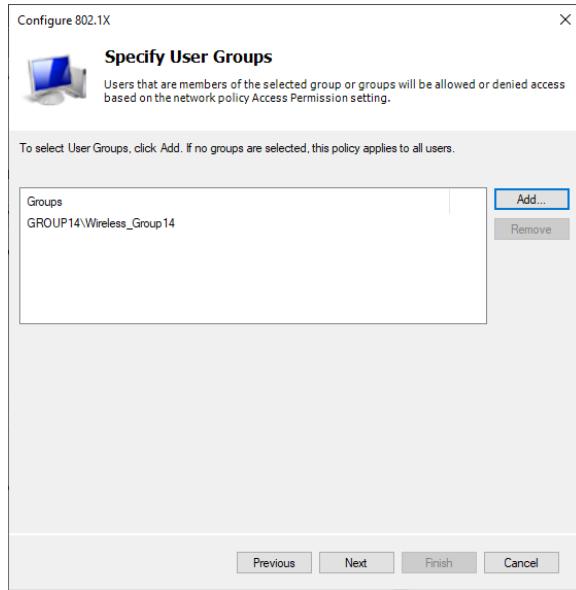


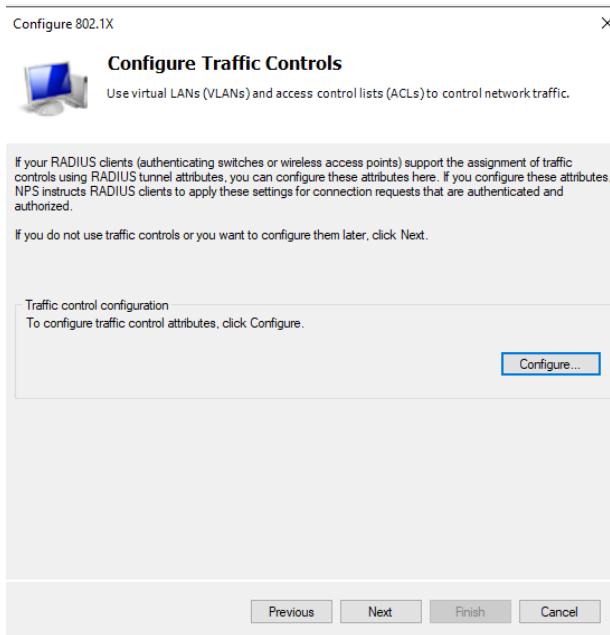
Figure 5. 106 : Configuration an Authentication Method

**STEP 7** : specify user groups by adding the wireless group created in the active directory and computer and click next.



*Figure 5. 107 : Specify User Group*

**STEP 8** : click next to finish the configuration.



*Figure 5. 108 : Configuration Traffic Controls*

**STEP 9 :** check the configuration if it is configure in the right way. Click finish.

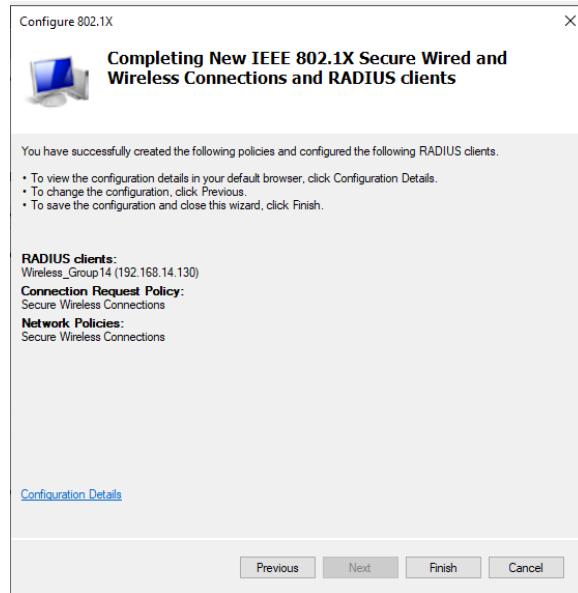


Figure 5. 109: Successful configure the Radius Client

**STEP 10 :** check whether the radius client for wireless is enable or not.

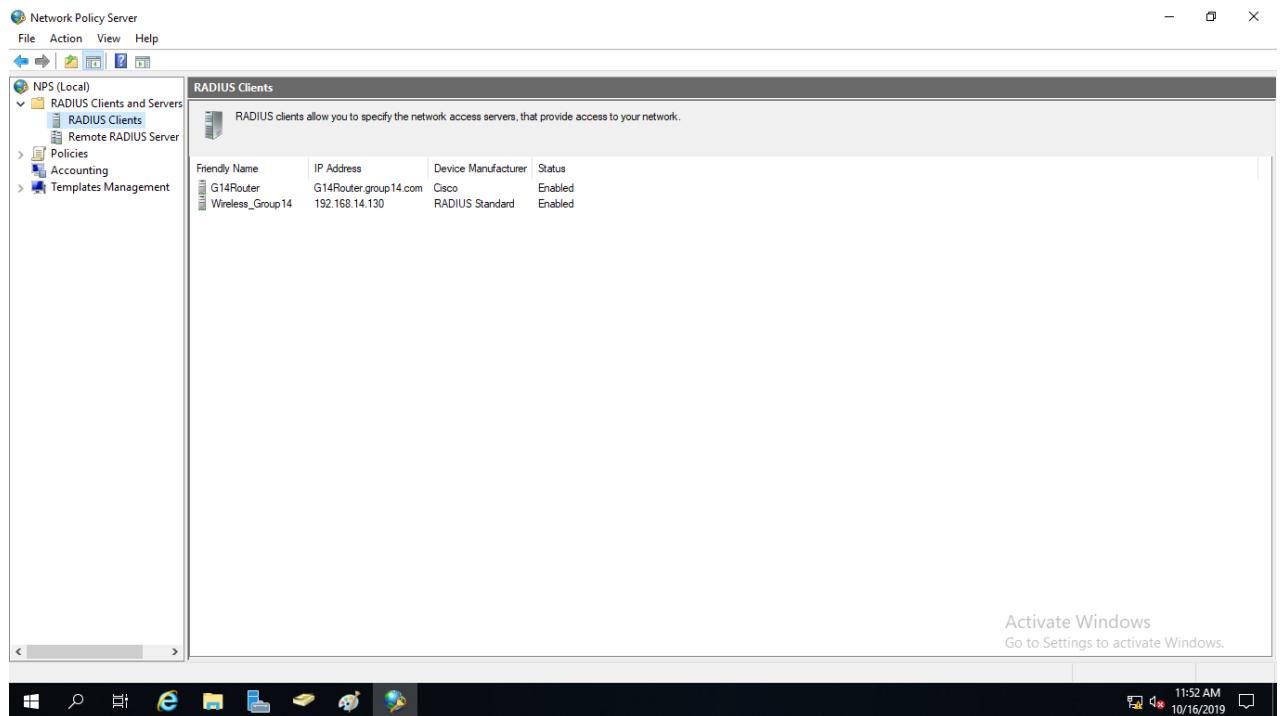
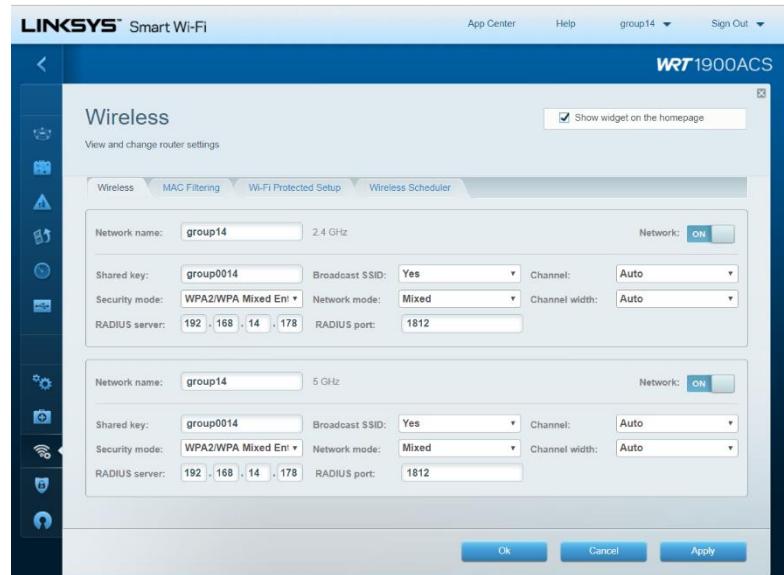


Figure 5. 110: Radius Client

**STEP 11 :** Configure the access point (192.168.14.162).

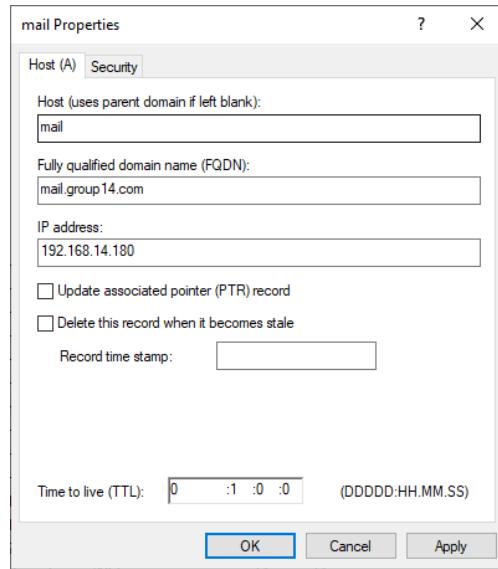


*Figure 5. 111 : Linksys Smart Wi-Fi Interface*

### **5.3.10 LINUX MAIL SERVER INSTALLING AND CONFIGURING POSTFIX**

**STEP 1.** Installing and configuring Postfix

**STEP 2.** Right click on group14.com option and choose new host then configure as picture below.



*Figure 5. 112: create host*

**STEP 3:** On Debian, open terminal and enter into root and perform an update for system.

```
su --
```

```
Group42019
```

```
apt update
```

```
group14@Group14:~$ su -
Password:
root@group14:~# apt update
Ign: http://ftp.us.debian.org/debian stretch InRelease
Hit: http://security.debian.org/debian-security stretch/updates InRelease
Hit:3 http://ftp.us.debian.org/debian stretch-updates InRelease
Hit:4 http://ftp.us.debian.org/debian stretch Release
Reading package lists... Done
Building dependency tree
Reading state information... Done
7 packages can be upgraded. Run 'apt list --upgradable' to see them.
root@Group14:~#
```

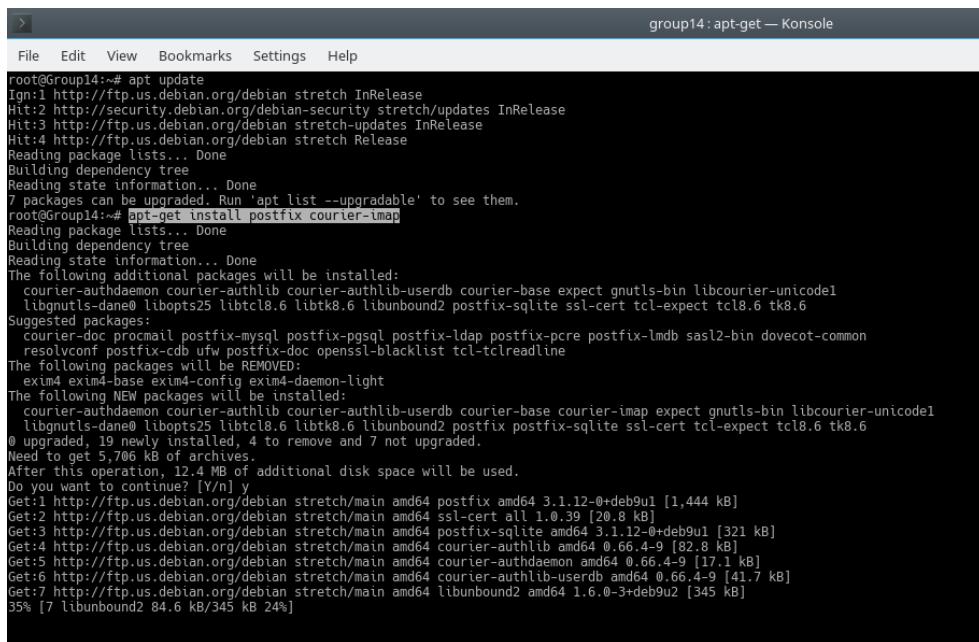
A screenshot of a terminal window titled 'group14:bash — Konsole'. The window shows a command-line session where the user runs 'su -' to become root, followed by 'apt update'. The output shows standard apt update progress: ignoring the main Debian mirror, hitting security.debian.org for updates, and hitting the local mirrors for stretch-updates and stretch releases. It concludes by stating that 7 packages can be upgraded and asks the user to run 'apt list --upgradable' to see them.

Figure 5. 113 : System Update

**STEP 4:** Install Postfix

```
apt-get install postfix courier-imap
```

```
y
```



```
group14:apt-get — Konsole
File Edit View Bookmarks Settings Help
root@group14:~# apt update
Ign:1 http://ftp.us.debian.org/debian stretch InRelease
Hit:2 http://security.debian.org/debian-security stretch/updates InRelease
Hit:3 http://ftp.us.debian.org/debian stretch-updates InRelease
Hit:4 http://ftp.us.debian.org/debian stretch Release
Reading package lists... Done
Building dependency tree
Reading state information... Done
7 packages can be upgraded. Run 'apt list --upgradable' to see them.
root@group14:~# apt-get install postfix courier-imap
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  courier-authdaemon courier-authlib courier-authlib-userdb courier-base expect gnutls-bin libcourier-unicodel
  libgnutls-dane0 libiptc25 libtcl8.6 libtunbound2 postfix-sqlite ssl-cert tcl-expect tcl8.6 tk8.6
Suggested packages:
  courier-doc procmail postfix-mysql postfix-pgsql postfix-ldap postfix-pcre postfix-lmdb sasl2-bin dovecot-common
  resolvconf postfix-cdb ufw postfix-doc openssh-blacklist tcl-tclreadline
The following packages will be REMOVED:
  exim4 exim4-base exim4-config exim4-daemon-light
The following NEW packages will be installed:
  courier-authdaemon courier-authlib courier-authlib-userdb courier-base courier-imap expect gnutls-bin libcourier-unicodel
  libgnutls-dane0 libiptc25 libtcl8.6 libtk8.6 libtunbound2 postfix postfix-sqlite ssl-cert tcl-expect tcl8.6 tk8.6
0 upgraded, 19 newly installed, 4 to remove and 7 not upgraded.
Need to get 5,706 kB of archives.
After this operation, 12.4 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://ftp.us.debian.org/debian stretch/main amd64 postfix amd64 3.1.12-0+deb9u1 [1,444 kB]
Get:2 http://ftp.us.debian.org/debian stretch/main amd64 ssl-cert all 1.0.39 [20.8 kB]
Get:3 http://ftp.us.debian.org/debian stretch/main amd64 postfix-sqlite amd64 3.1.12-0+deb9u1 [321 kB]
Get:4 http://ftp.us.debian.org/debian stretch/main amd64 courier-authlib amd64 0.66.4-9 [82.8 kB]
Get:5 http://ftp.us.debian.org/debian stretch/main amd64 courier-authdaemon amd64 0.66.4-9 [17.1 kB]
Get:6 http://ftp.us.debian.org/debian stretch/main amd64 courier-authlib-userdb amd64 0.66.4-9 [41.7 kB]
Get:7 http://ftp.us.debian.org/debian stretch/main amd64 libtunbound2 amd64 1.6.0-3+deb9u2 [345 kB]
35% [7 libtunbound2 84.6 kB/345 kB 24%]
```

Figure 5. 114 : Installing Postfix

**5.3.11.1 CONFIGURING COURIER**

**STEP 1:** Click ok

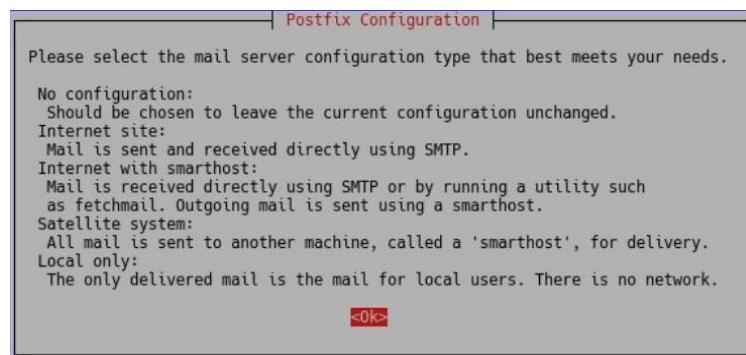


Figure 5. 115 : Directories Web Based

**STEP 2:** During installation, you will be asked to **choose** the type **of mail configuration**, choose “**Internet Site**”.

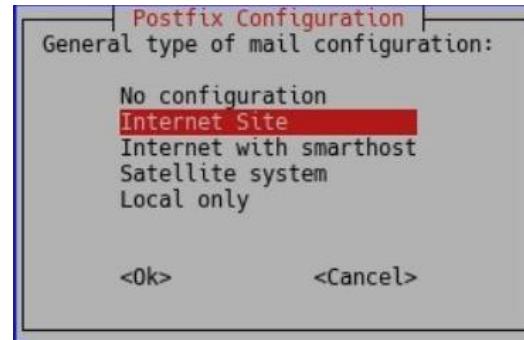


Figure 5. 116: Directories Web Based II

**STEP 3:** Enter system mail name then click ok

**STEP 4:** Install **apache2** and **php**

```
apt install apache2 php7.0 libapache2-mod-php7.0
```

A screenshot of a terminal window titled "group14: apt — Konsole". The window shows the command "apt install apache2 php7.0 libapache2-mod-php7.0" being run. The output indicates that the operation will free 592 kB of disk space. It shows the removal of apache2 (2.4.25-3+deb9u8), processing triggers for man-db (2.7.6.1-2), purging configuration files for apache2 (2.4.25-3+deb9u8), processing triggers for systemd (232-25+deb9u12), and installing apache2, php7.0, libapache2-mod-php7.0. It also lists suggested packages like apache2-doc and apache2-suexec-pristine. The terminal ends with a prompt "Do you want to continue? [Y/n]".

Figure 5. 117: Installation apache2 and php

## **STEP 5:** Checking apache2 and php version

apache2 -v

**php -v**

```
root@Group14:~# apache2 -v
Server version: Apache/2.4.25 (Debian)
Server built:   2019-08-19T19:25:31
root@Group14:~# php -v
PHP 7.0.33-0+deb9u5 (cli) (built: Sep 18 2019 09:55:34) ( NTS )
Copyright (c) 1997-2017 The PHP Group
Zend Engine v3.0.0, Copyright (c) 1998-2017 Zend Technologies
    with Zend OPcache v7.0.33-0+deb9u5, Copyright (c) 1999-2017, by Zend Technologies
root@Group14:~#
```

*Figure 5. 118 : Checking version apache2 and php*

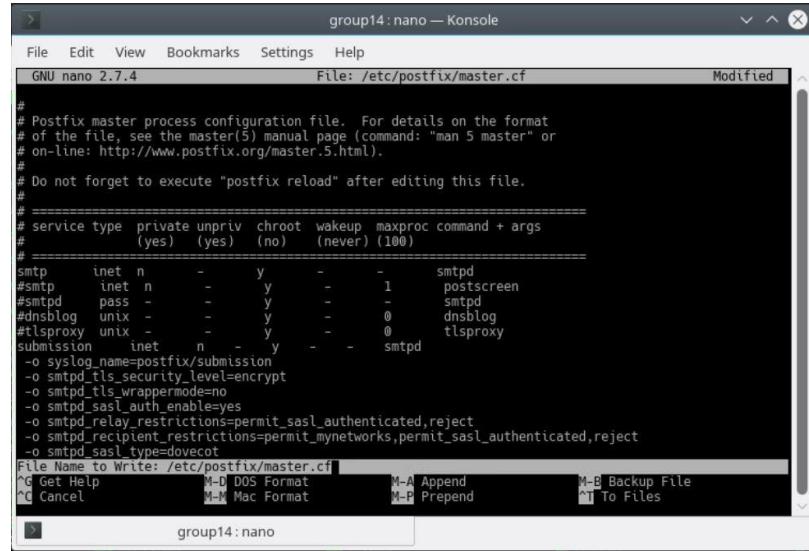
**STEP 6:** After installation enter country name, state & email address.

```
group14: bash — Konsole
File Edit View Bookmarks Settings Help
root@Group14:~# openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/group14.key -out /etc/ssl/certs/group14.pem
Generating a RSA private key
.....+++++
.....+++++
writing new private key to '/etc/ssl/private/group14.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:MY
State or Province Name (full name) [Some-State]:Melaka
Locality Name (eg, city) []:Durian Tunggal
Organization Name (eg, company) [Internet Widgits Pty Ltd]:UTeM
Organizational Unit Name (eg, section) []:ftmk
Common Name (e.g. server FQDN or YOUR name) []:mail@group14.com
Email Address []:mail@group14.com
root@Group14:~#
```

*Figure 5. 119 : Set Information*

**STEP 7:** To send emails from a desktop email client, enable the submission service of Postfix so that the email client can submit emails to Postfix SMTP server. Edit the master.cf file

```
nano /etc/postfix/master.cf
```

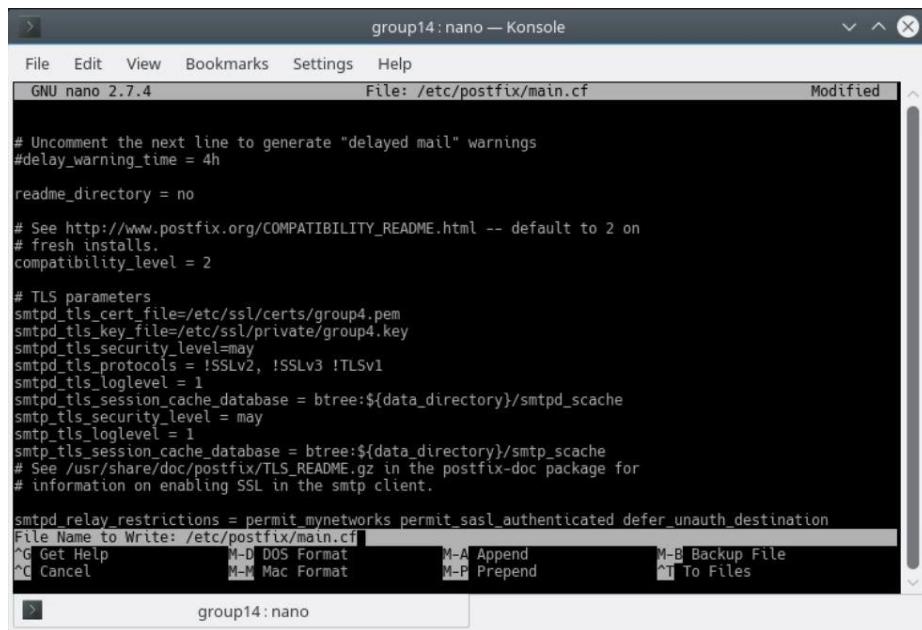


```
# Postfix master process configuration file. For details on the format
# of the file, see the master(5) manual page (command: "man 5 master" or
# on-line: http://www.postfix.org/master.5.html).
#
# Do not forget to execute "postfix reload" after editing this file.
#
# =====
# service type private unpriv chroot wakeup maxproc command + args
#           (yes)  (yes)  (no)   (never) (100)
# =====
smtp      inet  n   -y    -     -       smtpd
#smtp      inet  n   -y    -     1       postscreen
#smtpd     pass  -   -y    -     -       smtpd
#dnsblog   unix  -   -y    -     0       dnsblog
#tlsproxy  unix  -   -y    -     0       tlsproxy
submission inet  n   -y    -     -       smtpd
-o syslog_name=postfix/submission
-o smtpd_tls_security_level=encrypt
-o smtpd_tls_wrappermode=no
-o smtpd_sasl_auth_enable=yes
-o smtpd_relay_restrictions=permit_sasl_authenticated,reject
-o smtpd_recipient_restrictions=permit_mynetworks,permit_sasl_authenticated,reject
-o smtpd_sasl_type=dovecot
```

Figure 5. 120 : Edit master.cf

**STEP 8:** Next, let Postfix know where TLS certificate and private key are. Edit main.cf file.

```
nano /etc/postfix/main.cf
```



```
# Uncomment the next line to generate "delayed mail" warnings
#delay_warning_time = 4h

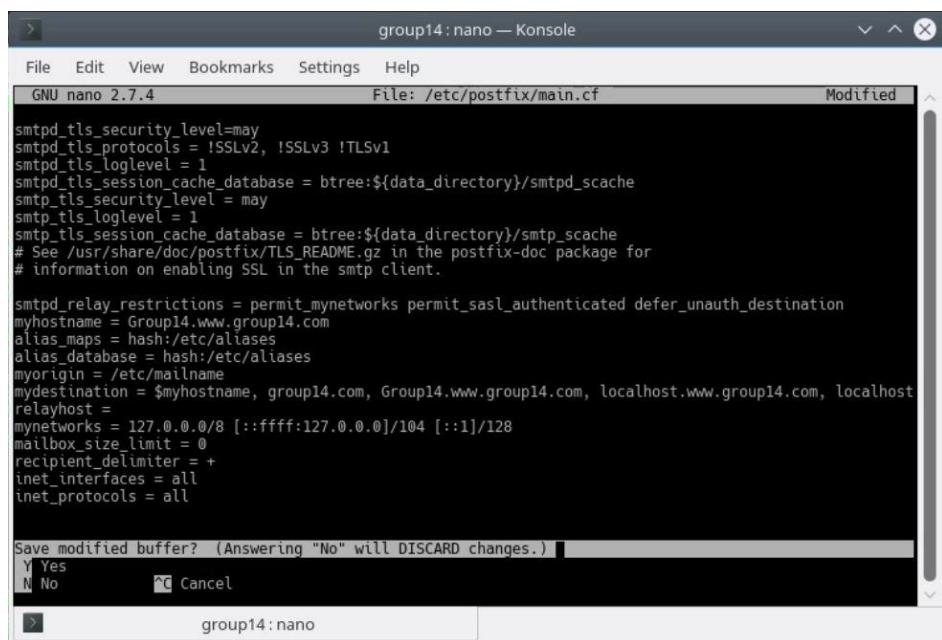
readme_directory = no

# See http://www.postfix.org/COMPATIBILITY_README.html -- default to 2 on
# fresh installs.
compatibility_level = 2

# TLS parameters
smtpd_tls_cert_file=/etc/ssl/certs/group4.pem
smtpd_tls_key_file=/etc/ssl/private/group4.key
smtpd_tls_security_level=may
smtpd_tls_protocols = !SSLv2, !SSLv3 !TLSv1
smtpd_tls_loglevel = 1
smtpd_tls_session_cache_database = btree:${data_directory}/smtpd_scache
smtp_tls_security_level = may
smtp_tls_loglevel = 1
smtp_tls_session_cache_database = btree:${data_directory}/smtp_scache
# See /usr/share/doc/postfix/TLS_README.gz in the postfix-doc package for
# information on enabling SSL in the smtp client.

smtpd_relay_restrictions = permit_mynetworks permit_sasl_authenticated defer_unauth_destination
File Name to Write: /etc/postfix/main.cf
^G Get Help      M-D DOS Format      M-A Append      M-B Backup File
^C Cancel        M-M Mac Format      M-P Prepend    ^T To Files
```

Figure 5. 121 : Edit main.cf



```
smtpd_tls_security_level=may
smtpd_tls_protocols = !SSLv2, !SSLv3 !TLSv1
smtpd_tls_loglevel = 1
smtpd_tls_session_cache_database = btree:${data_directory}/smtpd_scache
smtp_tls_security_level = may
smtp_tls_loglevel = 1
smtp_tls_session_cache_database = btree:${data_directory}/smtp_scache
# See /usr/share/doc/postfix/TLS_README.gz in the postfix-doc package for
# information on enabling SSL in the smtp client.

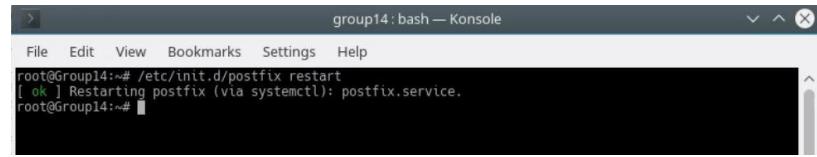
smtpd_relay_restrictions = permit_mynetworks permit_sasl_authenticated defer_unauth_destination
myhostname = Group14.www.group14.com
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
myorigin = /etc/mailname
mydestination = $myhostname, group14.com, Group14.www.group14.com, localhost.www.group14.com, localhost
relayhost =
mynetworks = 127.0.0.0/8 [::ffff:127.0.0.0]/104 [:1]/128
mailbox_size_limit = 0
recipient_delimiter = +
inet_interfaces = all
inet_protocols = all

Save modified buffer? (Answering "No" will DISCARD changes.)
Y Yes      N No      ^C Cancel
```

Figure 5. 122: Edit main.cf II

## **STEP 9:** Restart postfix

/etc/init.d/postfix restart



```
group14:bash — Konsole
File Edit View Bookmarks Settings Help
root@Group14:~# /etc/init.d/postfix restart
[ ok ] Restarting postfix (via systemctl): postfix.service.
root@Group14:~#
```

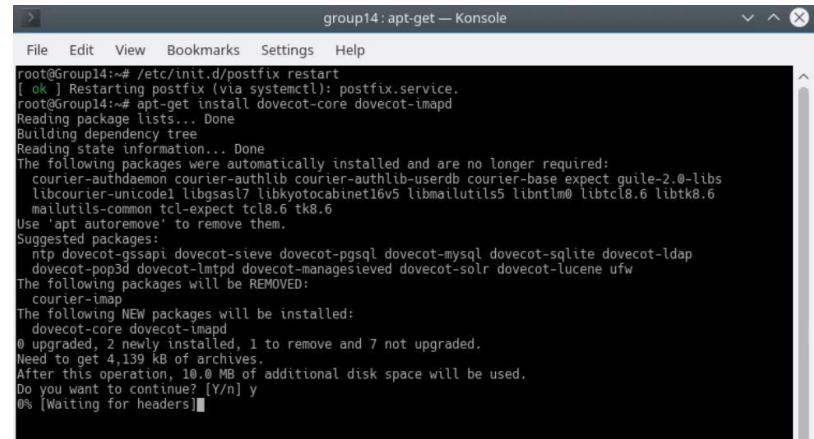
*Figure 5. 123 : Restarting postfix*

### **5.3.11.2 INSTALLING AND CONFIGURING DOVECOT IMAP SERVER**

#### **INSTALLING DOVECOT IMAP SERVER**

##### **STEP 1:** Install the Dovecot service.

apt-get install dovecot-core dovecot-imapd



```
group14:apt-get — Konsole
File Edit View Bookmarks Settings Help
root@Group14:~# /etc/init.d/postfix restart
[ ok ] Restarting postfix (via systemctl): postfix.service.
root@Group14:~# apt-get install dovecot-core dovecot-imapd
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
courier-authdaemon courier-authlib courier-authlib-userdb courier-base expect guile-2.0-libs
libcourier-unicodel libgsasl7 libkyotocabinet16v5 libmailutils5 libnl1 libtcl8.6 libtk8.6
mailutils-common tcl-expect tk8.6 tk8.6
Use 'apt autoremove' to remove them.
Suggested packages:
ntp dovecot-ssapi dovecot-sieve dovecot-pgsql dovecot-mysql dovecot-sqlite dovecot-ldap
dovecot-pop3d dovecot-lmtpd dovecot-managesieved dovecot-solr dovecot-lucene ufw
The following packages will be REMOVED:
courier-imap
The following NEW packages will be installed:
dovecot-core dovecot-imapd
0 upgraded, 2 newly installed, 1 to remove and 7 not upgraded.
Need to get 4,139 kB of archives.
After this operation, 10.0 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
0% [Waiting for headers]
```

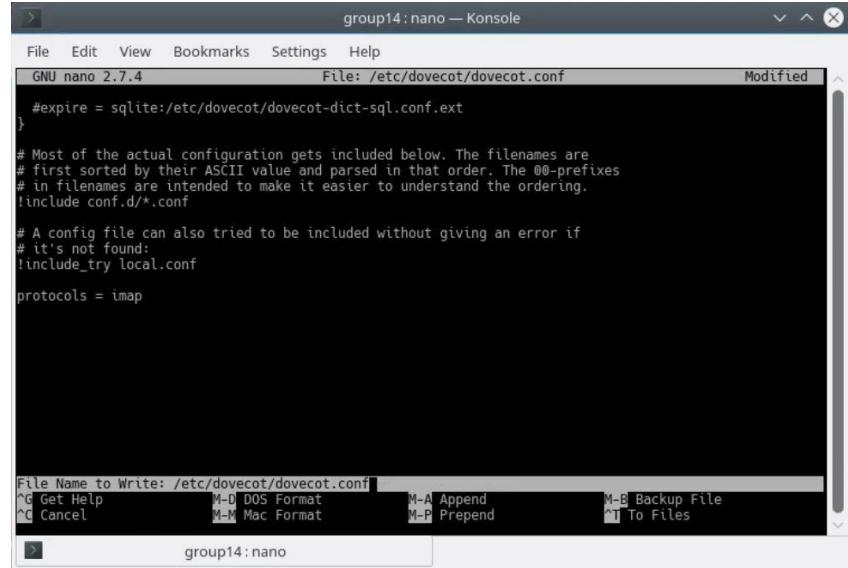
*Figure 5. 124 : Installing Dovecot*

## **CONFIGURING DOVECOT**

##### **STEP 1:** First, edit main configuration file and add the following line to enable IMAP protocol.

nano /etc/dovecot/dovecot.conf

protocols = imap



```
group14:nano — Konsole
File Edit View Bookmarks Settings Help
GNU nano 2.7.4 File: /etc/dovecot/dovecot.conf Modified
#expire = sqlite:/etc/dovecot/dovecot-dict-sql.conf.ext
}
# Most of the actual configuration gets included below. The filenames are
# first sorted by their ASCII value and parsed in that order. The 00-prefixes
# in filenames are intended to make it easier to understand the ordering.
!include conf.d/*.conf

# A config file can also tried to be included without giving an error if
# it's not found:
!include_try local.conf

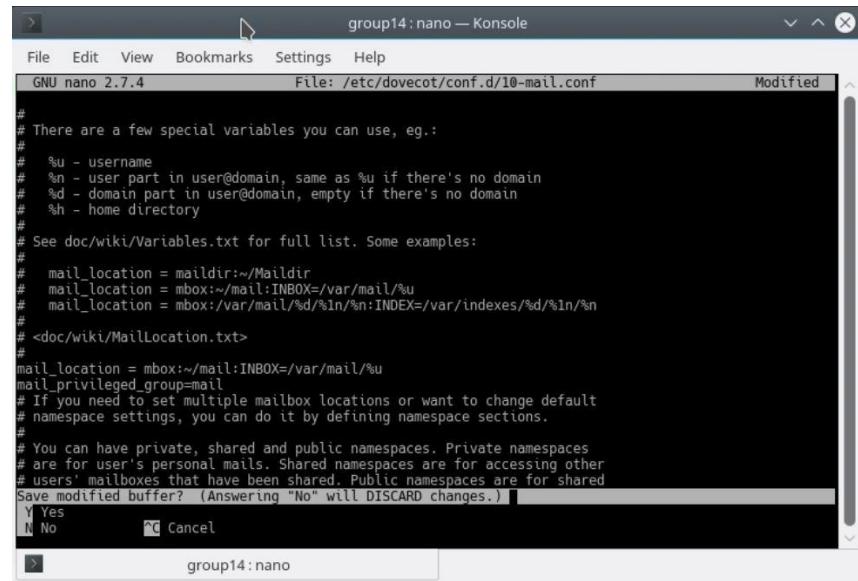
protocols = imap
```

Figure 5. 125 : Edit dovecot.conf

### 5.3.11.3 CONFIGURING MAILBOX LOCATION

**STEP 1:** The config file for mailbox location

nano /etc/dovecot/conf.d/10-mail.conf



```
group14:nano — Konsole
File Edit View Bookmarks Settings Help
GNU nano 2.7.4 File: /etc/dovecot/conf.d/10-mail.conf Modified
#
# There are a few special variables you can use, eg.:
#
# %u - username
# %n - user part in user@domain, same as %u if there's no domain
# %d - domain part in user@domain, empty if there's no domain
# %h - home directory
#
# See doc/wiki/Variables.txt for full list. Some examples:
#
# mail_location = maildir:~/Maildir
# mail_location = mbox:~/mail:INBOX=/var/mail/%u
# mail_location = mbox:/var/mail/%d/%n:INDEX=/var/indexes/%d/%n/%n
#
# <doc/wiki/MailLocation.txt>
#
# mail_location = mbox:~/mail:INBOX=/var/mail/%u
# mail_privileged_group=mail
# If you need to set multiple mailbox locations or want to change default
# namespace settings, you can do it by defining namespace sections.
#
# You can have private, shared and public namespaces. Private namespaces
# are for user's personal mails. Shared namespaces are for accessing other
# users' mailboxes that have been shared. Public namespaces are for shared
Save modified buffer? (Answering "No" will DISCARD changes.) [Y/N]
Y Yes
N No      ⌂ Cancel
```

Figure 5. 126: Edit 10-mail.conf

### 5.3.11.4 CONFIGURING AUTHENTICATION MECHANISM

**STEP 1:** Edit the authentication configuration file.

```
nano /etc/dovecot/conf.d/10-auth.conf
```

**STEP 2:** Uncomment the following line.

```
disable_plaintext_auth = yes
```

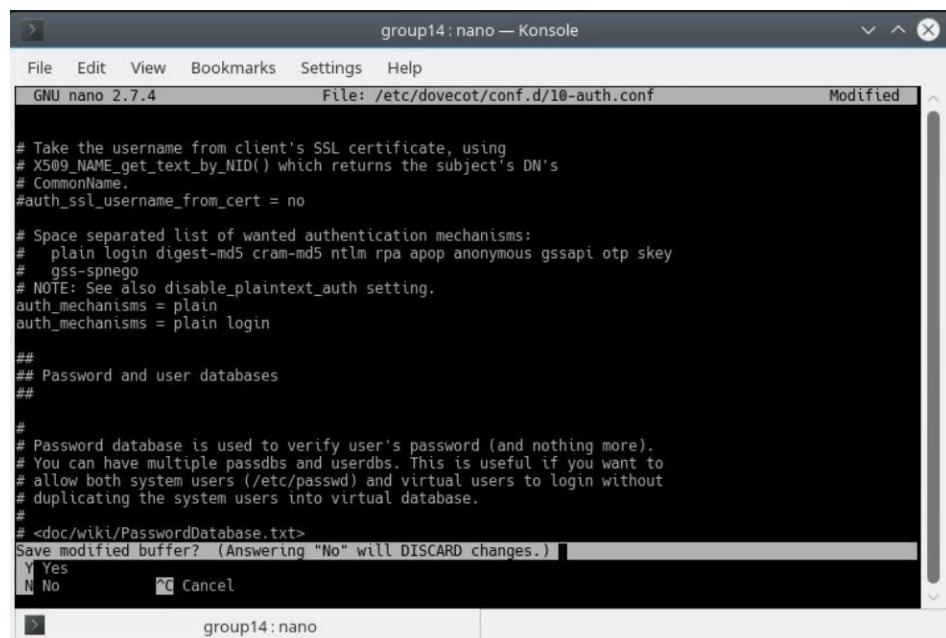
**STEP 3:** It will disable plaintext authentication when there is no SSL/TLS encryption. If want to use full email address (username@domain.com) to login, add the following line in the file.

```
auth_username_format = %n
```

**STEP 4:** Set the two line to enable plain and login authentication mechanism.

```
auth_mechanisms = plain
```

```
auth_mechanisms = plain login
```



```
# Take the username from client's SSL certificate, using
# X509_NAME_get_text_by_NID() which returns the subject's DN's
# CommonName.
#auth_ssl_username_from_cert = no

# Space separated list of wanted authentication mechanisms:
# plain login digest-md5 cram-md5 ntlm rpa apop anonymous gssapi otp skey
# gss-spnego
# NOTE: See also disable_plaintext_auth setting.
auth_mechanisms = plain
auth_mechanisms = plain login

##
## Password and user databases
##

#
# Password database is used to verify user's password (and nothing more).
# You can have multiple passdbs and userdbs. This is useful if you want to
# allow both system users (/etc/passwd) and virtual users to login without
# duplicating the system users into virtual database.
#
# <doc/wiki/PasswordDatabase.txt>
Save modified buffer? (Answering "No" will DISCARD changes.) [Y Yes] [N No] [C Cancel]
```

Figure 5. 127: Edit 10-auth.conf

### **5.3.11.5 CONFIGURING SSL/TLS ENCRYPTION**

**STEP 1:** Next, edit SSL/TLS configuration file. This configuration to make the communication between sender (Postfix) and receiver (Dovecot) more secure with encrypted data transfer.

```
nano /etc/dovecot/conf.d/10-ssl.conf
```

**STEP 2:** Change ssl = no to ssl = required.

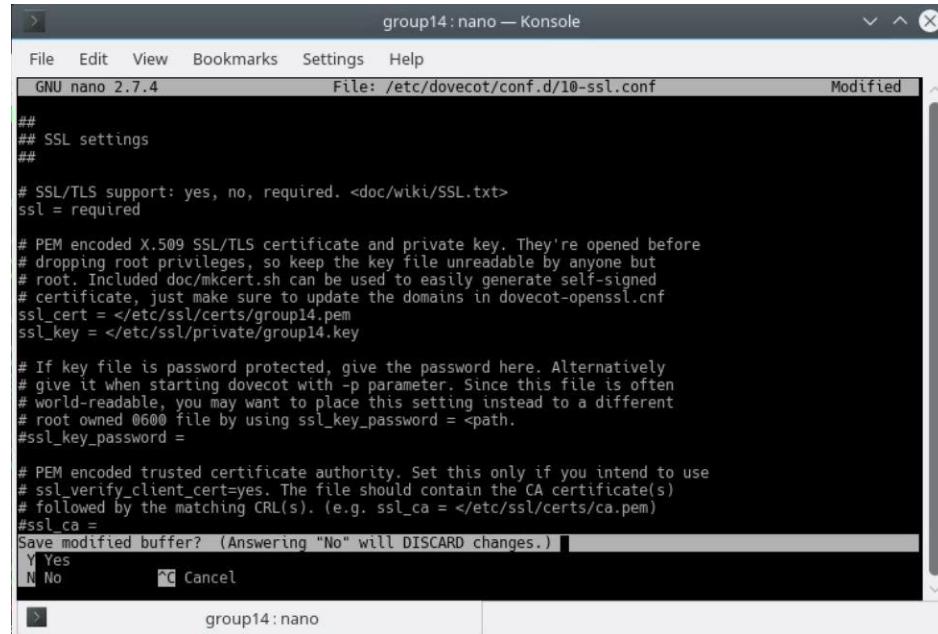
```
ssl = required
```

**STEP 3:** Then specify the location of, SSL/TLS cert and private key. Don't leave out character. It's necessary.

```
ssl_cert = </etc/ssl/certs/group4.pem
```

```
ssl_key = </etc/ssl/private/group4.key
```

Then, save the file and exit.



```
group14:nano — Konsole
File Edit View Bookmarks Settings Help
GNU nano 2.7.4 File: /etc/dovecot/conf.d/10-ssl.conf Modified
## SSL settings
## SSL/TLS support: yes, no, required. <doc/wiki/SSL.txt>
ssl = required

# PEM encoded X.509 SSL/TLS certificate and private key. They're opened before
# dropping root privileges, so keep the key file unreadable by anyone but
# root. Included doc/mkcert.sh can be used to easily generate self-signed
# certificate, just make sure to update the domains in dovecot-openssl.cnf
ssl_cert = </etc/ssl/certs/group14.pem
ssl_key = </etc/ssl/private/group14.key

# If key file is password protected, give the password here. Alternatively
# give it when starting dovecot with -p parameter. Since this file is often
# world-readable, you may want to place this setting instead to a different
# root owned 0600 file by using ssl_key_password = <path>.
#ssl_key_password =
# PEM encoded trusted certificate authority. Set this only if you intend to use
# ssl_verify_client_cert=yes. The file should contain the CA certificate(s)
# followed by the matching CRL(s). (e.g. ssl_ca = </etc/ssl/certs/ca.pem>
#ssl_ca =
Save modified buffer? (Answering "No" will DISCARD changes.) [Y/N/C]
Y Yes
N No
Cancel
```

Figure 5. 128 : Edit 10-ssl.conf

### 5.3.11.6 SASL AUTHENTICATION BETWEEN POSTFIX AND DOVECOT

**STEP 1:** Edit the following file.

```
nano /etc/dovecot/conf.d/10-master.conf
```

**STEP 2:** Change service auth section to the following so that Postfix can find the Dovecot authentication server.

```
unix_listener /var/spool/postfix/private/auth {
    mode = 8668
    user = postfix
    group = postfix
}
```

```

group14:nano — Konsole
File Edit View Bookmarks Settings Help
GNU nano 2.7.4 File: /etc/dovecot/conf.d/10-master.conf Modified
# get the results of everyone's userdb lookups.
#
# The default @666 mode allows anyone to connect to the socket, but the
# userdb lookups will succeed only if the userdb returns an "uid" field that
# matches the caller process's UID. Also if caller's uid or gid matches the
# socket's uid or gid the lookup succeeds. Anything else causes a failure.
#
# To give the caller full permissions to lookup all users, set the mode to
# something else than @666 and Dovecot lets the kernel enforce the
# permissions (e.g. 0777 allows everyone full permissions).
unix_listener /var/spool/postfix/private/auth {
mode = 8668
user = postfix
group = postfix
}
# Postfix smtp-auth
#unix_listener /var/spool/postfix/private/auth {
# mode = 0666
#}

# Auth process is run as this user.
#user = $default_internal_user
}

Save modified buffer? (Answering "No" will DISCARD changes.)
Y Yes
N No
C Cancel

```

Figure 5. 129: Edit 10-master.conf

**STEP 3:** Next, create includes: Drafts, Junk, Trash and Sent. These folders will be created at the user's home directory. Save and close all above configuration files, restart Dovecot.

sudo systemctl restart dovecot

```

group14:systemctl — Konsole
File Edit View Bookmarks Settings Help
root@Group14:~# systemctl restart dovecot.service
root@Group14:~# systemctl restart postfix.service
root@Group14:~# systemctl status dovecot.service
● dovecot.service - Dovecot IMAP/POP3 email server
   Loaded: loaded (/lib/systemd/system/dovecot.service; enabled; vendor preset: enabled)
   Active: active (running) since Sun 2019-10-13 22:47:36 PDT; 36s ago
     Docs: man:dovecot(1)
           http://wiki2.dovecot.org/
   Process: 26229 ExecStop=/usr/bin/doveadm stop (code=exited, status=0/SUCCESS)
   Process: 26234 ExecStart=/usr/sbin/dovecot (code=exited, status=0/SUCCESS)
 Main PID: 26235 (dovecot)
    Tasks: 4 (limit: 4915)
   CGroup: /system.slice/dovecot.service
           └─26235 /usr/sbin/dovecot
                 ├─26236 dovecot/anvil
                 ├─26237 dovecot/log
                 └─26239 dovecot/config

Oct 13 22:47:36 Group14 systemd[1]: Starting Dovecot IMAP/POP3 email server...
Oct 13 22:47:36 Group14 dovecot[26235]: master: Dovecot v2.2.27 (c0f36b0) starting up for imap (core du
Oct 13 22:47:36 Group14 systemd[1]: dovecot.service: PID file /var/run/dovecot/master.pid not readable
Oct 13 22:47:36 Group14 systemd[1]: Started Dovecot IMAP/POP3 email server.
lines 1-19/19 (END)


```

Figure 5. 130: Status

**STEP 4:** Dovecot will be listening on port 143 (IMAP) and 993 (IMAPS). If there is a configuration error, dovecot will fail to restart. Restart Postfix to allow the login authentication mechanism

```
sudo systemctl restart postfix
```

## INSTALLING RAINLOOP MAIL

**STEP 1:** Download and Install RainLoop webmail

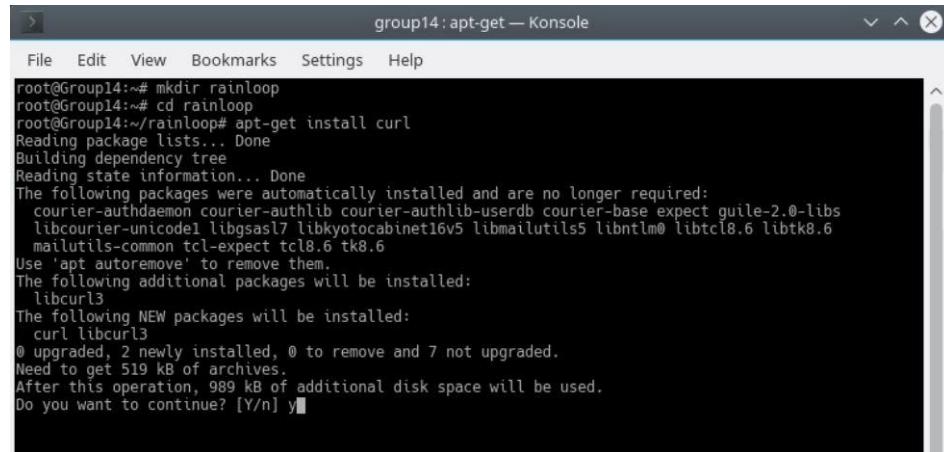
First, make a directory for rainloop in the current working directory.

```
mkdir rainloop
```

```
cd rainloop
```

**STEP 2:** Install Curl

```
apt-get install curl
```

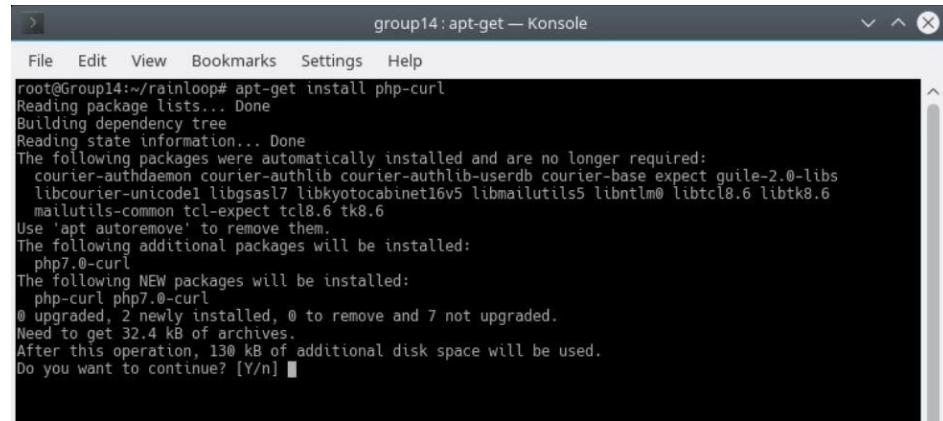


```
group14: apt-get — Konsole
File Edit View Bookmarks Settings Help
root@Group14:~# mkdir rainloop
root@Group14:~# cd rainloop
root@Group14:~/rainloop# apt-get install curl
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  courier-authdaemon courier-authlib courier-authlib-userdb courier-base expect guile-2.0-libs
  libcurl4-openssl-dev libgsasl7 libkyoto-cabinet16v5 libmailutils5 libnl3 libtcl8.6 libtk8.6
  mailutils-common tcl-expect tcl8.6 tk8.6
Use 'apt autoremove' to remove them.
The following additional packages will be installed:
  libcurl3
The following NEW packages will be installed:
  curl libcurl3
0 upgraded, 2 newly installed, 0 to remove and 7 not upgraded.
Need to get 519 kB of archives.
After this operation, 989 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
```

Figure 5. 131: Directory Rainloop and Install Curl

### STEP 3: Install Php-Curl

```
apt-get install php-curl
```

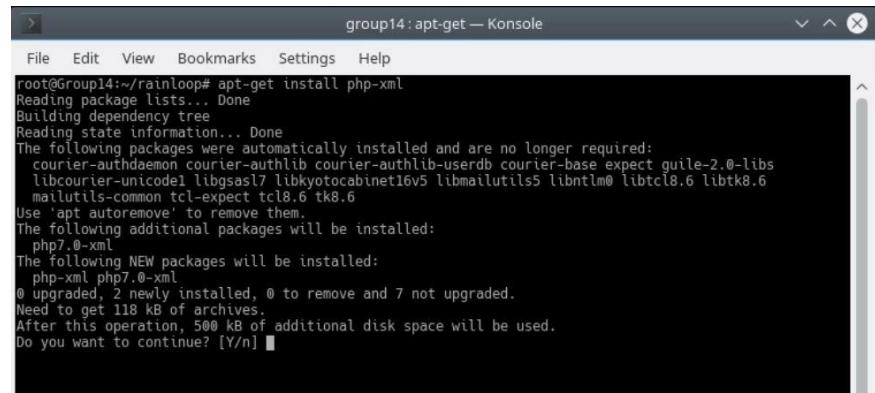


```
root@Group14:~/rainloop# apt-get install php-curl
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  courier-authdaemon courier-authlib courier-authlib-userdb courier-base expect guile-2.0-libs
  libcourier-unicode1 libgsasl7 libkyotocabinet16v5 libmailutils5 libnlm0 libtcl8.6 libtk8.6
  mailutils-common tcl-expect tcl8.6 tk8.6
Use 'apt autoremove' to remove them.
The following additional packages will be installed:
  php7.0-curl
The following NEW packages will be installed:
  php-curl php7.0-curl
0 upgraded, 2 newly installed, 0 to remove and 7 not upgraded.
Need to get 32.4 kB of archives.
After this operation, 130 kB of additional disk space will be used.
Do you want to continue? [Y/n] ■
```

Figure 5. 132: Install Php-Curl

### STEP 4: Install Php-Xml

```
apt-get install php-xml
```

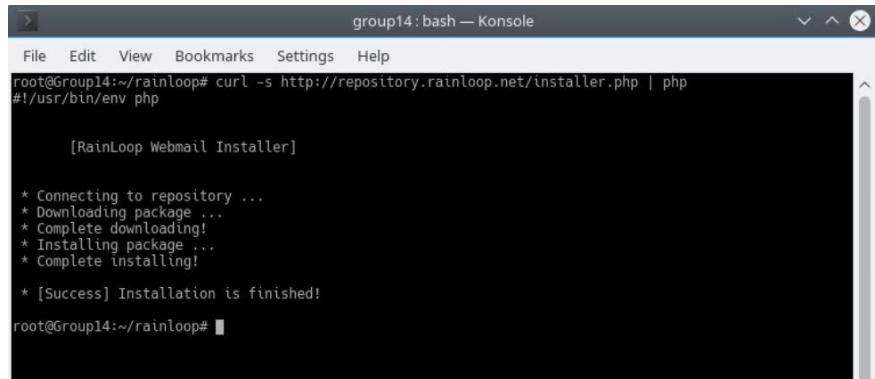


```
root@Group14:~/rainloop# apt-get install php-xml
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  courier-authdaemon courier-authlib courier-authlib-userdb courier-base expect guile-2.0-libs
  libcourier-unicode1 libgsasl7 libkyotocabinet16v5 libmailutils5 libnlm0 libtcl8.6 libtk8.6
  mailutils-common tcl-expect tcl8.6 tk8.6
Use 'apt autoremove' to remove them.
The following additional packages will be installed:
  php7.0-xml
The following NEW packages will be installed:
  php-xml php7.0-xml
0 upgraded, 2 newly installed, 0 to remove and 7 not upgraded.
Need to get 118 kB of archives.
After this operation, 500 kB of additional disk space will be used.
Do you want to continue? [Y/n] ■
```

Figure 5. 133: Install Php-Xml

**STEP 5:** Download the latest RainLoop community edition

```
curl -s http://repository.rainloop.net/installer.php | php
```



```
group14:bash — Konsole
File Edit View Bookmarks Settings Help
root@Group14:~/rainloop# curl -s http://repository.rainloop.net/installer.php | php
#!/usr/bin/env php

[RainLoop Webmail Installer]

* Connecting to repository ...
* Downloading package ...
* Complete downloading!
* Installing package ...
* Complete installing!

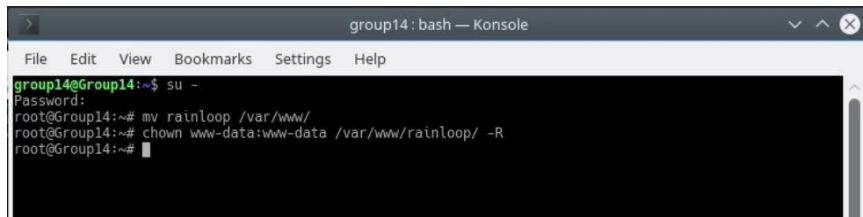
* [Success] Installation is finished!
root@Group14:~/rainloop#
```

Figure 5. 134: Download Rainloop

**STEP 6:** Next, move this directory to /var/www/ and set web server user (www-data) as the owner.

```
mv rainloop /var/www/
```

```
chown www-data:www-data /var/www/rainloop/ -R
```



```
group14:bash — Konsole
File Edit View Bookmarks Settings Help
group14@Group14:~$ su -
Password:
root@Group14:~# mv rainloop /var/www/
root@Group14:~# chown www-data:www-data /var/www/rainloop/ -R
root@Group14:~#
```

Figure 5. 135: Move Directory

**STEP 7:** Create the virtual host file with the following command:

```
sudo nano /etc/apache2/sites-available/rainloop.conf
```

Put the following text into the file. Replace red text with actual info

```
<VirtualHost *:80>
```

```

ServerName mail.group4.com

DocumentRoot "/var/www/rainloop/"

ServerAdmin mailadmin@group4.com

ErrorLog "/var/log/apache2/rainloop_error_log"

TransferLog "/var/log/apache2/rainloop_access_log"

<Directory />

    Options +Indexes +FollowSymLinks +ExecCGI

    AllowOverride All

    Order deny,allow

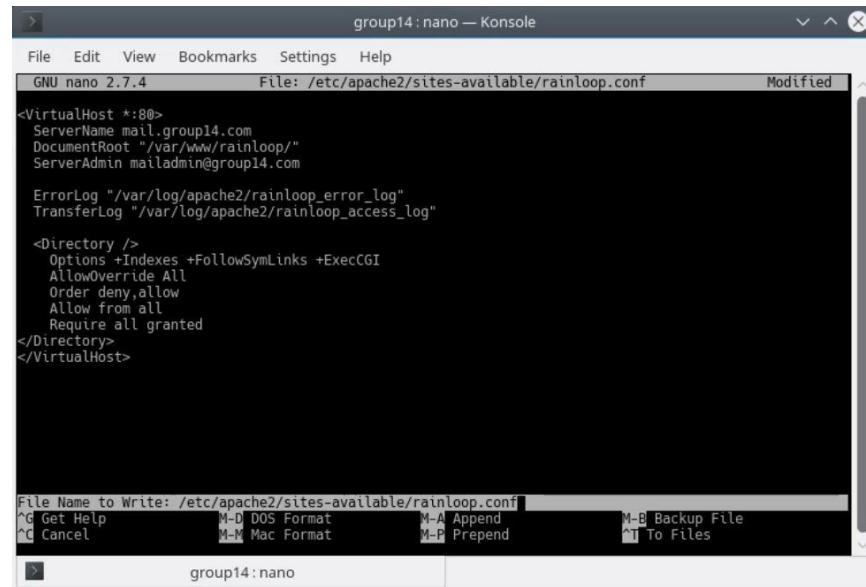
    Allow from all

    Require all granted

</Directory>

</VirtualHost>

```



The screenshot shows a terminal window titled "group14:nano — Konsole". The window displays an Apache configuration file named "rainloop.conf". The file content is as follows:

```

<VirtualHost *:80>
    ServerName mail.group14.com
    DocumentRoot "/var/www/rainloop/"
    ServerAdmin mailadmin@group14.com

    ErrorLog "/var/log/apache2/rainloop_error_log"
    TransferLog "/var/log/apache2/rainloop_access_log"

    <Directory />
        Options +Indexes +FollowSymLinks +ExecCGI
        AllowOverride All
        Order deny,allow
        Allow from all
        Require all granted
    </Directory>
</VirtualHost>

```

The nano editor interface includes a menu bar (File, Edit, View, Bookmarks, Settings, Help), a status bar at the bottom with file information ("File Name to Write: /etc/apache2/sites-available/rainloop.conf"), and a keyboard shortcut legend at the bottom right.

*Figure 5. 136: Virtual Host*

**STEP 8:** In order to start using it, you'll have to **create a new user** and **password** to do so, run.

Useradd anas

Passwd anas

Group14

Group14

Useradd farid

Passwd farid

Group14

Group14

```
root@Group14:~# useradd anas
root@Group14:~# passwd anas
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root@Group14:~#
```

Figure 5. 137: Create User Anas

```
root@Group14:~# useradd farid
root@Group14:~# passwd farid
Enter new UNIX password:
Retype new UNIX password: ■
```

Figure 5. 138: Create User Farid

**STEP 9: Create a home folder** for the **anas** in **/var/www/html/ anas** and make it **default** home directory.

```
mkdir -p /var/www/hmtl/anas
```

```
usermod -m -d /var/www/hmtl/anas
```

```
mkdir -p /var/www/hmtl/farid
```

```
usermod -m -d /var/www/hmtl/farid
```

**STEP 10:** Give the “megat and haikal” the complete permissions on its home holder

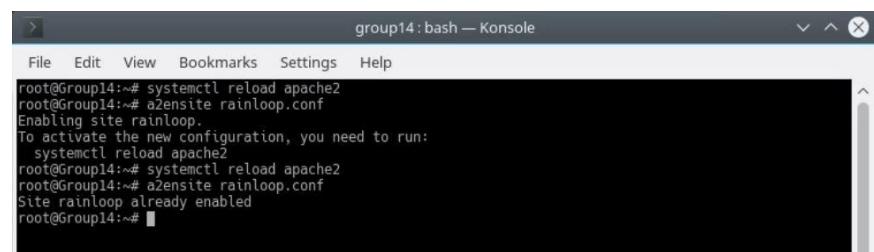
```
chown -R anas:anas /var/www/hmtl/anas
```

```
chown -R farid:farid /var/www/hmtl/farid
```

**STEP 11:** Save and close the file. Then enable this virtual host. Then reload Apache

```
systemctl reload apache2
```

```
a2ensite rainloop.conf
```



```
group14 : bash — Konsole
File Edit View Bookmarks Settings Help
root@Group14:~# systemctl reload apache2
root@Group14:~# a2ensite rainloop.conf
Enabling site rainloop.
To activate the new configuration, you need to run:
    systemctl reload apache2
root@Group14:~# systemctl reload apache2
root@Group14:~# a2ensite rainloop.conf
Site rainloop already enabled
root@Group14:~#
```

Figure 5. 139: Enable Virtual Host

**STEP 12:** The Rainloop mail now can access on browser, go to browser enter mail.group14.com/?admin that has been set in /etc/apache2/sites-available/rainloop.conf. This login for admin configuration to make the Rainloop use the port for communication. On the domain set the following configuration on the figure below than click test. On the

left menu, choose a domain menu and click on add domain.name “group14.com” .Use port 993 for IMAP and port 587 for SMTP. Click on test button and see if the IMAP and SMTP worked successfully by turning into green.

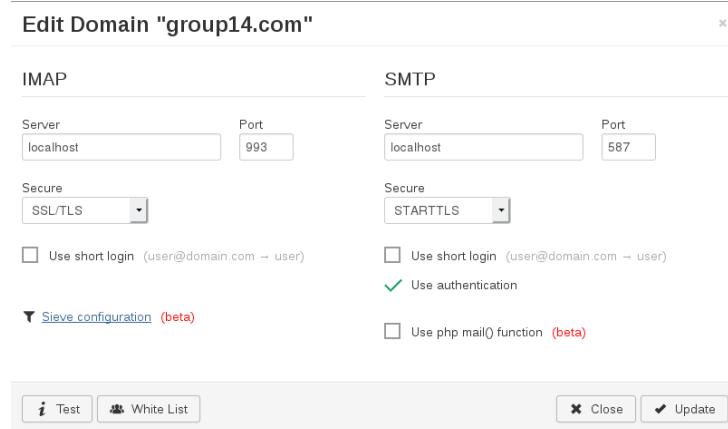


Figure 5. 140: Edit Domain

### 5.3.11 WEB, SSL & VIRTUAL HOSTING WEB

**STEP 1:** Install a Web Server (IIS), by open Server Manager and under Manage menu, select Add Roles and Features.

**STEP 2:** Select Role-based or Feature-based Installation.

**STEP 3:** Select the appropriate server (local is selected by default), as shown below

**STEP 4:** In the Add Roles and Features wizard, click Add Features if you want to install the IIS Management Console.

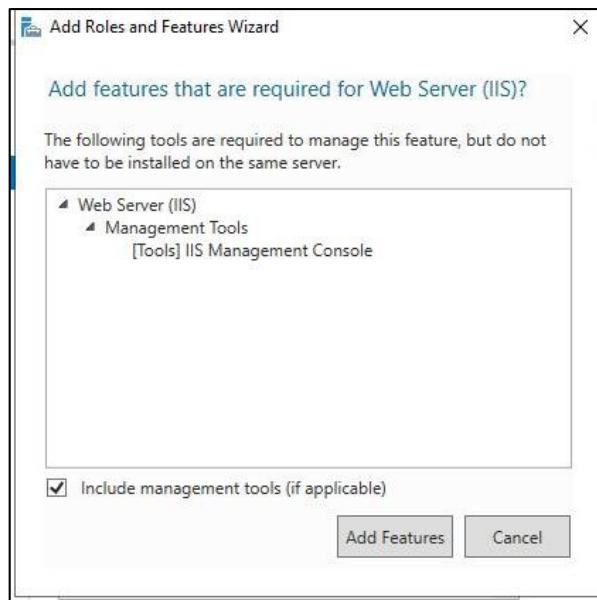
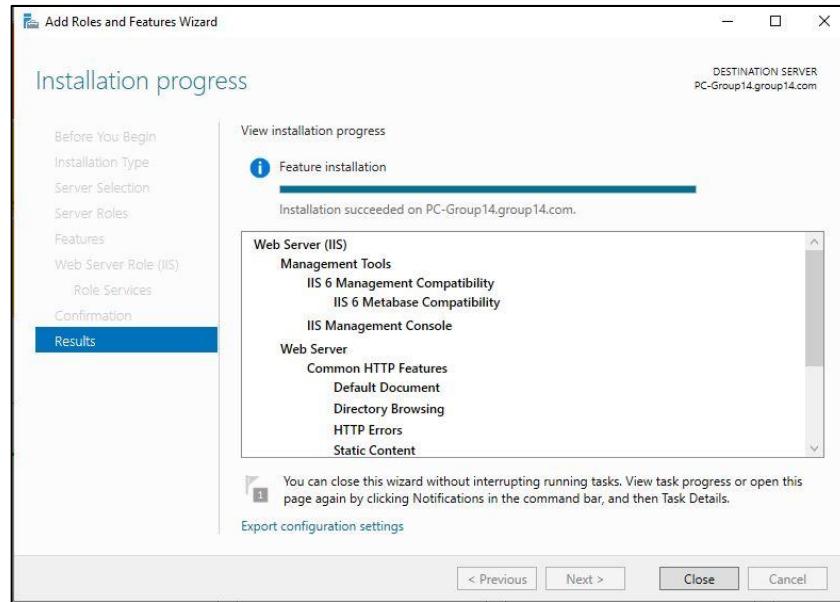


Figure 5. 141: Add Roles and Features wizard

**STEP 5:** Keeping click next until to reach confirmation page

**STEP 6:** In role services page click next and on the next page click install to start installing.

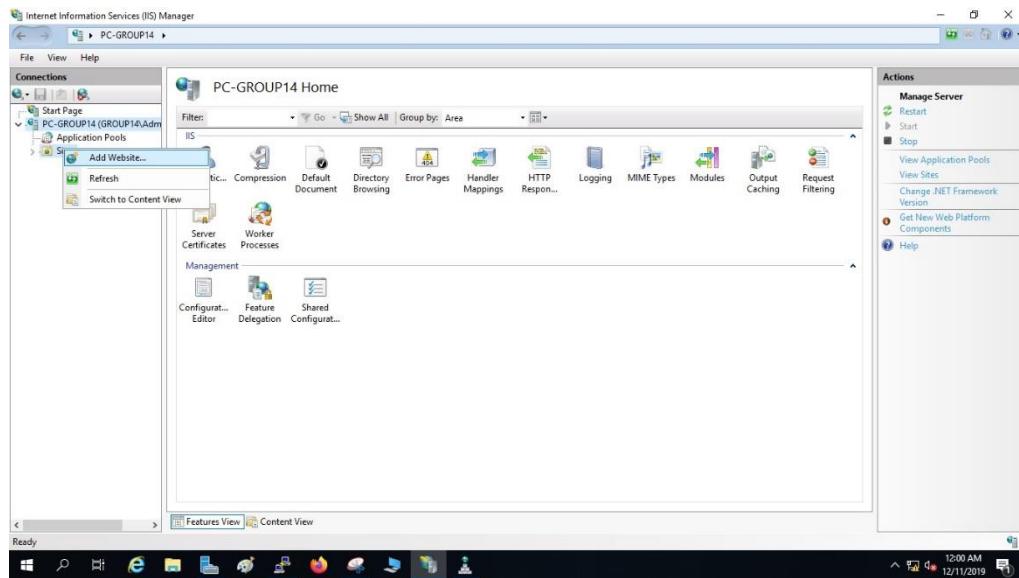
**STEP 7:** On the Results page, verify that the installation succeeds, and then click Close.



*Figure 5. 142: verify installation succeeds*

## **SECURE SOCKET LAYER (SSL)**

**STEP 1:** Open IIS manager and click add website.



*Figure 5. 143: Server Manager Properties*

## STEP 2: Add website

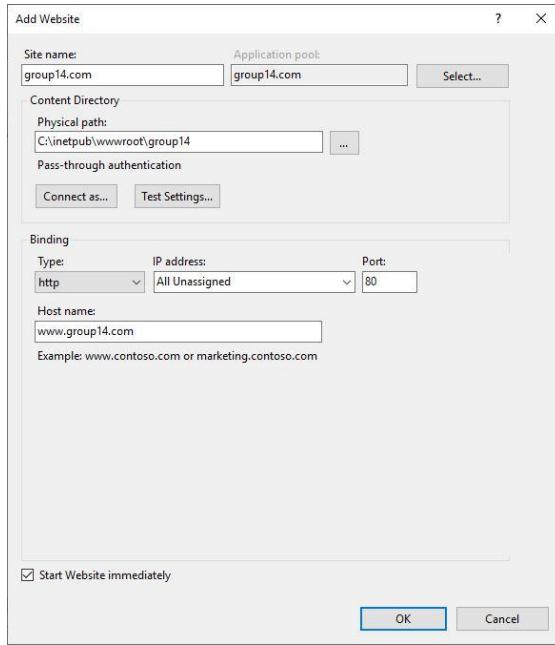


Figure 5. 144: Enter site name, bindings, and host name then press ok.

**STEP 3:** Create default document and save as html file in the directory and Add default document that we create in IIS.

**STEP 4:** Open DNS manager. Then go to forward lookup zone. Find Group14.com zone. Then create new host which is www for the web.

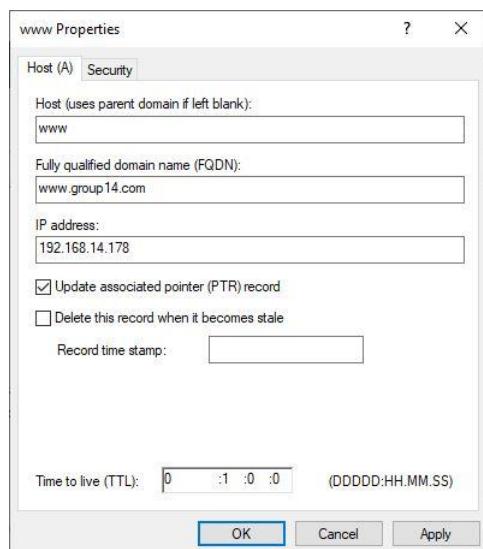


Figure 5. 145: Create new host

## STEP 5: group14.com web key bindings

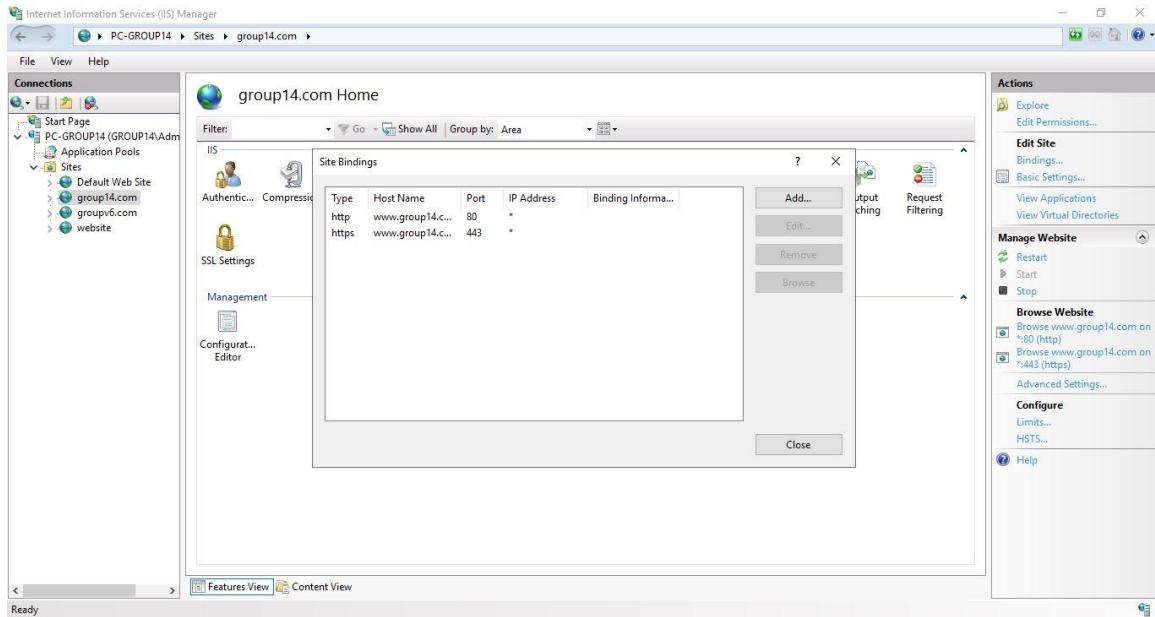


Figure 5. 146: Key Bindings

## VIRTUAL HOSTING

**STEP 1:** Go to Server Manager > Tools > Internet Information (IIS) Manager and at the connection column double-click WIN to expand it. Then, right-click on Sites and select Add Website.

