



## **FAKULTI TEKNOLOGI MAKLUMAT DAN KOMUNIKASI (FTMK)**

**SEMESTER 1 SESI 2020/2021**

**BITU 3923 WORKSHOP II**

**BITC & BITZ**

**FINAL REPORT**

**GROUP NUMBER: 2**

**PREPARED BY:**

NAME	MATRIC NO
AREEF AIMAN BIN ZAINUDDIN	B031810388
AMIRUL HAQIM BIN ZAMRI	B031810155
CHONG ZI QING	B031810174
SYAZA LIYANA BINTI MUHAMAD SHAPEE	B031810345
CHAI ROU SIN	B031810216
THIASAN A/L CHANDRAN	B031810244
HAMIZAH BINTI ROZALI	B031910278

**EVALUATED BY:**

SUPERVISOR	EVALUATOR
DR. NUR FADZILAH BINTI OTHMAN	DR. SHEKH FAISAL BIN ABDUL LATIP
TS. ZAKIAH BINTI AYOP	TS. ERMAN BIN HAMID

## **ACKNOWLEDGEMENT**

First and foremost, we would like to thank our project supervisors, TS. Zakiah binti Ayop and Dr. Nur Fadzilah binti Othman for their valuable guidance and advice that lead us to finish all the services in Workshop 2. Both of them inspired us greatly to work in this project. Their willingness that motivated us have contributed tremendously to our project. We also would like to thank them for answering patiently the question that we asked about the services of project. Besides that, they also taught us that we must think out of the box and from our comfort zone and try to make our service to be great and better. All of this really helped us a lot to complete the implementation of Workshop II. On the other hand, we would also like to thank our evaluator for this workshop, TS. Erman bin Hamid and Dr. Shekh Faisal bin Abdul Latip for taking their time to evaluate us. This evaluation gave us a deeper understanding of our services and what we must add to our service to make it better than we already do.

Moreover, we are also very grateful to the school the authority of Universiti Teknikal Malaysia Melaka (UTeM) for providing us with a good environment and facilities to deal with this project. Finally, an honourable mention goes to our families and friends for their understandings and supports in completing this project. With the help of everyone that are mentioned above, we were able to overcome many problems that occurred in Workshop II and complete our project successfully on time.

## **ABSTRACT**

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

The main objective in this Workshop II project is to be successful to go through the obstacles and challenges in completing the task given. The side objects to have deeper understanding about the service on how it works. We are grateful to experience this as it can help us to prepare for our industrial training as well as acquire the skills that will be needed in our future careers.

Our group had decided to use Window Server R2 in server 1 (Window) and Lubuntu in server 2. We choose this server operating system because it has many benefits. Our group also was assigned to set up 18 services listed. The 18 services listed are Network Management System, AAA (Authentication, Authorization, Accounting) using Radius, Linux Email Server, IPsec site-to-site tunneling, Active Directory, DNS (IPv4 and IPv6), DHCP (IPv4 and IPv6), Access Control List, Web, SSL and Virtual Hosting, Routing and Network Address Translation (NAT), IPsec VPN Server for remote employees, Samba Security Services, IDS Port Mirroring, Linux Server Hardening, Windows Server Hardening, User authentication by integrating Active Directory with Linux, Layer 2 Security (VLAN Security and Port Security) and Audit Compliance.

During the Workshop II, we faced many problems, but we still managed to overcome them and complete this project successful.

## **ABSTRAK**

Dalam projek Bengkel II ini, kita perlu menentukan, melaksanakan dan mengurus tugas-tugas yang telah diberikan. Tugasan ini bermula dari memilih pemimpin untuk mengetahui projek ini dari awal hingga akhir projek ini. Setiap ahli kumpulan telah dibahagikan dengan tugasan secara sama rata dan jadual tugasan juga dihasilkan untuk memastikan kami dapat menyelesaikannya pada masa yang ditetapkan. Ini adalah sangat penting untuk mengurus dan menganjurkan setiap tugas untuk mengelakkan sebarang masalah dan kesilapan di penhujung projek.

Objektif utama kami dalam projek Bengkel II ini adalah dapat mengatasi halangan dan cabaran yang dihadapi dalam proses ini supaya kami berjaya melaksanakan projek ini. Selain itu, objectif projek ini adalah membolehkan kami memahami lebih mendalam mengenai perkhidmatan, bagaimana ia berfungsi. Kami bersyukur kerana mendapat peluang ini untuk menyertai projek ini kerana pengalaman ini akan membantu kami bersedia untuk latihan perindustrian dan memperoleh kemahiran yang diperlui dalam pekerjaan masa depan kami.

Sistem operasi yang digunakan adalah Window Server R2 di pelayan 1 (Tetingkap) dan Lubuntu di pelayan 2. Kami memilih sistem operasi pelayan ini kerana ia mempunyai banyak manfaat. Tugasan untuk kumpulan kami adalah melaksanakan 18 perkhidmatan yang dalam rangkaian kami. Antara 18 perkhidmatan termasuk adalah Network Management System, AAA (Authentication, Authorization, Accounting) using Radius, Linux Email Server, IPsec site-to-site tunneling, Active Directory, DNS (IPv4 and IPv6), DHCP (IPv4 and IPv6), Access Control List, Web, SSL and Virtual Hosting, Routing and Network Address Translation (NAT), IPsec VPN Server for remote employees, Samba Security Services, IDS Port Mirroring, Linux Server Hardening, Windows Server Hardening, User authentication by integrating Active Directory with Linux, Layer 2 Security (VLAN Security and Port Security) and Audit Compliance.

Semasa melaksanakan projek Bengkel II, kami menghadapi kebanyakan masalah tetapi masih dapat mengatasinya dan berjaya menyelesaikan projek ini.

## Table of Contents

.....	1
<b>ACKNOWLEDGEMENT</b> .....	2
<b>ABSTRACT</b> .....	3
<b>ABSTRAK</b> .....	4
<b>CHAPTER 1: INTRODUCTION</b> .....	19
<b>1.1 INTRODUCTION</b> .....	19
<b>1.2 OBJECTIVE</b> .....	20
<b>1.3 PROJECT PLANNING / SCHEDULE</b> .....	20
<b>1.3.1 GANTT CHART FOR PROJECT PLANNING</b> .....	21
<b>1.4 CONCLUSION</b> .....	22
<b>CHAPTER 2: PROJECT REQUIREMENT</b> .....	23
<b>2.1 INTRODUCTION</b> .....	23
<b>2.2 TYPES OF OPERATING SYSTEM</b> .....	23
<b>2.2.1 Windows Server 2012</b> .....	23
<b>2.2.2 Lubuntu 18.04 LTS</b> .....	25
<b>2.3 CONCLUSION</b> .....	25
<b>CHAPTER 3: DESIGN</b> .....	26
<b>3.1 INTRODUCTION</b> .....	26
<b>3.2 SECURITY POLICY</b> .....	26
<b>3.2.1 Introduction</b> .....	26
<b>3.2.2 Objective</b> .....	26
<b>3.2.3 Password Protection Policy</b> .....	26
<b>3.2.4 Remote Access Policy</b> .....	27
<b>3.2.5 Server Security Policy</b> .....	27
<b>3.2.6 Router and Switch Security Policy</b> .....	29
<b>3.2.7 Email Policy</b> .....	30
<b>3.3 PHYSICAL DESIGN</b> .....	31
<b>3.4 LOGICAL DESIGN</b> .....	32
<b>3.5 VLAN AND VLSM ADDRESSING</b> .....	33
<b>3.5.1 VLAN ADDRESSING</b> .....	33
<b>3.5.2 IP ADDRESSING FOR DEVICE</b> .....	33
<b>3.6 CONCLUSION</b> .....	34
<b>CHAPTER 4: SERVICES</b> .....	35
<b>4.1 INTRODUCTION</b> .....	35

<b>4.2</b>	<b>TYPE OF SOFTWARE.....</b>	35
<b>4.2.1</b>	<b>LIST OF OPERATING SYSTEMS .....</b>	35
<b>4.2.2</b>	<b>LIST OF SERVICES .....</b>	35
<b>4.3</b>	<b>BRIEF OVERVIEW OF SERVICES .....</b>	36
<b>4.4</b>	<b>CONCLUSION .....</b>	42
<b>CHAPTER 5: INSTALLATION AND CONFIGURATION .....</b>		43
<b>5.1</b>	<b>INTRODUCTION.....</b>	43
<b>5.2</b>	<b>SERVICES AND CORRESPONDING PERSON IN CHARGE .....</b>	43
<b>5.3</b>	<b>SERVICE INSTALLATION AND CONFIGURATION.....</b>	45
<b>5.3.1</b>	<b>ACTIVE DIRECTORY.....</b>	45
<b>5.3.2</b>	<b>DHCP IPv4 &amp; IPV6 .....</b>	53
<b>5.3.3</b>	<b>DYNAMIC ROUTING &amp; NAT .....</b>	64
<b>5.3.4</b>	<b>IPSEC SITE-TO-SITE TUNNELING .....</b>	66
<b>5.3.5</b>	<b>ACCESS CONTROL LIST.....</b>	67
<b>5.3.6</b>	<b>DOMAIN NAME SYSTEM.....</b>	68
<b>5.3.7</b>	<b>LINUX EMAIL SERVER .....</b>	75
<b>5.3.8</b>	<b>WEB, SSL &amp; VIRTUAL HOSTING.....</b>	89
<b>5.3.9</b>	<b>NETWORK MONITORING SYSTEM .....</b>	130
<b>5.3.10</b>	<b>AAA (AUTHENTICATION AUTHORIZATION AND ACCOUNTING) USING RADIUS</b>	134
<b>5.3.11</b>	<b>VLAN &amp; PORT SECURITY .....</b>	163
<b>5.3.12</b>	<b>IDS WITH PORT MIRRORING .....</b>	165
<b>5.3.13</b>	<b>SAMBA .....</b>	173
<b>5.3.14</b>	<b>LINUX SERVER HARDENING.....</b>	181
<b>5.3.15</b>	<b>IPSEC VPN SERVER .....</b>	191
<b>5.3.16</b>	<b>USER AUTHENTICATION BY INTEGRATING AD WITH LINUX .....</b>	220
<b>5.3.17</b>	<b>WINDOWS SERVER HARDENING .....</b>	231
<b>CHAPTER 6: TESTING .....</b>		245
<b>6.1</b>	<b>INTRODUCTION.....</b>	245
<b>6.2</b>	<b>SERVICES TESTING .....</b>	245
<b>6.2.1</b>	<b>ACTIVE DIRECTORY.....</b>	245
<b>6.2.2</b>	<b>DHCP IPv4 &amp; IPV6 .....</b>	249
<b>6.2.3</b>	<b>DYNAMIC ROUTING &amp; NAT .....</b>	250
<b>6.2.4</b>	<b>IPSEC SITE-TO-SITE TUNNELING .....</b>	251
<b>6.2.5</b>	<b>ACCESS CONTROL LIST.....</b>	253
<b>6.2.6</b>	<b>DOMAIN NAME SYSTEM.....</b>	254

<b>6.2.7</b>	<b>LINUX EMAIL SERVER .....</b>	256
<b>6.2.8</b>	<b>WEB, SSL &amp; VIRTUAL HOSTING .....</b>	260
<b>6.2.9</b>	<b>NETWORK MONITORING SYSTEM .....</b>	262
<b>6.2.10</b>	<b>AAA (AUTHENTICATION AUTHORIZATION AND ACCOUNTING) USING RADIUS</b>	265
<b>6.2.11</b>	<b>LAYER 2 SECURITY VLAN &amp; PORT SECURITY .....</b>	267
<b>6.2.12</b>	<b>IDS WITH PORT MIRRORING .....</b>	269
<b>6.2.13</b>	<b>SAMBA AND SAMBA SECURITY SERVICES.....</b>	271
<b>6.2.14</b>	<b>LINUX SERVER HARDENING AND VULNERABILITY REPORT .....</b>	277
<b>6.2.15</b>	<b>IPSEC VPN SERVER FOR REMOTE EMPLOYEES .....</b>	281
<b>6.2.16</b>	<b>USER AUTHENTICATION BY INTEGRATING AD WITH LINUX .....</b>	285
<b>6.2.17</b>	<b>WINDOWS SERVER HARDENING AND VULNERABILITY REPORT .....</b>	288
<b>6.3</b>	<b>CONCLUSION .....</b>	291
<b>CHAPTER 7: CONCLUSION.....</b>		292
<b>7.1</b>	<b>INTRODUCTION.....</b>	292
<b>7.2</b>	<b>PROJECT ADVANTAGES .....</b>	292
<b>7.3</b>	<b>PROJECT DISADVANTAGES .....</b>	293
<b>7.4</b>	<b>PROJECT LIMITATION.....</b>	293
<b>7.5</b>	<b>CONCLUSION .....</b>	294
<b>APPENDIX A .....</b>		296
<b>APPENDIX B .....</b>		301
<b>APPENDIX C .....</b>		304
<b>AUDIT CHECK LIST .....</b>		304
<b>APPENDIX D .....</b>		313

## LIST OF FIGURES

Figure 1 : Physical Design .....	31
Figure 2 : Logical Design .....	32
Figure 3 Add Roles & Features Wizard.....	45
Figure 4 Select Server Role .....	45
Figure 5 AD Domain Server .....	46
Figure 6 Deployment Configuration .....	46
Figure 7 Active Directory Users .....	47
Figure 8 New Object – Use.....	48
Figure 9 Password & Confirm Password.....	48
Figure 10 Information Before Create.....	49
Figure 11 Add To a Group.....	49
Figure 12 Select Groups.....	50
Figure 13 ADDS message.....	50
Figure 14 Group Policy Management.....	51
Figure 15 Group Policy Management Editor.....	51
Figure 16 Policy Created .....	52
Figure 17 gpupdate Force .....	52
Figure 18 Dashboard.....	53
Figure 19 Add Roles & Features .....	54
Figure 20 Installation Type.....	54
Figure 21 Server Selection.....	55
Figure 22 Server Roles.....	55
Figure 23 Dashboard.....	56
Figure 24 New Scope.....	56
Figure 25 New Scope.....	57
Figure 26 Scope Name.....	57
Figure 27 IP Address Range .....	58
Figure 28 Exclusions.....	58
Figure 29 Lease Duration.....	59
Figure 30 Router Gateway .....	59
Figure 31 New Scope.....	60
Figure 32 Restart service .....	60
Figure 33 New Scope.....	61
Figure 34 New Scope.....	61
Figure 35 New Scope.....	62
Figure 36 Scope Prefix.....	62
Figure 37 Exclusion .....	63
Figure 38 New Scope.....	63
Figure 39 Router BGP and Router-ID .....	64
Figure 40 Network address .....	64
Figure 41: Set IP Address to neighbor router and Set IP NAT Outside .....	64
Figure 42: Set the static NAT public IP.....	64

Figure 43:Assign all VLANs under IP NAT inside .....	65
Figure 44:Create an ISAKMP phase 1 policy.....	66
Figure 45:Create the transform set.....	66
Figure 46:Set a source and destination address .....	66
Figure 47:Set a route.....	66
Figure 48:Deny the port .....	67
Figure 49:Configure the access-group .....	67
Figure 50>Create new DNS using wizard. ....	68
Figure 51:Configure a DNS action .....	68
Figure 52:Enter the zone name .....	69
Figure 53:Allow both non-secure and secure dynamic updates.....	69
Figure 54:Result of DNS configuration .....	70
Figure 55:Select IPv4 Reverse Lookup Zone .....	70
Figure 56:Enter Network ID .....	71
Figure 57:Select allow both non-secure and secure dynamic updates .....	71
Figure 58:Completed New Zone Wizard.....	72
Figure 59:Enter the Name and IP address.....	73
Figure 60:Select IPv6 Reverse Lookup Zone .....	73
Figure 61: Enter IPv6 Address Prefix .....	74
Figure 62:Create new pointer for reverse lookup IPv6.....	74
Figure 63: Updating apt .....	75
Figure 64: Installation of apache2 php7.2.....	75
Figure 65: Installation of libapache2-mod-php.....	76
Figure 66: Creating SSL certificate (Part 1) .....	76
Figure 67: Creating SSL certificate (Part 2) .....	77
Figure 70: Choosing Internet Site .....	78
Figure 71: Adding domain for mail.group2.com .....	79
Figure 72: Configuring Root and Postmaster Mail Recipient.....	79
Figure 73: Adding domain for email server that is capable of accepting the emails .....	80
Figure 76: Edit and add the codes in main.cf (Part 2).....	81
Figure 77: Edit and add the codes in main.cf (Part 2).....	82
Figure 78: Installing Dovecot for imap or pop3 .....	82
Figure 79: Configuring dovecot.conf (Part 1).....	83
Figure 80: Configuring dovecot.conf (Part 1).....	83
Figure 81: Configuring 10-master.conf file .....	84
Figure 82: Configuring 10-ssl.conf file.....	85
Figure 83: Checking the ports in netstat (Part 1) .....	86
Figure 84: Checking the ports in netstat (Part 2) .....	86
Figure 85: Adding a new user account.....	87
Figure 86: Install Rainloop Webmail.....	87
Figure 87: Login to Rainloop admin web interface .....	88
Figure 88: Configuring Domain name settings.....	88
Figure 89: Add role and features in server.....	89
Figure 90: Select Role-based or Feature-based Installation.....	89
Figure 91: Select Role-based or Feature-based Installation.....	90

Figure 92: Select Web Server (IIS).....	90
Figure 93: Add Roles and Features wizard.....	91
Figure 94: Keep clicking next until reaching to confirmation page.....	91
Figure 95: Installing conformation .....	92
Figure 96: Installation completed .....	92
Figure 97: Adding new website at IIS manager.....	93
Figure 98: Installing progress .....	93
Figure 99: Creating group2 directory with the group2.html file.....	94
Figure 100: Add new Default Document.....	94
Figure 101: Default html file for group2.com.....	95
Figure 102: Role-based or Feature-based Installation .....	96
Figure 103: Select Role-based or Feature-based Installation.....	96
Figure 104: Active Directory Certificate Services.....	97
Figure 105: Active Directory Certificate Services.....	97
Figure 106: Keep clicking next until reaching to confirmation page.....	98
Figure 107: Tick Certification Authority and Certificate Enrollment Policy Web Service.....	98
Figure 108: Installing conformation .....	99
Figure 109: Installation completed .....	99
Figure 110: AD CS Showing a warning message.....	100
Figure 111: Click “Configure Active Directory Certificate Services” .....	100
Figure 112: Credentials of AD CS .....	101
Figure 113: Select Certificate Enrollment Policy Web Service.....	101
Figure 114: Click Windows integrated authentication.....	102
Figure 115: AD CS configuration confirmation .....	102
Figure 116: Result tab.....	103
Figure 117: Select Certification Authority.....	103
Figure 118: Select Enterprise CA .....	104
Figure 119: Select RAS#Microsoft Software Key Storage Provider, SHA1 with key length 2048 .....	104
Figure 120: Specify the name of the CA.....	105
Figure 121: Specify the validity period.....	105
Figure 122: Specify the validity period.....	106
Figure 123: Confirmation tab for AD CS .....	106
Figure 124: Result tab for AD CS.....	107
Figure 125: Server Certificates .....	107
Figure 126: Create Domain Certificates .....	108
Figure 127: Fill in information for certificate .....	108
Figure 128: Select Online Certification Authority & fill in the Friendly name.....	109
Figure 129: List of Certificate.....	109
Figure 130: Add site binding for SSL.....	110
Figure 131: SSL settings.....	110
Figure 132: SSL Settings .....	111
Figure 133: Adding new website at IIS manager.....	112
Figure 134: Add new website .....	112
Figure 135: Creating vhgroup2 directory with the vhgroup2.html file.....	113
Figure 136: Add new Default Document.....	113

Figure 137: Default html file for vhgroup2.com.....	114
Figure 138: Creating new zone .....	114
Figure 139: Create new zone in forward lockup zones in DNS manager .....	115
Figure 140: Choosing primary zone.....	115
Figure 141: Choosing domain:group2.com in wizard for Web .....	116
Figure 142: Creating new zone name .....	116
Figure 143: Choosing dynamic update .....	117
Figure 144: Completing the New Zone wizard.....	117
Figure 145: Adding host .....	118
Figure 146: Entering ip address in new host.....	118
Figure 147: Host created.....	119
Figure 148: Click File and select Add/ Remove Snap-in.....	119
Figure 149: Select Certificates and click Add .....	120
Figure 150: Choose My user account .....	120
Figure 151: Selected Snap-ins .....	121
Figure 152: Export the certificate that want to trust .....	121
Figure 153: Certificate Export Wizard.....	122
Figure 154: Export file format .....	122
Figure 155: Name of the exported file .....	123
Figure 156: Completing the certificate export wizard .....	123
Figure 157: Export was successful.....	124
Figure 158: Creating SharedCert folder.....	124
Figure 159: Move the exported certificate to the SharedCert folder.....	125
Figure 160: Create a GPO in this group2.com.....	125
Figure 161: TrustSSLCert as name of new GPO .....	126
Figure 162: Windows Settings of policy.....	126
Figure 163: Security settings of Windows settings.....	127
Figure 164: Selecting Trusted Root Certification Authorities in security settings .....	127
Figure 165: Selecting import .....	128
Figure 166: Specify the file want to export.....	128
Figure 167: completing the certificate import wizard.....	129
Figure 168 apt update.....	130
Figure 169 Installing Nagios .....	130
Figure 170 Installing Apache .....	130
Figure 171 Start the Apache .....	130
Figure 172 Downloading Nagios Core archive .....	131
Figure 173Extracting the file .....	131
Figure 174 Run the configure file.....	131
Figure 175 Starting the compilation .....	131
Figure 176 Creating user & group.....	131
Figure 177 Installing configuration file .....	131
Figure 178 Configure permission.....	131
Figure 179 Configuration for web interfaces .....	131
Figure 180 Enable Apache.....	132
Figure 181 Setup authentication .....	132

Figure 182 Setting ownership .....	132
Figure 183 Restart Apache.....	132
Figure 184 Starting Nagios.....	132
Figure 185 Installing Nagios plugins.....	133
Figure 186 Frontend interface .....	133
Figure 187: Creating new group .....	134
Figure 188: Filling in the name of the new group.....	134
Figure 189: Adding user to a group .....	135
Figure 190: Selecting group.....	135
Figure 191: Domain Admins are the member of wkspgroup2.....	136
Figure 192: Server Manager .....	136
Figure 193: Add Roles and Features.....	137
Figure 194: Selection installation type.....	137
Figure 195: Add destination server .....	138
Figure 196: Selecting Network Policy and Access Services .....	138
Figure 197: Selecting features.....	139
Figure 198: Overview of Network Policy and Access Services .....	139
Figure 199: Selecting Network Policy Server.....	140
Figure 200: Confirm installation selections .....	140
Figure 201: Complete installation process.....	141
Figure 202: Navigate to Network Policy Server .....	141
Figure 203: Register servers in Active Directory .....	142
Figure 204: Adding Radius Client .....	142
Figure 205: Creating a new Radius Client .....	143
Figure 206: Selecting vendor name of the Radius Client in Advanced tab .....	143
Figure 207: Selecting Cisco as the vendor name .....	144
Figure 208: Complete creating a Radius Client .....	144
Figure 209: Creating a new Connection Request Policy .....	145
Figure 210: Filling in policy name.....	145
Figure 211: Selecting a condition .....	146
Figure 212: Filling in Client Friendly Name .....	146
Figure 213: Authentication setting of Specify Connection Request Forwarding .....	147
Figure 214: Continue with default setting.....	147
Figure 215: Continue with default setting.....	148
Figure 216: Overview of the connection request policy .....	148
Figure 217: Successfully create Connection Request Policy .....	149
Figure 218: Creating Network Policy .....	149
Figure 219: Filling in Network Policy name .....	150
Figure 220: Adding a new condition.....	150
Figure 221: Selecting a condition .....	151
Figure 222: Adding user groups.....	151
Figure 223: Selecting group.....	152
Figure 224: Successfully adding a condition .....	152
Figure 225: Selecting Access granted.....	153
Figure 226: Selecting less secure authentication methods.....	153

Figure 227: Continue with default setting.....	154
Figure 228: Deleting Framed-Protocol PPP at Standard attribute .....	154
Figure 229: Editing Service-Type on Standard attribute .....	155
Figure 230: Select Login at Attribute information.....	155
Figure 231: Adding Vendor Specification .....	156
Figure 232: Adding Vendor specific Attribute .....	156
Figure 233: Adding Vendor Attribute information.....	157
Figure 234: Filling in Vendor Specification .....	157
Figure 235: Overview of a New Network Policy.....	158
Figure 236: Successful create a New Network Policy .....	158
Figure 237: Configure Accounting in Network Policy Server.....	159
Figure 238: Introduction in Accounting configuration .....	159
Figure 239: Select Accounting option .....	160
Figure 240: Configure file logging .....	160
Figure 241: Summary page for Accounting Configuration .....	161
Figure 242: Conclusion Page for Accounting Configuration .....	161
Figure 243: Configuration in putty for aaa new model, Authentication & Authorization.....	162
Figure 244: Configuration in putty for Accounting .....	162
Figure 245: Assign Port to VLAN .....	163
Figure 246: Change status.....	163
Figure 247: Show VLAN.....	163
Figure 248: Configure Port for Windows Server.....	164
Figure 249: Configure Port for Ubuntu Server .....	164
Figure 250: Install all tools .....	165
Figure 251: Install all Installing libpcre3-dev .....	165
Figure 252: Installing zlib1g-dev .....	165
Figure 253: Installing bison flex .....	165
Figure 254: Make and change directory .....	165
Figure 255: Download DAQ.....	166
Figure 256: Extract file .....	166
Figure 257: Configure, make & make install command .....	166
Figure 258: Installing Snort latest version .....	166
Figure 259: Extract file .....	167
Figure 260: Enabling sourcefire.....	167
Figure 261: Updating libraries .....	167
Figure 262: Creating user and group.....	167
Figure 263: Creating folder.....	167
Figure 264: Creating folder in rules .....	168
Figure 265: Creating list and change permission.....	168
Figure 266: Copying configuration.....	168
Figure 267: Verify Snort.....	168
Figure 268: Protected IP .....	169
Figure 269: Modifying path to rules .....	169
Figure 270: Output Snort to log file.....	170
Figure 271: Uncomment any rules available .....	170

Figure 272: Output testing snort .....	171
Figure 273: Inserting rules .....	171
Figure 274: Verify the monitor session has created.....	172
Figure 275: Show status port .....	172
Figure 276 : Update the server.....	173
Figure 277 : Upgrade the server.....	173
Figure 278 : Installation of samba and some packages in Lubuntu .....	174
Figure 279 : Addition of new user for samba service .....	174
Figure 280 : Create a samba account .....	175
Figure 281 : Enable the samba service.....	175
Figure 282 : Restart the samba service .....	176
Figure 283 : Status checking for the samba service ( smbd )......	176
Figure 284 : Status checking for the samba service ( nmbd ) .....	177
Figure 285 : Creation of a folder for samba service.....	177
Figure 286 : Opening the samba configuration file .....	178
Figure 287 : Configuration of samba ( Part 1 ) .....	178
Figure 288 : Configuration of samba ( Part 2 ) .....	179
Figure 289 : Enabling the folder for sharing .....	179
Figure 290 : Testing of the samba configuration file .....	180
Figure 291 : Update for the system .....	181
Figure 292 : Upgrade for the system.....	181
Figure 294 : Editing configuration file (50unattended-upgrades).....	182
Figure 296 : Update common-password config file.....	183
Figure 297 : Update common-password config file.....	184
Figure 298 : Update login.defs file .....	184
Figure 299 : Change specify user (grp2) password expiration .....	185
Figure 300 : Change system files permission .....	186
Figure 301 : Change permission on user accessible file .....	186
Figure 302 : Discover listening port .....	188
Figure 303 : Discover listening port .....	188
Figure 305 : Discovered port on Nmap.....	189
Figure 306 : Stop CUPS services.....	190
Figure 307 : Installation of UFW .....	190
Figure 309 : Reload UFW .....	191
Figure 310 : Enable UFW .....	191
Figure 312 : Download SoftEther VPN .....	192
Figure 313 : Choose requirement.....	193
Figure 314 : Download section .....	193
.....	194
Figure 315 : Choose software component to install.....	194
Figure 316 : Agree to End user Agreement .....	194
Figure 317 : Important Notice.....	195
Figure 318 : Path Selection .....	195
Figure 319 : Wait for installation.....	196