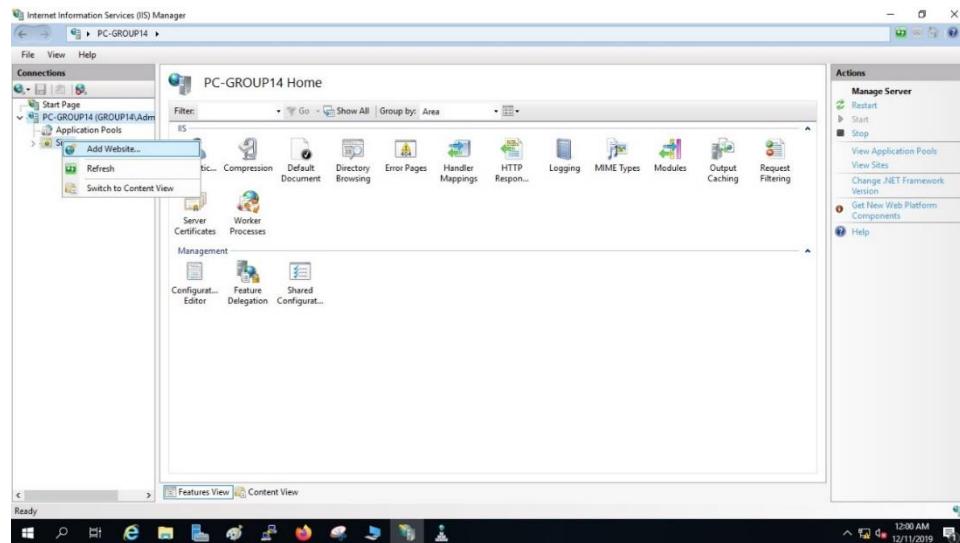


Figure 5. 147: Add Website

## STEP 2: Add virtual website

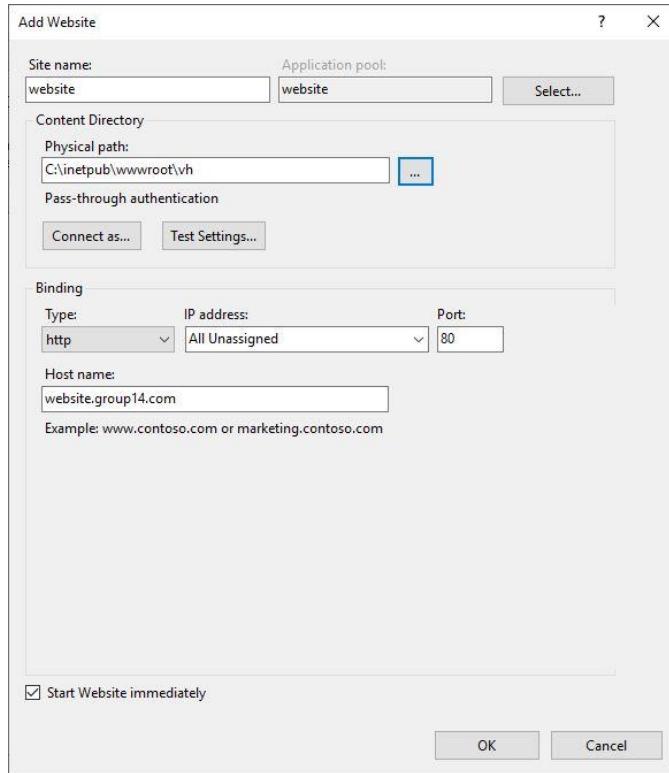
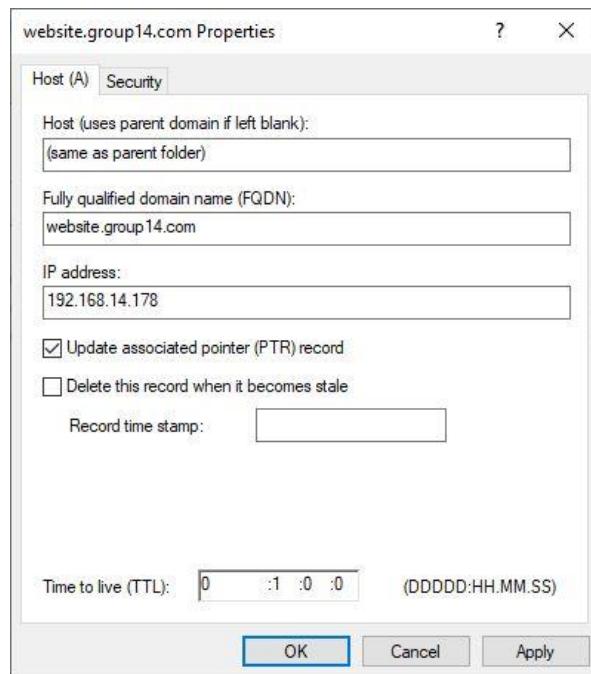


Figure 5. 148: Enter site name, bindings, and host name then press ok

**Step 3:** Create the directory for the website. Then, create new html file for the site and add default document to the site. Next, Open DNS Manager, create new Forward Lookup Zone and add host for website.group14.com. Select zone type as Primary Zone and choose “To all DNS servers running on domain controller this domain: group14.com”. Enter zone name as website.group14.com. Then, choose “Allow both nonsecure and secure dynamic updates”. After complete creating New Zone, Right click on the zone and choose new host. Add the host details and click add host button.

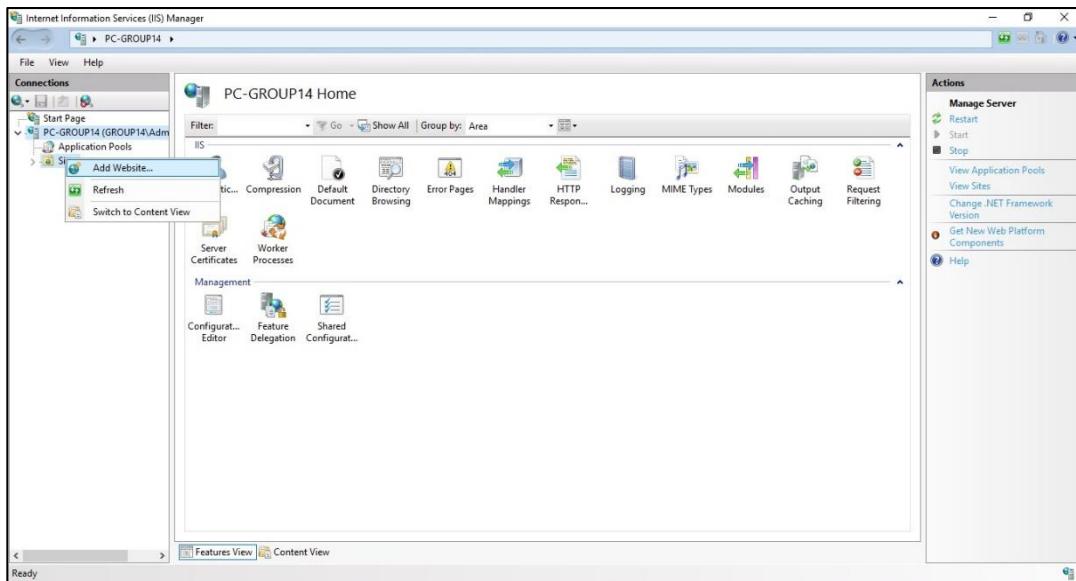


*Figure 5. 149: Create new virtual host*

### 5.3.12 IPV6 WEB & IPV6 TUNNELING

#### IPV6 WEB

**STEP 1:** Open IIS Manager and click add website



*Figure 5. 150: Server Manager Properties*

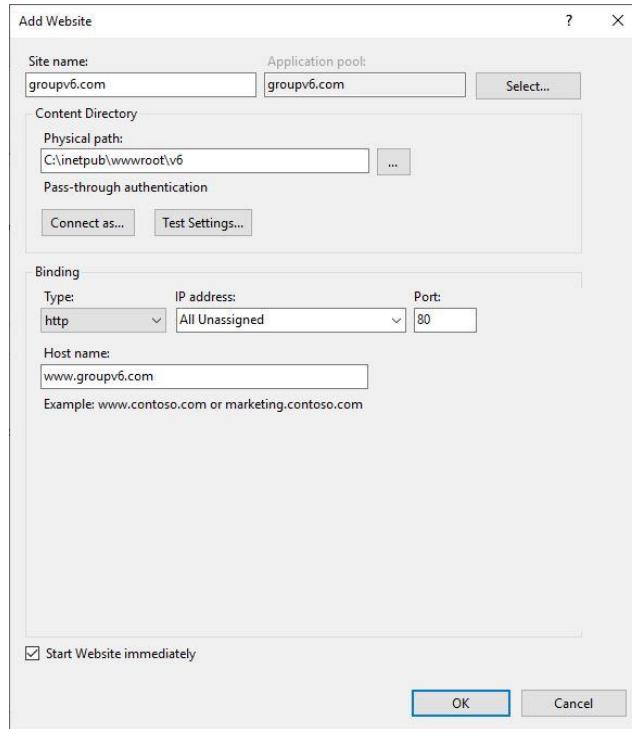
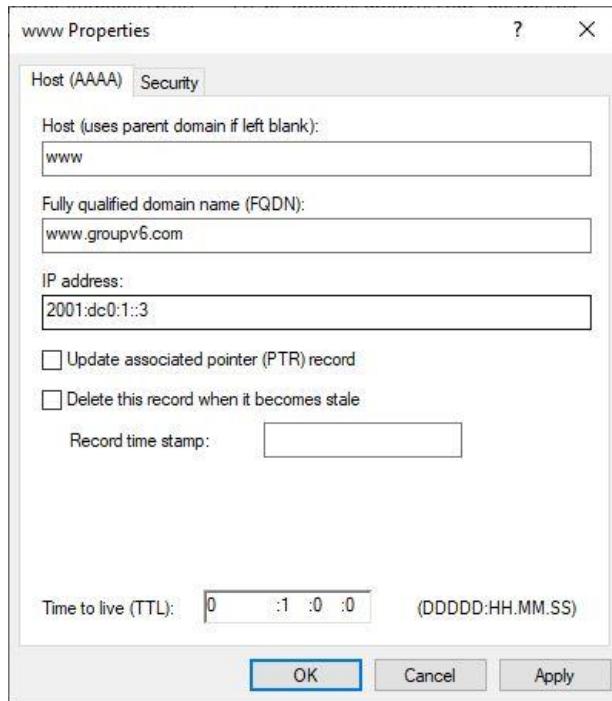
**STEP 2:** Add website

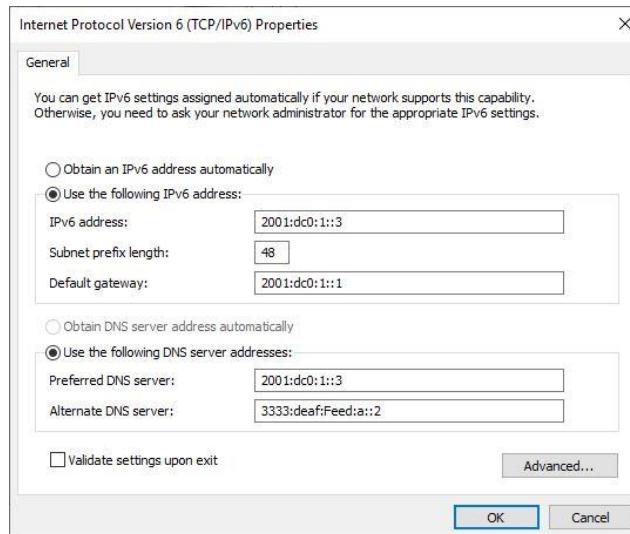
Figure 5. 151: Enter site name, bindings, and host name then press ok

**STEP 3:** Create the directory for the website. Then, create new html file for the site and add default document to the site. Next, Open DNS Manager, create new Forward Lookup Zone and add host for www.groupv6.com. Select zone type as Primary Zone and choose “To all DNS servers running on domain controller this domain: groupv6.com”. Enter zone name as groupv6.com. Then, choose “Allow both nonsecure and secure dynamic updates”. After complete creating New Zone, Right click on the zone and choose new host. Add the host details and click add host button.



*Figure 5. 152: Create new host*

#### **STEP 4:** Create static ipv6



*Figure 5. 153: ipv6 static*

#### **5.3.12.1 TUNNELLING CONFIGURATION**

**STEP 1:** Login into router and use config terminal command to start the configuration, then define the interface tunnel number and setup an IPv6 address for the tunneling.

**STEP 2:** To start an EIGRP for IPv6 routing configuration process, provide command as `ipv6 router eigrp 1`, where AS number is denoted as 1.

```
G14Router(config)#ipv6 router eigrp 1  
G14Router(config-rtr)#router-id 2.2.2.2
```

Figure 5. 154: ipv6 tunneling configuration

**STEP 3:** Configure the EIGRP for IPv6 on a gigabit Ethernet and serial interfaces on a router.

```
G14Router(config)#int g0/0.10  
G14Router(config-subif)#ipv6 eigrp 1  
G14Router(config-subif)#int g0/0.20  
G14Router(config-subif)#ipv6 eigrp 1  
G14Router(config-subif)#int g0/0.30  
G14Router(config-subif)#ipv6 eigrp 1  
G14Router(config-subif)#int g0/0.40  
G14Router(config-subif)#ipv6 eigrp 1
```

Figure 5. 155: ipv6 eigrp interface

**STEP 4:** Determine a neighbor adjacency

```
G14Router(config)#do show ipv6 eigrp neighbors  
EIGRP-IPv6 Neighbors for AS(1)  
H   Address                 Interface            Hold Uptime    SRTT      RTO  Q  S  
q  
q  
m  
0   Link-local address:     Se0/0/0                12 00:00:16    2   100  0  3  
    FE80::281:C4FF:FE39:7E00
```

Figure 5. 156: ipv6 eigrp neighbors

## STEP 5: Examine an EIGRP topology

```
G14Router#show ipv6 eigrp topology
EIGRP-IPv6 Topology Table for AS(1)/ID(2.2.2.2)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

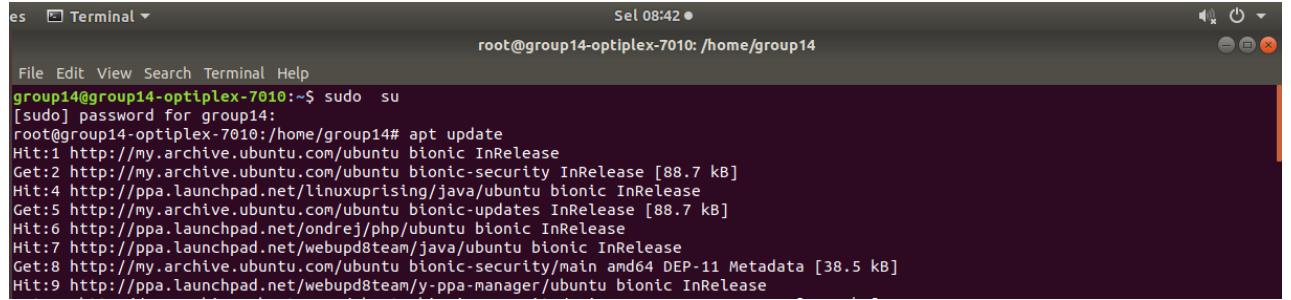
P 2001:DC0:1::/48, 1 successors, FD is 28160
      via Connected, GigabitEthernet0/0.10
P 2222:DEAF:FEED::/48, 1 successors, FD is 2172416
      via FE80::281:C4FF:FE39:7E00 (2172416/28160), Serial0/0/0
P 2001:DC0:3::/48, 1 successors, FD is 28160
      via Connected, GigabitEthernet0/0.30
P 1010:DEAF:FEED:A::/64, 1 successors, FD is 2172416
      via FE80::281:C4FF:FE39:7E00 (2172416/28160), Serial0/0/0
P 2001:DC0:5::/48, 1 successors, FD is 28160
      via Connected, GigabitEthernet0/0.40
P 2001:DC0:2::/48, 1 successors, FD is 28160
      via Connected, GigabitEthernet0/0.20
P 3333:DEAF:FEED::/48, 1 successors, FD is 2172416
      via FE80::281:C4FF:FE39:7E00 (2172416/28160), Serial0/0/0
P 1111:DEAF:FEED:A::/64, 1 successors, FD is 2172416
      via FE80::281:C4FF:FE39:7E00 (2172416/28160), Serial0/0/0
```

Figure 5. 157: *ipv6 eigrp topology*

### 5.3.13 NETWORK MANAGEMENT SYSTEM

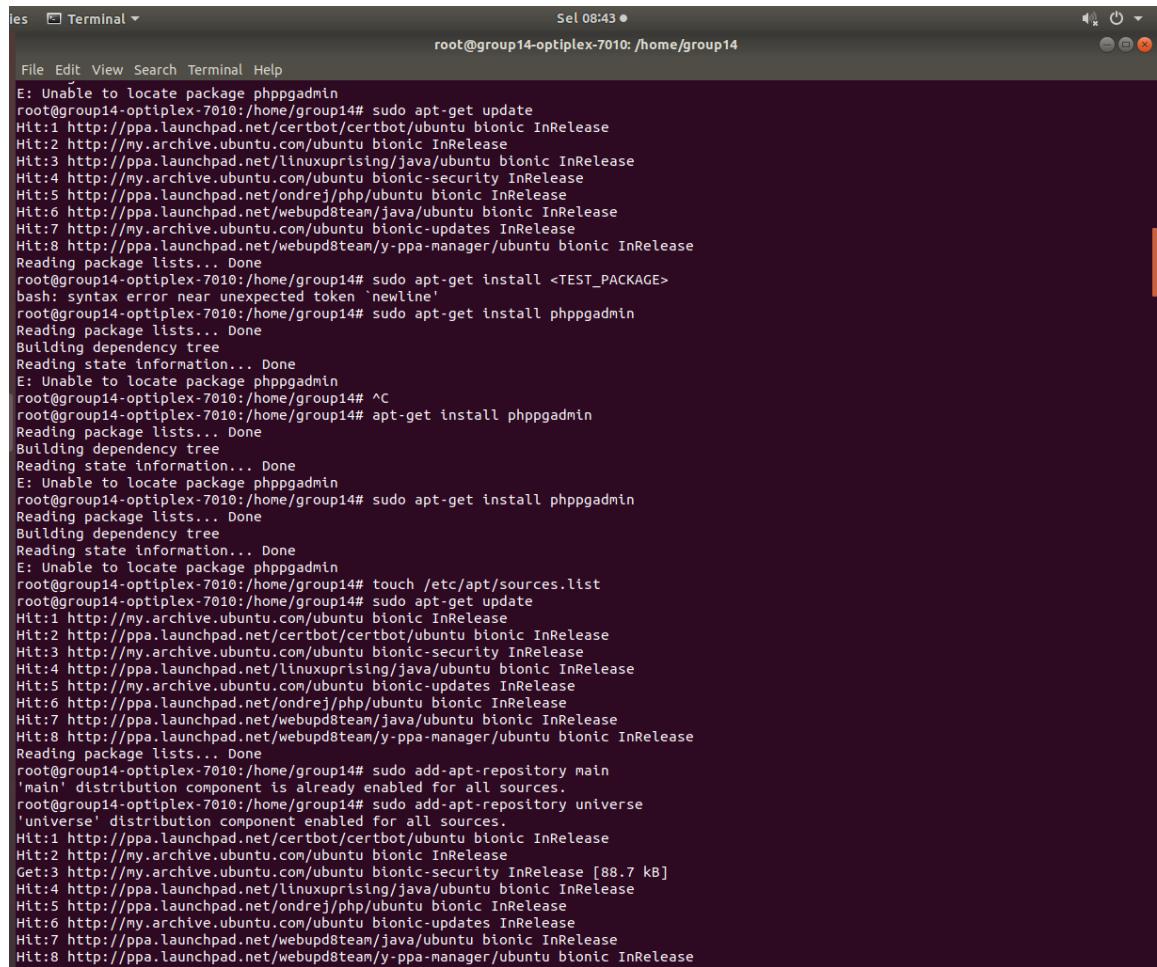
Step 1: First of all, before installing, the Ubuntu 14.04 Server is updated.

*apt update*



```
es Terminal ▾ Sel 08:42 •
root@group14-optiplex-7010: /home/group14
File Edit View Search Terminal Help
group14@group14-optiplex-7010:~$ sudo su
[sudo] password for group14:
root@group14-optiplex-7010:/home/group14# apt update
Hit:1 http://my.archive.ubuntu.com/ubuntu bionic InRelease
Get:2 http://my.archive.ubuntu.com/ubuntu bionic-security InRelease [88.7 kB]
Hit:4 http://ppa.launchpad.net/linuxuprising/java/ubuntu bionic InRelease
Get:5 http://my.archive.ubuntu.com/ubuntu bionic-updates InRelease [88.7 kB]
Hit:6 http://ppa.launchpad.net/ondrej/php/ubuntu bionic InRelease
Hit:7 http://ppa.launchpad.net/webupd8team/java/ubuntu bionic InRelease
Get:8 http://my.archive.ubuntu.com/ubuntu bionic-security/main amd64 DEP-11 Metadata [38.5 kB]
Hit:9 http://ppa.launchpad.net/webupd8team/y-ppa-manager/ubuntu bionic InRelease
```

Figure 5. 158: Update Ubuntu



```
les Terminal ▾ Sel 08:43 •
root@group14-optiplex-7010: /home/group14
File Edit View Search Terminal Help
E: Unable to locate package phppgadmin
root@group14-optiplex-7010:/home/group14# sudo apt-get update
Hit:1 http://ppa.launchpad.net/certbot/certbot/ubuntu bionic InRelease
Hit:2 http://my.archive.ubuntu.com/ubuntu bionic InRelease
Hit:3 http://ppa.launchpad.net/linuxuprising/java/ubuntu bionic InRelease
Hit:4 http://my.archive.ubuntu.com/ubuntu bionic-security InRelease
Hit:5 http://ppa.launchpad.net/ondrej/php/ubuntu bionic InRelease
Hit:6 http://ppa.launchpad.net/webupd8team/java/ubuntu bionic InRelease
Hit:7 http://my.archive.ubuntu.com/ubuntu bionic-updates InRelease
Hit:8 http://ppa.launchpad.net/webupd8team/y-ppa-manager/ubuntu bionic InRelease
Reading package lists... Done
root@group14-optiplex-7010:/home/group14# sudo apt-get install <TEST_PACKAGE>
bash: syntax error near unexpected token `newline'
root@group14-optiplex-7010:/home/group14# sudo apt-get install phppgadmin
Reading package lists... Done
Building dependency tree
Reading state information... Done
E: Unable to locate package phppgadmin
root@group14-optiplex-7010:/home/group14# ^C
root@group14-optiplex-7010:/home/group14# apt-get install phppgadmin
Reading package lists... Done
Building dependency tree
Reading state information... Done
E: Unable to locate package phppgadmin
root@group14-optiplex-7010:/home/group14# sudo apt-get install phppgadmin
Reading package lists... Done
Building dependency tree
Reading state information... Done
E: Unable to locate package phppgadmin
root@group14-optiplex-7010:/home/group14# touch /etc/apt/sources.list
root@group14-optiplex-7010:/home/group14# sudo apt-get update
Hit:1 http://my.archive.ubuntu.com/ubuntu bionic InRelease
Hit:2 http://ppa.launchpad.net/certbot/certbot/ubuntu bionic InRelease
Hit:3 http://my.archive.ubuntu.com/ubuntu bionic-security InRelease
Hit:4 http://ppa.launchpad.net/linuxuprising/java/ubuntu bionic InRelease
Hit:5 http://my.archive.ubuntu.com/ubuntu bionic-updates InRelease
Hit:6 http://ppa.launchpad.net/ondrej/php/ubuntu bionic InRelease
Hit:7 http://ppa.launchpad.net/webupd8team/java/ubuntu bionic InRelease
Hit:8 http://ppa.launchpad.net/webupd8team/y-ppa-manager/ubuntu bionic InRelease
Reading package lists... Done
root@group14-optiplex-7010:/home/group14# sudo add-apt-repository main
'main' distribution component is already enabled for all sources.
root@group14-optiplex-7010:/home/group14# sudo add-apt-repository universe
'universe' distribution component enabled for all sources.
Hit:1 http://ppa.launchpad.net/certbot/certbot/ubuntu bionic InRelease
Hit:2 http://my.archive.ubuntu.com/ubuntu bionic InRelease
Get:3 http://my.archive.ubuntu.com/ubuntu bionic-security InRelease [88.7 kB]
Hit:4 http://ppa.launchpad.net/linuxuprising/java/ubuntu bionic InRelease
Hit:5 http://ppa.launchpad.net/ondrej/php/ubuntu bionic InRelease
Hit:6 http://my.archive.ubuntu.com/ubuntu bionic-updates InRelease
Hit:7 http://ppa.launchpad.net/webupd8team/java/ubuntu bionic InRelease
Hit:8 http://ppa.launchpad.net/webupd8team/y-ppa-manager/ubuntu bionic InRelease
```

Figure 5. 159: Done Update Ubuntu

**Step 2:** Install postgresql by entering the following command.

*sudo apt-get install postgresql postgresql-contrib.*

```
root@group14-optiplex-7010:/home/group14# apt-get install postgresql postgresql-contrib
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libpq5 postgresql-10 postgresql-client-10 postgresql-client-common postgresql-common sysstat
Suggested packages:
  postgresql-doc locales-all postgresql-doc-10 libjson-perl isag
The following NEW packages will be installed:
  libpq5 postgresql postgresql-10 postgresql-client-10 postgresql-client-common postgresql-common postgresql-contrib sysstat
0 upgraded, 8 newly installed, 0 to remove and 0 not upgraded.
Need to get 5,293 kB of archives.
After this operation, 20.9 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://download.nus.edu.sg/mirror/ubuntu bionic/main amd64 postgresql-client-common all 190 [29.5 kB]
Get:2 http://download.nus.edu.sg/mirror/ubuntu bionic/main amd64 postgresql-common all 190 [157 kB]
Get:3 http://download.nus.edu.sg/mirror/ubuntu bionic/main amd64 postgresql all 10+190 [5,784 B]
Get:4 http://my.archive.ubuntu.com/ubuntu bionic-security/main amd64 libpq5 amd64 10.10-0ubuntu0.18.04.1 [108 kB]
Get:5 http://download.nus.edu.sg/mirror/ubuntu bionic/main amd64 postgresql-contrib all 10+190 [5,796 B]
Get:6 http://download.nus.edu.sg/mirror/ubuntu bionic/main amd64 sysstat amd64 11.6.1-1 [295 kB]
Get:7 http://my.archive.ubuntu.com/ubuntu bionic-security/main amd64 postgresql-client-10 amd64 10.10-0ubuntu0.18.04.1 [935 kB]
Get:8 http://my.archive.ubuntu.com/ubuntu bionic-security/main amd64 postgresql-10 amd64 10.10-0ubuntu0.18.04.1 [3,758 kB]
Fetched 5,293 kB in 44s (120 kB/s)
```

*Figure 5. 160: Install PostgreSQL*

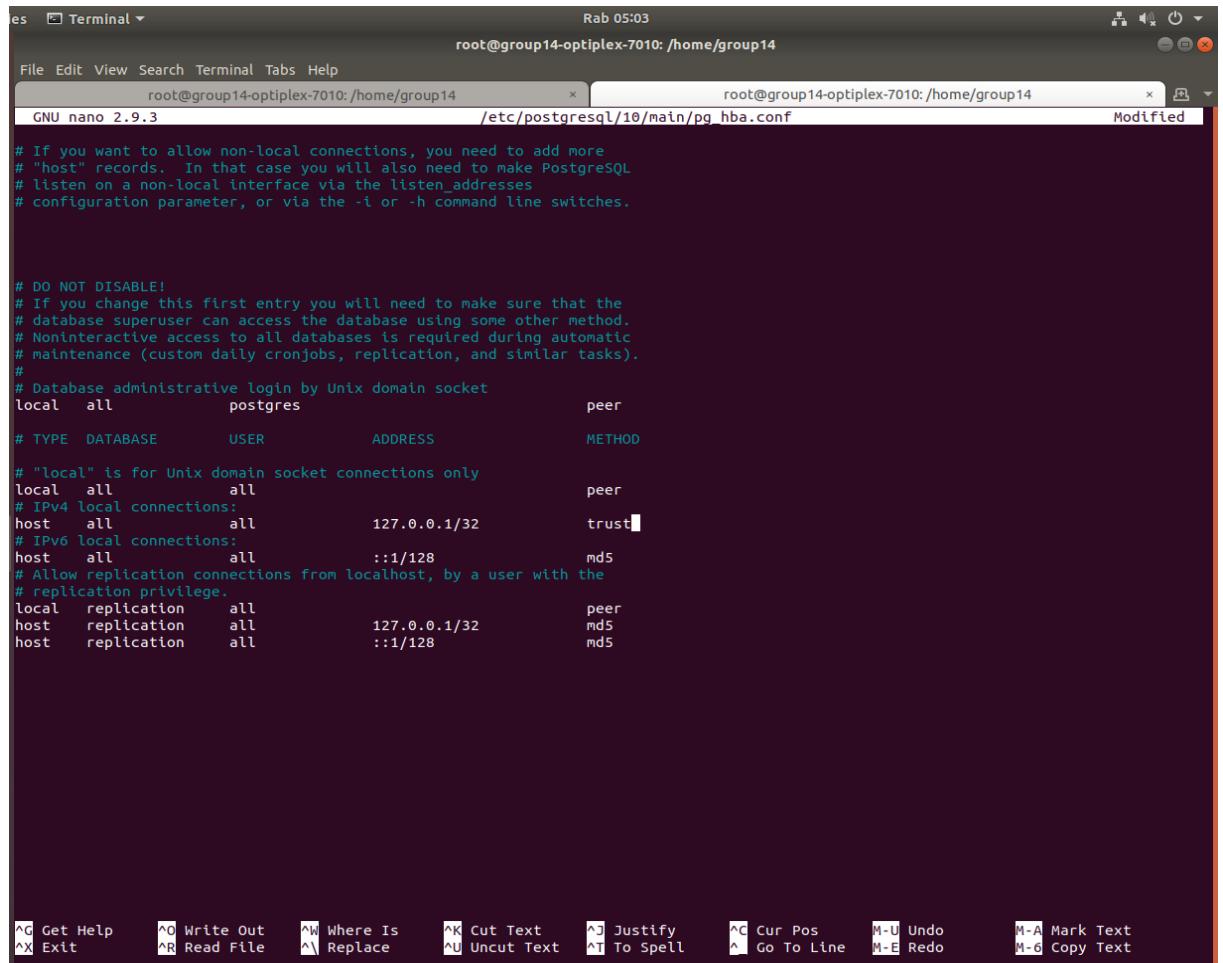
**Step 3:** The default database name and password as “**postgres**”. Therefore, to perform any postgresql related operation, first switch to the postgres user through *sudo -u postgres psql postgres* and set the postgres password. Then, install the PostgreSQL Adminpack through the **CREATE EXTENSION** command.

```
root@group14-optiplex-7010:/home/group14# sudo -u postgres psql postgres
psql (10.10 (Ubuntu 10.10-0ubuntu0.18.04.1))
Type "help" for help.

postgres=# \password postgres
Enter new password:
Enter it again:
postgres=# # CREATE EXTENSION adminpack;
ERROR:  syntax error at or near "postgres"
LINE 1: postgres=# 
^
postgres=# CREATE EXTENSION adminpack;
CREATE EXTENSION
postgres=# \q
root@group14-optiplex-7010:/home/group14#
```

*Figure 5. 161: PostgreSQL command*

**Step 4:** Configure PostgreSQL for MD5 authentication which requires the client supply an MD5-encrypted password for authentication. For that, **/etc/postgresql/9.3/main/pg\_hba.conf** file have to be edited.



The screenshot shows a terminal window titled "Terminal" with two tabs open. The left tab is at the root prompt in the home directory of "group14". The right tab is also at the root prompt, specifically at the path "/etc/postgresql/10/main/pg\_hba.conf". The file is being edited in the "GNU nano 2.9.3" text editor. The content of the file is a configuration for PostgreSQL's host-based authentication. It includes sections for local connections (peer), IPv4 local connections (trust), and IPv6 local connections (md5). It also specifies replication connections from localhost using the md5 method. The file ends with a note about not disabling the first entry if a database superuser needs access via another method.

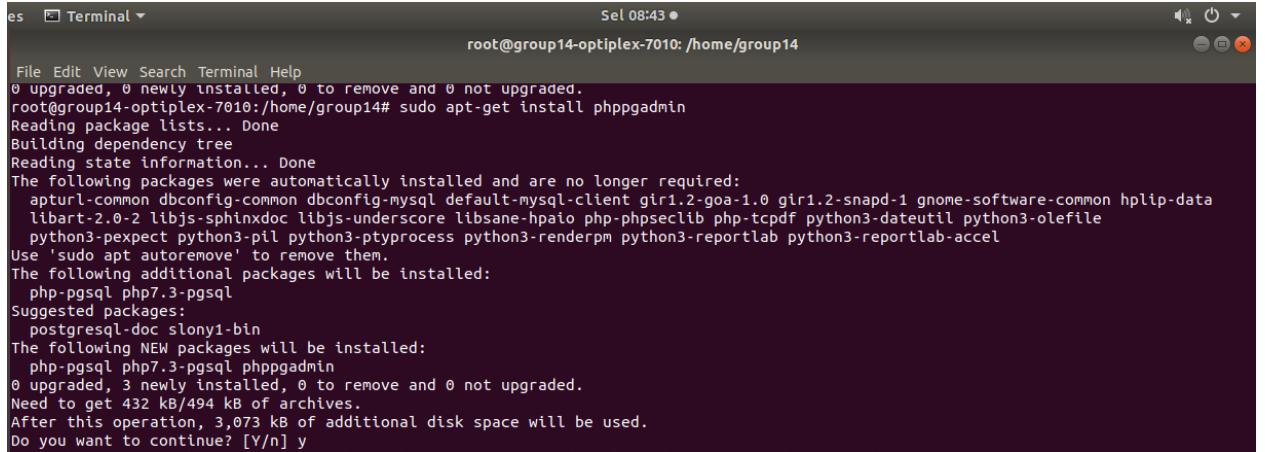
```
# If you want to allow non-local connections, you need to add more
# "host" records. In that case you will also need to make PostgreSQL
# listen on a non-local interface via the listen_addresses
# configuration parameter, or via the -i or -h command line switches.

# DO NOT DISABLE!
# If you change this first entry you will need to make sure that the
# database superuser can access the database using some other method.
# Noninteractive access to all databases is required during automatic
# maintenance (custom daily cronjobs, replication, and similar tasks).
#
# Database administrative login by Unix domain socket
local    all            postgres                      peer
# TYPE   DATABASE        USER            ADDRESS         METHOD
# "local" is for Unix domain socket connections only
local    all            all                          peer
# IPv4 local connections:
host     all            all            127.0.0.1/32      trust
# IPv6 local connections:
host     all            all            ::1/128          md5
# Allow replication connections from localhost, by a user with the
# replication privilege.
local   replication   all            peer
host   replication   all            127.0.0.1/32      md5
host   replication   all            ::1/128          md5
```

At the bottom of the terminal window, there is a menu bar with options like File, Edit, View, Search, Terminal, Tabs, Help, and a toolbar with various keyboard shortcuts for text editing.

Figure 5. 162: Configure PostgreSQL

**Step 5:** Install phpPgAdmin which is a web-based administration utility to manage PostgreSQL.



```

es  Terminal ①
Sel 08:43 ●
root@group14-optiplex-7010:/home/group14

File Edit View Search Terminal Help
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
root@group14-optiplex-7010:/home/group14# sudo apt-get install phppgadmin
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  apturl-common dbconfig-common dbconfig-mysql default-mysql-client gir1.2-goa-1.0 gir1.2-snapd-1 gnome-software-common hplip-data
  libart-2.0-2 libjs-sphinxdoc libjjs-underscore libsanep-hpato php-libsseclib php-tcpdf python3-dateutil python3-olefile
  python3-pexpect python3-pil python3-ptypocess python3-renderpm python3-reportlab python3-reportlab-accel
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  php-psql php7.3-psql
Suggested packages:
  postgresql-doc slony1-bin
The following NEW packages will be installed:
  php-psql php7.3-psql phppgadmin
0 upgraded, 3 newly installed, 0 to remove and 0 not upgraded.
Need to get 432 kB/494 kB of archives.
After this operation, 3,073 kB of additional disk space will be used.
Do you want to continue? [Y/n] y

```

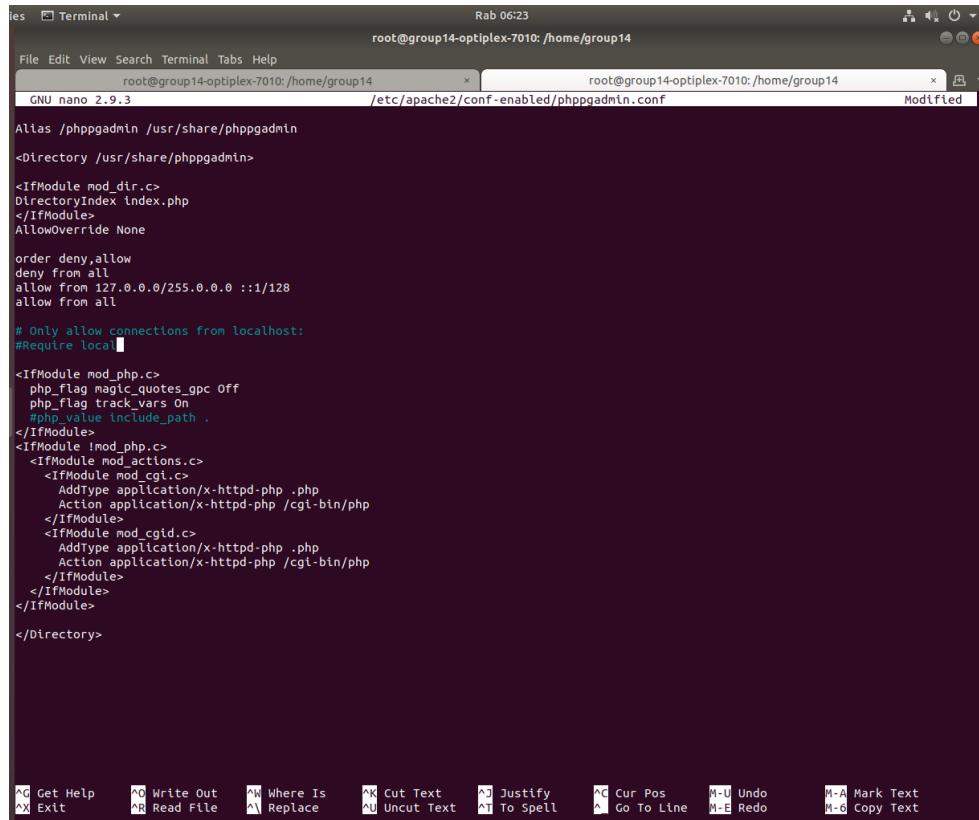
Figure 5. 163: Install phpPgAdmin

**Step 6:** Add command and uncomment “Require local”.

**order deny,allow**

**allow from all**

**allow 127.0.0.0/255.0.0.0 ::1/128 allow from all**



```

es  Terminal ②
Rab 06:23
root@group14-optiplex-7010:/home/group14

File Edit View Search Terminal Tabs Help
root@group14-optiplex-7010:/home/group14  /etc/apache2/conf-enabled/phppgadmin.conf  Modified
GNU nano 2.9.3

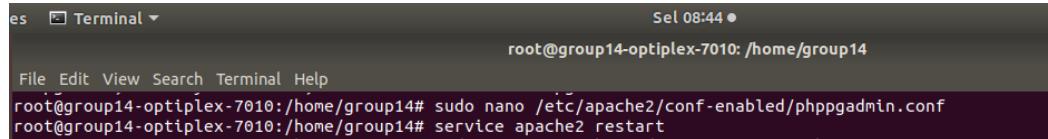
Alias /phppgadmin /usr/share/phppgadmin
<Directory /usr/share/phppgadmin>
<IfModule mod_dir.c>
  DirectoryIndex index.php
</IfModule>
  AllowOverride None
<Order deny,allow>
  Deny from all
  Allow from 127.0.0.0/255.0.0.0 ::1/128
  Allow from all
<# Only allow connections from localhost:>
<#Require local>

<IfModule mod_php.c>
  PHP_flag magic_quotes_gpc Off
  PHP_flag track_vars On
  PHP_value include_path .
</IfModule>
<IfModule mod_php.c>
  <IfModule mod_actions.c>
    <IfModule mod_cgi.c>
      AddType application/x-httpd-php .php
      Action application/x-httpd-php /cgi-bin/php
    </IfModule>
    <IfModule mod_cgid.c>
      AddType application/x-httpd-php .php
      Action application/x-httpd-php /cgi-bin/php
    </IfModule>
  </IfModule>
</IfModule>
</Directory>

```

Figure 5. 164: Edit /etc/apache2/conf.d/phppgadmin

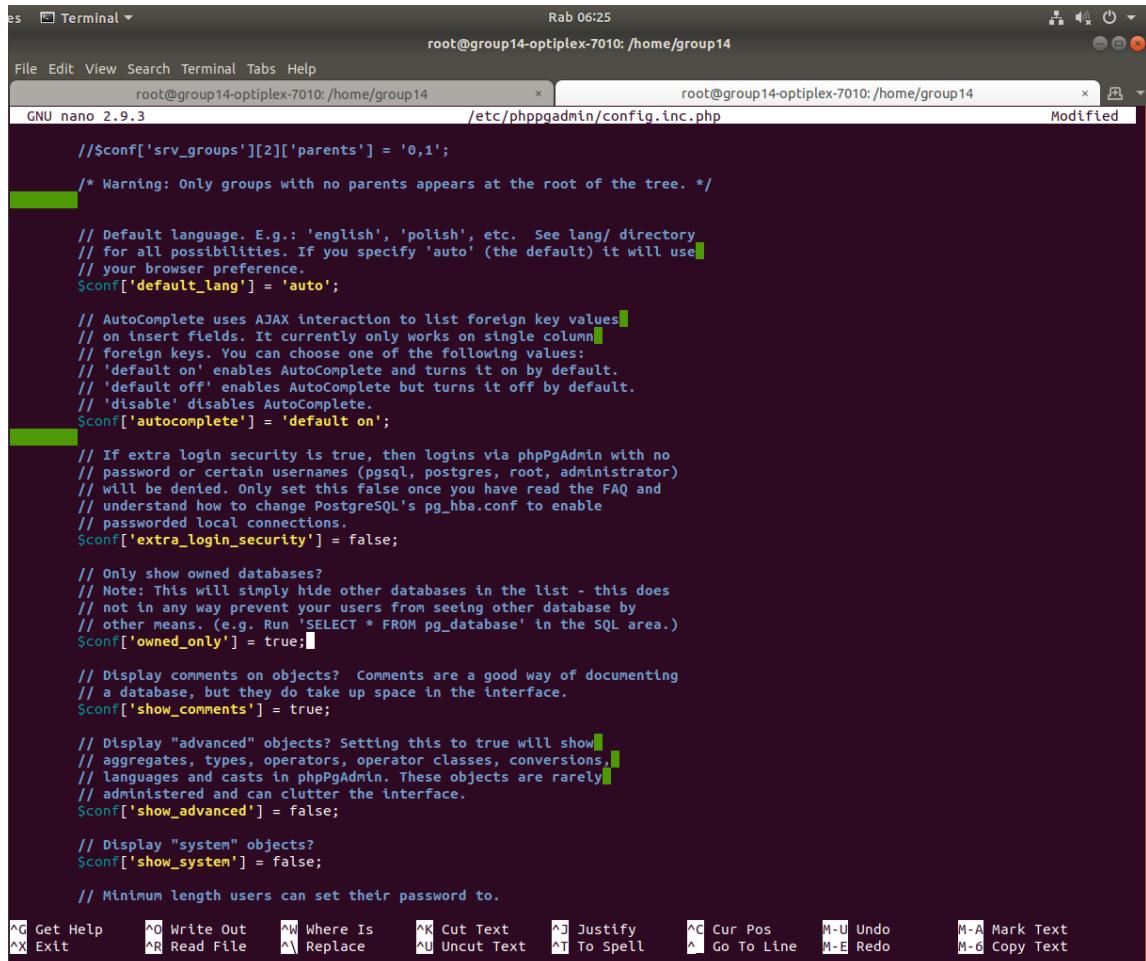
**Step 7:** Then, restart the apache service through *sudo service apache2 restart*.



```
es Terminal ▾ Sel 08:44 •
root@group14-optiplex-7010: /home/group14
File Edit View Search Terminal Help
root@group14-optiplex-7010:/home/group14# sudo nano /etc/apache2/conf-enabled/phppgadmin.conf
root@group14-optiplex-7010:/home/group14# service apache2 restart
```

Figure 5. 165: Restart services

**Step 8:** To configure phpPgAdmin, edit the */etc/phppgadmin/config.inc.php* file.



```
es Terminal ▾ Rab 06:25
root@group14-optiplex-7010: /home/group14
File Edit View Search Terminal Tabs Help
root@group14-optiplex-7010:/home/group14 x root@group14-optiplex-7010:/home/group14 x Modified
GNU nano 2.9.3 /etc/phppgadmin/config.inc.php
// $conf['srv_groups'][2]['parents'] = '0,1';
/* Warning: Only groups with no parents appears at the root of the tree. */

// Default language. E.g.: 'english', 'polish', etc. See lang/ directory
// for all possibilities. If you specify 'auto' (the default) it will use
// your browser preference.
$conf['default_lang'] = 'auto';

// AutoComplete uses AJAX interaction to list foreign key values
// on insert fields. It currently only works on single column
// foreign keys. You can choose one of the following values:
// 'default' on enables AutoComplete and turns it on by default.
// 'default off' enables AutoComplete but turns it off by default.
// 'disabled' disables AutoComplete.
$conf['autocomplete'] = 'default on';

// If extra login security is true, then logins via phpPgAdmin with no
// password or certain usernames (pgsql, postgres, root, administrator)
// will be denied. Only set this false once you have read the FAQ and
// understand how to change PostgreSQL's pg_hba.conf to enable
// passworded local connections.
$conf['extra_login_security'] = false;

// Only show owned databases?
// Note: This will simply hide other databases in the list - this does
// not in any way prevent your users from seeing other database by
// other means. (e.g. Run 'SELECT * FROM pg_database' in the SQL area.)
$conf['owned_only'] = true;

// Display comments on objects? Comments are a good way of documenting
// a database, but they do take up space in the interface.
$conf['show_comments'] = true;

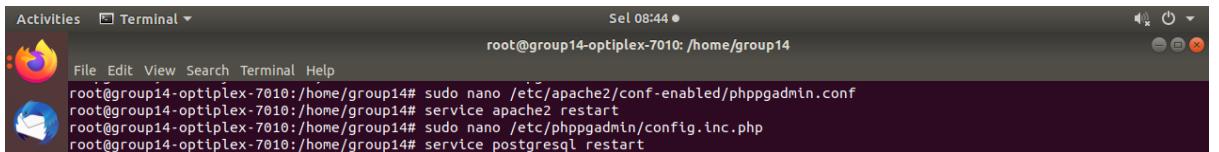
// Display "advanced" objects? Setting this to true will show
// aggregates, types, operators, operator classes, conversions,
// languages and casts in phpPgAdmin. These objects are rarely
// administered and can clutter the interface.
$conf['show_advanced'] = false;

// Display "system" objects?
$conf['show_system'] = false;

// Minimum length users can set their password to.
$conf['min_password_length'] = 6;
```

Figure 5. 166: Edit /etc/phppgadmin/config.inc.php

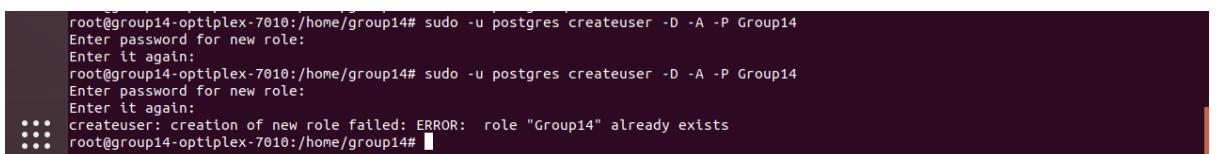
**Step 9:** Restart the postgresql service through the command  
**sudo service postgresql restart**



```
Activities Terminal Sel 08:44 ●
root@group14-optiplex-7010: /home/group14
File Edit View Search Terminal Help
root@group14-optiplex-7010:/home/group14# sudo nano /etc/apache2/conf-enabled/phppgadmin.conf
root@group14-optiplex-7010:/home/group14# service apache2 restart
root@group14-optiplex-7010:/home/group14# sudo nano /etc/phppgadmin/config.inc.php
root@group14-optiplex-7010:/home/group14# service postgresql restart
```

Figure 5. 167: Restart services

**Step 10:** Create a new user and database to be used in our desired network. The new user is called **Group2** with password **Gr@up22019** and a database called **mydb**.



```
root@group14-optiplex-7010:/home/group14# sudo -u postgres createuser -D -A -P Group14
Enter password for new role:
Enter it again:
root@group14-optiplex-7010:/home/group14# sudo -u postgres createuser -D -A -P Group14
Enter password for new role:
Enter it again:
createuser: creation of new role failed: ERROR:  role "Group14" already exists
root@group14-optiplex-7010:/home/group14#
```

Figure 5. 168: Create new user

**Step 10:** Open the browser and navigate to <http://127.0.1.1/phppgadmin> to see the phpPgAdmin website.

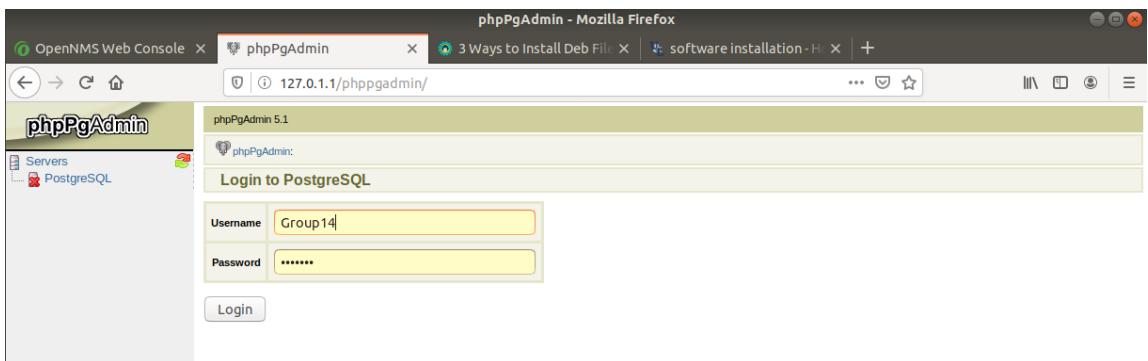


Figure 5. 169: Open phpPgAdmin website

**Step 11:** Login using the user that has been created before which is **Group14**.



Figure 5. 170: Login done

### 5.3.13.1 Install JDK

**Step 12:** Install JDK by following these steps.

***sudo add-apt-repository ppa:webupd8team/java***

```
root@group14-optiplex-7010:/home/group14# sudo add-apt-repository ppa:linuxuprising/java
^X^Z
[1]+  Stopped                  sudo add-apt-repository ppa:linuxuprising/java
root@group14-optiplex-7010:/home/group14# sudo add-apt-repository ppa:webupd8team/java
The Oracle JDK License has changed for releases starting April 16, 2019.

The new Oracle Technology Network License Agreement for Oracle Java SE is substantially different from prior Oracle JDK licenses. The new license permits certain uses, such as personal use and development use, at no cost -- but other uses authorized under prior Oracle JDK licenses may no longer be available. Please review the terms carefully before downloading and using this product. An FAQ is available here: https://www.oracle.com/technetwork/java/javase/overview/oracle-jdk-faqs.html

Oracle Java downloads now require logging in to an Oracle account to download Java updates, like the latest Oracle Java 8u211 / Java SE 8u212. Because of this I cannot update the PPA with the latest Java (and the old links were broken by Oracle).

For this reason, THIS PPA IS DISCONTINUED (unless I find some way around this limitation).

Oracle Java (JDK) Installer (automatically downloads and installs Oracle JDK8). There are no actual Java files in this PPA.

Important -> Why Oracle Java 7 And 6 Installers No Longer Work: http://www.webupd8.org/2017/06/why-oracle-java-7-and-6-installers-no.html

Update: Oracle Java 9 has reached end of life: http://www.oracle.com/technetwork/java/javase/downloads/jdk9-downloads-3848520.html

The PPA supports Ubuntu 18.10, 18.04, 16.04, 14.04 and 12.04.
```

Figure 5. 171: Step to install JDK

**Step 13:** Update Ubuntu by following these steps.

***sudo apt update***

```
root@group14-optiplex-7010:/home/group14# sudo apt update
Hit:1 http://ppa.launchpad.net/certbot/ubuntu bionic InRelease
Hit:2 http://my.archive.ubuntu.com/ubuntu bionic InRelease
Hit:3 http://ppa.launchpad.net/linuxuprising/java/ubuntu bionic InRelease
Hit:4 http://ppa.launchpad.net/ondrej/php/ubuntu bionic InRelease
Hit:5 http://ppa.launchpad.net/webupd8team/java/ubuntu bionic InRelease
Hit:6 http://ppa.launchpad.net/webupd8team/y-ppa-manager/ubuntu bionic InRelease
Get:7 http://my.archive.ubuntu.com/ubuntu bionic-security InRelease [88.7 kB]
Get:8 http://my.archive.ubuntu.com/ubuntu bionic-updates InRelease [88.7 kB]
Fetched 177 kB in 5s (37.1 kB/s)
Reading package lists... Done
Building dependency tree
Reading state information... Done
```

Figure 5. 172: Update

## Step 14: Install default JRE and JDK.

*sudo apt-get install default-jre*

```
root@group14-optiplex-7010:/home/group14# sudo apt-get install default-jre
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  default-jre-headless openjdk-11-jre openjdk-11-jre-headless
Suggested packages:
  fonts-ipafont-gothic fonts-ipafont-mincho fonts-wqy-microhei | fonts-wqy-zenhei
The following NEW packages will be installed:
  default-jre default-jre-headless openjdk-11-jre openjdk-11-jre-headless
0 upgraded, 4 newly installed, 0 to remove and 59 not upgraded.
Need to get 0 B/37.4 MB of archives.
After this operation, 171 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Selecting previously unselected package openjdk-11-jre-headless:amd64.
(Reading database ... 171508 files and directories currently installed.)
Preparing to unpack .../openjdk-11-jre-headless_11.0.4+11~1ubuntu2-18.04.3_amd64.deb ...
Unpacking openjdk-11-jre-headless:amd64 (11.0.4+11~1ubuntu2-18.04.3) ...
Selecting previously unselected package java-common:amd64.
Preparing to unpack .../default-jre-headless_2%3a11.68ubuntu1-18.04.1_amd64.deb ...
Unpacking default-jre-headless (2:11.68ubuntu1-18.04.1) ...
Selecting previously unselected package openjdk-11-jre:amd64.
Preparing to unpack .../openjdk-11-jre_11.0.4+11~1ubuntu2-18.04.3_amd64.deb ...
Unpacking openjdk-11-jre:amd64 (11.0.4+11~1ubuntu2-18.04.3) ...
Selecting previously unselected package default-jre.
Preparing to unpack .../default-jre_2%3a11.68ubuntu1-18.04.1_amd64.deb ...

```

Figure 5. 173: Install default JRE

```
Activities Terminal ▾ Sel 08:13 •
root@group14-optiplex-7010:/home/group14
group14@group14-optiplex-7010:~$ sudo apt install oracle-java13-set-default
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  apturl-common dbconfig-common dbconfig-mysql default-mysql-client
  glib1.2-goa-1.0 glib1.2-snapd-1 gnome-software-common hplip-data libart-2.0-2
  libjs-sphinxdoc libjs-underscore libsane-hpaio php-phpseclib php-tcpdf
  python3-dateutil python3-olefile python3-pexpect python3-pil
  python3-ptypyprocess python3-renderpm python3-reportlab
  python3-reportlab-accel
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  gsfonts-x11 oracle-java13-installer
Suggested packages:
  binfmt-support visualvm ttf-baekmuk | ttf-ufonts | ttf-ufonts-core
  ttf-kochi-gothic | ttf-sazanami-gothic ttf-kochi-mincho
  | ttf-sazanami-mincho ttf-archic-uming
The following NEW packages will be installed:
  gsfonts-x11 oracle-java13-installer oracle-java13-set-default
0 upgraded, 3 newly installed, 0 to remove and 0 not upgraded.
Need to get 43.3 kB of archives.
After this operation, 237 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://ppa.launchpad.net/linuxuprising/java/ubuntu bionic/main amd64 oracle-java13-installer amd64 13.0.1-1~linuxuprising0 [33.5 kB]
Get:2 http://my.archive.ubuntu.com/ubuntu bionic/universe amd64 gsfonts-x11 all 0.25 [7,264 B]
Get:3 http://ppa.launchpad.net/linuxuprising/java/ubuntu bionic/main amd64 oracle-java13-set-default amd64 13.0.1-1~linuxuprising0 [2,540 B]
Fetched 43.3 kB in 2s (26.3 kB/s)
Preconfiguring packages ...
Selecting previously unselected package oracle-java13-installer.
(Reading database ... 172655 files and directories currently installed.)
Preparing to unpack .../oracle-java13-installer_13.0.1-1~linuxuprising0_amd64.deb ...
Unpacking oracle-java13-installer (13.0.1-1~linuxuprising0) ...
Setting up oracle-java13-installer (13.0.1-1~linuxuprising0) ...
No /var/cache/oracle-jdk13-installer/wgetrc file found.
Creating /var/cache/oracle-jdk13-installer/wgetrc and
using default oracle-java13-installer wgetrc settings for it.
Downloading Oracle Java 13...
--2019-11-26 07:20:47--  http://download.oracle.com/otn-pub/java/jdk/13.0.1+9/cec27d702aa74d5a8630c65ae61e4305/jdk-13.0.1_linux-x64_bin.tar.gz
Resolving download.oracle.com (download.oracle.com)... 23.15.31.189
Connecting to download.oracle.com (download.oracle.com)|23.15.31.189|:80... connected.
HTTP request sent, awaiting response... 302 Moved Temporarily
Location: https://edelivery.oracle.com/otn-pub/java/jdk/13.0.1+9/cec27d702aa74d5a8630c65ae61e4305/jdk-13.0.1_linux-x64_bin.tar.gz [following]
--2019-11-26 07:20:48--  https://edelivery.oracle.com/otn-pub/java/jdk/13.0.1+9/cec27d702aa74d5a8630c65ae61e4305/jdk-13.0.1_linux-x64_bin.tar.gz
Resolving edelivery.oracle.com (edelivery.oracle.com)... 23.15.22.26, 2001:e68:2:180::366, 2001:e68:2:18d::366
Connecting to edelivery.oracle.com (edelivery.oracle.com)|23.15.22.26|:443... connected.
HTTP request sent, awaiting response... 302 Moved Temporarily

```

Figure 5. 174: Install Java 13

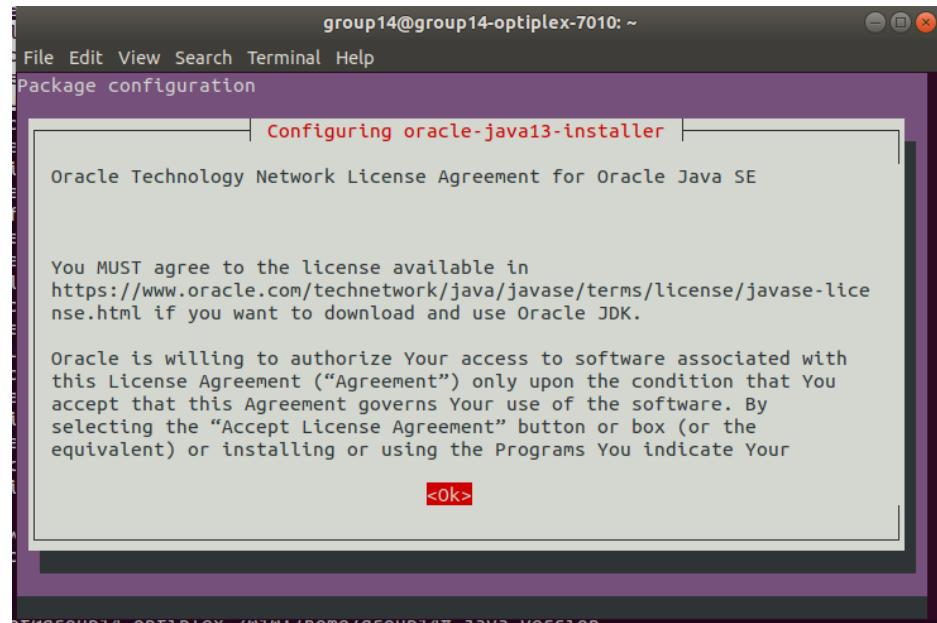


Figure 5. 175: OK

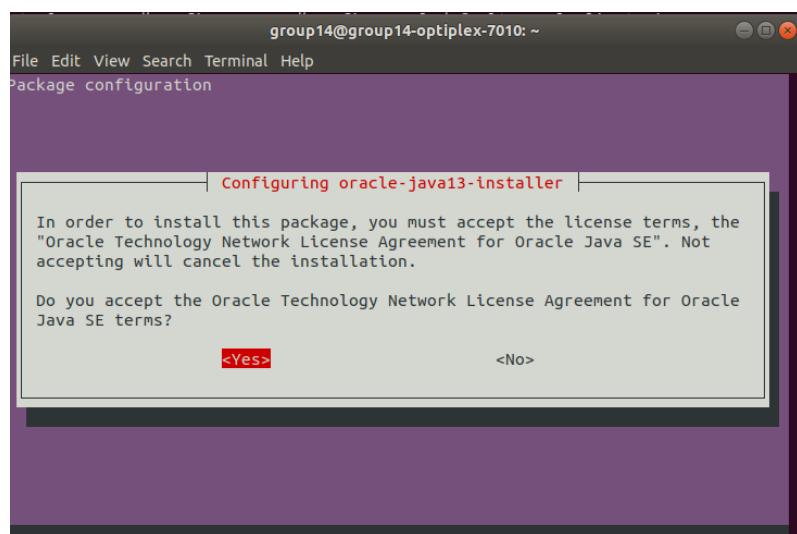
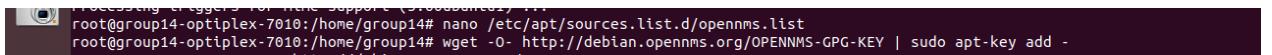


Figure 5. 176: Click Yes

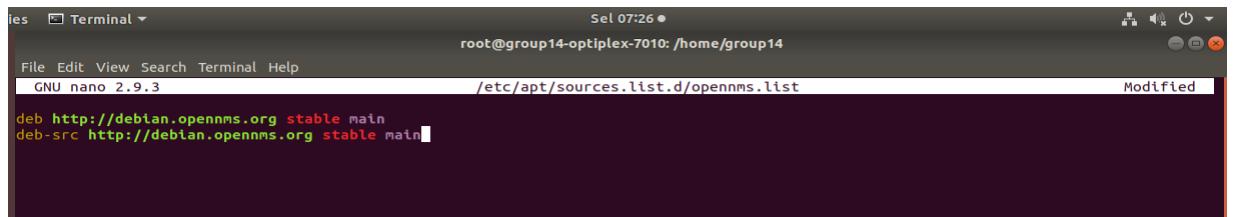
### 5.3.13.2 Install OpenNMS Repository

**Step 15:** Create a file called “`opennms.list`” in `nano /etc/apt/sources.list.d/opennms.list` directory. Add the OpenNMS APT repository.



```
root@group14-optiplex-7010:/home/group14# nano /etc/apt/sources.list.d/opennms.list
root@group14-optiplex-7010:/home/group14# wget -O http://debian.opennms.org/OPENNMS-GPG-KEY | sudo apt-key add -
```

Figure 5. 177 Add the OpenNMS APT repository



A screenshot of a terminal window titled "Terminal". The title bar shows "Sel 07:26" and "root@group14-optiplex-7010:/home/group14". The menu bar includes "File", "Edit", "View", "Search", "Terminal", and "Help". The status bar at the bottom right says "Modified". The main area of the terminal shows the command "nano /etc/apt/sources.list.d/opennms.list" being run. Below the command, the text "deb http://debian.opennms.org stable main" and "deb-src http://debian.opennms.org stable main" is visible, indicating the configuration of the OpenNMS repository.

Figure 5.178: Create a file

**Step 16:** Add the OpenNMS key.

`wget -O – http://debian.opennms.org/OPENNMS-GPG-KEY | sudo apt-key add –`



```
root@group14-optiplex-7010:/home/group14# wget -O http://debian.opennms.org/OPENNMS-GPG-KEY | sudo apt-key add -
--2019-11-26 07:28:15--  http://debian.opennms.org/OPENNMS-GPG-KEY
Resolving debian.opennms.org (debian.opennms.org)... 104.236.160.233, 2604:a880:1:20::d6:7001
Connecting to debian.opennms.org (debian.opennms.org)|104.236.160.233|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1725 (1.7K)
Saving to: 'STDOUT'

[=====>] 1.68K --.-KB/s in 0s

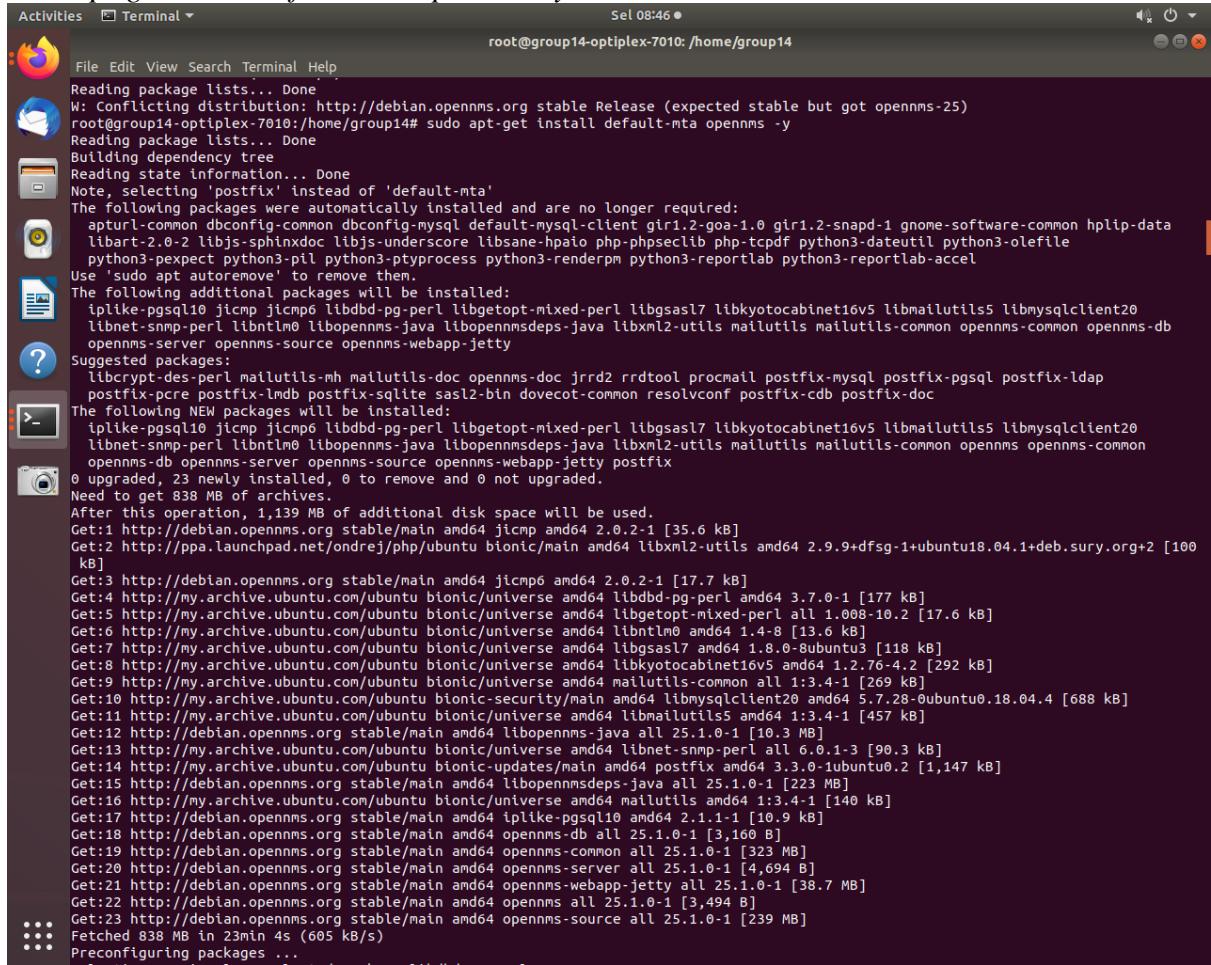
2019-11-26 07:28:16 (115 MB/s) - written to stdout [1725/1725]

OK
```

Figure 5.179: Add OpenNMS key

## Step 17: Install OpenNMS.

```
sudo apt-get install default-mta opennms -y
```



```
Reading package lists... Done
W: Conflicting distribution: http://debian.opennms.org stable Release (expected stable but got opennms-25)
root@group14-optiplex-7010:/home/group14# sudo apt-get install default-mta opennms -y
Reading package lists... Done
Building dependency tree
Reading state information... Done
Note, selecting 'postfix' instead of 'default-mta'
The following packages were automatically installed and are no longer required:
  apturl-common dbconfig-common dbconfig-mysql default-mysql-client gir1.2-goa-1.0 gir1.2-snapd-1 gnome-software-common hplip-data
  libart-2.0-2 libjs-sphinxdoc libjs-underscore libsane-hpaio php-phpseclib php-tcpdf python3-dateutil python3-olefile
  python3-pexpect python3-pil python3-ptyprocess python3-renderpm python3-reportlab python3-reportlab-accel
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  iplike-pgsql10 jicmp jicmp6 libdbd-pg-perl libgetopt-mixed-perl libgsasl7 libkyotocabinet16v5 libmailutils5 libmysqlclient20
  libnet-snmp-perl libntlm0 libopennms-java libopennmsdeps-java libxml2-utils mailutils mailutils-common opennms-common opennms-db
  opennms-server opennms-source opennms-webapp-jetty
Suggested packages:
  libcrypt-des-perl mailutils-mh mailutils-doc jrrd2 rrdtool procmail postfix-pgsql postfix-ldap
  postfix-pcre postfix-lmdb postfix-sqlite sasl2-bin dovecot-common resolvconf postfix-cdb postfix-doc
The following NEW packages will be installed:
  iplike-pgsql10 jicmp jicmp6 libdbd-pg-perl libgetopt-mixed-perl libgsasl7 libkyotocabinet16v5 libmailutils5 libmysqlclient20
  libnet-snmp-perl libntlm0 libopennms-java libopennmsdeps-java libxml2-utils mailutils mailutils-common opennms-common
  opennms-db opennms-server opennms-source opennms-webapp-jetty postfix
0 upgraded, 23 newly installed, 0 to remove and 0 not upgraded.
Need to get 838 MB of archives.
After this operation, 1,139 MB of additional disk space will be used.
Get:1 http://debian.opennms.org stable/main amd64 jicmp amd64 2.0.2-1 [35.6 kB]
Get:2 http://ppa.launchpad.net/ondrej/php/ubuntu bionic/main amd64 libxml2-utils amd64 2.9.9+dfsg-1+ubuntu18.04.1+deb.sury.org+2 [100 kB]
Get:3 http://debian.opennms.org stable/main amd64 jicmp6 amd64 2.0.2-1 [17.7 kB]
Get:4 http://my.archive.ubuntu.com/ubuntu bionic/universe amd64 libdbd-pg-perl amd64 3.7.0-1 [177 kB]
Get:5 http://my.archive.ubuntu.com/ubuntu bionic/universe amd64 libgetopt-mixed-perl all 1.008-10.2 [17.6 kB]
Get:6 http://my.archive.ubuntu.com/ubuntu bionic/universe amd64 libntlm0 amd64 1.4-8 [13.6 kB]
Get:7 http://my.archive.ubuntu.com/ubuntu bionic/universe amd64 libgsasl7 amd64 1.8.0-8ubuntu3 [118 kB]
Get:8 http://my.archive.ubuntu.com/ubuntu bionic/universe amd64 libkyotocabinet16v5 amd64 1.2.76-4.2 [292 kB]
Get:9 http://my.archive.ubuntu.com/ubuntu bionic/universe amd64 mailutils-common all 1:3.4-1 [269 kB]
Get:10 http://my.archive.ubuntu.com/ubuntu bionic-security/main amd64 libmysqlclient20 amd64 5.7.28-0ubuntu0.18.04.4 [688 kB]
Get:11 http://my.archive.ubuntu.com/ubuntu bionic/universe amd64 libmailutils5 amd64 1:3.4-1 [457 kB]
Get:12 http://debian.opennms.org stable/main amd64 libopennms-java all 25.1.0-1 [10.3 kB]
Get:13 http://my.archive.ubuntu.com/ubuntu bionic/universe amd64 libnet-snmp-perl all 6.0.1-3 [90.3 kB]
Get:14 http://my.archive.ubuntu.com/ubuntu bionic-updates/main amd64 postfix amd64 3.3.0-1ubuntu0.2 [1,147 kB]
Get:15 http://debian.opennms.org stable/main amd64 libopennmsdeps-java all 25.1.0-1 [223 kB]
Get:16 http://my.archive.ubuntu.com/ubuntu bionic/universe amd64 mailutils amd64 2.1.1-1 [140 kB]
Get:17 http://debian.opennms.org stable/main amd64 iplike-pgsql10 amd64 2.1.1-1 [10.9 kB]
Get:18 http://debian.opennms.org stable/main amd64 opennms-db all 25.1.0-1 [3,160 B]
Get:19 http://debian.opennms.org stable/main amd64 opennms-common all 25.1.0-1 [323 kB]
Get:20 http://debian.opennms.org stable/main amd64 opennms-server all 25.1.0-1 [4,694 B]
Get:21 http://debian.opennms.org stable/main amd64 opennms-webapp-jetty all 25.1.0-1 [38.7 kB]
Get:22 http://debian.opennms.org stable/main amd64 opennms all 25.1.0-1 [3,494 B]
Get:23 http://debian.opennms.org stable/main amd64 opennms-source all 25.1.0-1 [239 kB]
Fetched 838 MB in 23min 4s (605 kB/s)
Preconfiguring packages ...
```

Figure 5.180 : Install OpenNMS

**Step 18:** After a few minutes, the installer will be asked to run manually. Click Ok throughout

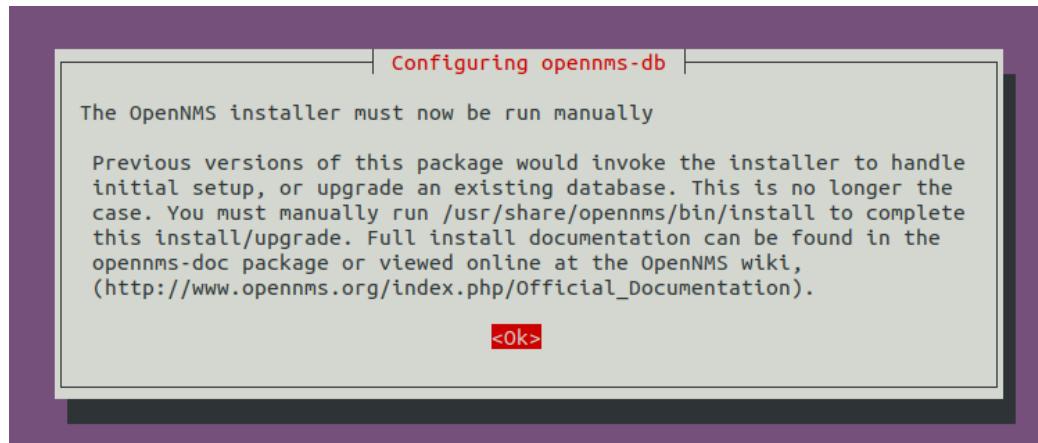


Figure 5.181: Click OK

**Step 19:** IPLIKE can be installed manually through the command

*sudo /usr/sbin/install\_iplike.sh*

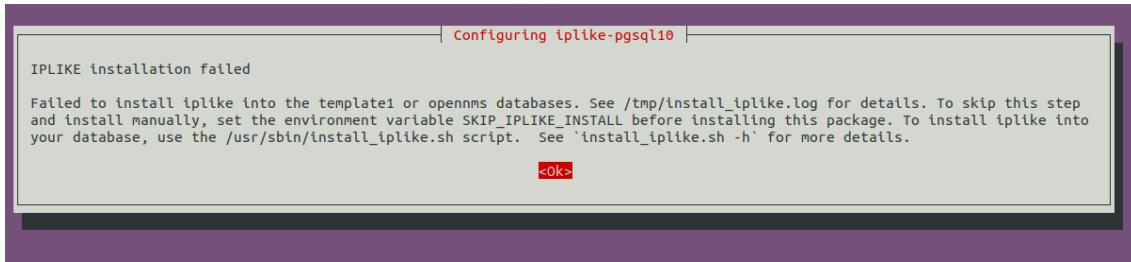


Figure 5.182: Click OK

### 5.3.13.3 Post Installation

**Step 20:** After that, inform OpenNMS on what version of Java are we using.

*sudo /usr/share/opennms/bin/runjava -s*

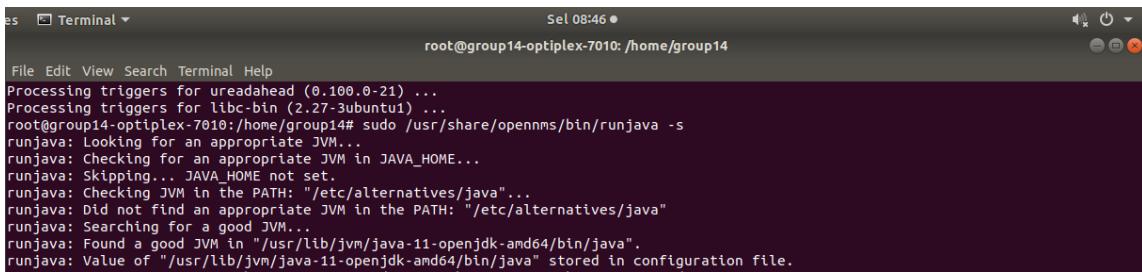


Figure 5.183: Inform OpenNMS on version of Java

**Step 21:** Create a database for OpenNMS.

```
sudo /usr/share/opennms/bin/install -dis
```

```
root@group14-optiplex-7010:/home/group14# sudo /usr/share/opennms/bin/install -dis
=====
OpenNMS Installer
=====

Configures PostgreSQL tables, users, and other miscellaneous settings.

DEBUG: Platform is IPv6 ready: true
- searching for libjicmp.so:
  - trying to load /libjicmp.so: NO
  - trying to load /usr/share/opennms/lib/libjicmp.so: NO
  - trying to load /usr/share/opennms/lib/linux64/libjicmp.so: NO
  - trying to load /usr/java/packages/lib/libjicmp.so: NO
  - trying to load /usr/lib/x86_64-linux-gnu/jni/libjicmp.so: NO
  - trying to load /lib/x86_64-linux-gnu/libjicmp.so: NO
  - trying to load /usr/lib/x86_64-linux-gnu/libjicmp.so: NO
  - trying to load /usr/lib/jni/libjicmp.so: OK
- searching for libjicmp6.so:
  - trying to load /libjicmp6.so: NO
  - trying to load /usr/share/opennms/lib/libjicmp6.so: NO
  - trying to load /usr/share/opennms/lib/linux64/libjicmp6.so: NO
  - trying to load /usr/java/packages/lib/libjicmp6.so: NO
  - trying to load /usr/lib/x86_64-linux-gnu/jni/libjicmp6.so: NO
  - trying to load /lib/x86_64-linux-gnu/libjicmp6.so: NO
  - trying to load /usr/lib/x86_64-linux-gnu/libjicmp6.so: NO
  - trying to load /usr/lib/jni/libjicmp6.so: OK
```

Figure 5.184: Create a database for OpenNMS

**Step 22:** Edit a file in OpenNMS.

```
nano /etc/default/opennms
```

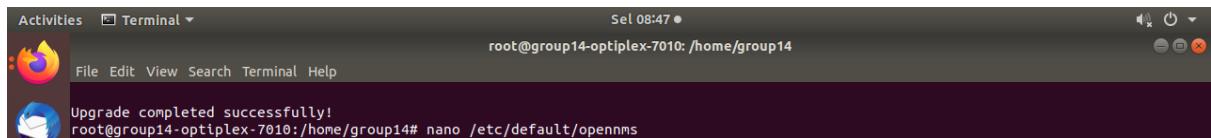


Figure 5.185: Edit a file in OpenNMS

**Uncomment JAVA\_HOME=/usr/lib/jvm/java-8-oracle**

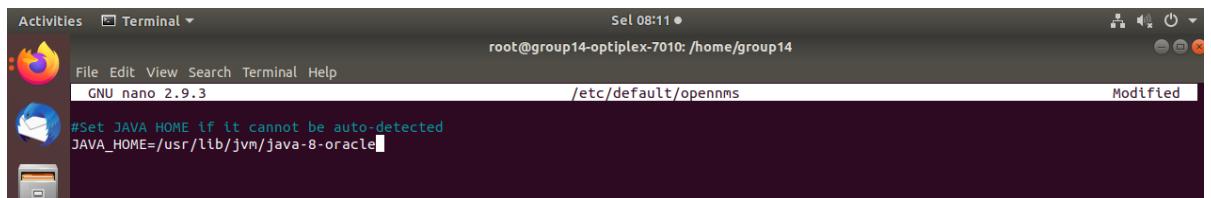
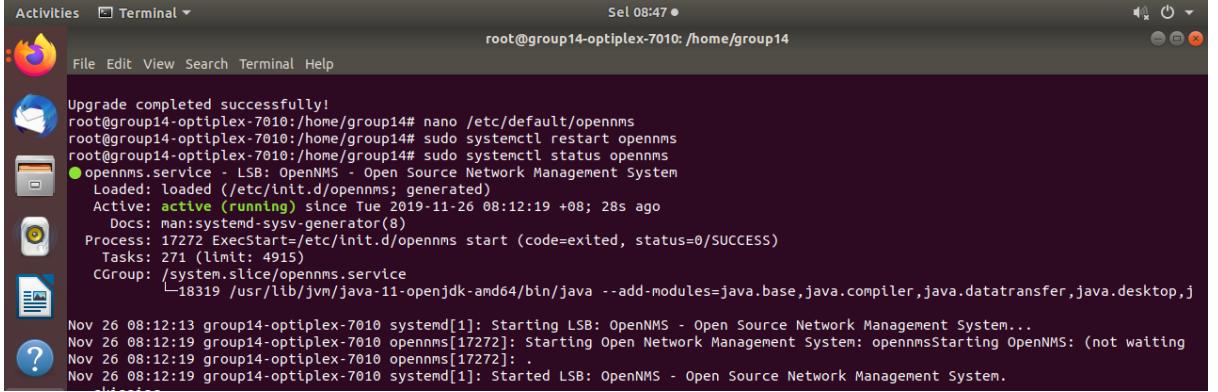


Figure 5.186: Editing file

**Step 23:** Restart and check status OpenNMS to see whether the opennms is active (running) or not.

```
sudo systemctl restart opennms
```

```
sudo systemctl status opennms
```



```
Activities Terminal ▾ Sel 08:47 ●
File Edit View Search Terminal Help
root@group14-optiplex-7010: /home/group14

Upgrade completed successfully!
root@group14-optiplex-7010:/home/group14# nano /etc/default/opennms
root@group14-optiplex-7010:/home/group14# sudo systemctl restart opennms
root@group14-optiplex-7010:/home/group14# sudo systemctl status opennms
● opennms.service - LSB: OpenNMS - Open Source Network Management System
  Loaded: loaded (/etc/init.d/opennms; generated)
  Active: active (running) since Tue 2019-11-26 08:12:19 +08; 28s ago
    Docs: man:systemd-sysv-generator(8)
  Process: 17272 ExecStart=/etc/init.d/opennms start (code=exited, status=0/SUCCESS)
    Tasks: 271 (limit: 4915)
   CGrou... /system.slice/opennms.service
          └─18319 /usr/lib/jvm/java-11-openjdk-amd64/bin/java --add-modules=java.base,java.compiler,java.datatransfer,java.desktop,j

Nov 26 08:12:13 group14-optiplex-7010 systemd[1]: Starting LSB: OpenNMS - Open Source Network Management System...
Nov 26 08:12:19 group14-optiplex-7010 opennms[17272]: Starting Open Network Management System: opennmsStarting OpenNMS: (not waiting
Nov 26 08:12:19 group14-optiplex-7010 opennms[17272]: .
Nov 26 08:12:19 group14-optiplex-7010 systemd[1]: Started LSB: OpenNMS - Open Source Network Management System.

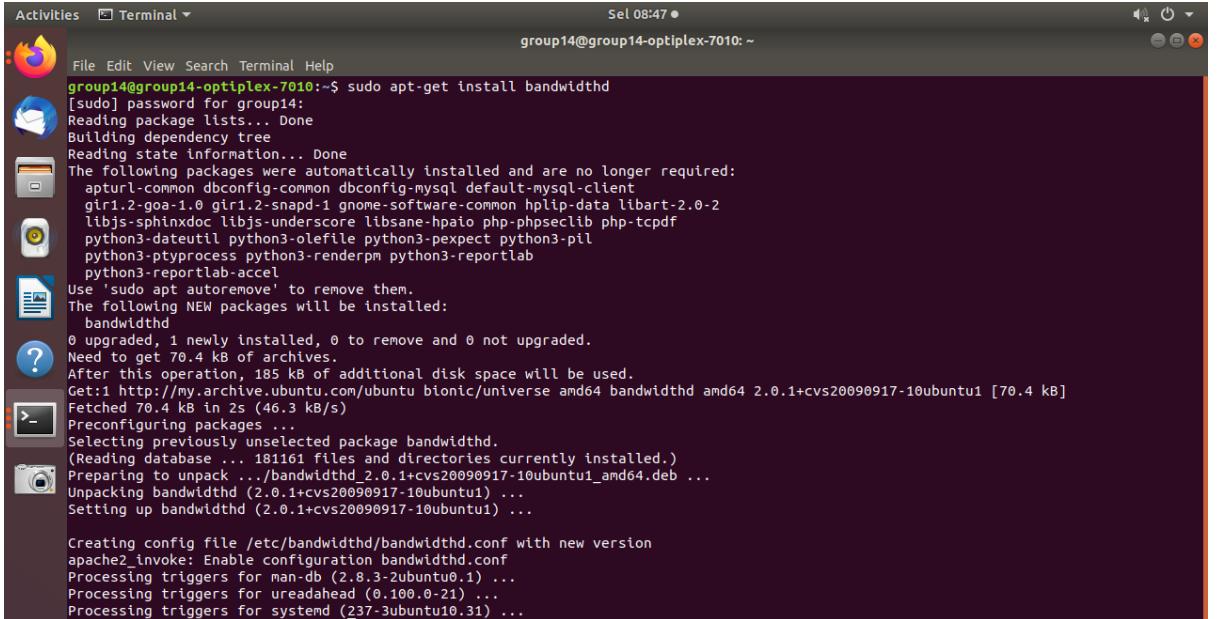
```

Figure 5.187: Restart and Check status OpenNMS

#### 5.3.13.4 Install bandwidthd

**Step 24:** Install **bandwidthd** to view the service up and down in graph.

```
sudo apt-get install bandwidthd
```



```
Activities Terminal ▾ Sel 08:47 ●
File Edit View Search Terminal Help
group14@group14-optiplex-7010: ~
group14@group14-optiplex-7010:~$ sudo apt-get install bandwidthd
[sudo] password for group14:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  apturl-common dbconfig-common dbconfig-mysql default-mysql-client
  gir1.2-goa-1.0 gir1.2-snapd-1 gnome-software-common hplib-data libart-2.0-2
  libjs-sphinxdoc libjs-underscore libsane-hpaio php-phpseclib php-tcpdf
  python3-dateutil python3-olefile python3-pexpect python3-pil
  python3-ptyprocess python3-renderpm python3-reportlab
  python3-reportlab-accel
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  bandwidthd
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 70.4 kB of additional disk space will be used.
After this operation, 185 kB of additional disk space will be used.
Get:1 http://my.archive.ubuntu.com/ubuntu bionic/universe amd64 bandwidthd amd64 2.0.1+cvs20090917-10ubuntu1 [70.4 kB]
Fetched 70.4 kB in 2s (46.3 kB/s)
Preconfiguring packages ...
Selecting previously unselected package bandwidthd.
(Reading database ... 181161 files and directories currently installed.)
Preparing to unpack .../bandwidthd_2.0.1+cvs20090917-10ubuntu1_amd64.deb ...
Unpacking bandwidthd (2.0.1+cvs20090917-10ubuntu1) ...
Setting up bandwidthd (2.0.1+cvs20090917-10ubuntu1) ...

Creating config file /etc/bandwidthd/bandwidthd.conf with new version
apache2_invoke: Enable configuration bandwidthd.conf
Processing triggers for man-db (2.8.3-2ubuntu0.1) ...
Processing triggers for ureadahead (0.100.0-21) ...
Processing triggers for systemd (237-3ubuntu10.31) ...
```

Figure 5.188: Install bandwidth

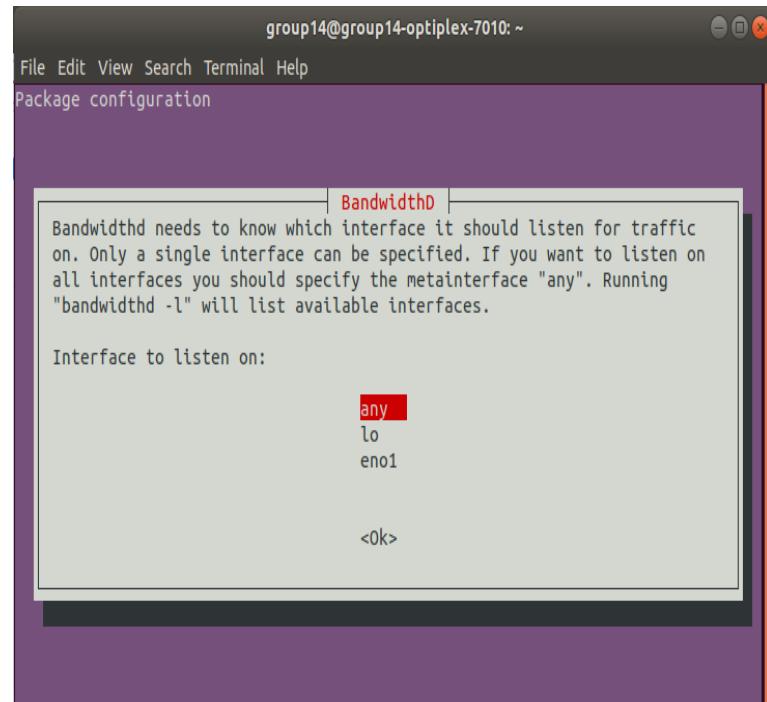


Figure 5.189: Interface to running in Bandwidthd choose any

Insert IP address and subnet mask to create graphs in bandwidthd

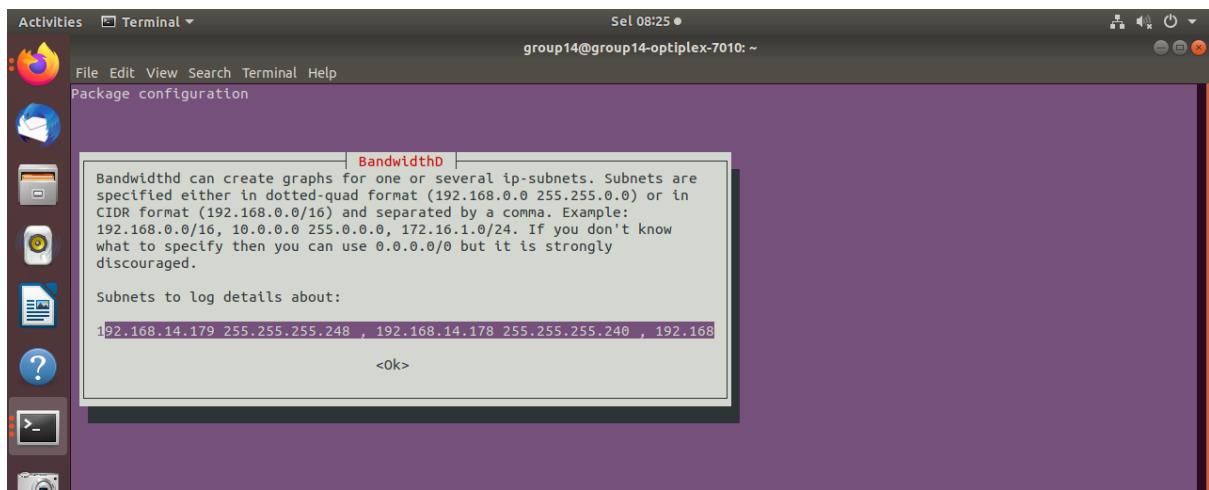
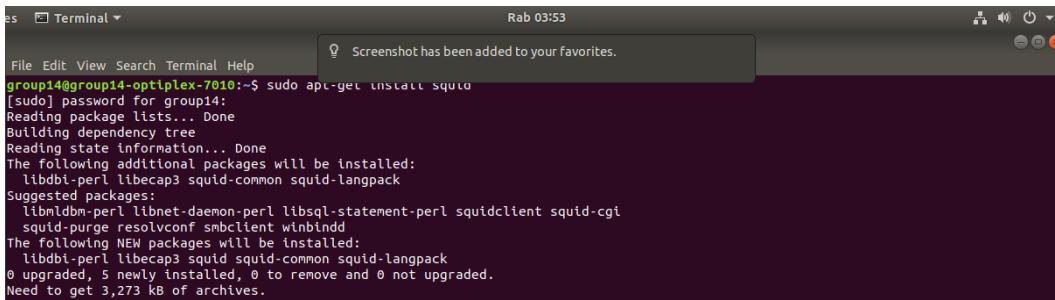


Figure 5.190: Insert IP address and subnet mask

### 5.3.14 PROXY SERVER

**Step 1:** Open Terminal and install squid package



```
es Terminal Rab 03:53
File Edit View Search Terminal Help
group14@group14-optiplex-7010:~$ sudo apt-get install squid
[sudo] password for group14:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
libdbi-perl libecap3 squid-common squid-langpack
Suggested packages:
  libmemcached-perl libsql-statement-perl squidclient squid-cgi
  squid-purge resolvconf smbclient winbind
The following NEW packages will be installed:
  libdbi-perl libecap3 squid squid-common squid-langpack
0 upgraded, 5 newly installed, 0 to remove and 0 not upgraded.
Need to get 3,273 kB of archives.
```

Figure 5.191: Install squid package

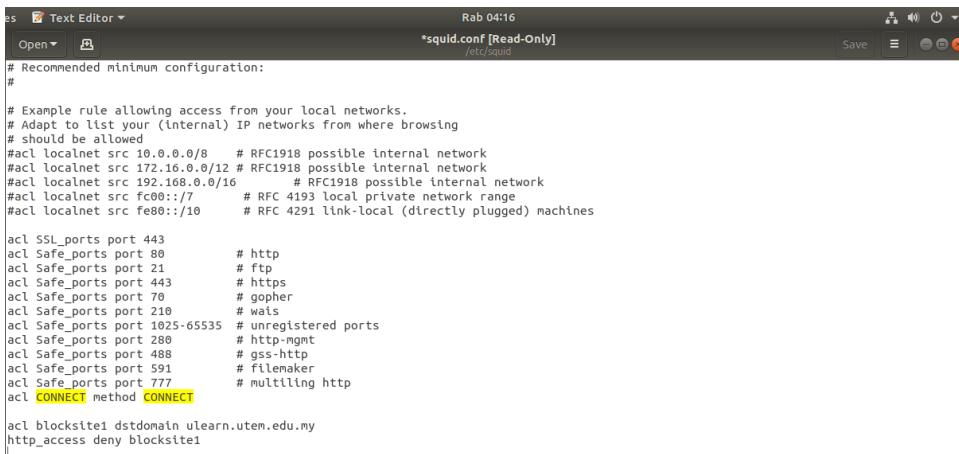
**Step 2:** Check squid status after installation



```
acl blocksitel dstdomain www.group13.com
http_access deny blocksitel
group14@group14-optiplex-7010:~$ service squid status
● squid.service - LSB: Squid HTTP Proxy version 3.x
  Loaded: loaded (/etc/init.d/squid; generated)
  Active: active (running) since Wed 2019-10-23 03:52:19 +08; 1min 55s ago
    Docs: man:systemd-sysv-generator(8)
  Tasks: 4 (limit: 4915)
  CGroup: /system.slice/squid.service
          └─11143 /usr/sbin/squid -YC -f /etc/squid/squid.conf
              ├─11145 (squid-1) -YC -f /etc/squid/squid.conf
              ├─11149 (logfile-daemon) /var/log/squid/access.log
              └─11150 (pinger)
```

Figure 5.192: Checking squid status

**Step 3:** Edit configuration file, run command on terminal “gedit /etc/squid/squid.conf” and add the command below. This configuration shows how to block ulearn and other’s group web server



```
# Recommended minimum configuration:
#
# Example rule allowing access from your local networks.
# Adapt to list your (internal) IP networks from where browsing
# should be allowed
acl localnet src 10.0.0.0/8      # RFC1918 possible internal network
acl localnet src 172.16.0.0/12    # RFC1918 possible internal network
acl localnet src 192.168.0.0/16   # RFC1918 possible internal network
acl localnet src fc00::/7        # RFC 4193 local private network range
acl localnet src fe80::/10       # RFC 4291 link-local (directly plugged) machines

acl SSL_ports port 443          # https
acl Safe_ports port 80            # http
acl Safe_ports port 21            # ftp
acl Safe_ports port 443           # https
acl Safe_ports port 70            # gopher
acl Safe_ports port 210           # wais
acl Safe_ports port 1025-65535   # unregistered ports
acl Safe_ports port 280           # http-mgmt
acl Safe_ports port 488           # gss-http
acl Safe_ports port 591           # filemaker
acl Safe_ports port 777           # multilingual http
acl CONNECT method CONNECT

acl blocksitel dstdomain ulearn.utm.edu.my
http_access deny blocksitel
```

Figure 5.193: Configure the proxy file

**Step 4:** Save the configuration file and restart squid, terminal command “squid service restart”.

**Step 5:** Open browser > Preference > Advanced > Network & Setting > Manual Proxy configuration to setup proxy

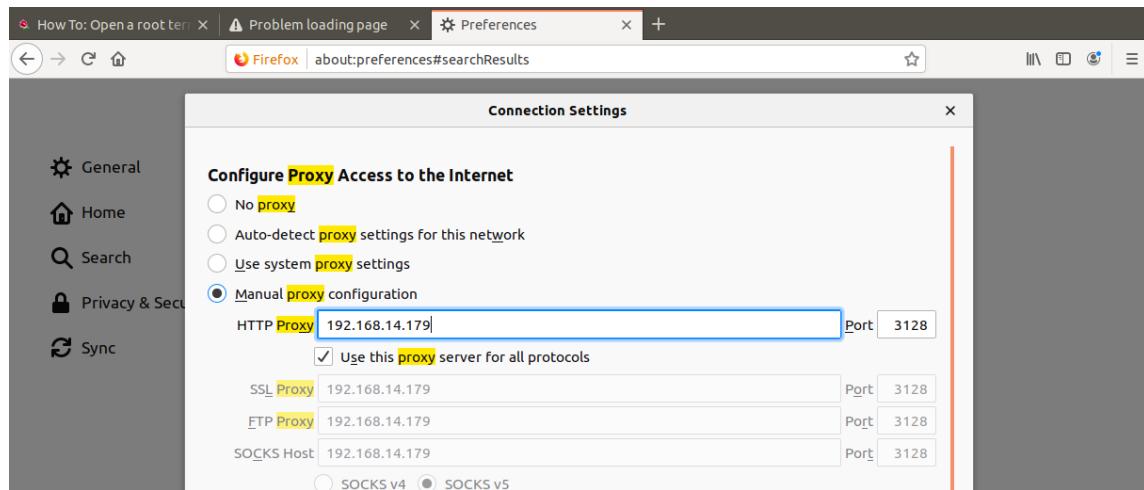
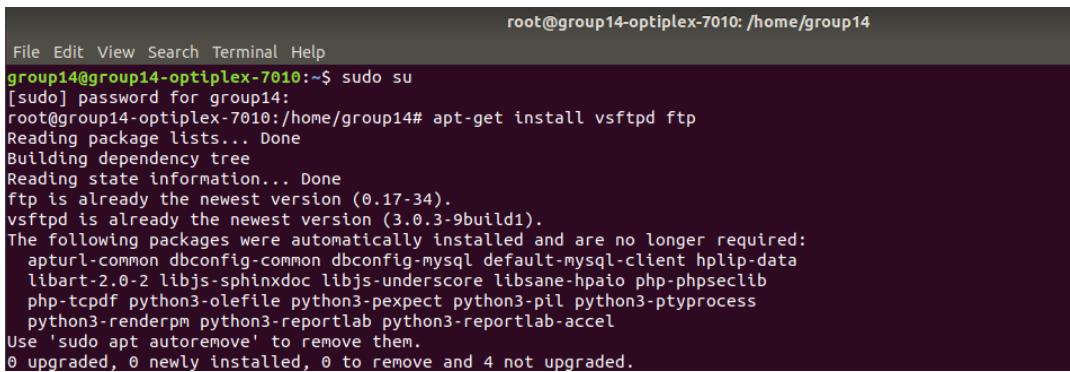


Figure 5.194: Setup proxy on browser

### 5.3.15 SECURED FTP

**Step 1:** Open terminal and type these command to install vsftpd.



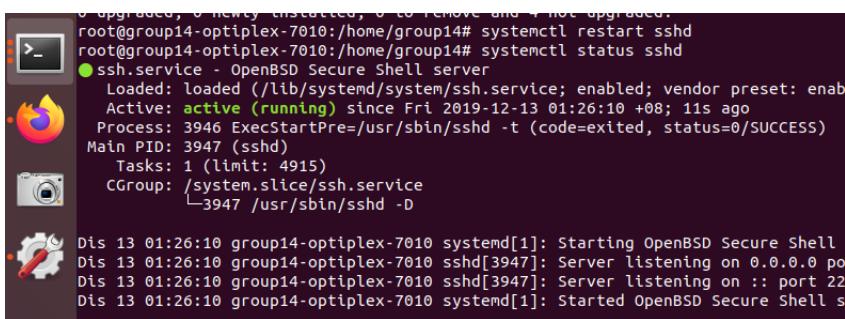
```
root@group14-optiplex-7010: /home/group14
File Edit View Search Terminal Help
group14@group14-optiplex-7010:~$ sudo su
[sudo] password for group14:
root@group14-optiplex-7010:/home/group14# apt-get install vsftpd ftp
Reading package lists... Done
Building dependency tree
Reading state information... Done
ftp is already the newest version (0.17-34).
vsftpd is already the newest version (3.0.3-9build1).
The following packages were automatically installed and are no longer required:
  apturl-common dbconfig-common dbconfig-mysql default-mysql-client hplip-data
  libart-2.0-2 libjs-sphinxdoc libjs-underscore libsane-hpaio php-phpseclib
  php-tcpdf python3-olefile python3-pexpect python3-pil python3-ptyprocess
  python3-renderpm python3-reportlab python3-reportlab-accel
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 4 not upgraded.
```

Figure 5.195: Install vsftpd

**Step 2:** To start and to see the status of the system, type command

systemctl start vsftpd

systemctl status vsftpd



```
0 upgraded, 0 newly installed, 0 to remove and 4 not upgraded.
root@group14-optiplex-7010:/home/group14# systemctl restart sshd
root@group14-optiplex-7010:/home/group14# systemctl status sshd
● ssh.service - OpenBSD Secure Shell server
  Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enab
  Active: active (running) since Fri 2019-12-13 01:26:10 +08; 11s ago
    Process: 3946 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 3947 (sshd)
     Tasks: 1 (limit: 4915)
    CGroup: /system.slice/ssh.service
           └─3947 /usr/sbin/sshd -D

Dis 13 01:26:10 group14-optiplex-7010 systemd[1]: Starting OpenBSD Secure Shell
Dis 13 01:26:10 group14-optiplex-7010 sshd[3947]: Server listening on 0.0.0.0 po
Dis 13 01:26:10 group14-optiplex-7010 sshd[3947]: Server listening on :: port 22
Dis 13 01:26:10 group14-optiplex-7010 systemd[1]: Started OpenBSD Secure Shell s
```

Figure 5.196: Open systemctl start vsftpd

**Step 3:** In root user, open vsftpd config file and change some parameter to configure the FTP server.



```
[1]+  Stopped                  vi /etc/vsftpd.conf
root@group14-optiplex-7010:/home/group14# vim -r /etc/vsftpd.conf
```

Figure 5.197: Open vsftpd config file

**Step 4:** Do not enable anonymous user to login to the FTP server.

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

Figure 5.198: Allow anonymous FTP

**Step 5:** Uncomment **write\_enable=YES**.

```
#  
# Uncomment this to enable any form of FTP write command.  
write_enable=YES  
#
```

Figure 5.199: Uncomment **write\_enable=YES**

**Step 6:** Uncomment **xferlog\_file=/var/log/vsftpd.conf** to enabling log for FTP server.

```
# You may override where the log file goes if you like. The default is shown  
# below.  
xferlog_file=/var/log/vsftpd.log  
#
```

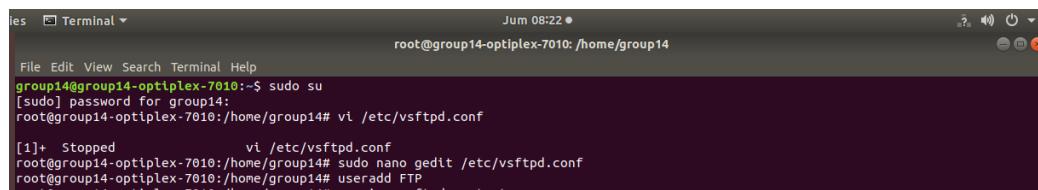
Figure 5.200: FTP server log

**Step 7:** Use **local\_root=public\_html** and **use\_localtime =YES** to the end.

```
#  
# Uncomment this to indicate that vsftpd use a utf8 filesystem.  
#utf8_filesystem=YES  
  
local_root=public_html  
use_localtime=YES
```

Figure 5.201: Adding comment to the end

**Step 8:** Then, add a user in Ubuntu using this command **useradd FTP**



The screenshot shows a terminal window with the following session:

```
File Edit View Search Terminal Help  
group14@group14-optiplex-7010:~$ sudo su  
[sudo] password for group14:  
root@group14-optiplex-7010:/home/group14# vi /etc/vsftpd.conf  
[1]+ Stopped vi /etc/vsftpd.conf  
root@group14-optiplex-7010:/home/group14# sudo nano gedit /etc/vsftpd.conf  
root@group14-optiplex-7010:/home/group14# useradd FTP
```

Figure 5.202: Add new user

**Step 9:** Restart vsftpd to accept the changes that have been made.

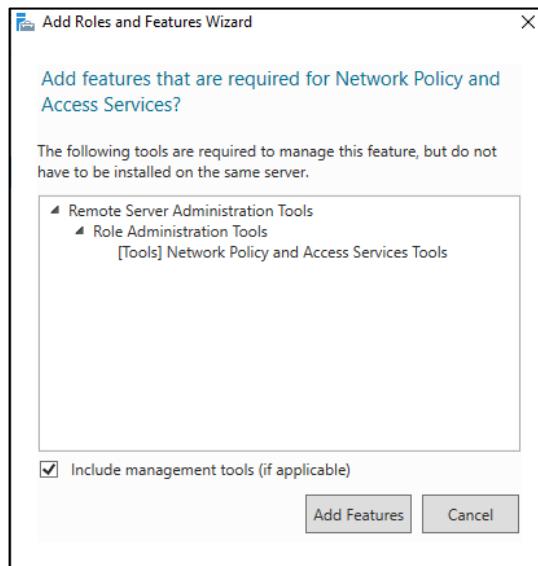
```
root@group14-optiplex-7010:/home/group14# service vsftpd restart  
root@group14-optiplex-7010:/home/group14# service vsftpd restart  
root@group14-optiplex-7010:/home/group14#
```

Figure 5.203: Restart vsftpd

### **5.3.16 AAA (AUTHENTICATION, AUTHORIZATION AND ACCOUNTING) USING RADIUS.**

**STEP 1:** Open server manager, click “Roles” and then “Add Roles”. After that, select the server selection which is server pool and click “Next”.

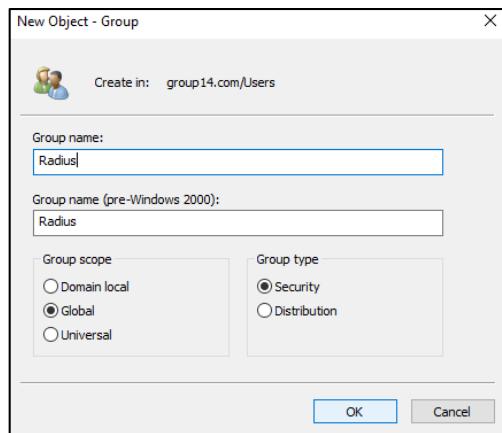
**STEP 2:** At the Server Roles, click on “Network Policy and Access Services” and click “Next” to continue.



*Figure 5.204: Add Roles*

**STEP 3:** At the confirmation click the install button and wait until the installation finish and click “close”

**STEP 4:** Create a new group in Active Directory such as Radius as the group name.



*Figure 5.205: Create a new group*

**STEP 5:** Create a user for example raduser with a password and set it into the group that just created.

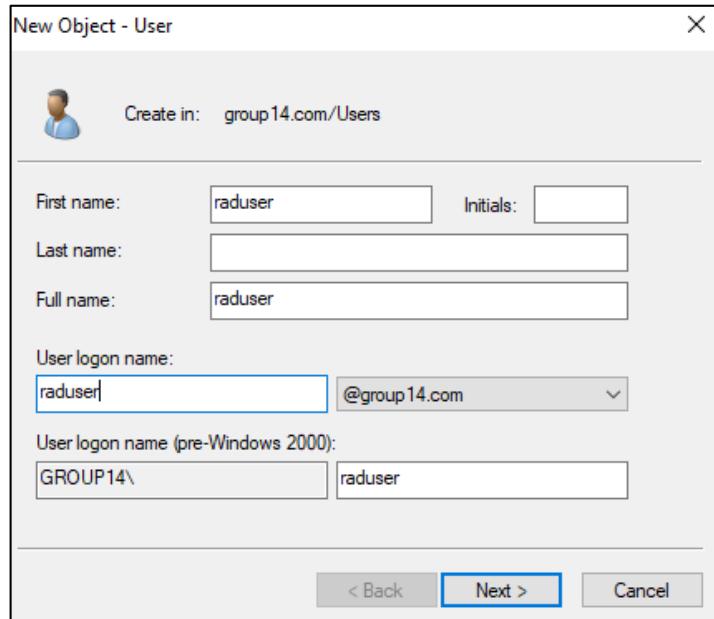


Figure 5.206: Create new user

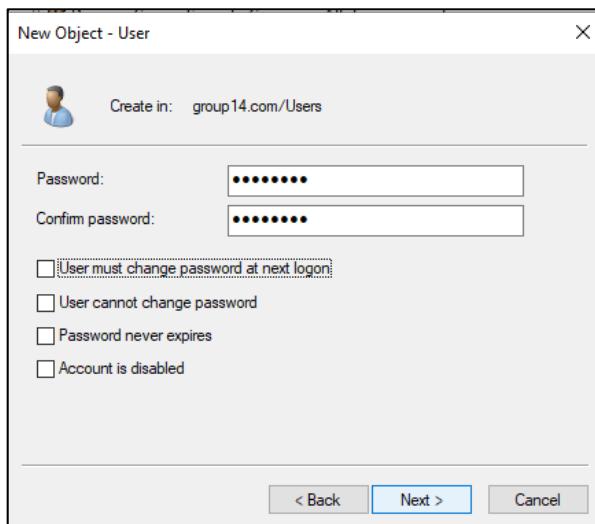


Figure 5.207: Input password for the user

**STEP 6:** Create AAA in DNS Manager, click New Host (A or AAAA)

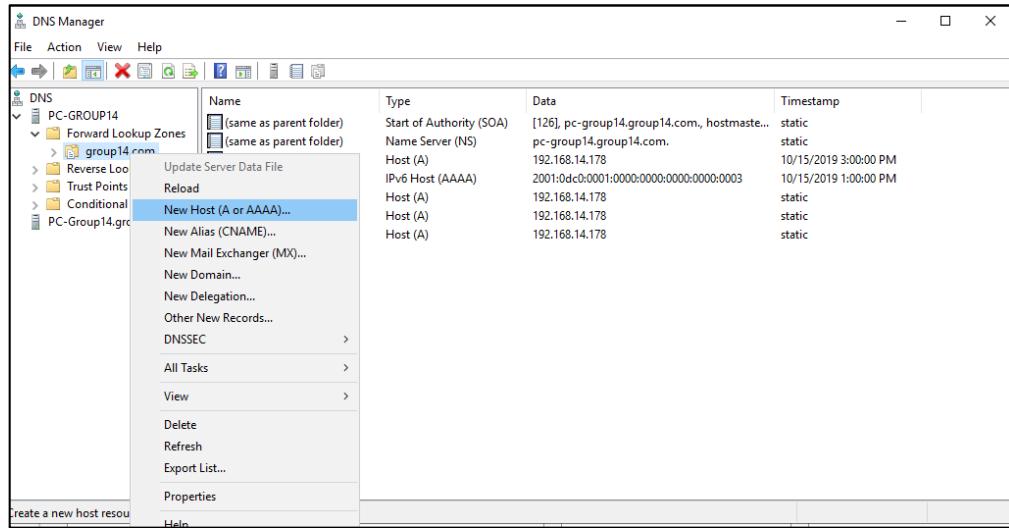


Figure 5.208: Create AAA in DNS Manager

**STEP 7:** Insert the router name with its IP gateway such as G14Router and IP address of 192.168.14.177

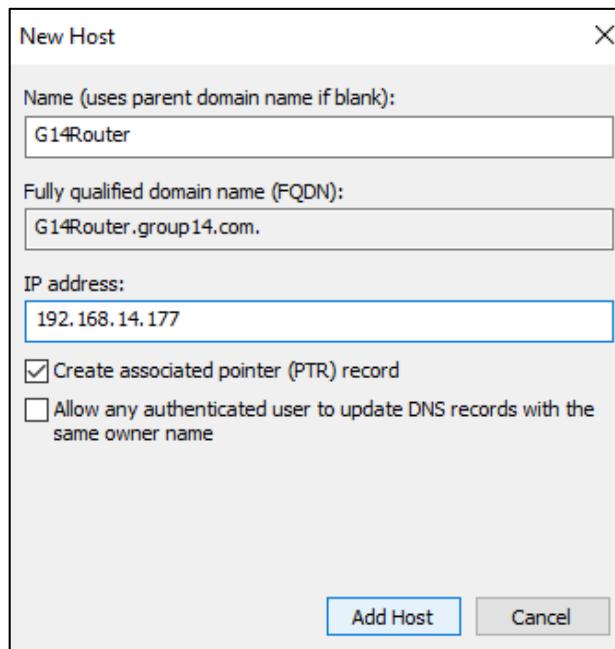


Figure 5.209: Set a new host

**STEP 8:** After that, open Network Policy Server (NPS) and right click on it to register the server in Active Directory (AD).

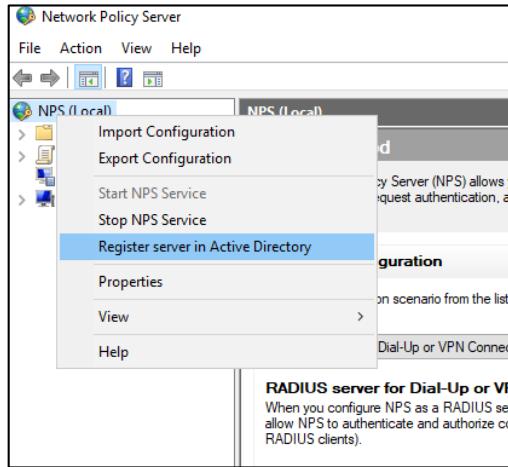


Figure 5.210: Register server to Active Directory

**STEP 9:** Next, create a new RADIUS Clients. Set the friendly name as the router name, DNS name and for the shared secret, pick manual and insert our own password or shared secret.

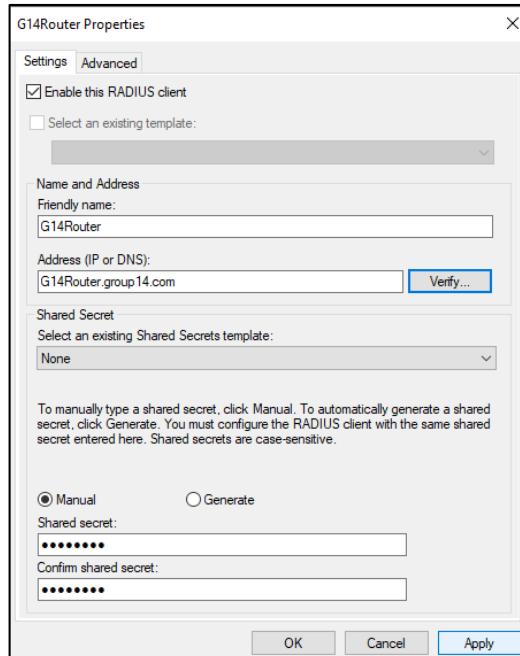


Figure 5.211: Set the friendly name and Shared secret

**STEP 10:** Click on verify to verify the DNS and click on resolve to show the IP address. Go to the advanced tab and change the vendor name to Cisco.

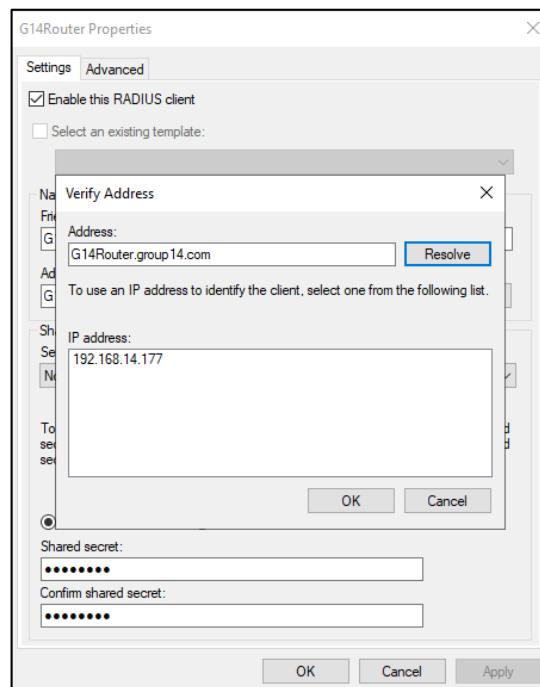


Figure 5.212: Verify the Address

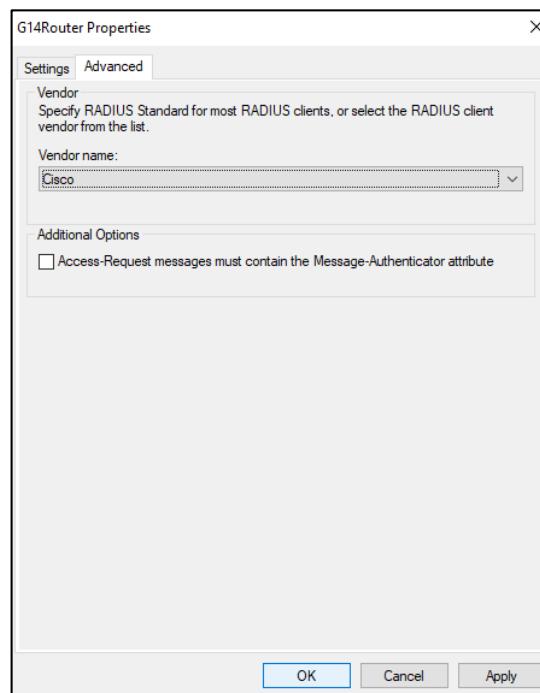


Figure 5.213: Change the vendor name

**STEP 11:** Next, create a new policy. Right click on the network policies and click new.

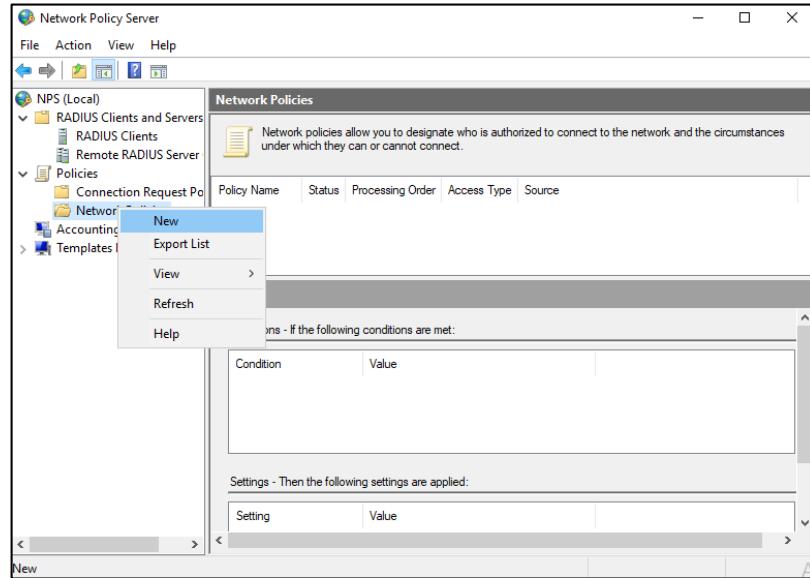


Figure 5.214: Creating new policy

**Step 12:** Set the policy name and add a new condition which is for the user groups and choose Radius group and click Next.

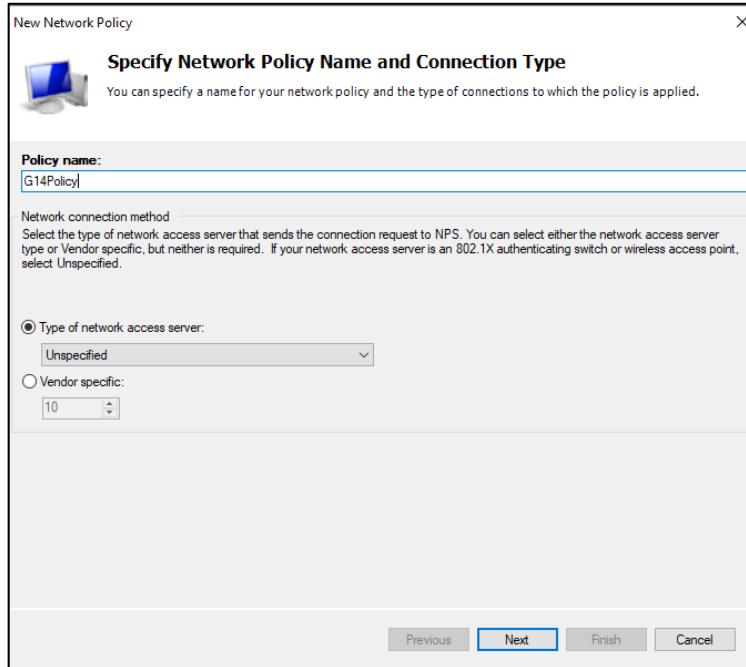


Figure 5.215: Set policy name

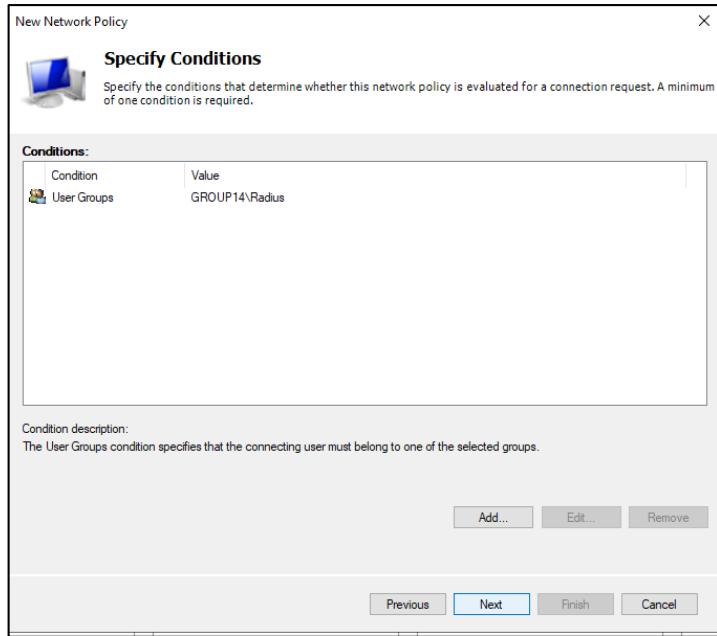


Figure 5.216: Set a specify conditions (user group)

**STEP 13:** Choose access granted and click Next, and choose the two authentication methods as shown in the figure and click Next to continue.

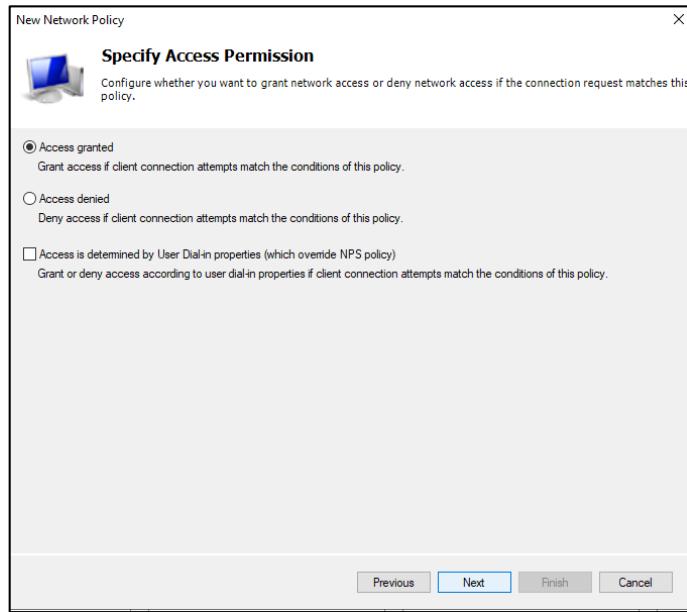
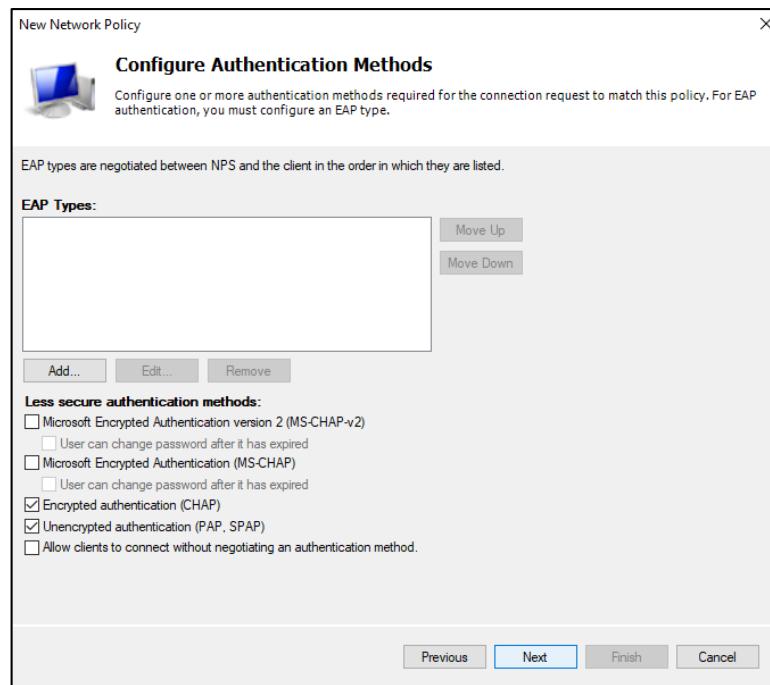
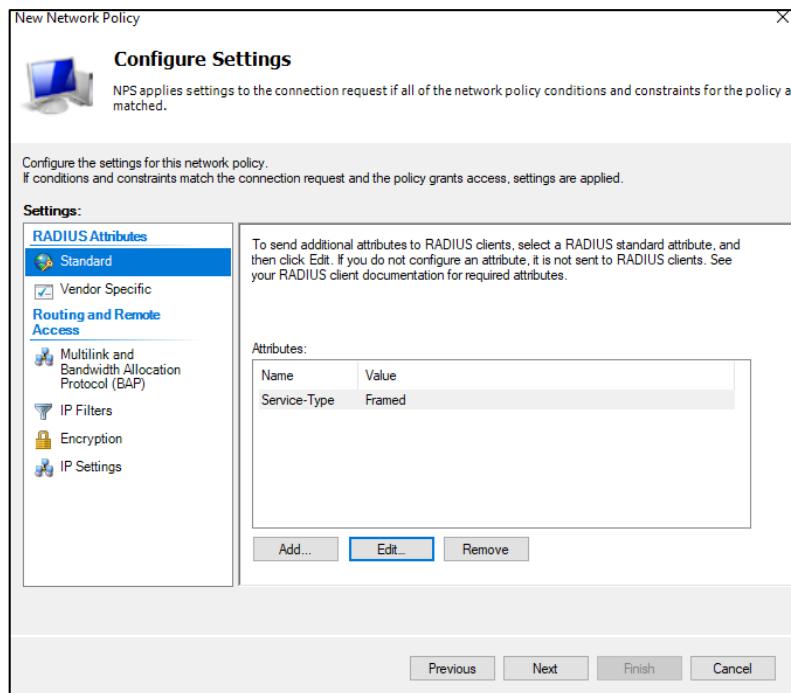


Figure 5. 217: Select the access granted permission



*Figure 5. 218: Choose the authentication methods*

**STEP 14:** At the standard tab, change the service-type from framed into others (Login).



*Figure 5. 219: Change the value of service-type*

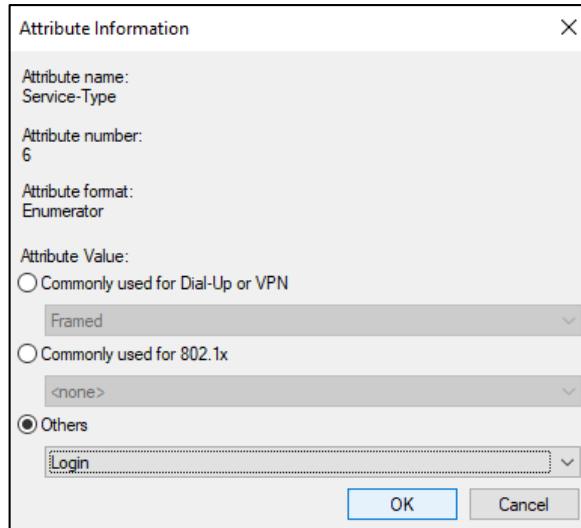


Figure 5. 220: Choose the others attribute and set it to login

**STEP 15:** At the vendor tab click on the add vendor specific attributes and choose cisco as the vendor.

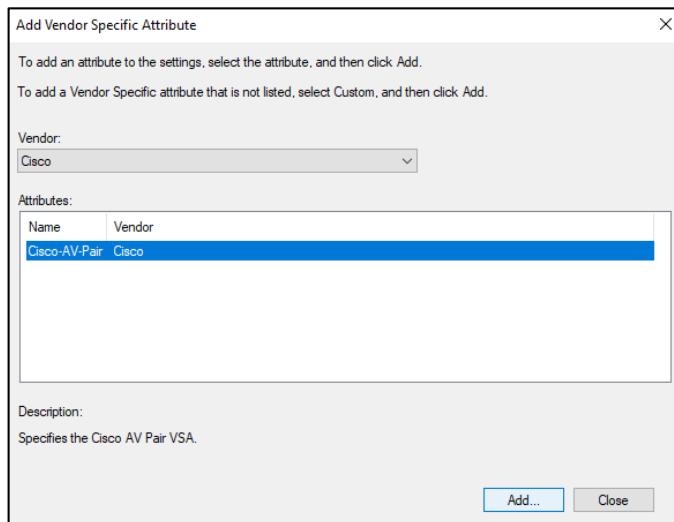


Figure 5. 221: Add the vendor

**STEP 16:** Add the attribute value as shell:priv-lvl=15 and click Next and Finish.

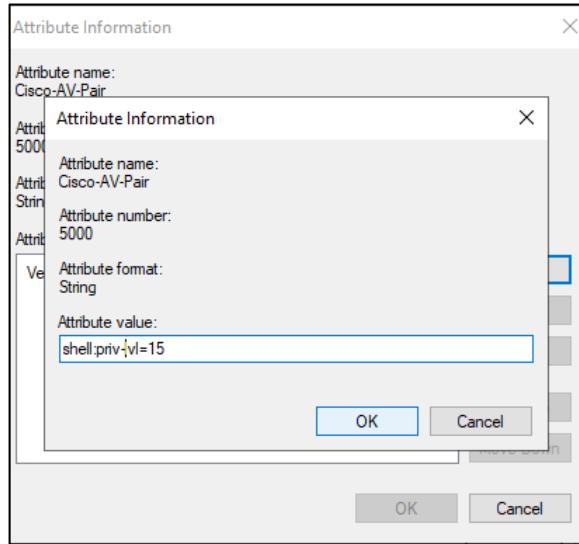


Figure 5. 222: Add the attribute value

**STEP 17:** Click on the accounting and configure a new accounting.

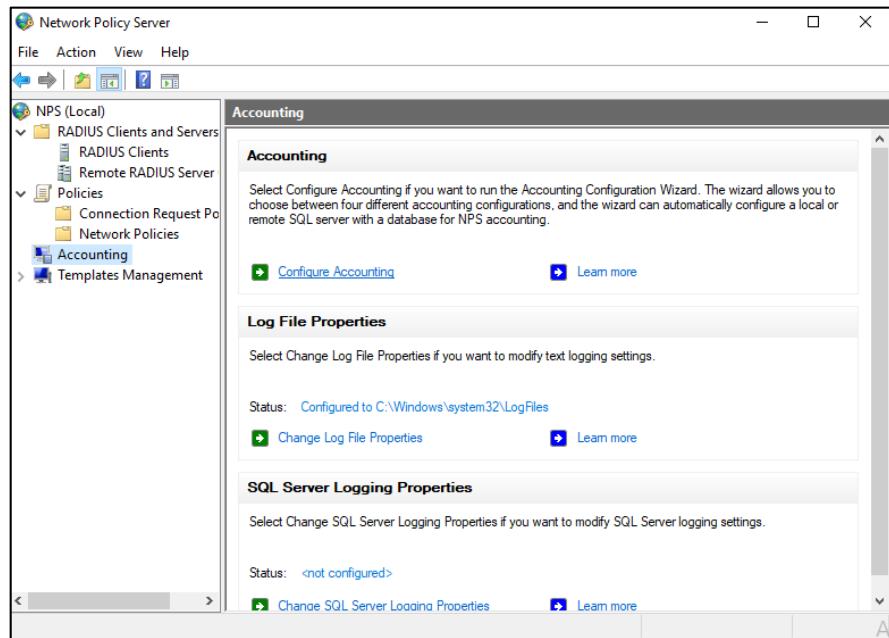


Figure 5. 223: Configure new accounting

**STEP 18:** Select the log to a text file on the local computer.

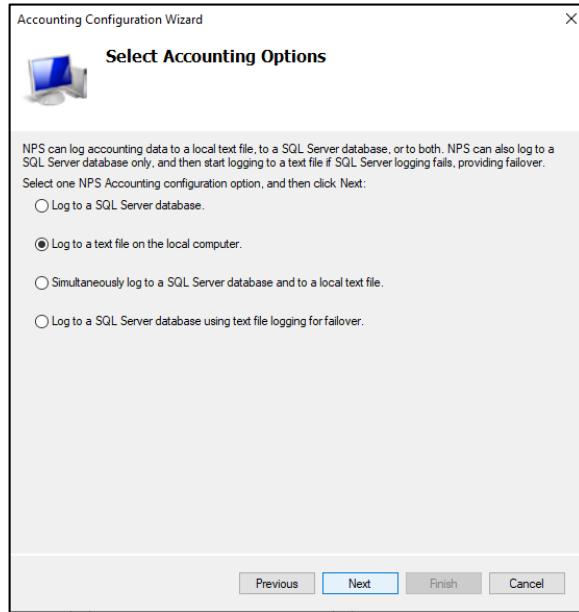


Figure 5.224: Select Accounting options

**STEP 19:** Select the location for the log file, usually let it be default.

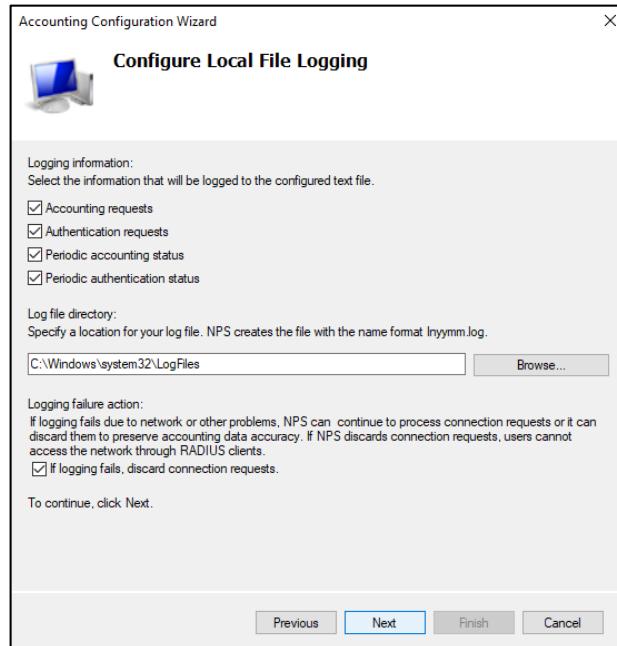
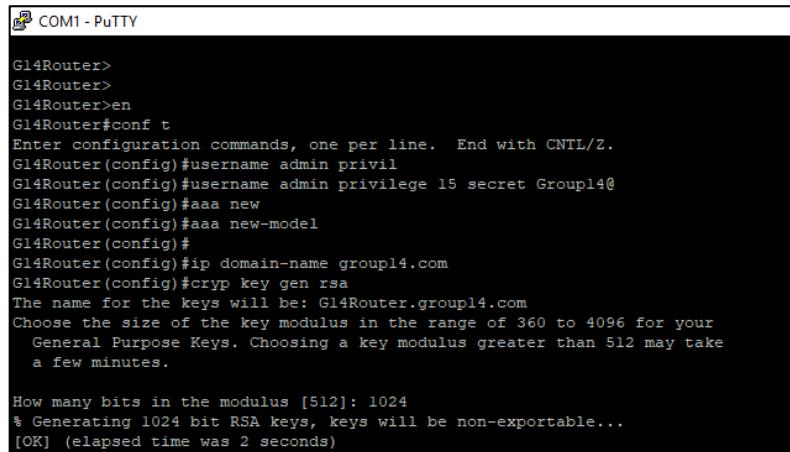


Figure 5.225: Configure Local File

**STEP 20:** Close the accounting configuration wizard by clicking the close button.

**STEP 21:** Configure the AAA inside the router with the configuration shown in the figure below.

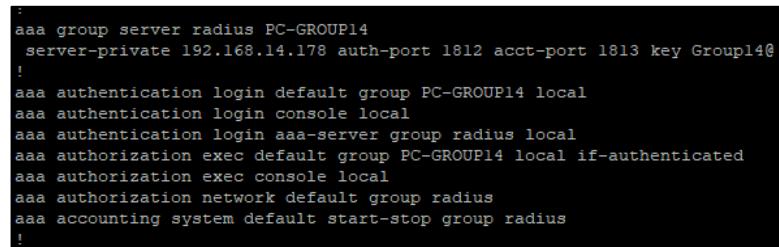


A screenshot of a PuTTY terminal window titled "COM1 - PuTTY". The window displays the configuration of AAA on a Cisco router. The configuration includes creating a new AAA model, specifying a domain name, generating RSA keys, and setting the key modulus size. The session identifier "G14Router" is visible at the top left.

```
G14Router>
G14Router>
G14Router>en
G14Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
G14Router(config)#username admin privilege 15 secret Group14@
G14Router(config)#aaa new
G14Router(config)#aaa new-model
G14Router(config)#
G14Router(config)#ip domain-name group14.com
G14Router(config)#crypt key gen rsa
The name for the keys will be: G14Router.group14.com
Choose the size of the key modulus in the range of 360 to 4096 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 2 seconds)
```

*Figure 5. 226: Configuration for local user*



The configuration text shows the complete AAA setup. It starts with an "aaa group server radius PC-GROUP14" command, followed by "server-private 192.168.14.178 auth-port 1812 acct-port 1813 key Group14@!". Subsequent lines define authentication methods (login default group, login console), authorization (exec default group, exec console), and accounting (network default group, accounting system start-stop group).

```
aaa group server radius PC-GROUP14
    server-private 192.168.14.178 auth-port 1812 acct-port 1813 key Group14@
!
aaa authentication login default group PC-GROUP14 local
aaa authentication login console local
aaa authentication login aaa-server group radius local
aaa authorization exec default group PC-GROUP14 local if-authenticated
aaa authorization exec console local
aaa authorization network default group radius
aaa accounting system default start-stop group radius
!
```

*Figure 5. 227: Configuration for the AAA*

**STEP 22:** After configuration, restart the putty and this time we need to log in into the router before we can use the router.