Figure 320 : Finish installation .....	196
Figure 321: Select local host.....	197
Figure 322 : Set up local host.....	198
Figure 323 : Set administrator password.....	198
Figure 325 : Set up confirmation notice.....	199
Figure 326 : Setup Virtual Hub Name .....	199
Figure 327 : Disable VPN Azure Services.....	200
Figure 328 : Create a new user.....	201
Figure 329 : Set up new user.....	201
Figure 331: Manage user .....	202
Figure 332 : Set up local bridge.....	203
Figure 333 : Manage Virtual Hub .....	203
Figure 334 : Enable SecueNAT .....	204
Figure 335 : Enable SecureNAT alert.....	204
Figure 336 : Ip address provided by SecureNAT.....	205
Figure 337 : Select Encryption and Network.....	205
Figure 338 : Modify encryption algorithm name .....	206
Figure 339 : Select IPsec / L2TP Setting .....	206
Figure 340 : Virtual Hub is created.....	207
Figure 341 : Go to website and click download.....	207
Figure 342 : Download SoftEther VPN .....	208
Figure 343 : Choose requirement.....	208
Figure 344 : Download section .....	209
Figure 345 : Choose software component to install.....	209
Figure 346 : Agree to End user Agreement .....	210
Figure 347 : Important Notice.....	210
Figure 348 : Path Selection .....	211
Figure 349 : Wait for installation.....	211
Figure 350 : Finish installation .....	212
Figure 351 : GUI of SoftEther VPN Client Manager .....	212
Figure 352 : Create new Virtual Network Adapter.....	213
Figure 353 : Set up Virtual Network Adapter name .....	213
Figure 354 : New virtual network adapter .....	214
Figure 355 : Set up VPN Connection.....	215
Figure 356 : VPN Connection created .....	215
Figure 357 : GUI of SoftEther VPN Client Manager .....	216
Figure 358 : Create new Virtual Network Adapter.....	216
Figure 359 : Set up Virtual Network Adapter name .....	217
Figure 360 : New virtual network adapter .....	217
Figure 361 : Set up VPN Connection.....	218
Figure 362 : VPN Connection created .....	219
Figure 363 : Lubuntu Server Update.....	220
Figure 364 : Lubuntu Server Upgrade .....	220
Figure 365 : Download the PBIS from GitHub .....	221
Figure 366 : Permission changes for downloaded PBIS package.....	221

Figure 367 : Installation of PBIS .....	222
Figure 368 : AD group with users created .....	222
Figure 369 : Domain Joining Between Lubuntu server and Windows Active Directory .....	223
Figure 370 : Login Settings.....	224
Figure 371 : Change to pam.d directory .....	225
Figure 372 : Open the common-session configuration file.....	225
Figure 373 : Edited common-session configuration file .....	226
Figure 374 : Change directory to lightdm.conf.d.....	226
Figure 375 : Configured lightdm.conf.d configuration file.....	228
Figure 376 : Change the directory file to /home/grp2.....	228
Figure 377 : Open the sudoers configuration file .....	229
Figure 378 : Configured sudoers configuration file .....	229
Figure 379 : Welcome Page of Security Configuration Wizard .....	231
Figure 380 : Configuration Action Tab.....	231
Figure 381 : Server Selection Tab.....	232
Figure 382 : Completion of Process Tab .....	232
Figure 383 : Welcome Tab of Role-Based Service Configuration .....	233
Figure 384 : Server Roles Lists Tab.....	233
Figure 385 : Client Features Lists Tab.....	234
Figure 386 : Administration and Other Options Lists Tab .....	234
Figure 387 : Handling Unspecified Services Tab .....	235
Figure 388 : Confirmation of Service Changes List Tab .....	235
Figure 389 : Welcome page of Network Security Tab .....	236
Figure 390 : Network Security Rules Lists Tab.....	236
Figure 391 : Welcome page of Registry Settings Tab .....	237
Figure 392 : SMB Security Signatures Requirement Tab.....	238
Figure 393 : LDAP Signing Requirement Tab .....	238
Figure 394 : Outbound Authentication Methods Tab .....	239
Figure 395 : Attributes Selection of Outbound Authentication using Domain Accounts Tab.....	239
Figure 396 : Summary of Registry Settings Tab.....	240
Figure 397 : Welcome page for Audit Policy Tab .....	241
Figure 398 : Selection of auditing objectives of System Audit Policy Tab .....	241
Figure 399 : Summary of Audit Policy Tab.....	242
Figure 400 : Security Policy Tab To Save The Policy .....	242
Figure 401 : File Saving for Security Policy File Name and File Location Tab.....	243
Figure 402 : Application Completion for Security Policy Tab .....	243
Figure 403 :Completion of Security Configuration Wizard Tab .....	244
Figure 404 : System Properties .....	245
Figure 405 : Changes client to Domain .....	246
Figure 406 : Windows Security .....	246
Figure 407 : Computer Name/Domain Changes.....	247
Figure 408 : Before The Policy is Enable .....	247
Figure 409 .....	248
Figure 410 : After The Policy is Enable .....	248
Figure 411 : ipconfig on client HQ .....	249

Figure 412 : Lease expiration .....	249
Figure 413 : Ping Public IP Address .....	250
Figure 414 : NAT translation .....	250
Figure 415 : Ping Public IP Address .....	250
Figure 416 : Details about Tunnel.....	251
Figure 417 : Session information .....	251
Figure 418 : Tunnel Status.....	252
Figure 419 : Ping status.....	252
Figure 420 : TELNET testing .....	253
Figure 421 : nslookup result.....	254
Figure 422 : nslookup result.....	255
Figure 423: Login to RainLoop Webmail Client .....	256
Figure 424: Compose and send email in RainLoop Webmail .....	257
Figure 425: Email is sent successfully .....	257
Figure 426: Login to another mail account.....	258
Figure 427: Recipient have received the email .....	259
Figure 428: RainLoop main page at ClientHQ .....	259
Figure 429: Group website.....	260
Figure 430: Group website with SSL.....	260
Figure 431: Virtual hosting website.....	261
Figure 432 Stop DHCP service .....	262
Figure 433 DHCP service status .....	262
Figure 434 Starting DHCP service.....	263
Figure 435 DHCP service status .....	263
Figure 436 Monitored network device status.....	264
Figure 437: Enter username and password in router.....	265
Figure 438: IN2012.log.....	266
Figure 439: IN2101.log.....	266
Figure 440: VLAN brief .....	267
Figure 441: Summary of shutdown ports.....	267
Figure 442: To display port security information .....	267
Figure 443: To display port security information .....	268
Figure 444: Verify installation.....	269
Figure 445: Snort successfully validated.....	269
Figure 446: Run command snort.....	270
Figure 447: Snort alert .....	270
Figure 448: Log file shown.....	270
Figure 449 : Samba folder sharing enabled .....	271
Figure 450 : Add a network location .....	271
Figure 451 : Welcome page of add network location wizard .....	272
Figure 452 : Option to choose a custom network location.....	272
Figure 453 : Typed samba location address.....	273
Figure 454 : Name for the samba shared network location .....	273
Figure 455 : Completion of adding network location wizard .....	274
Figure 456 : Folders and files created in samba share .....	274

Figure 457 : All shared folders lists .....	275
Figure 458 : Network credentials requirement for security purpose.....	275
Figure 459 : Restricted action warning .....	276
Figure 460 : Verify application up to date .....	277
Figure 461 : Verify password change .....	277
Figure 462 : Verify for password age .....	278
Figure 463 : Verify on system file permission.....	278
Figure 464 : Verify on users accessible file permission .....	278
Figure 465 : CUPS port closed .....	279
Figure 466 : Display disabled service .....	279
Figure 467 : Display allow port, services and UFW status.....	280
Figure 468 : GUI of SoftEther VPN Client Manager .....	281
Figure 469 : Connect to VPN.....	281
Figure 470 : Connected to VPN.....	282
Figure 471 : Connection successful .....	282
Figure 472 : Verify VPN Connection .....	282
Figure 473 : Verify IP address .....	283
Figure 474 : GUI of SoftEther VPN Client Manager .....	283
Figure 475 : Connect to VPN.....	284
Figure 476 : Fail connected to VPN.....	284
Figure 477 : Domain join connection with domain Group2.com .....	285
Figure 478 : Log in using registered user in Active Directory .....	285
Figure 479 : Logged username in terminal .....	286
Figure 480 : Checking of user's home directory ( Successful ) .....	286
Figure 481 : Connected Lubuntu Server in Active Directory .....	286
Figure 482 : Invalid user denied from login .....	287
Figure 483 : Leave domain .....	287
Figure 484 : Audit Policy checking .....	288
Figure 485 : Firewall Overview settings checking .....	288
Figure 486 : Password Policy Checking .....	289
Figure 487 : Account Lockout Policy checking.....	290
Figure 488 : Kerberos Policy checking.....	290

# **CHAPTER 1: INTRODUCTION**

## **1.1 INTRODUCTION**

Workshop 2 projects with code BITU 3923 is taken in Semester 1 for third year BITC and BITZ students. This project gives an occasion to the students to apply their knowledge from previous subjects. This workshop likewise develops students' understanding of the problem-solving method to tackle an issue based on the project scenario description. This project requires students to design, plan, and implement secure network infrastructure by using the available tools.

For project implementation, it requires each group of BITC and BITZ students to determine the distributed tasks to implement the network infrastructure. Each of the BITC students is responsible for a minimum of three services in developing the network infrastructure. Meanwhile, each of BITZ students is also responsible for three security services, including configurations and implementation.

Based on the project scenario given, we need to design and develop a secure infrastructure for the company ZBC that need to cover all the networking functions for internal and external IT communications such as routers, DNS servers, user management, port security and remote access to the network for telecommuters and network monitoring. There are different operating systems required to install such as Windows and Lubuntu server.

Therefore, BITC students are responsible to setup the network with 10 services which are Network Monitoring System, AAA (Authentication, Authorization, Accounting) using Radius, Linux Email Server, IPsec site-to-site tunneling, Active Directory, DNS (IPv4 and IPv6), DHCP (IPv4 and IPv6), Access Control List, Web, SSL and Virtual Hosting, Routing and Network Address Translation (NAT). For BITZ students, there are 8 network security services that need to be configured which consists of IPsec VPN Server for remote employees, Samba Security Services, IDS Port Mirroring, Linux Server Hardening, Windows Server Hardening, User authentication by integrating Active Directory with Linux, Layer 2 Security (VLAN Security and Port Security) and Audit Compliance.

## **1.2 OBJECTIVE**

The main objective of this project is to set up and design a secure network infrastructure by managing and monitoring the secure network infrastructure, services and configuration through the use of the tools available. Therefore, based on the requirement of a secured network environment, to install and configure network infrastructure, services, and configuration. Other than that, this project is aimed at helping students to build and integrate infrastructure for network services to meet the network environment and the security policies that have been developed.

## **1.3 PROJECT PLANNING / SCHEDULE**

We are assigned to the respective supervisors in the second and third weeks. We meet together to divide the task for us to complete during the next week after we have been assigned to supervisors and have proposal discussions among the group members. Then, we will prepare the project proposal that includes project details such as introduction, logical and physical network design to illustrate the topology of the network, Gantt chart to highlight the project timeline, and project distribution where the project manager will assign the tasks accordingly to all the group members. Also, we will submit the finalized proposal by the end of week 3.

We were then asked to log in to the VNC Viewer to access the server at the FTMK lab to install the operating system. We continue to set up at least 30 percent of the services required for this project in week 2 following the submission of the project proposal to week 5. During this time, we plan to install five services, which are VLAN, IPv6, AD, DNS, and DHCP services. We are therefore planning Progress Report 1, which will consist of the details of the service setup and installation. We then submit to the supervisors the finalized Progress Report 1 by the end of week 5.

We expect to continue setting up the other 70 percent of services from week 6 to week 10 and to prepare Progress Report 2, which will consist of the setup details of the services. We will continue to complete all the setups of the entire network and set up all the requisite services throughout Week 11 to Week 13. At the same time, we will be planning a video and a Linux Email Server poster to be presented to the Workshop 2 host and jury.

Upon the completion of the network, we will demonstrate to the supervisor and evaluator our respective services individually, and the video and poster presentation also be

presented at week 14 during the project presentation for updates to the final exhibition. During study week, which is equal to week 15, the finalized final report and individual logbook will be submitted.

### 1.3.1 GANTT CHART FOR PROJECT PLANNING

No	Task/ Activity	Week													
		1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	<ul style="list-style-type: none"> <li>• Proposal discussion between group members and supervisors</li> <li>• Proposal preparation</li> </ul>														
2	Proposal Submission														
3	<ul style="list-style-type: none"> <li>• Project Progress 1</li> <li>• Setup minimum 30% services</li> </ul>														
4	<ul style="list-style-type: none"> <li>• Project Progress 2</li> <li>• Setup minimum 70% services</li> </ul>														
5	<ul style="list-style-type: none"> <li>• Project Progress 3</li> <li>• Complete setup 100% services</li> <li>• Demonstrate individual and group task respectively</li> </ul>														
6	Video & Poster preparation														
7	Workshop II Competition (Project Demo)														
8	Final Report, Peer Assessment Report and Log Book														

## **1.4 CONCLUSION**

We would apply all the knowledge we have gained before and doing this project, which can help us overcome all the problems that arise during the implementation of the project. Also, we can acquire more knowledge about how to manage and maintain a network, and it also allows us to develop our skills in the field of networking and security. With the cooperation and tolerance of all the team members, the project can deliver in time.

## **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 2 servers with combination of different platforms. Besides, we need to install and configure 18 services and they will be divided among the 2 servers. There are 10 services for computer networking and 8 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 II, we have been provided with the computer in wireless lab at faculty. We install Virtual Network Computing (VNC) which allows us to use personal computer to remote this computer for implementing Workshop II. We are required to design, set up, maintain and monitor a network environment.

### **2.2 TYPES OF OPERATING SYSTEM**

#### **2.2.1 Windows Server 2012**

To develop the network security infrastructure for the company, our team decided to use Windows Server 2012 as one of the servers. We chose this based on few criteria's and features such as:

##### **2.2.1.1 Shared Nothing-Live Migration**

With Windows Server 2012, the new, shared nothing-live migration allows you to move a VM between servers, however, the servers must be able to see each other via an Ethernet connection. Any changes during a shared nothing-live migration are logged, and once the original copy is complete, the updated version will be applied to the source and destination virtual hard disk (VHD) files. Once the sync is complete, the copied VM on the destination host is brought online, and then the copy on the source is erased.

### **2.2.1.2 VM Direct Connect**

Connecting to a running VM over RDP requires an active network connection, which we cannot always count on. To have an active network connection, the VM must have an IP address reachable by the system attempting to connect. All this changed in Windows Server 2012 R2 and Hyper-V with the addition of VM Direct Connect. This feature allows a direct remote desktop connection to any running VM over what is called VM Bus.

### **2.2.1.3 Storage Qos**

Windows Server 2012 R2 has the ability to limit individual VMs to a specific level of I/O throughput. If we have applications capable of consuming larger amounts of I/O, we will want to consider this setting to ensure that a single I/O-hungry VM would not starve neighbor VMs or take down the entire host.

### **2.2.1.4 Dynamic Memory support for Linux**

In the Windows Server 2012 R2, Hyper-V gains the ability to dynamically expand the amount of memory available to a running VM. This capability is especially handy for any Linux workload which our team will implement in this network infrastructure. In environments with many Linux VMs, dynamic memory becomes even more critical to efficiently manage the total memory used by all running VMs. Windows Server 2012 R2 Hyper-V also brings Windows Server backups to Linux guests.

### **2.2.1.5 Online VM exporting and cloning**

One of the downsides before this is the system needs to stop a running VM before we can export or clone it. Now, it is possible to export or clone a running VM from System Center Virtual Machine Manager 2012 R2 with a few mouse clicks.

Server Requirement	
Processor	1.4 GHz, x64
Memory	512 MB
Disk Space	32 GB (more if there is at least 16 GB of RAM)

### 2.2.2 Lubuntu 18.04 LTS

Lubuntu is a fast and lightweight operating system with a clean and easy-to-use user interface. It is a Linux system, that uses the minimal desktop LXDE/LXQT, and a selection of light applications. Because of this, Lubuntu has very low hardware requirements. It is a variant of Ubuntu. We have chosen Lubuntu 18.04 since it is the latest version of Lubuntu.

Server Requirement	
Processor	1.4 GHz, x64
Memory	8 GB
Disk Space	32 GB (more if there is at least 16 GB of RAM)

## 2.3 CONCLUSION

Eventually, prior to installing the operating systems, we can ensure that VMware meets the minimum specifications. Installing and integrating two different types of operating systems with at least 20 different services into a network infrastructure is difficult for us. We have to consider the demand for the operating system and determine which server is the best to implement. In order to install the core and main services in Window Server 2012 and the least essential services in Lubuntu Server, we must also make a good decision.

# **CHAPTER 3: DESIGN**

## **3.1 INTRODUCTION**

We have to identify, plan, execute and manage network services in this Workshop 2. Each group needs to implement the network design that is necessary to be implemented in GNS3 and VMware. We need to build a network that involves three separate servers, a router, a switch, and the design of a client host.

## **3.2 SECURITY POLICY**

### **3.2.1 Introduction**

A security policy is a set of security objectives for a company, rules of behavior for users and administrators, and system requirements. These objectives, rules, and requirements collectively ensure the security of a network, the data, and the computer systems in an organization.

### **3.2.2 Objective**

Workshop 2 Group 2 Security Policy created to minimize the impact of security incidents. This policy also aims to facilitate the sharing of information between two operating systems. This can only be achieved by ensuring that all the assets are protected. Administrations and all users must adhere to all the policy.

### **3.2.3 Password Protection Policy**

#### **3.2.3.1 Purpose**

The purpose of this policy is to establish a standard for creation of strong passwords and the protection of the passwords.

- Passwords must not be shared with anyone, including supervisors and coworkers.
- Must contain eight characters or more.
- Passwords should contain characters from the four primary categories, including: uppercase letters, lowercase letters, numbers, and characters.
- Set passwords expiry for 180 days.

- Do not use the “Remember Password” feature of an application (for example, web browser).

### **3.2.4 Remote Access Policy**

#### **3.2.4.1 Purpose**

The purpose is to define rules and requirements for connecting to a company's network from any host. These rules and requirements are designed to minimize the potential exposure to company from damages which may result from unauthorized use of company resources.

- Secure remote access must be strictly controlled with encryption (Virtual Private Networks (VPN)) and pass-phrases.
- While using a company owned computer to remotely connect to a company's corporate network, Authorized Users shall ensure the remote host is not connected to any other network at the same time, with the exception of personal networks that are under their complete control or under the complete control of an Authorized User or Third Party.
- All hosts that are connected to company name internal networks via remote access technologies must use the most up-to-date anti-virus software.
- Personal equipment used to connect to company's networks must meet the requirements of company owned equipment for remote access as stated in the Hardware and Software Configuration Standards for Remote Access to company Networks.

### **3.2.5 Server Security Policy**

#### **3.2.5.1 Purpose**

To establish standards for the base configuration of internal server equipment that is owned and /or operated by the company. Effective implementation of this policy will minimize unauthorized access to company proprietary information and technology.

## **I General**

- Servers must be registered within the corporate enterprise management system. At a minimum, the following information is required to positively identify the point of contact:
  - ✓ Server contact(s) and location, and backup contact
  - ✓ Hardware and Operating System/Version
  - ✓ Main functions and applications, if applicable
- Information in the corporate enterprise management system must be kept up-to-date.
- Configuration changes for production servers must follow the appropriate change management procedures.

## **II Configuration requirement**

- Operating System configuration should be in accordance with approved InfoSec guidelines.
- Services and applications that will not be used must be disable where practical.
- Access to services should be logged and/or protected through access-control methods such as a web application firewall, if possible.
- Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication is sufficient.
- If a methodology for secure channel connection is available (i.e technically feasible), privileged access must be performed over secure channels, (i.e.encrypted network connections using SSH or IPSec).
- Always use standard security principles of least required access to perform a function.
- Setup radius server as a security measure that runs on the server to maintain user profiles in the central database and to have control over who can connect to the network.

- Perform AAA (Authentication, Authorization, and Accounting) security for effective network management and security.

### **3.2.6 Router and Switch Security Policy**

#### **3.2.6.1 Purpose**

The purpose is to define a minimal security configuration for all routers and switches connecting to a production network or used in a production capacity at or on behalf of a company.

- Must have a local user as a backup incase unable to authenticate using AAA.
- Routers and switches must use RADIUS for all user authentication.
- The enable password on the router or switch must be kept in a secure encrypted form. The router or switch must have the enabled password set to the current production router/switch password from the device's support organization.
- The following services or features must be disable:
  - ✓ IP directed broadcasts
  - ✓ Incoming packets at the router/switch sourced with invalid addresses such as RFC1918 addresses.
  - ✓ All source routing and switching.
  - ✓ Company discovery protocol in Internet connected interfaces.
  - ✓ Telnet and FTP
  - ✓ Auto-configuration.
- All routing updates shall be done using secure routing updates.
- Access control lists must be used to limit the source and type of traffic that can terminate on the device itself.
- The router must be included in the corporate enterprise management system with a designated point of contact.
- Telnet 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.

- Dynamic routing protocols must use authentication in routing updates sent to neighbors.
- The corporate router configuration standard will define the category of sensitive routing and switching devices, and 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 FRC1918 addresses, or those that could be used to spoof network traffic shall be dropped.
  - Router console and modem access must be restricted by additional security controls.

### **3.2.7 Email Policy**

#### **3.2.7.1 Purpose**

To ensure the proper use of the company email system and make sure users are aware of what the company deems as acceptable and unacceptable use of its email system.

- User's email and password must be linked with an Active Directory user.
- All use of email must be consistent with company policies and procedures of ethical conduct, safety, compliance with applicable laws and proper business practices.
- Company email accounts should be used primarily for company business related purposes, personal communication is permitted on a limited basis, but non company related commercial uses are prohibited.
- Users are prohibited from automatically forwarding company email to a third-party email system. Individual messages which are forwarded by the user must not contain company confidential information.

### 3.3 PHYSICAL DESIGN

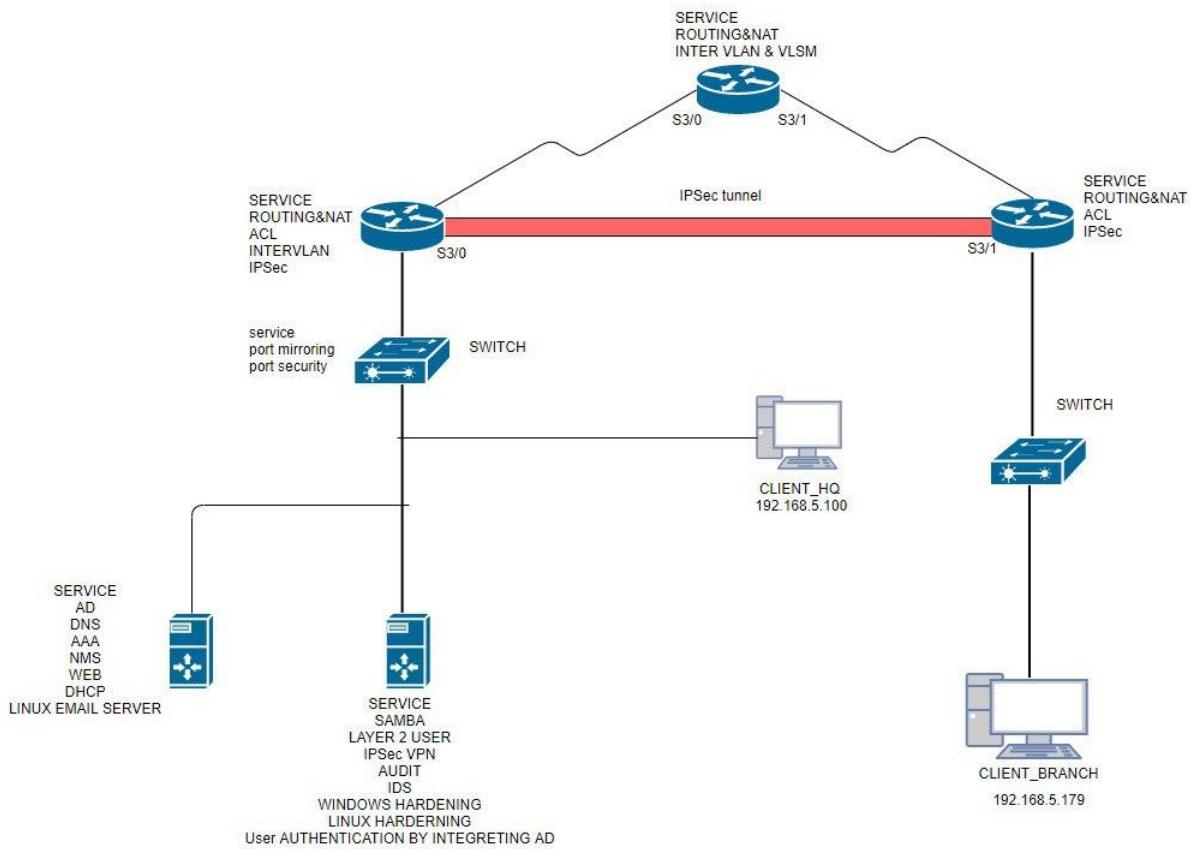


Figure 1 : Physical Design

### 3.4 LOGICAL DESIGN

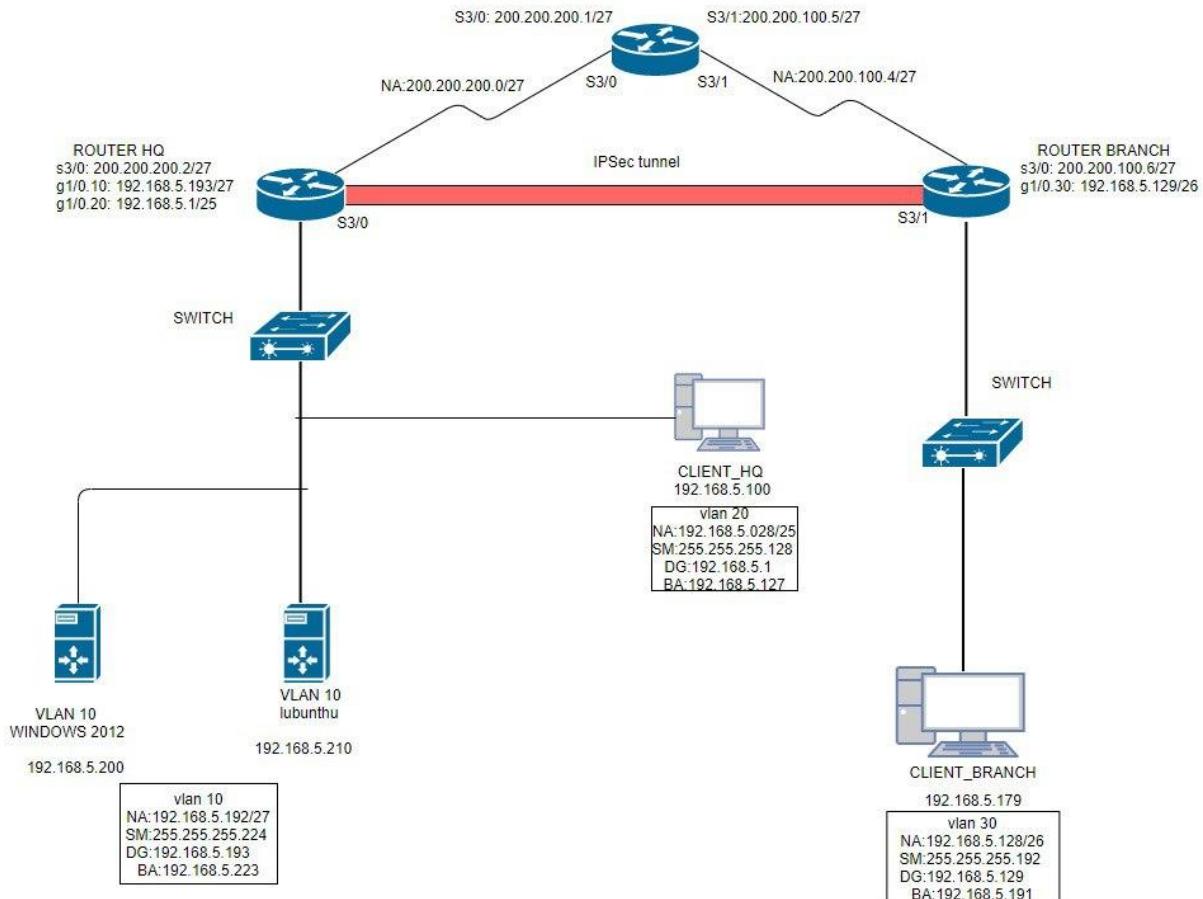


Figure 2 : Logical Design

### 3.5 VLAN AND VLSM ADDRESSING

#### 3.5.1 VLAN ADDRESSING

VLAN NAME	NEEDED SIZE	ALLOCATE D SIZE	ADDRESS	MASK	SUBNET MASK	IP RANGE	BROADCAST
CLIENT_HQ Vlan 20	100	126	192.168.5.0	/25	255.255.255.128	192.168.5.1 – 192.168.5.126	192.168.5.127
CLIENT_BRANCH Vlan 30	50	62	192.168.5.128	/26	255.255.255.192	192.168.5.129 – 192.168.5.190	192.168.5.191
VLAN_SERVER Vlan 10	20	30	192.168.5.192	/27	255.255.255.224	192.168.5.193 – 192.168.5.222	192.168.5.223

#### 3.5.2 IP ADDRESSING FOR DEVICE

DEVICE NAME	IP ADDRESS
WINDOWS SERVER	192.168.5.200
LUBUNTU SERVER	192.168.5.210
ROUTER HQ	192.168.5.100
ROUTER BRANCH	192.168.5.179

### **3.6 CONCLUSION**

When designing a network, the network architecture is an important element. There is no idea how to begin the implementation of the network without network architecture. In implementing network architecture that involves, few main factors need to be considered, including the planning of network complexity must be in line with the network administrator, redundancy, standards, and maintenance factors. All of these factors are needed to ensure that the network can be implemented, flexible, and easy to maintain for future implementation. After taking these factors into account, we implemented the network as a physical design and going through to the next phase of implementation, planning of network services implementation.

# **CHAPTER 4: SERVICES**

## **4.1 INTRODUCTION**

In this chapter, each installed service will be listed and explained. Explanation includes the functions of the services, the problems solved by the installation of the services, and the types of software used.

## **4.2 TYPE OF SOFTWARE**

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

1. Windows Server 2012
2. Lubuntu Server

### **4.2.2 LIST OF SERVICES**

1. Network Monitoring System,
2. AAA (Authentication, Authorization, Accounting) using Radius
3. Linux Email Server
4. IPsec site-to-site tunneling
5. Active Directory
6. DNS (IPv4 and IPv6)
7. DHCP (IPv4 and IPv6)
8. Access Control List,
9. Web, SSL and Virtual Hosting
10. Routing and Network Address Translation (NAT)
11. IPsec VPN Server for remote employees
12. Samba and Samba Security Services
13. IDS Port Mirroring
14. Linux Server Hardening
15. Windows Server Hardening
16. User authentication by integrating Active Directory with Linux
17. Layer 2 Security (VLAN Security and Port Security)
18. Audit Compliance

## **4.3 BRIEF OVERVIEW OF SERVICES**

### **4.3.1 Network Monitoring System (NMS)**

Network Monitoring System is a system designed for monitoring, maintaining, and optimizing a network. It enables network administrators to manage a network's independent components inside a bigger network management framework. Both software and hardware components in a network can be monitored using NMS. It usually records data from a network's remote points to carry out central reporting to a system administrator. NMS provides services including network monitoring, device detection, performance analysis, device management and fault management. In workshop 2, we install Nagios Core as the NMS in our designed network. It helps to administrators to monitor and maintain the individual components of a network within larger management framework.

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

Remote Authentication Dial-In User Service (RADIUS) is often used to implement authentication, authorization, and accounting (AAA). It uses the client/server model and prevents unauthorized access to networks that require high security and control of remote user access. AAA is a system for tracking user activities on an IP-based network and controlling their access to network resources. When AAA accounting is enabled, the network access server reports user activity to the RADIUS security server (depending on which security method is implemented) in the form of accounting records.

### **4.3.3 Linux Email Server**

A mail server (or Mail Transport Agent) is a computer system that sends and receives email. It handles both sending and receiving mails using protocols such as SMTP (Simple Mail Transfer Protocol) or ESMTP (Extended SMTP) for sending mails and POP3 (Post Office Protocol 3) or IMAP (Internet Message Access Protocol) for receiving mails. Sendail, Postflix, Exim and qmail are the email servers which are most popular on Linux. In workshop II, we have installed RainLoop as the web-based email client.

### **4.3.4 IPSec site-to-site tunneling**

Site-to-Site IPSec VPN Tunnels are used to allow the secure transmission of data, voice and video between two sites. The VPN tunnel is created over the Internet public

network and encrypted using a number of advanced encryption algorithms to provide confidentiality of the data transmitted between the two sites. IPsec tunnel mode is used between two dedicated routers, with each router acting as one end of a virtual "tunnel" through a public network.

#### **4.3.5 Active Directory**

Active Directory (AD) is a directory service developed by Microsoft for Windows domain networks used to manage computers and other devices on a network. It is a primary feature of Windows Server, an operating system that runs both local and Internet-based servers. It allows network administrators to create and manage domains, users, and objects within a network. UAC (User Account Control) is a new mechanism introduced by Microsoft which provides an additional level of protection against unauthorized modification. UAC settings can be managed using the slider and GPO which is a solution for deploying the requirements for Active Directory domain user passwords.

#### **4.3.6 DNS (IPV4 & IPV6)**

The Domain Name System (DNS) is a hierarchical and decentralized naming system for resources connected to the Internet or a private network. DNS translates domain names to IP addresses so that browsers can load Internet resources. Each device connected to the Internet has a unique IP address which other machines use to find the device. DNS servers eliminate the need for humans to memorize IP addresses.

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

DHCP is a protocol that automatically assigns a unique IP address to each device that connects to a network. DHCP permits a node to be configured automatically, thus avoiding the necessity of involvement by a network administrator. DHCP is used for Internet Protocol version 4 (IPv4) and IPv6. While both versions serve the same purpose, the details of the protocol for IPv4 and IPv6 differ sufficiently that they may be considered separate protocols.

#### **4.3.8 Access Control List (ACL)**

Access control list (ACL) refers to the permissions attached to an object that specify which users are granted access to that object and the operations it is allowed to perform. It defines what users and groups can access the object and what operations they can perform. Read, write, and execute are the operations that are typically included. ACL provides a straightforward method of managing file and folder permissions. They are used by most operating systems, including Windows and Linux systems

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

A web server is a computer that runs websites. It processes incoming network requests over HTTP and several other related protocols. Web server is mainly used to store, process and deliver web pages to clients. Secure Sockets Layer (SSL) is a standard security technology for establishing an encrypted link between a server and a client, which are typically a web server and a browser.

It is used to secure credit card transactions, data transfer and logins, and more recently is becoming the norm when securing browsing of social media sites. Virtual hosting is a method which generally allows multiple IT appliances, such as websites and applications, to share a single Web server.

#### **4.3.10 Routing & NAT**

Routing refers to the process of selecting a path for moving packets in a network or between multiple networks. Network Address Translation (NAT) is the process where a network device, usually a firewall, assigns a public address to a computer (or group of computers) inside a private network. It is mainly used to limit the number of public IP addresses an organization or company must use, for both economy and security purposes as well as to avoid the need to assign a new address to every host when a network was moved, or when the upstream Internet service provider was replaced.

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

IPsec VPN is a set of protocols used to ensure the secure and private communication over Internet Protocol (IP) networks, which is achieved by the authentication and encryption of IP packets between two-end-points. It allows the employees to create a secure virtual tunnel to their office network through the public network such as the internet.

Besides, IPsec VPN server protects confidentiality and integrity of data as it travels over the public internet by using cryptographic security services. In addition, IPSec VPN uses tunneling to establish a private connection for the network traffic. Unlike other protocols that function at the application layer, it operates at the network layer. It allows the protocol to encrypt the entire packet. Hence, the tool applied for this service is SoftEther VPN.

#### **4.3.12 Samba and Samba Security Services**

Samba is an open-source implementation of the SMB file sharing protocol that provides file and print services to SMB/CIFS clients. Samba allows a non-Windows server to communicate with the same networking protocol as the Windows products. 21 Samba was originally developed for UNIX but can now run on Linux, FreeBSD and other UNIX variants. It is freely available under the GNU General Public License. The name Samba is a variant of SMB, the protocol from which it stems.

#### **4.3.13 IDS Port Mirroring**

An intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations to produce report to a Management Station. IDS detect a potential security breach, logs the info and signals an alert on the console and owner. To ensure that IDS analyses the required or specific data, we mirror the traffic of a switch port or VLAN. For this, we will use the "port mirroring" mechanism which the switch duplicates the traffic on the chosen interface or VLAN and send it to Snort.

Besides, on the IDS system, need at least one network interface to listen to the traffic, but if we can have two network ports, this will be much better as we will able to dedicate one of both for the IDS management and the other one will be configured without

IP address just to receive the mirrored (or spanned) traffic. In this case, the IDS management data will not "pollute" the mirrored traffic.

#### **4.3.14 Linux Server Hardening**

Linux server hardening is a process of securing a Linux system by reducing its surface of vulnerability. There are a few different ways to approach this process. At the machine level, drives can be encrypted, and the BIOS can be secured. At a system level, login security can be considered and password policies can be enacted. At the network level, ports can be blocked and firewalls can be configured.

Overall, alerting can be configured, logging can be set up, and audits can be performed. The end goal of this process is balancing security with effectiveness and accessibility. A completely open system may be the easiest to use - but is a security risk and may not be usable for long. A completely locked down system, while secure, offers no value if it cannot be accessed when called upon. Here's a breakdown of the best practices for hardening Linux servers.

To harden Linux server, enforcing stronger password is the tip to prevent the password might be hacked with a dictionary based or brute-force attacks as a few users use soft or weak passwords. Update the common-password configuration file for Pluggable Authentication Modules (PAM) services with setting a maximum of 3 attempts for getting an acceptable password, a 8 character of minimum length, a requirement that the password contain at least one each of digit, lower-case character, and upper-case character. Furthermore, enabling Linux firewall is one of the methods of hardening service and crucial to secure unauthorized access of the servers. By activating firewall of Linux server, it can specify the source and destination address to allow and deny in specific UDP or TCP port number. Besides, unnecessary service and port are disabled for example disable CUPS service as it is a common UNIX printing system which allows a computer to act as a print server.

#### **4.3.15 Windows Server Hardening**

Windows Server hardening involves identifying and remediating security vulnerabilities to limit entry points. The first way to harden Windows servers is to think security from the very start. During the first way, choose NTFS (new technology file system) for all volumes as it was introduced with Windows NT and provides a number of security features FAT does not, including access control lists (ACLs) and file system

journaling, which logs changes before committing them to the main file system. Next, through the way of configuring the security policy, new security policies can be created and existing policies can be edited or applied to other servers on the network. The third way to harden Windows servers is to disable or delete unnecessary accounts, ports and services. Instead, the administrative rights should be assigned to an individual user or a group object. This makes it much harder for a hacker to figure out which user has administrative rights. Setting up appropriate access control to the physical machine and logical components is the following way to harden Windows servers and it is crucial to ensure that only properly authenticated users have permission to access and edit the registry. The last way is to protect the critical servers like create a baseline backup, institute a strong audit and logging policy and keep patches up-to-date.

#### **4.3.16 User Authentication by integrating AD with Linux**

Active Directory (AD) serves as a central location for network administration and security. It is responsible for authenticating and authorizing all users and computers within a network of Windows domain type, assigning and enforcing security policies for all computers in a network and installing or updating software on network 14 computers. Active directory uses Lightweight Directory Access Protocol (LDAP) version2,3 and DNS. At this project, we need to integrate Active Directory with Linux.

#### **4.3.17 Layer 2 Security (VLAN Security and Port Security)**

##### **VLAN Security**

VLAN security provides the network administrator a means by which the network can be barricaded against dreaded insider attacks. A malicious user can no longer just plug their workstation into any switch port and sniff the network traffic using a packet sniffer. The network administrator controls each port and whatever resources it is allowed to use. VLANs help to restrict sensitive traffic originating from an enterprise department within itself.

Moreover, VLAN-based security requires the use of special tools and following a few best security practices to achieve the desired result. These best practices include removing console-port cables and introducing password-protected console or virtual terminal access with specified timeouts and restricted access policies, applying the same

commands to the virtual terminal section and creating an access-list to restrict telnet access from specific networks and hosts, avoiding use of using the default VLAN as the network data VLAN, disabling high-risk protocols on any port that does not require them, deploying VTP domain, VTP pruning and password protections, and controlling inter-VLAN routing through the use of IP access lists.

### **Port Security**

Port security is a traffic control service on Cisco switches where the administrator can configure a specified number of MAC addresses that can be used in a single port. The use of port security is to avoid the addition of dumb switches by users who wants to illegally extends the network reach. Port security can be configured with dynamically learned or static MAC addresses to restrict any ingress traffic into the ports. When a registered MAC address connects to the port, the device will have the full bandwidth of the port it is registered to.

#### **4.3.18 Audit Compliance**

A compliance audit is an independent evaluation to ensure that an organization is following external laws, rules, and regulations or internal guidelines, such as corporate bylaws, controls, and policies and procedures. Compliance audits may also determine if an organization is conforming to an agreement, such as when an entity accepts government or other funding. A compliance audit gauges how well an organization adheres to rules and regulations, standards, and even internal bylaws and codes of conduct. Part of an audit may also review the effectiveness of an organization's internal controls.

## **4.4 CONCLUSION**

Each service does have various types of software or packages to be installed on the server for each service function. Service can be simple, but it can be very critical and some services need to be integrated to work effectively with other services that make the servers work.

# 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 which have been set. The configuration is to ensure the functioning of the service are successfully installed and configure.

## 5.2 SERVICES AND CORRESPONDING PERSON IN CHARGE

BITC STUDENT		
NO.	NAME	SERVICES
1	Amirul Haqim bin Zamri	<ol style="list-style-type: none"><li>Network Monitoring System (NMS)</li><li>DHCP (IPv4 &amp; IPv6)</li></ol>
2	Chong Zi Qing	<ol style="list-style-type: none"><li>AAA (Authentication, Authorization and Accounting) using Radius</li><li>Web, SSL &amp; Virtual Hosting</li><li>Linux Email Server</li></ol>
3	Syaza Liyana binti Muhamad Shapee	<ol style="list-style-type: none"><li>Domain Name System (DNS) IPv4 &amp; IPv6</li><li>IPSec Site-to-Site Tunneling</li><li>Network Address Translation (NAT)</li></ol>
4	Areef Aiman bin Zainuddin	<ol style="list-style-type: none"><li>Active Directory with minimum of 2 UAC/GPO according to security policy</li><li>Routing</li><li>Access Control List (ACL) with minimum of 4 rules</li></ol>

BITZ STUDENT		
<b>5</b>	Chai Rou Sin	<ul style="list-style-type: none"> <li>1. IPSec VPN Server for Remote Employees</li> <li>2. Linux Server Hardening and Vulnerability Report</li> </ul>
<b>6</b>	Thiasan A/L Chandran	<ul style="list-style-type: none"> <li>1. Samba and Samba security services with minimum of 3 security features</li> <li>2. User authentication user by integrating AD with Linux</li> <li>3. Windows Server Hardening and Vulnerability Report</li> </ul>
<b>7</b>	Hamizah binti Rozali	<ul style="list-style-type: none"> <li>1. IDS Port Mirroring</li> <li>2. Layer 2 Security- VLAN and Port Security</li> <li>3. Audit Compliance</li> </ul>

## 5.3 SERVICE INSTALLATION AND CONFIGURATION

### 5.3.1 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.

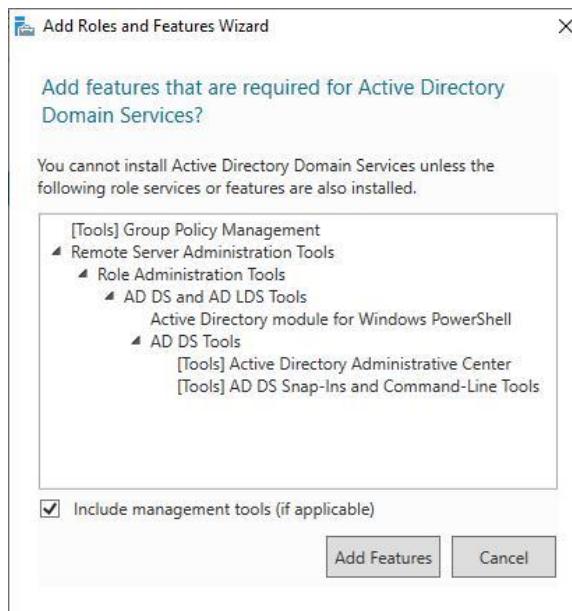


Figure 3 Add Roles & Features Wizard

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

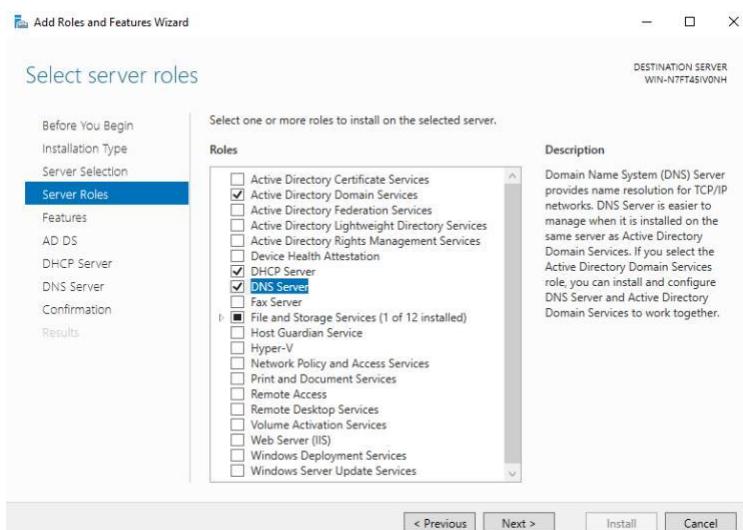
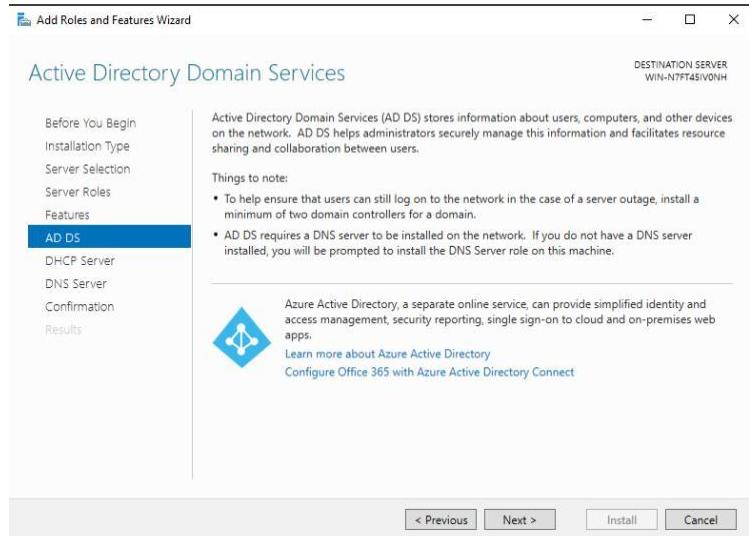


Figure 4 Select Server Role

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

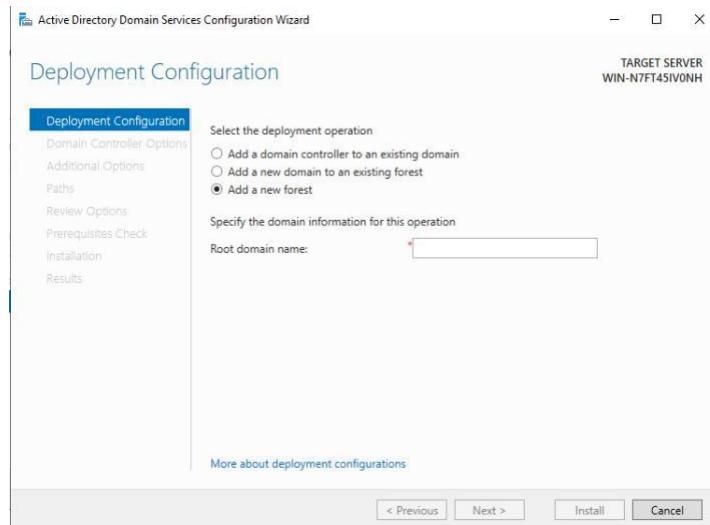


*Figure 5 AD Domain Server*

**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 6 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.

**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”.

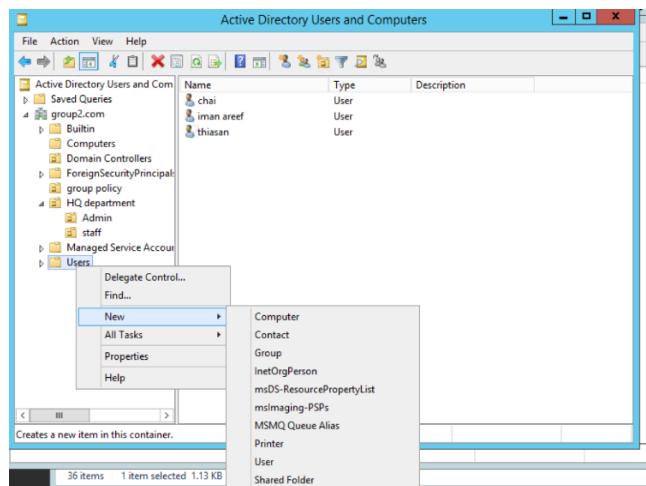
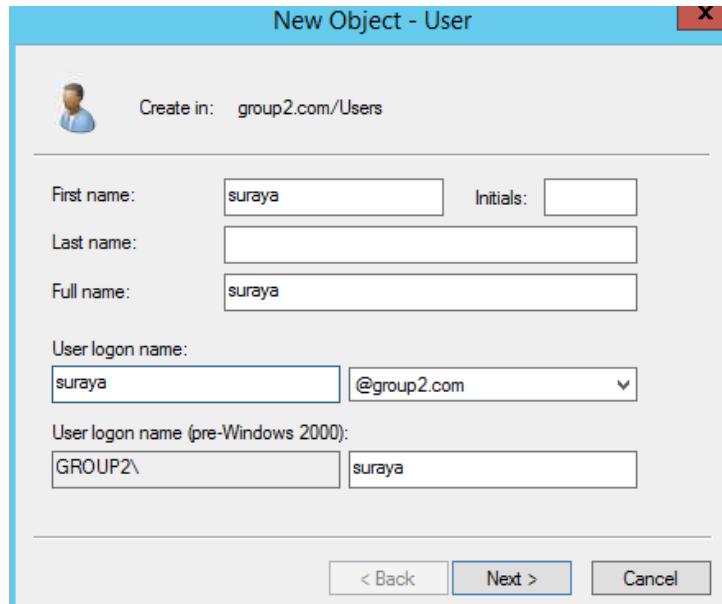


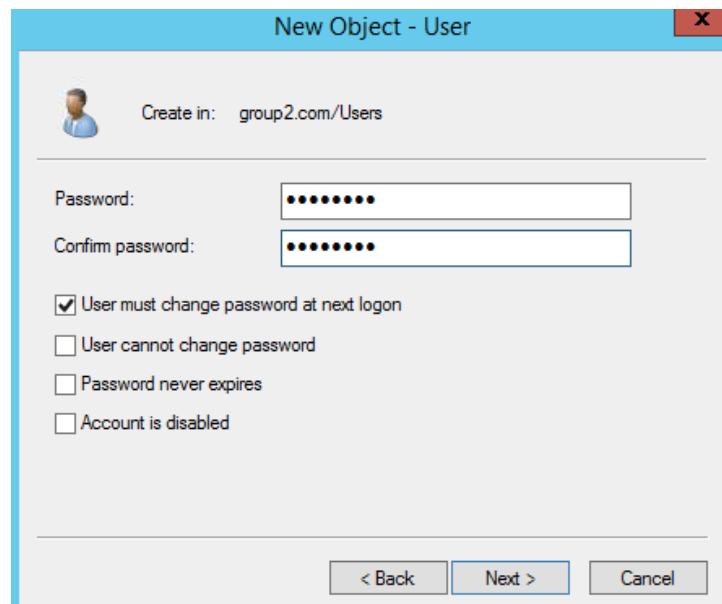
Figure 7 Active Directory Users

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



*Figure 8 New Object – Use*

**STEP 15:** Next, insert the password for the user. Pick user must change password at next logon and click next.



*Figure 9 Password & Confirm Password*

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

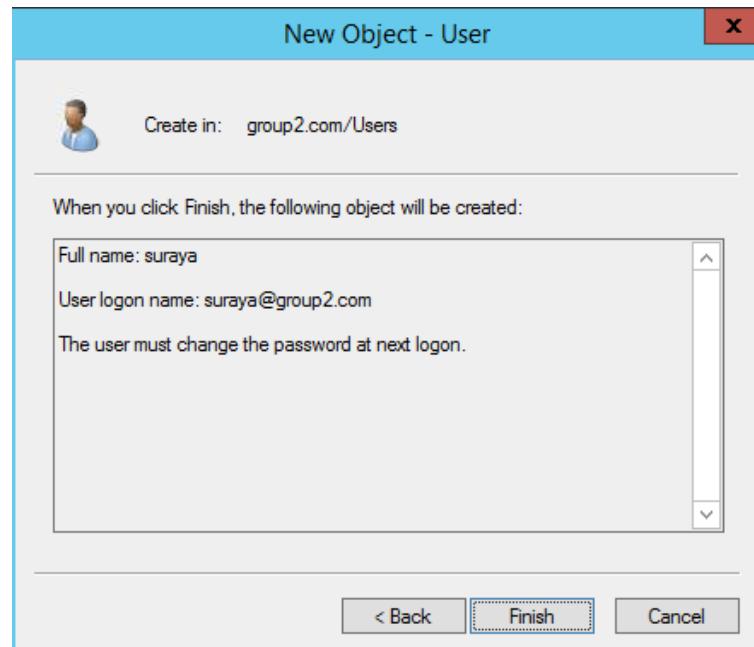


Figure 10 Information Before Create

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

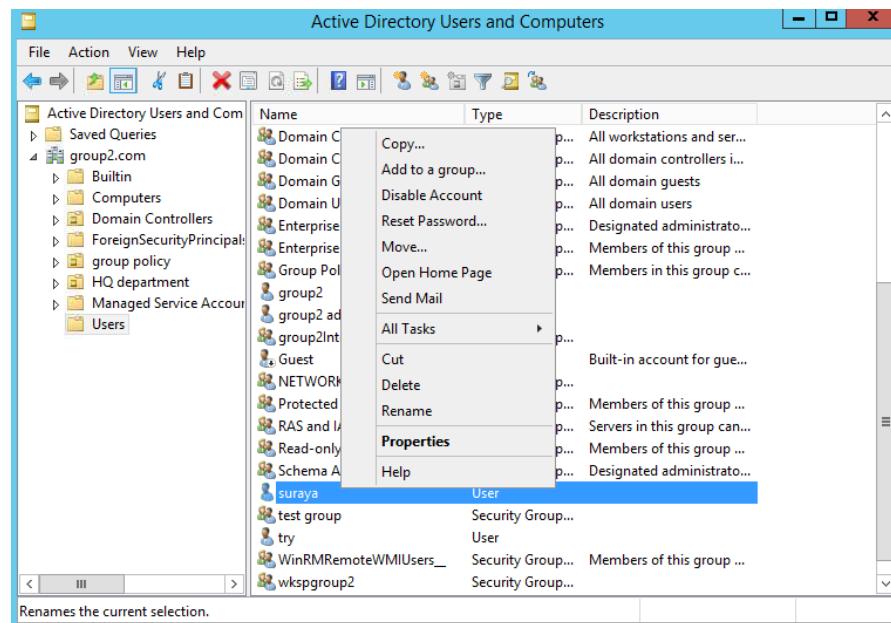
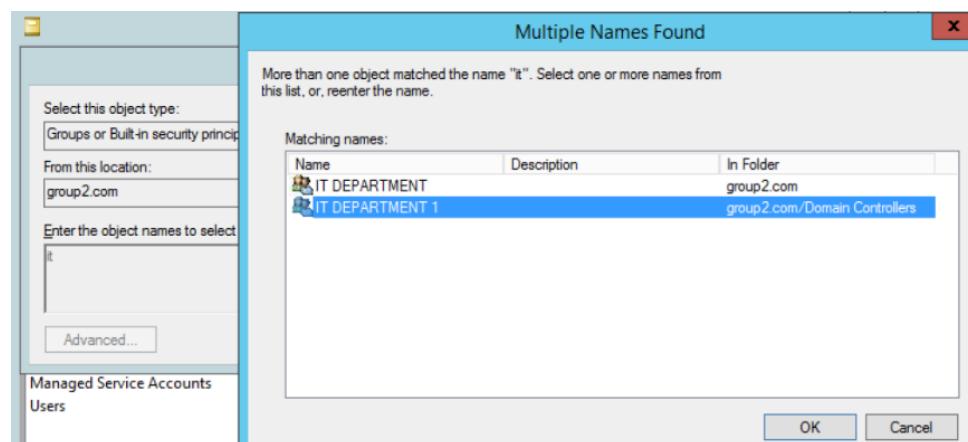


Figure 11 Add To a Group

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



*Figure 12 Select Groups*

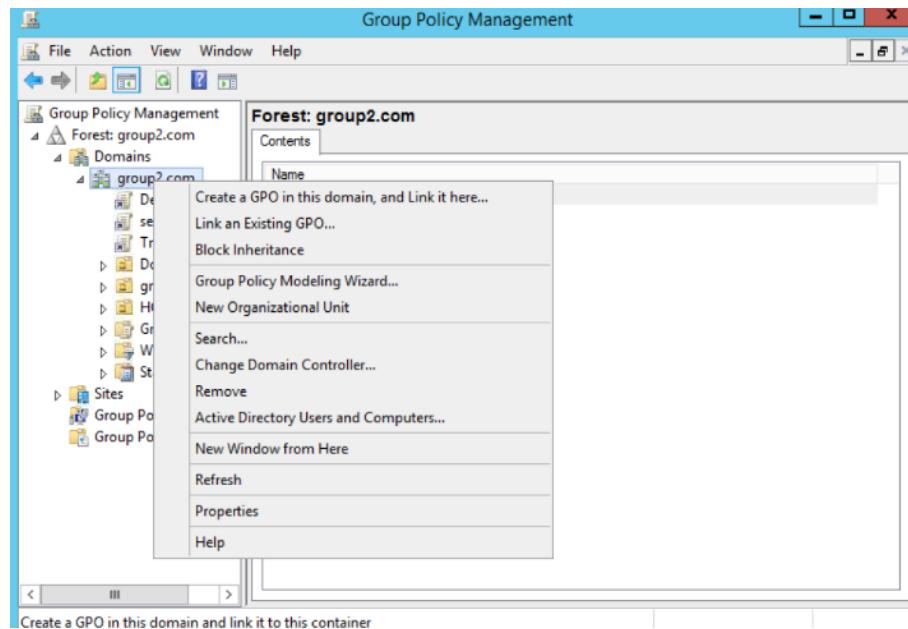
**STEP 19:** A message will appear. Then click ok.