### 5.3.17 VLAN AND PORT SECURITY

#### 5.3.17.1 VLAN SECURITY

**STEP 1:** Create a new vlan which is VLAN60 and name it as unused\_ports. After that, change the state into suspend.

```
G14_switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
G14_switch(config)#vlan 60
G14_switch(config-vlan)#state suspend
G14_switch(config-vlan)#end
G14_switch#con
```

Figure 5.228: Create VLAN60

**STEP 2:** Put the unused port which is g0/1 and g0/2 into VLAN60

```
G14_switch(config)#int range g0/1-2
G14_switch(config-if-range)#switchport mode access
G14_switch(config-if-range)#switchport access vlan 60
G14_switch(config-if-range)#end
G14_switch#
```

Figure 5.229: Put unused port into VLAN60

**STEP 3:** Assign used vlan into trunk ports and change native vlan into 3

```
COM1 - PuTTY
G14_switch(config)#int fa0/24
G14_switch(config-if)#swit
G14_switch(config-if)#switchport mode trunk
G14_switch(config-if)#switchport trunk allowed vlan 10,20,30,40,1
G14_switch(config-if)#end
```

Figure 5.230: Assign all usable ports into trunk

```
G14_switch(config)#int fa0/24
G14_switch(config-if)#swi
G14_switch(config-if)#switchport trunk native vlan 3
G14_switch(config-if)#exi
```

Figure 5.231: Change native vlan into 3

### 5.3.17.2 PORT SECURITY

**STEP 1:** Type a command for errdisable which is to avoid having to manually intervene every time a port-security violation forces an interface into the error-disabled state, one can enable auto-recovery for port security violations.

```
errdisable recovery cause psecure-violation
errdisable recovery interval 600
```

*Figure 5.232: Command for violation*

**STEP 2:** Set the port which one port will remember only one mac address by using static mac address

```
interface FastEthernet0/1
switchport access vlan 10
switchport mode access
switchport port-security
switchport port-security violation restrict
switchport port-security mac-address sticky
```

*Figure 5.233: Command for WIndows Server*

```
interface FastEthernet0/2
switchport access vlan 10
switchport mode access
switchport port-security
switchport port-security violation restrict
switchport port-security mac-address sticky
!
```

*Figure 5.234: Command for Ubuntu Server*

```
interface FastEthernet0/3
switchport access vlan 10
switchport mode access
switchport port-security
switchport port-security violation restrict
switchport port-security mac-address sticky
!
```

*Figure 5.235: Command for Debian Server*

## 5.3.18 WEB HARDENING

### 5.3.18.1 WINDOWS AUTHENTICATION

#### STEP 1: Add Roles and Features in IIS Servers

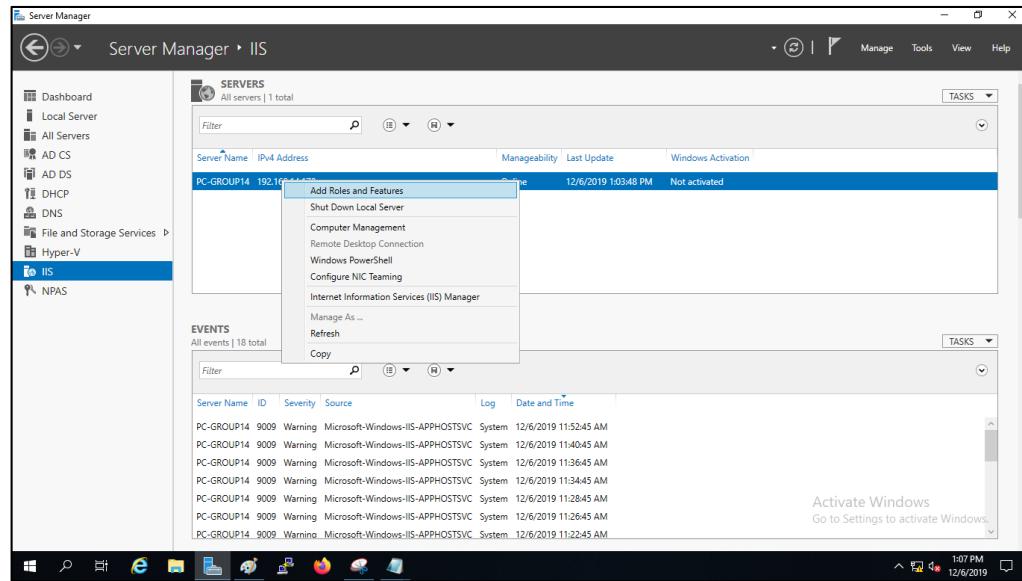


Figure 5.236: Add Roles and Features

#### STEP 2: Choose Windows Authentication and click Next and Install the features.

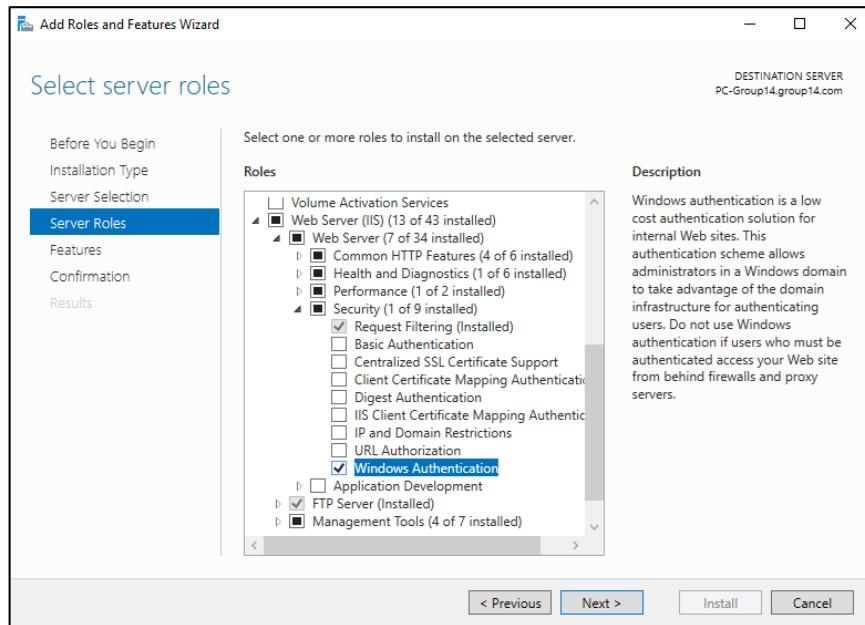
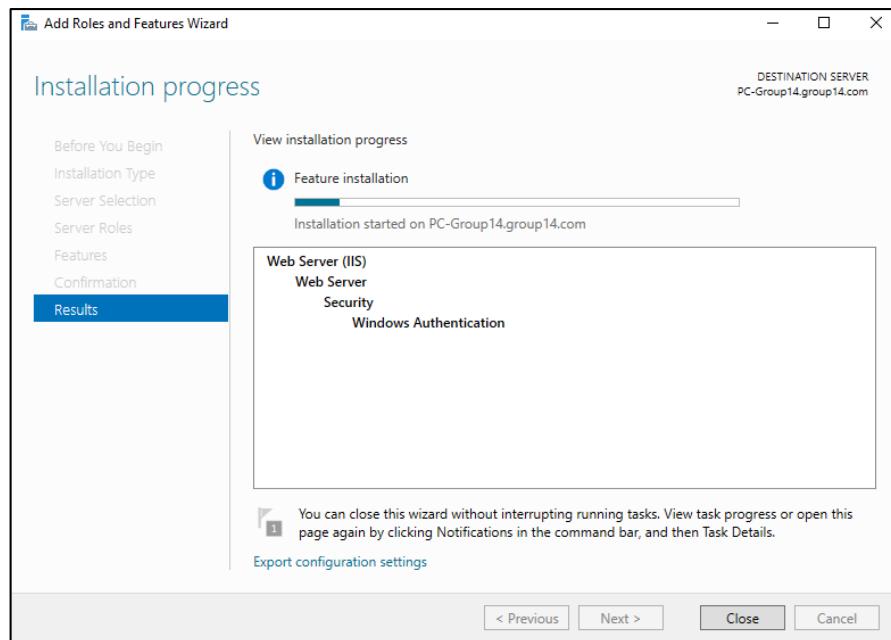
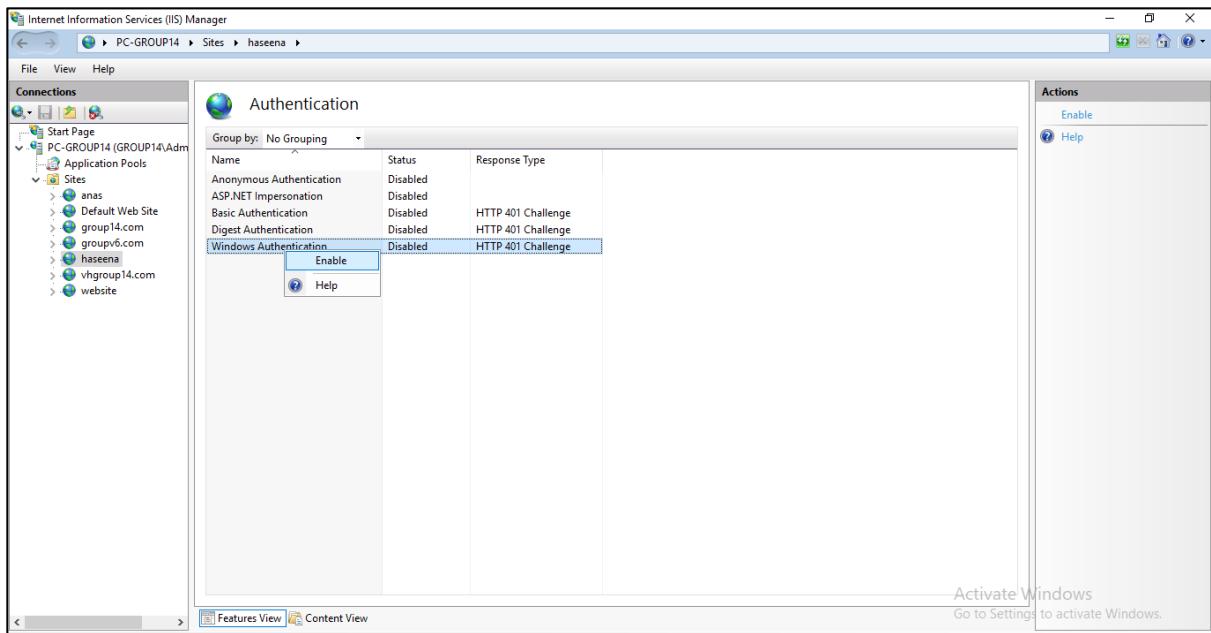


Figure 5.237: Choose Windows Authentication



*Figure 5. 238: Install Windows Authentication*

**STEP 3:** Open the IIS Server and go to the authentication and disable the anonymous authentication and enable the windows authentication



*Figure 5. 239: Disable the anonymous authentication and enable the Windows authentication*

### 5.3.18.2 BASIC AUTHENTICATION

**STEP 1:** Add Roles and Features in IIS Servers and choose basic authentication and click Next.

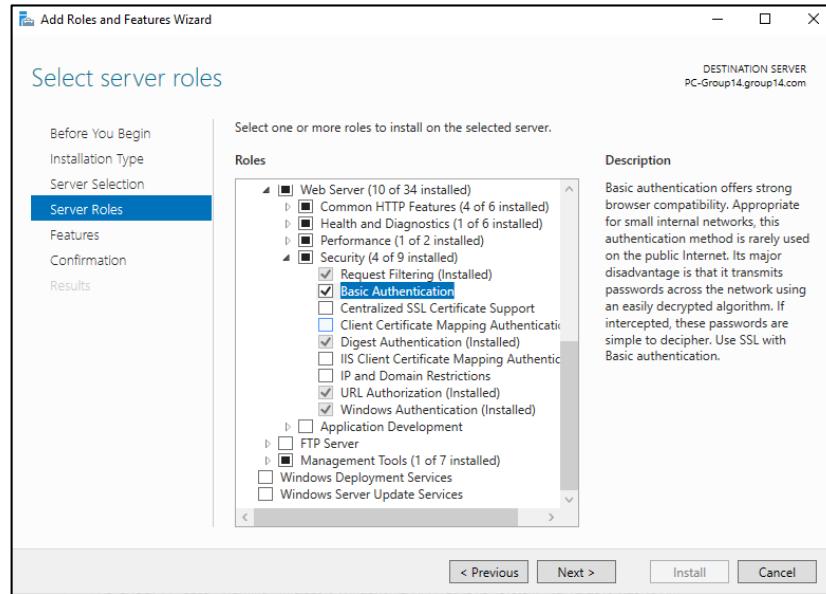


Figure 5. 240: Choose basic authentication

**STEP 2:** Click install and wait until it finishes install and click close.

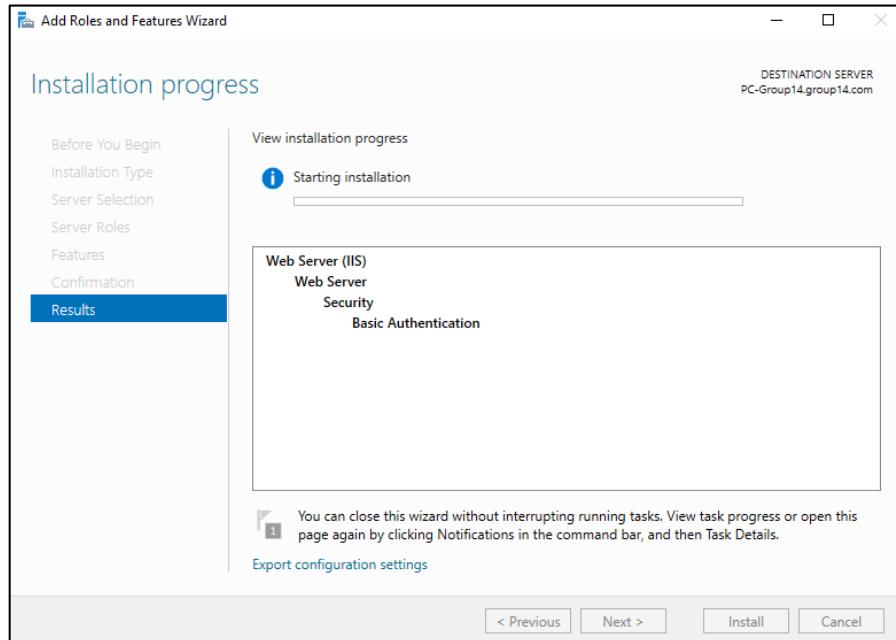


Figure 5. 241: Install basic authentication features

**STEP 3:** Open the IIS Server and go to the authentication and disable the all the authentication except the basic authentication.

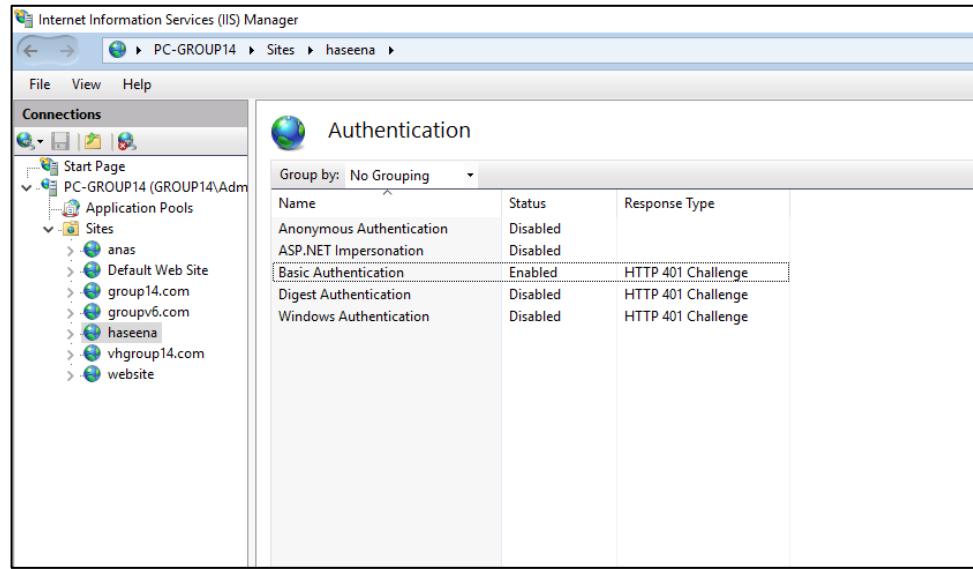


Figure 5. 242: Enable the basic authentication

### 5.3.18.3 URL AUTHORIZATION

**STEP 1:** Right click on the IIS Server and click on Add Roles and Features and choose URL Authorization.

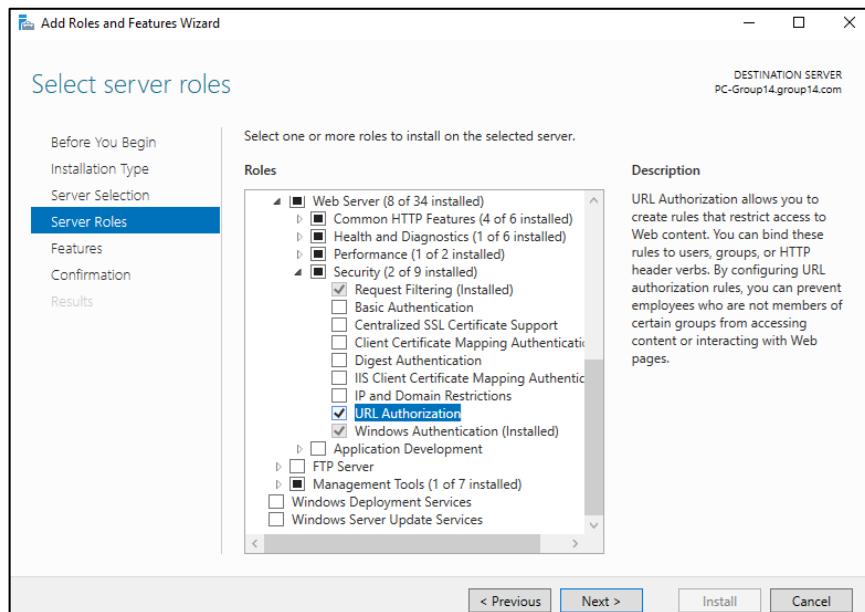


Figure 5. 243: Add URL Authorization features

**STEP 2:** Click install and wait until the features finishes download and click close.

**STEP 3:** Open the IIS server manager and click on the Authorization Rules and remove the existing rule.

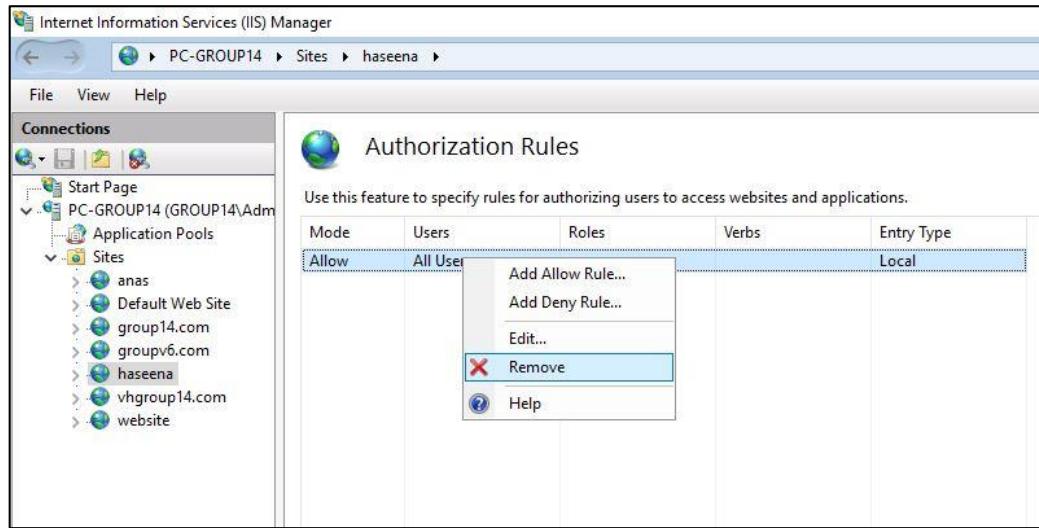


Figure 5. 244: Remove the existing rule

**STEP 4:** Add new authorization rule on the specific website. In this case, the authorization rule is for only specific users which is ‘nuthaseena’ that only can access the haseena.group14.com

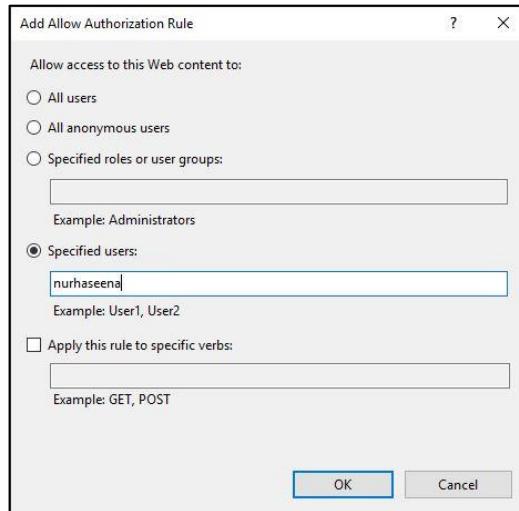


Figure 5. 245: Specific users for the authorization rule

#### 5.3.18.4 IP AND DOMAIN RESTRICTION

**STEP 1:** Click on Add Roles and Features on the IIS Server and choose the IP and Domain Restriction.

**STEP 2:** Click on the install button to install the features and close it after finishes the installation.

**STEP 3:** Click on the desired website to put the IP restriction. In this case, the IP that being used is 192.168.14.180 which is the Debian and click okay to close it.

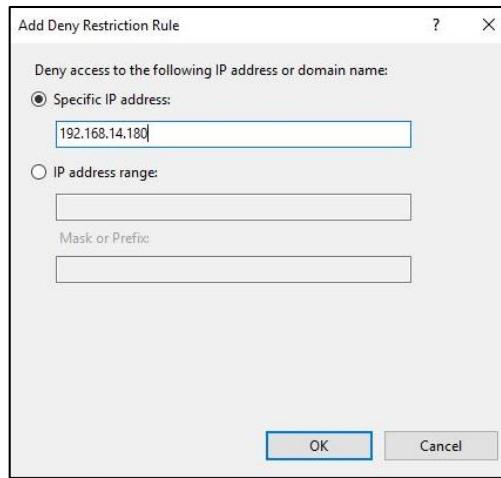


Figure 5. 246: Insert the IP Address to restrict from access the websites

**STEP 4:** Right click and click on edit the settings and change the access for unspecified clients to ‘deny’ and close it.

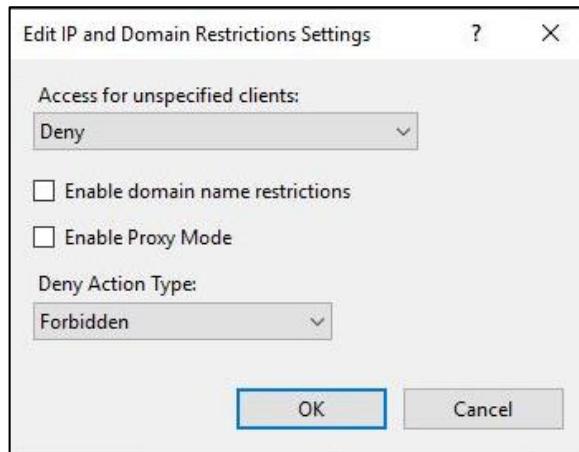


Figure 5. 247: Change the settings

### 5.3.18.5 REQUEST FILTERING

**STEP 1:** Install the request filtering features if it is not install yet. In this case, the request filtering was already installed. Make sure that the website contains any picture or any file extension. For example, the website contains a picture in .png format.

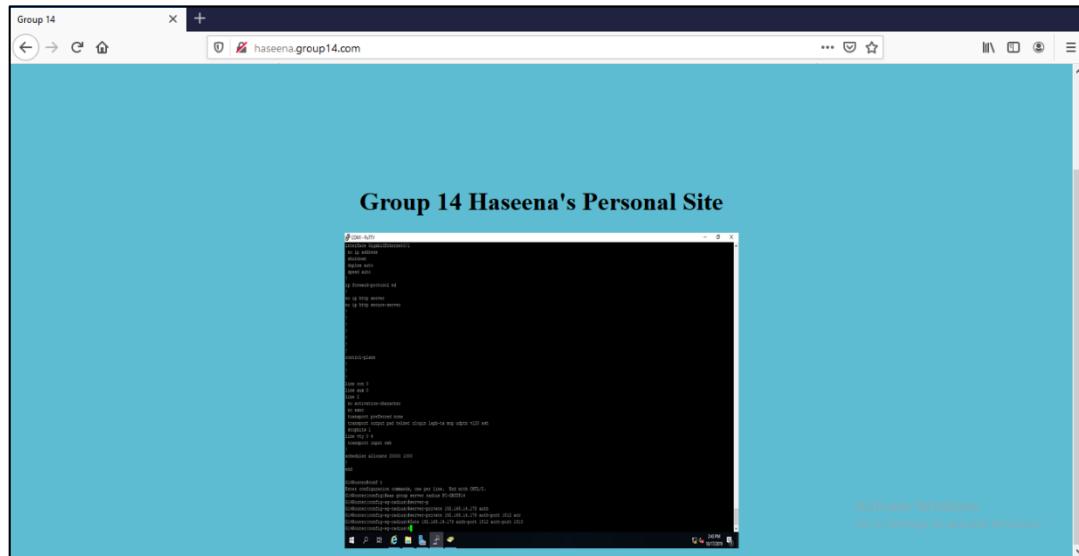


Figure 5. 248: The website that contains.png picture

**STEP 2:** Open the IIS Server and click on the deny file extension and add .png to deny any picture in .png format.

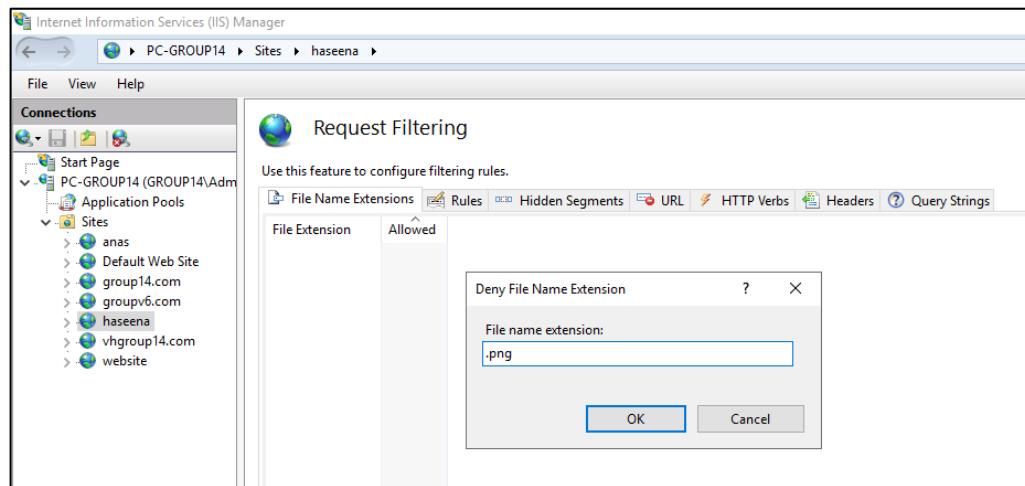


Figure 5. 249: Deny the .png file extension

### 5.3.18.6 LOGGING

**STEP 1:** Open IIS Server and click on logging. At the ‘Log Event Destination’, choose the log file only and choose the directory in which the log was save.

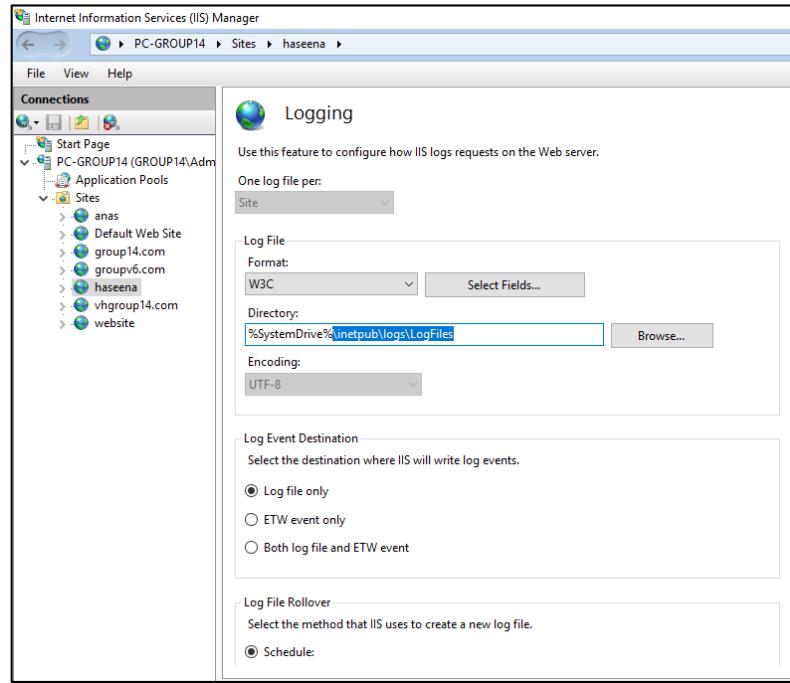


Figure 5. 250: Configure the place to save the log files.

## 5.3.19 IDS WITH PORT MIRROR

### 5.3.19.1 Intrusion Detection System

#### STEP 1: Install Snort Pre-Requisite

```
group14@group14-optiplex-7010:~$ sudo su
[sudo] password for group14:
root@group14-optiplex-7010:~/home/group14# sudo apt install -y gcc libpcre3-dev zlib1g-dev libluajit-5.1-dev libpcap-dev openssl libs
1-dev libnghttp2-dev libdumbnet-dev bison Flex libdbd
Reading package lists... Done
Building dependency tree
Reading state information... Done
openssl is already the newest version (1:1.1d-1+ubuntu18.04.1-deb.sury.org+2).
openssl set to manually installed.
The following packages were automatically installed and are no longer required:
  apturl-common dbconfig-common dbconfig-mysql default-mysql-client
  gir1.2-goa-1.0 gir1.2-snapd-1 gnome-software-common hplip-data llbapt-2.0-2
  libtbs-sphinxdox libtbs-underscore libtbs-hpate php-libsclib php-tcpdf
  python3-dateutil python3-olefile python3-pexpect python3-pil
  python3-ptprocess python3-renderpm python3-reportlab
  python3-reportlab-accel
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  build-essential dpkg-dev fakeroot g++-7 gcc-7 libalgorithm-diff-perl
  libalgorithm-diff-xs-perl libalgorithm-merge-perl libasan4 libatomic1
  libbison-dev libc-dev bin libc0-dev libcurlkrts libdumbnet1 libfakeroot
  libfl-dev libfl2 libgcc-7-dev libtiny liblsan0 libluajit-5.1-2
  libluajit-5.1-common libmpx2 libpcap0.8-dev libpcre16-3 libpcre32-3
  libpcrecppa5 libquadmath0 libsigsegv2 libstdc++-7-dev libtsan0 libubsan0
  linux-libc-dev m4 make nmap-dev pkg-config
Suggested packages:
  bison-doc debian-keyring flex-doc g++-multilib g++-7-multilib gcc-7-doc
  libstdc++-v6-7-dbg gcc-multilib autoconf automake libtool gcc-doc
  gcc-7-multilib gcc-7-locales libgcc1-dbg libomp1-dbg libitm1-dbg
  libatomic1-dbg libasan1-dbg libtsan0-dbg libubsan0-dbg libubsan0-dbg
  libcurlkrts5-dbg libmpx2-dbg libquadmath0-dbg libgcc-doc dnet-common
  libnghttp2-doc libssl1-doc libstdc++-7-doc m4-doc make-doc
The following NEW packages will be installed:
  bison build-essential dpkg-dev fakeroot flex g++-7 gcc gcc-7
  libalgorithm-diff-perl libalgorithm-diff-xs-perl libalgorithm-merge-perl
  libasan4 libatomic1 libbison-dev libc-dev bin libc0-dev libcurlkrts libdumbnet1 libfakeroot libfl-dev libgcc-7-dev libtiny
libdumbnet-dev libdumbnet1 libfakeroot libfl2 libgcc-7-dev libtiny
```

Figure 5.251: Command line

```
Setting up libc6-dev:amd64 (2.27-3ubuntu1) ...
Setting up libdnet:amd64 (2.65) ...
Setting up libltn1:amd64 (8.3.0-2ubuntu1-18.04.1) ...
Setting up libluajit-5.1-dev:amd64 (2.1.0-beta3+dfsg-5.1) ...
Setting up zlib1g-dev:amd64 (1:1.2.11.dfsg-0ubuntu2) ...
Setting up libpcre3-dev:amd64 (2:8.43-1+ubuntu18.04.1+deb.sury.org+1) ...
Setting up flex (2.6.4-6) ...
Setting up libpcap0.8-dev:amd64 (1.8.1-6ubuntu1) ...
Setting up libdumbnet-dev (1.12-7build1) ...
Setting up fakeroot (1.22-2ubuntu1) ...
update-alternatives: using /usr/bin/fakeroot-sysv to provide /usr/bin/fakeroot (fakeroot) in auto mode
Setting up libgcc-7-dev:amd64 (7.4.0-1ubuntu1-18.04.1) ...
Setting up libfl-dev:amd64 (2.6.4-6)
Setting up libstdc++-7-dev:amd64 (7.4.0-1ubuntu1-18.04.1) ...
Setting up libalgorithm-merge-perl (0.08-3) ...
Setting up pkg-config (0.29-1ubuntu2) ...
Setting up libalgorithm-diff-xs-perl (0.04-5) ...
Setting up libpcap-dev:amd64 (1.8.1-6ubuntu1) ...
Setting up libnghttp2-dev (1.30.0-6ubuntu1) ...
Setting up gcc-7 (7.4.0-1ubuntu1-18.04.1) ...
Setting up g++-7 (7.4.0-1ubuntu1-18.04.1) ...
Setting up gcc (4:7.4.0-1ubuntu2.3) ...
Setting up g++ (4:7.4.0-1ubuntu2.3) ...
update-alternatives: using /usr/bin/g++ to provide /usr/bin/c++ (c++) in auto mode
Setting up build-essential (12.4ubuntu1) ...
Processing triggers for libc-bin (2.27-3ubuntu1) ...
Processing triggers for install-info (6.5.0.dfsg.1-2) ...
root@group14-optiplex-7010:~/home/group14# mkdir ~snort_src & cd ~snort_src
root@group14-optiplex-7010:~/snort_src wget https://www.snort.org/downloads/snort/daq-2.0.6.tar.gz
--2019-12-03 13:04:13-- https://www.snort.org/downloads/snort/daq-2.0.6.tar.gz
Resolving www.snort.org (www.snort.org)... 104.18.138.9, 104.18.139.9, 206.47.0.0:812:Ba09, ...
Connecting to www.snort.org (www.snort.org)|104.18.138.9|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://snort.org-site.s3.amazonaws.com/production/release_files/files/000/011/803/original/daq-2.0.6.tar.gz?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIXACIED2SPMSCT7GA2F20191202%2Fus-east-1%2F%3%2Faws4_request&X-Amz-Date=20191202T140011Z&X-Amz-Expires=36008X&X-Amz-SignedHeaders=host&X-Amz-Signature=a8ffe5ccbc0c230eef00b654a23edesa5fc280f035b8abcb4ae5cfdd890ab487e [following]
--2019-12-03 13:04:14-- https://snort.org-site.s3.amazonaws.com/production/release_files/files/000/011/803/original/daq-2.0.6.tar.gz?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIXACIED2SPMSCT7GA2F20191202%2Fus-east-1%2F%3%2Faws4_request&X-Amz-Date=20191202T140011Z&X-Amz-Expires=36008X&X-Amz-SignedHeaders=host&X-Amz-Signature=a8ffe5ccbc0c230ecf00b654a23ede58fb8c280f035b8abcb4ae5cfdd890ab487
```

Figure 5.252: Command line

```

Setting up libc6-dev:amd64 (2.27-3ubuntu1) ...
Setting up libdnet:amd64 (2.65) ...
Setting up libitm1:amd64 (8.3.0-6ubuntu1-18.04.1) ...
Setting up libluajit-5.1-dev:amd64 (2.1.0-beta3+dfsg-5.1) ...
Setting up zlib1g-dev:amd64 (1:1.2.11.dfsg-0ubuntu2) ...
Setting up libpcre3-dev:amd64 (2:8.43-1+ubuntu18.04.1+deb.sury.org+1) ...
Setting up flex (2.6.4-6) ...
Setting up libpcap0.8-dev:amd64 (1.8.1-6ubuntu1) ...
Setting up libdumbnet-dev (1.12-7build1) ...
Setting up fakeroot (1.22-2ubuntu1) ...
update-alternatives: using /usr/bin/fakeroot-sysv to provide /usr/bin/fakeroot (fakeroot) in auto mode
Setting up libgcc-7-dev:amd64 (7.4.0-1ubuntu1-18.04.1) ...
Setting up libfl-dev:amd64 (2.6.4-6) ...
Setting up libstdc++-7-dev:amd64 (7.4.0-1ubuntu1-18.04.1) ...
Setting up libalgorithm-merge-perl (0.08-3) ...
Setting up pkg-config (0.29.1-0ubuntu2) ...
Setting up libalgorithm-diff-xs-perl (0.04-5) ...
Setting up libpcap-dev:amd64 (1.8.1-6ubuntu1) ...
Setting up libnghttp2-dev (1.30.0-1ubuntu1) ...
Setting up gcc-7 (7.4.0-1ubuntu1-18.04.1) ...
Setting up g++-7 (7.4.0-1ubuntu1-18.04.1) ...
Setting up gcc (4:7.4.0-1ubuntu2.3) ...
Setting up g++ (4:7.4.0-1ubuntu2.3) ...
update-alternatives: using /usr/bin/g++ to provide /usr/bin/c++ (c++) in auto mode
Setting up build-essential (12.4ubuntu1) ...
Processing triggers for libc-bin (2.27-3ubuntu1) ...
Processing triggers for man-db (2.8.3-2ubuntu0.1) ...
Processing triggers for install-info (6.5.0.dfsg.1-2) ...

```

*Figure 5.253: Command line*

## STEP 2: Download, build and install the latest DAQ (2.0.6)

```

root@group14-optiplex-7010:~/snort_src# Wget https://www.snort.org/downloads/snort/daq-2.0.6.tar.gz
--2019-12-03 13:04:13-- https://www.snort.org/downloads/snort/daq-2.0.6.tar.gz
Resolving www.snort.org (www.snort.org)... 104.18.138.9, 104.18.139.9, 2606:4700::6812:8a09, ...
Connecting to www.snort.org (www.snort.org)|104.18.138.9|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://snort-org-site.s3.amazonaws.com/production/release_files/files/000/011/803/original/daq-2.0.6.tar.gz?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIXACIE02SPM5C7GA%2F20191202%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20191202T140011Z&X-Amz-Expires=3600&X-Amz-SignedHeaders=host&X-Amz-Signature=8ffe5ccb0c230ecf00b654a23eds58fc286f035b8abcb4ae5cf6d6d890ab487e [following]
--2019-12-03 13:04:14-- https://snort-org-site.s3.amazonaws.com/production/release_files/files/000/011/803/original/daq-2.0.6.tar.gz?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIXACIE02SPM5C7GA%2F20191202%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20191202T140011Z&X-Amz-Expires=3600&X-Amz-SignedHeaders=host&X-Amz-Signature=8ffe5ccb0c230ecf00b654a23eds58fc286f035b8abcb4ae5cf6d6d890ab487e
Resolving snort-org-site.s3.amazonaws.com (snort-org-site.s3.amazonaws.com)... 52.216.132.219
Connecting to snort-org-site.s3.amazonaws.com (snort-org-site.s3.amazonaws.com)|52.216.132.219|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 518013 (506K) [binary/octet-stream]
Saving to: 'daq-2.0.6.tar.gz'

daq-2.0.6.tar.gz          100%[=====] 505.87K   387KB/s    in 1.3s

2019-12-03 13:04:17 (387 KB/s) - 'daq-2.0.6.tar.gz' saved [518013/518013]

```

*Figure 5.254: Download daq 2.0.6*

```

daq-2.0.6/os-daq-modules/daq_pcaps.c
daq-2.0.6/os-daq-modules/daq_nfq.c
daq-2.0.6/os-daq-modules/daq_afpacket.c
daq-2.0.6/os-daq-modules/daq-modules-config.in
daq-2.0.6/os-daq-modules/Makefile.am
daq-2.0.6/os-daq-modules/daq_netmap.c
daq-2.0.6/os-daq-modules/daq_static_modules.h
daq-2.0.6/os-daq-modules/daq_dump.c
daq-2.0.6/os-daq-modules/Makefile.in
daq-2.0.6/api/
daq-2.0.6/api/daq_base.c
daq-2.0.6/api/daq.h
daq-2.0.6/api/Makefile.am
daq-2.0.6/api/daq_common.h
daq-2.0.6/api/daq_api.h
daq-2.0.6/api/daq_mod_ops.c
daq-2.0.6/api/Makefile.in
daq-2.0.6/aclocal.m4
daq-2.0.6/config.guess
daq-2.0.6/COPYING
daq-2.0.6/ltmain.sh
daq-2.0.6/README
daq-2.0.6/config.h.in
daq-2.0.6/depcomp
daq-2.0.6/Makefile.in
daq-2.0.6/m4/
daq-2.0.6/m4/ax_cflags_gcc_option.m4
daq-2.0.6/m4/ltSugar.m4
daq-2.0.6/m4/sf.m4
daq-2.0.6/m4/libtool.m4
daq-2.0.6/m4/ltVersion.m4
daq-2.0.6/m4/lt-obsolete.m4
daq-2.0.6/m4/ltOptions.m4
daq-2.0.6/configure.ac

```

*Figure 5.255: List of daq*

**STEP 3:** Unpack the files, configure, make and then install. Run the configuration script with defaults, the use make to compile the program and then finally install daq.

```

root@group14-optiplex-7010:/snort_src# cd daq-2.0.6
root@group14-optiplex-7010:/snort_src/daq-2.0.6# ./configure && make && sudo make install
checking for a BSD-compatible install... /usr/bin/install -c
checking whether build environment is sane... yes
checking for a thread-safe mkdir -p... /bin/mkdir -p
checking for gawk... no
checking for nawk... nawk
checking whether make sets $(MAKE)... yes
checking whether make supports nested variables... yes
checking for gcc... gcc
checking whether the C compiler works... yes
checking for C compiler default output file name... a.out
checking for suffix of executables...
checking whether we are cross compiling... no
checking for suffix of object files... o
checking whether we are using the GNU C compiler... yes
checking whether gcc accepts -g... yes
checking for gcc option to accept ISO C89... []

```

*Figure 5.256: Configure and make install daq*

### 5.3.19.2 Snort Installation

STEP 1: Download and install the latest Snort version (2.9.15):

```
root@group14-optiplex-7010:~/snort_src# wget https://www.snort.org/downloads/snort/snort-2.9.15.tar.gz
--2019-12-03 13:07:40-- https://www.snort.org/downloads/snort/snort-2.9.15.tar.gz
Resolving www.snort.org (www.snort.org)... 104.18.139.9, 104.18.138.9, 2606:4700::6812:8a09, ...
Connecting to www.snort.org (www.snort.org)|104.18.139.9|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://snort-org-site.s3.amazonaws.com/production/release_files/files/000/011/796/original/snort-2.9.15.tar.gz?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIXACIE2SPMSC7GAX2F20191202%2Fus-east-1%2F53%2Faws4_request&X-Amz-Date=20191202T140339Z&X-Amz-Expires=3600&X-Amz-SignedHeaders=host&X-Amz-Signature=d55e05046ef3644c0a08f0349cb9025d6ca0bc8bcd3b5385d2b218c9226135b2 [following]
--2019-12-03 13:07:41-- https://snort-org-site.s3.amazonaws.com/production/release_files/files/000/011/796/original/snort-2.9.15.tar.gz?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIXACIE2SPMSC7GAX2F20191202%2Fus-east-1%2F53%2Faws4_request&X-Amz-Date=20191202T140339Z&X-Amz-Expires=3600&X-Amz-SignedHeaders=host&X-Amz-Signature=d55e05046ef3644c0a08f0349cb9025d6ca0bc8bcd3b5385d2b218c9226135b2
Resolving snort-org-site.s3.amazonaws.com (snort-org-site.s3.amazonaws.com)... 52.216.192.24
Connecting to snort-org-site.s3.amazonaws.com (snort-org-site.s3.amazonaws.com)|52.216.192.24|:443... connected.
[]
```

Figure 5.257: Install Snort 2.9.15

```
root@group14-optiplex-7010:~/snort_src# cd snort-2.9.15
root@group14-optiplex-7010:~/snort_src/snort-2.9.15# ./configure --enable-sourcefire && make && sudo make install
checking for a BSD-compatible install... /usr/bin/install -c
checking whether build environment is sane... yes
checking for a thread-safe mkdirr -p... /bin/mkdir -p
checking for gawk... no
checking for mawk
checking whether make sets $(MAKE)... yes
checking whether make supports nested variables... yes
checking whether make supports the include directive... yes (GNU style)
checking for gcc... gcc
checking whether the C compiler works... yes
checking for c compiler default output file name... a.out
checking for suffix of executables...
checking whether we are cross compiling... no
checking for suffix of object files... o
checking whether we are using the GNU C compiler... yes
checking whether gcc accepts -g... yes
checking for gcc option to accept ISO C89... none needed
checking whether gcc understands -c and -o together... yes
checking dependency style of gcc... gcc3
checking for gcc option to accept ISO C99... none needed
checking for gcc option to accept ISO Standard C... (cached) none needed
checking for gcc... (cached) gcc
checking whether we are using the GNU C compiler... (cached) yes
checking whether gcc accepts -g... (cached) yes
checking for gcc option to accept ISO C99... (cached) none needed
checking whether gcc understands -c and -o together... (cached) yes
checking dependency style of gcc... (cached) gcc3
checking build system type... x86_64-pc-linux-gnu
checking host system type... x86_64-pc-linux-gnu
checking how to print strings... printf
checking for a sed that does not truncate output... /bin/sed
checking for grep that handles long lines and -e... /bin/grep
checking for egrep... /bin/grep -E
checking for fgrep... /bin/grep -F
checking for ld used by gcc... /usr/bin/ld
checking if the linker (/usr/bin/ld) is GNU ld... yes
checking for BSD- or MS-compatible name linker (nm)... /usr/bin/nm -B
checking the name linker (/usr/bin/nm -B) interface... BSD nm
checking whether ln -s works... yes
checking the maximum length of command line arguments... 1572864
checking how to convert x86_64-pc-linux-gnu file names to x86_64-pc-linux-gnu format... func_convert_file_noop
checking how to convert x86_64-pc-linux-gnu file names to toolchain format... func_convert_file_noop
checking for /usr/bin/ld option to reload object files... -r
checking for objdump... objdump
checking how to recognize dependent libraries... pass_all
checking for dltool... no
checking how to associate runtime and link libraries... printf %s\n
checking for ar... ar
checking for archiver @FILE support... []
```

Figure 5.258: Enable sourcefire and install

### Step 3: Snort Configuration

- 1) Create unprivileged Snort account and required initial files. Next, you need to setup Snort for your system, this includes editing some configuration files, downloading rules that Snort will follow and taking Snort for a test run.
- 2) Update the shared libraries to avoid any error when try to running Snort.

```
root@group14-optiplex-7010:~/snort_src/snort-2.9.15# sudo ldconfig
```

Figure 5.259: Update shared library

- 3) Create a symlink to the Snort library

```
root@group14-optiplex-7010:~/snort_src/snort-2.9.15# sudo ln -s /usr/local/bin/snort /usr/sbin/snort
```

Figure 5.260: Create a symlink

- 4) Create a normal user and a group to run the snort daemon

```
root@group14-optiplex-7010:~/snort_src/snort-2.9.15# sudo groupadd snort  
root@group14-optiplex-7010:~/snort_src/snort-2.9.15# sudo useradd snort -r -s /sbin/nologin -c SNORT_IDS -g snort
```

Figure 5.261: Creating user

- 5) Create necessary files and directory required by Snort and change the permissions for the new directories

```
root@group14-optiplex-7010:~/snort_src/snort-2.9.15# sudo mkdir -p /etc/snort/rules  
root@group14-optiplex-7010:~/snort_src/snort-2.9.15# sudo mkdir /var/log/snort  
root@group14-optiplex-7010:~/snort_src/snort-2.9.15# sudo mkdir /usr/local/lib/snort_dynamicrules  
root@group14-optiplex-7010:~/snort_src/snort-2.9.15# sudo chmod -R 5775 /etc/snort  
root@group14-optiplex-7010:~/snort_src/snort-2.9.15# sudo chmod -R 5775 /var/log/snort  
root@group14-optiplex-7010:~/snort_src/snort-2.9.15# sudo chmod -R 5775 /usr/local/lib/snort_dynamicrules  
root@group14-optiplex-7010:~/snort_src/snort-2.9.15# sudo chown -R snort:snort /etc/snort  
root@group14-optiplex-7010:~/snort_src/snort-2.9.15# sudo chown -R snort:snort /var/log/snort  
root@group14-optiplex-7010:~/snort_src/snort-2.9.15# sudo chown -R snort:snort /usr/local/lib/snort_dynamicrules
```

Figure 5.262: Create files and permissions

- 6) Create new files for the while and black lists as well as the local rules

```
root@group14-optiplex-7010:~/snort_src/snort-2.9.15# sudo touch /etc/snort/rules/white_list.rules  
root@group14-optiplex-7010:~/snort_src/snort-2.9.15# sudo touch /etc/snort/rules/black_list.rules  
root@group14-optiplex-7010:~/snort_src/snort-2.9.15# sudo touch /etc/snort/rules/local.rules
```

Figure 5.263: Create files in rules

7) Copy the configuration files and the dynamic preprocessors

```
root@group14-optiplex-7010:~/snort_src/snort-2.9.15# sudo cp -r /snort_src/snort-2.9.15/etc/*.* /etc/snort  
root@group14-optiplex-7010:~/snort_src/snort-2.9.15# sudo cp ~/snort_src/snort-2.9.15/etc/*.*.map /etc/snort
```

Figure 5.264: Copy configuration

**Step 4:** Install community rules

```
root@group14-optiplex-7010:~/snort_src/snort-2.9.15# wget https://www.snort.org/rules/community -O ~/community.tar.gz  
--2019-12-03 13:15:31-- https://www.snort.org/rules/community  
Resolving www.snort.org (www.snort.org)... 104.18.139.9, 104.18.138.9, 2606:4700::6B12:Ba09, ...  
Connecting to www.snort.org (www.snort.org)|104.18.139.9|:443... connected.  
HTTP request sent, awaiting response... 302 Found  
Location: https://snort-org-site.s3.amazonaws.com/production/release_files/files/000/012/264/original/community-rules.tar.gz?X-Amz-Algori  
thm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIXACIE2SPMSC7GAx2F20191202K2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20191202T141130Z  
&X-Amz-Expires=3600&X-Amz-SignedHeaders=host&X-Amz-Signature=7cd7233350d55b86acac9ce0586a9a8c7c4975fb33602731de1b5969e782b481 [follow  
ing]  
--2019-12-03 13:15:32-- https://snort-org-site.s3.amazonaws.com/production/release_files/files/000/012/264/original/community-rules.  
tar.gz?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIXACIE2SPMSC7GAx2F20191202K2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=2  
0191202T141130Z&X-Amz-Expires=3600&X-Amz-SignedHeaders=host&X-Amz-Signature=7cd7233350d55b86acac9ce0586a9a8c7c4975fb33602731de1b5969e  
782b481  
Resolving snort-org-site.s3.amazonaws.com (snort-org-site.s3.amazonaws.com)... 52.216.89.19  
Connecting to snort-org-site.s3.amazonaws.com (snort-org-site.s3.amazonaws.com)|52.216.89.19|:443... connected.  
HTTP request sent, awaiting response... 200 OK  
Length: 331033 (323K) [application/gzip]  
Saving to: '/root/community.tar.gz'  
  
/root/community.tar.gz      100%[=====] 323.27K   318KB/s   in 1.0s  
  
2019-12-03 13:15:35 (318 KB/s) - '/root/community.tar.gz' saved [331033/331033]
```

Figure 5.265: Install community rules

```
root@group14-optiplex-7010:~/snort_src/snort-2.9.15# sudo tar -xvf ~/community.tar.gz -C ~/  
community-rules/  
community-rules/community.rules  
community-rules/VRT-License.txt  
community-rules/LICENSE  
community-rules/AUTHORS  
community-rules/snort.conf  
community-rules/sid-msg.map  
root@group14-optiplex-7010:~/snort_src/snort-2.9.15# sudo cp ~/community-rules/* /etc/snort/rules
```

Figure 5.266: Extract the downloaded community rules

### 5.3.20 SAMBA AND SAMBA SECURITY DEVICES

#### 1. Install the Samba package

```
root@group14:/home/group14# apt install samba
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  apg gnome-control-center-faces gnome-online-accounts libbcdio-cdda2
  libcdio-paranoid2 libcdio17 libcolor-gtk1 libgtop-2.0-11 libgtop2-common
  libnss-myhostname libwhoopsie-preferences0 mobile-broadband-provider-info
  network-manager-gnome python3-macaroonbakery python3-nacl python3-protoBuf
  python3-pymacaroons python3-rfc3339 python3-tz ubuntu-system-service
  whoopsie-preferences
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  samba-common samba-common-bin
Suggested packages:
  bind9 bindutils ctdb ldb-tools ntp | chrony smbdap-tools winbind
  heimdal-clients
The following NEW packages will be installed:
  samba samba-common samba-common-bin
0 upgraded, 3 newly installed, 0 to remove and 29 not upgraded.
Need to get 1,447 kB of archives.
After this operation, 13.1 MB of additional disk space will be used.
```

Figure 5.267: Installation

- Once the installation is completed, the Samba service will start automatically. To check whether the Samba server is running

```
root@group14-optiplex-7010:/home/group14# systemctl status smbd
● smbd.service - Samba SMB Daemon
  Loaded: loaded (/lib/systemd/system/smbd.service; enabled; vendor preset: enabled)
  Active: active (running) since Wed 2019-12-18 12:36:36 +08; 22s ago
    Docs: man:smbd(8)
          man:samba(7)
          man:smb.conf(5)
   Main PID: 7291 (smbd)
      Status: "smbd: ready to serve connections..."
        Tasks: 4 (limit: 4915)
       CGroup: /system.slice/smbd.service
               ├─7291 /usr/sbin/smbd --foreground --no-process-group
               ├─7293 /usr/sbin/smbd --foreground --no-process-group
               ├─7294 /usr/sbin/smbd --foreground --no-process-group
               └─7297 /usr/sbin/smbd --foreground --no-process-group

Dec 18 12:36:36 group14 systemd[1]: Starting Samba SMB Daemon...
Dec 18 12:36:36 group14 systemd[1]: Started Samba SMB Daemon.
root@group14-optiplex-7010:/home/group14# systemctl status nmbd
● nmbd.service - Samba NMB Daemon
  Loaded: loaded (/lib/systemd/system/nmbd.service; enabled; vendor preset: enabled)
  Active: active (running) since Wed 2019-12-18 12:36:37 +08; 24s ago
    Docs: man:nmbd(8)
          man:samba(7)
          man:smb.conf(5)
   Main PID: 7363 (nmbd)
      Status: "nmbd: ready to serve connections..."
        Tasks: 1 (limit: 4915)
       CGroup: /system.slice/nmbd.service
               └─7363 /usr/sbin/nmbd --foreground --no-process-group
```

Figure 5.268: Server running

3. Create a backup for future reference purposes

```
root@group14:/home/group14# cp /etc/samba/smb.conf(.,.backup)
```

Figure 5.269: Create backup

4. Create the /samba directory

```
root@group14:/home/group14# mkdir /samba
```

Figure 5.270: Directory

5. Set the group ownership to sambashare

```
root@group14:/home/group14# chown group14samba:sambashare /samba/group14samba
```

Figure 5.271: Set group

6. Configuring the sambashare

7. Once done, restart the Samba services

```
root@group14-optiplex-7010:/home/group14# systemctl status smbd
● smbd.service - Samba SMB Daemon
  Loaded: loaded (/lib/systemd/system/smbd.service; enabled; vendor preset: enabled)
  Active: active (running) since Wed 2019-12-18 12:36:36 +08; 22s ago
    Docs: man:smbd(8)
          man:samba(7)
          man:smb.conf(5)
   Main PID: 7291 (smbd)
  Status: "smbd: ready to serve connections..."
     Tasks: 4 (limit: 4915)
    CGroup: /system.slice/smbd.service
            └─7291 /usr/sbin/smbd --foreground --no-process-group
              ├─7293 /usr/sbin/smbd --foreground --no-process-group
              ├─7294 /usr/sbin/smbd --foreground --no-process-group
              └─7297 /usr/sbin/smbd --foreground --no-process-group

Dec 18 12:36:36 group14 systemd[1]: Starting Samba SMB Daemon...
Dec 18 12:36:36 group14 systemd[1]: Started Samba SMB Daemon.
root@group14-optiplex-7010:/home/group14# systemctl status nmbd
● nmbd.service - Samba NMB Daemon
  Loaded: loaded (/lib/systemd/system/nmbd.service; enabled; vendor preset: enabled)
  Active: active (running) since Wed 2019-12-18 12:36:37 +08; 24s ago
    Docs: man:nmbd(8)
          man:samba(7)
          man:smb.conf(5)
   Main PID: 7363 (nmbd)
  Status: "nmbd: ready to serve connections..."
     Tasks: 1 (limit: 4915)
    CGroup: /system.slice/nmbd.service
            └─7363 /usr/sbin/nmbd --foreground --no-process-group
```

Figure 5.272: Restart

### 5.3.21 LINUX SERVER HARDENING

#### 1) System update

Keeping the system up to date is necessary after installing any operating system. This will reduce known vulnerabilities that are in your system.

#### 2) Password expiration

When creating user accounts, we make the policy where it have minimum and maximum password age to force the user to change password.

```
root@group14-optiplex-7010:/home/group14# sudo chage -W 14 group14
root@group14-optiplex-7010:/home/group14# sudo chage -l group14
Last password change : Jan 28, 2018
Password expires      : never
Password inactive     : never
Account expires       : never
Minimum number of days between password change : 0
Maximum number of days between password change : 99999
Number of days of warning before password expires: 14
root@group14-optiplex-7010:/home/group14#
```

Figure 5.273: Password information

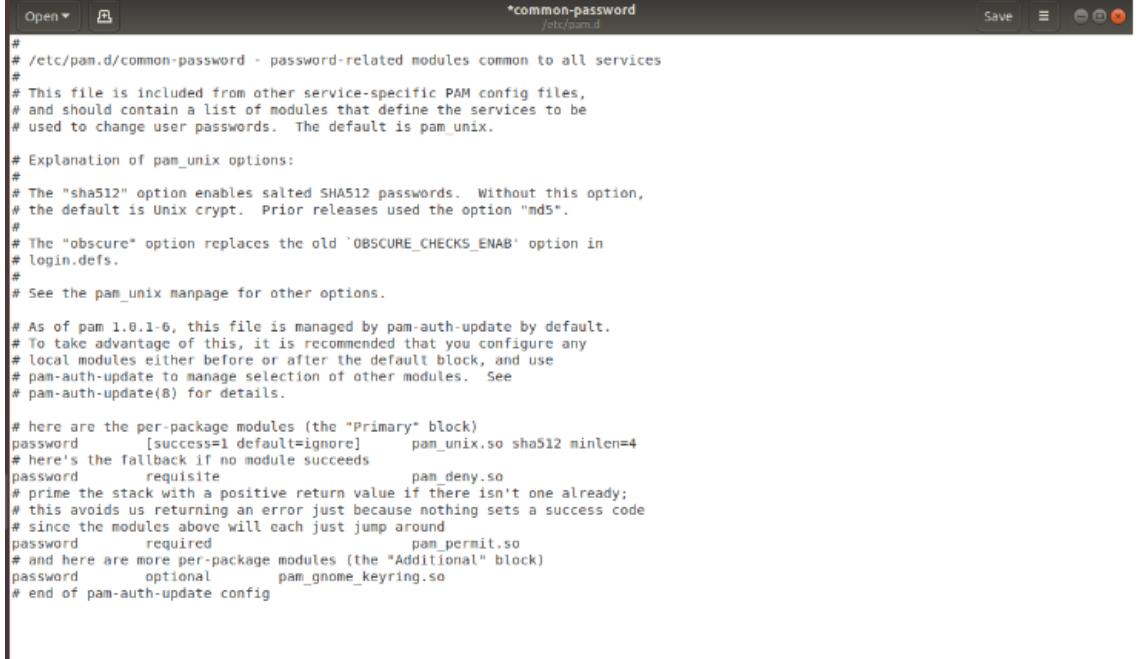
#### 3) Set the minimum number of password

We set the minimum number of password to avoid the password to be crack easily.

```
root@group14-optiplex-7010:/home/group14# apt-get install libpam-cracklib --force-yes -y
Reading package lists... Done
Building dependency tree
Reading state information... Done
libpam-cracklib is already the newest version (1.1.8-3.6ubuntu2.18.04.1).
The following packages were automatically installed and are no longer required:
  apturl-common dbconfig-common dbconfig-mysql default-mysql-client hplip-data libart-2.8-2 libjs-sphinxdoc libjs-underscore
  libsane-hpaio php-phpseclib php-tcpdf python3-olefile python3-pexpect python3-pil python3-ptyprocess python3-renderpm
  python3-reportlab python3-reportlab-accel
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 1 not upgraded.
W: --force-yes is deprecated, use one of the options starting with --allow instead.
```

Figure 5.274: Install library for minimum password

## Edit the configuration file



```
*common-password
/etc/pam.d

#
# /etc/pam.d/common-password - password-related modules common to all services
#
# This file is included from other service-specific PAM config files,
# and should contain a list of modules that define the services to be
# used to change user passwords. The default is pam_unix.

# Explanation of pam_unix options:
#
# The "sha512" option enables salted SHA512 passwords. Without this option,
# the default is Unix crypt. Prior releases used the option "md5".
#
# The "obscure" option replaces the old 'OBSCURE_CHECKS_ENAB' option in
# login.defs.
#
# See the pam_unix manpage for other options.

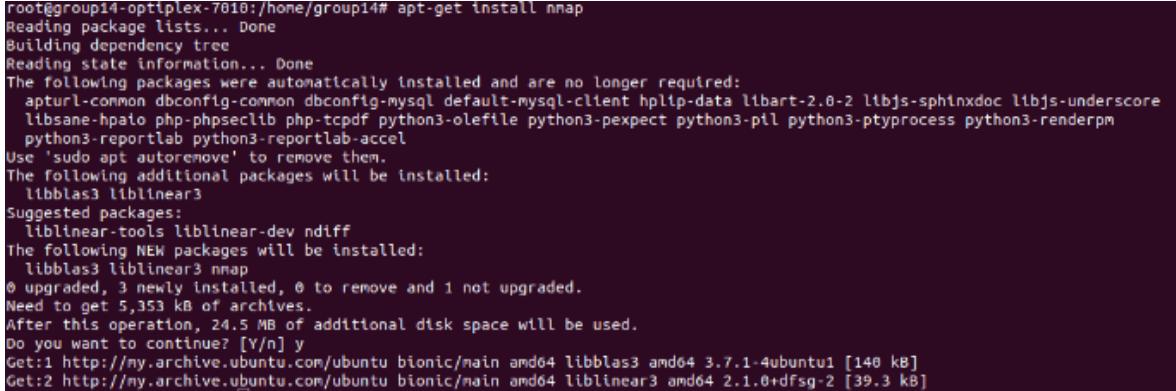
# As of pam 1.0.1-6, this file is managed by pam-auth-update by default.
# To take advantage of this, it is recommended that you configure any
# local modules either before or after the default block, and use
# pam-auth-update to manage selection of other modules. See
# pam-auth-update(8) for details.

# here are the per-package modules (the "Primary" block)
password      [success=1 default=ignore]      pam_unix.so sha512 minlen=4
# here's the fallback if no module succeeds
password      requisite                  pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
# since the modules above will each just jump around
password      required                  pam_permit.so
# and here are more per-package modules (the "Additional" block)
password      optional                 pam_gnome_keyring.so
# end of pam-auth-update config
```

Figure 5.275: Configuration file for minimum password

## 4) Port Scanning

To find out which services are currently running, we need to install nmap which is software for scanning port that has been used and running.



```
root@group14-optiplex-7010:/home/group14# apt-get install nmap
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  apturl-common dbconfig-common dbconfig-mysql default-mysql-client hplip-data libart-2.0-2 libjs-sphinxdoc libjs-underscore
  libsane-hpaio php-phpseclib php-tcpdf python3-olefile python3-pexpect python3-pil python3-ptyprocess python3-renderpm
  python3-reportlab python3-reportlab-accel
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  libblas3 liblinear3
Suggested packages:
  liblinear-tools liblinear-dev ndiff
The following NEW packages will be installed:
  libblas3 liblinear3 nmap
0 upgraded, 3 newly installed, 0 to remove and 1 not upgraded.
Need to get 5,353 kB of archives.
After this operation, 24.5 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://my.archive.ubuntu.com/ubuntu bionic/main amd64 libblas3 amd64 3.7.1-4ubuntu1 [140 kB]
Get:2 http://my.archive.ubuntu.com/ubuntu bionic/main amd64 liblinear3 amd64 2.1.0+dfsg-2 [39.3 kB]
```

Figure 5.276: Installing nmap

```

root@group14-optiplex-7010:/home/group14# sudo nmap -v -sS localhost
Starting Nmap 7.60 ( https://nmap.org ) at 2019-12-10 12:23 +08
Initiating SYN Stealth Scan at 12:23
Scanning localhost (127.0.0.1) [1000 ports]
Discovered open port 80/tcp on 127.0.0.1
Discovered open port 445/tcp on 127.0.0.1
Discovered open port 22/tcp on 127.0.0.1
Discovered open port 3306/tcp on 127.0.0.1
Discovered open port 25/tcp on 127.0.0.1
Discovered open port 139/tcp on 127.0.0.1
Discovered open port 1199/tcp on 127.0.0.1
Discovered open port 1099/tcp on 127.0.0.1
Discovered open port 631/tcp on 127.0.0.1
Discovered open port 2008/tcp on 127.0.0.1
Discovered open port 5432/tcp on 127.0.0.1
Discovered open port 3128/tcp on 127.0.0.1
Completed SYN Stealth Scan at 12:23, 1.58s elapsed (1000 total ports)
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000013s latency).
Not shown: 988 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
25/tcp    open  smtp
80/tcp    open  http
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
631/tcp   open  ipp
1099/tcp  open  rmiregistry
1199/tcp  open  dmidi
2008/tcp  open  conf
3128/tcp  open  squid-http
3306/tcp  open  mysql
5432/tcp  open  postgresql

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.67 seconds
Raw packets sent: 1063 (46.772KB) | Rcvd: 2139 (90.062KB)

```

*Figure 5.277: List of port in Ubuntu server*

Explanation of each port:

**Port 22:** Used for ssh service

**Port 25:** Used for smtp service

**Port 80:** Port that server ‘listens to’ or expects to receive from a Web client

**Port 143:** The IMAP is a mail protocol used for accessing email on a remote web server from a local client.

**Port 631:** Internet protocol for communication between computers and printers

**Port 993:** Use a defined protocol to communicate between computers and printers.

**Port 3306:** MySql Database

A protocol is a set of formalized rules that explains how data is communicated over a network.

## 5) Backup

Backup is one of the most important thing in the system. If system down or anything happened to our server, backup will save all important data in the system so that it can restore all the data back to normal without losing anything.

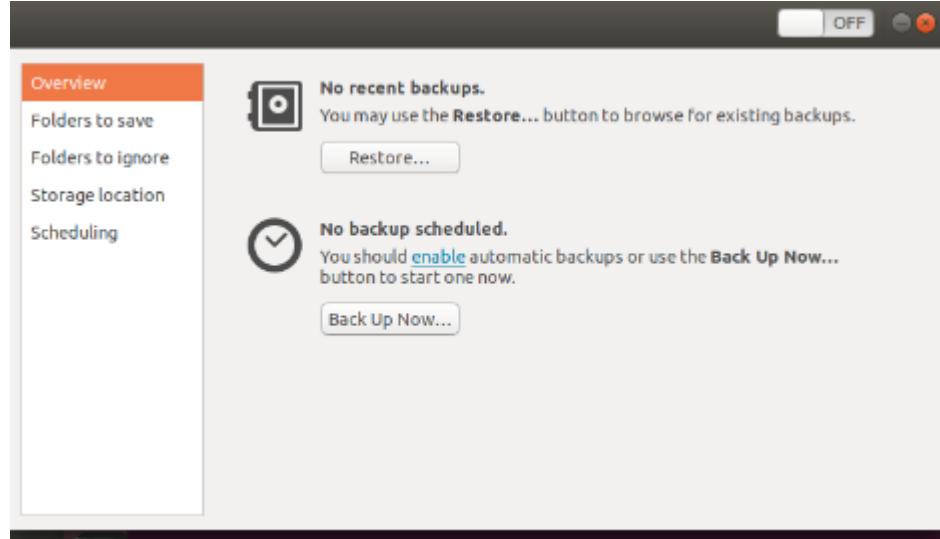


Figure 5.278: Backup interface

## 5.3.22 IPSEC VPN SERVER FOR REMOTE EMPLOYEE

### 5.3.22.1 VPN SERVER

**STEP 1:** Install the VPN server manager in windows server.



Figure 5.279: Install the VPN

**STEP 2:** Select Softether VPN Server.

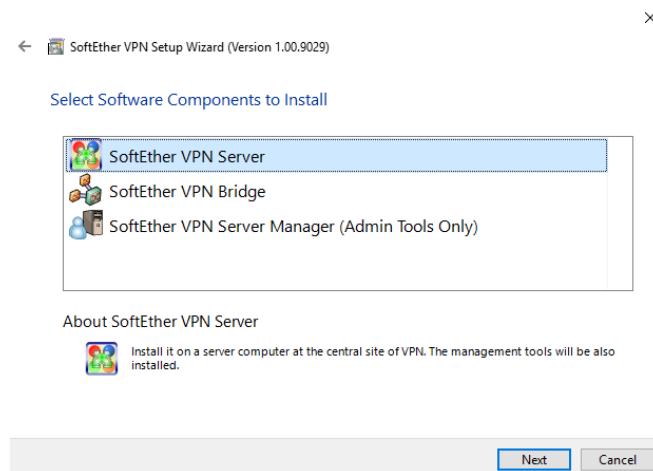


Figure 5.280: Select Softether VPN Server

**STEP 3:** Tick on agree and click Next.

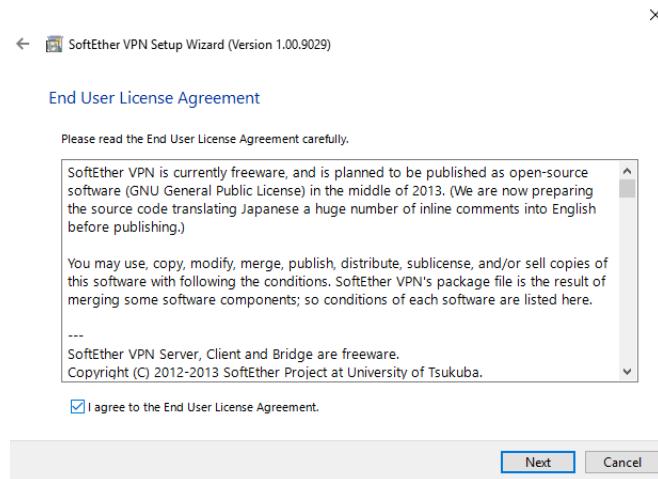


Figure 5.281: User to the License Agreement

**STEP 4:** Click Next.

**STEP 5:** Softether VPN Server is ready to install and click Next.

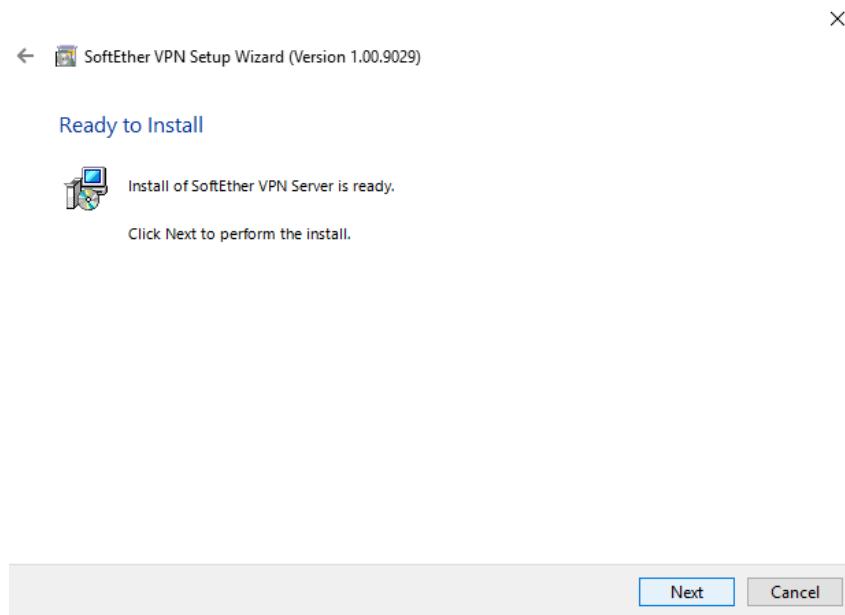


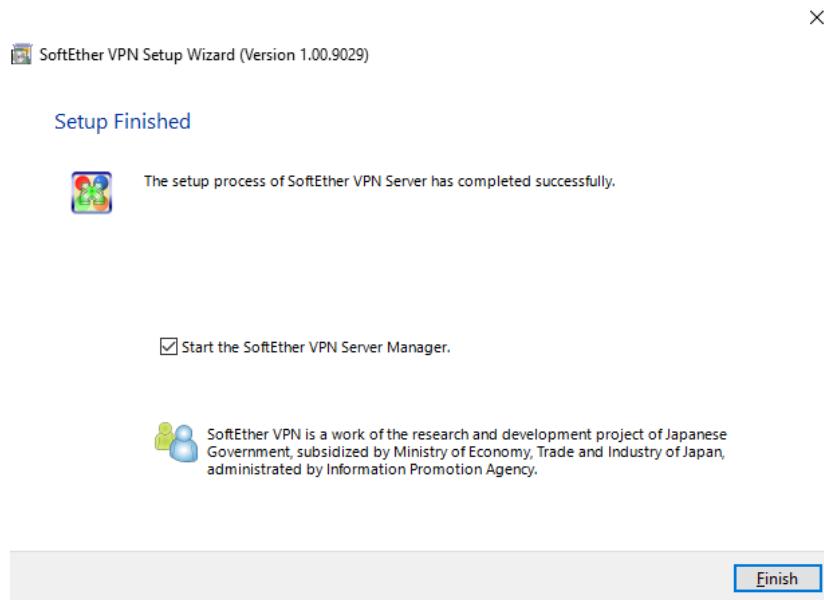
Figure 5.282: Confirm install

**STEP 6:** Installation in progress.



*Figure 5.283: Progress installation*

**STEP 7:** Finish the installation.



*Figure 5.284: Finish the installation.*

**STEP 8:** Run the Softether VPN Server Manager and double click on the localhost.



Figure 5.285: Run the Softether

**STEP 9:** Set the setting name as VPN, fill the host name with IP address of the server and select Port Number 5555. Set the password to connect administration mode. Then, click OK.

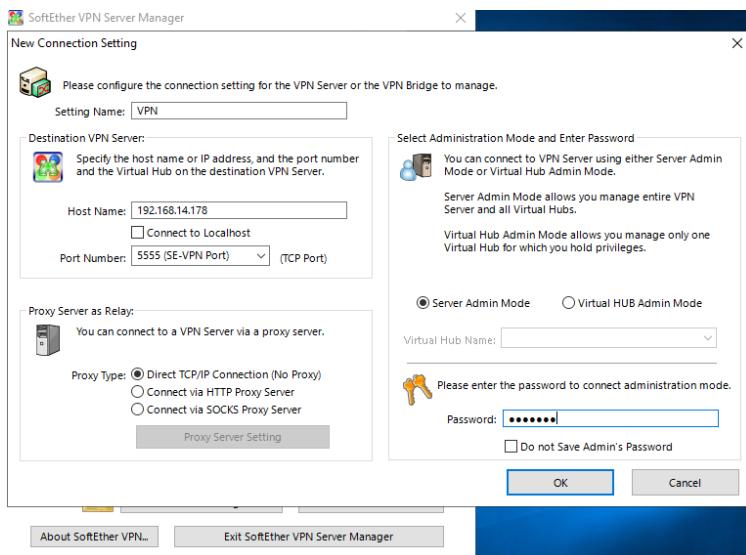


Figure 5.286: Setting name

**STEP 10:** The setting will change as below.



*Figure 5.287: Setting*

**STEP 11:** Tick at the Remote Access VPN Server and click Next.



*Figure 5.288: Remote access*

## STEP 12: Popup Easy Setup shows the default Virtual Hub Name is VPN.

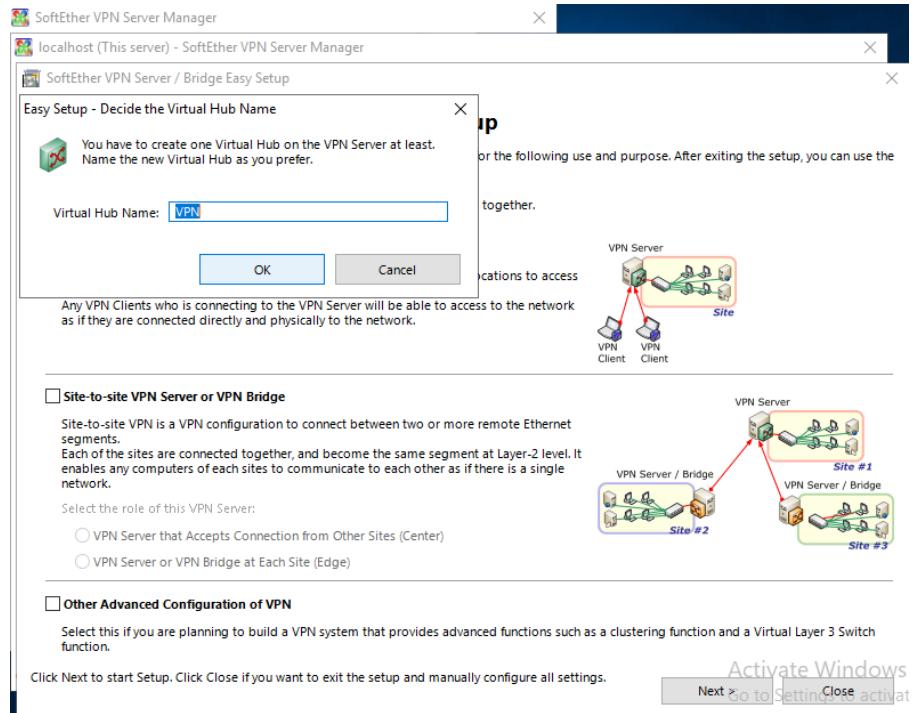


Figure 5.289: Set default

## STEP 13: The Dynamic DNS Hostname is given and click Exit.

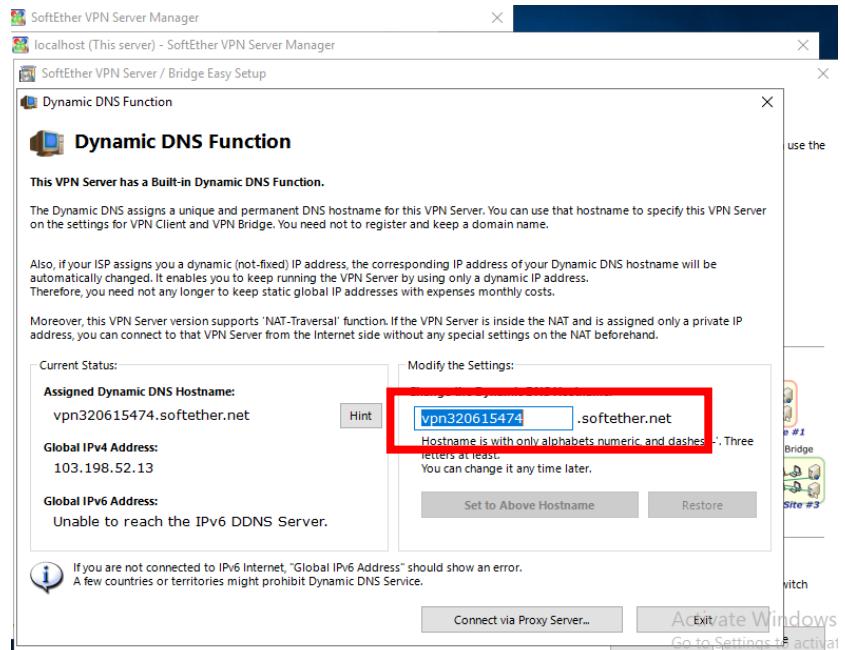


Figure 5.290: DNS hostname

**STEP 14:** Tick both of the Enable L2TP Server Function (L2TP over IPSec) and Enable L2TP Server Function (Raw L2TP with No Encryption). Click OK.