*Figure 13 ADDS message*

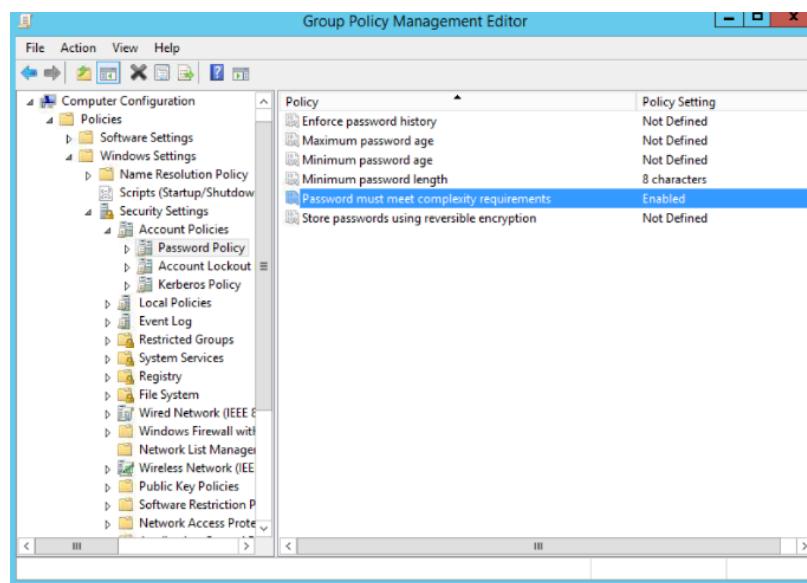
## Group Policy Object :

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



*Figure 14 Group Policy Management*

**STEP 2 :** Click the windows > security policy > account policy : Password policy. Pick any policy to be edit. For example “minimum password length”. Click 8 character, apply and OK.



*Figure 15 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.

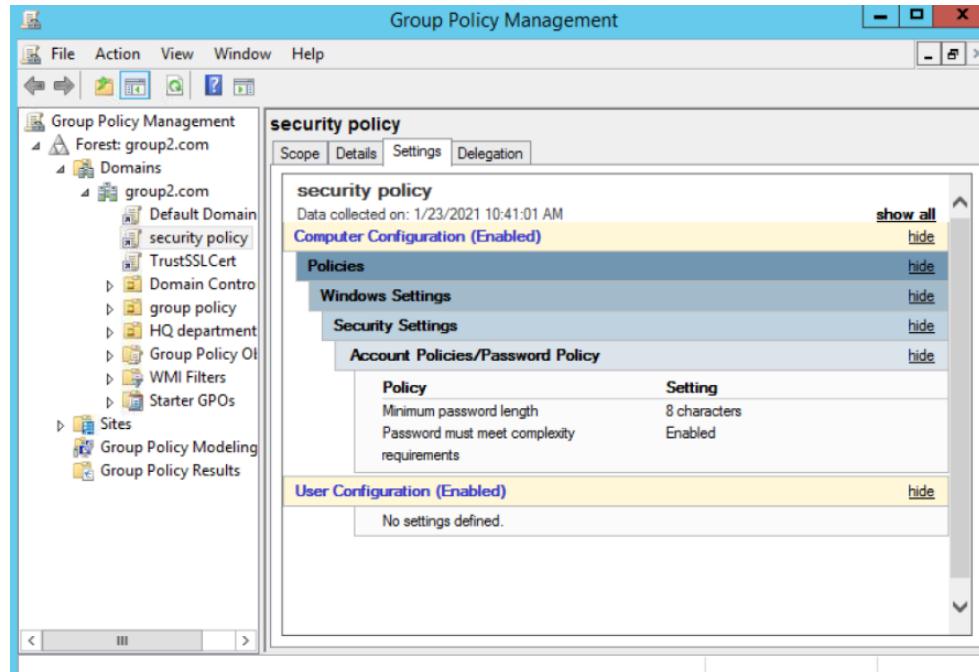


Figure 16 Policy Created

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

```
Administrator: Command Prompt
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\aiman>gpupdate
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.

C:\Users\aiman>
```

Figure 17 gpupdate Force

### 5.3.2 DHCP IPv4 & IPV6

#### 5.3.2.1 DHCP IPv4

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

**Step 2:** Expand and click on Roles > Add Roles

**Step 3:** Choose Add Roles and Features

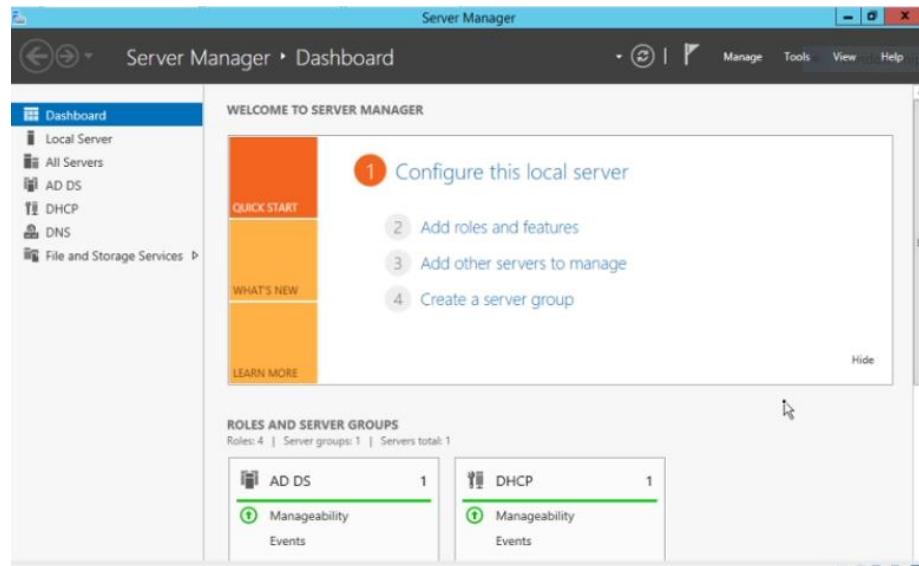


Figure 18 Dashboard

**Step 4:** Before running the installation wizard, make sure that administrator account has a strong password, static IP is configured, and security updates from Windows updates are installed. After it is done, click next.

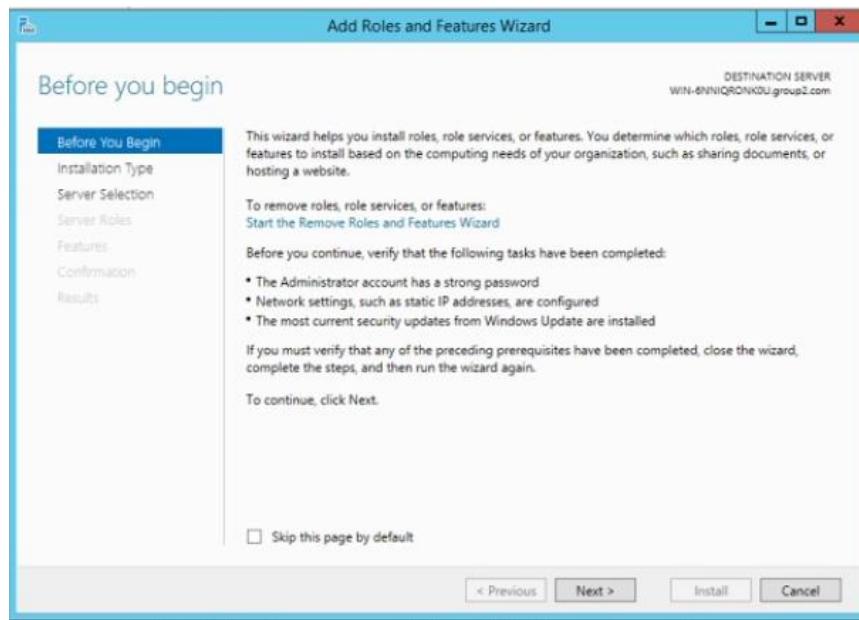


Figure 19 Add Roles & Features

**Step 5:** Select Role-based or Feature-based installation and click next.

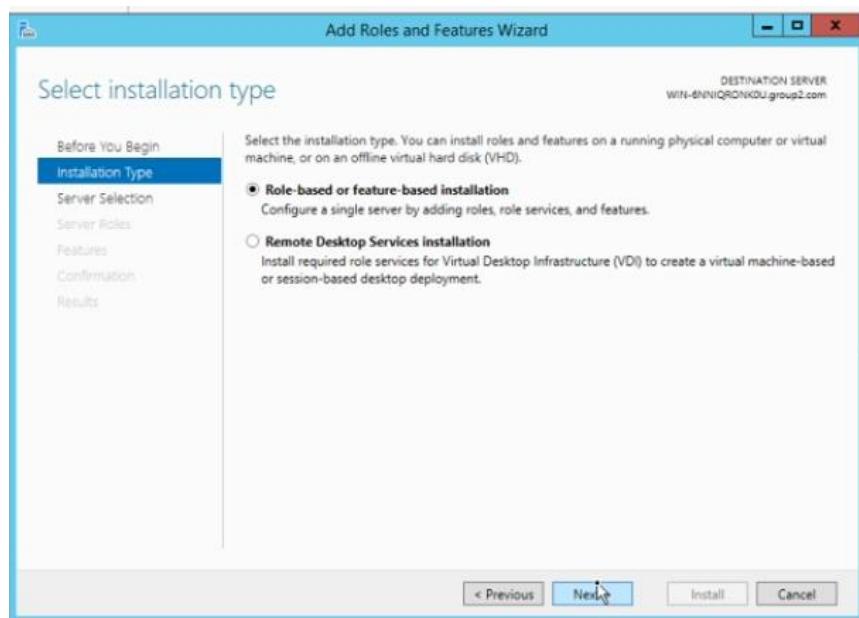


Figure 20 Installation Type

**Step 6:** Select destination server that we want to install the DHCP server. For our workshop, there is only one server which is local server and it is selected by default. Then click next.

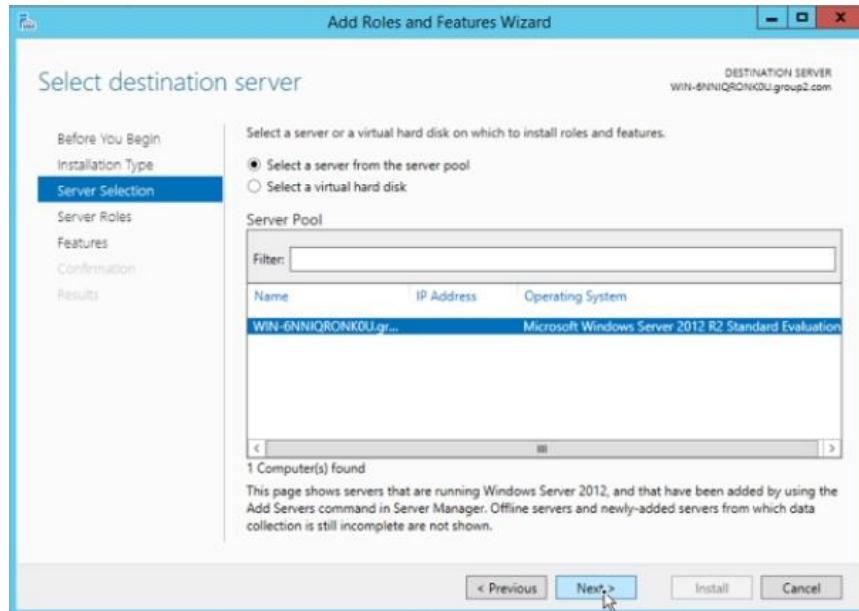


Figure 21 Server Selection

**Step 7:** For the server roles, use default setting and click next.

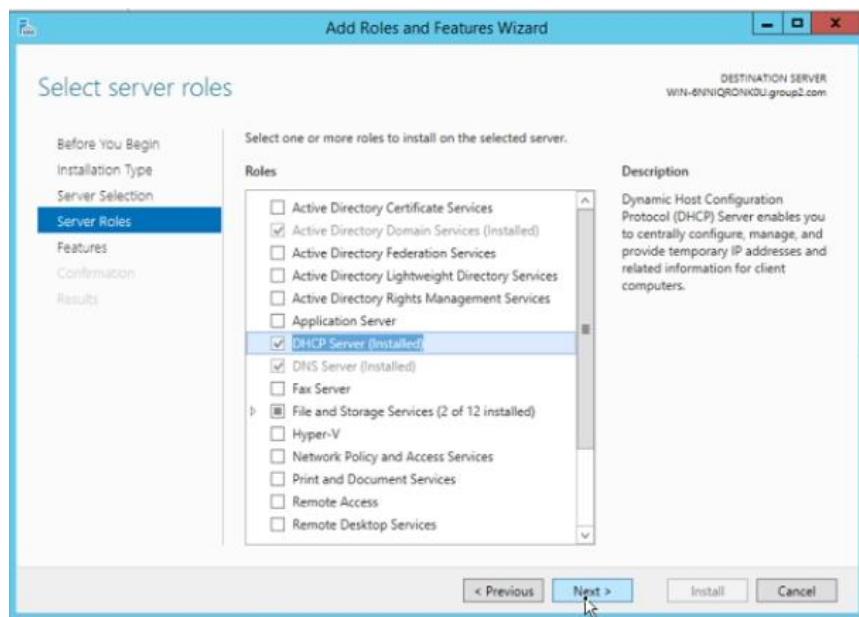


Figure 22 Server Roles

**Step 8:** Go to Server Manager and click tools. Choose DHCP on the dropdown list.

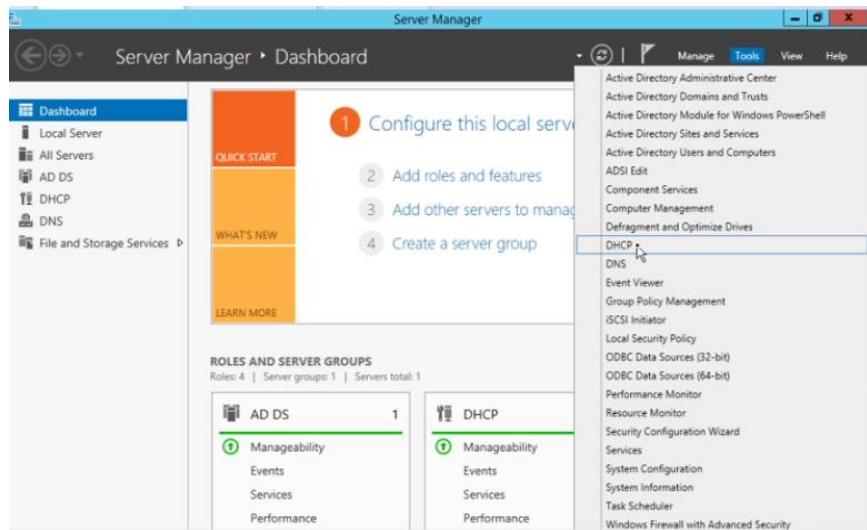


Figure 23 Dashboard

**Step 9:** Right click on IPv4 and click on New scope.

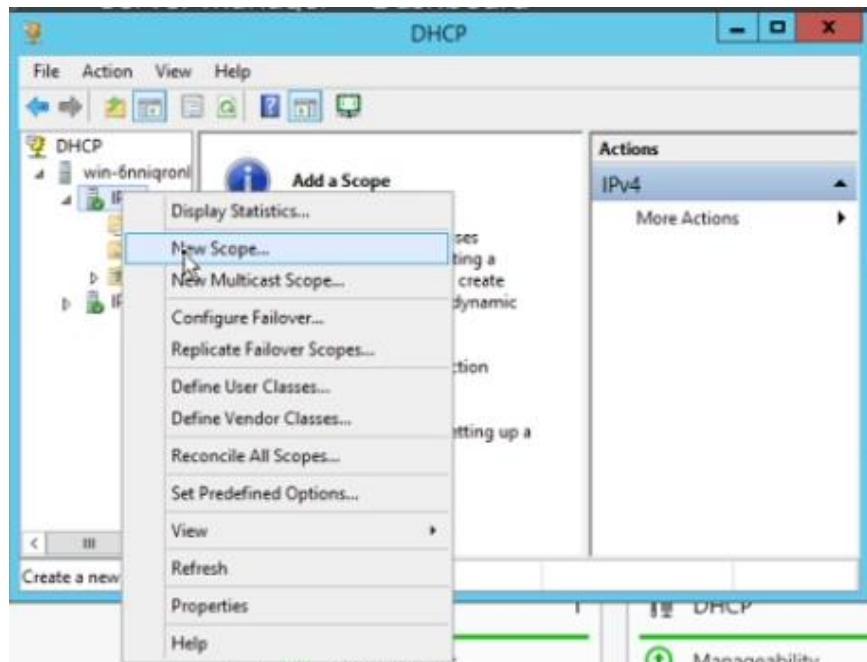


Figure 24 New Scope

**Step 10:** Click next



*Figure 25 New Scope*

**Step 11:** Provide name and meaningful description of the new scope and click next.



*Figure 26 Scope Name*

**Step 12:** Provide IP address range along with subnet mask that need to be distributed to the client machines and click next.



Figure 27 IP Address Range

**Step 13:** Provide any IP addresses that need to be excluded from the pool and click add. Then click next.

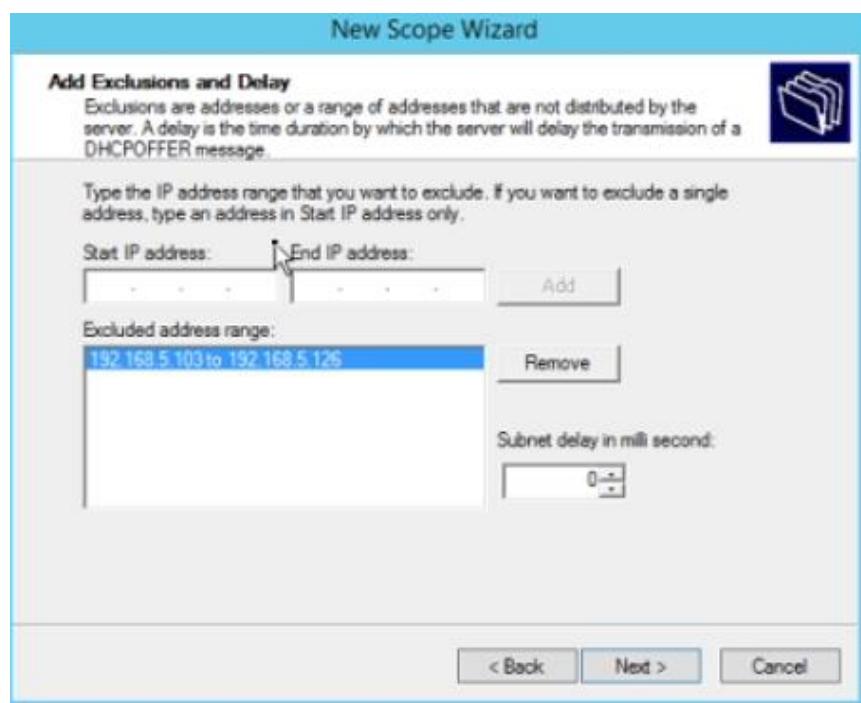


Figure 28 Exclusions

**Step 14:** Keep the lease duration as 8 days and click next.

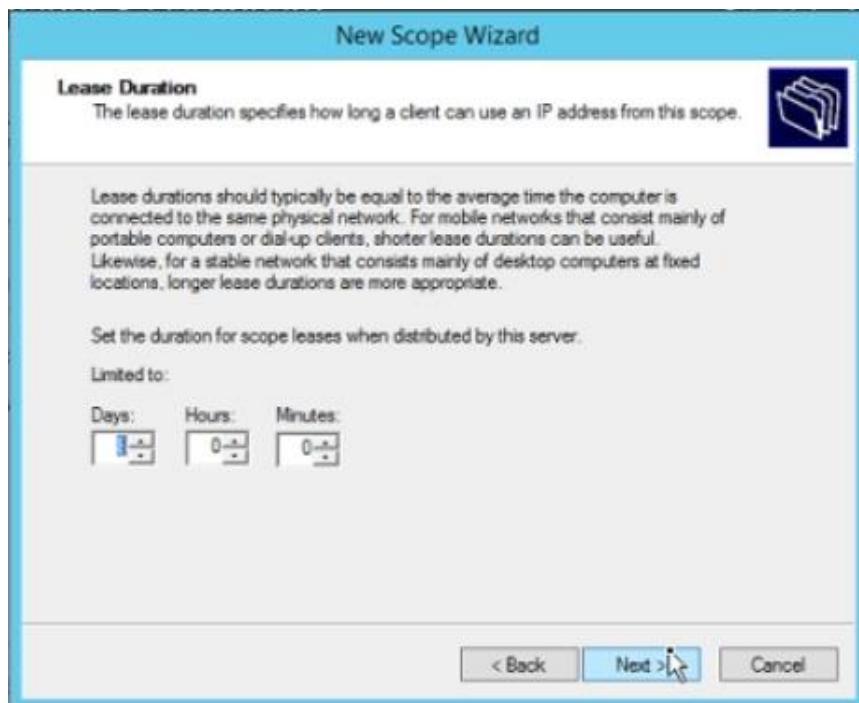


Figure 29 Lease Duration

**Step 15:** Enter the router default gateway.

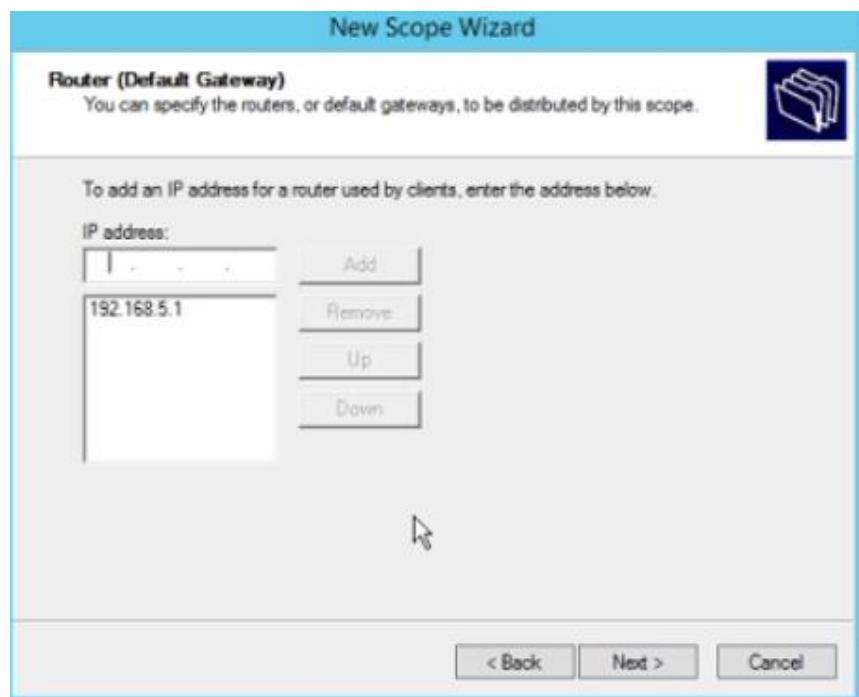


Figure 30 Router Gateway

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



Figure 31 New Scope

**Step 17:** Right-click on the server, click All Tasks and then click Restart to finish the configuration.

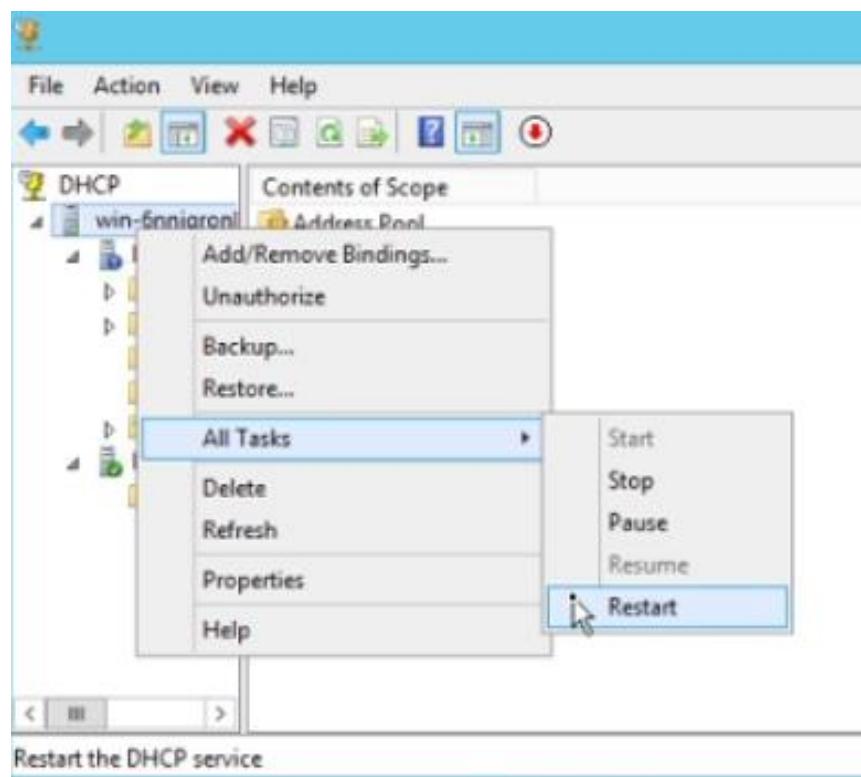


Figure 32 Restart service

### 5.3.2.2 DHCP IPv6

**Step 1:** Right-click on IPv6 and click New Scope.

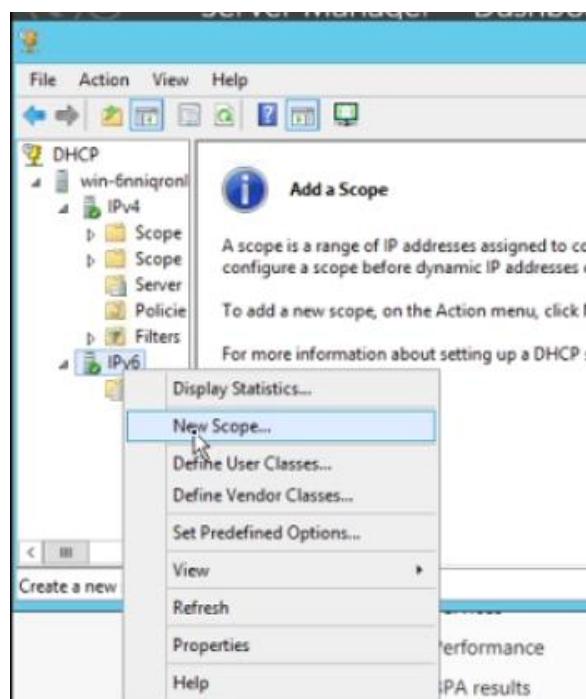


Figure 33 New Scope

**Step 2:** Click Next.

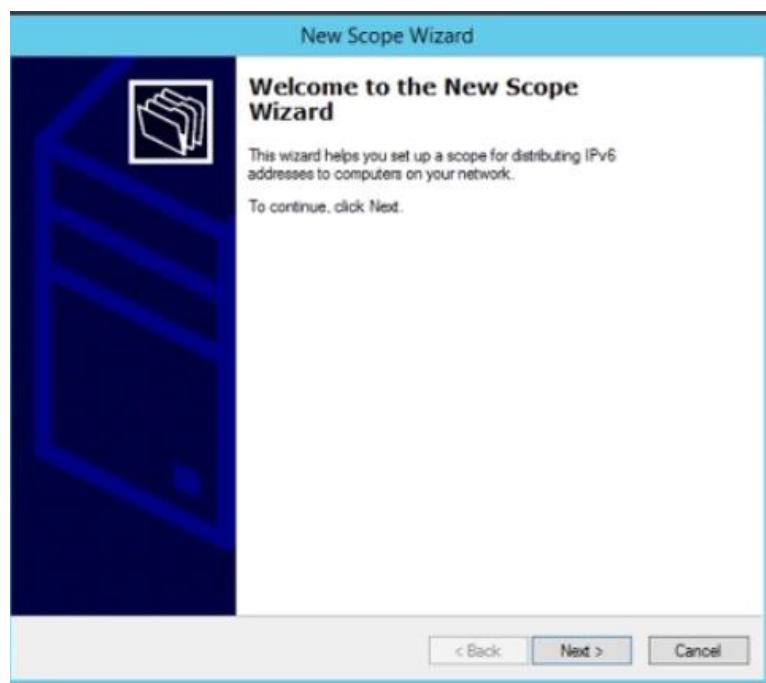


Figure 34 New Scope

**Step 3:** Provide name and meaningful description for the new scope and click next.

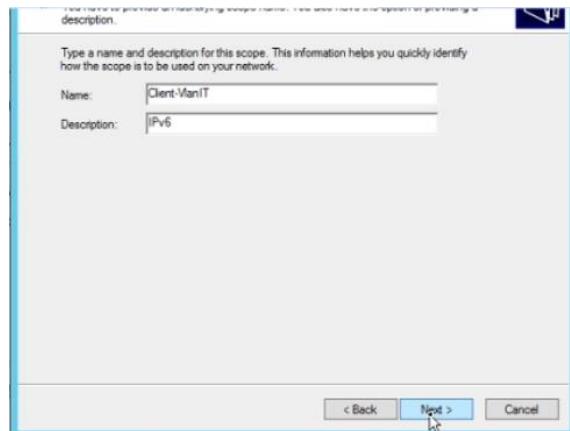


Figure 35 New Scope

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

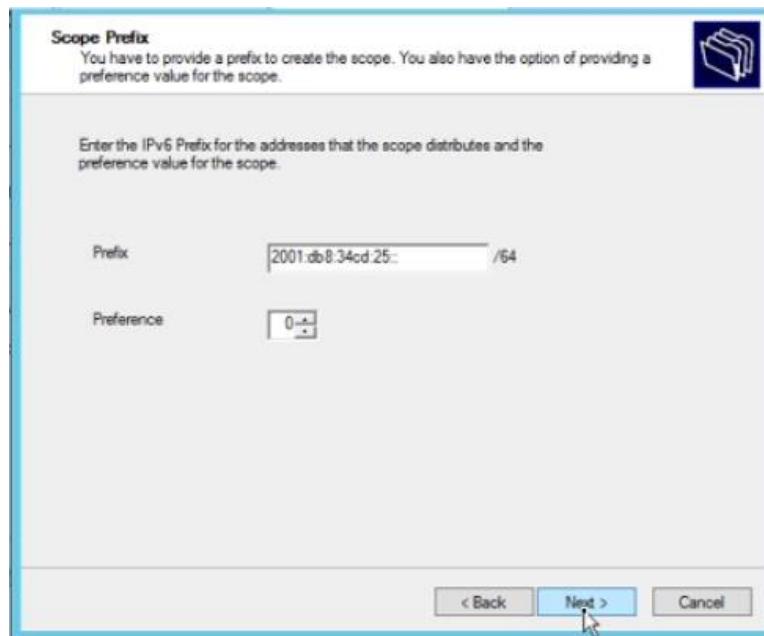


Figure 36 Scope Prefix

**Step 5:** Provide any IP addresses that need to be excluded from the pool and click Add. Then click Next.

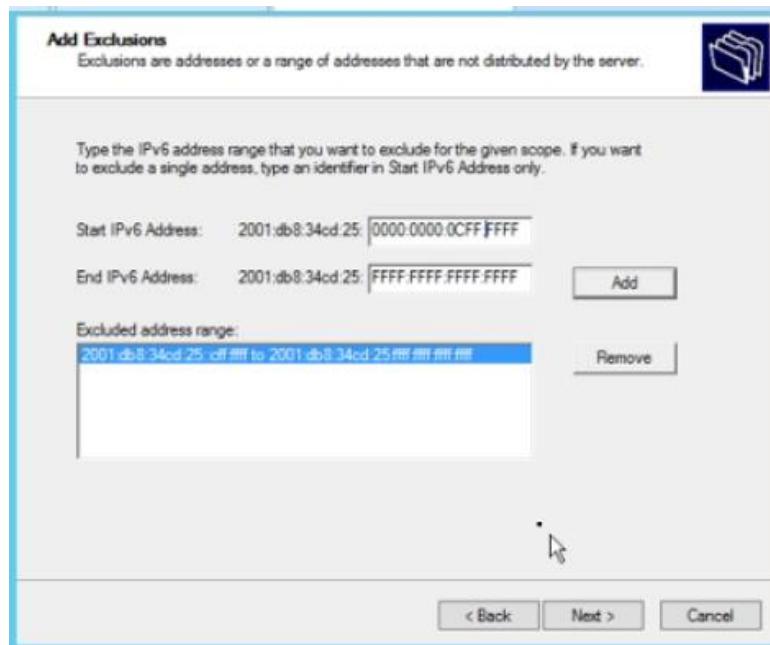


Figure 37 Exclusion

**Step 6:** Click Finish to complete the configuration.

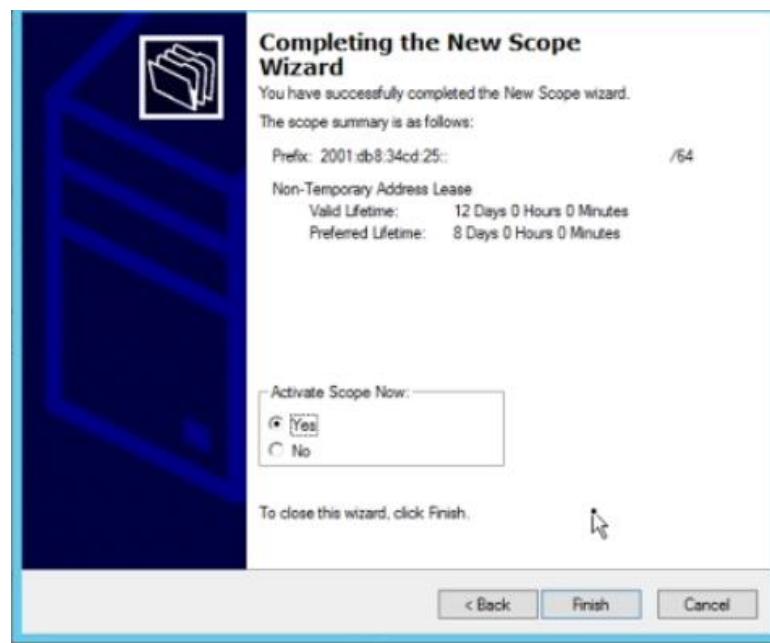


Figure 38 New Scope

### 5.3.3 DYNAMIC ROUTING & NAT

#### 5.3.3.1 STATIC ROUTING

**STEP 1:** Configure router BGP and remote-as 101

```
RouterHQ(config-router)#router bgp 100
RouterHQ(config-router)#neighbor 200.200.200.1 remote-as 101
RouterHQ(config-router)#neighbor 200.200.200.5 remote-as 101
```

*Figure 39 Router BGP and Router-ID*

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

```
RouterHQ(config-router)#network 200.200.200.0 mask 255.255.255.252
RouterHQ(config-router)#network 192.168.5.192 mask 255.255.255.224
RouterHQ(config-router)#network 192.168.5.0 mask 255.255.255.128
```

*Figure 40 Network address*

#### 5.3.3.2 NETWORK ADDRESS TRANSLATION (NAT)

**Step 1:** Set IP Address to the interface connected to neighbor router  
and set IP NAT outside.

```
interface Serial3/0
  ip address 200.200.200.2 255.255.255.224
  ip access-group deny-telnet in
  ip nat outside
  ipv6 address FE80::1 link-local
  ipv6 address 2001:DB8:34CD:16::1/64
  ipv6 enable
  serial restart-delay 0
```

*Figure 41: Set IP Address to neighbor router and Set IP NAT Outside*

**Step 2:** Set the static NAT public IP to all servers.

```
:
ip nat pool HQ_Pool 200.200.200.5 200.200.200.15 netmask 255.255.255.224
ip nat inside source list 2 pool HQ_Pool
ip nat inside source static 192.168.5.200 200.200.200.3
ip nat inside source static 192.168.5.210 200.200.200.4
ip forward-protocol nd
:
```

*Figure 42: Set the static NAT public IP*

**Step 3:** Assign all VLANs under IP NAT inside as follows.

```
interface GigabitEthernet1/0.10
  encapsulation dot1Q 10
  ip address 192.168.5.193 255.255.255.224
  ip access-group permit-http_https out
  ip nat inside
  ipv6 address FE80::1 link-local
  ipv6 address 2001:DB8:34CD:15::4/64
  ipv6 enable
!
interface GigabitEthernet1/0.20
  encapsulation dot1Q 20
  ip address 192.168.5.1 255.255.255.128
  ip access-group permit-email in
  ip access-group permit-email out
  ip helper-address 192.168.5.200
  ip helper-address 192.168.5.210
  ip nat inside
  ipv6 address FE80::1 link-local
  ipv6 address 2001:DB8:34CD:14::1/64
  ipv6 enable
  ipv6 dhcp relay destination 2001:DB8:34CD:15::3
  ipv6 dhcp relay destination 2001:DB8:34CD:15::2
```

Figure 43:Assign all VLANs under IP NAT inside

### 5.3.4 IPSEC SITE-TO-SITE TUNNELING

#### Router HQ

**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. Then, create the pre share key authentication with our peer (neighbor router).

```
crypto isakmp policy 1
  encr aes
  authentication pre-share
  group 2
crypto isakmp key group_2 address 200.200.100.6
```

*Figure 44:Create an ISAKMP phase 1 policy*

**Step 2:** Create the transform set used to protect our data. We have named it as “group2\_transform”. Then, create the profile as “group2\_profile”.

```
crypto ipsec transform-set group2_transform esp-aes esp-sha-hmac
  mode tunnel
!
!
crypto ipsec profile group2_profile
  set transform-set group2_transform
```

*Figure 45:Create the transform set*

**Step 3:** We combine everything on the tunnel interface. We set a source and destination address.

```
interface Tunnel0
  ip address 2.2.2.1 255.255.255.0
  tunnel source 200.200.200.2
  tunnel mode ipsec ipv4
  tunnel destination 200.200.100.6
  tunnel protection ipsec profile group2_profile
```

*Figure 46:Set a source and destination address*

**Step 4:** We set a route that points to the subnet on the other side.

```
ip route 192.168.5.128 255.255.255.192 Tunnel0
```

*Figure 47:Set a route*

**Step 5:** Do the same configuration for router Branch from step 1 to 4, exactly the same in router HQ except for the IP addresses.

### 5.3.5 ACCESS CONTROL LIST

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

```
RouterHQ#conf t
Enter configuration commands, one per line. End with CNTL/Z.
RouterHQ(config)#ip access-list extended PERMIT-HTTP_HTTPS
RouterHQ(config-ext-nacl)#$8.5.179 0.0.0.63 192.168.5.200 0.0.0.31 eq 80
RouterHQ(config-ext-nacl)#$8.5.179 0.0.0.63 192.168.5.200 0.0.0.31 eq 443
RouterHQ(config-ext-nacl)#      deny any any
```

*Figure 48: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 49:Configure the access-group*

### 5.3.6 DOMAIN NAME SYSTEM

#### 5.3.6.1 FORWARD LOOKUP ZONE (PRIMARY DNS)

**Step 1:** Create new DNS using wizard.



Figure 50: Create new DNS using wizard.

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

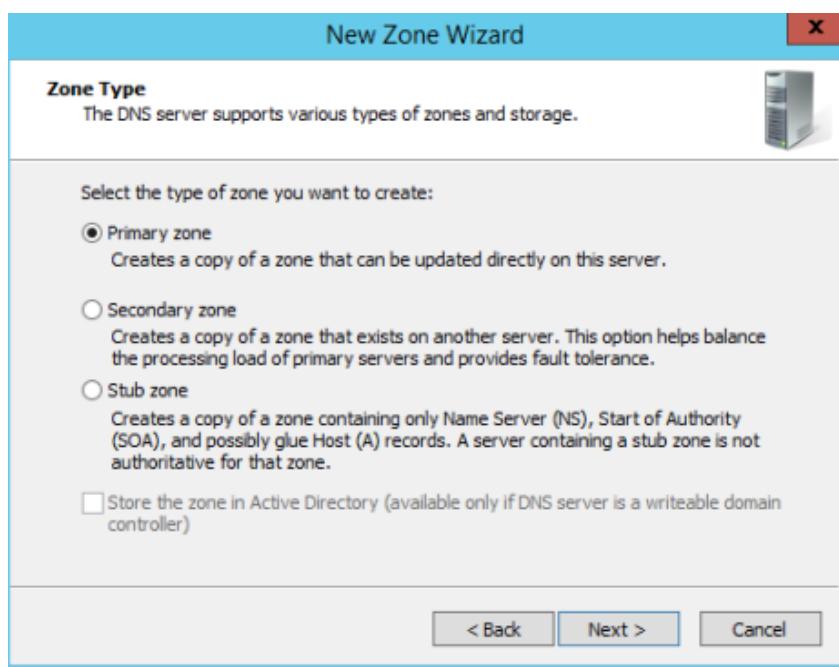


Figure 51: Configure a DNS action

**Step 3:** Then, enter the zone name (examples: group2.com).



Figure 52:Enter the zone name

**Step 4:** For Dynamic Updates, select allow both non-secure and secure dynamic updates. Then, click next.



Figure 53:Allow both non-secure and secure dynamic updates

**Step 5:** As a result of DNS configuration, it will show all the detail that you have enter.

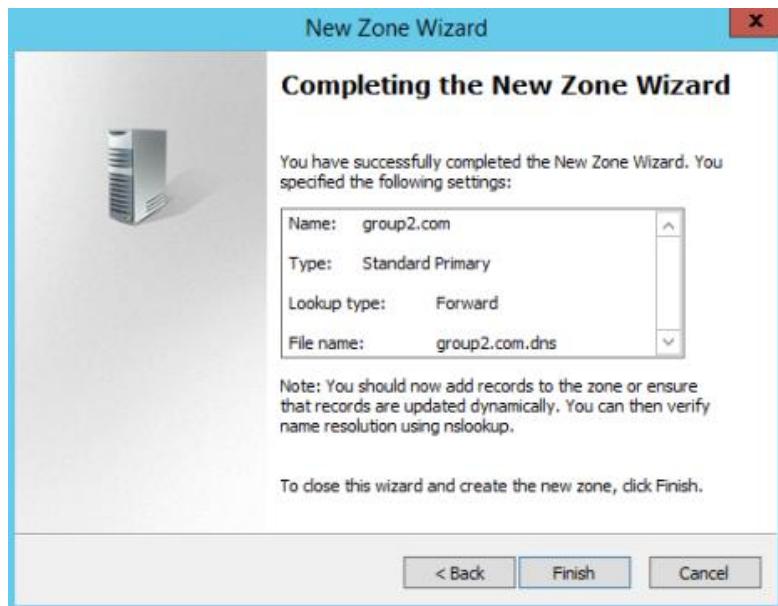


Figure 54:Result of DNS configuration

### 5.3.6.2 REVERSE LOOKUP ZONE (IPv4)

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

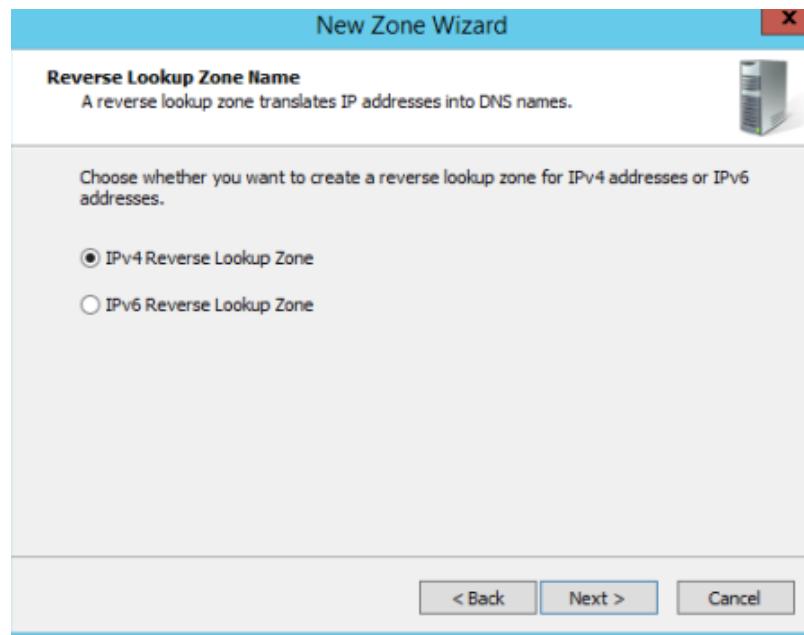


Figure 55:Select IPv4 Reverse Lookup Zone

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

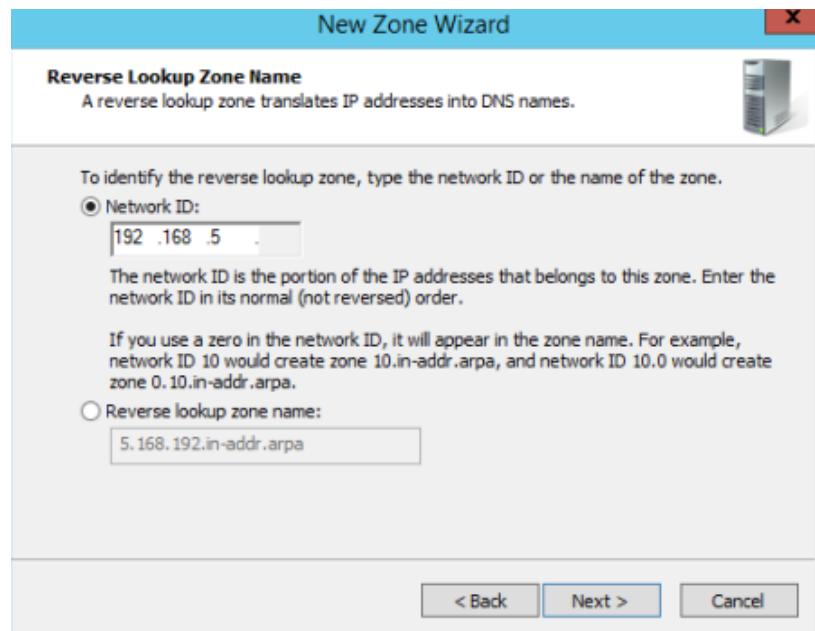


Figure 56:Enter Network ID

**Step 3:** For Dynamic Updates, select allow both non-secure and secure dynamic updates. Then, click next.



Figure 57:Select allow both non-secure and secure dynamic updates

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



*Figure 58:Completed New Zone Wizard*

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

**Step 6:** Click on group2.com and right click then click on New Host (A or AAAA).

**Step 7:** Enter the Name and IP address 192.168.5.200. Tick at Create associated pointer (PTR) record and then, click Add Host.

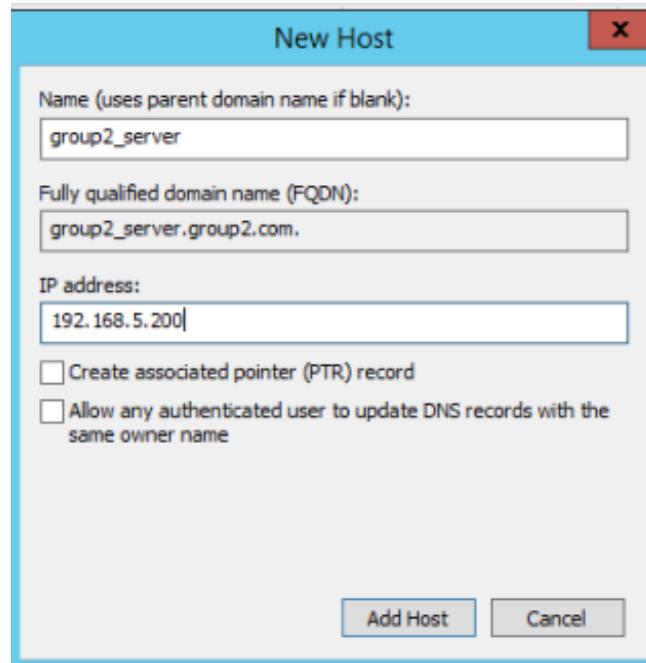


Figure 59:Enter the Name and IP address

#### 5.3.6.3 REVERSE LOOKUP ZONE (IPv6)

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

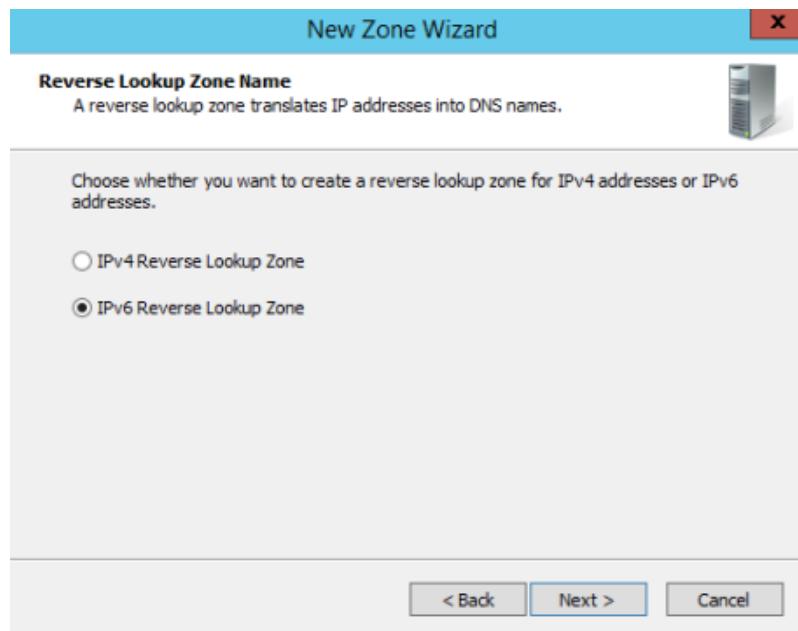
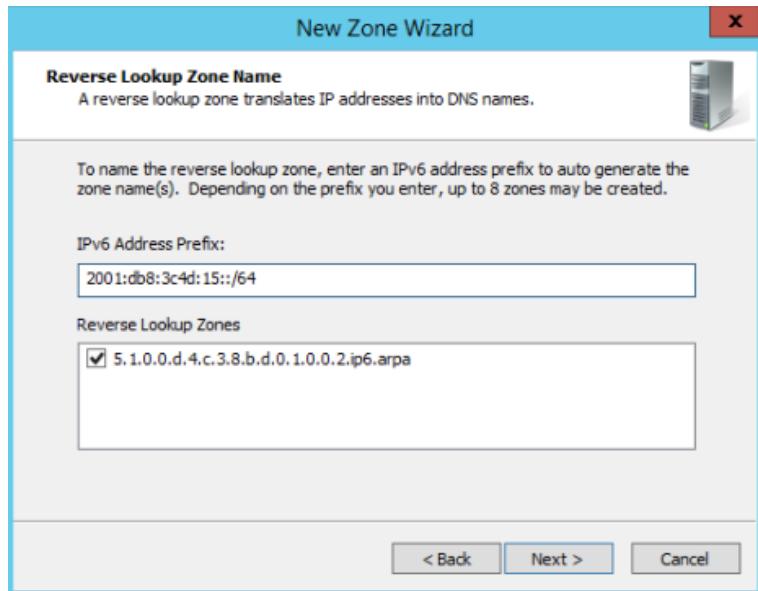


Figure 60:Select IPv6 Reverse Lookup Zone

**Step 2:** Enter IPv6 Address Prefix, 2001:db8:34cd:15::/64 and click next. Then, click Finish.



*Figure 61: Enter IPv6 Address Prefix*

**Step 3:** Create new pointer for reverse lookup IPv6 and browse the Host IP Address and host name from. Then, click OK.

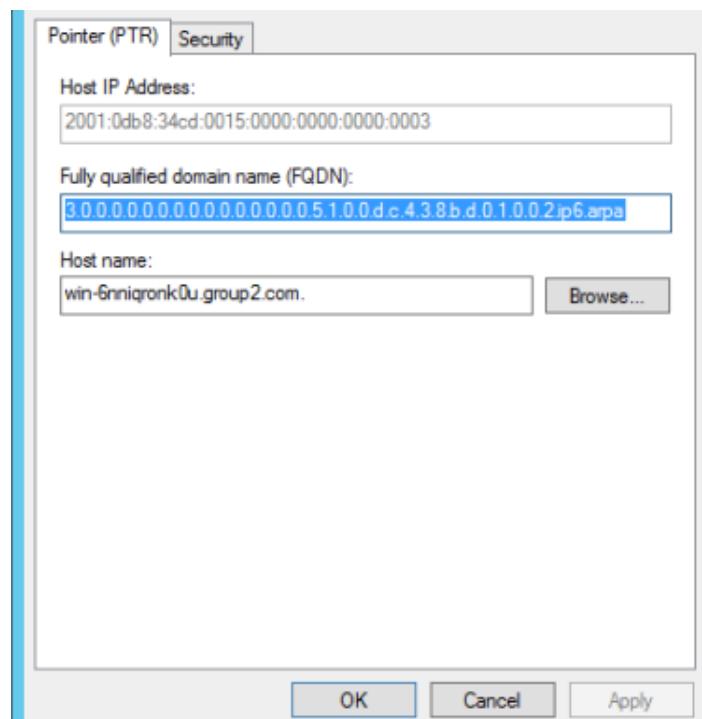
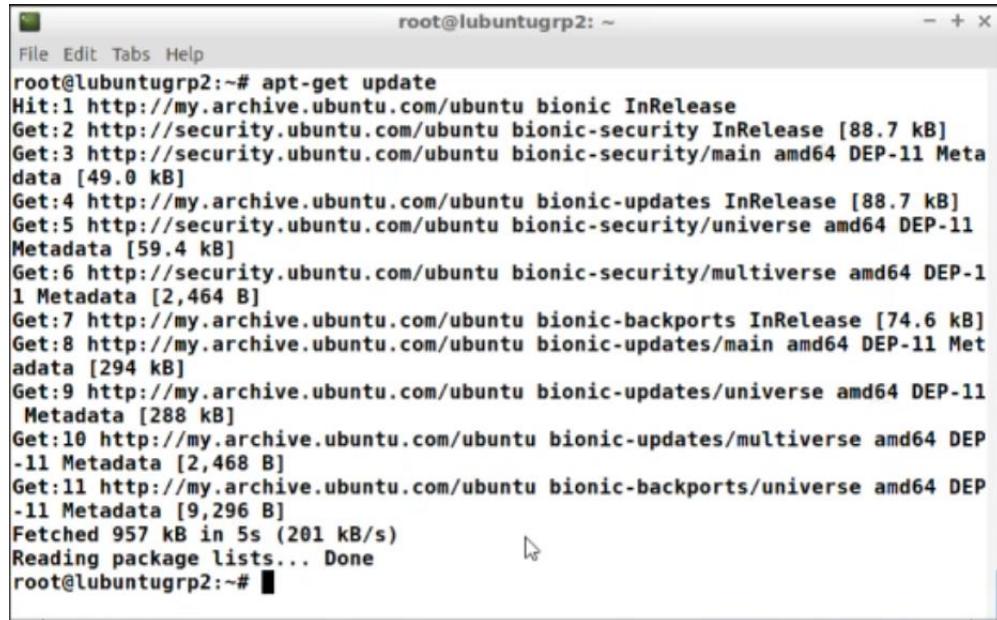


Figure 62: Create new pointer for reverse lookup IPv6

### 5.3.7 LINUX EMAIL SERVER

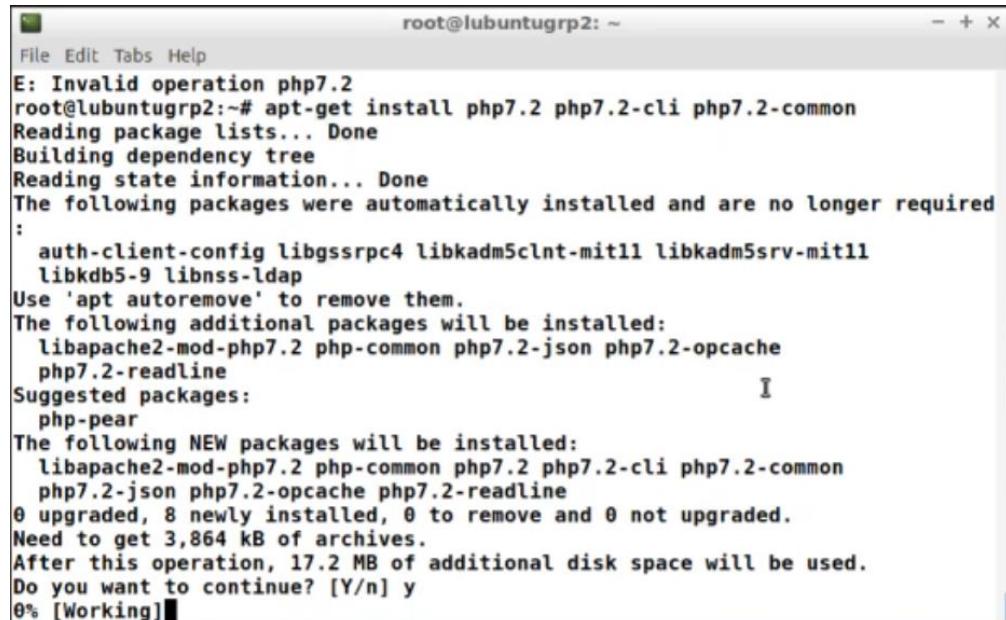
#### Step 1: Install & Update apt



```
root@lubuntugrp2:~# apt-get update
Hit:1 http://my.archive.ubuntu.com/ubuntu bionic InRelease
Get:2 http://security.ubuntu.com/ubuntu bionic-security InRelease [88.7 kB]
Get:3 http://security.ubuntu.com/ubuntu bionic-security/main amd64 DEP-11 Meta
data [49.0 kB]
Get:4 http://my.archive.ubuntu.com/ubuntu bionic-updates InRelease [88.7 kB]
Get:5 http://security.ubuntu.com/ubuntu bionic-security/universe amd64 DEP-11
Metadata [59.4 kB]
Get:6 http://security.ubuntu.com/ubuntu bionic-security/multiverse amd64 DEP-1
1 Metadata [2,464 B]
Get:7 http://my.archive.ubuntu.com/ubuntu bionic-backports InRelease [74.6 kB]
Get:8 http://my.archive.ubuntu.com/ubuntu bionic-updates/main amd64 DEP-11 Met
adata [294 kB]
Get:9 http://my.archive.ubuntu.com/ubuntu bionic-updates/universe amd64 DEP-11
Metadata [288 kB]
Get:10 http://my.archive.ubuntu.com/ubuntu bionic-updates/multiverse amd64 DEP
-11 Metadata [2,468 B]
Get:11 http://my.archive.ubuntu.com/ubuntu bionic-backports/universe amd64 DEP
-11 Metadata [9,296 B]
Fetched 957 kB in 5s (201 kB/s)
Reading package lists... Done
root@lubuntugrp2:~#
```