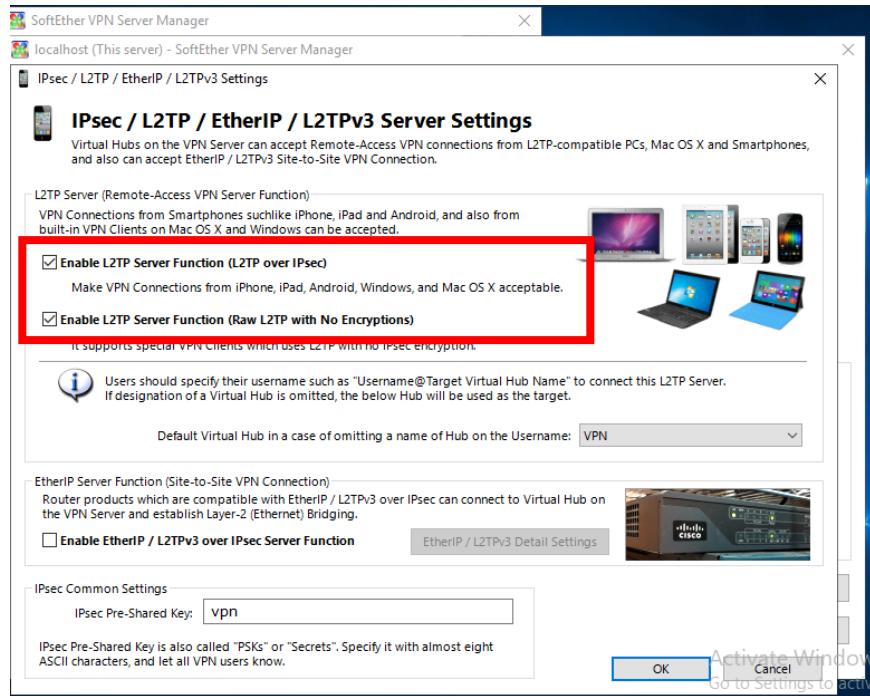


Figure 5.291: Enable L2TP

**STEP 15:** Now, let's create a user. Click on Manage Virtual Hub and Create Users. Create a user name, client1, full name and the password for client1.

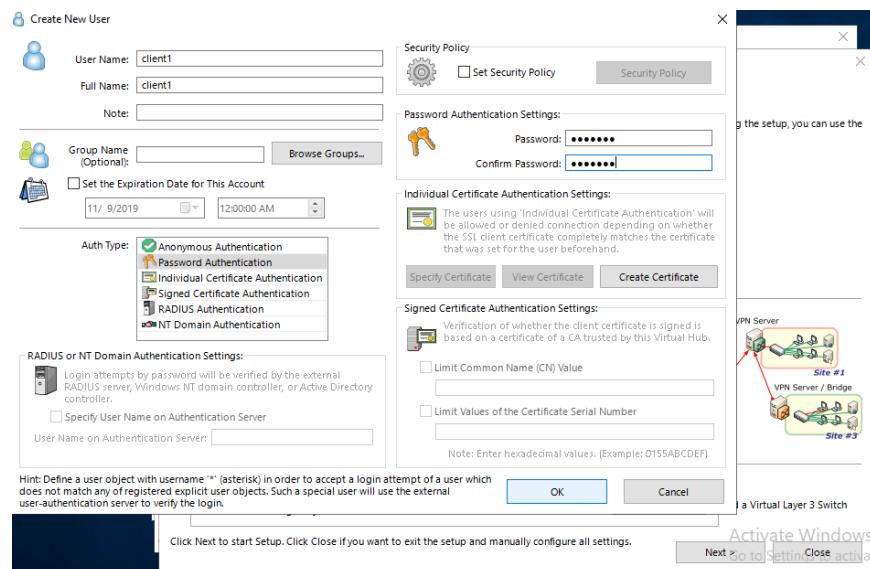


Figure 5.292: Manage Virtual Hub

**STEP 16:** User client1 has been created. Click Exit.

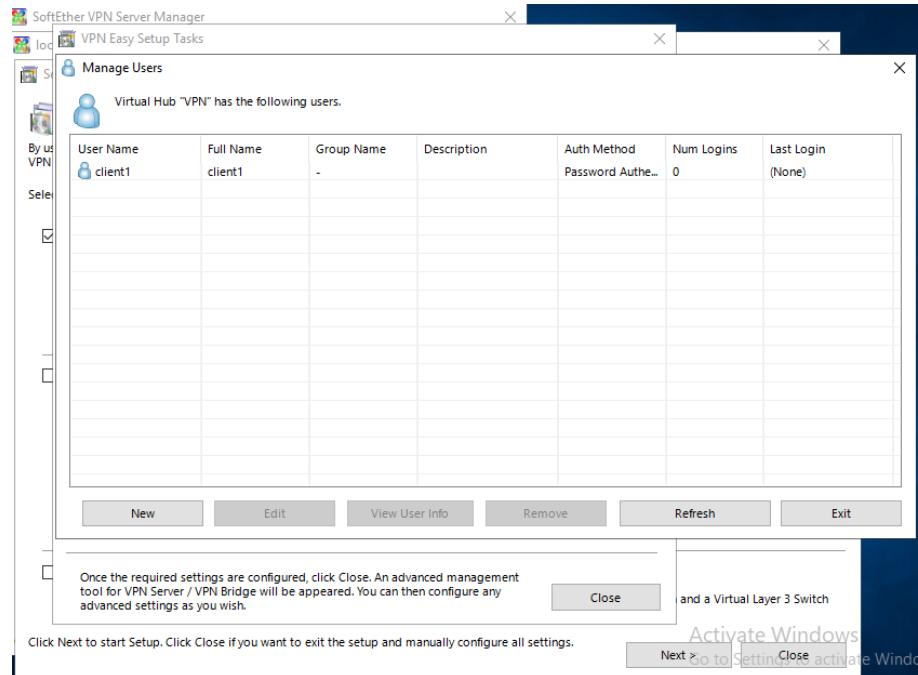


Figure 5.293: Create Client

**STEP 17:** Create a certificate for the user client1 by filling the blank. Next, click OK.

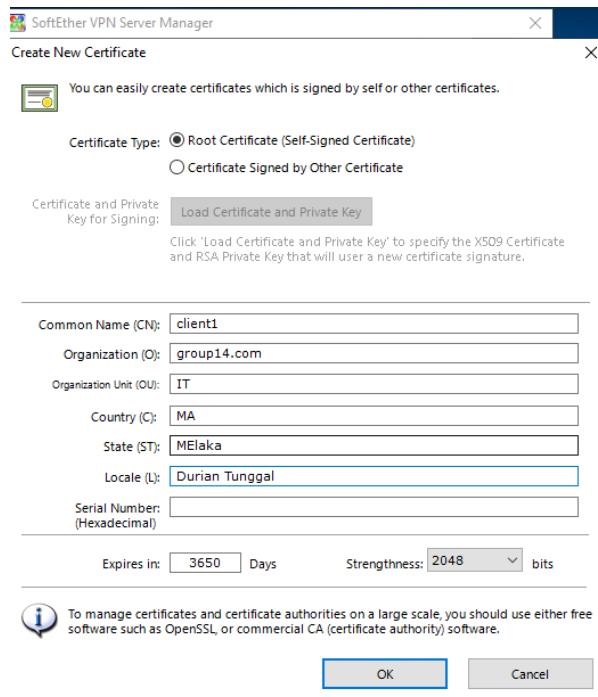


Figure 5.294: Create Cert

**STEP 18:** Save the certificate as X509 Certificate (.CER) and Private Key file (.KEY).  
Set the passphrase of the certificate to encrypt.

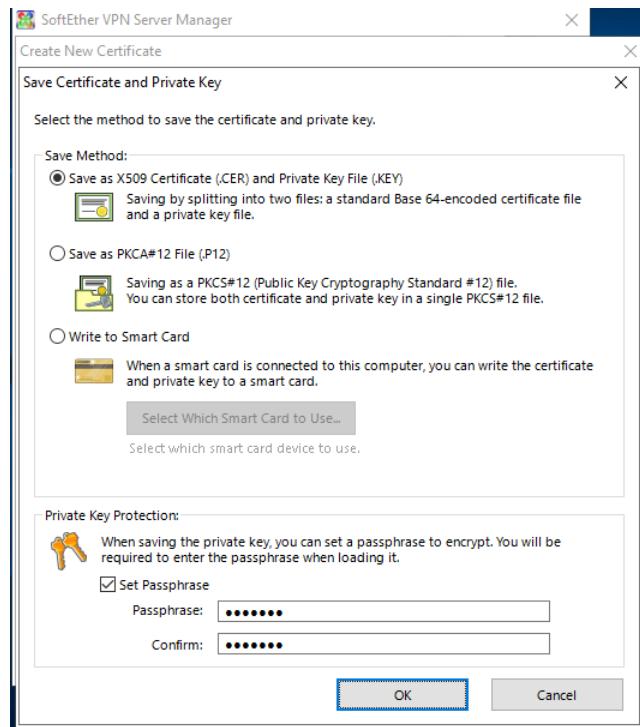


Figure 5.295: Save Cert

**STEP 19:** The certificate of the client1 has been saved in the folder IPSec VPN.

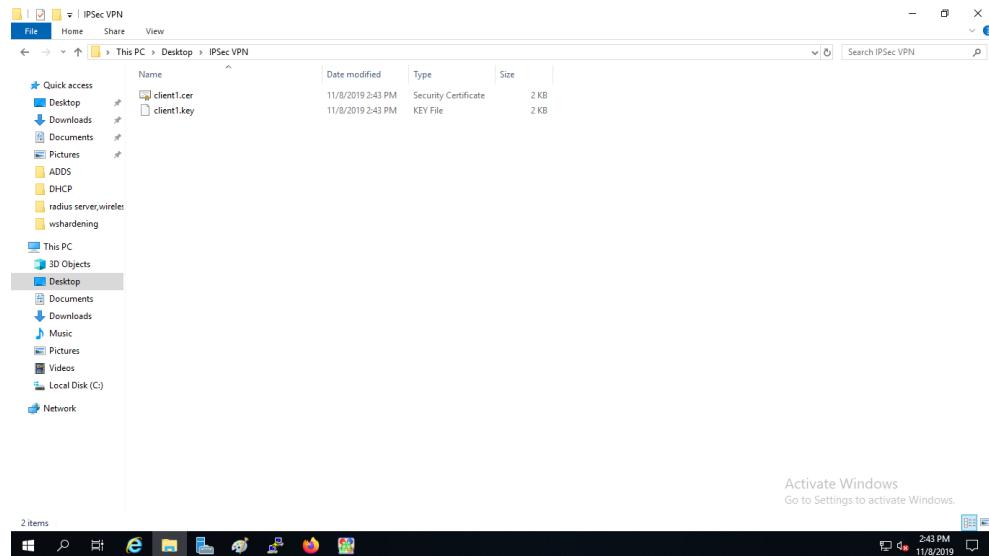


Figure 5.296: Ipsec VPN

### 5.3.2.22 VPN CLIENT

**STEP 1:** Starting to install the Softether VPN Client Manager in client server.

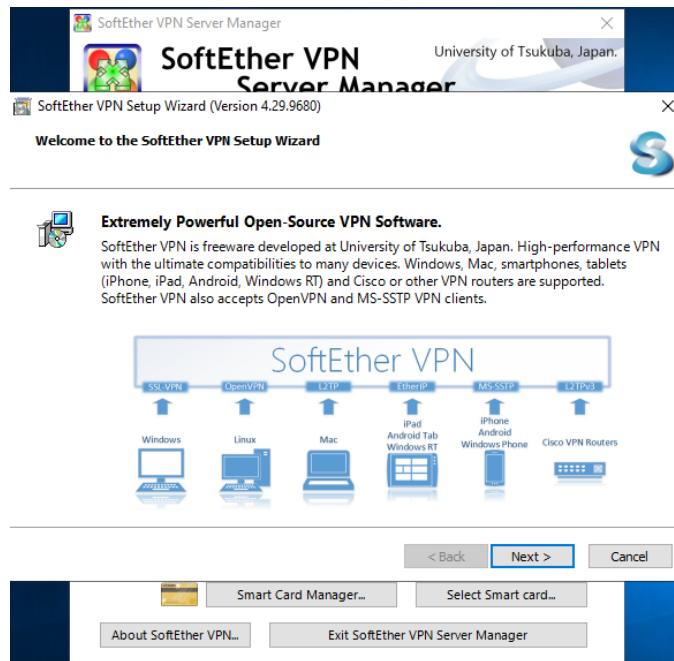


Figure 5.297: install the Sofether

**STEP 2:** Choose Sofether VPN Client.



Figure 5.298: Choose Sofether VPN Client

**STEP 3:** Tick I agree and click Next.

**STEP 4:** Click Next.

**STEP 5:** Now, VPN Client is ready to install. Click Next.

**STEP 6:** Installation begins.

**STEP 7:** Finish the installation.

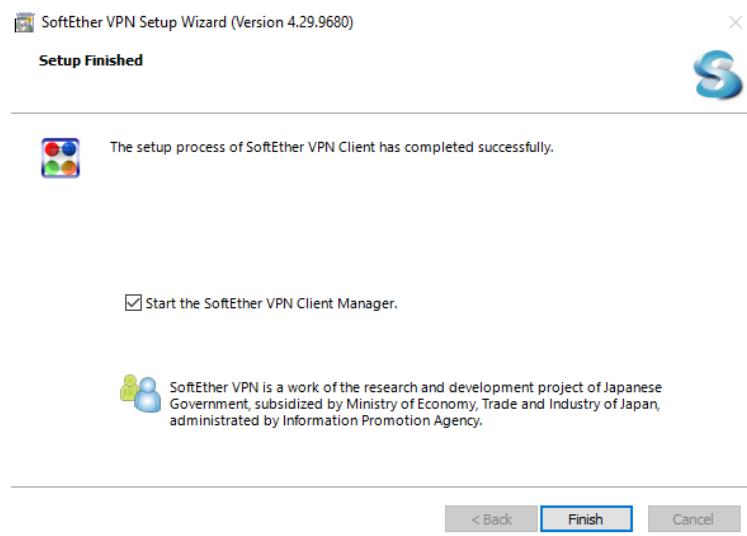


Figure 5.299: Finish Installation

**STEP 8:** Start to configure VPN Client Manager. Add a new VPN Connection Setting.

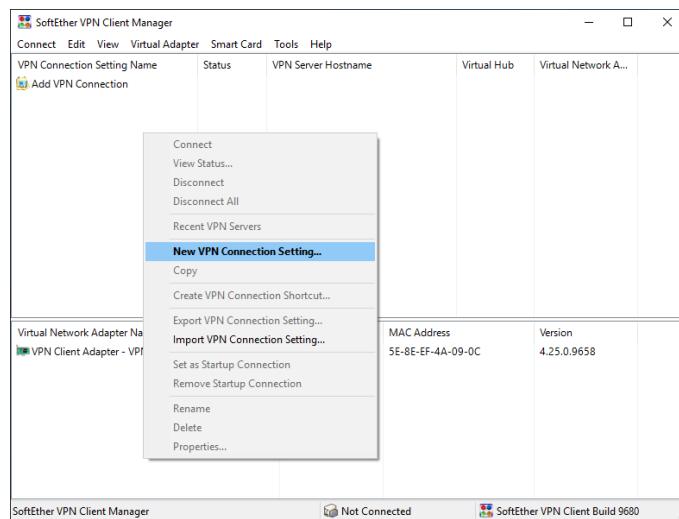


Figure 5.300: Configure VPN Client Manager

**STEP 9:** Set the Setting Name as the name of VPN Server, host name is the IP address of the server and supply the client credential that has been created at the server previously.

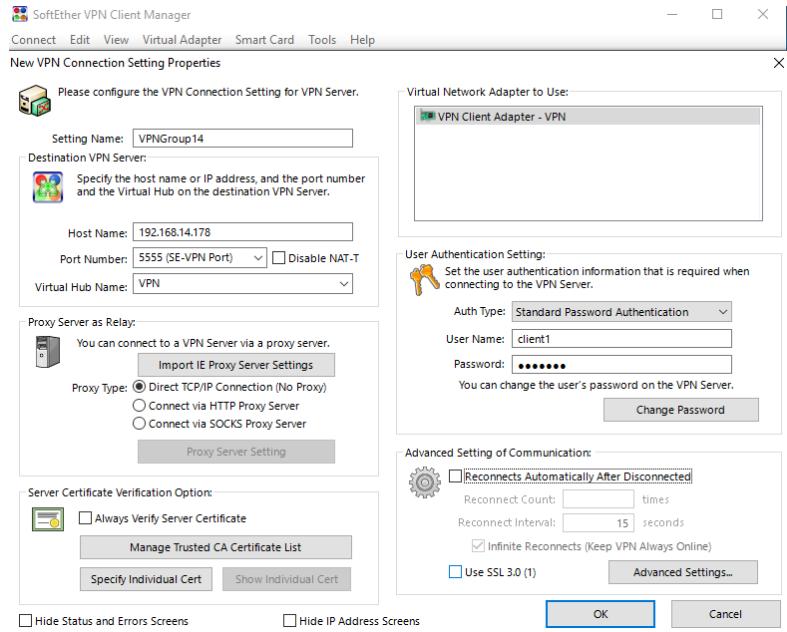


Figure 5.301: VPN Server

### 5.3.23 USER AUTHENTICATION BY INTEGRATING AD WITH LINUX

**STEP 1:** Go to the following address and download the most current version of PBIS:

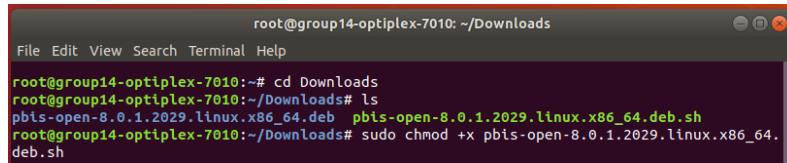
<http://download1.beyondtrust.com/Technical-Support/Downloads/PowerBroker-Identity-Services-Open-Edition/?Pass=True>

Or, from a terminal type the following commands:

```
sudo wget http://download.beyondtrust.com/PBISO/8.0.1/linux.deb.x64/pbis-open-8.0.1.2029.linux.x86_64.deb.sh
```

**STEP 2:** After downloading, in the terminal, navigate to the directory where the previous PBIS is located and execute the following command:

```
sudo chmod +x pbis-open-8.0.1.2029.linux.x86_64.deb.sh
```



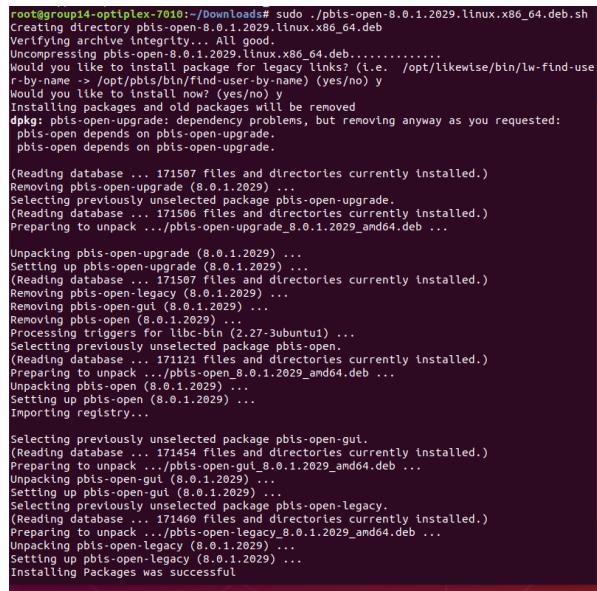
A screenshot of a terminal window titled "root@group14-optiplex-7010: ~/Downloads". The window shows the following command being run:

```
root@group14-optiplex-7010:~# cd Downloads
root@group14-optiplex-7010:~/Downloads# ls
pbis-open-8.0.1.2029.linux.x86_64.deb  pbis-open-8.0.1.2029.linux.x86_64.deb.sh
root@group14-optiplex-7010:~/Downloads# sudo chmod +x pbis-open-8.0.1.2029.linux.x86_64.deb.sh
```

Figure 5.302: Navigate Directory

**STEP 3:** Next, type the following command to install the PBIS open.

```
sudo ./pbis-open-8.0.1.2029.linux.x86_64.deb.sh
```



A screenshot of a terminal window titled "root@group14-optiplex-7010:~/Downloads". The window shows the following command being run:

```
root@group14-optiplex-7010:~/Downloads# sudo ./pbis-open-8.0.1.2029.linux.x86_64.deb.sh
Creating directory pbis-open-8.0.1.2029.linux.x86_64.deb
Verifying archive integrity... All good.
Uncompressing pbis-open-8.0.1.2029.linux.x86_64.deb.....
Would you like to install package for legacy links? (i.e. /opt/likewise/bin/lw-find-user-by-name -> /opt/pbis/bin/find-user-by-name) (yes/no) y
Would you like to install now? (yes/no) y
Installing packages and old packages will be removed
dpkg: pbis-open-upgrade: dependency problems, but removing anyway as you requested:
  pbis-open depends on pbis-open-upgrade.
  pbis-open depends on pbis-open-upgrade.

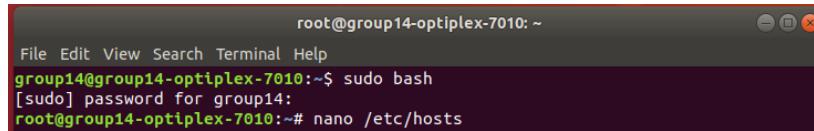
(Reading database ... 171507 files and directories currently installed.)
Removing pbis-open-upgrade (8.0.1.2029) ...
Selecting previously unselected package pbis-open-upgrade.
(Reading database ... 171506 files and directories currently installed.)
Preparing to unpack .../pbis-open-upgrade_8.0.1.2029_amd64.deb ...

Unpacking pbis-open-upgrade (8.0.1.2029) ...
Setting up pbis-open-upgrade (8.0.1.2029) ...
(Reading database ... 171507 files and directories currently installed.)
Removing pbis-open-legacy (8.0.1.2029) ...
Removing pbis-open-gui (8.0.1.2029) ...
Removing pbis-open (8.0.1.2029) ...
Processing triggers for liblc-bin (2.27-SubUnt1) ...
Selecting previously unselected package pbis-open.
(Reading database ... 171121 files and directories currently installed.)
Preparing to unpack .../pbis-open_8.0.1.2029_amd64.deb ...
Unpacking pbis-open (8.0.1.2029) ...
Setting up pbis-open (8.0.1.2029) ...
Importing registry...

Selecting previously unselected package pbis-open-gui.
(Reading database ... 171454 files and directories currently installed.)
Preparing to unpack .../pbis-open-gui_8.0.1.2029_amd64.deb ...
Unpacking pbis-open-gui (8.0.1.2029) ...
Setting up pbis-open-gui (8.0.1.2029) ...
Selecting previously unselected package pbis-open-legacy.
(Reading database ... 171460 files and directories currently installed.)
Preparing to unpack .../pbis-open-legacy_8.0.1.2029_amd64.deb ...
Unpacking pbis-open-legacy (8.0.1.2029) ...
Setting up pbis-open-legacy (8.0.1.2029) ...
Installing Packages was successful
```

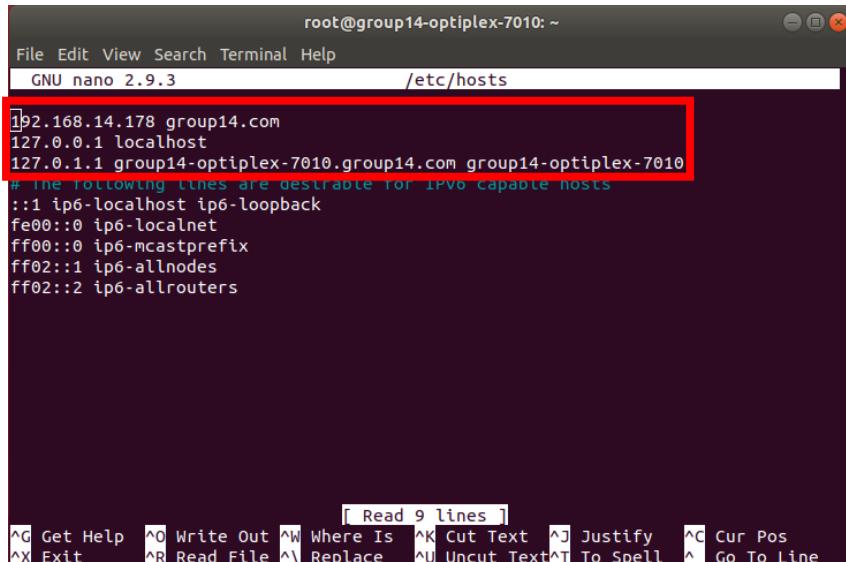
Figure 5.303: Install the PBIS

**STEP 4:** Type *nano /etc/hosts* to add ip address and domain name of Active Directory.



```
root@group14-optiplex-7010:~$ sudo bash  
[sudo] password for group14:  
root@group14-optiplex-7010:~# nano /etc/hosts
```

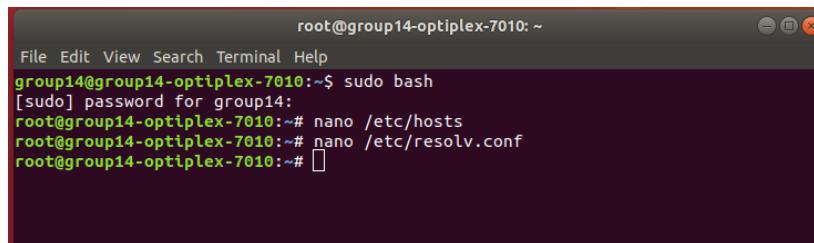
Figure 5.304: Direct to */etc/hosts*



```
root@group14-optiplex-7010:~$  
File Edit View Search Terminal Help  
GNU nano 2.9.3           /etc/hosts  
192.168.14.178 group14.com  
127.0.0.1 localhost  
127.0.0.1 group14-optiplex-7010.group14.com group14-optiplex-7010  
# The following lines are desirable for IPv6 capable hosts  
::1 ip6-localhost ip6-loopback  
fe00::0 ip6-localnet  
ff00::0 ip6-mcastprefix  
ff02::1 ip6-allnodes  
ff02::2 ip6-allrouters  
  
[ Read 9 lines ]  
^G Get Help  ^O Write Out  ^W Where Is  ^K Cut Text  ^J Justify  ^C Cur Pos  
^X Exit  ^R Read File  ^V Replace  ^U Uncut Text  ^T To Spell  ^L Go To Line
```

Figure 5.305: Edit */etc/hosts*

**STEP 5:** Type *nano /etc/resolv.conf* to add ip address of the windows server.



```
root@group14-optiplex-7010:~$ sudo bash  
[sudo] password for group14:  
root@group14-optiplex-7010:~# nano /etc/hosts  
root@group14-optiplex-7010:~# nano /etc/resolv.conf  
root@group14-optiplex-7010:~#
```

Figure 5.306: Direct to */etc/resolv.conf*

```

root@group14-optiplex-7010: ~
File Edit View Search Terminal Help
GNU nano 2.9.3          /etc/resolv.conf          Modified
# This file is managed by man:systemd-resolved(8). Do not edit.
#
# This is a dynamic resolv.conf file for connecting local clients to the
# internal DNS stub resolver of systemd-resolved. This file lists all
# configured search domains.
#
# Run "systemd-resolve --status" to see details about the uplink DNS servers
# currently in use.
#
# Third party programs must not access this file directly, but only through the
# symlink at /etc/resolv.conf. To manage man:resolv.conf(5) in a different way,
# replace this symlink by a static file or a different symlink.
#
# See man:systemd-resolved.service(8) for details about the supported modes of
# operation for /etc/resolv.conf.
nameserver 192.168.14.178
nameserver 127.0.0.53
options edns0

^G Get Help  ^O Write Out  ^W Where Is  ^K Cut Text  ^J Justify  ^C Cur Pos
^X Exit      ^R Read File  ^P Replace   ^U Uncut Text  ^T To Spell  ^L Go To Line

```

Figure 5.307: Edit /etc/resolv.conf

#### STEP 6: Setup the Active Directory login settings.

```

root@group14-optiplex-7010:~# sudo /opt/pbis/bin/config UserDomainPrefix group14
.com
root@group14-optiplex-7010:~# sudo /opt/pbis/bin/config AssumeDefaultDomain true
root@group14-optiplex-7010:~# sudo /opt/pbis/bin/config LoginShellTemplate /bin/
bash
root@group14-optiplex-7010:~# sudo /opt/pbis/bin/config HomeDirTemplate %H/%D/%U
root@group14-optiplex-7010:~# sudo /opt/pbis/bin/config RequireMembershipOf grou
p14.com\\IntegrateAD

```

Figure 5.308: Setup AD settings

#### STEP 7: Change to *pam.d* directory and open the *common-session* file.

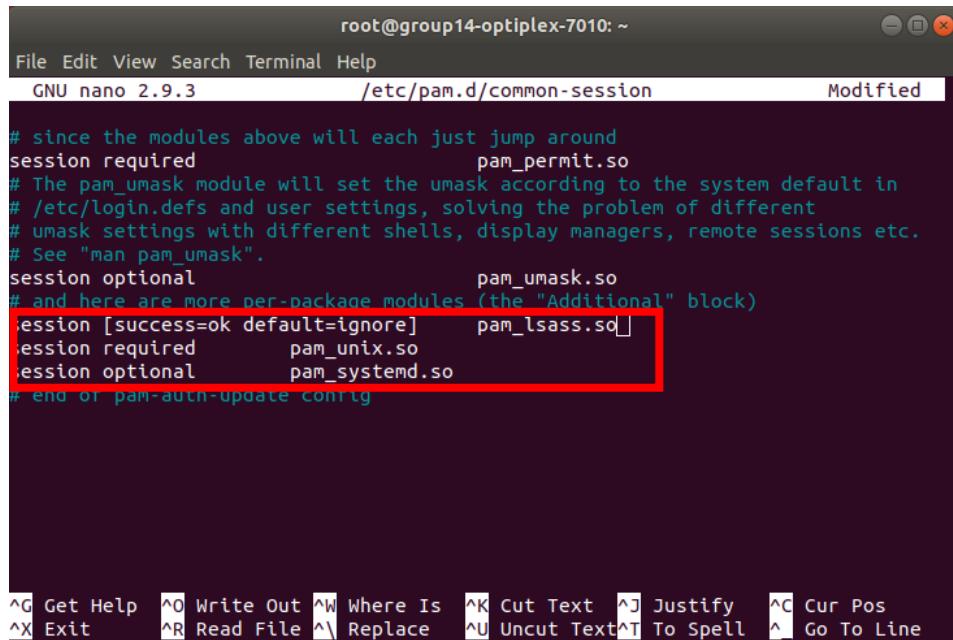
```

root@group14-optiplex-7010:/opt/pbis/bin# cd /etc/pam.d/common-session
bash: cd: /etc/pam.d/common-session: Not a directory
root@group14-optiplex-7010:/opt/pbis/bin# nano /etc/pam.d/common-session
Use "fg" to return to nano.

[1]+  Stopped                  nano /etc/pam.d/common-session
root@group14-optiplex-7010:/opt/pbis/bin# cd
root@group14-optiplex-7010:~# nano /etc/pam.d/common-session

```

Figure 5.309: Direct to pam.d/common-session



```

root@group14-optiplex-7010: ~
File Edit View Search Terminal Help
GNU nano 2.9.3          /etc/pam.d/common-session          Modified
# since the modules above will each just jump around
# session required          pam_permit.so
# The pam_umask module will set the umask according to the system default in
# /etc/login.defs and user settings, solving the problem of different
# umask settings with different shells, display managers, remote sessions etc.
# See "man pam_umask".
session optional          pam_umask.so
# and here are more per-package modules (the "Additional" block)
session [success=ok default=ignore]    pam_lsass.so
session required          pam_unix.so
session optional          pam_systemd.so
# end of pam-auth-update config

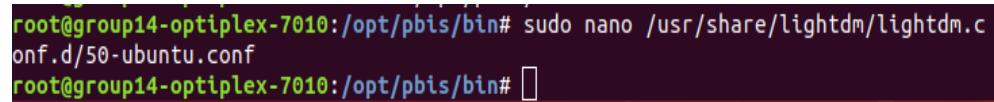
```

^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos  
 ^X Exit ^R Read File ^\ Replace ^U Uncut Text ^T To Spell ^\_ Go To Line

Figure 5.310: Edit pam.d/common-session

STEP 8: Then, open the lightfm configuration file and append the following lines:

`sudo nano /usr/share/lightdm/lightdm.conf.d/50-ubuntu.conf`

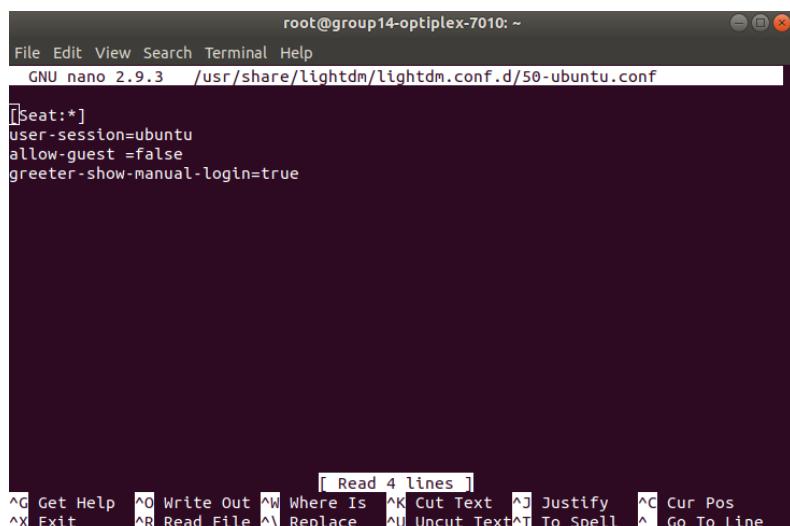


```

root@group14-optiplex-7010:/opt/pbis/bin# sudo nano /usr/share/lightdm/lightdm.conf.d/50-ubuntu.conf
root@group14-optiplex-7010:/opt/pbis/bin# 

```

Figure 5.311: Edit lightdm



```

root@group14-optiplex-7010: ~
File Edit View Search Terminal Help
GNU nano 2.9.3          /usr/share/lightdm/lightdm.conf.d/50-ubuntu.conf
[seat:*]
user-session=ubuntu
allow-guest =false
greeter-show-manual-login=true

```

[ Read 4 lines ]  
 ^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos  
 ^X Exit ^R Read File ^\ Replace ^U Uncut Text ^T To Spell ^\_ Go To Line

Figure 5.312: Lightdm configuration

**STEP 9:** Now, to integrate with Active Directory with a user created on Active Directory by using following commands:

```
sudo domainjoin-cli join --disable ssh group14.com Administrator@group14.com
```

When prompted for a password, supply the credentials and should receive a “SUCCESS” prompt when finished.

```
root@group14-optiplex-7010:~# sudo domainjoin-cli join --disable ssh group14.com
Administrator@group14.com
Joining to AD Domain: group14.com
With Computer DNS Name: group14-optiplex-7010.group14.com

Administrator@GROUP14.COM's password:
SUCCESS
```

*Figure 5.313: Integrate with Active Directory*

### 5.3.24 WINDOWS SERVER HARDENING

#### Configure Auditing policy

**STEP 1:** Go to Start, Administrative Tools, and then click on Group Policy Management.

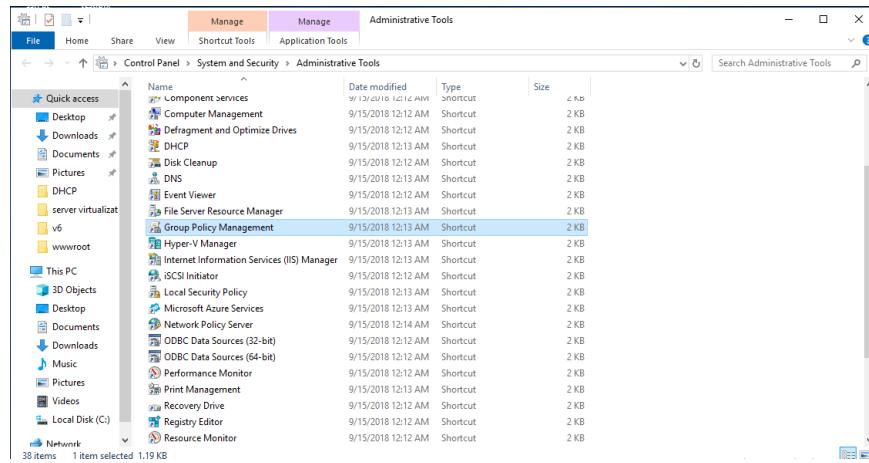


Figure 5.314: Configuring Group Policy Management

**STEP 2:** Right click on Default Domain Controller Policy and then left click on Edit.

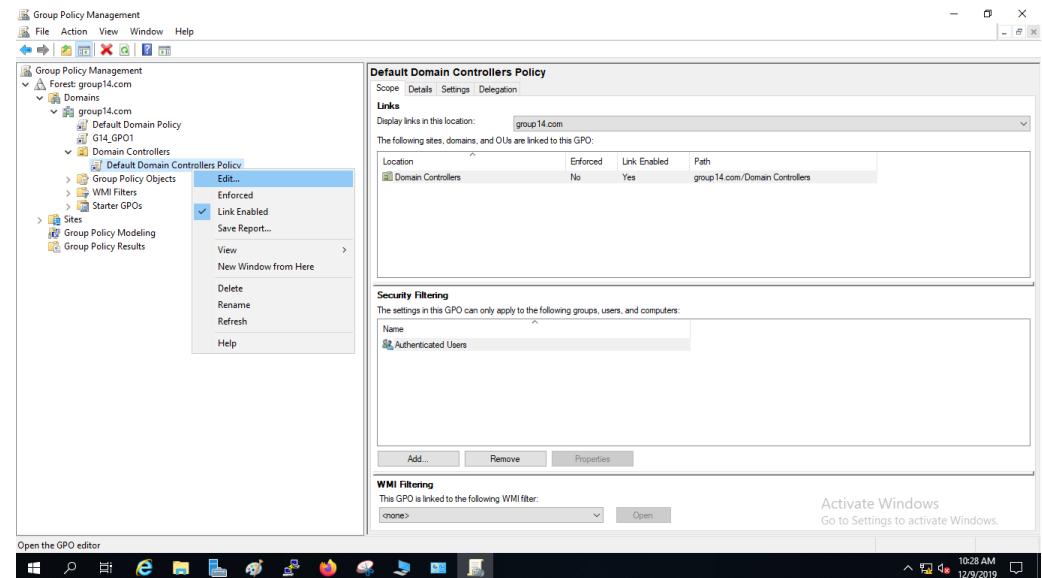


Figure 5.315: Edit the GPO for Domain

**STEP 3:** Navigate under Computer Configuration → Policies → Windows Setting → Security Settings → Local Policies → Audit Policy

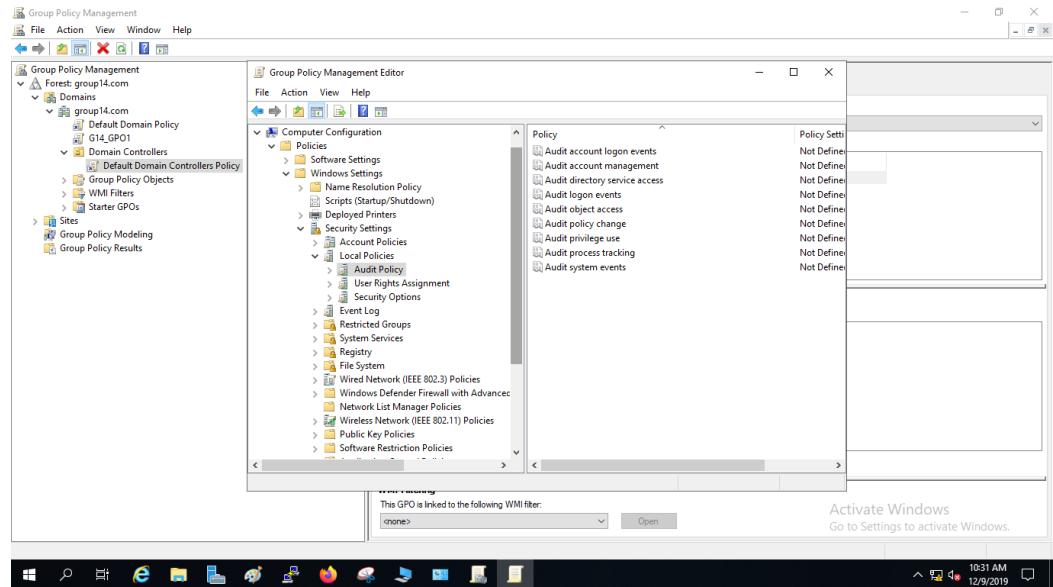


Figure 5.316: Edit the Audit Policy

**STEP 4:** Right click on Audit Directory Service Access, and then click Properties.

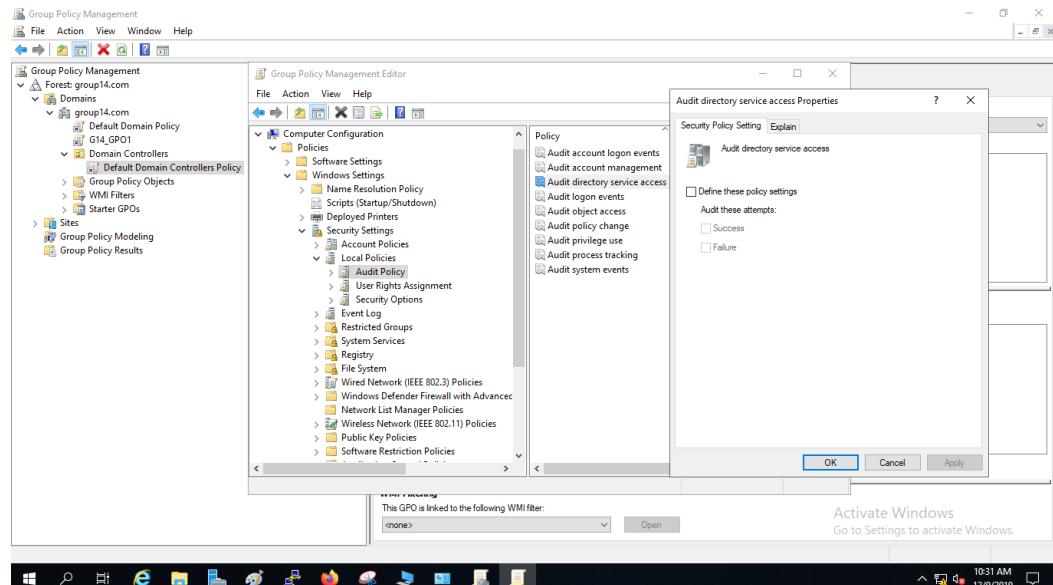


Figure 5.317: Change the properties of the service

**STEP 5:** Tick on Define these policy settings and select Success. Click on Apply and then OK.

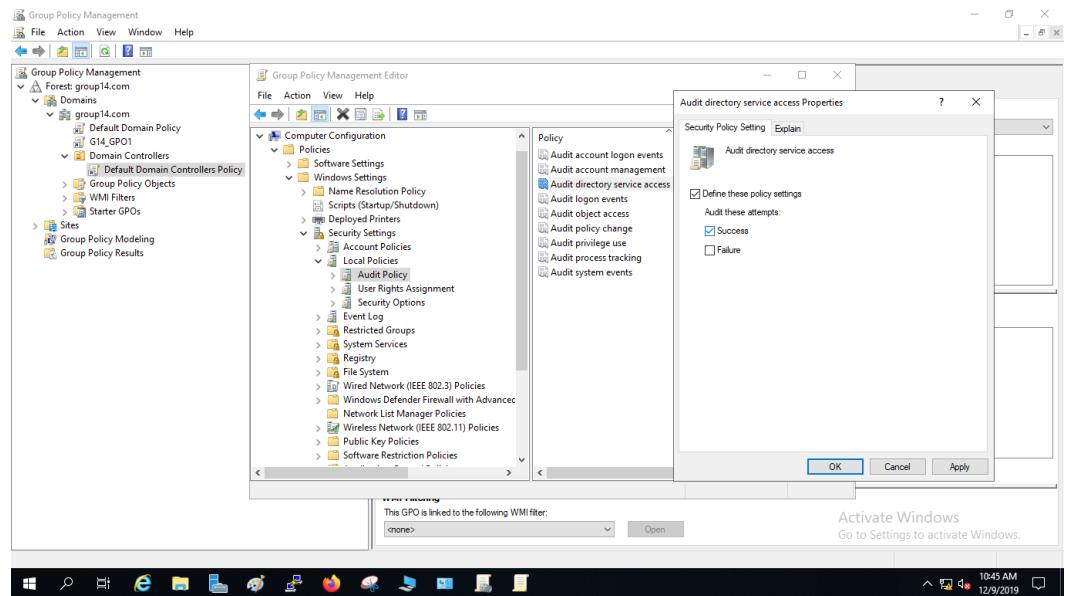


Figure 5.318: Select Success

**STEP 6:** The policy setting will change as below.

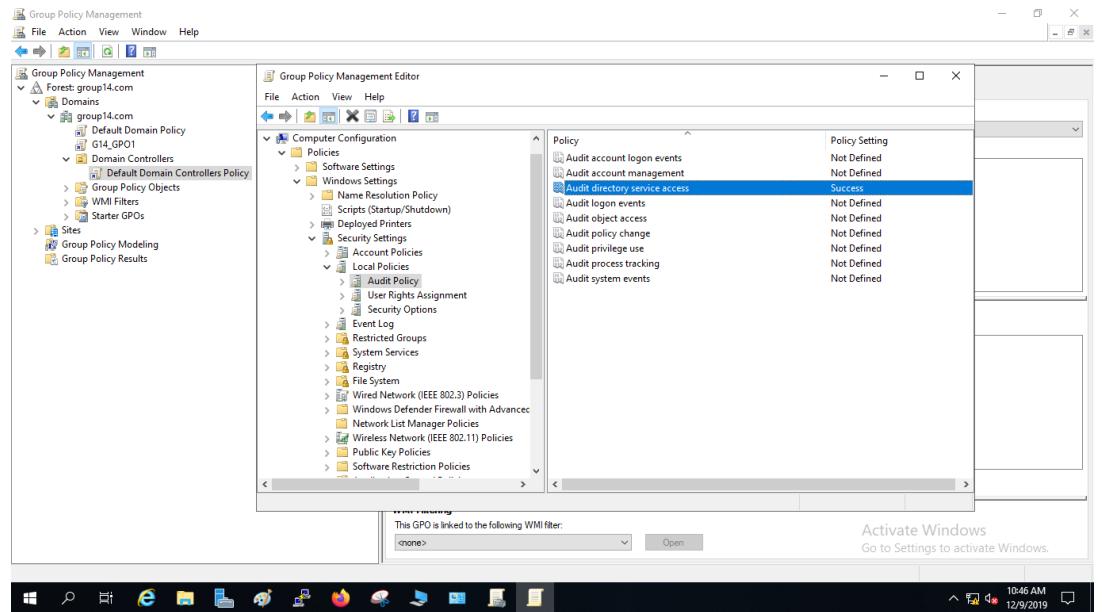


Figure 5.319: The policy setting changed

**STEP 7:** Run the command prompt and type the following command:

```
#auditpol /set /subcategory:"directory service changes" /success:enable
```

The successful message will appear.

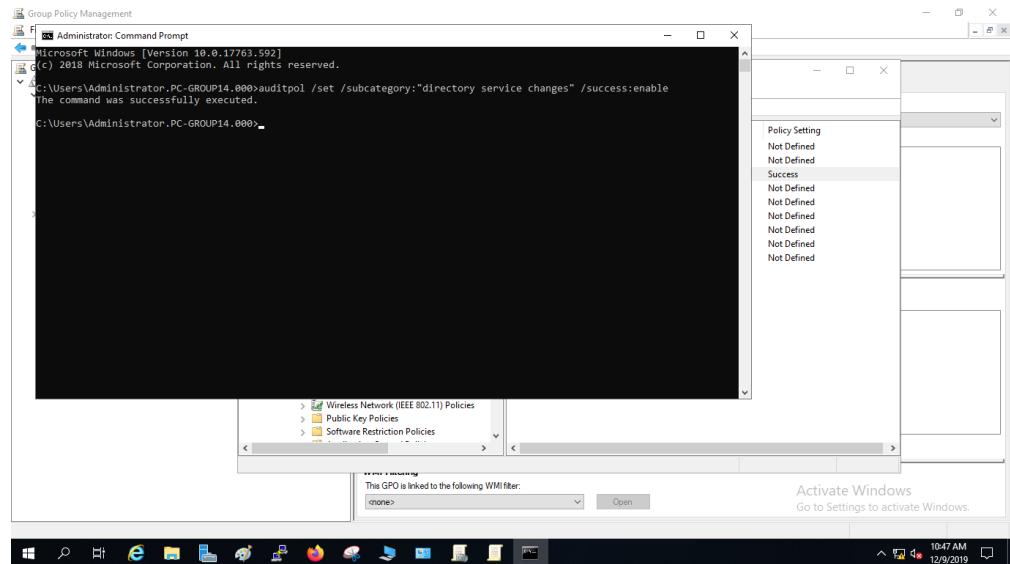


Figure 5.320: Execute the changes

### Enable Windows Firewall.

**STEP 1:** Go to System and Security → Windows Defender Firewall.

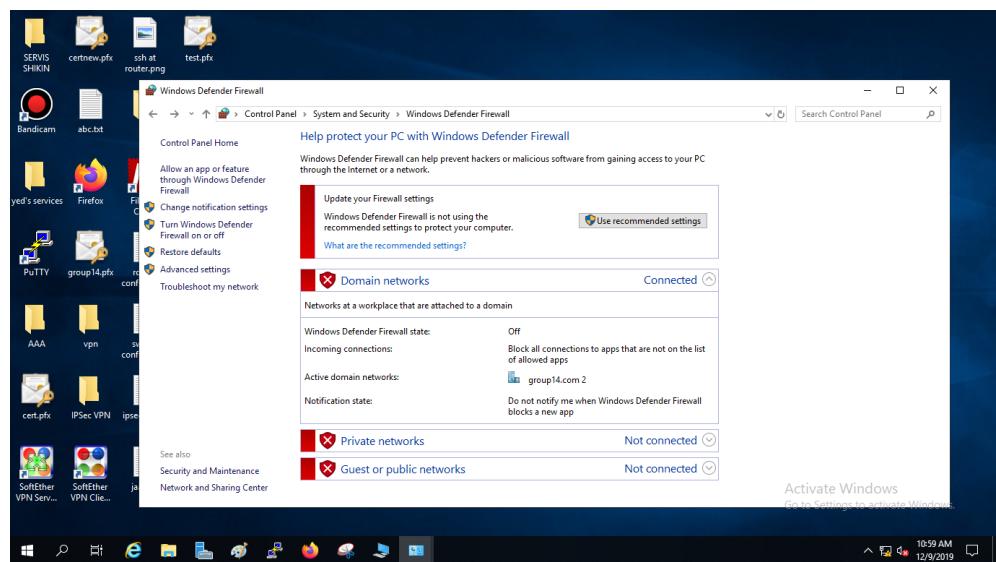


Figure 5.321: Windows Firewall Setting

## STEP 2: Turn on the Windows Firewall.

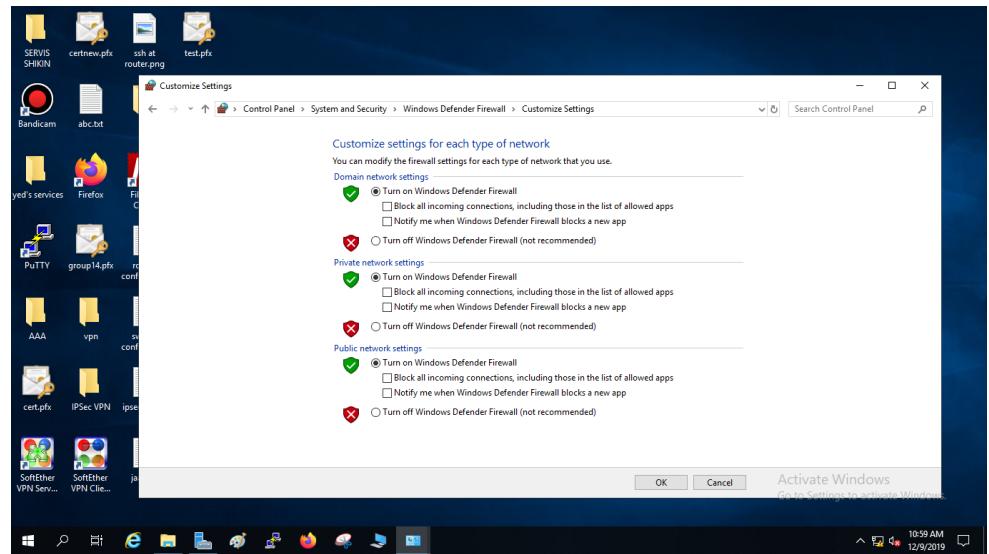


Figure 5.322: Turn on the Windows Firewall

## STEP 3: Now, the firewall is turned on.

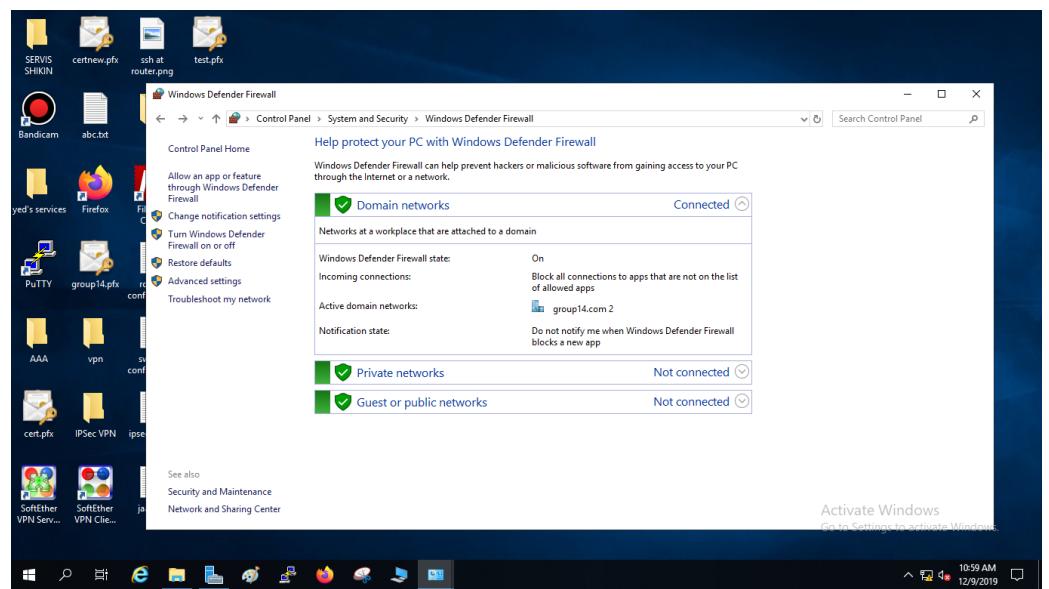


Figure 5.323: The green indicates the firewall is turned on

## Disable Automatic Services.

**STEP 1:** Go to Services.

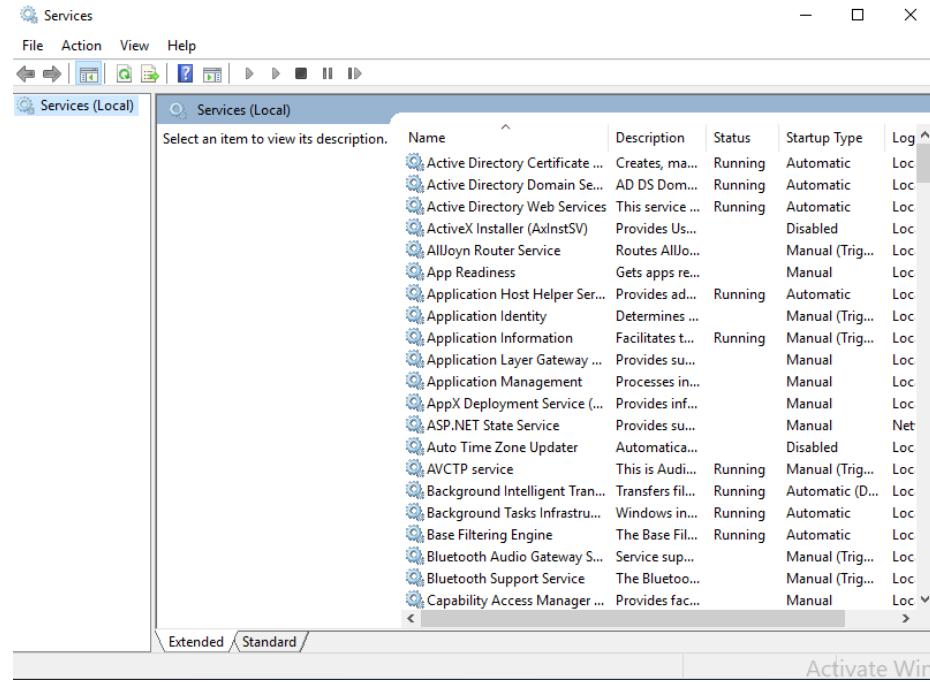


Figure 5.324: Go to Services

**STEP 2:** Choose Distributed Transaction Coordinator. The startup type is Automatic.

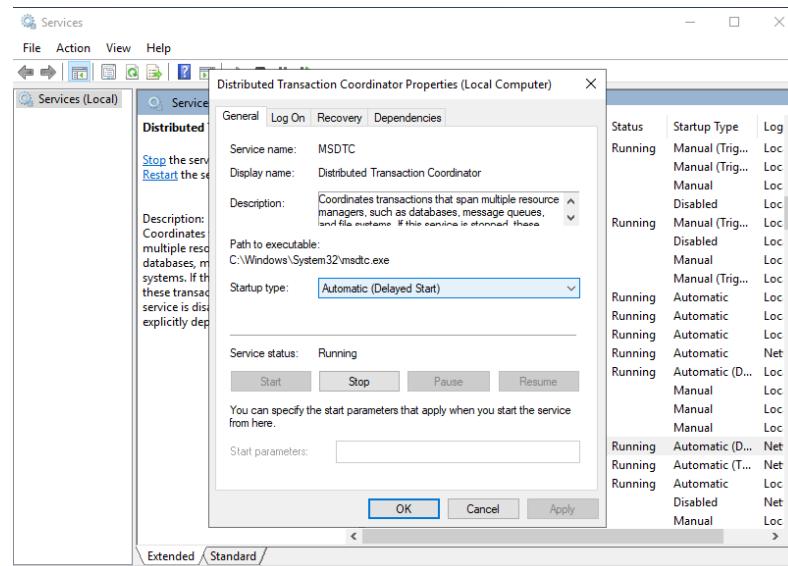


Figure 5.325: Change the startup type

**STEP 3:** Change the startup type to Disabled. This is an unused service where it coordinates transaction and distributed across multiple computer systems or resource managers such as databases, message queues, file system or other transaction-protected resource managers.

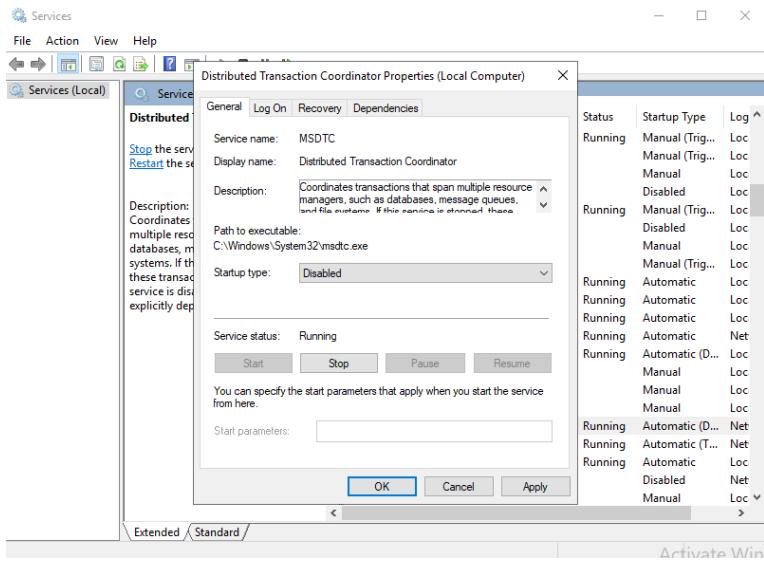


Figure 5.326: Change from Automatic to Disabled

### Disable or delete unnecessary/unused accounts.

**STEP 1:** Go to Active Directory User and Computers in Server Manager.

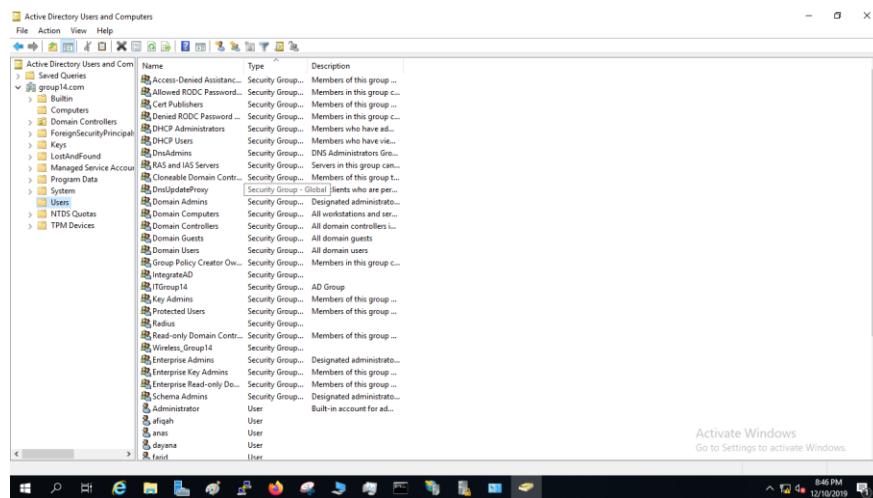
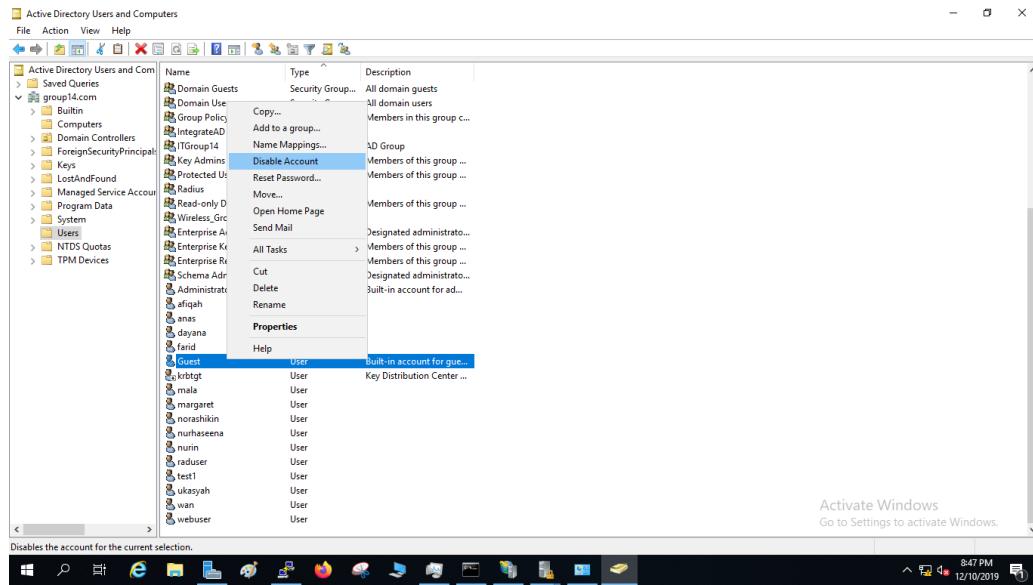


Figure 5.327: Go to AD Users and Computers

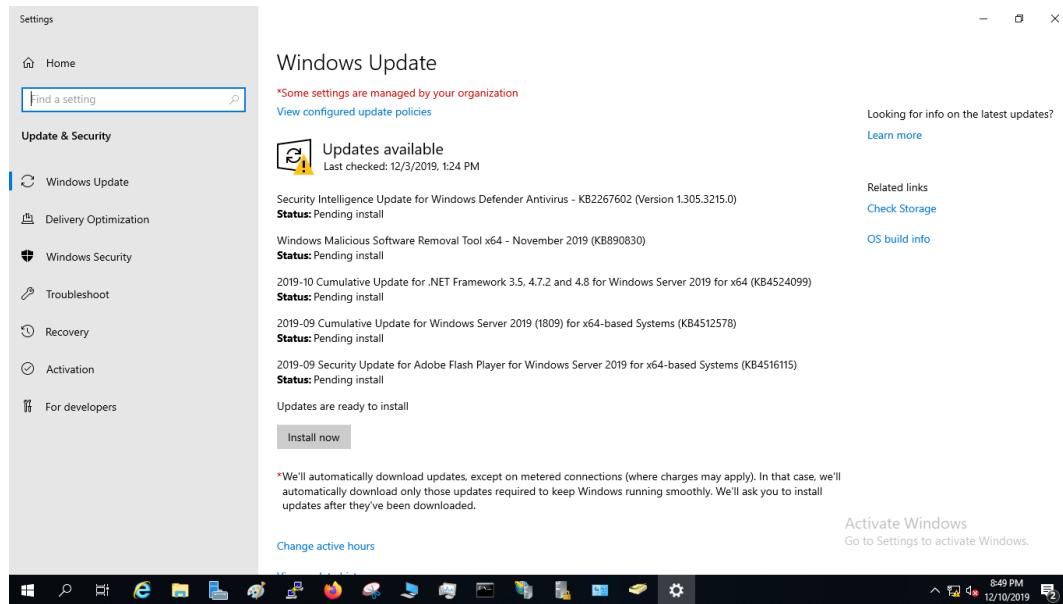
**STEP 2:** Click Users folder and right click on Guest. Select Disable Account.



*Figure 5.328: Disable the unused account: Guest*

## Updates and patches.

### **STEP 1:** Search for Windows Update Setting.



*Figure 5.329: Go to Windows Update*

## STEP 2: Automatically updates when there is Internet connection.

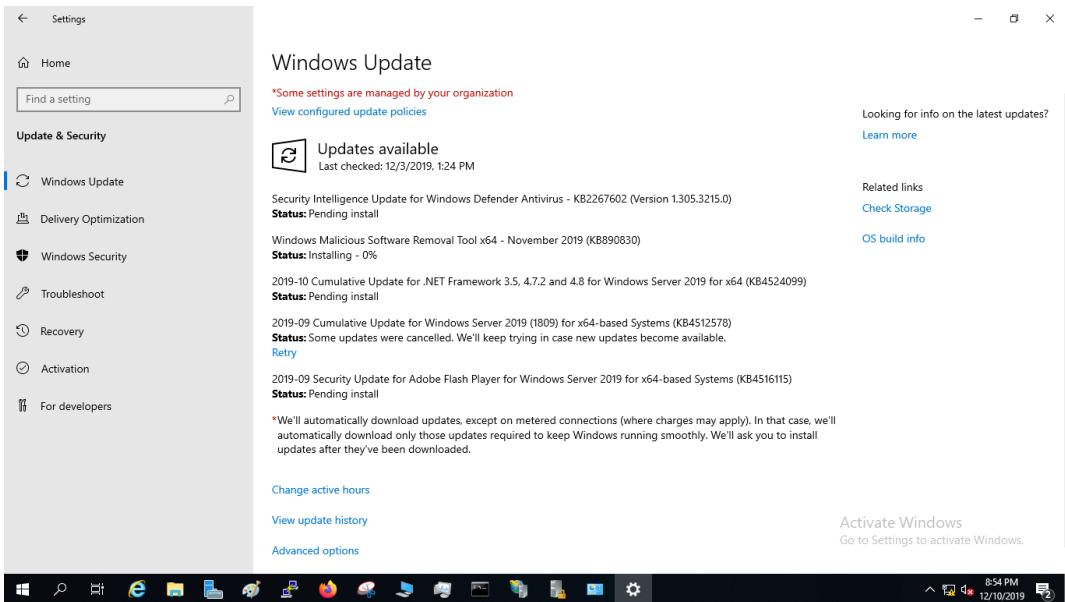


Figure 5.330: Automatically update

### 5.3.25 REMOTE LOGIN USING SSH

#### 5.3.25.1 Configuration SSH in Router

**Step 1:** Open PuTTY and log in to Router using Serial.

**Step 2:** Install SSH using this command below.

```
G14Router#  
G14Router#conf t  
Enter configuration commands, one per line. End with CNTL/Z.  
G14Router(config)#  
G14Router(config)#ip domain-name group14.com  
G14Router(config)#crypto key generate rsa general-keys modulus 1024  
The name for the keys will be: G14Router.group14.com  
  
% The key modulus size is 1024 bits  
% Generating 1024 bit RSA keys, keys will be non-exportable...  
[OK] (elapsed time was 1 seconds)  
  
G14Router(config)#  
*Nov 27 10:25:26.997: %SSH-5-ENABLED: SSH 1.99 has been enabled  
G14Router(config)#line vty 0 4  
G14Router(config-line)#transport input ssh  
G14Router(config-line)#username group14 privilege 15 secret g14l23456  
G14Router(config)#ip ssh version 2  
G14Router(config)#exit  
G14Router#  
*Nov 27 10:29:25.617: %SYS-5-CONFIG_I: Configured from console by raduser on con  
sole  
G14Router#wr  
Building configuration...  
  
[OK]  
G14Router#
```

Figure 5.331: SSH configuration in router

### 5.3.25.2 Configuration SSH in Ubuntu

**Step 1:** Open Terminal in Ubuntu.

**Step 2:** Firstly, update package list from the repository before installing the SSH.

**Step 3:** Then, install openssh-server package using the command below.

```
group14@group14-optiplex-7010:~$ sudo bash
[sudo] password for group14:
root@group14-optiplex-7010:~# sudo apt install -y openssh-server
Reading package lists... Done
Building dependency tree
Reading state information... Done
openssh-server is already the newest version (1:7.6p1-4ubuntu0.3).
The following packages were automatically installed and are no longer required:
  apturl-common dbconfig-common dbconfig-mysql default-mysql-client hplip-data
  libart-2.0-2 libjs-sphinxdoc libjs-underscore libsane-hpaio php-phpseclib
  php-tcpdf python3-olefile python3-pexpect python3-pil python3-ptyprocess
  python3-renderpm python3-reportlab python3-reportlab-accel
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 4 not upgraded.
root@group14-optiplex-7010:~#
```

Figure 5.332: SSH configuration in Ubuntu

**Step 4:** SSH service be started and enabled by default after the installation. To do a confirmation, it can be checked the status using command below.

```
root@group14-optiplex-7010:~# sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
  Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enab
  Active: active (running) since Mon 2019-12-16 10:14:12 +08; 22h ago
    Process: 20498 ExecReload=/bin/kill -HUP $MAINPID (code=exited, status=0/SUCCE
    Process: 20491 ExecReload=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
    Process: 21869 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 21870 (sshd)
      Tasks: 1 (limit: 4915)
        CGroup: /system.slice/ssh.service
               └─21870 /usr/sbin/sshd -D

Dis 17 08:58:02 group14-optiplex-7010 systemd[1]: Reloading OpenBSD Secure Shell
Dis 17 08:58:02 group14-optiplex-7010 sshd[21870]: Received SIGHUP; restarting.
Dis 17 08:58:02 group14-optiplex-7010 systemd[1]: Reloaded OpenBSD Secure Shell
Dis 17 08:58:02 group14-optiplex-7010 sshd[21870]: Server listening on 0.0.0.0 p
Dis 17 08:58:02 group14-optiplex-7010 sshd[21870]: Server listening on :: port 2
Dis 17 08:58:04 group14-optiplex-7010 systemd[1]: Reloading OpenBSD Secure Shell
Dis 17 08:58:04 group14-optiplex-7010 sshd[21870]: Received SIGHUP; restarting.
Dis 17 08:58:04 group14-optiplex-7010 systemd[1]: Reloaded OpenBSD Secure Shell
Dis 17 08:58:04 group14-optiplex-7010 sshd[21870]: Server listening on 0.0.0.0 p
Dis 17 08:58:04 group14-optiplex-7010 sshd[21870]: Server listening on :: port 2
lines 1-21 (END)
```

Figure 5.333: Check the status of the SSH

### 5.3.25.3 Configuration SSH in Debian

**Step 1:** Open Terminal in Debian.

**Step 2:** Change User to root.

```
group14@group14:~$ su  
Password:  
root@group14:/home/group14#
```

Figure 5.334: Change user to root

**Step 3:** Install SSH using command as shown below.

```
root@group14:/home/group14# sudo apt install -y openssh-server  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
The following additional packages will be installed:  
  openssh-sftp-server  
Suggested packages:  
  molly-guard monkeysphere rssh ufw  
The following NEW packages will be installed:  
  openssh-server openssh-sftp-server  
0 upgraded, 2 newly installed, 0 to remove and 66 not upgraded.  
Need to get 396 kB of archives.  
After this operation, 1,609 kB of additional disk space will be used.  
Get:1 http://deb.debian.org/debian buster/main amd64 openssh-sftp-server a  
md64 1:7.9p1-10+deb10u1 [44.6 kB]  
Get:2 http://deb.debian.org/debian buster/main amd64 openssh-server amd64  
1:7.9p1-10+deb10u1 [352 kB]  
Fetched 396 kB in 1s (292 kB/s)  
Preconfiguring packages ...  
Selecting previously unselected package openssh-sftp-server.  
(Reading database ... 357710 files and directories currently installed.)  
Preparing to unpack .../openssh-sftp-server_1%3a7.9p1-10+deb10u1_amd64.deb  
...
```

Figure 5.335: SSH command to install

**Step 4:** After finished the installation, start the SSH service.

```
root@group14:/home/group14# sudo systemctl start ssh  
root@group14:/home/group14#
```

Figure 5.336: Start the SSH Service

**Step 5:** Then, checked the status of SSH service. If the status is active, that's mean that the SSH is already start.

```
root@group14:/home/group14# sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
  Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset:
    Active: active (running) since Tue 2019-12-17 08:52:35 +08; 3min 25s ag
      Docs: man:sshd(8)
             man:sshd config(5)
   Main PID: 8319 (sshd)
     Tasks: 1 (limit: 4915)
    Memory: 1.2M
      CGroup: /system.slice/ssh.service
              └─8319 /usr/sbin/sshd -D

Dec 17 08:52:35 group14 systemd[1]: Starting OpenBSD Secure Shell server..
Dec 17 08:52:35 group14 sshd[8319]: Server listening on 0.0.0.0 port 22.
Dec 17 08:52:35 group14 sshd[8319]: Server listening on :: port 22.
Dec 17 08:52:35 group14 systemd[1]: Started OpenBSD Secure Shell server.
Lines 1-15/15 (END)
```

Figure 5.337: Check the status of SSH service

### 5.3.26 MEDIA SERVER

**Step 1:** Download the installer of Plex media server.

```
group14@group14:~$ sudo bash
[sudo] password for group14:
root@group14:~# wget https://downloads.plex.tv/plex-media-server/1.14.1.5488-cc2
60c476/plexmediaserver_1.14.1.5488-cc260c476_amd64.deb
--2019-12-19 08:24:48-- https://downloads.plex.tv/plex-media-server/1.14.1.5488-
_cc260c476/plexmediaserver_1.14.1.5488-cc260c476_amd64.deb
Resolving downloads.plex.tv (downloads.plex.tv)... 104.18.156.41, 104.18.157.41,
2606:4700::6812:9c29, ...
Connecting to downloads.plex.tv (downloads.plex.tv)|104.18.156.41|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 105175642 (100M) [application/octet-stream]
Saving to: 'plexmediaserver_1.14.1.5488-cc260c476_amd64.deb'

    plexm 37%[=====]>                                ] 37.11M 2.87MB/s eta 25s  □
```

Figure 5.338: Downloading of Plex media sever installer .