Figure 63: Updating apt

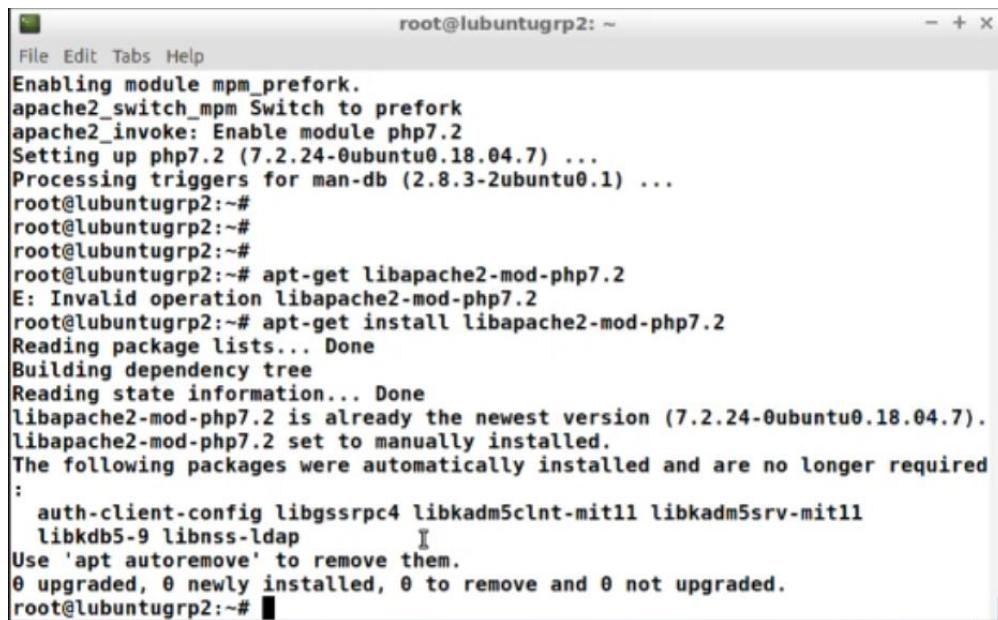
#### Step 2: Install apache php 7.2.



```
E: Invalid operation php7.2
root@lubuntugrp2:~# apt-get install php7.2 php7.2-cli php7.2-common
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required
:
  auth-client-config libgssrpc4 libkadm5clnt-mit11 libkadm5srv-mit11
  libkdb5-9 libnss-ldap
Use 'apt autoremove' to remove them.
The following additional packages will be installed:
  libapache2-mod-php7.2 php-common php7.2-json php7.2-opcache
    php7.2-readline
Suggested packages:
  php-pear
The following NEW packages will be installed:
  libapache2-mod-php7.2 php-common php7.2 php7.2-cli php7.2-common
    php7.2-json php7.2-opcache php7.2-readline
0 upgraded, 8 newly installed, 0 to remove and 0 not upgraded.
Need to get 3,864 kB of archives.
After this operation, 17.2 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
0% [Working]
```

Figure 64: Installation of apache2 php7.2

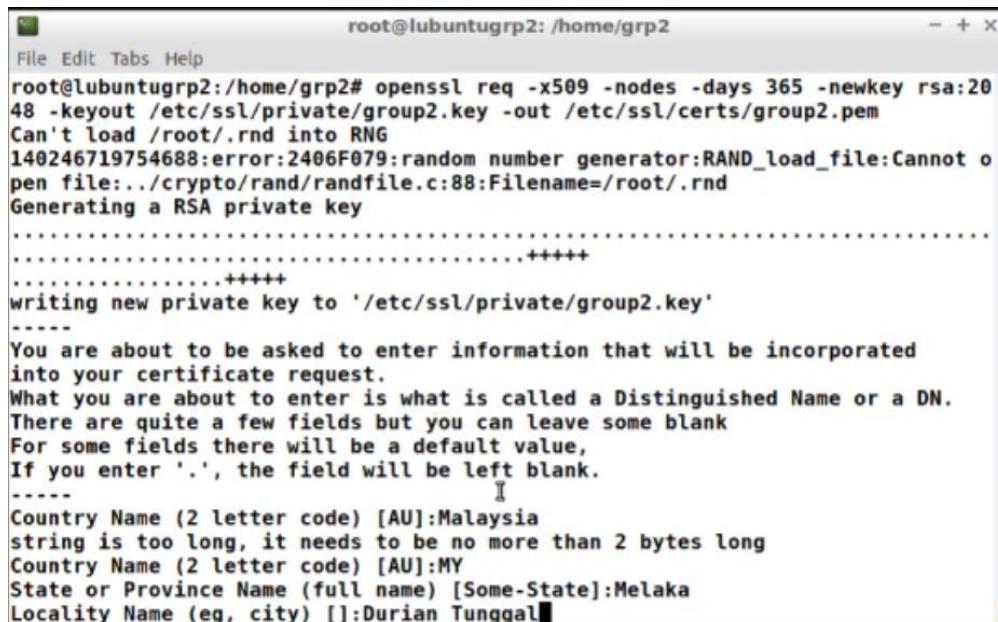
**Step 3:** Install libapache2-mod-php.



```
root@lubuntugrp2: ~
File Edit Tabs Help
Enabling module mpm_prefork.
apache2_switch_mpm Switch to prefork
apache2_invoke: Enable module php7.2
Setting up php7.2 (7.2.24-0ubuntu0.18.04.7) ...
Processing triggers for man-db (2.8.3-2ubuntu0.1) ...
root@lubuntugrp2:~
root@lubuntugrp2:~
root@lubuntugrp2:~
root@lubuntugrp2:~# apt-get libapache2-mod-php7.2
E: Invalid operation libapache2-mod-php7.2
root@lubuntugrp2:~# apt-get install libapache2-mod-php7.2
Reading package lists... Done
Building dependency tree
Reading state information... Done
libapache2-mod-php7.2 is already the newest version (7.2.24-0ubuntu0.18.04.7).
libapache2-mod-php7.2 set to manually installed.
The following packages were automatically installed and are no longer required
:
  auth-client-config libgssrpc4 libkadm5clnt-mit11 libkadm5srv-mit11
  libkdb5-9 libnss-ldap
Use 'apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
root@lubuntugrp2:~#
```

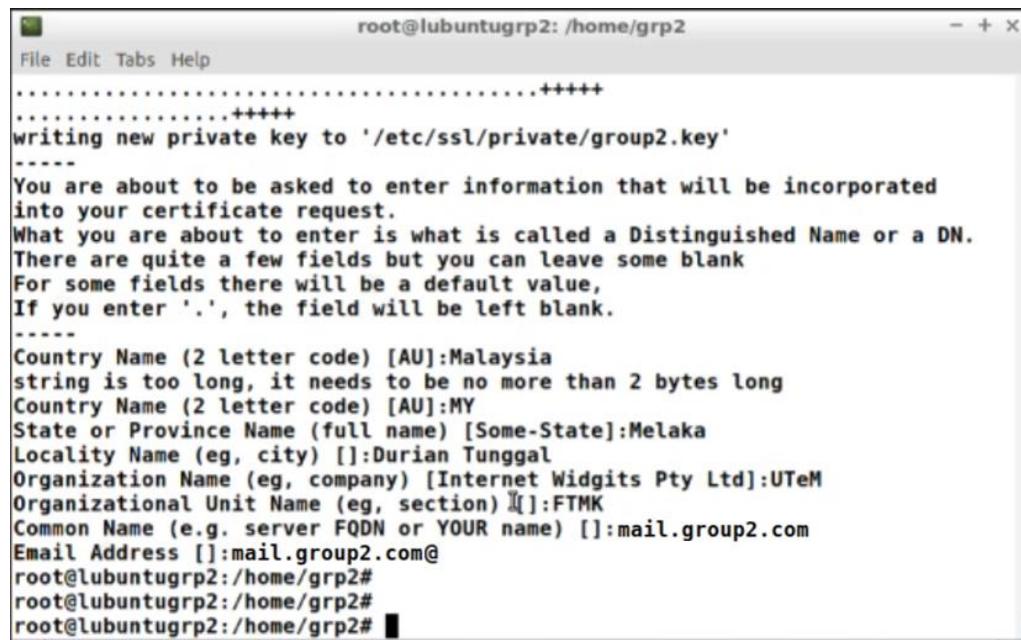
Figure 65: Installation of libapache2-mod-php

**Step 4:** Creating SSL certificate.



```
root@lubuntugrp2: /home/grp2
File Edit Tabs Help
root@lubuntugrp2:/home/grp2# openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/group2.key -out /etc/ssl/certs/group2.pem
Can't load /root/.rnd into RNG
140246719754688:error:2406F079:random number generator:RAND_load_file:Cannot open file:../crypto/rand/randfile.c:88:Filename=/root/.rnd
Generating a RSA private key
-----
.....+++++
.....+++++
writing new private key to '/etc/ssl/private/group2.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]:Malaysia
string is too long, it needs to be no more than 2 bytes long
Country Name (2 letter code) [AU]:MY
State or Province Name (full name) [Some-State]:Melaka
Locality Name (eg, city) []:Durian Tunggal
```

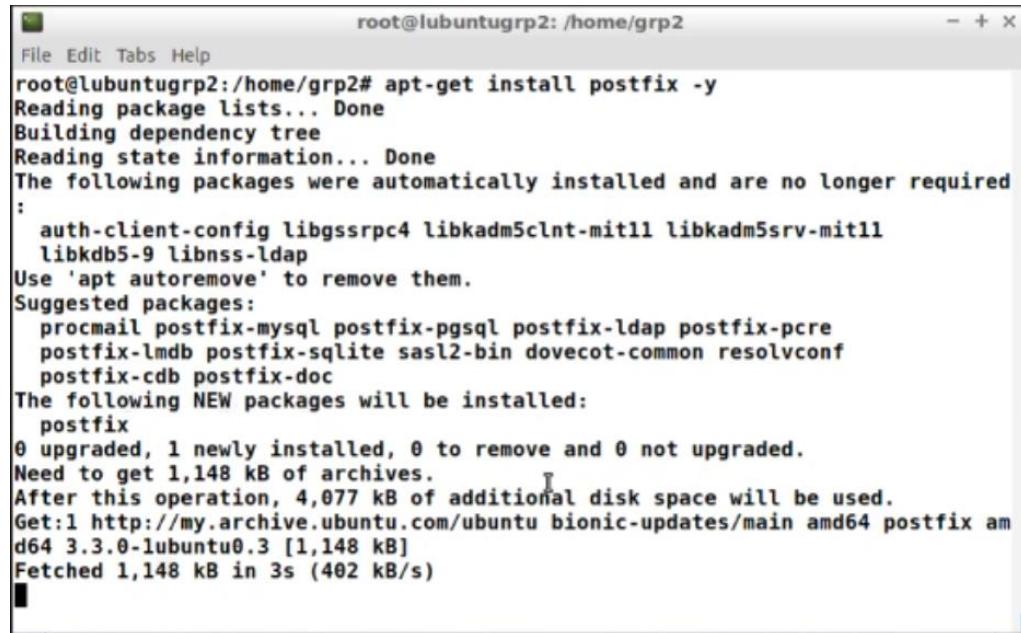
Figure 66: Creating SSL certificate (Part 1)



```
root@lubuntugrp2: /home/grp2
File Edit Tabs Help
.....+++++
.....+++++
writing new private key to '/etc/ssl/private/group2.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]:Malaysia
string is too long, it needs to be no more than 2 bytes long
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.group2.com
Email Address []:mail.group2.com@
root@lubuntugrp2:/home/grp2#
root@lubuntugrp2:/home/grp2#
root@lubuntugrp2:/home/grp2#
```

Figure 67: Creating SSL certificate (Part 2)

### Step 5: Installing Postfix.



```
root@lubuntugrp2: /home/grp2
File Edit Tabs Help
root@lubuntugrp2:/home/grp2# apt-get install postfix -y
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required
:
  auth-client-config libgssrpc4 libkadm5clnt-mit11 libkadm5srv-mit11
  libkdb5-9 libnss-ldap
Use 'apt autoremove' to remove them.
Suggested packages:
  procmail postfix-mysql 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:
  postfix
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 1,148 kB of archives.
After this operation, 4,077 kB of additional disk space will be used.
Get:1 http://my.archive.ubuntu.com/ubuntu bionic-updates/main amd64 postfix am
d64 3.3.0-1ubuntu0.3 [1,148 kB]
Fetched 1,148 kB in 3s (402 kB/s)
#
```

Figure 68: Installing Postfix

**Step 6:** During installation, you will be asked to choose the default file configuration for your Server. Select **Ok**.

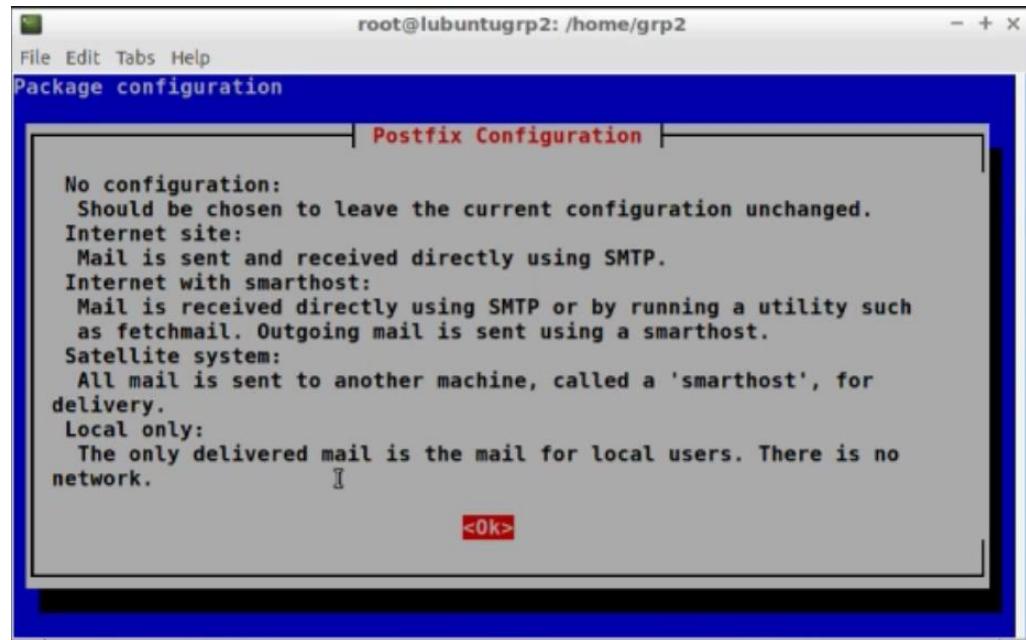


Figure 69: Postfix configuration

**Step 7:** Select “Internet Site” as type of mail configuration.

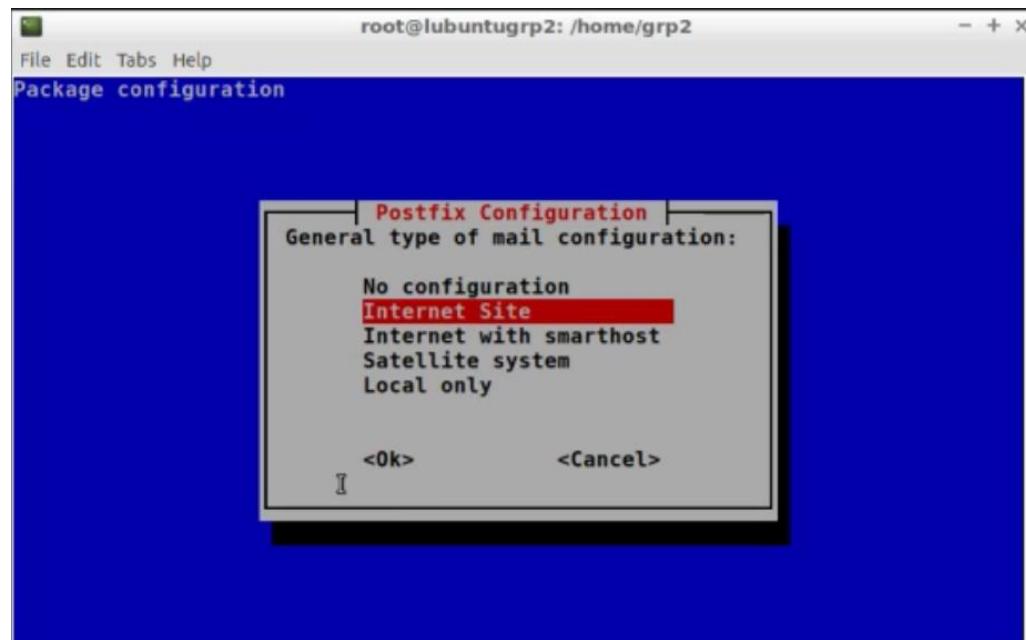


Figure 70: Choosing Internet Site

**Step 8:** At the next Postfix Configuration interface, type in the domain name which is “mail.group7.com”.

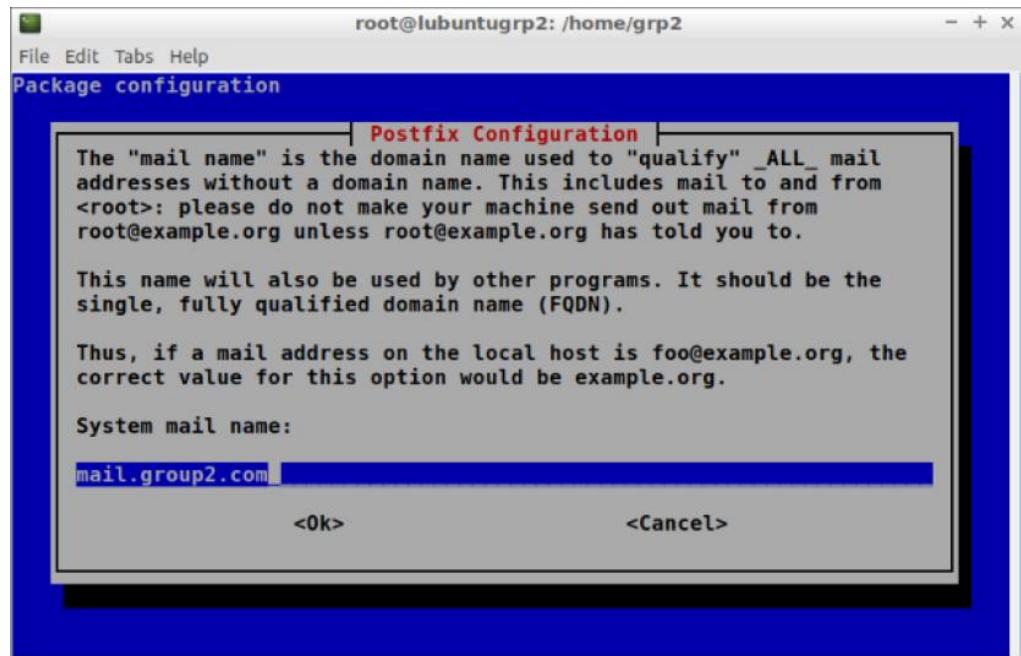


Figure 71: Adding domain for mail.group2.com

**Step 9:** Enter mail.group2@ as the Root and Postmaster Mail Recipient.

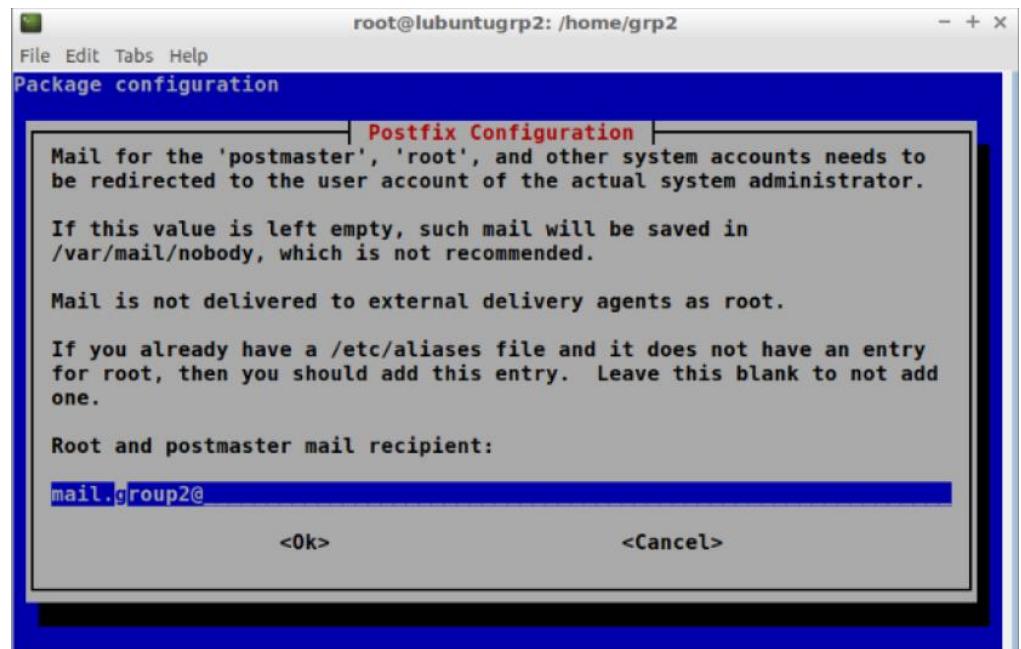


Figure 72: Configuring Root and Postmaster Mail Recipient

**Step 10:** Type in the possible domains for which the email server is capable of accepting the emails.

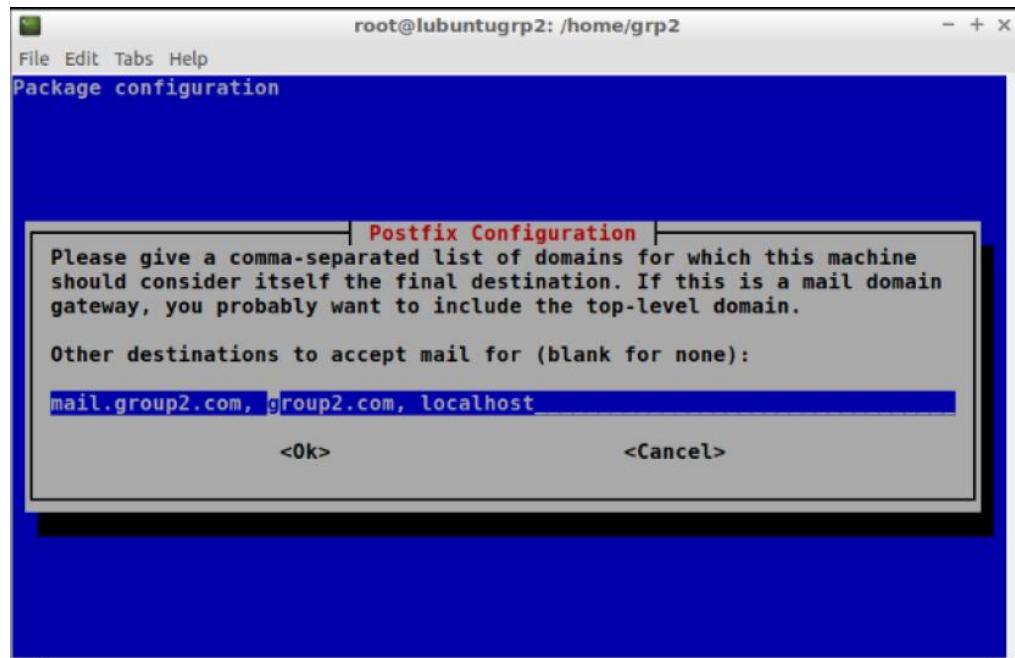


Figure 73: Adding domain for email server that is capable of accepting the emails

**Step 11:** Configuring Postfix in master.cf file

A screenshot of a terminal window titled "root@lubuntugrp2: /home/grp2". Inside the terminal, a nano editor window is open with the file "/etc/postfix/master.cf". The file contains the following configuration:

```
-o syslog_name=postfix/submission
-o smtpd_tls_security_level=encrypt
-o smtpd_sasl_auth_enable=yes
-o smtpd_tls_auth_only=yes
-o smtpd_tls_wrappermode=no
# -o smtpd_reject_unlisted_recipient=no
# -o smtpd_client_restrictions=$mua_client_restrictions
# -o smtpd_helo_restrictions=$mua_helo_restrictions
# -o smtpd_sender_restrictions=$mua_sender_restrictions
-o smtpd_recipient_restrictions=permit_mynetworks,permit_sasl_authenticated,reject
-o smtpd_relay_restrictions=permit_sasl_authenticated,reject
-o smtpd_sasl_type=dovecot
-o smtpd_sasl_path=private/auth

# -o milter_macro_daemon_name=ORIGINATING
#smtps      inet  n       -       y       -       -          smtpd
# -o syslog_name=postfix/smtps
```

The status bar at the bottom of the nano window shows "[ Wrote 131 lines ]". Below the status bar are standard nano key bindings: ^G Get Help, ^O Write Out, ^W Where Is, ^K Cut Text, ^J Justify, ^X Exit, ^R Read File, ^\ Replace, ^U Uncut Text, ^T To Spell.

Figure 74: Edit and add the codes in master.cf

**Step 12:** Configuring Postfix in main.cf file.

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

```
# See /usr/share/postfix/main.cf.dist for a commented, more complete version

# Debian specific: Specifying a file name will cause the first
# line of that file to be used as the name. The Debian default
# is /etc/mailname.
#myorigin = /etc/mailname

smtpd_banner = $myhostname ESMTP
biff = no

# appending .domain is the MUA's job.
append_dot_mydomain = no

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

readme_directory = no

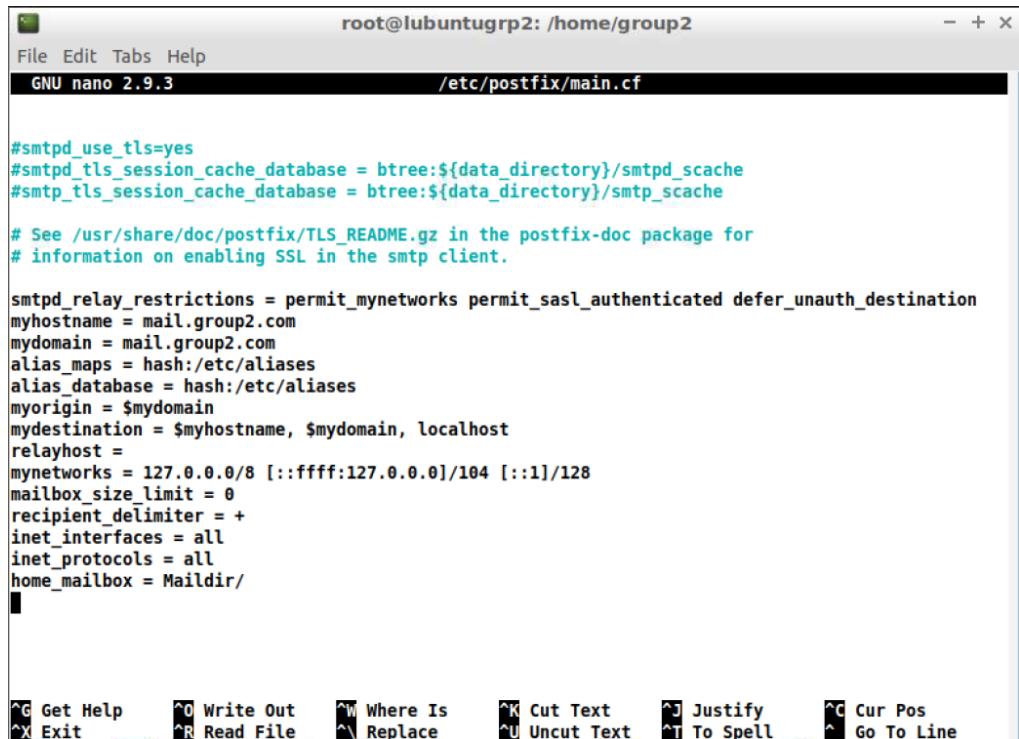
# See http://www.postfix.org/COMPATIBILITY_README.html -- default to 2 on
# fresh installs.
compatibility_level = 2
```

Figure 75: Edit and add the codes in main.cf (Part 1)

```
compatibility_level = 2

# TLS parameters
smtpd_tls_cert_file=/etc/ssl/certs/group2.pem
smtpd_tls_key_file=/etc/ssl/private/group2.key
smtpd_tls_security_level=may
smtpd_tls_protocols = !SSLv2, !SSLv3 !TLSv1
smtpd_tls_loglevel = 1
smtpd_tls_session_cache_database = btree:${data_directory}/smtpd_scache
smtp_tls_loglevel = 1
smtp_tls_security_level = may
smtp_tls_session_cache_database = btree:${data_directory}/smtp_scache
```

Figure 76: Edit and add the codes in main.cf (Part 2)



```

root@lubuntugrp2: /home/group2
File Edit Tabs Help
GNU nano 2.9.3          /etc/postfix/main.cf

#smtpd_use_tls=yes
#smtpd_tls_session_cache_database = btree:${data_directory}/smtpd_scache
#smtp_tls_session_cache_database = btree:${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.

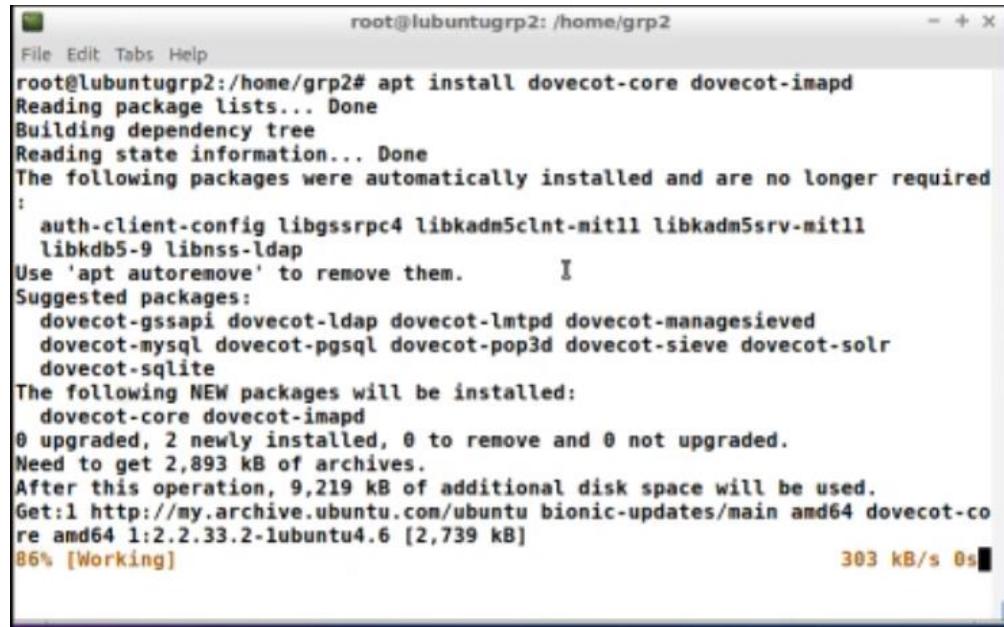
smtpd_relay_restrictions = permit_mynetworks permit_sasl_authenticated defer_unauth_destination
myhostname = mail.group2.com
mydomain = mail.group2.com
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
myorigin = $mydomain
mydestination = $myhostname, $mydomain, localhost
relayhost =
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
home_mailbox = Maildir/

```

Toolbar icons: Get Help, Write Out, Where Is, Cut Text, Justify, Cur Pos, Exit, Read File, Replace, Uncut Text, To Spell, Go To Line.

Figure 77: Edit and add the codes in main.cf (Part 2)

### Step 13: Installing Dovecot.



```

root@lubuntugrp2: /home/grp2
File Edit Tabs Help
root@lubuntugrp2:/home/grp2# apt 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:
:
  auth-client-config libgssrpc4 libkadm5clnt-mit11 libkadm5srv-mit11
  libkdb5-9 libnss-ldap
Use 'apt autoremove' to remove them.           I
Suggested packages:
  dovecot-gssapi dovecot-ldap dovecot-lmtpd dovecot-managesieved
  dovecot-mysql dovecot-pgsql dovecot-pop3d dovecot-sieve dovecot-solr
  dovecot-sqlite
The following NEW packages will be installed:
  dovecot-core dovecot-imapd
0 upgraded, 2 newly installed, 0 to remove and 0 not upgraded.
Need to get 2,893 kB of archives.
After this operation, 9,219 kB of additional disk space will be used.
Get:1 http://my.archive.ubuntu.com/ubuntu bionic-updates/main amd64 dovecot-core amd64 1:2.2.33.2-lubuntu4.6 [2,739 kB]
86% [Working]                                303 kB/s 0s

```

Figure 78: Installing Dovecot for imap or pop3

**Step 14:** Configure Dovecot in etc/dovecot/dovecot.conf file.

```
nano /etc/dovecot/dovecot.conf
```

The screenshot shows a terminal window titled "root@lubuntugrp2: /home/group2". The title bar also displays "GNU nano 2.9.3" and the file path "/etc/dovecot/dovecot.conf". The main area of the window contains the configuration file content. The configuration includes sections for protocols (imap), default values, installed protocols, and various settings like disable\_plaintext\_auth and ssl. It also defines a listen address of '\*' and a base directory of "/var/run/dovecot". The bottom of the window shows the nano editor's command bar with various keyboard shortcuts for navigation and editing.

```
# protocol imap { }, local 127.0.0.1 { }, remote 10.0.0.0/8 { }

# Default values are shown for each setting, it's not required to uncomment
# those. These are exceptions to this though: No sections (e.g. namespace {})
# or plugin settings are added by default, they're listed only as examples.
# Paths are also just examples with the real defaults being based on configure
# options. The paths listed here are for configure --prefix=/usr
# --sysconfdir=/etc --localstatedir=/var

# Enable installed protocols
!include_try /usr/share/dovecot/protocols.d/*.protocol

disable_plaintext_auth=no
ssl=yes
# A comma separated list of IPs or hosts where to listen in for connections.
# "*" listens in all IPv4 interfaces, ":::" listens in all IPv6 interfaces.
# If you want to specify non-default ports or anything more complex,
# edit conf.d/master.conf.
listen = *, ::

# Base directory where to store runtime data.
#base_dir = /var/run/dovecot

# Name of this instance. In multi-instance setup dovecadm and other commands
```

Figure 79: Configuring dovecot.conf (Part 1)

The screenshot shows a continuation of the configuration file in the nano editor. It includes sections for dict (with quota and expire settings), protocols (imap), and mail\_location (mbox and maildir). The configuration is described as being sorted by ASCII value and parsed in that order, with 00-prefixes in filenames.

```
dict {
    #quota = mysql:/etc/dovecot/dovecot-dict-sql.conf.ext
    #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

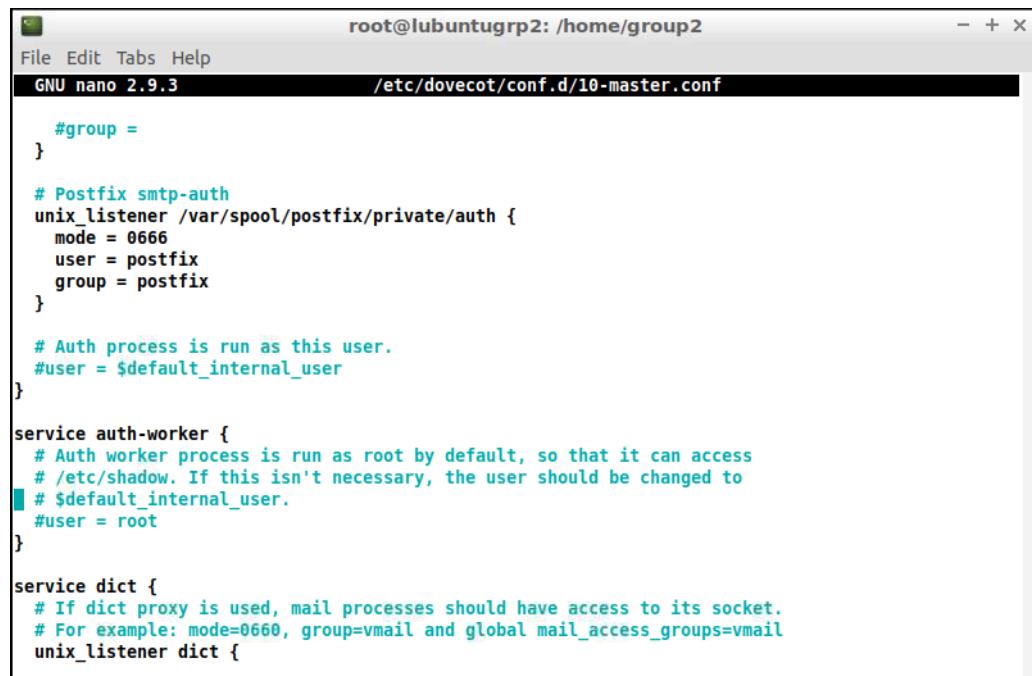
# A config file can also tried to be included without giving an error if
# it's not found:
!include_try local.conf

protocols = imap
mail_location = mbox:~/mail:INBOX=/var/mail/%u
mail_location = maildir:~/Maildir
```

Figure 80: Configuring dovecot.conf (Part 1)

**Step 15:** Configuring Dovecot in etc/dovecot/conf.d/10-master.conf file. Also, uncomment unix\_listener and add postfix to user & group.

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



```
root@lubuntugrp2: /home/group2
File Edit Tabs Help
GNU nano 2.9.3          /etc/dovecot/conf.d/10-master.conf

#group =
}

# Postfix smtp-auth
unix_listener /var/spool/postfix/private/auth {
    mode = 0666
    user = postfix
    group = postfix
}

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

service auth-worker {
    # Auth worker process is run as root by default, so that it can access
    # /etc/shadow. If this isn't necessary, the user should be changed to
    # $default_internal_user.
    #user = root
}

service dict {
    # If dict proxy is used, mail processes should have access to its socket.
    # For example: mode=0660, group=vmail and global mail_access_groups=vmail
    unix_listener dict {
```

Figure 81: Configuring 10-master.conf file

**Step 16:** SSL/TLS config file by changing “ssl = no” to “ssl = required”

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

```
#  
## 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/group2.pem  
ssl_key = </etc/ssl/private/group2.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 =  
  
[ Read 63 lines ]
```

Figure 82: Configuring 10-ssl.conf file

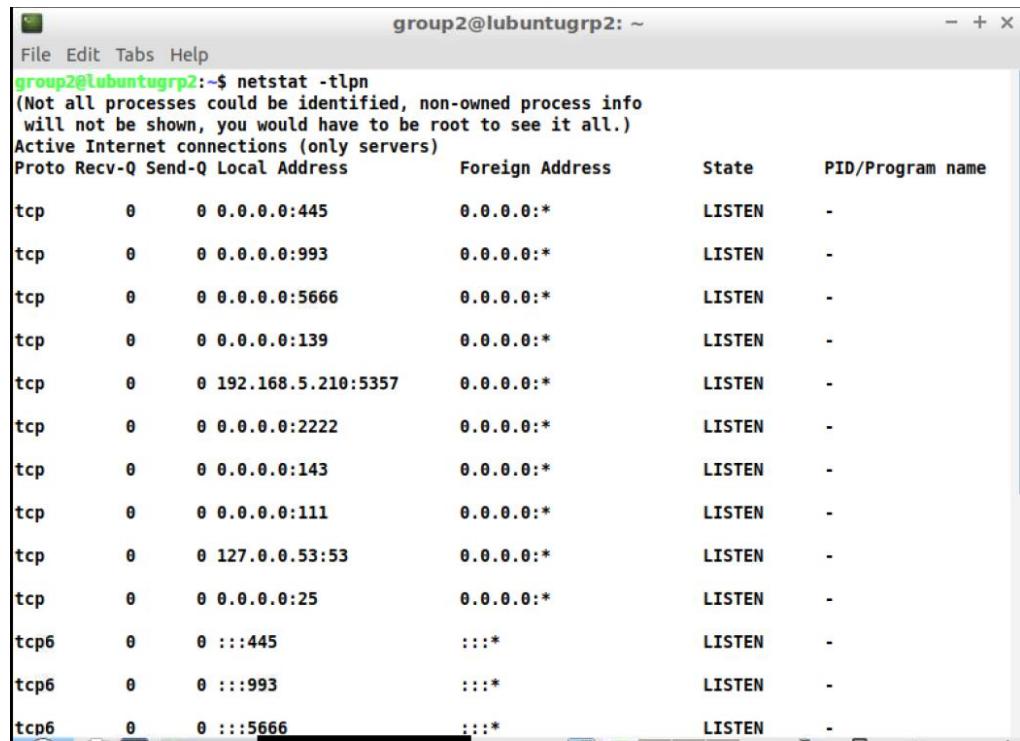
**Step 17:** Restart the Dovecot and Postfix. Then, Check the status of Dovecot and Postfix.

```
systemctl restart dovecot.service
```

```
systemctl restart postfix.service
```

```
systemctl restart status dovecot.service
```

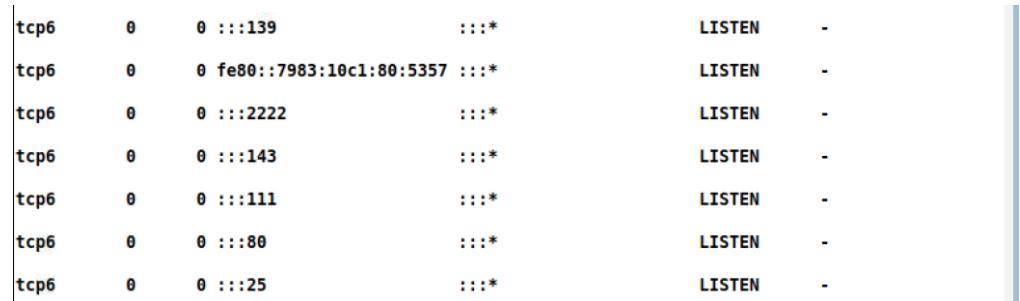
**Step 18:** Check the port for 143 and 25.



The screenshot shows a terminal window titled "group2@lubuntugrp2: ~". The window contains the command "netstat -tlpn" and its output. The output lists active Internet connections (only servers) with columns for Proto, Recv-Q, Send-Q, Local Address, Foreign Address, State, and PID/Program name. The "Local Address" column includes both IPv4 and IPv6 entries. The "Foreign Address" column shows mostly ":::\*" for IPv6 and "0.0.0.0:/\*" for IPv4. The "State" column shows all entries as "LISTEN". The "PID/Program name" column shows "-" for all entries. The "Local Address" column has several entries highlighted in blue, specifically 0.0.0.0:445, 0.0.0.0:993, 0.0.0.0:5666, 0.0.0.0:139, 0.0.0.0:210:5357, 0.0.0.0:2222, 0.0.0.0:143, 0.0.0.0:111, 0.0.0.0:53:53, 0.0.0.0:25, and 0.0.0.0::445.

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State	PID/Program name
tcp	0	0	0.0.0.0:445	0.0.0.0:*	LISTEN	-
tcp	0	0	0.0.0.0:993	0.0.0.0:*	LISTEN	-
tcp	0	0	0.0.0.0:5666	0.0.0.0:*	LISTEN	-
tcp	0	0	0.0.0.0:139	0.0.0.0:*	LISTEN	-
tcp	0	0	0.0.0.0:210:5357	0.0.0.0:*	LISTEN	-
tcp	0	0	0.0.0.0:2222	0.0.0.0:*	LISTEN	-
tcp	0	0	0.0.0.0:143	0.0.0.0:*	LISTEN	-
tcp	0	0	0.0.0.0:111	0.0.0.0:*	LISTEN	-
tcp	0	0	0.0.0.0:53:53	0.0.0.0:*	LISTEN	-
tcp	0	0	0.0.0.0:25	0.0.0.0:*	LISTEN	-
tcp6	0	0	0.0.0.0::445	:::*	LISTEN	-
tcp6	0	0	0.0.0.0::993	:::*	LISTEN	-
tcp6	0	0	0.0.0.0::5666	:::*	LISTEN	-

Figure 83: Checking the ports in netstat (Part 1)



The screenshot shows a terminal window containing the same "netstat -tlpn" command and output as Figure 83. The output is identical, listing active Internet connections with columns for Proto, Recv-Q, Send-Q, Local Address, Foreign Address, State, and PID/Program name. The "Local Address" column includes both IPv4 and IPv6 entries. The "Foreign Address" column shows mostly ":::\*" for IPv6 and "0.0.0.0:/\*" for IPv4. The "State" column shows all entries as "LISTEN". The "PID/Program name" column shows "-" for all entries. The "Local Address" column has several entries highlighted in blue, specifically 0.0.0.0::139, 0.0.0.0::210:5357, 0.0.0.0::2222, 0.0.0.0::143, 0.0.0.0::111, 0.0.0.0::80, and 0.0.0.0::25.

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State	PID/Program name
tcp6	0	0	0.0.0.0::139	:::*	LISTEN	-
tcp6	0	0	0.0.0.0::210:5357	:::*	LISTEN	-
tcp6	0	0	0.0.0.0::2222	:::*	LISTEN	-
tcp6	0	0	0.0.0.0::143	:::*	LISTEN	-
tcp6	0	0	0.0.0.0::111	:::*	LISTEN	-
tcp6	0	0	0.0.0.0::80	:::*	LISTEN	-
tcp6	0	0	0.0.0.0::25	:::*	LISTEN	-

Figure 84: Checking the ports in netstat (Part 2)

**Step 19:** Adding a new user account for the mail.group2.com. Then, adding another account for the testing of sending and receiving mail between users.

The screenshot shows a terminal window with the title bar "root@lubuntugrp2: /etc/dovecot/conf.d". The terminal output is as follows:

```
link/ether 00:0c:29:33:44:a8 brd ff:ff:ff:ff:ff:ff
root@lubuntugrp2:/etc/dovecot/conf.d# sudo add user chong
sudo: /etc/sudoers.d is world writable
sudo: add: command not found
root@lubuntugrp2:/etc/dovecot/conf.d# sudo adduser chong
sudo: /etc/sudoers.d is world writable
Adding user `chong' ...
Adding new group `chong' (1007) ...
Adding new user `chong' (1005) with group `chong' ...
Creating home directory `/home/chong' ...
Copying files from `/etc/skel' ...
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: password updated successfully
Changing the user information for chong
Enter the new value, or press ENTER for the default
  Full Name []: chong
  Room Number []:
  Work Phone []:
  Home Phone []:
  Other []:
Is the information correct? [Y/n]
root@lubuntugrp2:/etc/dovecot/conf.d#
```

Figure 85: Adding a new user account

**Step 20:** Install Rainloop for webmail access.

The screenshot shows a terminal window with the title bar "root@lubuntugrp2: /var/www/html/mail". The terminal output is as follows:

```
root@lubuntugrp2:/var/www/html# cd mail
root@lubuntugrp2:/var/www/html/mail# ls
root@lubuntugrp2:/var/www/html/mail# curl -sL https://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@lubuntugrp2:/var/www/html/mail#
```

Figure 86: Install Rainloop Webmail

**Step 21:** Using the server IP address to navigate to the Rainloop mail page. Then, login to Rainloop admin web interface by using ‘admin’ as username and ‘12345’ as it password.

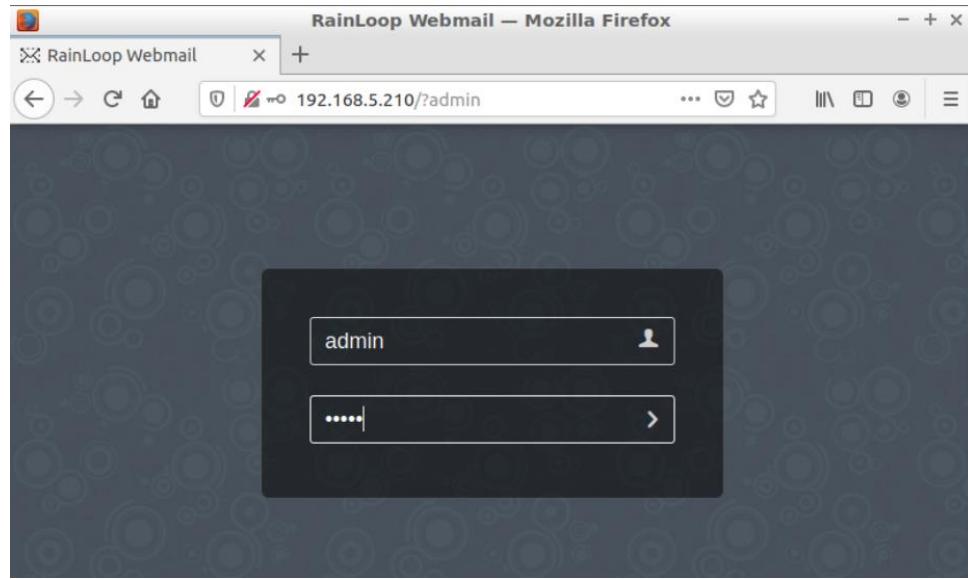


Figure 87: Login to Rainloop admin web interface

**Step 22:** Add domain “mail.group2.com” and fill in domain name settings as shown in below.

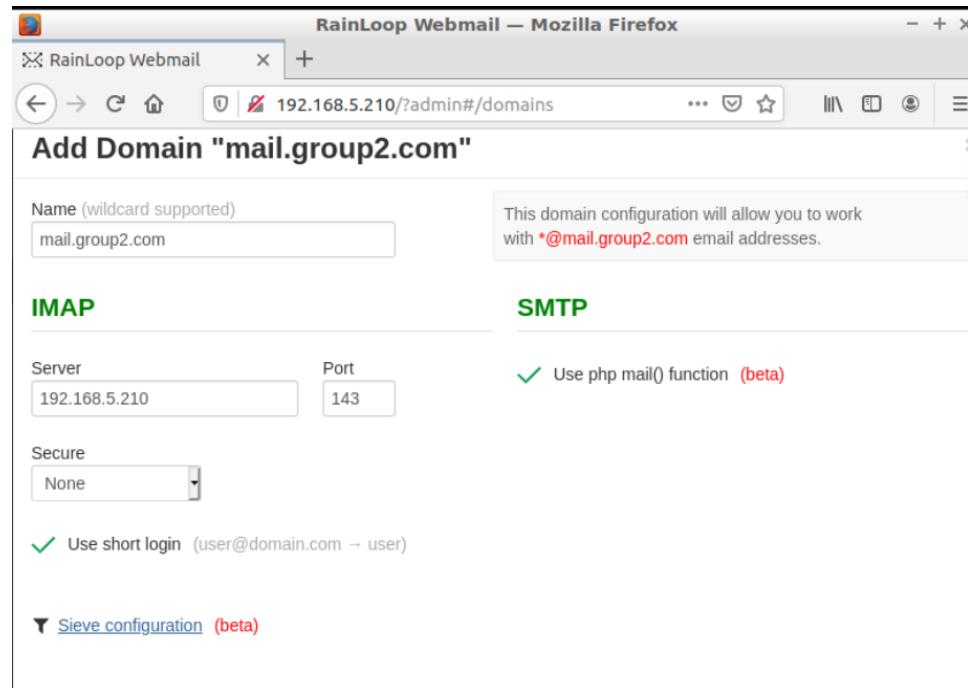


Figure 88: Configuring Domain name settings

### 5.3.8 WEB, SSL & VIRTUAL HOSTING

#### Web

**Step 1:** Install a Web Server (IIS) by open Server Manager, then click Manage menu and select Add Roles and Features. Then, click **Next** at the **Before you begin** window.

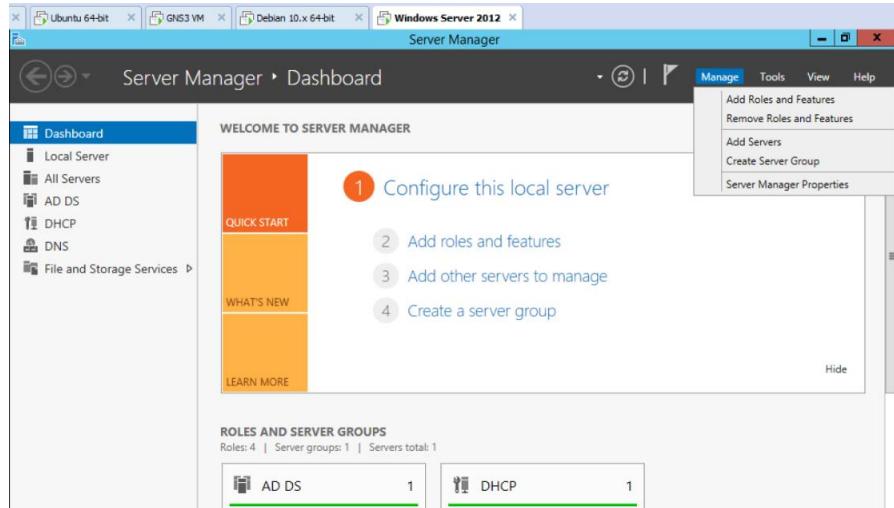


Figure 89: Add role and features in server

**Step 2:** Select Role-based or Feature-based Installation when select installation type.

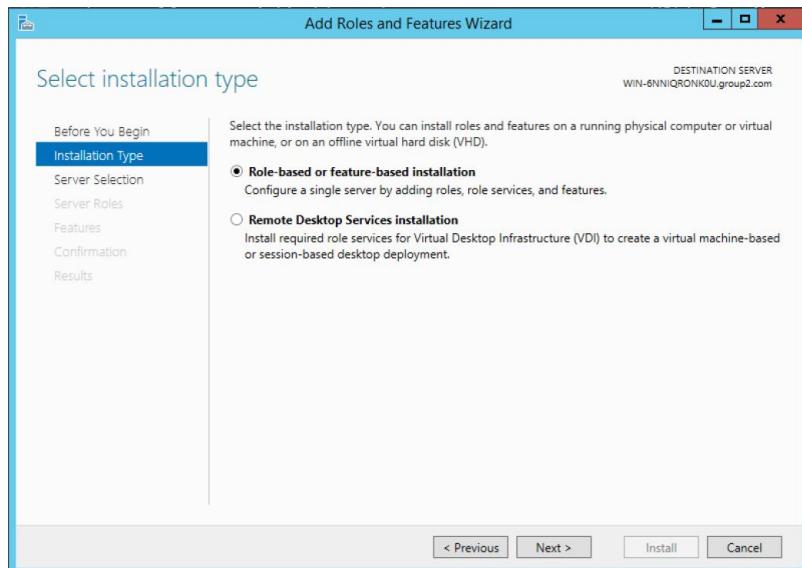
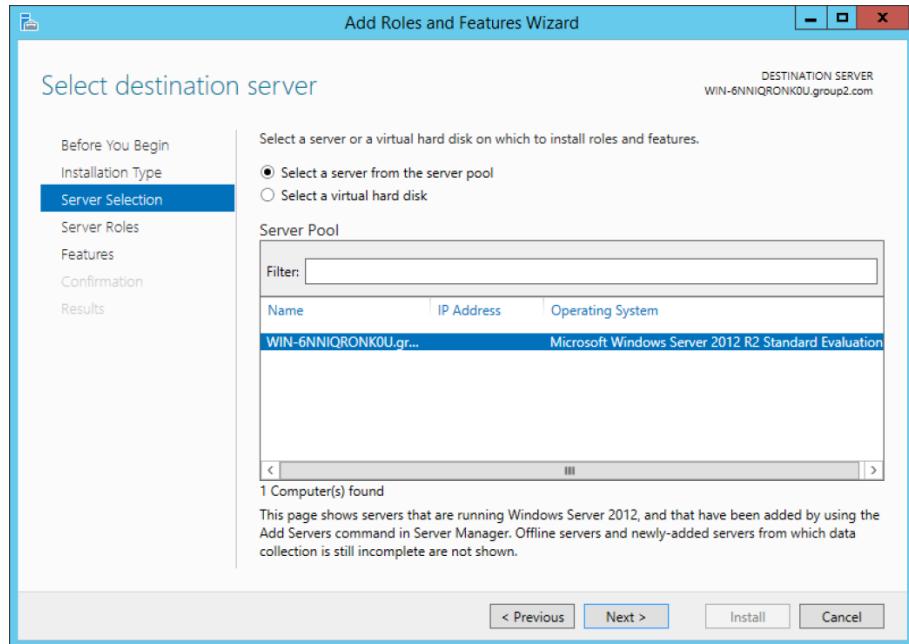


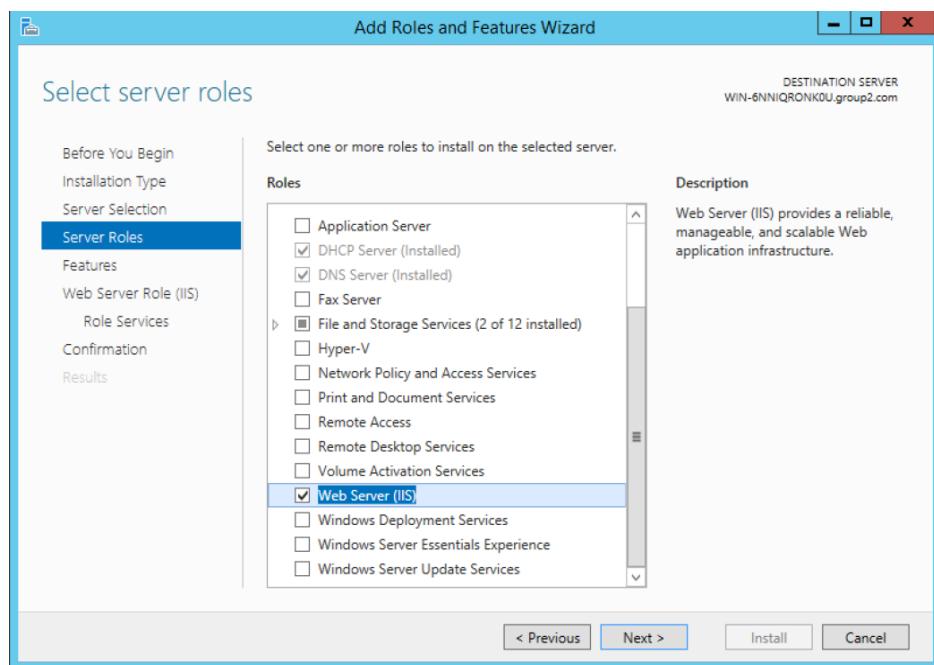
Figure 90: Select Role-based or Feature-based Installation