**Step 2:** Install the Plex media server using command below.

```
root@group14:~# sudo dpkg -i plexmediaserver*.deb
dpkg: warning: downgrading plexmediaserver from 1.18.2.2058-e67a4e892 to 1.14.1.
5488-cc260c476
(Reading database ... 194397 files and directories currently installed.)
Preparing to unpack plexmediaserver_1.14.1.5488-cc260c476_amd64.deb ...
Removed /etc/systemd/system/multi-user.target.wants/plexmediaserver.service.
Unpacking plexmediaserver (1.14.1.5488-cc260c476) over (1.18.2.2058-e67a4e892) .
..
Setting up plexmediaserver (1.14.1.5488-cc260c476) ...
Installing new version of config file /etc/init/plexmediaserver.conf ...
Created symlink /etc/systemd/system/multi-user.target.wants/plexmediaserver.servic
ice → /lib/systemd/system/plexmediaserver.service.
Processing triggers for libc-bin (2.27-3ubuntu1) ...
Processing triggers for systemd (237-3ubuntu10.33) ...
Processing triggers for ureadahead (0.100.0-21) ...
Processing triggers for gnome-menus (3.13.3-11ubuntu1.1) ...
Processing triggers for desktop-file-utils (0.23-1ubuntu3.18.04.2) ...
Processing triggers for mime-support (3.60ubuntu1) ...
```

Figure 5.339: Installation of Plex media server.

**Step 3:** Enable Plex Media Server to start on reboot, and then start the server.

```
root@group14:~# sudo systemctl enable plexmediaserver.service
root@group14:~# sudo systemctl start plexmediaserver.service
```

Figure 5.340: Enable and start Plex media server.

**Step 4:** Enter `http://localhost:32400/web` into the browser to view the Plex web interface, as shown below.



*Figure 5.341: Plex web interface.*

### 5.3.27 ROUTER HARDENING

**Step 1:** Open PuTTY Configuration and login with username “Group14”, then enter password.

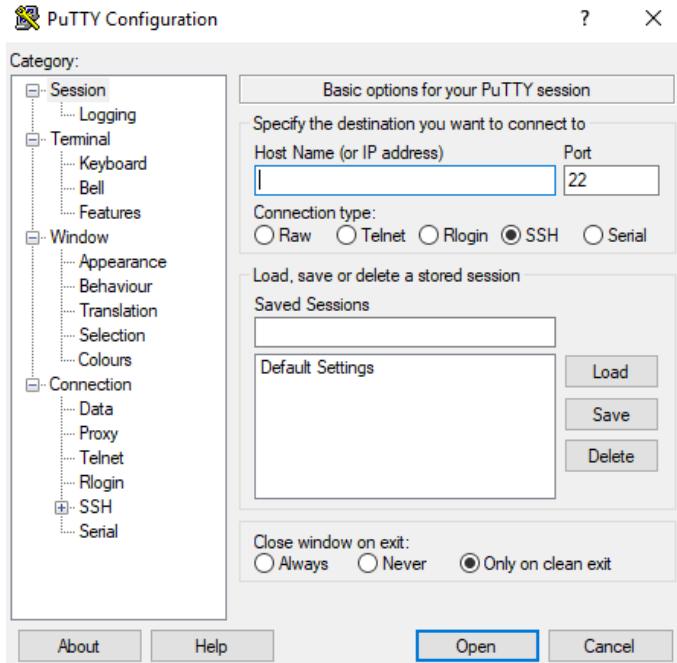


Figure 5.342: Putty Login

**Step 2:** Get into terminal and type “banner motd \*” to enter login banner.

```
G14Router>en
G14Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
G14Router(config)#banner motd *
Enter TEXT message. End with the character '*'.
#####
#      WELCOME TO WORKSHOP 2      #
#
#          GROUP 14          #
#
#  UNAUTHORIZED USER IS PROHIBITED  #
#####
*
G14Router(config)#

```

Figure 5.343: Banner motd

#### Disable log to console or monitor sessions

It is always advised to send logging information to the local log buffer, which can be viewed with the show logging command rather than to send log messages to monitor

and console sessions. The monitor and console sessions are interactive management sessions and it can elevate the CPU load of router.

**Step 1:** Type “show log” to show system log.

```
Enter TEXT message, End with CNTL/Z.
#####
#      WELCOME TO WORKSHOP 2      #
#
#      GROUP 14      #
#
#  UNAUTHORIZED USER IS PROHIBITED  #
#####
*
G14Router(config)#
G14Router(config)#exit
G14Router#
*Dec 11 14:27:29.005: %SYS-5-CONFIG_I: Configured from console by admin on conso
le
G14Router#show log
Syslog logging: enabled (0 messages dropped, 3 messages rate-limited, 0 flushes,
0 overruns, xml disabled, filtering disabled)

No Active Message Discriminator.

No Inactive Message Discriminator.

Console logging: level debugging, 11502 messages logged, xml disabled,
filtering disabled
Monitor logging: level debugging, 0 messages logged, xml disabled,
filtering disabled
Buffer logging: level debugging, 11502 messages logged, xml disabled,
```

Figure 5.344: System Log

**Step 2:** Then get into configuration and type “no logging console” and “no logging monitor” to disable console and monitor logs.

```
G14Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
G14Router(config)#
G14Router(config)#no logging console
G14Router(config)#no logging monitor
G14Router(config)#exit
G14Router#show log
Syslog logging: enabled (0 messages dropped, 3 messages rate-limited, 0 flushes,
0 overruns, xml disabled, filtering disabled)

No Active Message Discriminator.

No Inactive Message Discriminator.

Console logging: disabled
Monitor logging: disabled
Buffer logging: level debugging, 11505 messages logged, xml disabled,
filtering disabled
Exception Logging: size (4096 bytes)
```

Figure 5.345: Disable console and monitor logs

### 5.3.25.5 Enable configuration change notification and logging

To send notification of configuration changes to the software system logging (syslog) process. Syslog notifications allow monitoring of the configuration log information without performing polling and information gathering tasks. Then, it allows the tracking of configuration changes entered by users on a per-session and per-user basis. This tool allows administrators to track any configuration change made to the software running configuration, and identify the user that made that change.

**Step 1:** Get into PuTTY configuration and enter following commands.

```
G14Router#  
G14Router#config t  
Enter configuration commands, one per line. End with CNTL/Z.  
G14Router(config)#archive  
G14Router(config-archive)#log config  
G14Router(config-archive-log-cfg)#logging enable  
G14Router(config-archive-log-cfg)#logging size 300  
G14Router(config-archive-log-cfg)#hidekeys  
G14Router(config-archive-log-cfg)#notify syslog  
          ^  
% Invalid input detected at '^' marker.  
  
G14Router(config-archive-log-cfg)#notify syslog  
G14Router(config-archive-log-cfg)#end
```

Figure 5.346: Enable syslog

**Step 2:** Then type “**show archive log config 1 5**” to show archive from line 1 to line 5.

```
G14Router(config-archive-log-cfg)#notify syslog  
G14Router(config-archive-log-cfg)#end  
G14Router#  
G14Router#show archive log config 1 2  
idx sess      user@line      Logged command  
  1   1        admin@console | logging enable  
  2   1        admin@console | logging size 300  
  
G14Router#show archive log config 1 5  
idx sess      user@line      Logged command  
  1   1        admin@console | logging enable  
  2   1        admin@console | logging size 300  
  3   1        admin@console | hidekeys  
  4   1        admin@console | notify syslog  
  
G14Router#show archive log config all provisioning  
archive  
  log config  
    logging enable  
    logging size 300  
    hidekeys  
    notify syslog  
  
G14Router#
```

Figure 5.347: Show Archive log config

### 5.2.29 Configure Intervlan in Vlan 10,20, and 30.

Step 1: Create Vlan in switch.

```
G14_switch(config)#vlan 10
G14_switch(config-vlan)#name Server
G14_switch(config-vlan)#vlan 20
G14_switch(config-vlan)#name Client
G14_switch(config-vlan)#vlan 30
G14_switch(config-vlan)#name Guess
G14_switch(config-vlan)#exit
G14_switch(config)#do show vlan
```

*Figure 5.348: Assign VLAN in switch*

Step 2: Assign ports in every VLANs in switch.

```
G14_switch#
G14_switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
G14_switch(config)#int range fa0/1 - 3
G14_switch(config-if-range)#switchport mode access
G14_switch(config-if-range)#switchport access vlan 10
G14_switch(config-if-range)#no shut
G14_switch(config-if-range)#int range fa0/4 - 12
G14_switch(config-if-range)#switchport mode access
G14_switch(config-if-range)#switchport access vlan 20
G14_switch(config-if-range)#no shut
G14_switch(config-if-range)#int range fa0/13 - 20
G14_switch(config-if-range)#switchport mode access
G14_switch(config-if-range)#switchport access vlan 30
G14_switch(config-if-range)#no shut
```

*Figure 5.349: Assigns port in switch*

Step 3: Configure default getaway in each VLANs in router.

```

G14Router(config-if)#int f0/0.10
G14Router(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.10, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.10,
changed state to up

G14Router(config-subif)#encapsulation dot1Q 10
G14Router(config-subif)#ip add 192.168.14.177 255.255.255.192
G14Router(config-subif)#exit
G14Router(config)#int fa0/0.20
G14Router(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.20, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.20,
changed state to up

G14Router(config-subif)#encapsulation dot1Q 20
G14Router(config-subif)#ip add 192.168.14.1 255.255.255.192
G14Router(config-subif)#exit

```

*Figure 5.350: Configure default gateway*

Step 4: Configure trunk in switch using ports 24.

```

G14_switch(config)#int fa0/24
G14_switch(config-if)#switchport trunk allowed vlan all
G14_switch(config-if)#switchport mode trunk
G14_switch(config-if)#exit

```

*Figure 5.351: Configure trunk*

## CHAPTER 6 – TESTING

### 6.1 INTRODUCTION

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

### 6.2 SERVICES TESTING

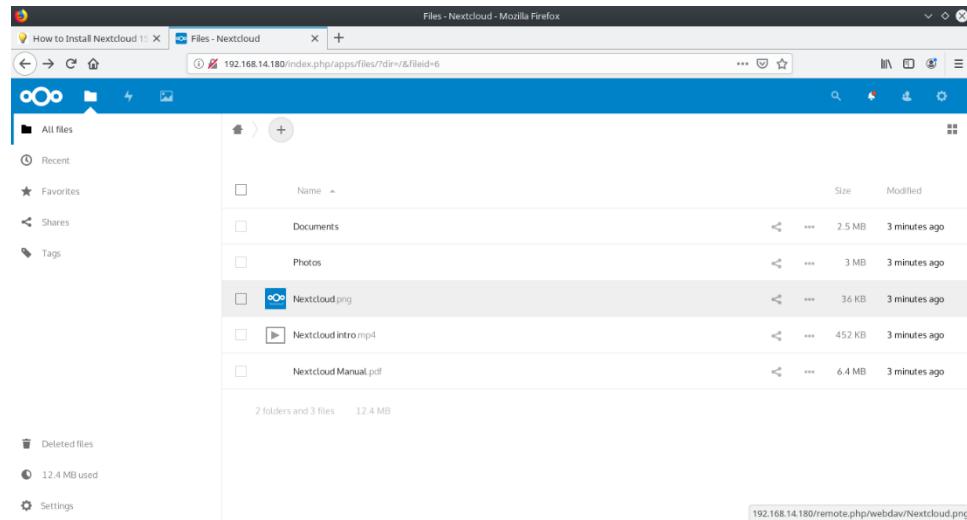
#### 6.2.1 CLOUD SERVER

**STEP 1:** Access NextCloud via 192.168.14.180.com



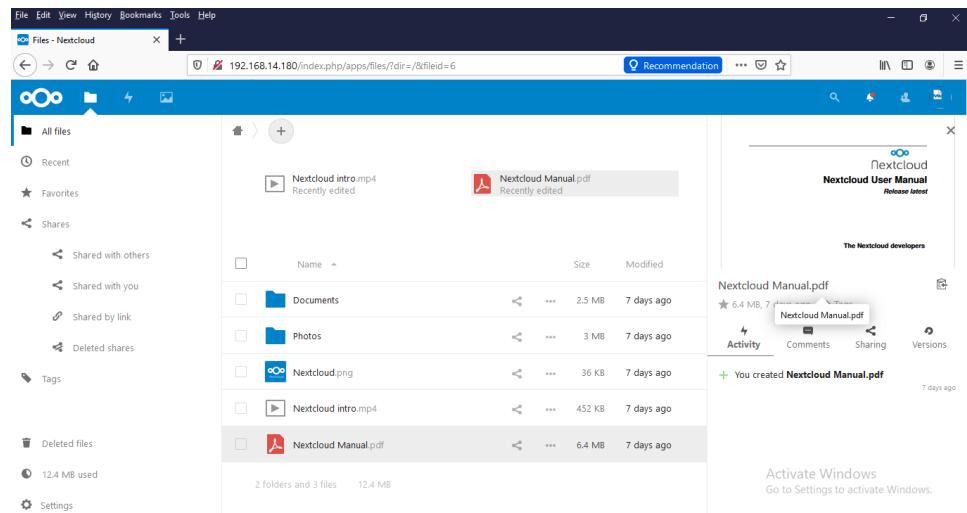
*Figure 6. 1: Login to NextClouD*

**STEP 2:** Login using previously created user and a Home page will be displayed.



*Figure 6. 2: Homepage after login*

### STEP 3: Access from another host in the network.



*Figure 6.3: Access NextCloud from Windows Server*

## 6.2.2 DHCP IPv4 & IPv6

### 6.2.2.1 IPV4 TESTING

STEP 1: Successfully to connect to ws14.

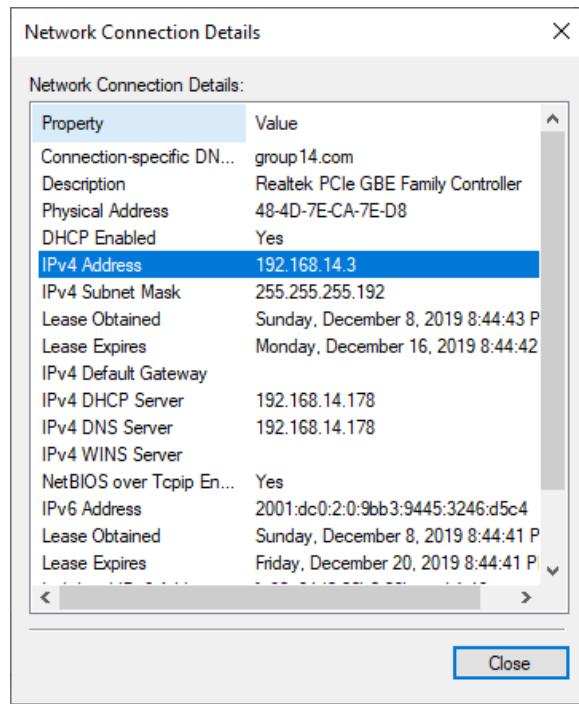


Figure 6.4: IPV4 in Client's PC

STEP 2: Ping from Client to Windows Server.

```
C:\Users\aa>ping 192.168.14.178
Pinging 192.168.14.178 with 32 bytes of data:
Reply from 192.168.14.178: bytes=32 time=1ms TTL=127

Ping statistics for 192.168.14.178:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
C:\Users\aa>
```

Figure 6. 5: Ping from Client to Server IPV4

### 6.2.2.2 IPv6 TESTING

**STEP 1:** Successfully connect to ws14.

Client IPv6 Address	Name	Lease Expiration	IAID	Type	Unique ID	Description
2001:dc0:2:0:9bb...	DESKTOP-007BIRK	12/19/2019 10:28:26 PM	105401726	IANA	000100012...	

```
C:\Users\a>ipconfig

Windows IP Configuration

Unknown adapter VPN - VPN Client:
  Connection-specific DNS Suffix  . : group14.com
  Link-local IPv6 Address . . . . . : fe80::9104:c05:86f:8dab%24
  IPv4 Address. . . . . : 192.168.30.11
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 192.168.30.1

Ethernet adapter Ethernet:
  Connection-specific DNS Suffix  . : group14.com
  IPv6 Address . . . . . : 2001:dc0:2:0:9bb3:9445:3246:d5c4
  Link-local IPv6 Address . . . . . : fe80::91d2:20b0:29b:aeab%13
  IPv4 Address. . . . . : 192.168.14.3
  Subnet Mask . . . . . : 255.255.255.192
  Default Gateway . . . . . : fe80::281:c4ff:fe38:c9a0%13
```

Figure 6. 6 Client connect to DNS

**STEP 2:** Ping from Client to Windows Server.

```
C:\Users\a>ping 2001:dc0:1::3

Pinging 2001:dc0:1::3 with 32 bytes of data:
Reply from 2001:dc0:1::3: time=1ms
Reply from 2001:dc0:1::3: time=1ms
Reply from 2001:dc0:1::3: time=1ms
Reply from 2001:dc0:1::3: time=1ms

Ping statistics for 2001:dc0:1::3:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
  Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

Figure 6. 7 Ping from Client to Windows Server IPV

## 6.2.3 DYNAMIC ROUTING & NAT

### 6.2.3.1 DYNAMIC ROUTING

**STEP 1:** Run command “*show ip ospf neighbour*” in Router.

```
G14Router#show ip ospf neighbor  
  
Neighbor ID      Pri   State        Dead Time     Address          Interface  
1.1.1.1          0     FULL/ -      00:00:32    200.200.200.1  Serial0/0/0
```

Figure 6. 8 OSPF Neighbor

### 6.2.3.2 NAT

**STEP 2:** Show mapping inside global/local and outside global/local by using command “*show ip nat translation*”.

```
G14Router#show ip nat translations  
Pro Inside global      Inside local      Outside local      Outside global  
icmp 200.200.200.4:1  192.168.14.178:1  192.168.1.48:1  192.168.1.48:1  
5  
udp 200.200.200.4:53  192.168.14.178:53  200.200.200.3:49535  200.200.200.3:4953  
1  
5  
udp 200.200.200.4:53  192.168.14.178:53  200.200.200.3:50011  200.200.200.3:5001  
1  
4  
udp 200.200.200.4:53  192.168.14.178:53  200.200.200.3:50294  200.200.200.3:5029  
4  
4  
udp 200.200.200.4:53  192.168.14.178:53  200.200.200.3:50384  200.200.200.3:5038  
2  
5  
udp 200.200.200.4:53  192.168.14.178:53  200.200.200.3:50632  200.200.200.3:5063  
5  
5  
udp 200.200.200.4:53  192.168.14.178:53  200.200.200.3:50645  200.200.200.3:5064  
6  
5  
udp 200.200.200.4:53  192.168.14.178:53  200.200.200.3:50686  200.200.200.3:5068  
5  
5
```

Figure 6. 9 IP NAT translations

**STEP 2:** Testing connection by ping public ip neighbour using command “ping”.

```
C:\Users\Administrator.PC-GROUP14.000>ping 200.200.200.3  
  
Pinging 200.200.200.3 with 32 bytes of data:  
Reply from 200.200.200.3: bytes=32 time=3ms TTL=126  
Reply from 200.200.200.3: bytes=32 time=3ms TTL=126  
Reply from 200.200.200.3: bytes=32 time=2ms TTL=126  
Reply from 200.200.200.3: bytes=32 time=3ms TTL=126  
  
Ping statistics for 200.200.200.3:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
    Approximate round trip times in milli-seconds:  
        Minimum = 2ms, Maximum = 3ms, Average = 2ms
```

Figure 6. 10 Ping IP Public Neighbor

## 6.2.4 IPSEC SITE TO SITE TUNNELING

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

```

G14Router#show crypto ipsec sa

interface: Serial0/0/0
    Crypto map tag: CMAP, local addr 200.200.200.2

    protected vrf: (none)
    local ident (addr/mask/prot/port): (192.168.14.176/255.255.255.240/0/0)
    remote ident (addr/mask/prot/port): (192.168.1.144/255.255.255.240/0/0)
    current_peer 200.200.200.1 port 500
        PERMIT, flags={origin_is_acl,}
        #pkts encaps: 45, #pkts encrypt: 45, #pkts digest: 45
        #pkts decaps: 45, #pkts decrypt: 45, #pkts verify: 45
        #pkts compressed: 0, #pkts decompressed: 0
        #pkts not compressed: 0, #pkts compr. failed: 0
        #pkts not decompressed: 0, #pkts decompress failed: 0
        #send errors 0, #recv errors 0

        local crypto endpt.: 200.200.200.2, remote crypto endpt.: 200.200.200.1
        plaintext mtu 1446, path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
        current outbound spi: 0xB6E8DB(3069163739)
        PFS (Y/N): N, DH group: none

        inbound esp sas:
            spi: 0x64D92076(1691951222)

--More-- █

```

*Figure 6. 11: Show crypto ipsec sa*

**STEP 2:** Show detailed information about the session

```

G14Router#show crypto session
Crypto session current status

Interface: Serial0/0/0
Session status: UP-ACTIVE
Peer: 200.200.200.1 port 500
    Session ID: 0
    IKEv1 SA: local 200.200.200.2/500 remote 200.200.200.1/500 Active
    IPSEC FLOW: permit ip 192.168.14.176/255.255.255.240 192.168.1.144/255.255.255.24
0
    Active SAs: 2, origin: crypto map

```

*Figure 6. 12: Show crypto session*

**STEP 3:** Ping to beside group router to our router

```

G14Router#ping 192.168.1.145 sou 192.168.14.177
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.145, timeout is 2 seconds:
Packet sent with a source address of 192.168.14.177
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

```

*Figure 6. 13: Ping 172.168.1.145 source 192.168.14.178*

**STEP 4:** Show that packets has been encrypt.

```

G14Router#show crypto ipsec sa

interface: Serial0/0/0
  Crypto map tag: CMAP, local addr 200.200.200.2

  protected vrf: (none)
  local  ident (addr/mask/prot/port): (192.168.14.176/255.255.255.240/0/0)
  remote ident (addr/mask/prot/port): (192.168.1.144/255.255.255.240/0/0)
  current_peer 200.200.200.1 port 500
    PERMIT, flags={origin_is_acl,}
    #pkts encaps: 45, #pkts encrypt: 45, #pkts digest: 45
    #pkts decaps: 45, #pkts decrypt: 45, #pkts verify: 45
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

    local crypto endpt.: 200.200.200.2, remote crypto endpt.: 200.200.200.1
    plaintext mtu 1446, path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
    current outbound spi: 0xB6E8DB(3069163739)
    PFS (Y/N): N, DH group: none

    inbound esp sas:
      spi: 0x64D92076(1691951222)

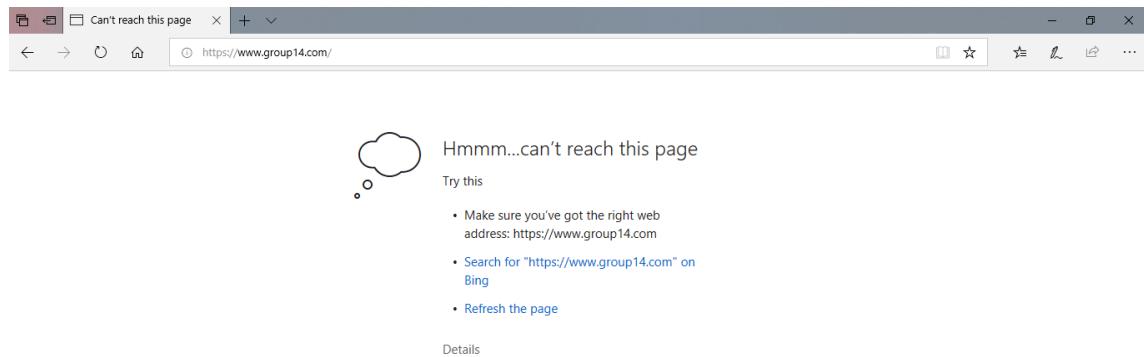
--More-- █

```

*Figure 6. 14: Show crypto ipsec sa*

## 6.2.6 ACCESS CONTROL LIST

**STEP 1:** Test the HTTPS using browser, it can't be opened the web server.



*Figure 6.15 HTTPS testing*

## STEP 2: Test the SFTP using browser, it can't be login from client

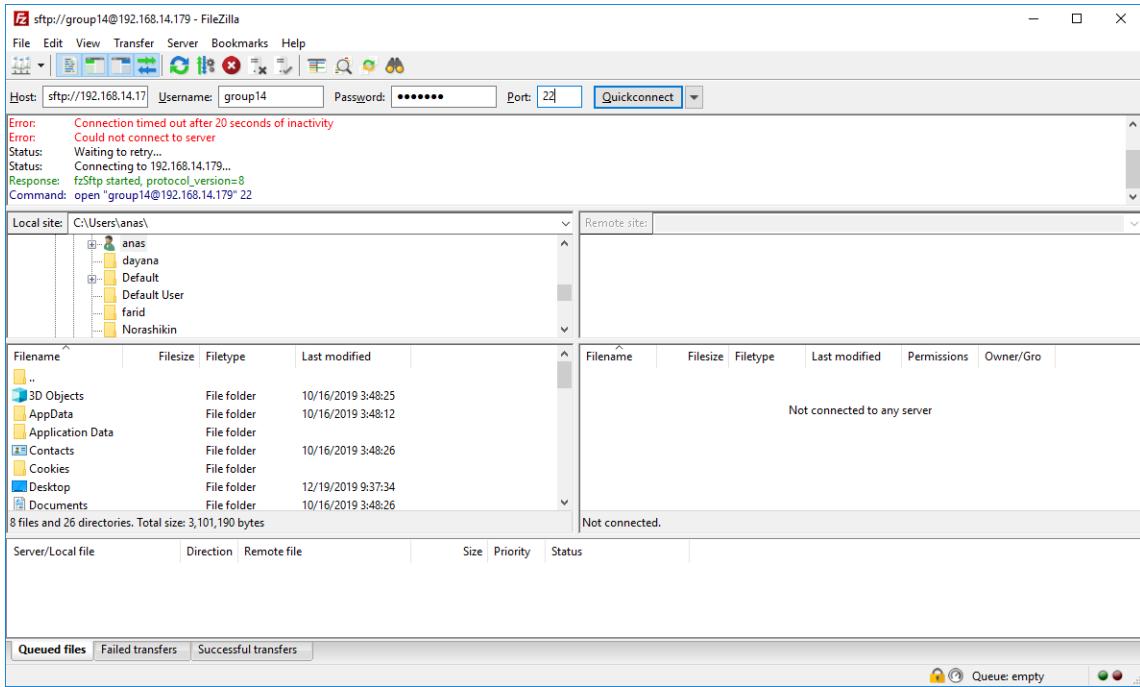


Figure 6. 16: SFTP testing

## STEP 3: Try to ping client to windows server, it can't be ping into windows server

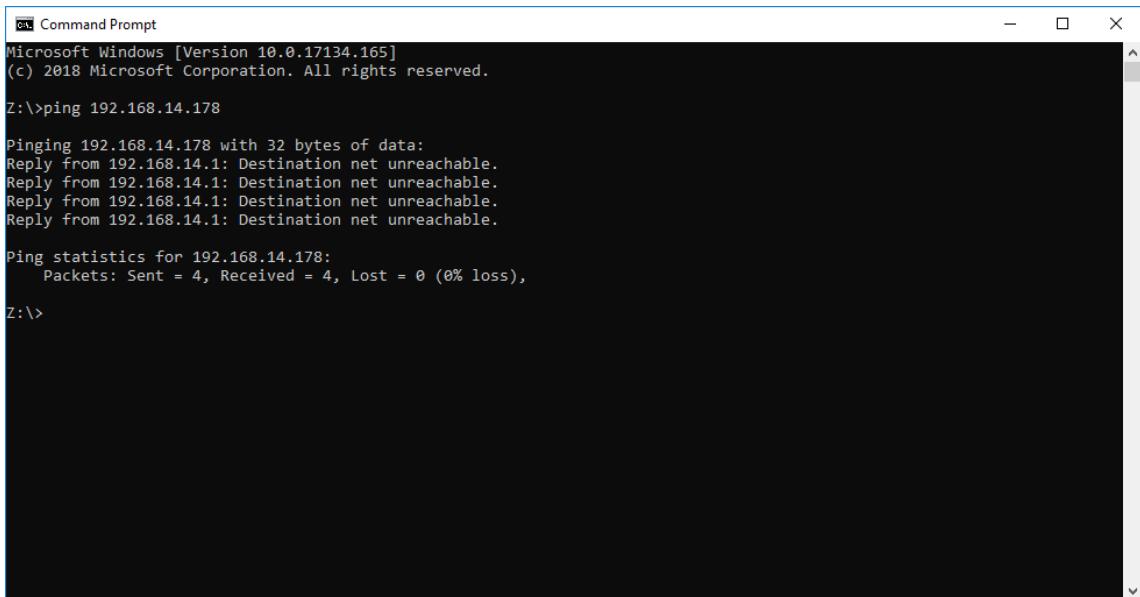
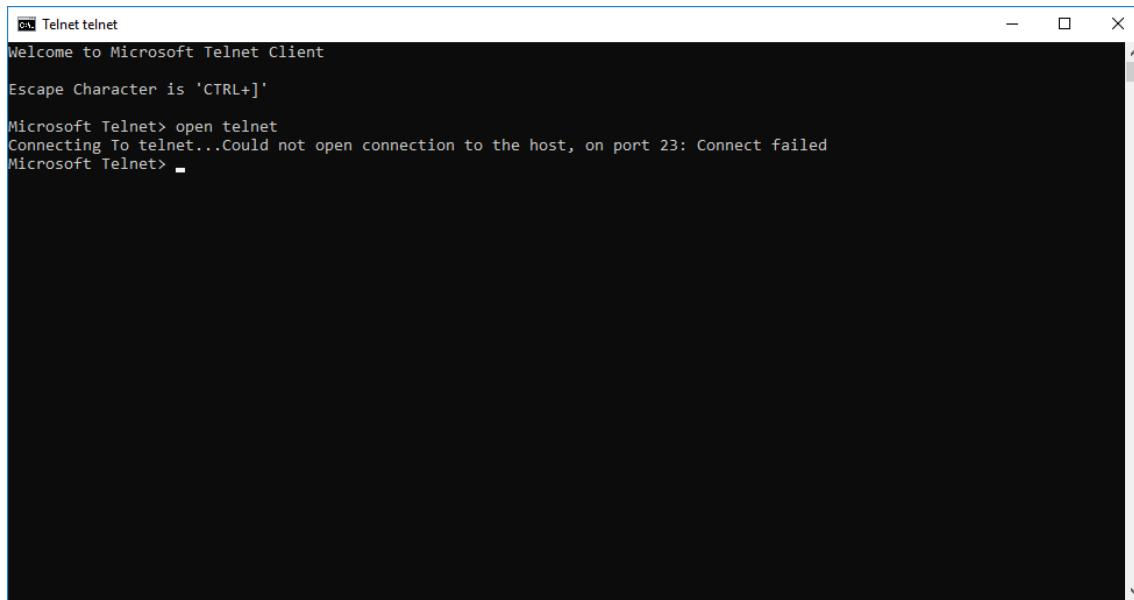


Figure 6. 17: PING testing

**STEP 4:** Try to remote windows server from client using telnet, it can't be remote.

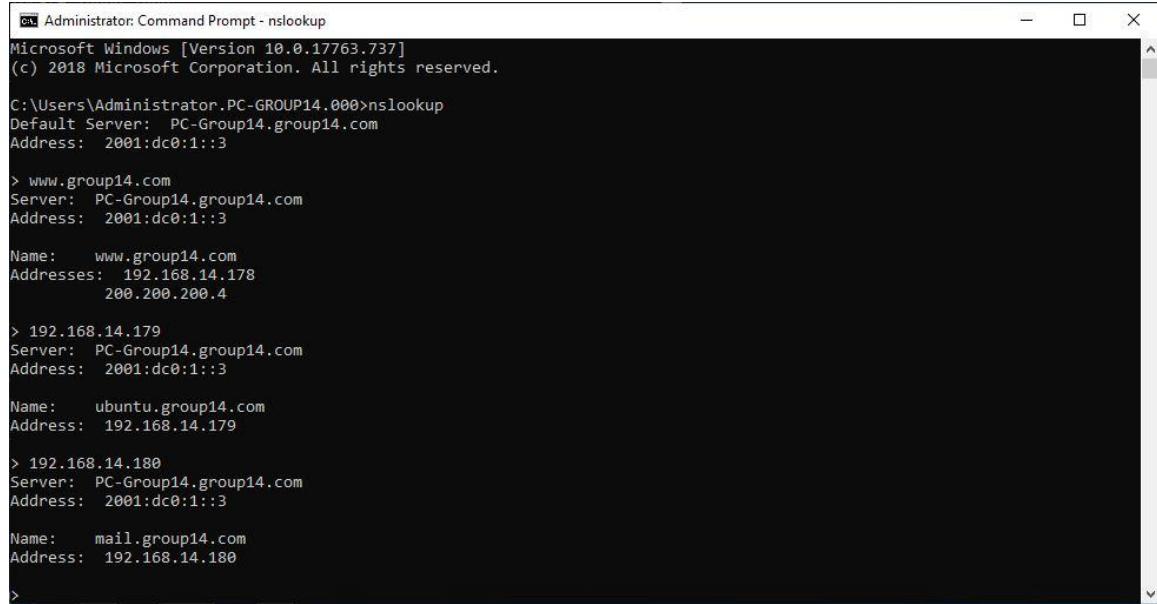


The screenshot shows a Microsoft Telnet window titled "Telnet telnet". It displays the following text:  
Welcome to Microsoft Telnet Client  
Escape Character is 'CTRL+]'  
Microsoft Telnet> open telnet  
Connecting To telnet...Could not open connection to the host, on port 23: Connect failed  
Microsoft Telnet> -

*Figure 6. 18: TELNET testing*

## 6.2.6 DOMAIN NAME SYSTEM

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



```
Administrator: Command Prompt - nslookup
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator.PC-GROUP14.000>nslookup
Default Server: PC-Group14.group14.com
Address: 2001:dc0:1::3

> www.group14.com
Server: PC-Group14.group14.com
Address: 2001:dc0:1::3

Name: www.group14.com
Addresses: 192.168.14.178
          200.200.200.4

> 192.168.14.179
Server: PC-Group14.group14.com
Address: 2001:dc0:1::3

Name: ubuntu.group14.com
Address: 192.168.14.179

> 192.168.14.180
Server: PC-Group14.group14.com
Address: 2001:dc0:1::3

Name: mail.group14.com
Address: 192.168.14.180

>
```

Figure 6. 19: Testing DNS

## 6.2.7 SERVER VIRTUALIZATION

**STEP 1:** Open Filezilla client in window server, insert the host ip address which is the virtual ip address, username and password. Next, click Quickconnect.

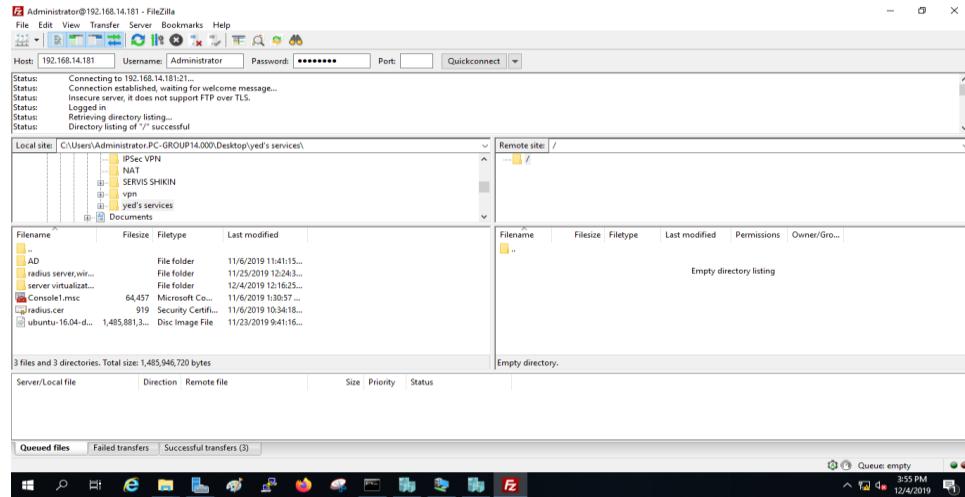


Figure 6. 20: FileZilla Administrator

**STEP 2 :** Now, drag one file from window server to virtual server

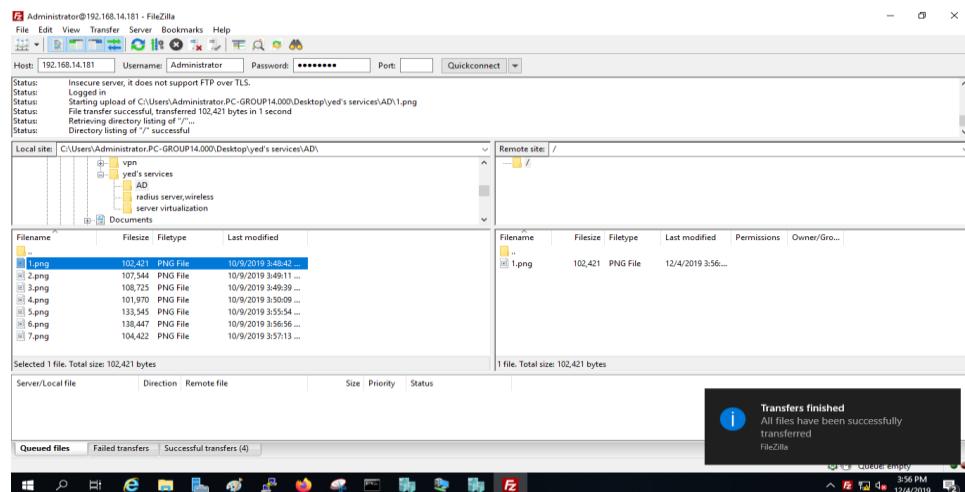


Figure 6. 21: File Sharing

**STEP 3 :** Check at the virtual machine whether the file successfully transfer or not.

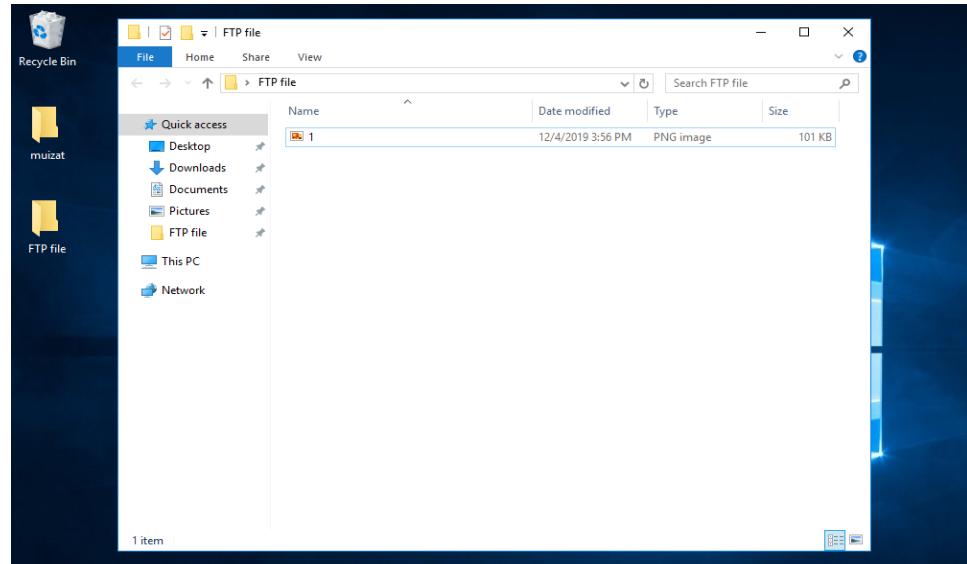


Figure 6. 22: FTP file for file sharing

**STEP 4 :** Then, create a text from virtual machine and share it to the window server.

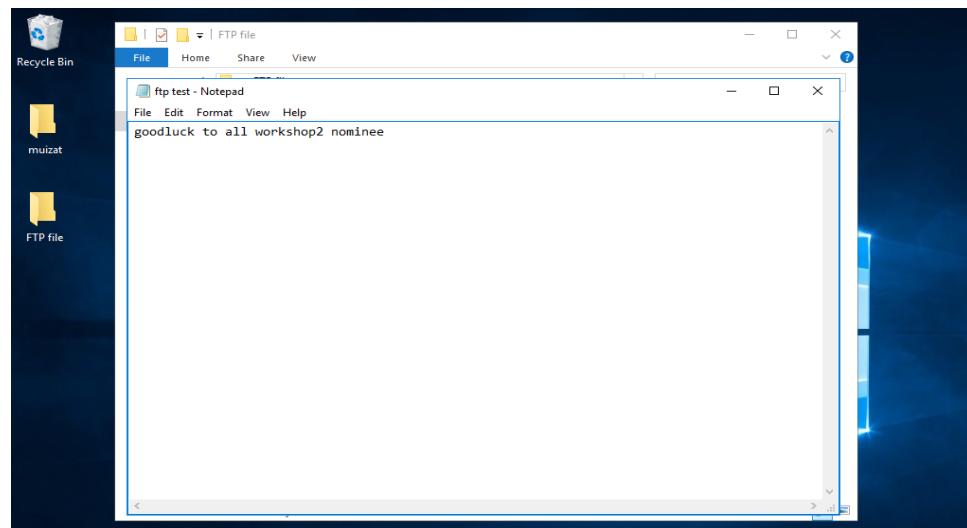


Figure 6. 23: Create a text in Notepad

**Step 5 :** Refresh the filezilla client in window server. The txt file will appear. Download that file.

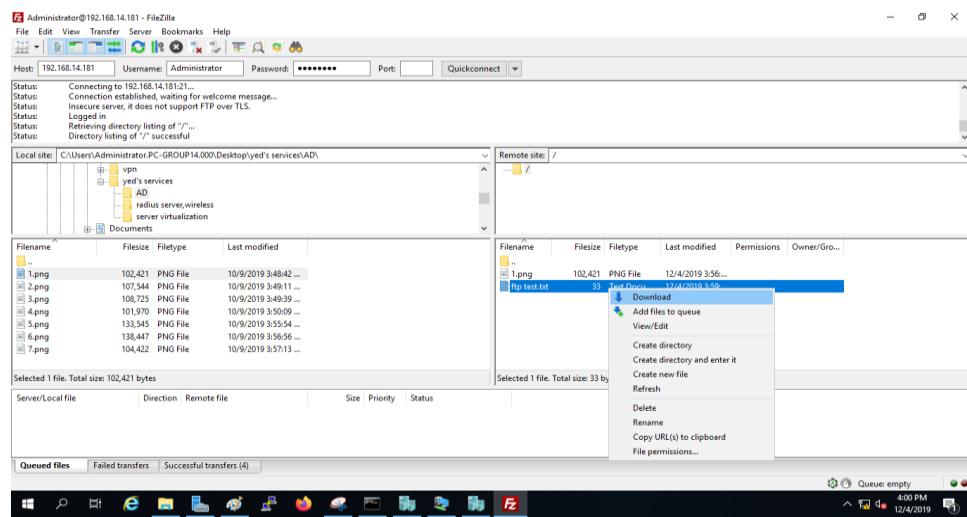


Figure 6. 24: Share TXT.File from virtual machine to window server

**Step 6 :** Open the txt.file and the text will appear. File sharing is success.

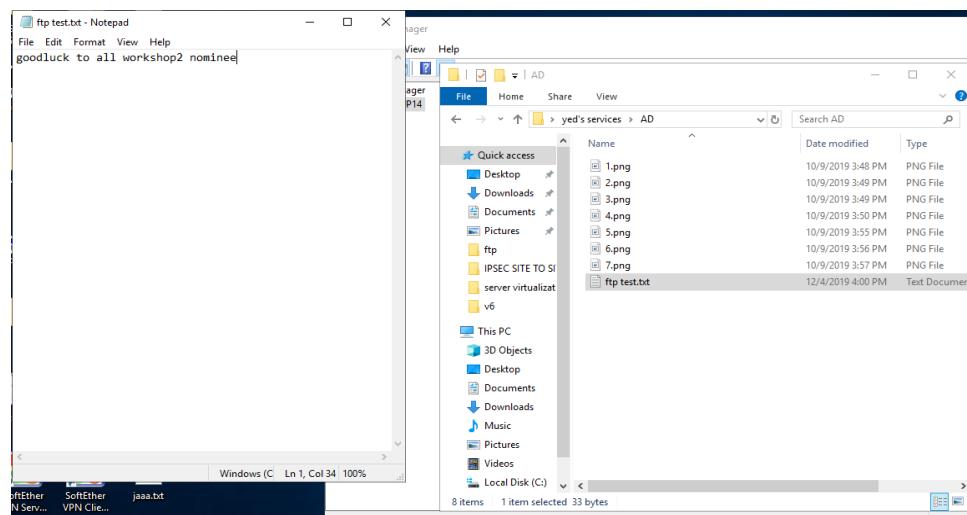


Figure 6. 25: TXT.file success sharing

## 6.2.8 ACTIVE DIRECTORY

**Step 1 :** At client, open the system properties and then click change. The system by default is in workgroup. So change it by choose the Domain and insert the root name. Then click ok.

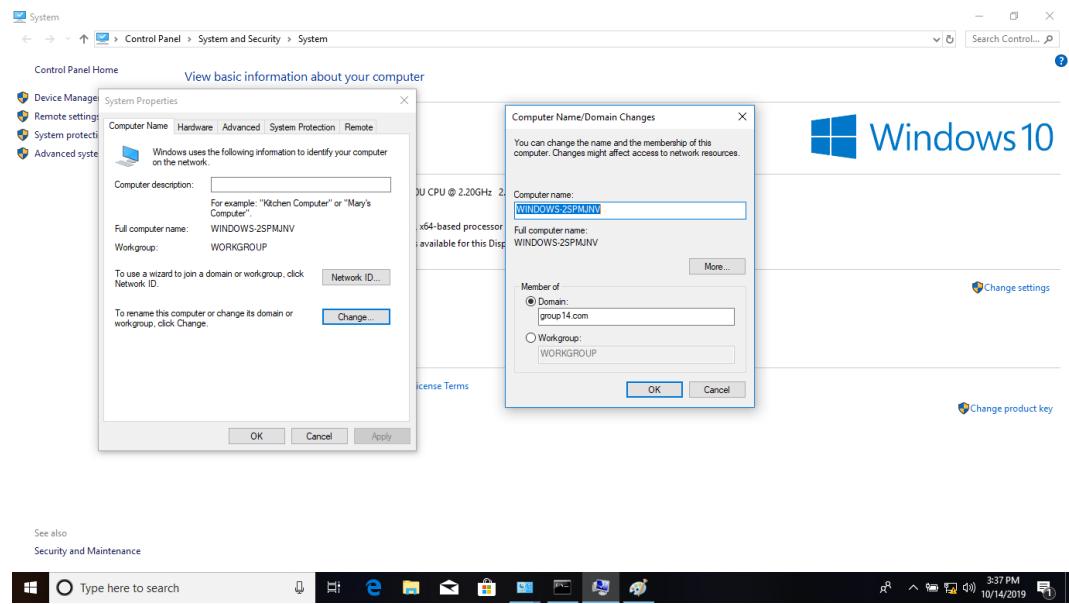


Figure 6. 26: Changes client to Domain

**Step 2 :** A username and password are require as a security purpose. Then, click ok.

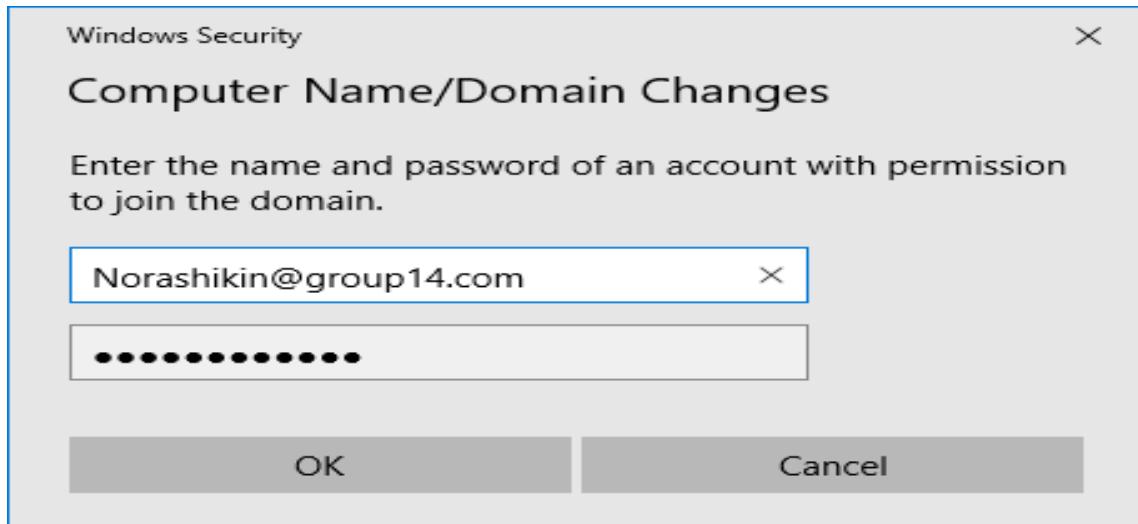


Figure 6. 27: Windows Security

**Step 3 :** To see whether the domain is success or not, a message will appear says that “Welcome to the group14.com domain”. After that, the system need to be restart in order to change it to domain.

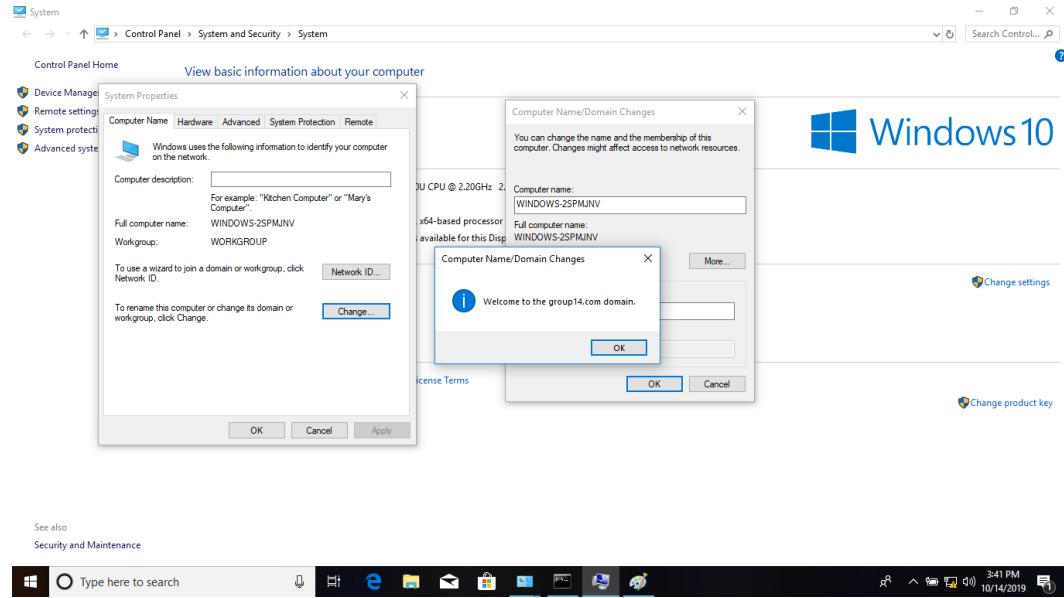


Figure 6. 28: Computer Name/Domain Changes

**Step 4 :** At pc client, enter the user as Anas. Before the policy enable, the recycle bin icon still there and can make changes in the desktop.



Figure 6. 29: Before The Policy is Enable

**Step 5 :** After the policy is enable by configure in the Group Policy Management Editor, the recycle bin icon will not appear and the user are not able to make any changes.

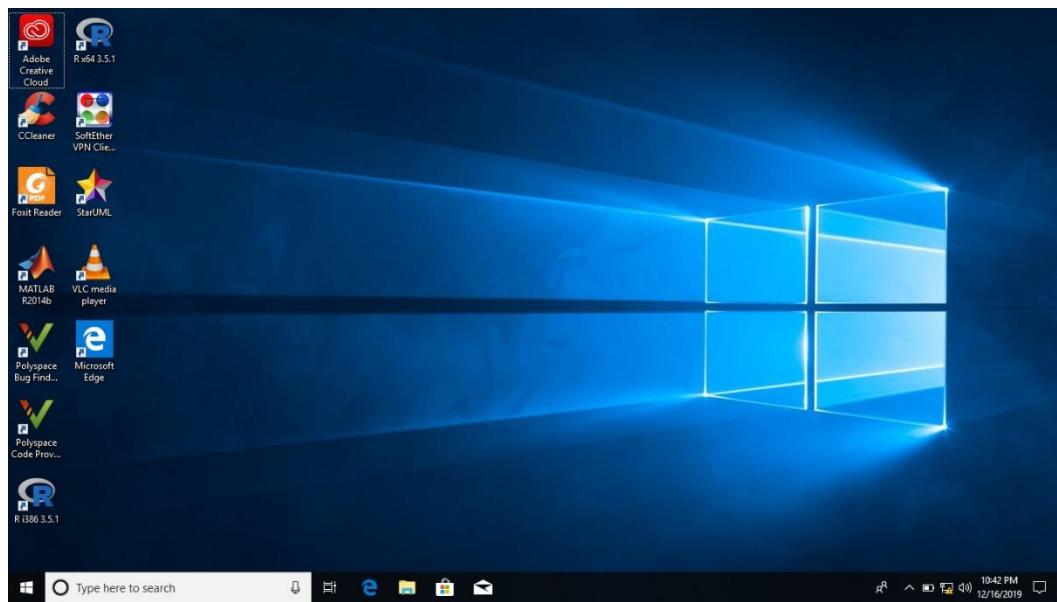


Figure 6. 30: After The Policy is Enable

## 6.2.9 WIRELESS USER AUTHENTICATION USING RADIUS SERVER

**Step 1 :** try ping IP address of the window server in the access point interface.

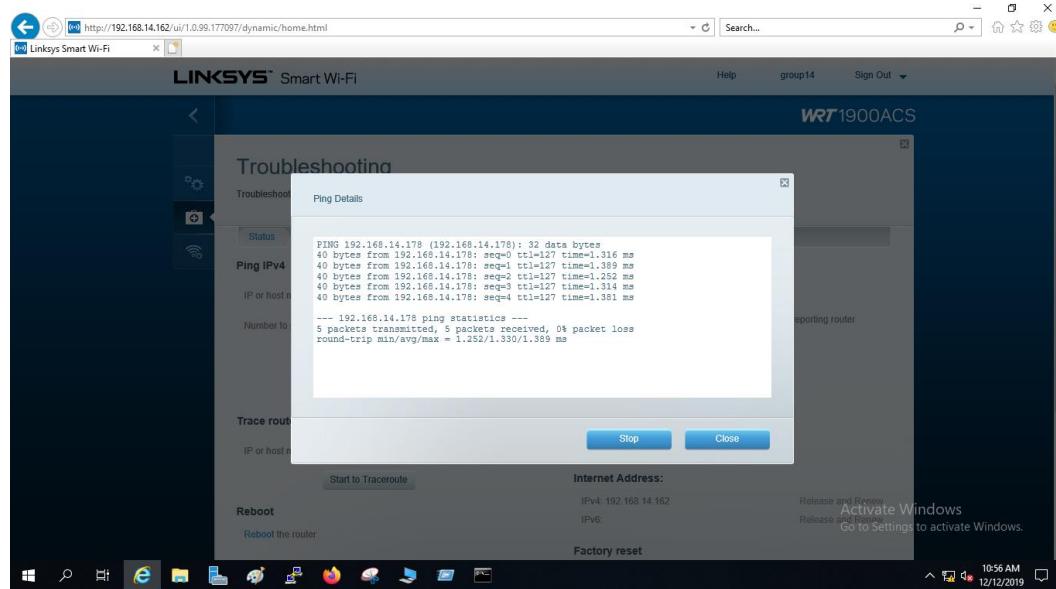


Figure 6. 31: Linksys Smart Wi-Fi Ping Details

**Step 2 :** try ping IP address of the access point in the command prompt of the window server.

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator.PC-GROUP14.000>ping 192.168.14.162

Pinging 192.168.14.162 with 32 bytes of data:
Reply from 192.168.14.162: bytes=32 time=1ms TTL=63

Ping statistics for 192.168.14.162:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\Users\Administrator.PC-GROUP14.000>
```

Figure 6. 32: Command Prompt Window Server

**Step 3 :** access the Wi-Fi group14 using AD user authentication from a smartphone.

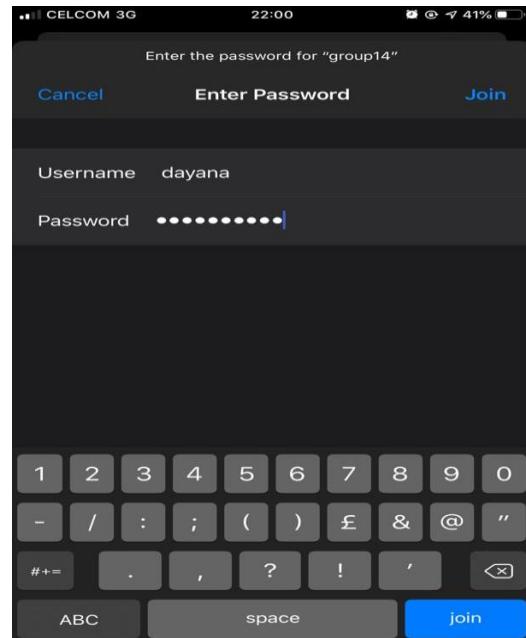


Figure 6. 33: group14 Wi-Fi

Step 4 : a certificate will pop out before access the connection.

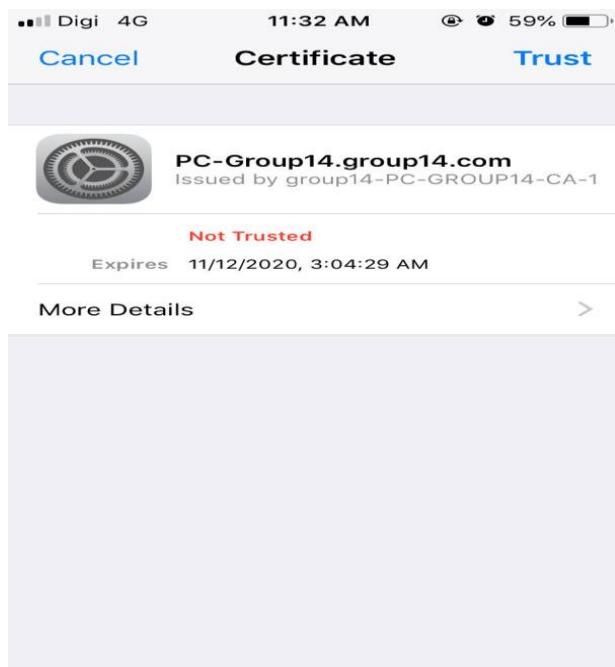


Figure 6. 34: Certificate

**Step 5 :** the connection can be access.



Figure 6. 35: Connected Group14 Wi-Fi

**Step 6 :** at laptop also can access the connection of the Wi-Fi.

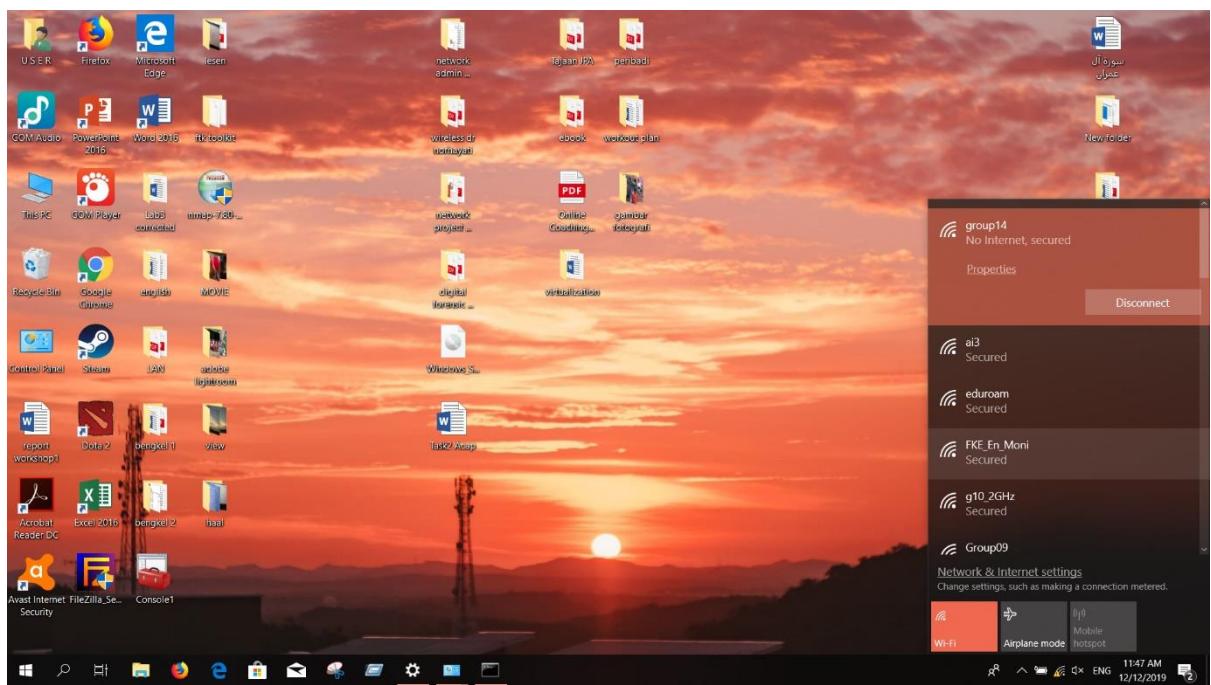


Figure 6. 36: Connected at laptop

**Step 7 :** check whether the devices connected to the access point or not by go the DHCP manager.

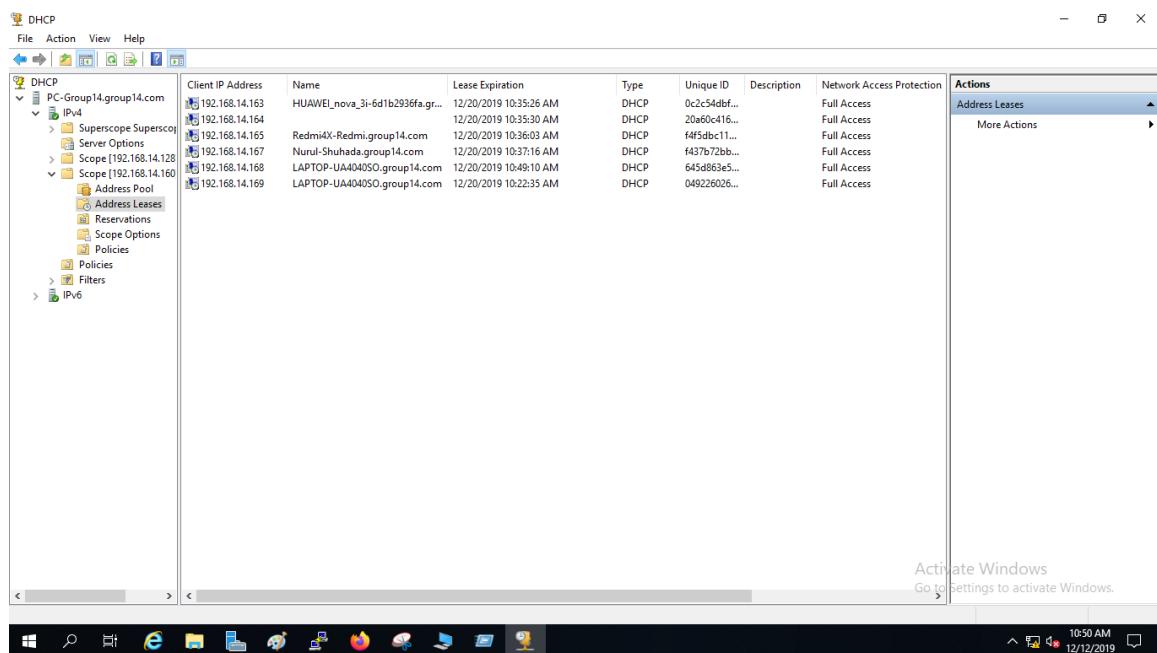


Figure 6. 37: DHCP Manager

## 6.2.10 LINUX EMAIL SERVER

### 6.2.10.1 Testing using Rainloop

Test the email function with send the message from user that create from Debian server account to another user in the server. From this project, the user that send the message is name haikal that on login account use ali@group14.com and the receiver is name abu@group14.com. Use the same password as need been set to the two user in the Debian server.

**STEP 1:** Send message from ali account send some massage to abu account.

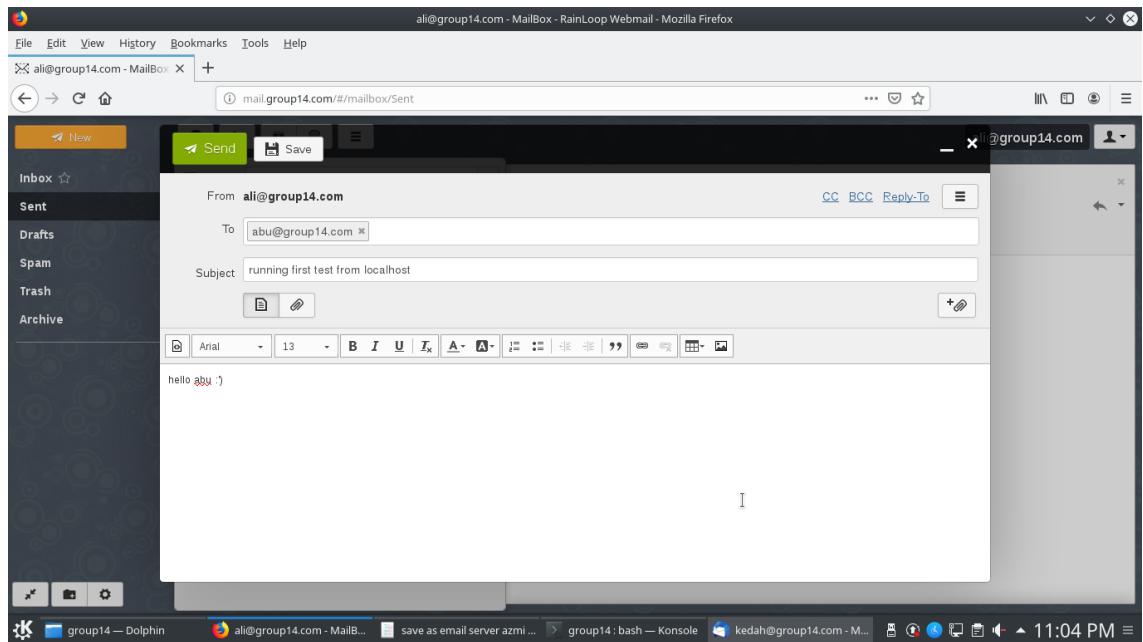


Figure 6. 38: Sending Message

**STEP 2:** Check sent box from ali to confirm the message was send.

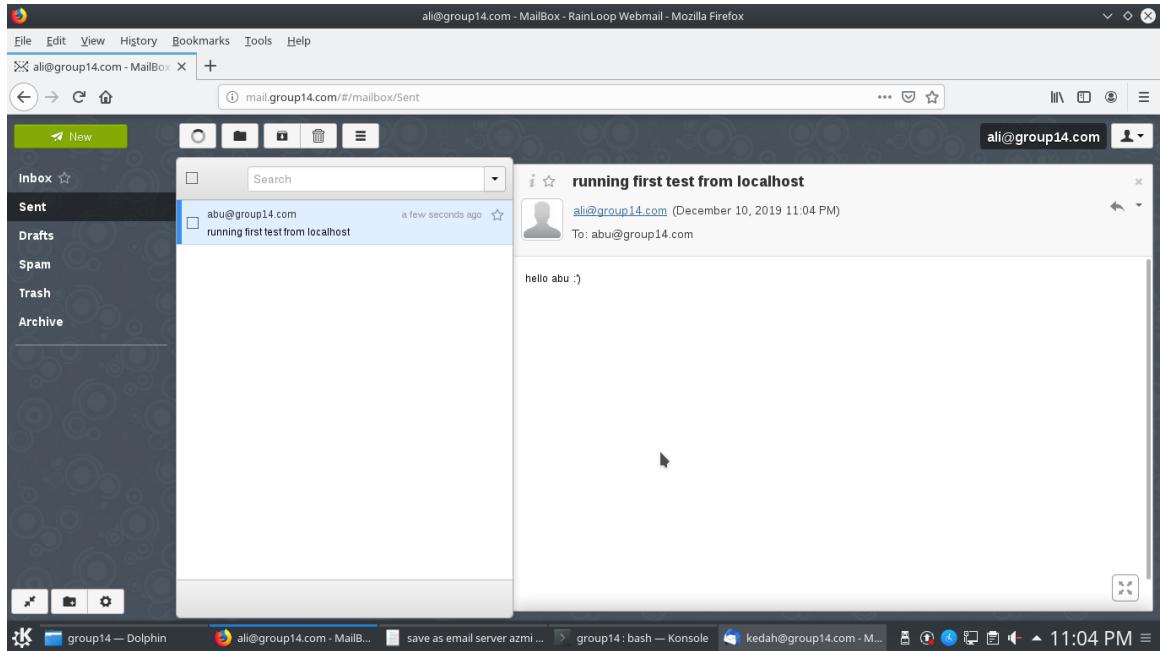


Figure 6. 39: Sent item

**STEP 3:** Check the email receive on abu account on mailbox. If the email receives as send from ali account than the testing success.

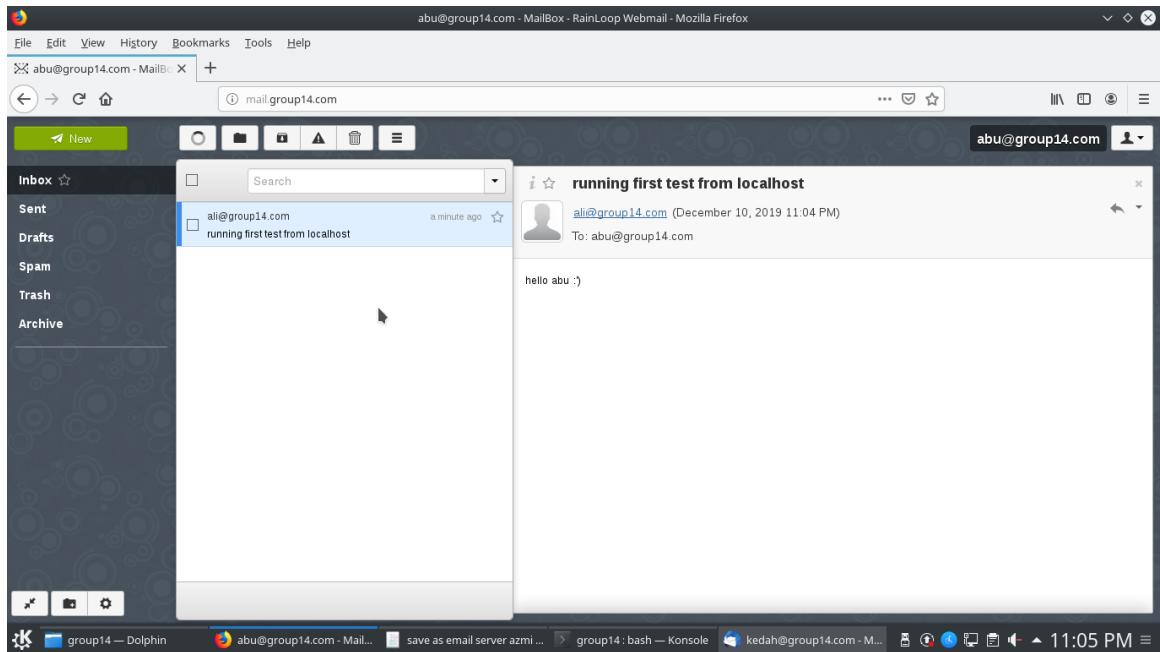


Figure 6. 40: Abu Inbox

## Testing using Thunderbird

Test the email function with send the message from user that create from Debian server account to another user in the windows server. From this project, the user that send the message is ali using ali@group14.com and the receiver is name abu using abu@group14.com. Use the same password as need been set to the two user in the Debian server.

### STEP 1: Login ali using thunderbird

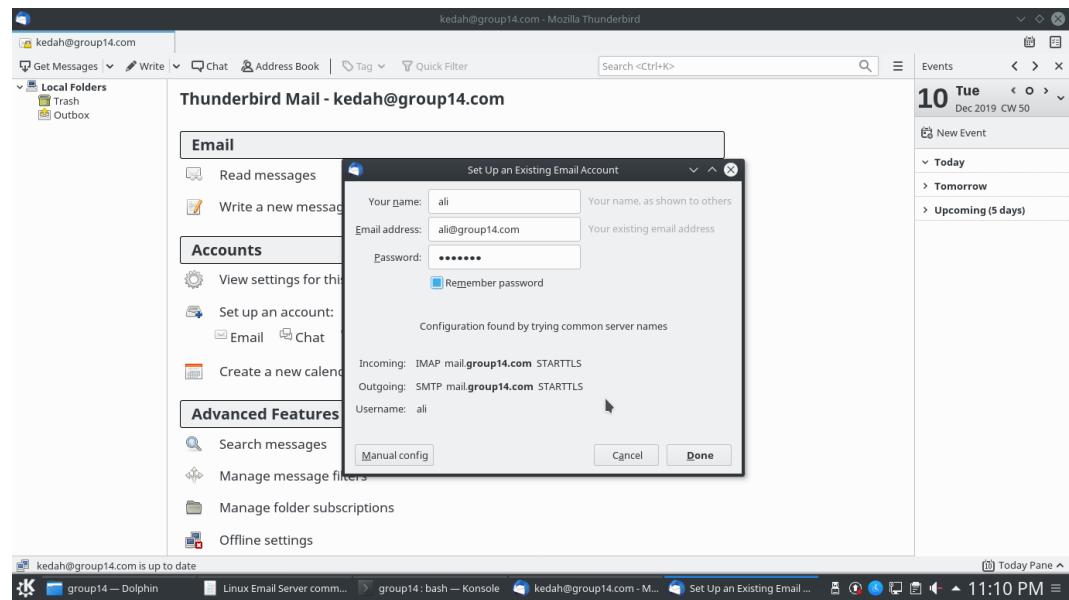


Figure 6. 41: Thunderbird Ali Login

**STEP 2:** Send message from ali account send some message to abu account.

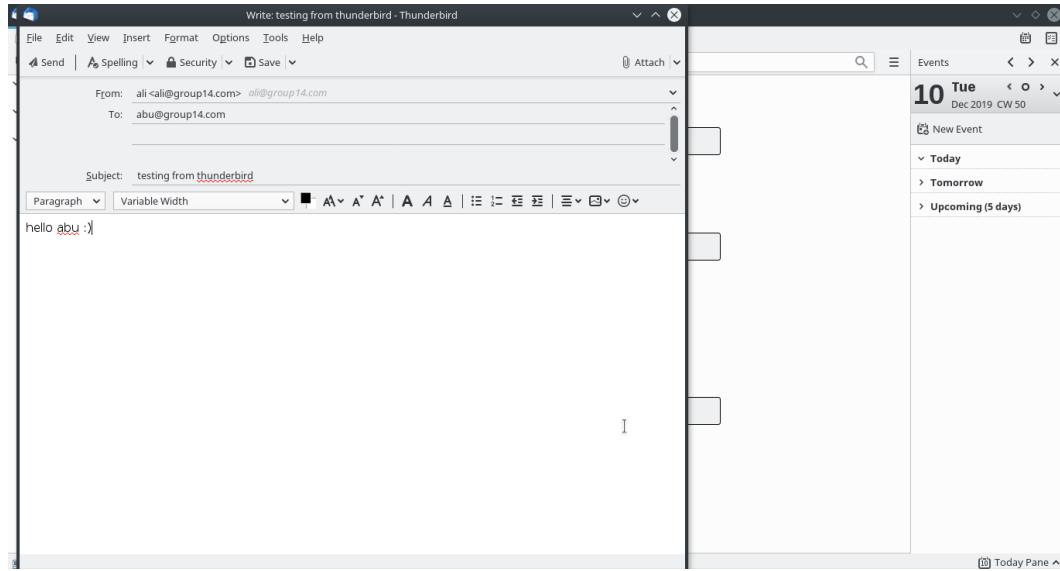


Figure 6. 42: Thunderbird Ali Sending a Message

**STEP 3:** Check sent box from ali to confirm the text was send.

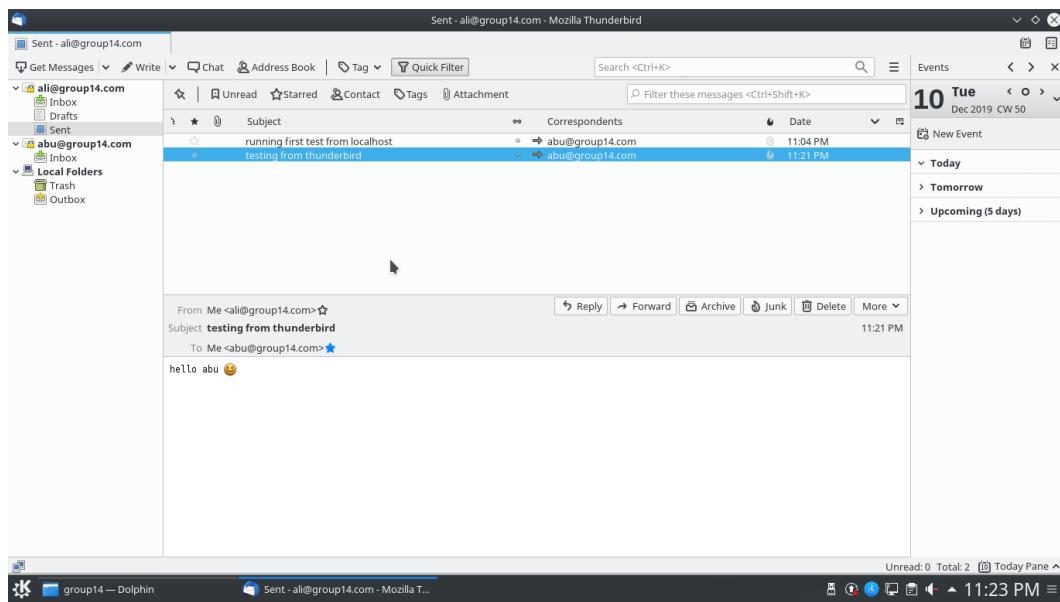


Figure 6. 43: Thunderbird Ali sent Item

## STEP 4: Abu Login using Thunderbird

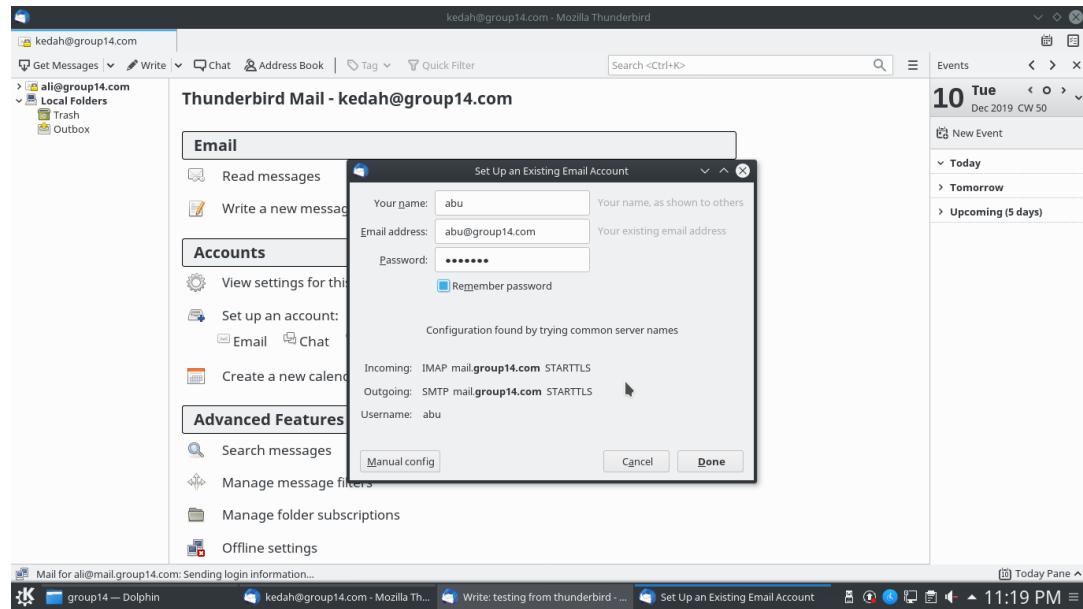


Figure 6. 44: Thunderbird Haikal Login

**STEP 5:** Check the email receive on abu account on mailbox. If the email receives as send from ali account than the testing using Thunderbird success.

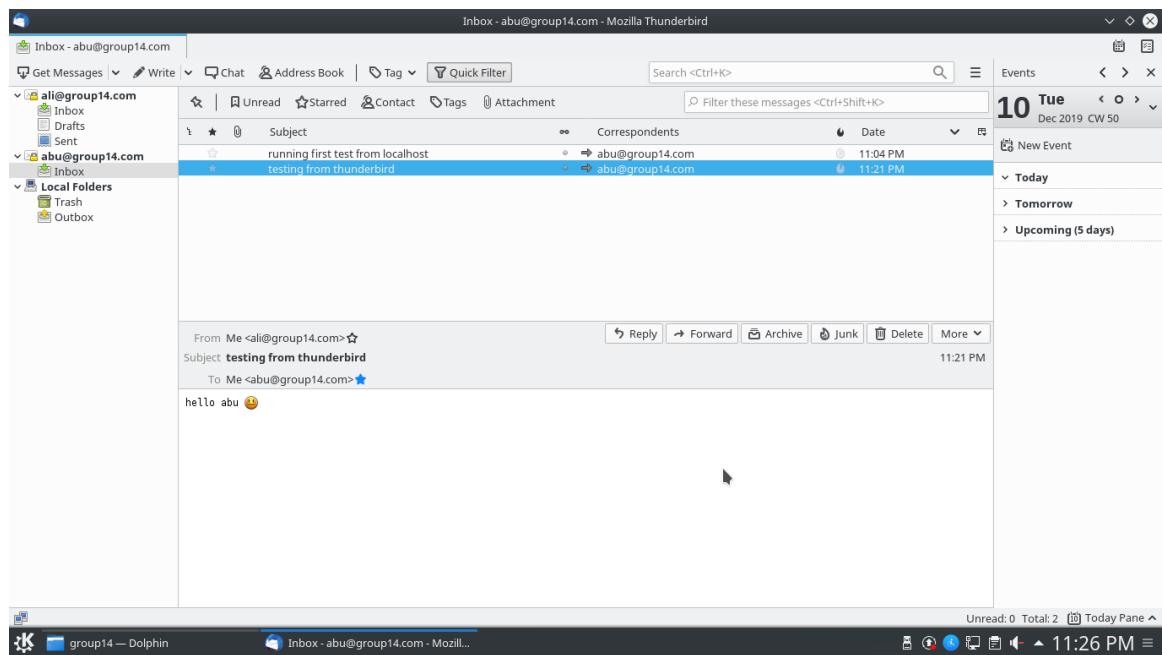


Figure 6. 45: Thunderbird Abu Inbox.

## 6.2.11 WEB, SSL & VIRTUAL HOSTING

**Step1:** Browse <http://www.group14.com>



Figure 6. 46: Main website (<http://www.group14.com>)

### 6.2.11.1 Secure Socket Layer (SSL)

**Step2:** Browse <https://www.group14.com>

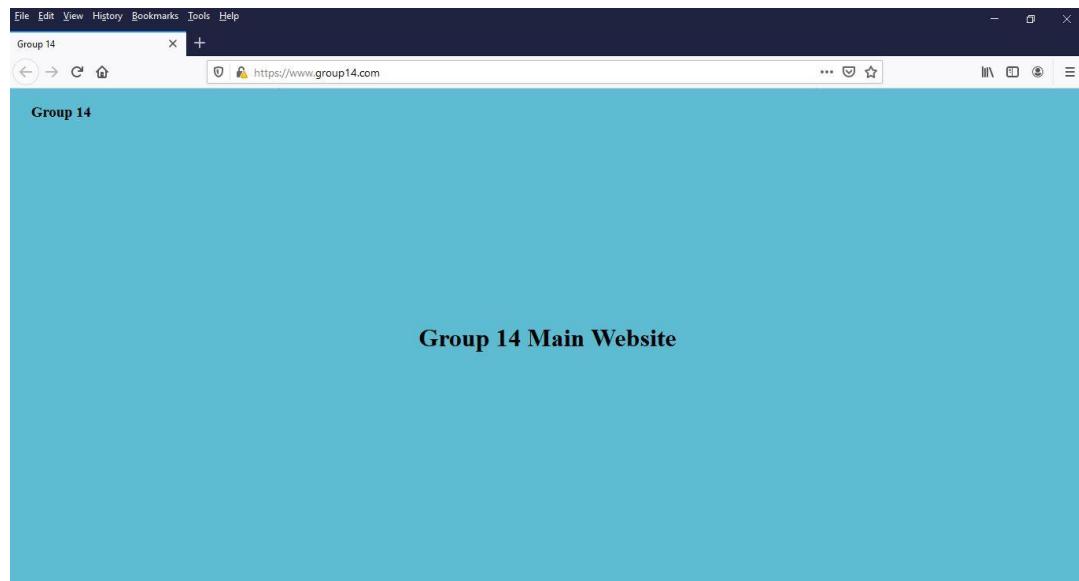


Figure 6. 47: Main website (<https://www.group14.com>)

### 6.2.11.2 Virtual Hosting

Step3: Browse <http://website.group14.com>



Figure 6. 48: Second webpage using virtual hosting (<http://website.group14.com>)

## 6.2.12 IPV6 WEB WITH IPV6 TUNNELLING

Step1: Browse <http://www.groupv6.com>

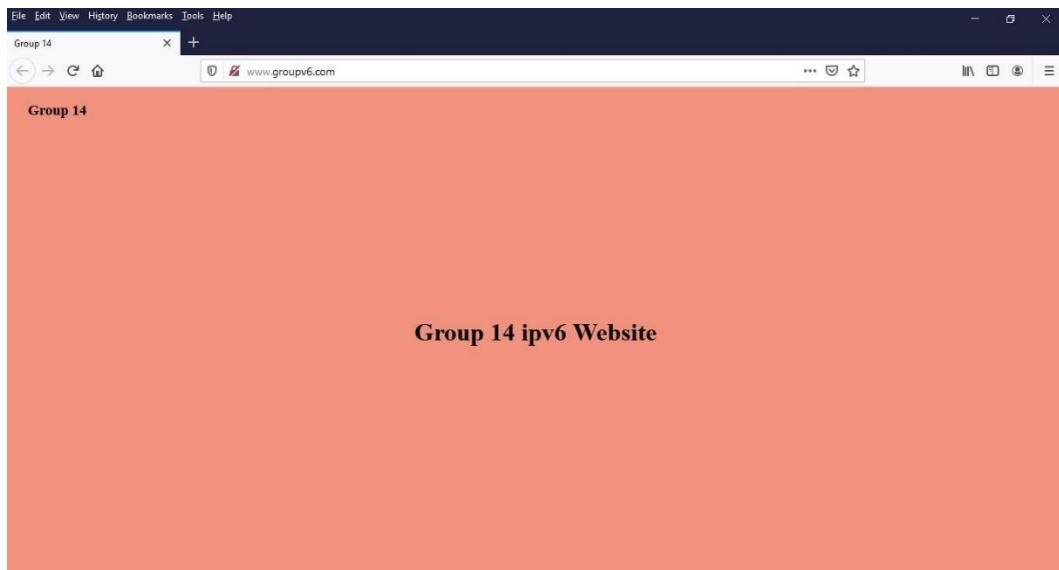


Figure 6. 49: ipv6 web

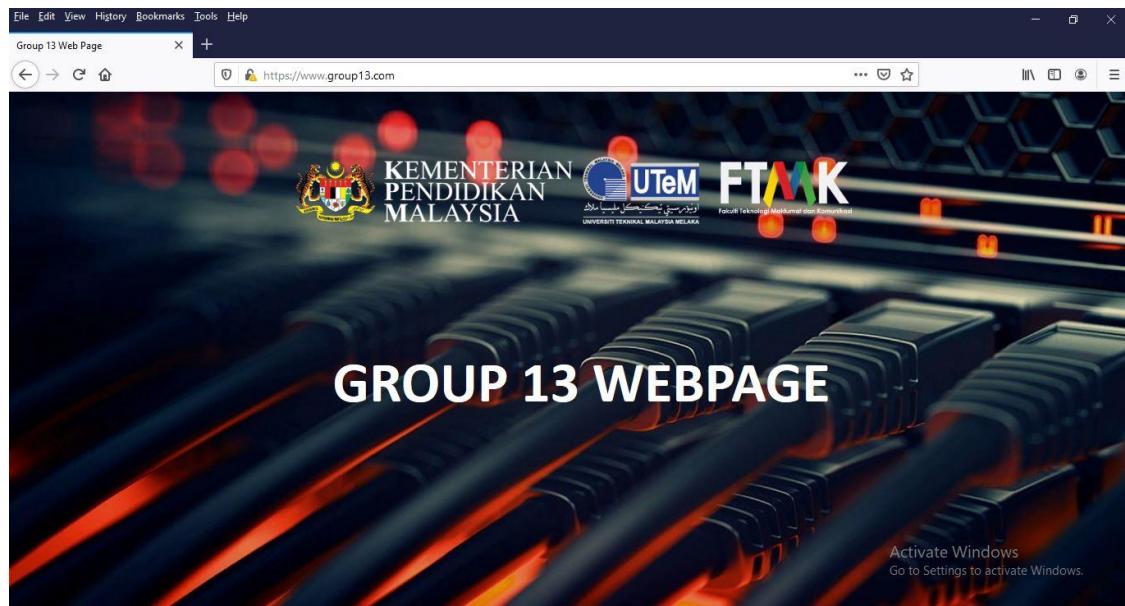
### 6.2.12.1 Testing on neighbor

Step 1: Browse <http://www.webipv6.com>



Figure 6. 50: neighbour ipv6 web

**Step 2:** Browse <https://www.group13.com>



*Figure 6. 51: neighbour ipv4 web*

### 6.2.13 NETWORK MANAGEMENT SYSTEM

**Step 1:** Open the browser and navigate to <http://192.168.14.179:8980/opennms/login.jsp> to monitor the services.

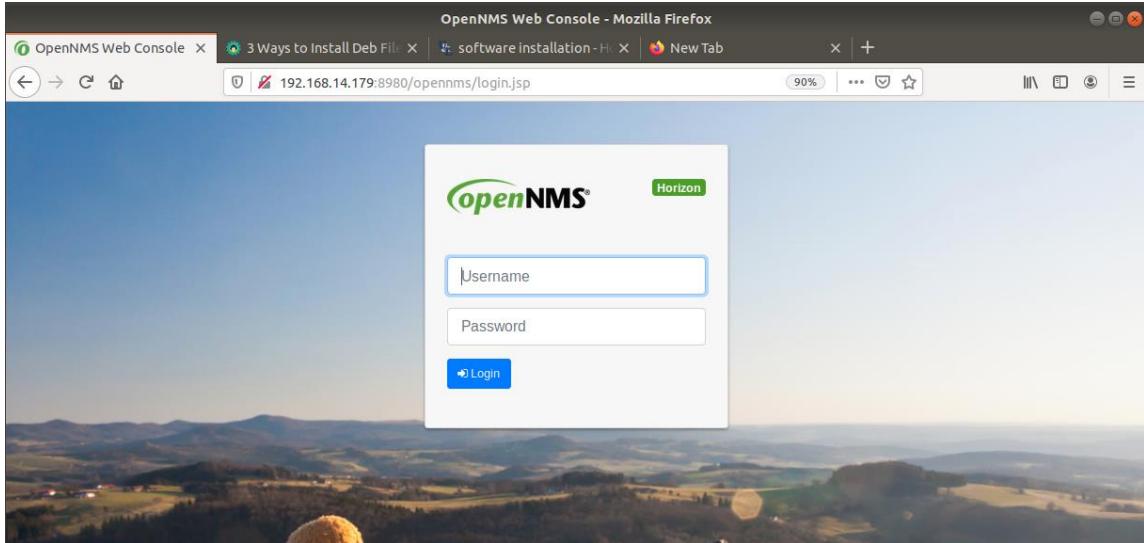


Figure 6. 52: Browse OpenNMS Horizon website.

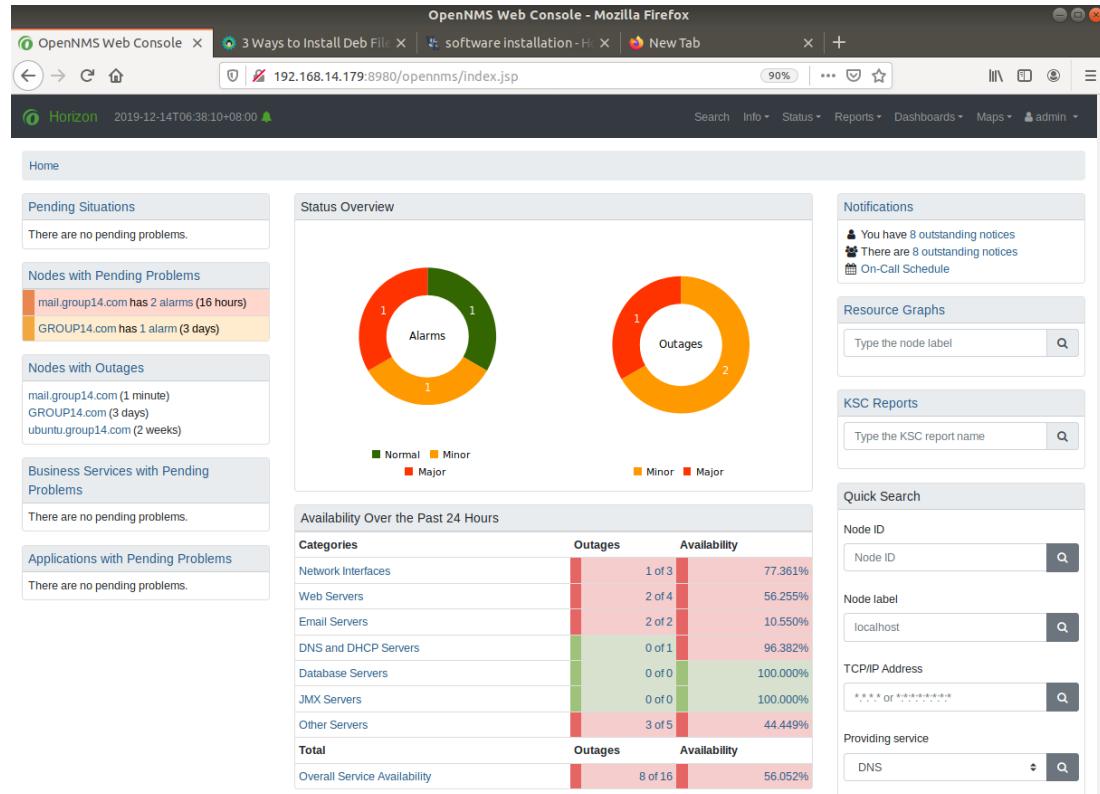


Figure 6. 53: Login done.

**Step 2:** Click **Configure Notifications** to add email of a user to get notifications through email if any services in any nodes are down.

The screenshot shows the OpenNMS Web Console interface. The title bar reads "OpenNMS Web Console - Mozilla Firefox". The address bar shows the URL "192.168.14.179:8980/opennms/admin/notification/index.jsp". The main content area has a sidebar titled "Configure Notifications" with options: "Configure Event Notifications", "Configure Destination Paths", and "Configure Path Outages". To the right of the sidebar are three boxes: "Event Notifications" (describing how to configure notifications for events), "Destination Paths" (describing what users or groups receive notifications), and "Path Outages" (describing how to configure path outages). At the bottom of the page is a footer with the text "OpenNMS Copyright © 2002-2019 The OpenNMS Group, Inc. OpenNMS® is a registered trademark of The OpenNMS Group, Inc. - Version: 25.1.0".

*Figure 6. 54: Configure Notifications*

**Step 3:** Then, go to **Configure Destination Paths** after that click edit.

The screenshot shows the OpenNMS Web Console interface. The title bar reads "Destination Paths | Admin | OpenNMS Web Console - Mozilla Firefox". The address bar shows the URL "192.168.14.179:8980/opennms/admin/notification/destinationPaths.jsp". The main content area shows a table with one row labeled "Email-Admin". Below the table are "Edit" and "Delete" buttons. At the bottom of the page is a footer with the text "OpenNMS Copyright © 2002-2019 The OpenNMS Group, Inc. OpenNMS® is a registered trademark of The OpenNMS Group, Inc. - Version: 25.1.0".

*Figure 6. 55: Destination Path*

**Step 4:** Editing path by **adding email** of admin on initial target for example.  
**margaret@group14.com**

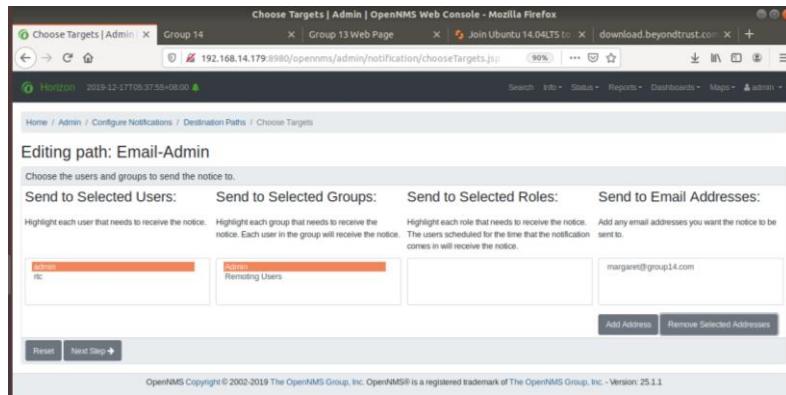


Figure 6. 56: Editing Path

**Step 5:** Choose the **users and groups** to send the notice to by email addresses.

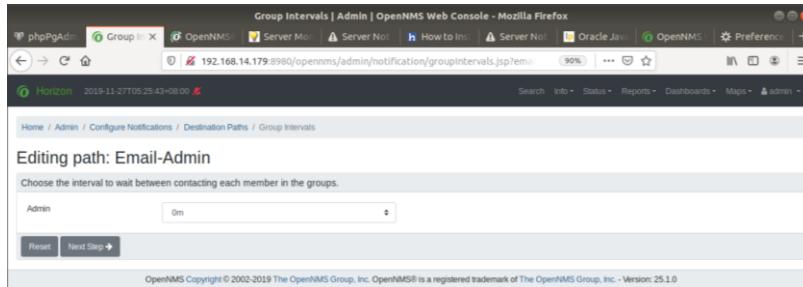


Figure 6. 57: Choose users and groups

**Step 6:** Choose the commands **javaEmail** to use and click „**on**“ for the automatic notification on “**UP**” events. After that, click **Finish** to save it.

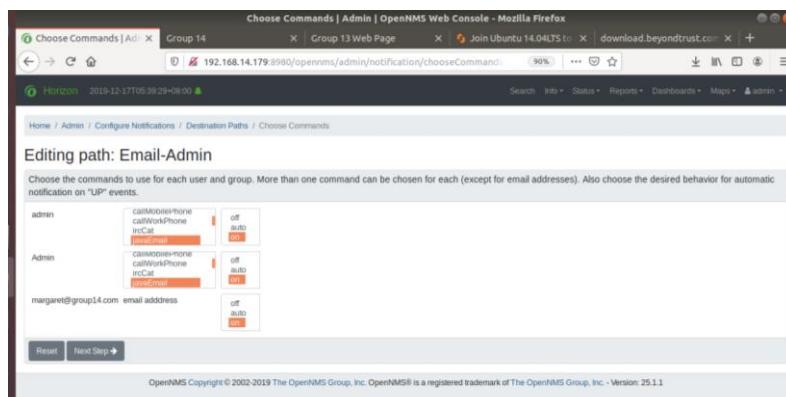


Figure 6. 58: Editing path: Email-Admin

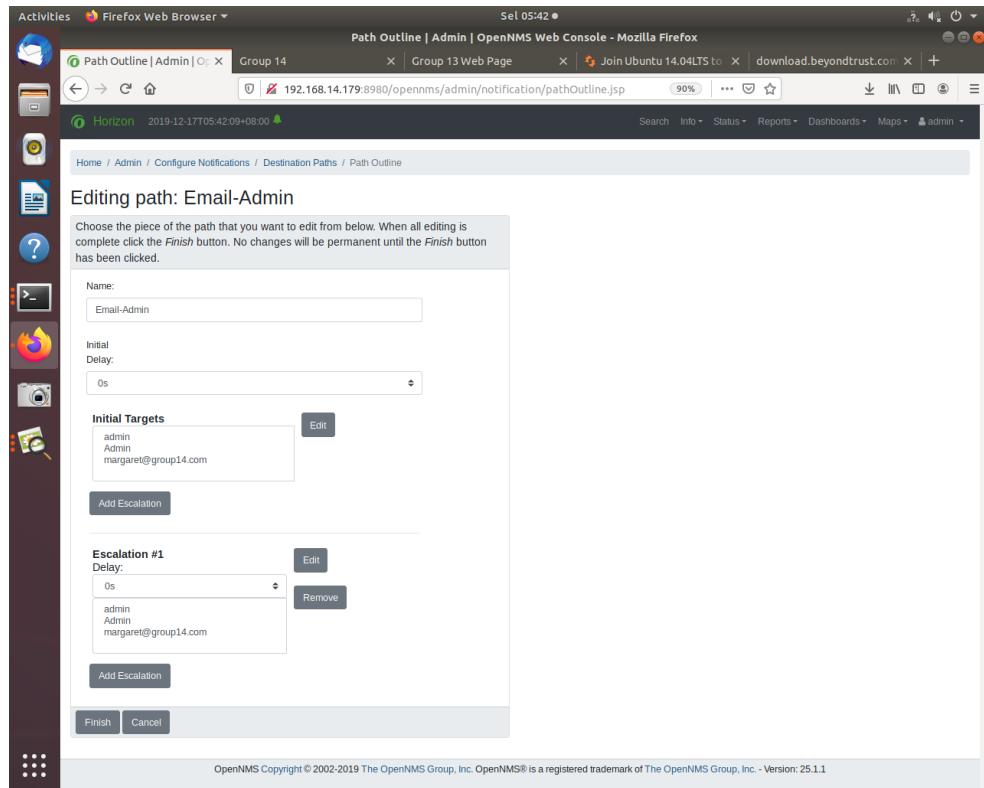


Figure 6. 59: Finish adding Email-Admin

### Step 7: Notification Status select “On” and click “Update”

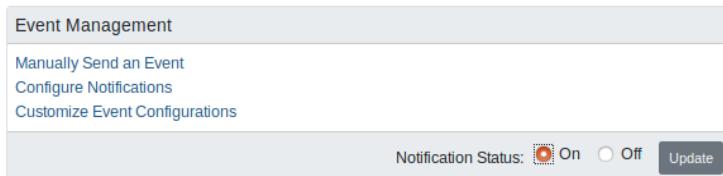


Figure 6.60: Update Notification Status

### Step 8: Select **Manually Add an Interface** on **Provisioning part** to insert IP address from other VLAN.

<div style="border: 1px solid #ccc; padding: 5px;"> <b>Provisioning</b> <ul style="list-style-type: none"> <li><a href="#">Manage Provisioning Requisitions</a></li> <li><a href="#">Import and Export Asset Information</a></li> <li><a href="#">Manage Surveillance Categories</a></li> <li><a href="#">Configure Discovery</a></li> <li><a href="#">Run Single Discovery Scan</a></li> <li><a href="#">Configure SNMP Community Names by IP Address</a></li> <li><a href="#"><b>Manually Add an Interface</b></a></li> <li><a href="#">Delete Nodes</a></li> <li><a href="#">Configure Generator Service</a></li> </ul> </div>	<div style="border: 1px solid #ccc; padding: 5px;"> <p>users. Roles are built from groups and provide a mechanism to implement calendar-based on-call staff rotations. (User: A person, Group: Administrators, Role: On Duty Staff)</p> <p><b>Manage Provisioning Requisitions:</b> Add nodes, interfaces and services to OpenNMS based partly or completely on the contents of a Requisition rather than strictly by having OpenNMS discover the network.</p> <p><b>Import and Export Asset Information:</b> Export and import data into OpenNMS's asset inventory. The comma-delimited file format is supported by most spreadsheet and database applications.</p> <p><b>Manage Surveillance Categories:</b> Manage surveillance categories (also known as node categories) and edit the list of nodes belonging to each category.</p> </div>
---	---

Figure 6. 61: Manually Add an Interface

**Step 9:** Insert IP Address **192.168.14.178** from Windows Server to generate a new Event and it will add a node to the OpenNMS database for this device.

Figure 6.62: Insert IP Address

**Step 10:** After add node and the services will show in the availability, select representative node that contain service **DNS**.

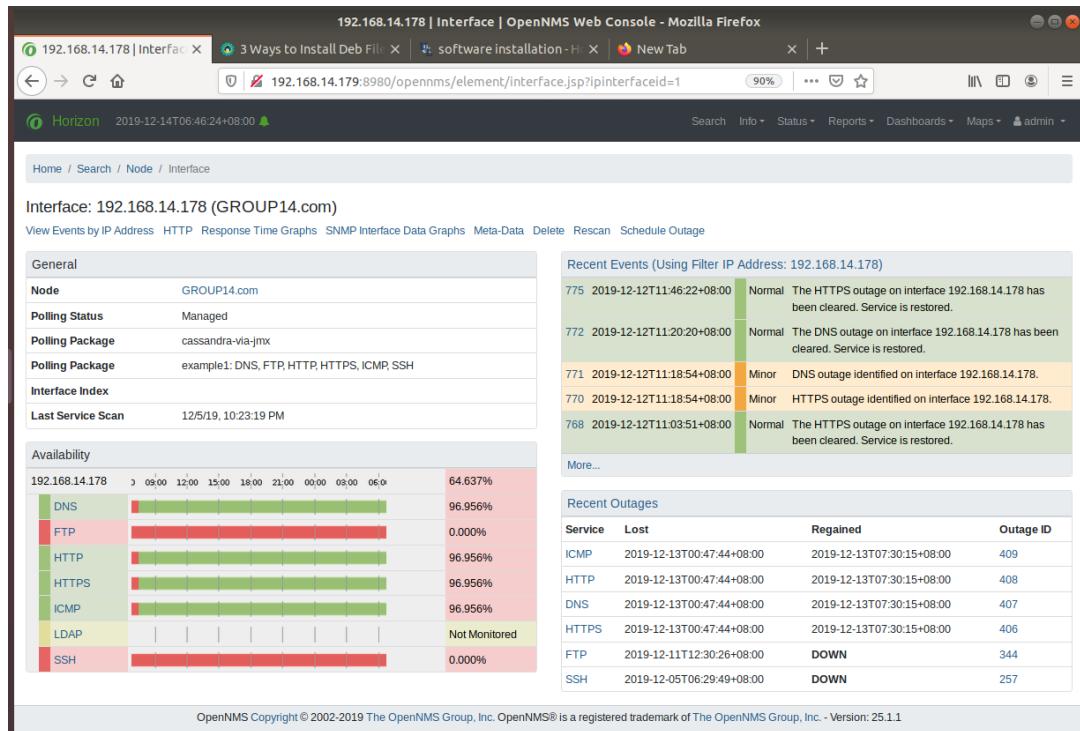


Figure 6.63: Select perspective node

## Step 11: Turn off DNS service in Windows Server

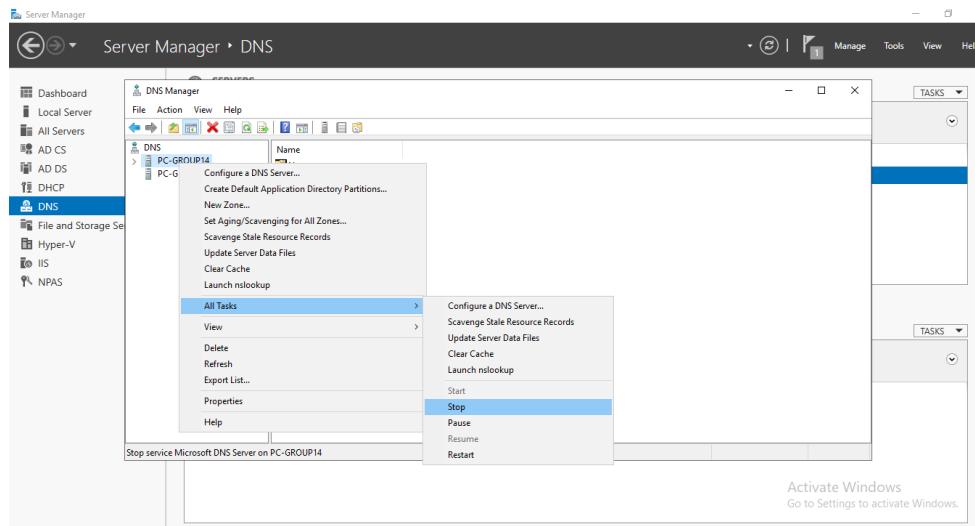


Figure 6.64: Turn OFF DNS service

## Step 12: DNS service turn red colour when service down

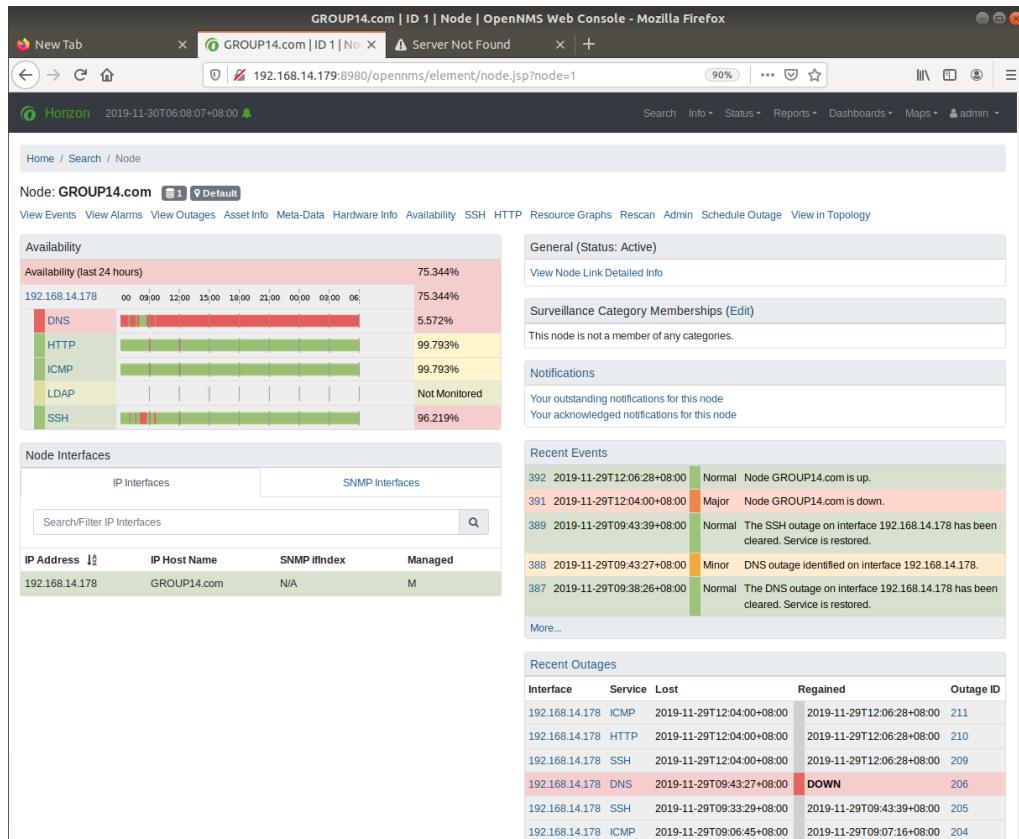


Figure 6.65: DNS service down

ID	Severity	Time	Source Location	System-ID	Node	Node Location	Interface	Service	Alarm ID
822	Major	2019-12-14T06:36:43+08:00	Default	00000000-0000-0000-0000-000000000000	mail.group14.com	Default			213
			uei.opennms.org/hodes/nodeDown					Edit notifications for event	
			Node mail.group14.com is down.						
821	Normal	2019-12-14T06:14:08+08:00	Default	00000000-0000-0000-0000-000000000000	mail.group14.com	Default			212
			uei.opennms.org/hodes/nodeUp					Edit notifications for event	
			Node mail.group14.com is up.						
820	Major	2019-12-14T05:53:27+08:00	Default	00000000-0000-0000-0000-000000000000	mail.group14.com	Default			212
			uei.opennms.org/hodes/nodeDown					Edit notifications for event	
			Node mail.group14.com is down.						
819	Normal	2019-12-14T05:36:19+08:00	Default	00000000-0000-0000-0000-000000000000	mail.group14.com	Default	192.168.14.180	IMAP	211
			uei.opennms.org/hodes/nodeRegainedService					Edit notifications for event	
			The IMAP outage on interface 192.168.14.180 has been cleared. Service is restored.						
818	Minor	2019-12-14T05:33:21+08:00	Default	00000000-0000-0000-0000-000000000000	mail.group14.com	Default	192.168.14.180	IMAP	211
			uei.opennms.org/hodes/nodeLostService					Edit notifications for event	
			IMAP outage identified on interface 192.168.14.180.						
817	Normal	2019-12-14T05:33:21+08:00	Default	00000000-0000-0000-0000-000000000000	mail.group14.com	Default			210
			uei.opennms.org/hodes/nodeUp						

Figure 6.66: Recent Event to view service up and down

### Step 13: Turn on DNS service in Windows Server

Figure 6.67: Turn ON DNS service

## Step 14: DNS service turn green when service up.

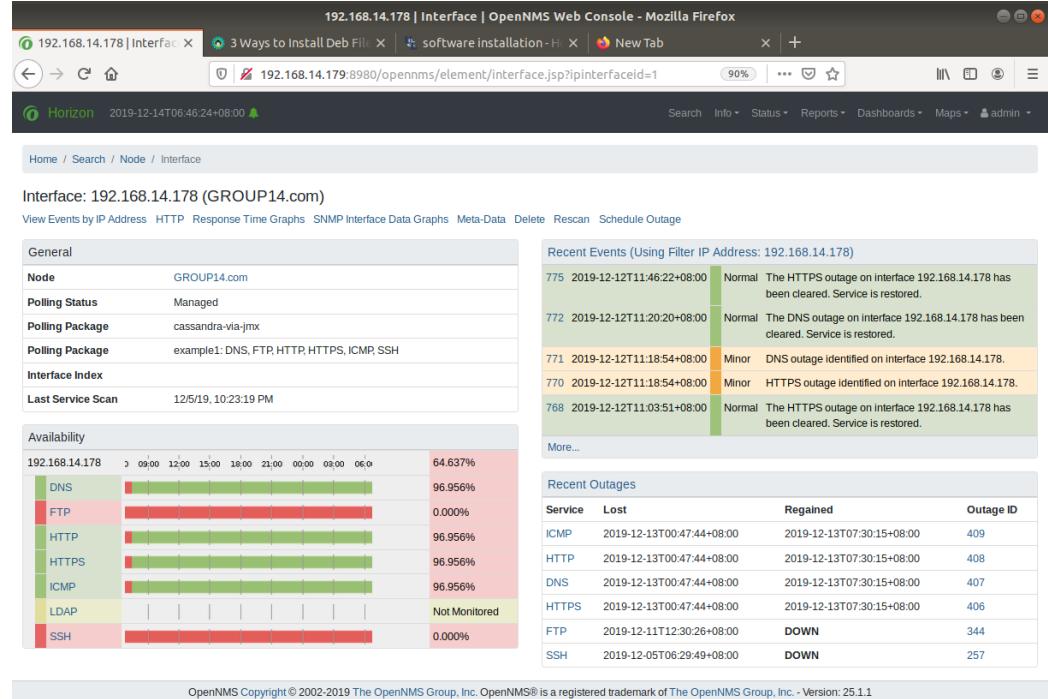


Figure 6.68: DNS service up

**Step 15:** Select charts to view all chart by each service on Alarms Graph (Event Services), Last 7 Days Outages (Service that has resolved), Node Inventory (Node, Interface, Services)

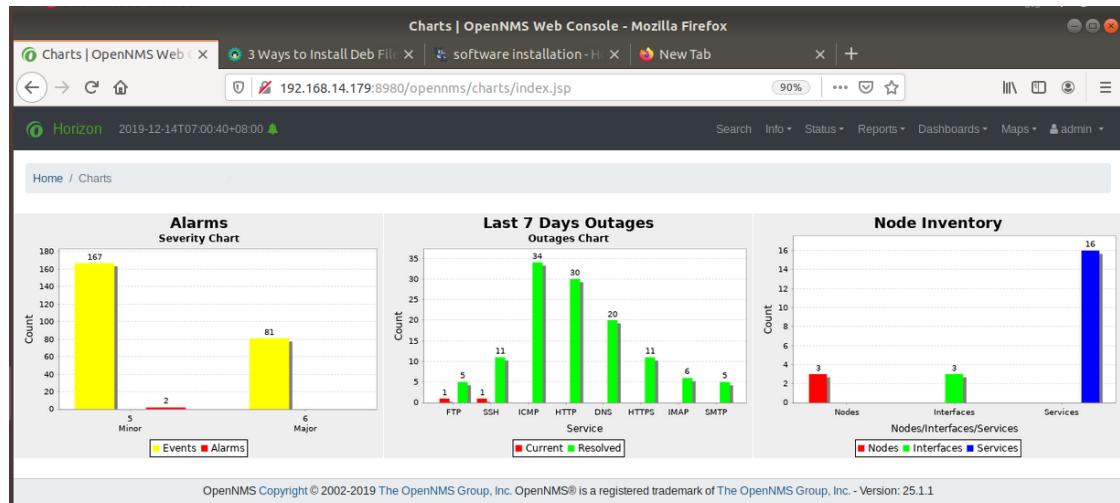


Figure 6.69: View Charts

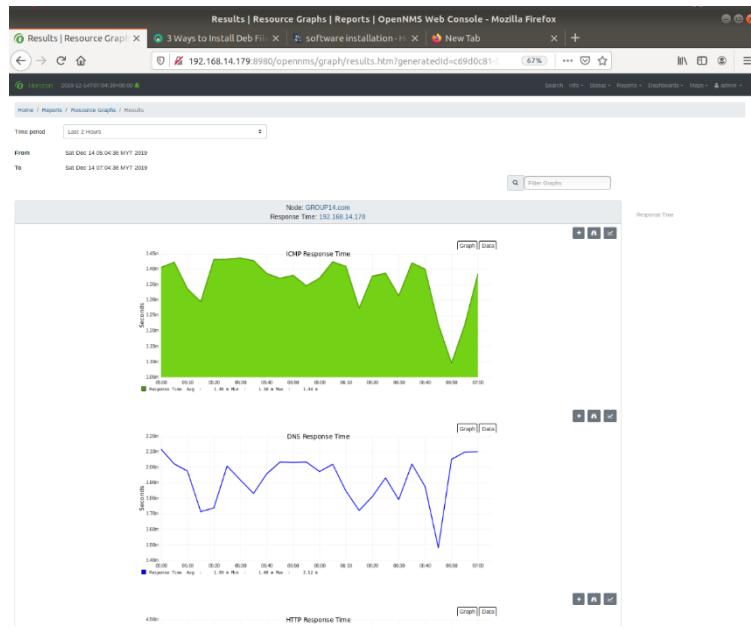


Figure 6.70: View graph by each service on 192.168.14.178

**Step 16:** Open the browser and navigate to `localhost/bandwidthd/` to view graph on each node IP address by each services.

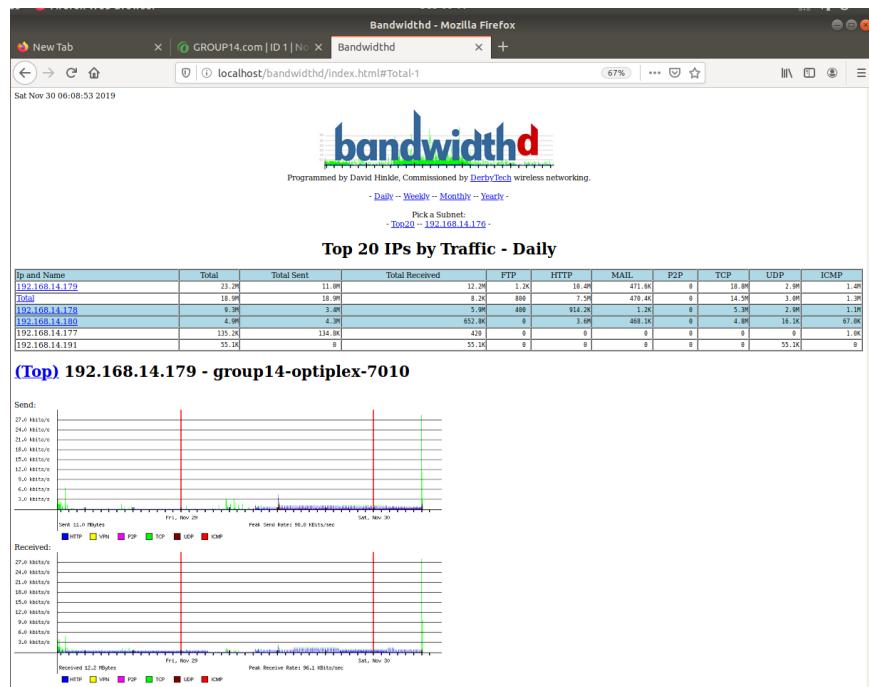


Figure 6.71: View graph on each node

### 6.2.14 PROXY SERVER

**STEP 1:** Open Web Browser and browse website that have been configure to block and if it success it will appear “access denied”. Some of the blocked website are “ulearn.utem.edu.my”.

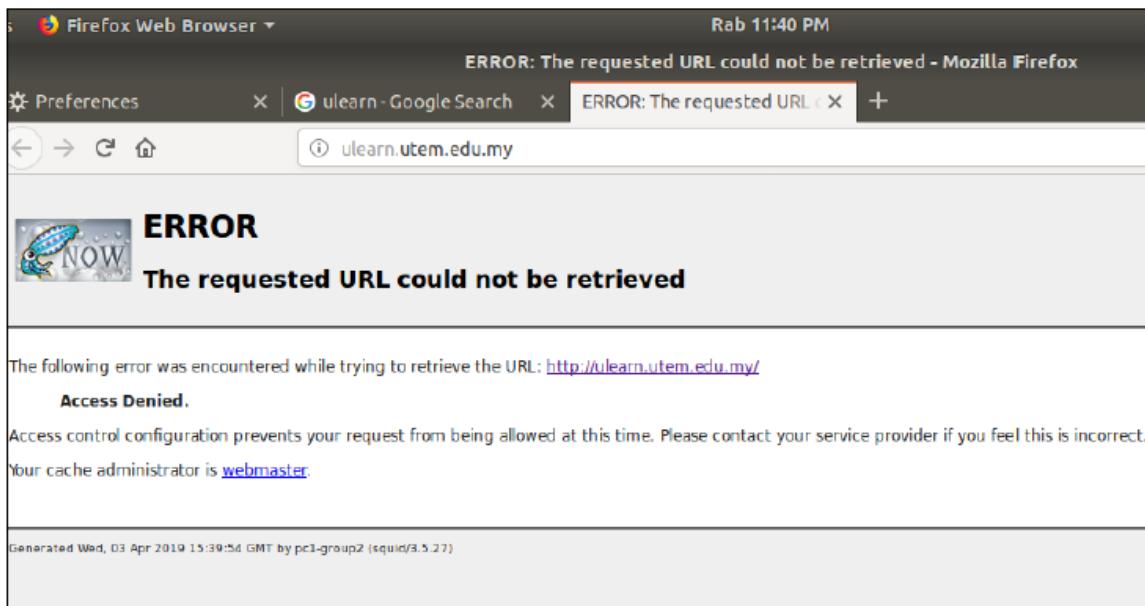


Figure 6.72: Ulearn Blocked website

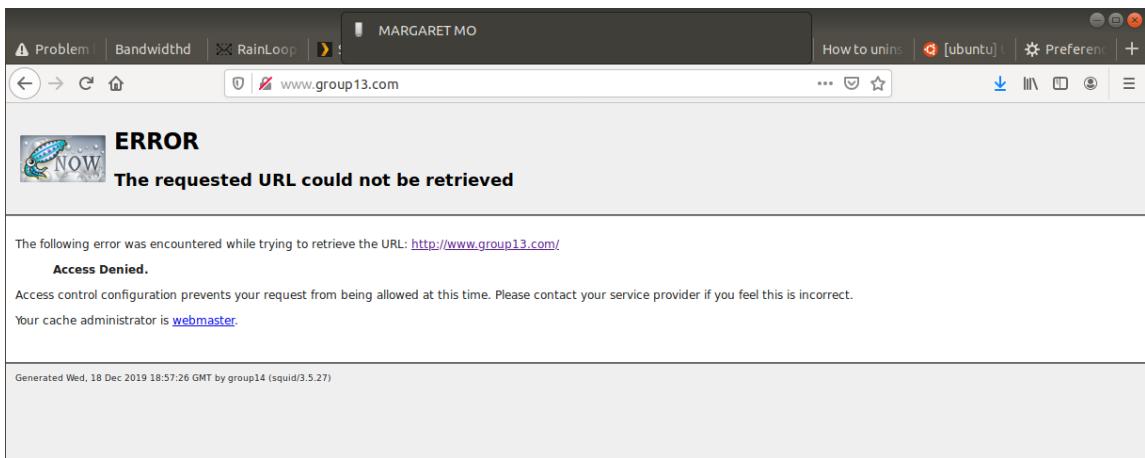


Figure 6.73: Group13 Blocked website

## 6.2.15 SECURE FTP

**Step 1:** Open FileZilla

**Step 2:** Enter the hostname **192.168.14.179**

**Step 3:** Enter the Username **group14** and password with port **22**

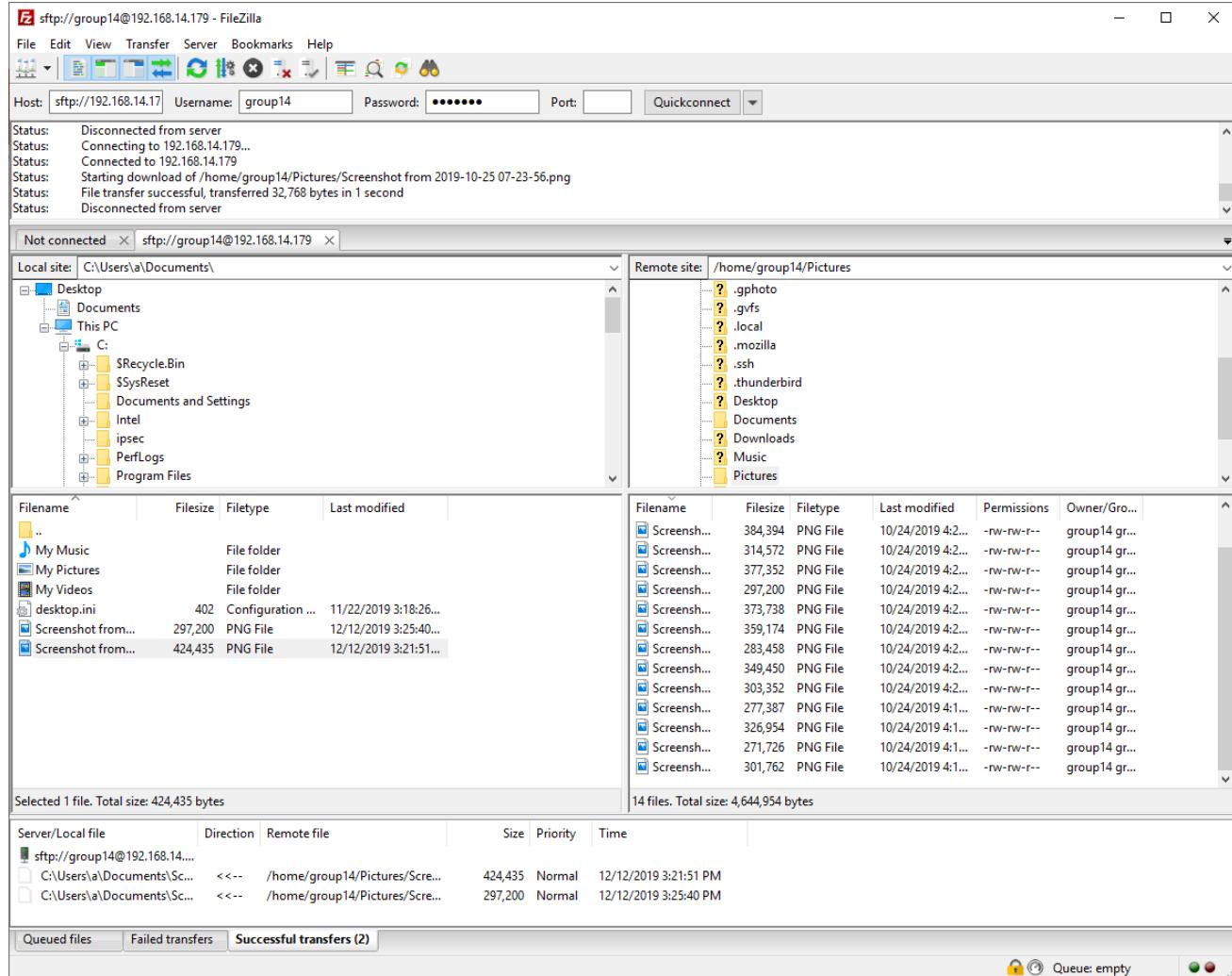


Figure 6.74: Successful Connected

#### Step 4: Next, upload “screenshot.png” to be transferred

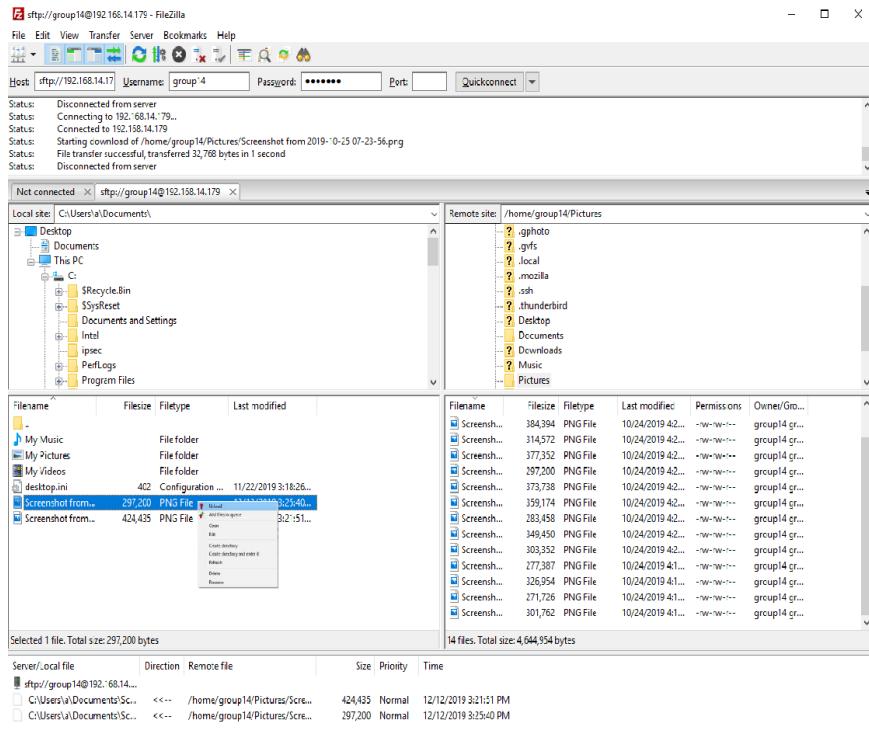


Figure 6.75: Uploading a file

#### Step 5: A notification prompt will be displayed after the file has successfully been uploaded.

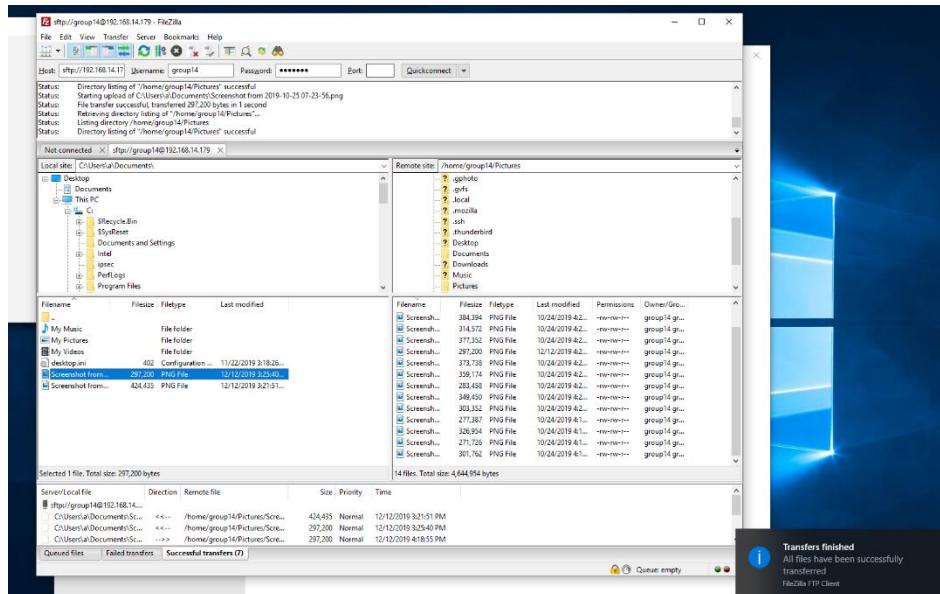


Figure 6.76: File Transfer Process

## Step 6: Capture the packets during the file transfer and filter the contents to SSH only.

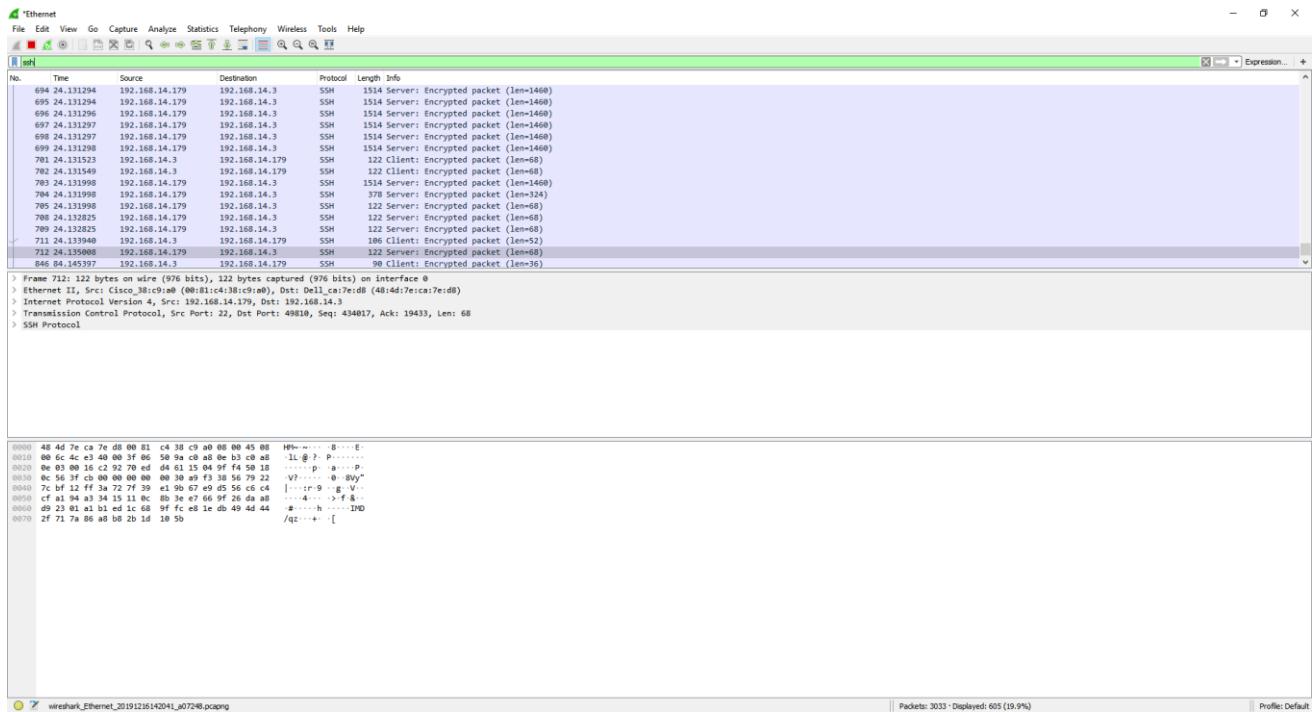
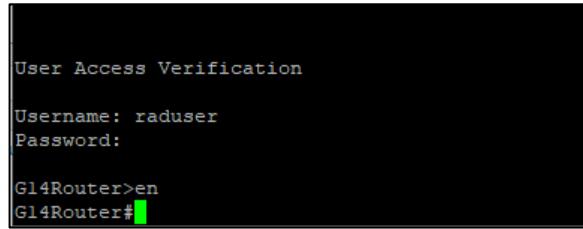


Figure 6.77: Captured FTP packets

## 6.2.16 AAA (AUTHENTICATION, AUTHORIZATION, AND ACCOUNTING) USING RADIUS

**Step 1:** Open putty and try to log in into the router using the username and password in the AD which is raduser and the password is R@diusg14. Authentication is valid if it can log in.



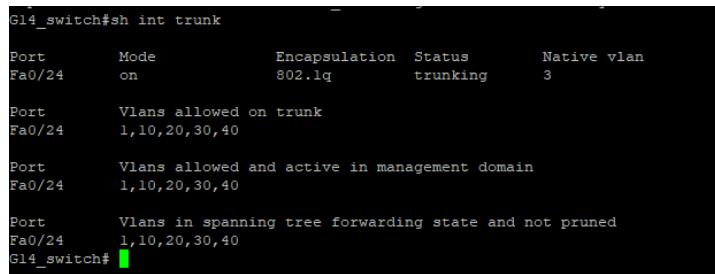
```
User Access Verification  
  
Username: raduser  
Password:  
  
Gl4Router>en  
Gl4Router#
```

Figure 6.78: Result when login into the router

## 6.2.17 VLAN AND PORT SECURITY

### 6.2.18.1 VLAN

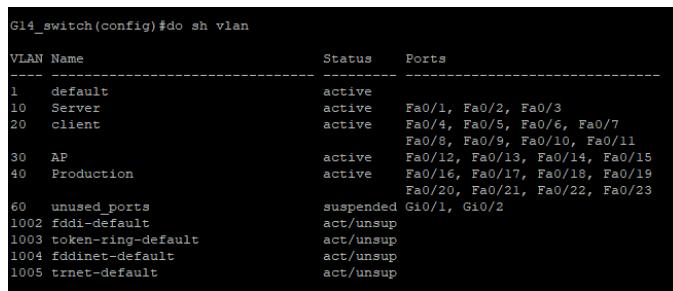
**Step 1:** Use command ‘sh int trunk’ to view trunk settings



```
Gl4_switch#sh int trunk  
  
Port      Mode          Encapsulation  Status        Native vlan  
Fa0/24    on           802.1q         trunking     3  
  
Port      Vlans allowed on trunk  
Fa0/24    1,10,20,30,40  
  
Port      Vlans allowed and active in management domain  
Fa0/24    1,10,20,30,40  
  
Port      Vlans in spanning tree forwarding state and not pruned  
Fa0/24    1,10,20,30,40  
Gl4_switch#
```

Figure 6.79: Trunk setting in port

**Step 2:** Type command ‘do show vlan’ to show every vlan that existed.



```
Gl4_switch(config)#do sh vlan  
  
VLAN Name          Status    Ports  
----  
1    default        active    Fa0/1, Fa0/2, Fa0/3  
10   Server         active    Fa0/4, Fa0/5, Fa0/6, Fa0/7  
20   client         active    Fa0/8, Fa0/9, Fa0/10, Fa0/11  
30   AP             active    Fa0/12, Fa0/13, Fa0/14, Fa0/15  
40   Production     active    Fa0/16, Fa0/17, Fa0/18, Fa0/19  
60   unused_ports   suspended  Fa0/20, Fa0/21, Fa0/22, Fa0/23  
1002 fddi-default  act/unsup  
1003 token-ring-default  act/unsup  
1004 fdnet-default  act/unsup  
1005 trnet-default  act/unsup
```

Figure 6.80: Show every VLAN

### 6.2.18.2 PORT SECURITY

Step 1: Check port security using command ‘sh port-security’.

```
G14_switch#  
G14_switch#sh port  
G14_switch#sh port-security  
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action  
          (Count)      (Count)      (Count)  
-----  
Fa0/1           1           1           0       Restrict  
Fa0/2           1           1           0       Restrict  
Fa0/3           1           1           0       Restrict  
-----  
Total Addresses in System (excluding one mac per port) : 0  
Max Addresses limit in System (excluding one mac per port) : 8192  
G14_switch#
```

Figure 6.81: Check Port Security status

### 6.2.18 WEB HARDENING

#### 6.2.18.1 Windows Authentication and Basic Authentication

Step 1: Open browser and enter haseena.group14.com and a window will pop ups asking for the username and password.

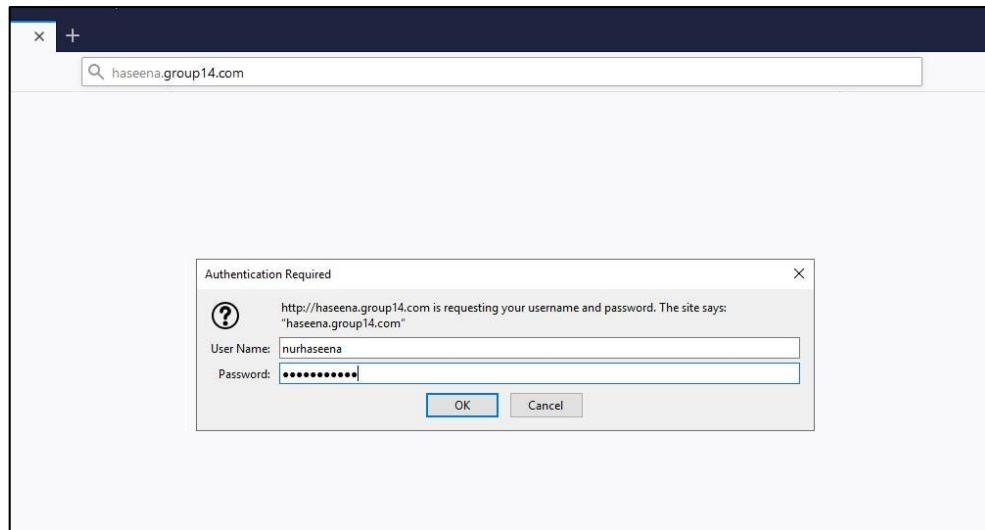
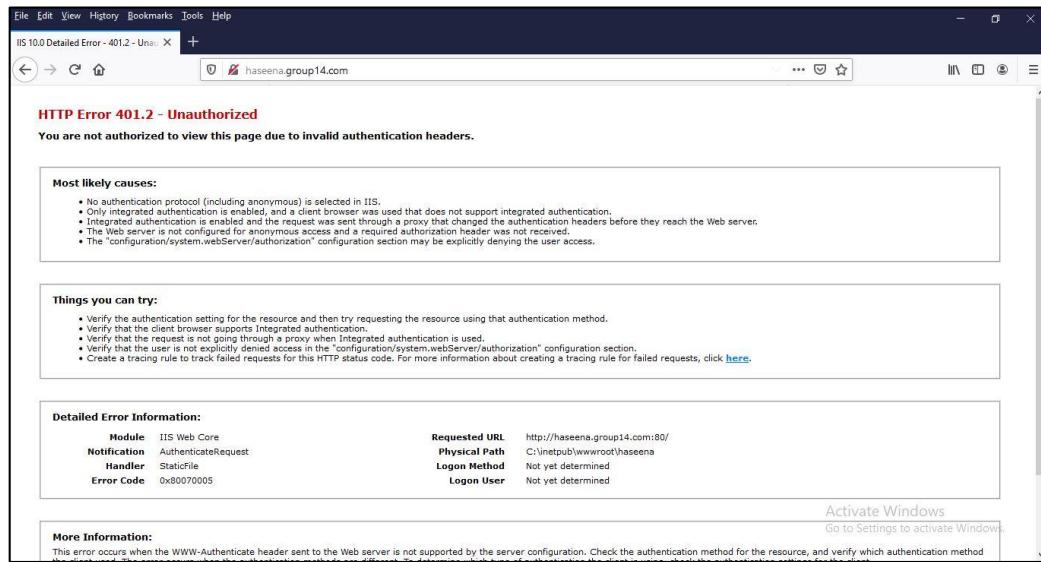


Figure 6.82: Authentication Testing successful

**Step 2:** If the authentication is invalid, it will show error.



*Figure 6.83: Unsuccessful authenticate*

### 6.2.18.2 URL Authorization

**Step 1:** Try to log in at website haseena.group14.com using ‘anas’ user which is other than ‘nurhaseena’ user. The log in will not be successful.

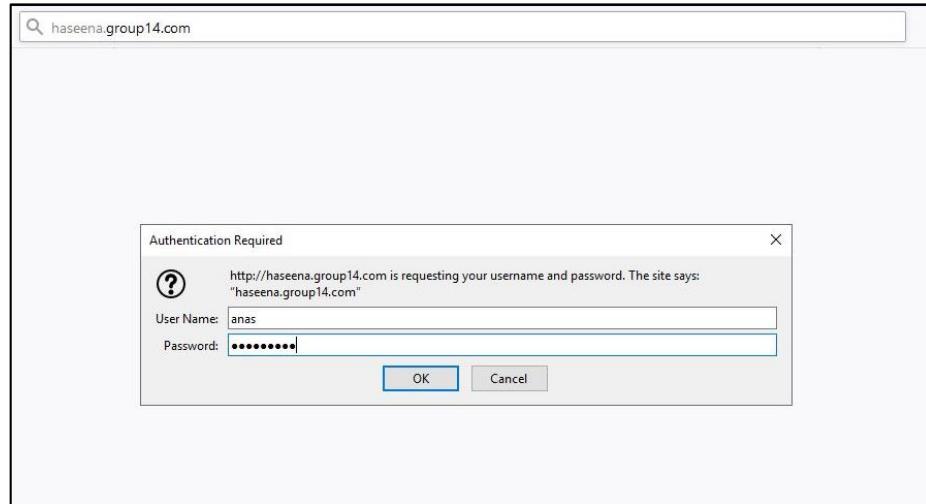


Figure 6.84: Log in using user anas

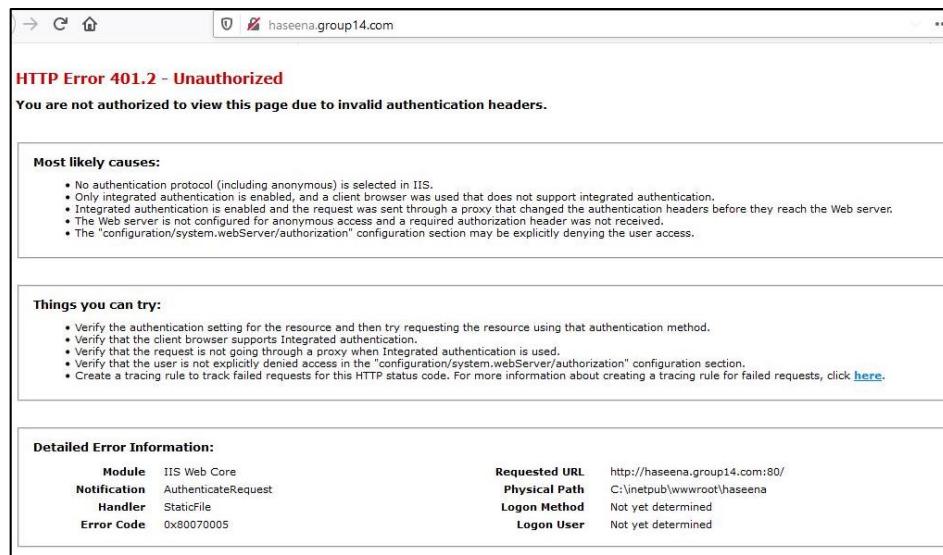


Figure 6.85: Error unauthorized

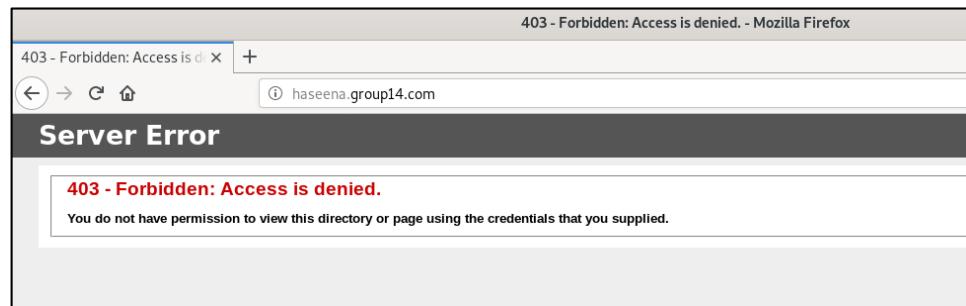
**Step 2:** Log in using user ‘nurhaseena’ and it will be successful.



*Figure 6.86: Successful URL Authorization*

#### 6.2.18.3 IP and Domain Restriction

**Step 1:** Try to access the website ‘haseena.group14.com’ using Debian which the IP has been restricted from access the websites. The result will show that the access is denied.



*Figure 6.87: Access denied*

#### 6.2.18.4 Request Filtering

**Step 1:** Open the website before configuring the request filtering. Try and look at the picture consists in the website.

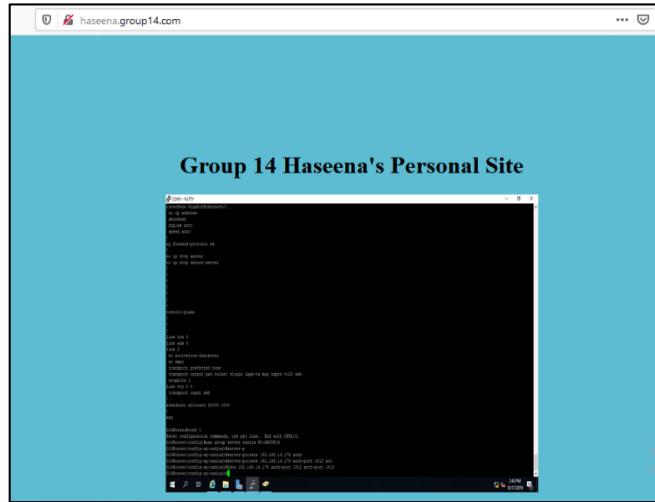


Figure 6.88: Website that consists a picture

**Step 2:** After configuring, try and open back the website and see the difference which is the picture is not available to see.

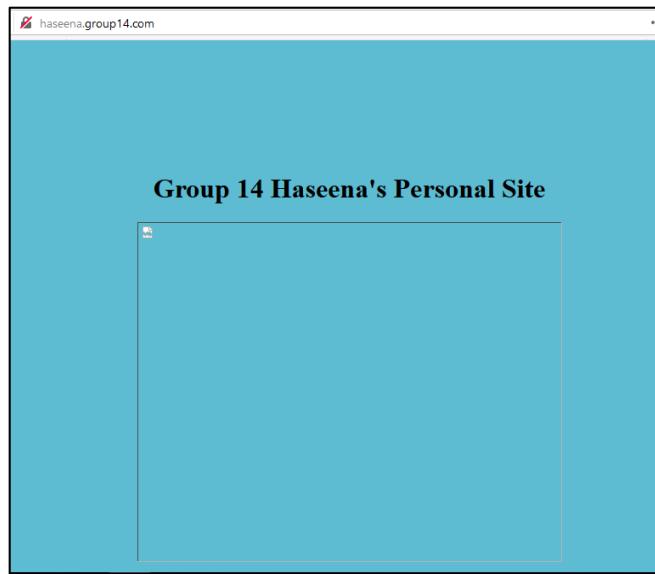


Figure 6.89: The picture has been filtered

## 6.2.18.5 Logging

**Step 1:** Open the log file location. Copy and paste the given path.

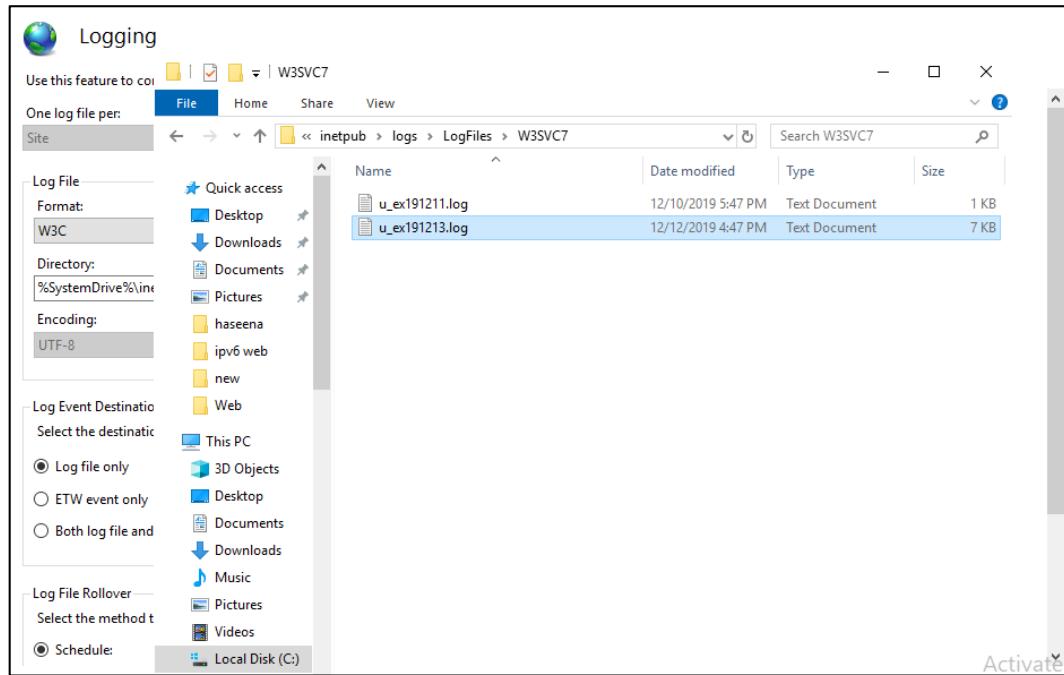


Figure 6.90: Locate the log files

**Step 2:** Open the log files and look at the logs.

```

u_ex191213.log - Notepad
File Edit Format View Help
2019-12-13 00:25:51 192.168.14.178 Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64;+rv:71.0)+Gecko/20100101+Firefox/71.0 - 401 2 5 0
2019-12-13 00:26:01 192.168.14.178 Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64;+rv:71.0)+Gecko/20100101+Firefox/71.0 - 200 0 0 0
2019-12-13 00:26:01 192.168.14.178 GET /favicon.ico - 80 nurhaseena 192.168.14.178 Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64;+rv:71.0)+Gecko/20100101+Firefox/71.0 - 404
2019-12-13 00:26:31 192.168.14.178 Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64;+rv:71.0)+Gecko/20100101+Firefox/71.0 - 401 2 5 0
2019-12-13 00:26:58 192.168.14.178 GET / - 80 nurhaseena 192.168.14.178 Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64;+rv:71.0)+Gecko/20100101+Firefox/71.0 - 200 0 0 0
2019-12-13 00:26:58 192.168.14.178 GET /favicon.ico - 80 nurhaseena 192.168.14.178 Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64;+rv:71.0)+Gecko/20100101+Firefox/71.0 - 404
2019-12-13 00:28:19 192.168.14.178 Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64;+rv:71.0)+Gecko/20100101+Firefox/71.0 - 401 2 5 1
2019-12-13 00:28:27 192.168.14.178 GET / - 80 anas 192.168.14.178 Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64;+rv:71.0)+Gecko/20100101+Firefox/71.0 - 401 2 5 1
2019-12-13 00:28:52 192.168.14.178 GET / - 80 anas 192.168.14.178 Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64;+rv:71.0)+Gecko/20100101+Firefox/71.0 - 401 2 5 0
2019-12-13 00:28:52 192.168.14.178 GET /favicon.ico - 80 - 192.168.14.178 Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64;+rv:71.0)+Gecko/20100101+Firefox/71.0 - 401 2 5 0
2019-12-13 00:29:51 192.168.14.178 Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64;+rv:71.0)+Gecko/20100101+Firefox/71.0 - 401 2 5 0
2019-12-13 00:35:02 192.168.14.178 GET / - 80 - 192.168.14.178 Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64;+rv:71.0)+Gecko/20100101+Firefox/71.0 - 401 2 5 1
2019-12-13 00:35:15 192.168.14.178 GET / - 80 nurhaseena 192.168.14.178 Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64;+rv:71.0)+Gecko/20100101+Firefox/71.0 - 200 0 0 1
2019-12-13 00:35:15 192.168.14.178 GET /favicon.ico - 80 nurhaseena 192.168.14.178 Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64;+rv:71.0)+Gecko/20100101+Firefox/71.0 - 404
2019-12-13 00:35:15 192.168.14.178 GET /favicon.ico - 80 nurhaseena 192.168.14.178 Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64;+rv:71.0)+Gecko/20100101+Firefox/71.0 - 404
2019-12-13 00:36:34 192.168.14.178 GET / - 80 nurhaseena 192.168.14.178 Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64;+rv:71.0)+Gecko/20100101+Firefox/71.0 - 304 0 0 1
2019-12-13 00:36:41 192.168.14.178 GET / - 80 - 192.168.14.178 Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64;+rv:71.0)+Gecko/20100101+Firefox/71.0 - 401 2 5 1
2019-12-13 00:37:08 192.168.14.178 GET / - 80 nurhaseena 192.168.14.178 Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64;+rv:71.0)+Gecko/20100101+Firefox/71.0 - 200 0 0 0
2019-12-13 00:37:05 192.168.14.178 GET /favicon.ico - 80 nurhaseena 192.168.14.178 Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64;+rv:71.0)+Gecko/20100101+Firefox/71.0 - 404
#Software: Microsoft Internet Information Services 10.0
#Version: 1.0
#Date: 2019-12-13 00:44:34
#Fields: date time s-ip cs-method cs-uri-stem cs-uri-query s-port cs-username c-ip cs(User-Agent) cs(Referer) sc-status sc-substatus sc-win32-status time-taken
2019-12-13 00:44:34 192.168.14.178 Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64;+rv:71.0)+Gecko/20100101+Firefox/71.0 - 401 2 5 1
2019-12-13 00:44:34 192.168.14.178 GET /favicon.ico - 80 - 192.168.14.178 Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64;+rv:71.0)+Gecko/20100101+Firefox/71.0 - 401 2 5 0
2019-12-13 00:44:36 192.168.14.178 Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64;+rv:71.0)+Gecko/20100101+Firefox/71.0 - 401 2 5 0
2019-12-13 00:44:52 192.168.14.178 Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64;+rv:71.0)+Gecko/20100101+Firefox/71.0 - 401 2 5 0
2019-12-13 00:44:59 192.168.14.178 Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64;+rv:71.0)+Gecko/20100101+Firefox/71.0 - 401 2 5 0
2019-12-13 00:45:25 192.168.14.178 Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64;+rv:71.0)+Gecko/20100101+Firefox/71.0 - 401 2 5 0
2019-12-13 00:45:59 192.168.14.178 Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64;+rv:71.0)+Gecko/20100101+Firefox/71.0 - 401 2 5 0
2019-12-13 00:45:35 192.168.14.178 GET / - 80 nurhaseena 192.168.14.178 Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64;+rv:71.0)+Gecko/20100101+Firefox/71.0 - 404
2019-12-13 00:46:58 192.168.14.178 GET / - 80 nurhaseena 192.168.14.178 Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64;+rv:71.0)+Gecko/20100101+Firefox/71.0 - 304 0 0 0

```

Figure 6.91: The log files

## 6.2.19 IDS WITH PORT MIRROR

### Intrusion Detection System Testing

**Step 1:** Start snort service and check status snort

```
root@group14-optiplex-7010:/home/group14# sudo systemctl status snort
● snort.service - Snort NIDS Daemon
  Loaded: loaded (/lib/systemd/system/snort.service; disabled; vendor preset: enabled)
  Active: active (running) since Fri 2019-12-13 12:30:14 +08; 6s ago
    Main PID: 21807 (snort)
      Tasks: 2 (limit: 4915)
     CGroup: /system.slice/snort.service
             └─21807 /usr/local/bin/snort -q -u snort -c /etc/snort/snort.conf -i enp1s2
```

Figure 6.92: Check status snort service

**Step 2:** Test snort

```
group14@group14-optiplex-7010:~$ sudo su
[sudo] password for group14:
root@group14-optiplex-7010:/home/group14# sudo nano /etc/snort/rules/local.rules
root@group14-optiplex-7010:/home/group14# sudo snort
-A console -i enp1s2 -u snort -g snort -c /etc/snort/snort.conf
running in IDS mode

--- Initializing Snort ---
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "/etc/snort/snort.conf"
PortVar 'HTTP_PORTS' defined : [ 80:81 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2809 3037 3128 3702 4343 4848 5250 6988 700
8:7061 7144:7145 7510 7777 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 8243 8280 8300 8800 8888 8899 9000 9060 9
880 9090:9091 9443 9999 11371 34443:34444 41080 50002 55555 ]
PortVar 'SHELLCODE_PORTS' defined : [ 0:79 81:5535 ]
PortVar 'ORACLE_PORTS' defined : [ 1024:65535 ]
PortVar 'SSH_PORTS' defined : [ 22 ]
PortVar 'FTP_PORTS' defined : [ 21 2100 3535 ]
PortVar 'SIP_PORTS' defined : [ 5060:5061 5600 ]
PortVar 'FILE_DATA_PORTS' defined : [ 80:81 110 143 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2809 3037 3128 3702 4343 4848
5250 6988 7000:7001 7144:7145 7510 7777 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 8243 8280 8300 8800 8888 8899
9 9000 9060 9080 9090:9091 9443 9999 11371 34443:34444 41080 50002 55555 ]
PortVar 'GTP_PORTS' defined : [ 2123 2152 3386 ]
detection:
  Search-Method = AC-Full-Q
  Split Any/Any group = enabled
  Search-Method-Optimizations = enabled
  Maximum pattern length = 20
Tagged Packet Limit: 256
Loading dynamic engine /usr/local/lib/snort_dynamicengine/libsf_engine.so... done
Loading all dynamic detection libs from /usr/local/lib/snort_dynamicrules...
WARNING: No dynamic libraries found in directory /usr/local/lib/snort_dynamicrules.
Finished Loading all dynamic detection libs from /usr/local/lib/snort_dynamicrules
Loading all dynamic preprocessor libs from /usr/local/lib/snort_dynamicpreprocessor/...
  Loading dynamic preprocessor library /usr/local/lib/snort_dynamicpreprocessor//libsf_appld_preproc.so... done
  Loading dynamic preprocessor library /usr/local/lib/snort_dynamicpreprocessor//libsf_dns_preproc.so... done
  Loading dynamic preprocessor library /usr/local/lib/snort_dynamicpreprocessor//libsf_ftptelnet_preproc.so... done
  Loading dynamic preprocessor library /usr/local/lib/snort_dynamicpreprocessor//libsf_reputation_preproc.so... done
  Loading dynamic preprocessor library /usr/local/lib/snort_dynamicpreprocessor//libsf_ssl_preproc.so... done
  Loading dynamic preprocessor library /usr/local/lib/snort_dynamicpreprocessor//libsf_gtp_preproc.so... done
  Loading dynamic preprocessor library /usr/local/lib/snort_dynamicpreprocessor//libsf_lnat_preproc.so... done
  Loading dynamic preprocessor library /usr/local/lib/snort_dynamicpreprocessor//libsf_stp_preproc.so... done
  Loading dynamic preprocessor library /usr/local/lib/snort_dynamicpreprocessor//libsf_modbus_preproc.so... done
  Loading dynamic preprocessor library /usr/local/lib/snort_dynamicpreprocessor//libsf_ntp_preproc.so... done
  Loading dynamic preprocessor library /usr/local/lib/snort_dynamicpreprocessor//libsf_sdf_preproc.so... done
  Loading dynamic preprocessor library /usr/local/lib/snort_dynamicpreprocessor//libsf_dce2_preproc.so... done
  Loading dynamic preprocessor library /usr/local/lib/snort_dynamicpreprocessor//libsf_ssh_preproc.so... done
  Loading dynamic preprocessor library /usr/local/lib/snort_dynamicpreprocessor//libsf_dnp3_preproc.so... done
  Loading dynamic preprocessor library /usr/local/lib/snort_dynamicpreprocessor//libsf_pop_preproc.so... done
Finished Loading all dynamic preprocessor libs from /usr/local/lib/snort_dynamicpreprocessor/
Log directory = /var/log/snort
```

Figure 6.93: Test snort

```

Preprocessor Object: SF_SIP Version 1.1 <Build 1>
Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
Preprocessor Object: SF_GTP Version 1.1 <Build 1>
Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>
Preprocessor Object: SF_FPTTELNET Version 1.2 <Build 13>
Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Preprocessor Object: appid Version 1.1 <Build 5>
Commencing packet processing (pid=6657)
12/06-03:00:02.225254 [**] [1:10000001:1] ICMP test [**] [Priority: 0] [ICMP] 192.168.14.177 -> 192.168.14.178
12/06-03:00:03.131678 [**] [1:10000001:1] ICMP test [**] [Priority: 0] [ICMP] 192.168.14.177 -> 192.168.14.178
12/06-03:00:04.039651 [**] [1:10000001:1] ICMP test [**] [Priority: 0] [ICMP] 200.200.200.3 -> 192.168.14.178
12/06-03:00:04.944307 [**] [1:10000001:1] ICMP test [**] [Priority: 0] [ICMP] 192.168.14.177 -> 192.168.14.178
12/06-03:00:06.062934 [**] [1:10000001:1] ICMP test [**] [Priority: 0] [ICMP] 192.168.14.177 -> 192.168.14.178
12/06-03:00:07.663322 [**] [1:10000001:1] ICMP test [**] [Priority: 0] [ICMP] 192.168.14.177 -> 192.168.14.178
12/06-03:00:09.475215 [**] [1:10000001:1] ICMP test [**] [Priority: 0] [ICMP] 192.168.14.177 -> 192.168.14.178
12/06-03:00:10.382595 [**] [1:10000001:1] ICMP test [**] [Priority: 0] [ICMP] 192.168.14.177 -> 192.168.14.178
12/06-03:00:11.801024 [**] [1:10000001:1] ICMP test [**] [Priority: 0] [ICMP] 192.168.14.177 -> 192.168.14.178
12/06-03:00:13.100155 [**] [1:10000001:1] ICMP test [**] [Priority: 0] [ICMP] 192.168.14.177 -> 192.168.14.178
12/06-03:00:13.851881 [**] [1:10000001:1] ICMP test [**] [Priority: 0] [ICMP] 192.168.14.177 -> 192.168.14.178
12/06-03:00:14.009847 [**] [1:10000001:1] ICMP test [**] [Priority: 0] [ICMP] 200.200.200.3 -> 192.168.14.178
12/06-03:00:14.913541 [**] [1:10000001:1] ICMP test [**] [Priority: 0] [ICMP] 192.168.14.177 -> 192.168.14.178
12/06-03:00:15.818836 [**] [1:10000001:1] ICMP test [**] [Priority: 0] [ICMP] 192.168.14.177 -> 192.168.14.178
12/06-03:00:16.726637 [**] [1:10000001:1] ICMP test [**] [Priority: 0] [ICMP] 192.168.14.177 -> 192.168.14.178
12/06-03:00:19.445863 [**] [1:10000001:1] ICMP test [**] [Priority: 0] [ICMP] 192.168.14.177 -> 192.168.14.178
12/06-03:00:20.350330 [**] [1:10000001:1] ICMP test [**] [Priority: 0] [ICMP] 192.168.14.177 -> 192.168.14.178
12/06-03:00:21.256645 [**] [1:10000001:1] ICMP test [**] [Priority: 0] [ICMP] 192.168.14.177 -> 192.168.14.178
12/06-03:00:22.162927 [**] [1:10000001:1] ICMP test [**] [Priority: 0] [ICMP] 192.168.14.177 -> 192.168.14.178
12/06-03:00:23.069176 [**] [1:10000001:1] ICMP test [**] [Priority: 0] [ICMP] 192.168.14.177 -> 192.168.14.178
12/06-03:00:23.975420 [**] [1:10000001:1] ICMP test [**] [Priority: 0] [ICMP] 192.168.14.177 -> 192.168.14.178
12/06-03:00:23.978812 [**] [1:10000001:1] ICMP test [**] [Priority: 0] [ICMP] 200.200.200.3 -> 192.168.14.178
12/06-03:00:24.882610 [**] [1:10000001:1] ICMP test [**] [Priority: 0] [ICMP] 192.168.14.177 -> 192.168.14.178
12/06-03:00:25.788667 [**] [1:10000001:1] ICMP test [**] [Priority: 0] [ICMP] 192.168.14.177 -> 192.168.14.178
12/06-03:00:26.616794 [**] [1:10000001:1] ICMP test [**] [Priority: 0] [ICMP] 192.168.14.177 -> 192.168.14.178
12/06-03:00:27.600838 [**] [1:10000001:1] ICMP test [**] [Priority: 0] [ICMP] 192.168.14.177 -> 192.168.14.178
12/06-03:00:29.413751 [**] [1:10000001:1] ICMP test [**] [Priority: 0] [ICMP] 192.168.14.177 -> 192.168.14.178
12/06-03:00:30.319930 [**] [1:10000001:1] ICMP test [**] [Priority: 0] [ICMP] 192.168.14.177 -> 192.168.14.178
12/06-03:00:31.086008 [**] [1:10000001:1] ICMP test [**] [Priority: 0] [ICMP] 192.168.14.177 -> 192.168.14.178
12/06-03:00:31.227815 [**] [1:10000001:1] ICMP test [**] [Priority: 0] [ICMP] 200.200.200.3 -> 192.168.14.178
12/06-03:00:32.132272 [**] [1:10000001:1] ICMP test [**] [Priority: 0] [ICMP] 192.168.14.177 -> 192.168.14.178
12/06-03:00:32.135152 [**] [1:10000001:1] ICMP test [**] [Priority: 0] [ICMP] 200.200.200.3 -> 192.168.14.178
12/06-03:00:33.038507 [**] [1:10000001:1] ICMP test [**] [Priority: 0] [ICMP] 192.168.14.177 -> 192.168.14.178
12/06-03:00:33.945150 [**] [1:10000001:1] ICMP test [**] [Priority: 0] [ICMP] 192.168.14.177 -> 192.168.14.178
12/06-03:00:34.850610 [**] [1:10000001:1] ICMP test [**] [Priority: 0] [ICMP] 192.168.14.177 -> 192.168.14.178
12/06-03:00:35.765417 [**] [1:10000001:1] ICMP test [**] [Priority: 0] [ICMP] 192.168.14.177 -> 192.168.14.178
12/06-03:00:35.768417 [**] [1:10000001:1] ICMP test [**] [Priority: 0] [ICMP] 200.200.200.3 -> 192.168.14.178
12/06-03:00:36.671827 [**] [1:10000001:1] ICMP test [**] [Priority: 0] [ICMP] 192.168.14.177 -> 192.168.14.178
12/06-03:00:37.579382 [**] [1:10000001:1] ICMP test [**] [Priority: 0] [ICMP] 192.168.14.177 -> 192.168.14.178
12/06-03:00:37.582331 [**] [1:10000001:1] ICMP test [**] [Priority: 0] [ICMP] 200.200.200.3 -> 192.168.14.178
12/06-03:00:39.392060 [**] [1:10000001:1] ICMP test [**] [Priority: 0] [ICMP] 192.168.14.177 -> 192.168.14.178
12/06-03:00:40.173588 [**] [1:10000001:1] ICMP test [**] [Priority: 0] [ICMP] 192.168.14.177 -> 192.168.14.178
12/06-03:00:40.306784 [**] [1:10000001:1] ICMP test [**] [Priority: 0] [ICMP] 200.200.200.3 -> 192.168.14.178
12/06-03:00:41.392050 [**] [1:10000001:1] ICMP test [**] [Priority: 0] [ICMP] 192.168.14.177 -> 192.168.14.178

```

Figure 6.94: Test snort

### 6.2.20 SAMBA AND SAMBA SECURITY SERVICES

1. Type the Ubuntu ip address

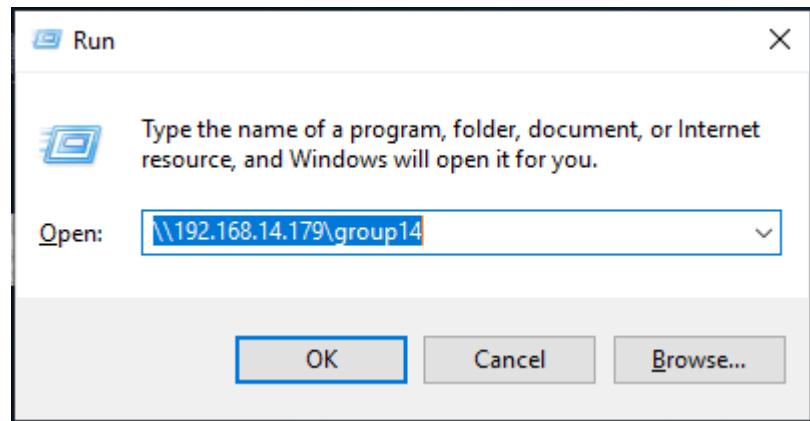


Figure 6.95: Ubuntu ip address

2. Folder shared by Ubuntu can be seen in the client

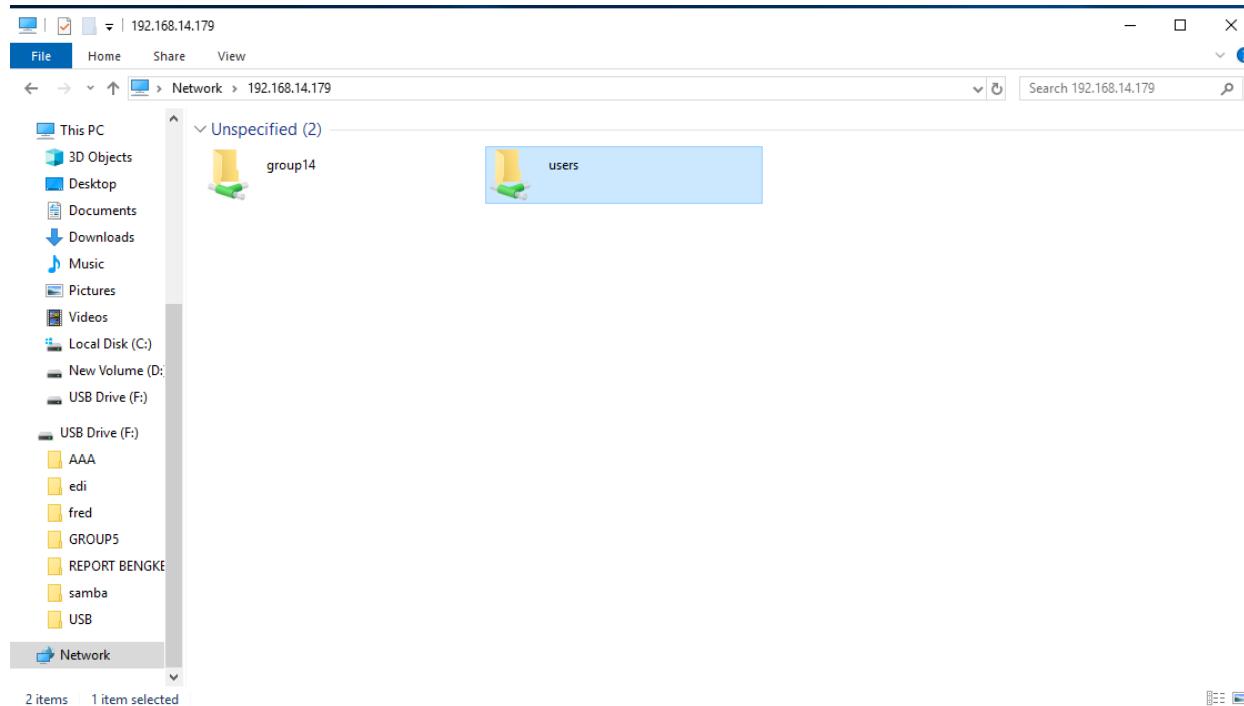


Figure 6.96: Folder shared

### 3. Both folder share in Ubuntu and client can be access

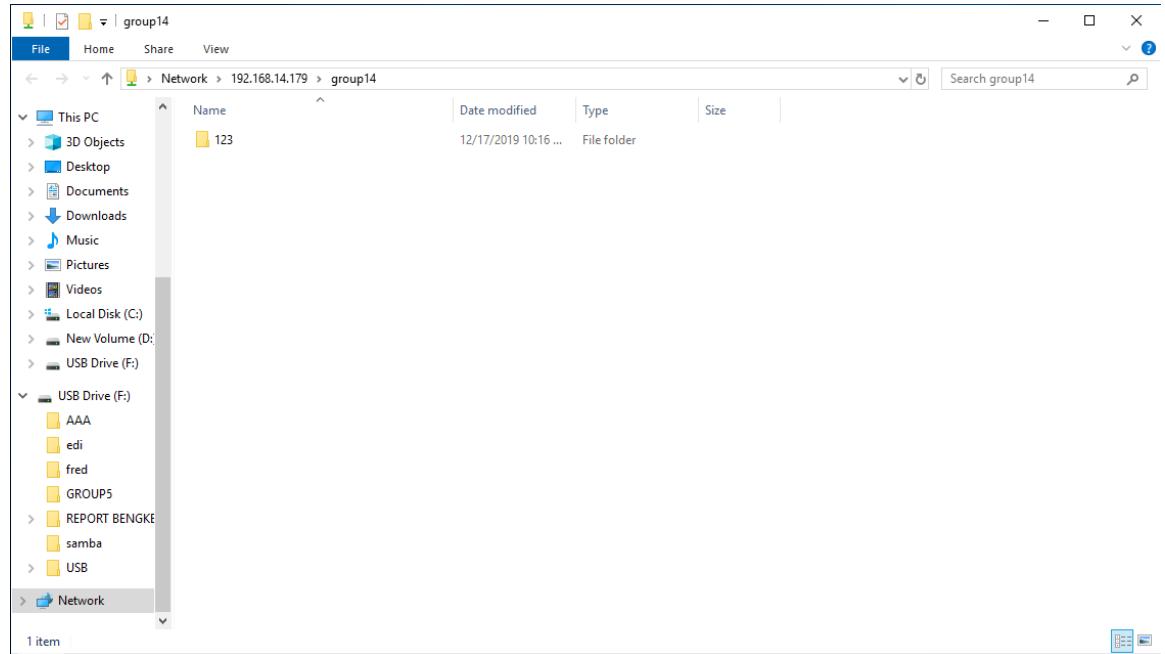


Figure 6.97: Folder that is shared

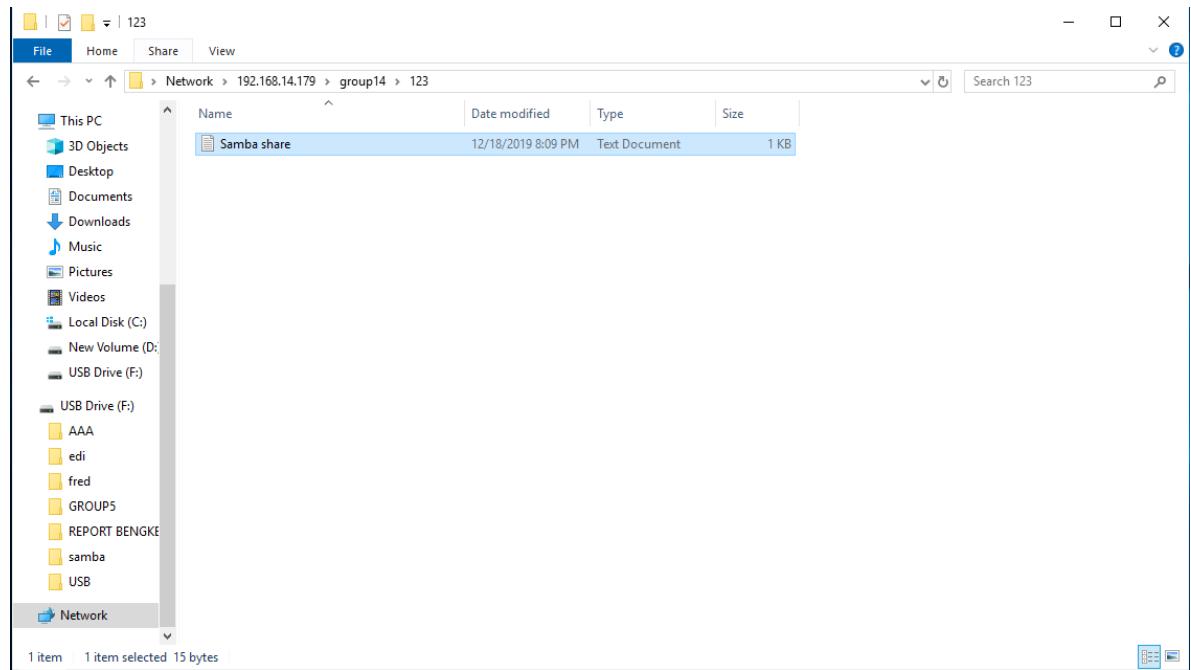


Figure 6.98: Shared Folder

## 6.2.21 LINUX SERVER HARDENING

### 1. Check disable service

```
Starting Nmap 7.60 ( https://nmap.org ) at 2019-12-10 12:23 +08
Initiating SYN Stealth Scan at 12:23
Scanning localhost (127.0.0.1) [1000 ports]
Discovered open port 80/tcp on 127.0.0.1
Discovered open port 445/tcp on 127.0.0.1
Discovered open port 22/tcp on 127.0.0.1
Discovered open port 3306/tcp on 127.0.0.1
Discovered open port 25/tcp on 127.0.0.1
Discovered open port 139/tcp on 127.0.0.1
Discovered open port 1199/tcp on 127.0.0.1
Discovered open port 1099/tcp on 127.0.0.1
Discovered open port 631/tcp on 127.0.0.1
Discovered open port 2008/tcp on 127.0.0.1
Discovered open port 5432/tcp on 127.0.0.1
Discovered open port 3128/tcp on 127.0.0.1
Completed SYN Stealth Scan at 12:23, 1.58s elapsed (1000 total ports)
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000013s latency).
Not shown: 988 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
25/tcp    open  smtp
80/tcp    open  http
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
631/tcp   open  ipp
1099/tcp  open  rmiregistry
1199/tcp  open  dmdi
2008/tcp  open  conf
3128/tcp  open  squid-http
3306/tcp  open  mysql
5432/tcp  open  postgresql

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.67 seconds
Raw packets sent: 1063 (46.772KB) | Rcvd: 2139 (90.062KB)
```

Figure 6.99: Display port that have been disabled

### 2. Check password change

```
root@group14-optiplex-7010:/home/group14# sudo chage -W 14 group14
root@group14-optiplex-7010:/home/group14# sudo chage -l group14
Last password change : Jan 28, 2018
Password expires       : never
Password inactive     : never
Account expires        : never
Minimum number of days between password change : 0
Maximum number of days between password change  : 99999
Number of days of warning before password expires : 14
root@group14-optiplex-7010:/home/group14#
```

Figure 6.100: Display password information

### 3. Check disable bluetooth

```
root@group14-optiplex-7010:/home/group14# systemctl status bluetooth
● bluetooth.service - Bluetooth service
  Loaded: loaded (/lib/systemd/system/bluetooth.service; enabled; vendor preset: enabled)
  Active: inactive (dead)
    Docs: man:bluetoothd(8)
```

Figure 6.101: Disabled bluetooth

#### 6.2.22 IPSEC VPN SERVER FOR REMOTE EMPLOYEES

**STEP 1:** Try to connect your VPN Server from another network. Specify each information and add new VPN Connection Setting.

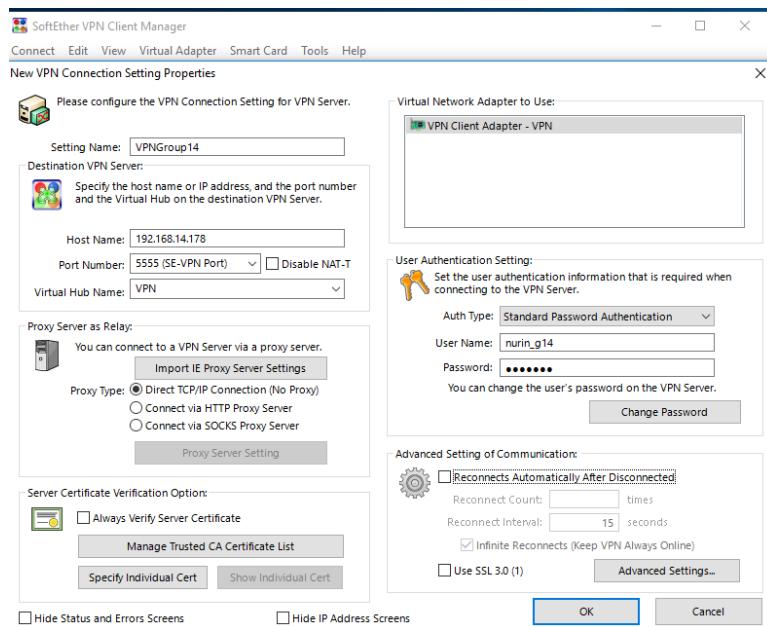
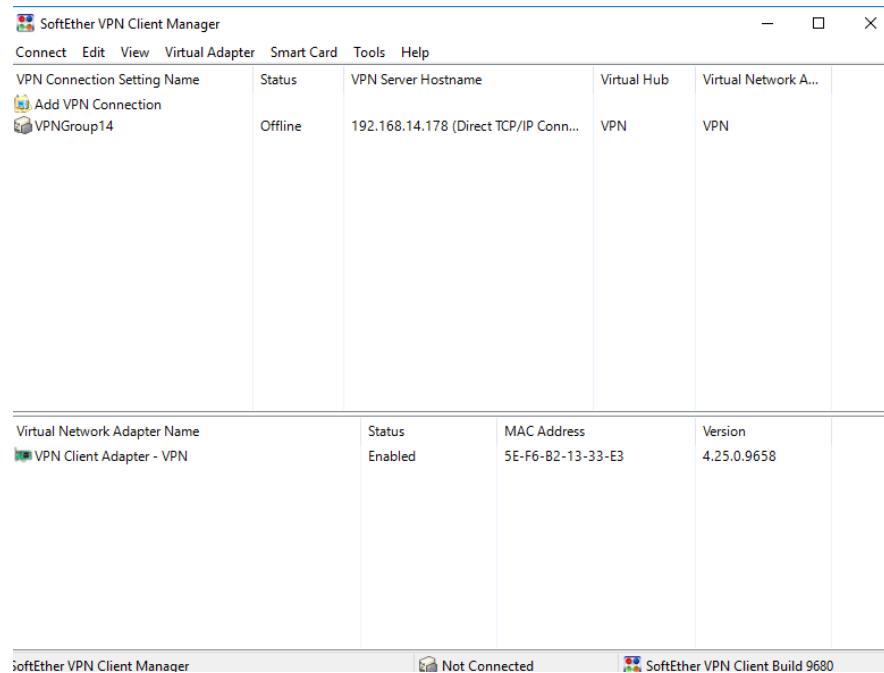


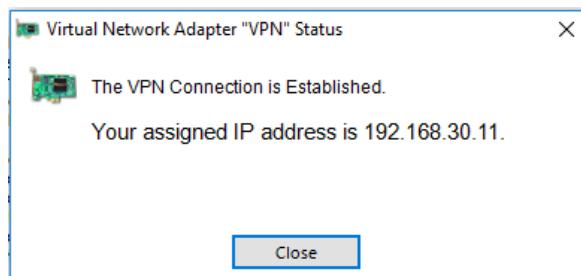
Figure 6.102: Setup the client of remote network

**STEP 3:** The connection is created.



*Figure 6.103: A VPN connection is created.*

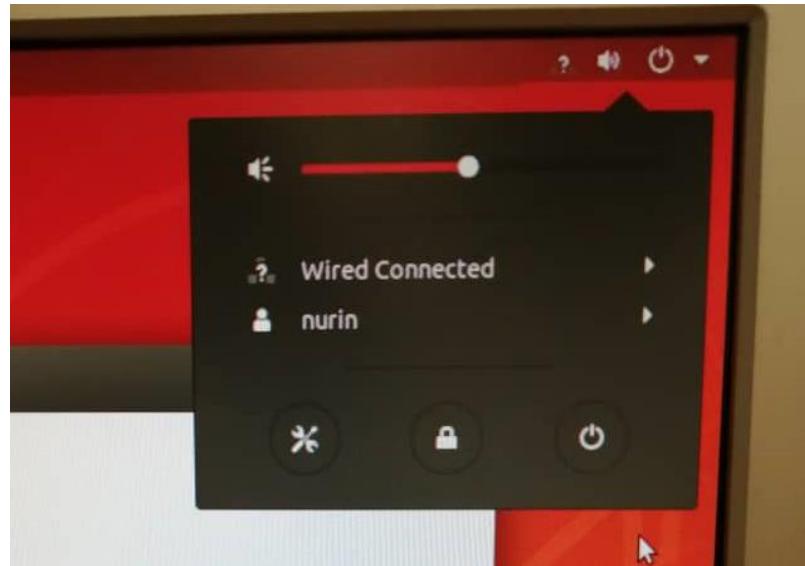
**STEP 4:** Successfully connected.



*Figure 6.104: Success connection*

### **6.2.23 USER AUTHENTICATION BY INTEGRATING AD WITH LINUX**

**STEP 1:** Logout the current user and sign in for the integrated active directory accounts.



*Figure 6.105: Login successful*

### **6.2.24 WINDOWS SERVER HARDENING**

Windows Server is a critical underlying system for Active Directory, database and file servers, business applications, web services and many other important elements of an IT infrastructure. Auditing Windows Server is an absolute must for most organizations.

## 6.2.25 REMOTE LOGIN USING SSH

### 6.2.25.1 Testing SSH in Fedora

**Step 1:** Start the SSH service if it is not started.

```
group14@group14-optiplex-7010:~$ sudo systemctl start ssh
[sudo] password for group14:
```

Figure 6.106: Start SSH

**Step 2:** Login to Debian from Ubuntu and create the file.

```
group14@group14-optiplex-7010:~$ ssh group14@192.168.14.180
group14@192.168.14.180's password:
Linux group14 4.9.0-11-amd64 #1 SMP Debian 4.9.189-3+deb9u2 (2019-11-11) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
You have new mail.
Last login: Wed Nov 27 18:20:25 2019 from 192.168.14.179
group14@group14:~$ ls
Desktop      Templates      opennms-install-1.4
Documents    Videos        opennms-install-master
Downloads   bandicam     zabbix-release_4.0-2+bionic_all.deb
Music       group14.pfx   zabbix-release_4.0-2+bionic_all.deb.1
Pictures    master.zip
Public      opennms-install-1.1
group14@group14:~$ cd Documents/
group14@group14:~/Documents$ mkdir fiqa
group14@group14:~/Documents$ cd fiqa/
group14@group14:~/Documents/fiqa$ touch fiqa.txt
group14@group14:~/Documents/fiqa$ ls -la
total 8
drwxr-xr-x 2 group14 group14 4096 Nov 27 18:34 .
drwxr-xr-x 3 group14 group14 4096 Nov 27 18:33 ..
-rw-r--r-- 1 group14 group14    0 Nov 27 18:34 fiqa.txt
group14@group14:~/Documents/fiqa$
```

Figure 6.107: Login and create files

**Step 3:** Check at Debian whether the file that has been created exist or not.

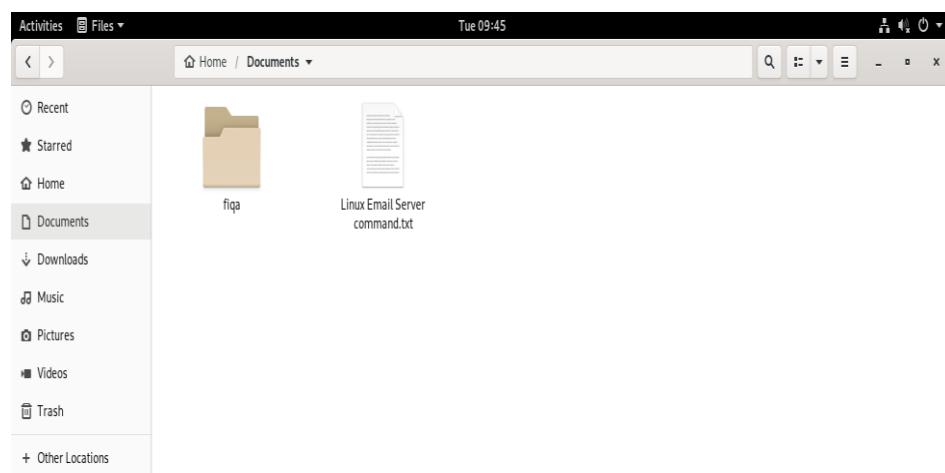


Figure 6.108: Check file at Debian.



Figure 6.109: Check file .txt in fiqa folder

### 6.2.25.2 Testing SSH at Debian

**Step 1:** Start SSH at Debian.

```
group14@group14:~$ sudo systemctl start ssh
[sudo] password for group14:
```

Figure 6.110: start SSH.

**Step 2:** Log in to Ubuntu from Debian.

```
group14@group14:~$ ssh group14@192.168.14.179
The authenticity of host '192.168.14.179 (192.168.14.179)' can't be established.
ECDSA key fingerprint is SHA256:TBwPno04GelobAhREfYZagNLmHtxzCbBRJsYpad8++M.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.14.179' (ECDSA) to the list of known hosts.
Password:
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 5.0.0-37-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

 * Canonical Livepatch is available for installation.
 - Reduce system reboots and improve kernel security. Activate at:
   https://ubuntu.com/livepatch
```

Figure 6.111: Login Ubuntu from Fedora

**Step 3** Create the file at Ubuntu from Debian.

```
Last login: Mon Dec 10 09:47:38 2018
group14@group14-optiplex-7010:~$ cd Desktop
group14@group14-optiplex-7010:~/Desktop$ mkdir Group14
group14@group14-optiplex-7010:~/Desktop$ touch Group14.txt
group14@group14-optiplex-7010:~/Desktop$ exit
logout
Connection to 192.168.14.179 closed.
group14@group14:~$
```

Figure 6.112: Create Ubuntu file from Fedora

**Step 4:** Check whether the file exist or not at the Desktop.



Figure 6.113: Check existing file at Desktop

### 6.2.26 MEDIA SERVER

**Step 1:** Open our Plex media server installation url in the following way, which is <http://localhost:32400/web/> and we will be redirected to the Plex login as below. Then, click the ‘SIGN IN’ button.

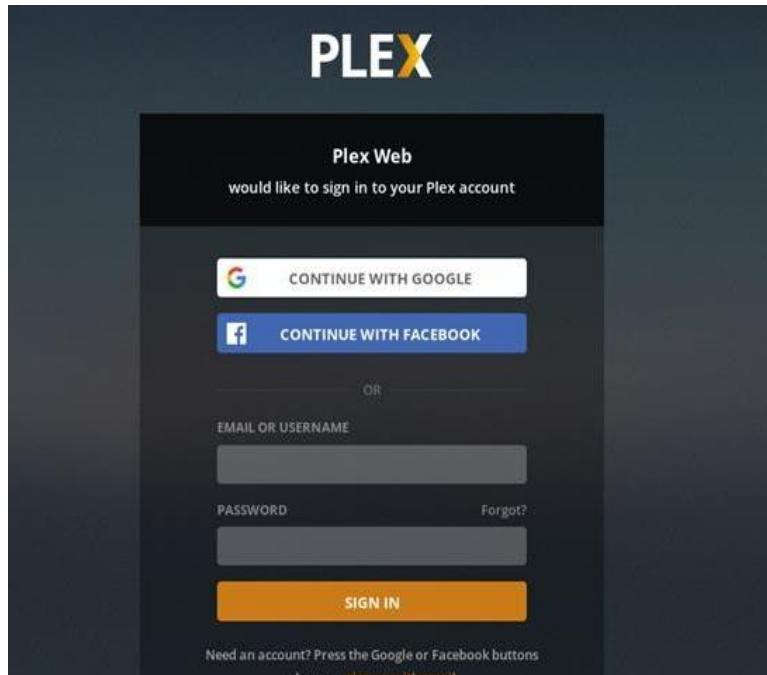


Figure 6.114: Plex Web interface.

**Step 2:** Now, we can add media files to our Plex media server. Click ‘Add library’.

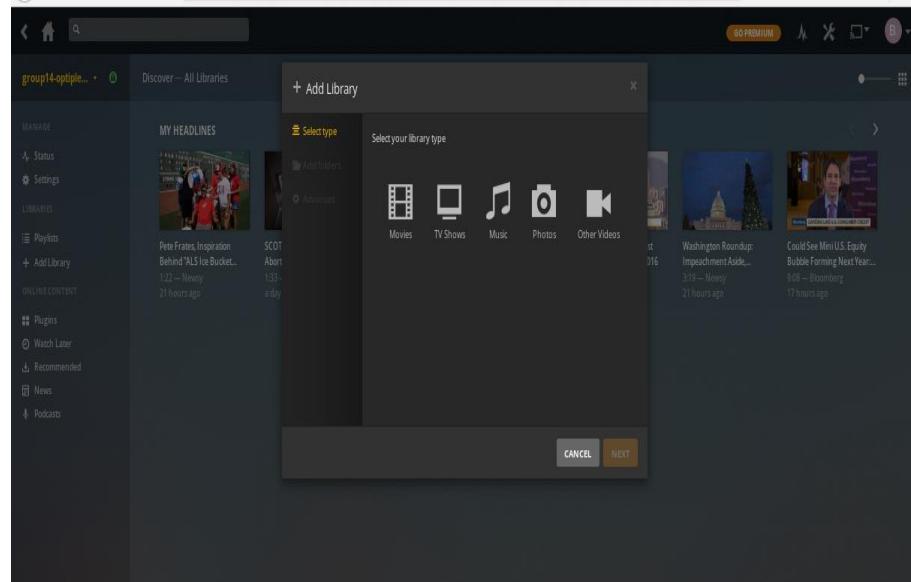


Figure 6.115: Add library for add media files

**Step 3:** Choose media that want to upload and click “**Next**”

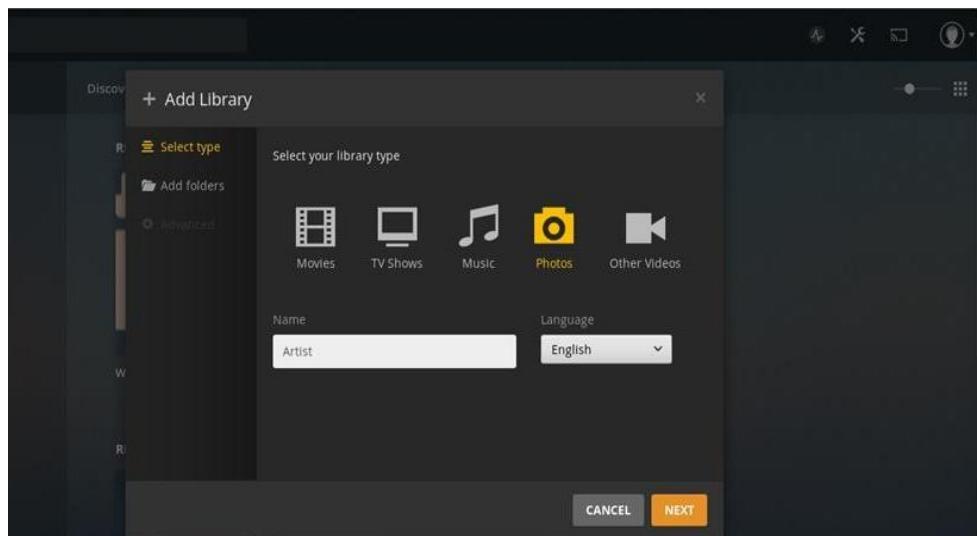


Figure 6.116: Choose media to upload

**Step 4:** Click “*Browse for Media Folder*”

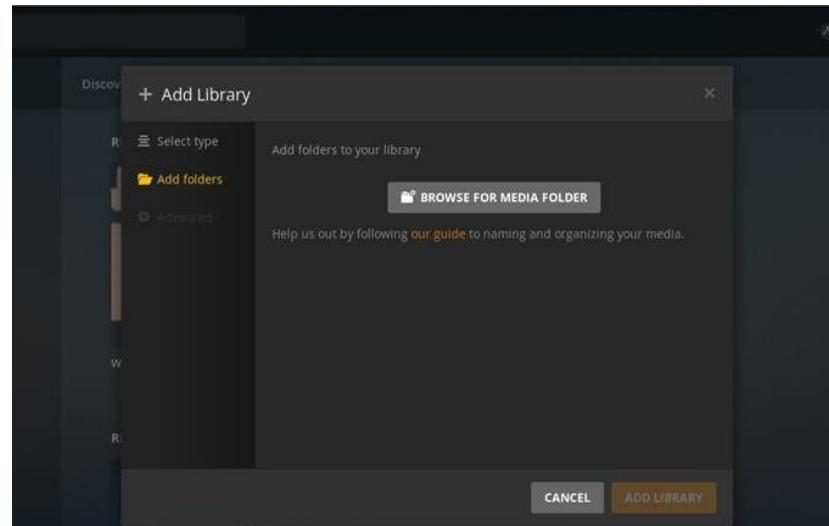


Figure 6.117: *Browse media folder*

**Step 5:** Choose the media and click “*Add*”

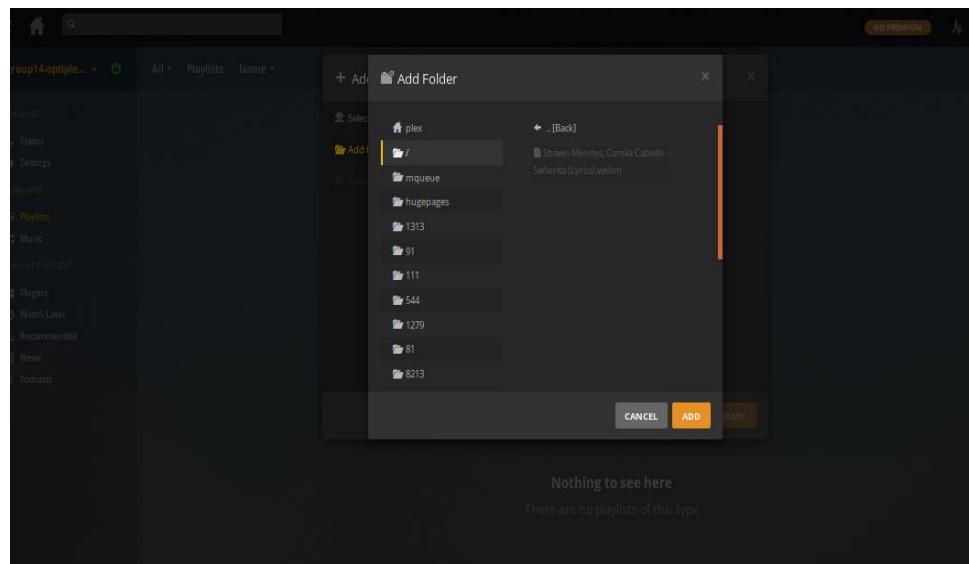


Figure 6.118: *Add the media*

**Step 6:** Last step click “*Add Library*”

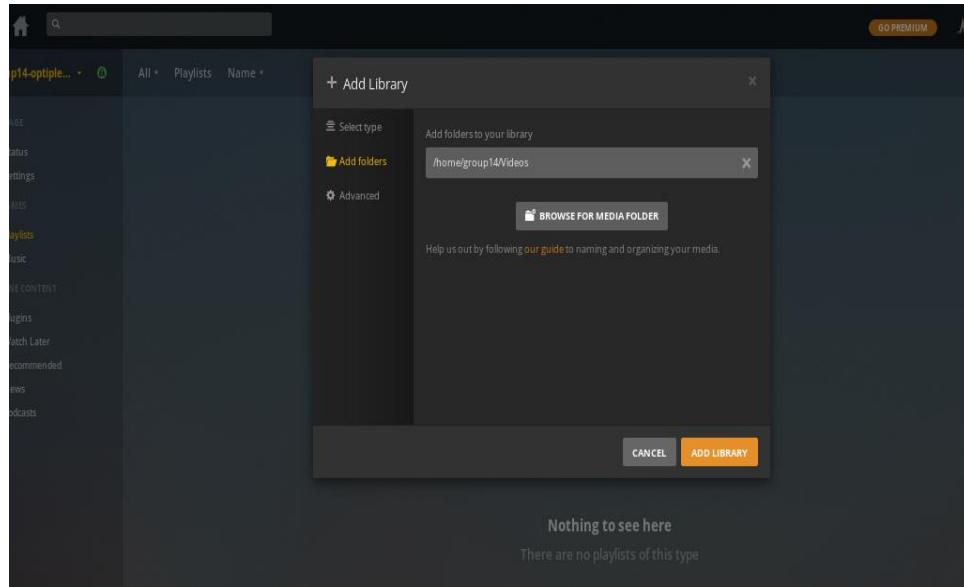


Figure 6.119: *Add Library*

**Step 7:** Photo successfully uploaded.

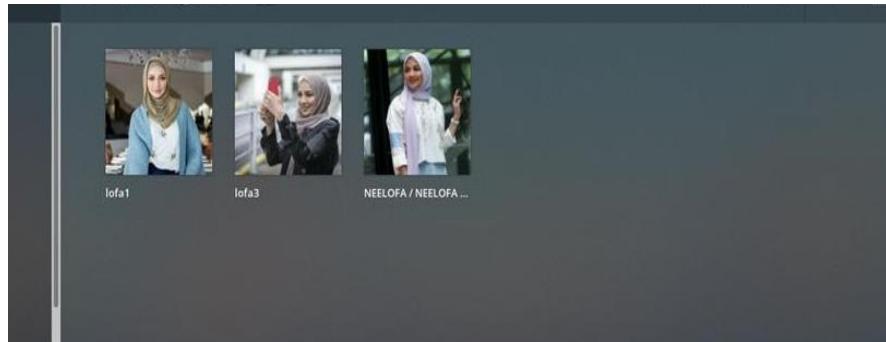


Figure 6.120: *Successfully photo uploaded*

### 6.2.27 ROUTER HARDENING

**Step 1:** Go to PuTTY configuration and under the category > Session, select Logging. At Logging, click on Browse button to save log file.

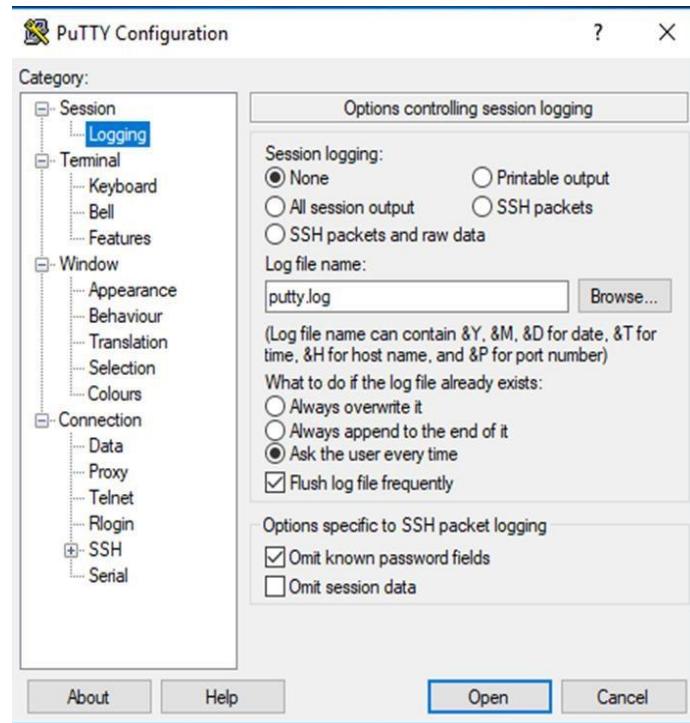


Figure 6.121: Options controlling session logging

**Step 2:** Type the log file name and save it.

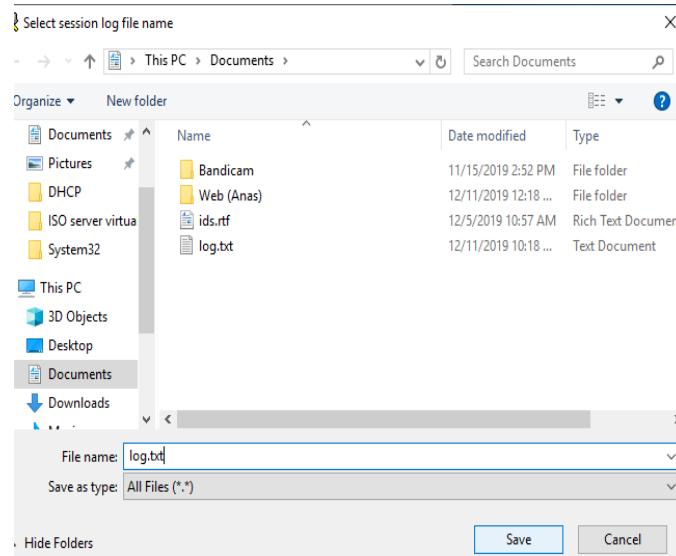


Figure 6.122: save log file name

**Step 3:** Then get into PuTTY and login to router. In the configuration, type something to create log file.

```
#####
#      WELCOME TO WORKSHOP 2      #
#
#          GROUP 14          #
#
#  UNAUTHORIZED USER IS PROHIBITED  #
#####

User Access Verification

Username: admin
Password:

G14Router>en
G14Router#show log
Syslog logging: enabled (0 messages dropped, 3 messages rate-limited, 0 flushes,
0 overruns, xml disabled, filtering disabled)

No Active Message Discriminator.

No Inactive Message Discriminator.

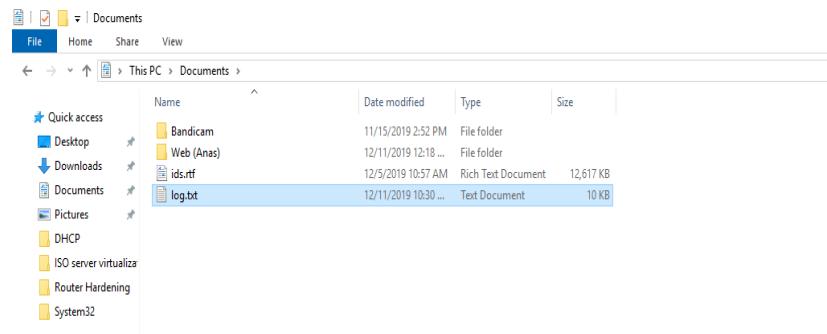
Console logging: disabled
Monitor logging: disabled
Buffer logging: level debugging, 11509 messages logged, xml disabled,
filtering disabled
Exception Logging: size (4096 bytes)
Count and timestamp logging messages: disabled
Persistent logging: disabled

No active filter modules.

Trap logging: level informational, 347 message lines logged
Logging Source-Interface:          VRF Name:
--More--
```

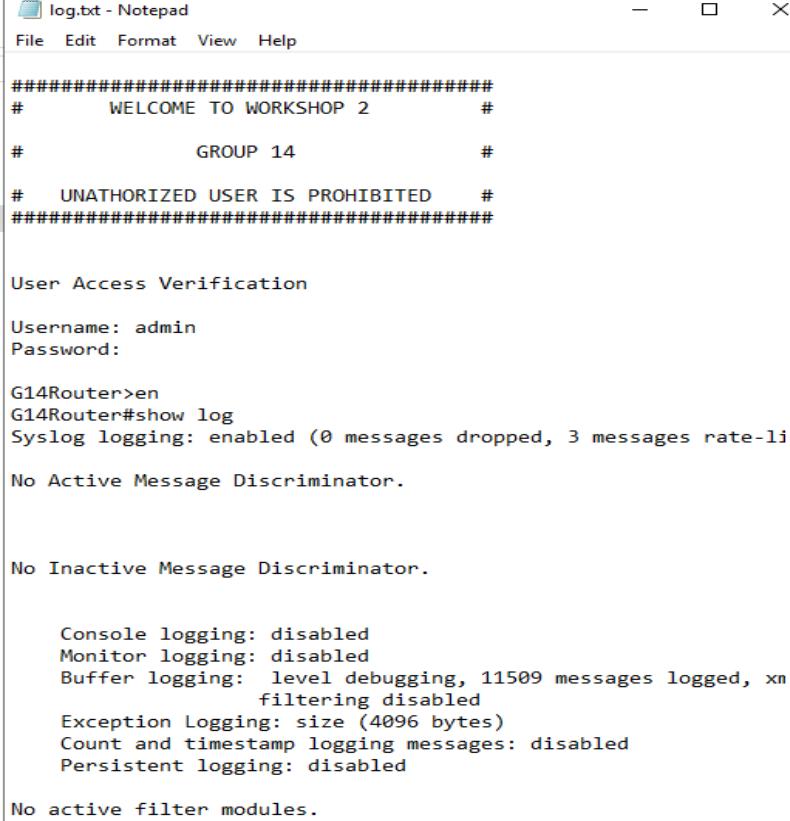
*Figure 6.123: Create log file in router*

**Step 4:** After log file created, exit configuration and go to location that save log file.



*Figure 6.124: Location and save of log file*

**Step 5:** Click the log file and it will show what we do just now in configuration.



The screenshot shows a Notepad window titled "log.txt - Notepad". The content of the log file is as follows:

```
#####
#      WELCOME TO WORKSHOP 2      #
#
#          GROUP 14          #
#
#  UNAUTHORIZED USER IS PROHIBITED  #
#####

User Access Verification

Username: admin
Password:

G14Router>en
G14Router#show log
Syslog logging: enabled (0 messages dropped, 3 messages rate-limited)
No Active Message Discriminator.

No Inactive Message Discriminator.

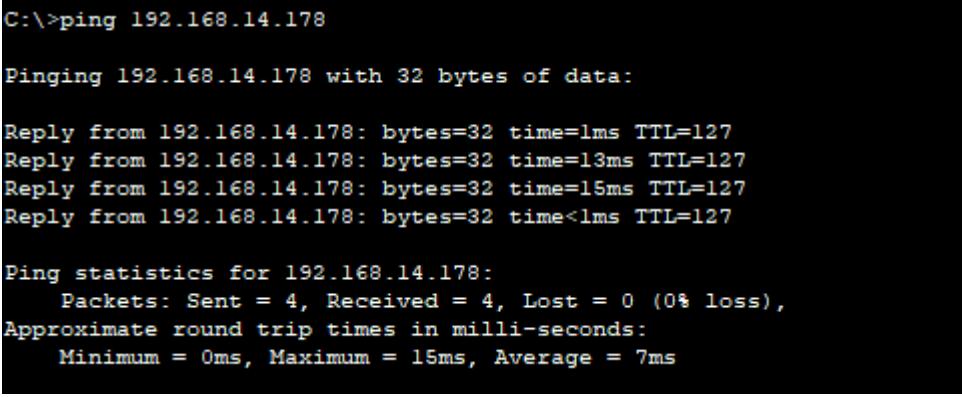
Console logging: disabled
Monitor logging: disabled
Buffer logging: level debugging, 11509 messages logged, xnull filtering disabled
Exception Logging: size (4096 bytes)
Count and timestamp logging messages: disabled
Persistent logging: disabled

No active filter modules.
```

Figure 6.125: Show the configuration of log file

### 6.2.28 INTER VLAN

Step 1: Use command “ping” in cmd to test the connection between VLAN.



The screenshot shows a Command Prompt window with the following output:

```
C:\>ping 192.168.14.178

Pinging 192.168.14.178 with 32 bytes of data:

Reply from 192.168.14.178: bytes=32 time=1ms TTL=127
Reply from 192.168.14.178: bytes=32 time=13ms TTL=127
Reply from 192.168.14.178: bytes=32 time=15ms TTL=127
Reply from 192.168.14.178: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.14.178:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 15ms, Average = 7ms
```

Figure 6.126: Ping from VLAN 20 to VLAN 10

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.14.178

Pinging 192.168.14.178 with 32 bytes of data:

Reply from 192.168.14.178: bytes=32 time=2ms TTL=127
Reply from 192.168.14.178: bytes=32 time=18ms TTL=127
Reply from 192.168.14.178: bytes=32 time=14ms TTL=127
Reply from 192.168.14.178: bytes=32 time=17ms TTL=127

Ping statistics for 192.168.14.178:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 18ms, Average = 12ms
```

Figure 6.127: Ping from VLAN 30 to VLAN 10

## **CHAPTER 7 CONCLUSION**

### **7.0 CONCLUSION**

#### **7.1 Introduction**

Through these numerous weeks, a lot of things have been studied such as method to setup, configure, maintain, and troubleshoot and all of the basic of the services in this Workshop 2. All of the lessons learnt from this Workshop 2 is the prerequisite for industrial training.

To define, implement and manage this Workshop starting from selecting a leader to lead this project from the beginning until the end of the project. The overall performance of this workshop is acceptable. Our group has successfully done all of the services before the due date. Tasks have been distributed equally to each member and a schedule has been created to manage the flow of it. This is very important in managing and organizing every task in order to prevent the error from occurring before the due date.

This network is the combination of network and network security. This network is very suitable for Small and Medium Enterprise Business because it is easy to manage and implement. In this network, all of the basic services and security services are included to maintain and control the network services infrastructure. We are very grateful to gain all of the knowledge and experiences by accomplishing this project as to prepare each and every one of us for the industrial training.

#### **7.2 Project Advantages**

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

1. To design the network infrastructure for this project.
2. Learned to install and configure these services.
3. Learned how to design, monitor, and maintain a simple network.

4. Learned the methods to setup a small and simple network and the ways to manage the hardware like switch and router.
5. Learned to troubleshoot and overcome any problems during setup the services.
6. Know more about the configuration and functions of services that installed in the Windows Server 2019, Debian, Linux Ubuntu.
7. Learned to develop a simple networking system to allow communication between computers in different platform.
8. Increase the communication between network student and security student in developing a good network environment.

### **7.3 Project Disadvantages**

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

1. Lack of knowledge about some of the services done by other group member.
2. Some of the network equipment not in a good condition, it may not work as well as expected.
3. The servers provided to do this project are too old and causing the problems thus complicates the development of the project.
4. The students have to spend much time to setup the network.
5. The lab environment during the night time is very humid because the air condition is turned off and all of the servers are running causing the servers to heat up.

### **7.4 Project Limitation**

These limitations prevent us to maximize the full potential of the project. Due to this limitation, we had to adapt and work harder to succeed. These limitations are:

1. The network only implemented in wired environment.
2. The equipment that provided to each group is not in good condition.

3. The network used in this project is small because it only involves 3 servers which is Windows Server, Ubuntu and Debian. It is not really exposed to large network set ups and management.
4. Do not have chance and opportunity to try and implement any wireless technology.
5. The provided network equipment can only be used to build a small network.

## **7.5 Conclusion**

Upon the completion of this Workshop 2, we are expected to be able to install, configure, set up, monitor and maintain own network given the necessary network equipment's. We will use heterogeneous operating system such as Microsoft Windows Server 2019 Server Enterprise Edition, Ubuntu 14.04.3 and Debian. We also can design our own network and maintain a good network environment.

Moreover, in workshop 2, we learn to setup some security configuration such as server hardening, port security, access control list (ACL), and so forth to enhance the security level of our network and protect the network being access or hack by unauthorized access. To give an opportunity to apply the concept or knowledge that we learned during the lecture such as Local Area Network (LAN), Wide Area Network (WAN), Network analysis and Design, Data Communication and Networking, and so on.

Finally, this project is a very good real world exposure to us and at the end of this project we manage to complete all the tasks given and setup the network successfully. We have learned and understood the services from our supervisor and co-supervisor. We are very grateful and we appreciate our supervisor and co-supervisor for guiding us to a successful workshop completion.

## BIBLIOGRAPHY

Xiao Guo An (July 12, 2018). How to install RainLoop Webmail on Ubuntu

16.04 from <https://www.linuxbabe.com/mail-server/install-rainloop-webmail-ubuntu-16-04>

Rahul (November 27, 2018). How to install Zabbix Agent on Ubuntu 18.04 &

16.04 from <https://tecadmin.net/install-zabbix-agent-on-ubuntu-and-debian/>

ACL configuration from

<https://docs.oracle.com/cd/E19859-01/820-3252-11/FP44ucgACL.html>

About Samba. (n.d.). Retrieved from Samba <https://www.samba.org/samba/>

Active Directory, (June 18) Retrieved from

<https://searchwindowsserver.techtarget.com/definition/Active-Directory>

How to Make Your Website Available Over IPv6, (June 6, 2014) from

<https://www.internetsociety.org/blog/2014/06/how-to-make-your-website-available-over-ipv6/>

Harry, J. (August 20, 2009). "Configure a Cisco Router to use RADIUS for

Authentication." from <http://blog.pluralsight.com/using-radius-for-authentication>

## APPENDIX

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