**Step 3:** Select the appropriate server (set default).



*Figure 91: Select Role-based or Feature-based Installation*

**Step 4:** Select Web Server (IIS).



*Figure 92: Select Web Server (IIS)*

**Step 5:** In the **Add Roles and Features wizard**, click Add Features to install the IIS Management Console.

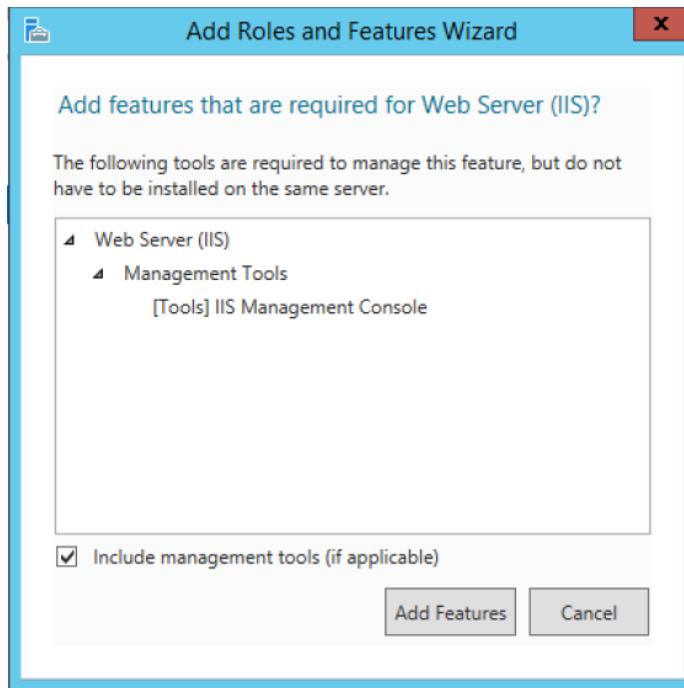


Figure 93: Add Roles and Features wizard

**Step 6:** Keep clicking next (use default setting) until to reach confirmation page.

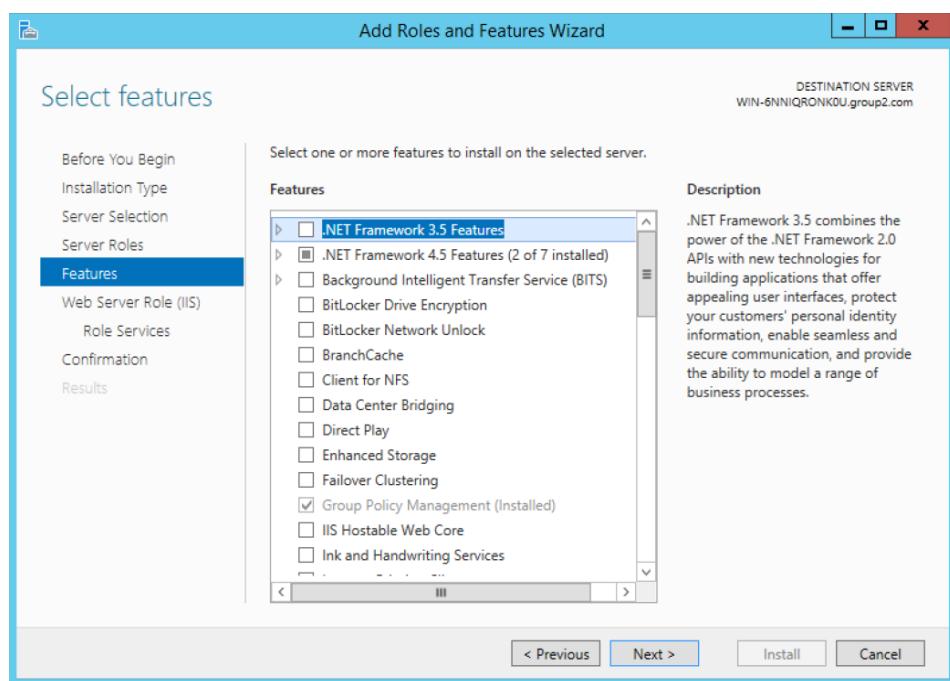
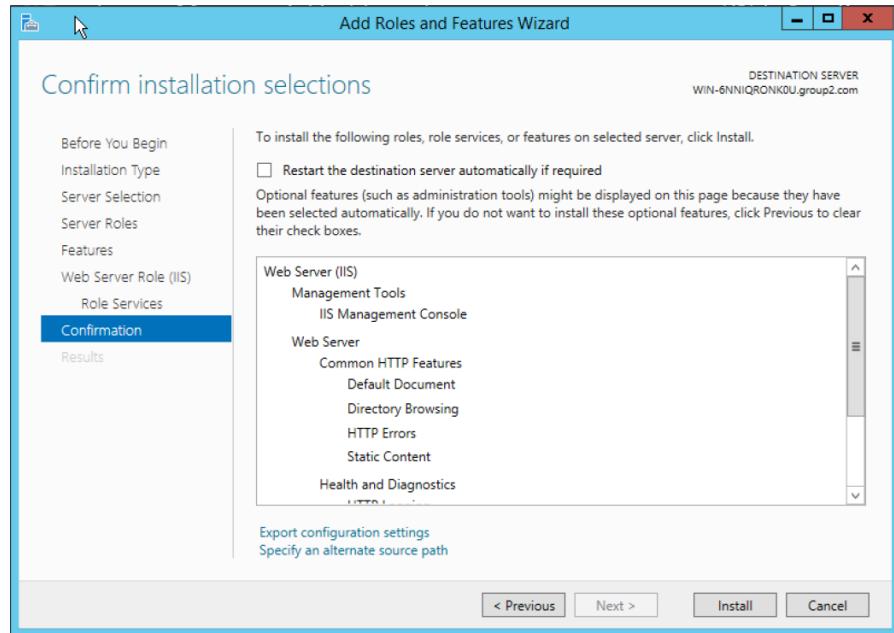


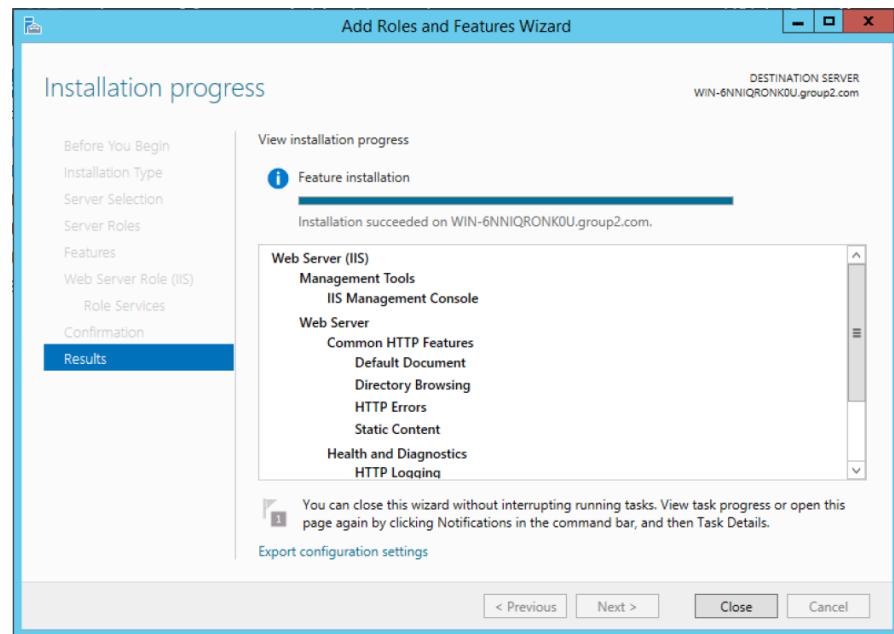
Figure 94: Keep clicking next until reaching to confirmation page

**Step 7:** Click **Install** to start installing in conformation page.



*Figure 95: Installing conformation*

**Step 8:** Click **Close** after installation is completed.



*Figure 96: Installation completed*

**Step 10:** After the installation was completed, open **Administrator** tools and select **Internet Information Service (IIS)**. Right click at **Sites** and select **Add website** to add a new website.

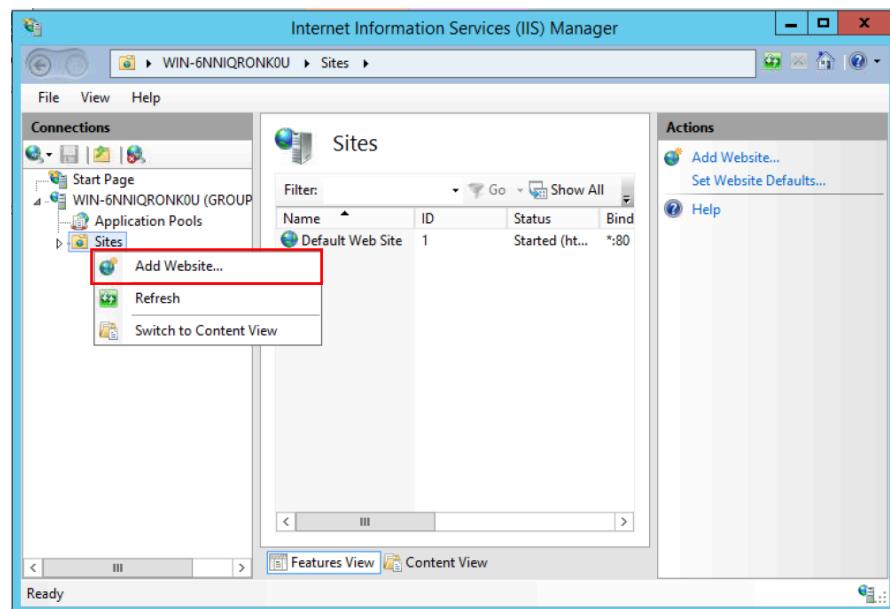


Figure 97: Adding new website at IIS manager

**Step 11:** Fill in all the details of the website at the **Add Website** window and click OK.

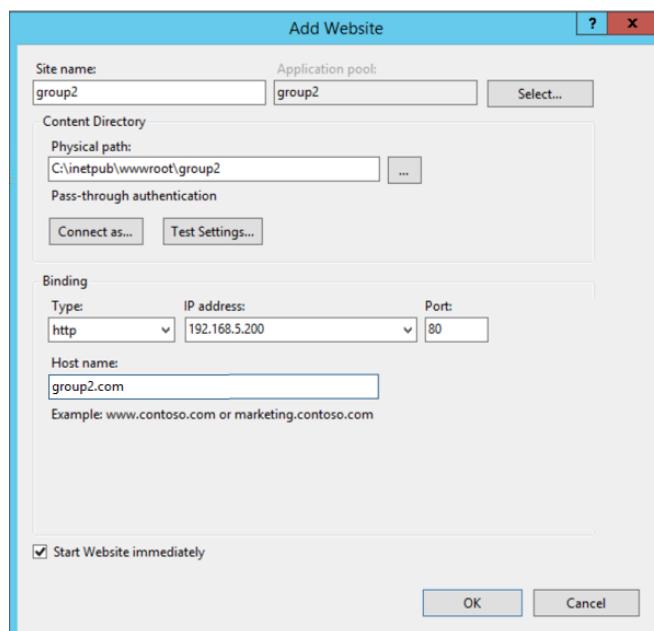


Figure 98: Installing progress

**Step 12:** Go *This PC* > *Local Disk (C:)* > *inetpub* > *wwwroot*. Create a folder named ‘group2’ and move in the default html file as well as the involved photo inside the folder.

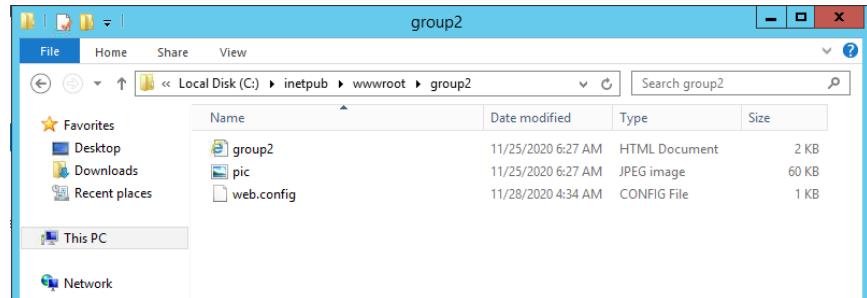


Figure 99: Creating group2 directory with the group2.html file

**Step 13:** Add a Default document for the website by select **Default Document**.

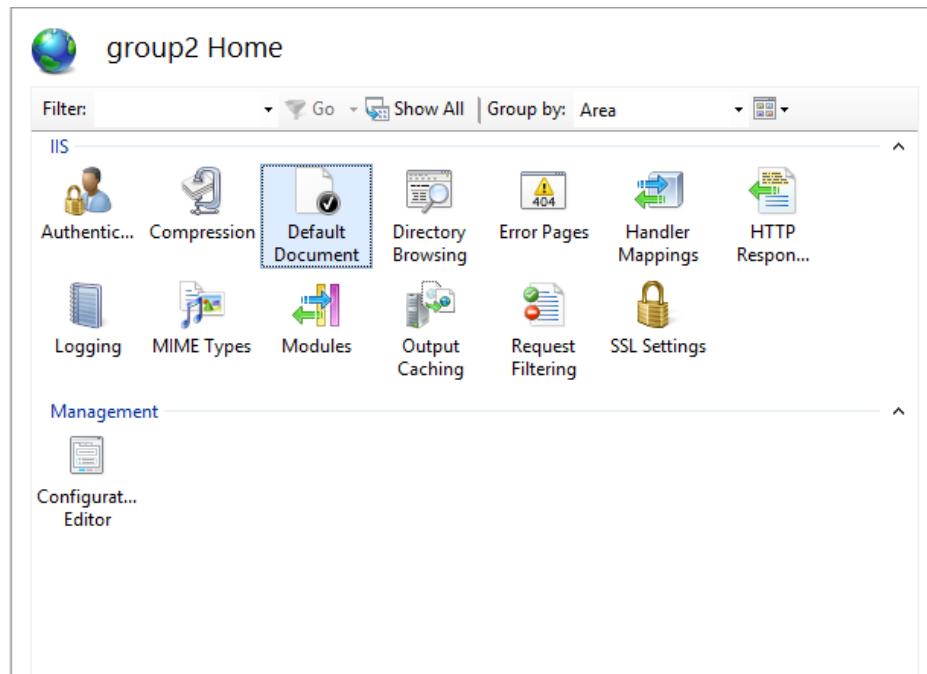


Figure 100: Add new Default Document

**Step 14:** Add new html file with the file name called **vhgroup2.html** and click **OK**.

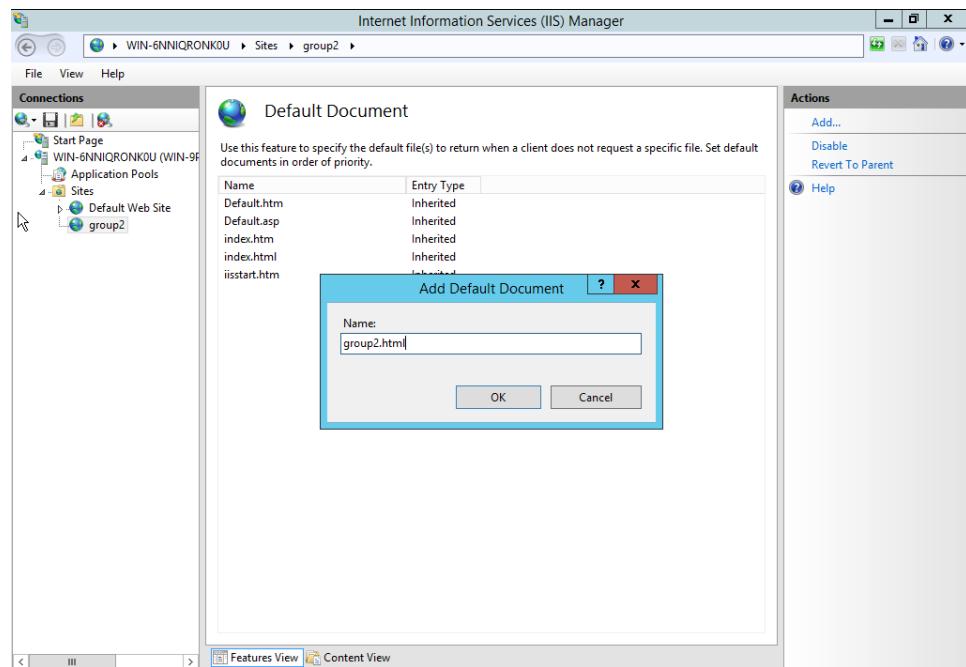


Figure 101: Default html file for group2.com

## Secure Socket Layer (SSL)

**Step 1:** Install Active Directory Certificate Service (AD CS) to create Domain certificates. First, go to Server Manager and click Manage menu and select Add Roles and Features. Then, click **Next** at the **Before you begin** window.

**Step 2:** Select Role-based or Feature-based Installation when select installation type.

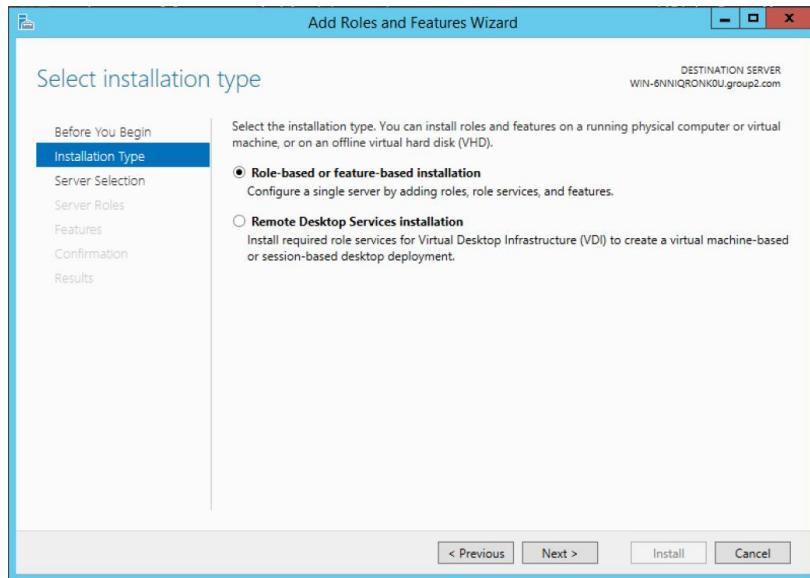


Figure 102: Role-based or Feature-based Installation

**Step 3:** Select the appropriate server (set default).

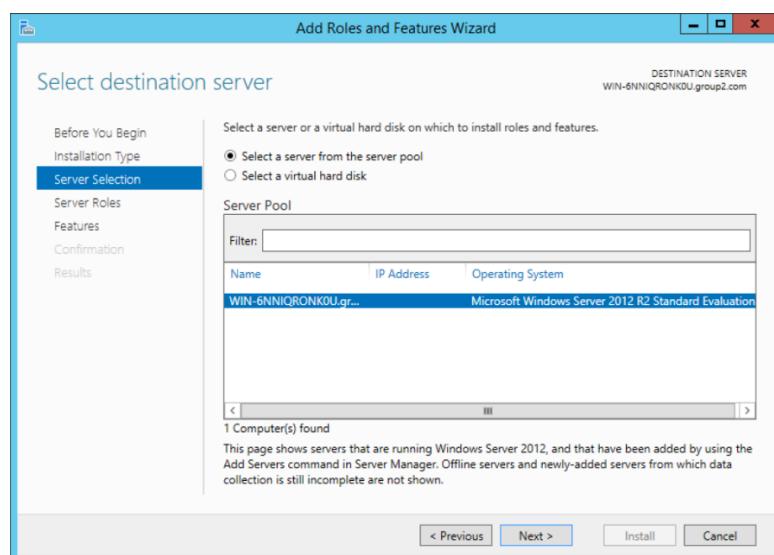
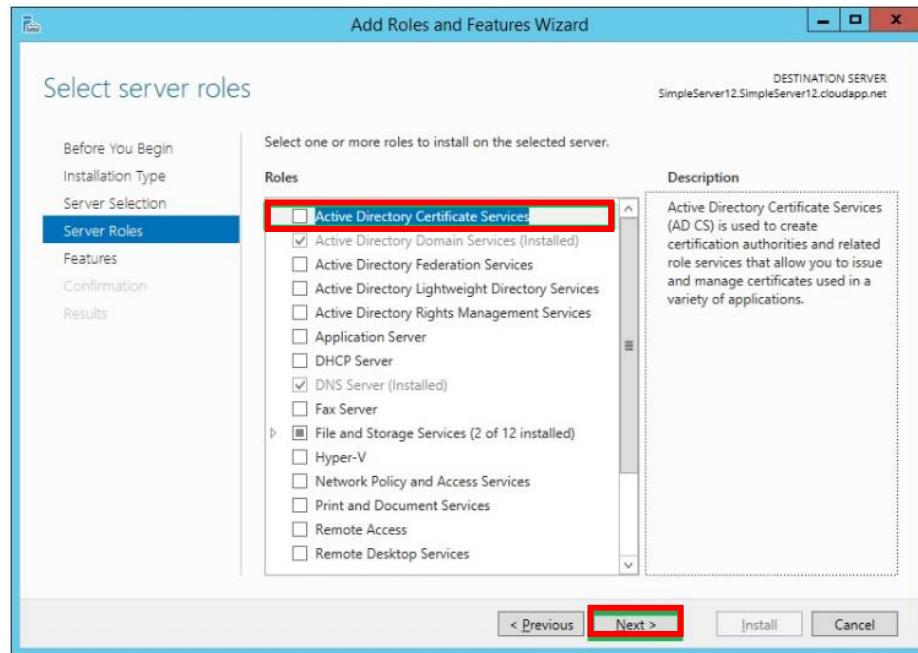


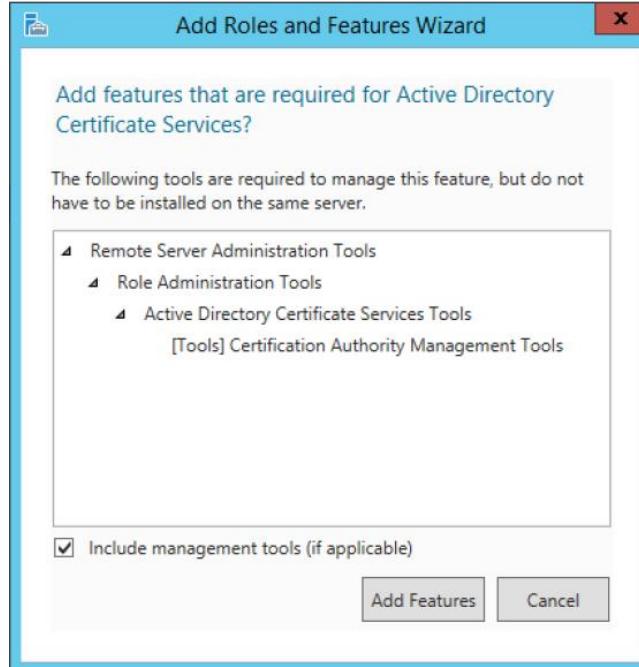
Figure 103: Select Role-based or Feature-based Installation

**Step 4: Select Active Directory Certificate Service (AD CS).**



*Figure 104: Active Directory Certificate Services*

**Step 5: In the Add Roles and Features wizard, click Add Features to install the Certification Authority Management Tools.**



*Figure 105: Active Directory Certificate Services*

**Step 6:** Keep clicking next (use default setting) until to reach confirmation page

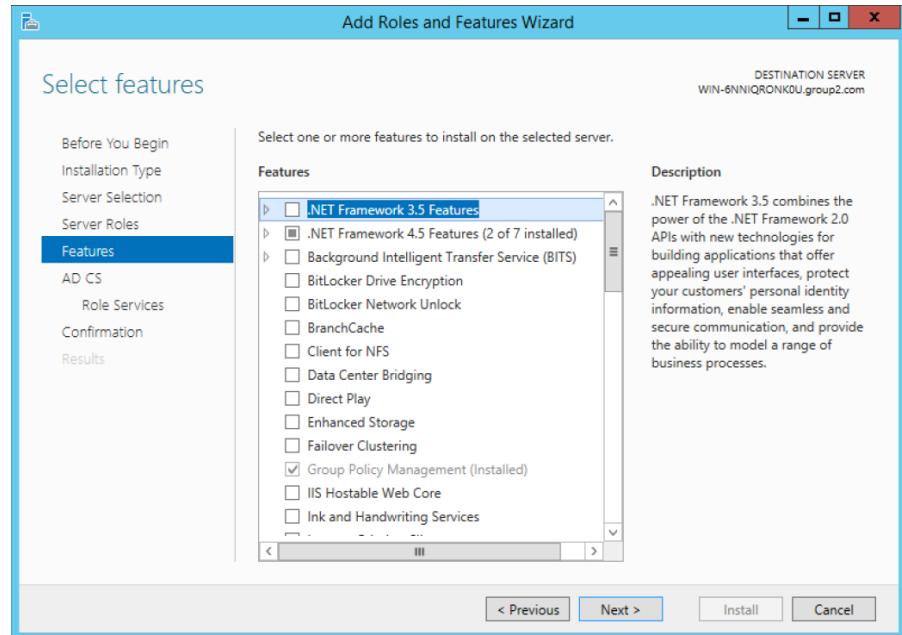


Figure 106: Keep clicking next until reaching to confirmation page

**Step 7:** Tick **Certification Authority** and **Certificate Enrollment Policy Web Service** when select role services.

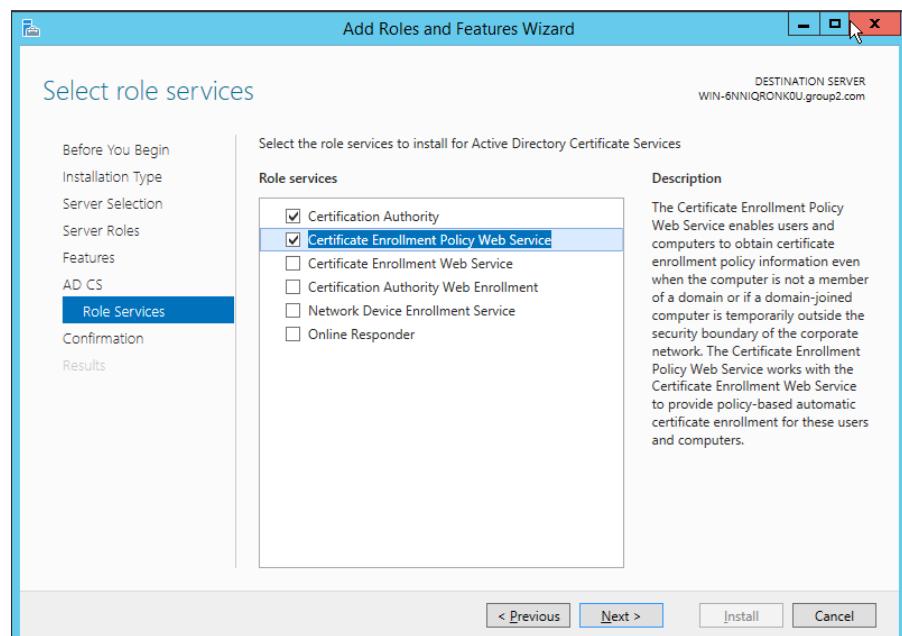


Figure 107: Tick Certification Authority and Certificate Enrollment Policy Web Service

**Step 8:** Click **Install** to start installing in conformation page.

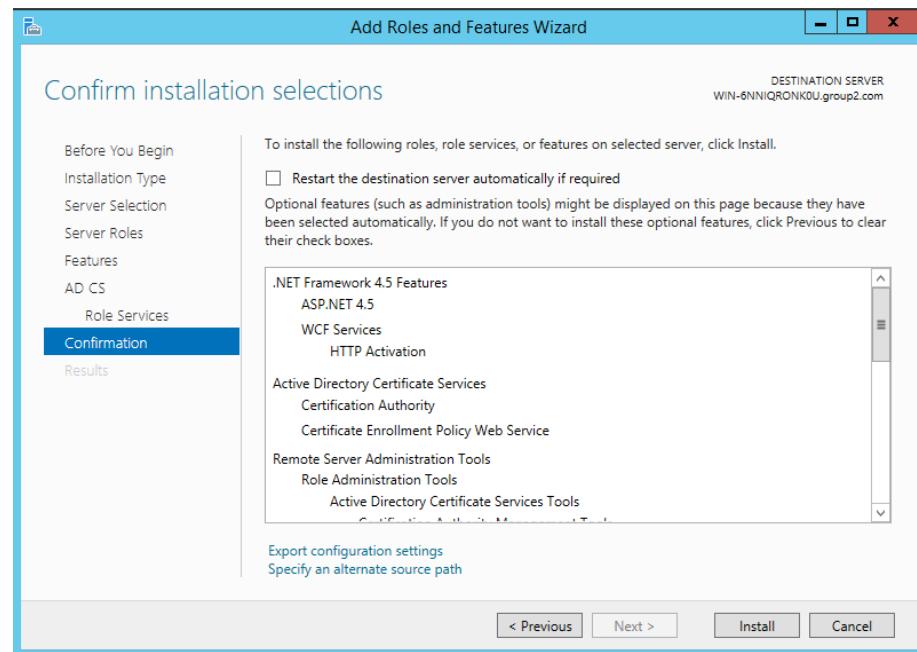


Figure 108: Installing conformation

**Step 9:** Click **Close** after installation is completed.

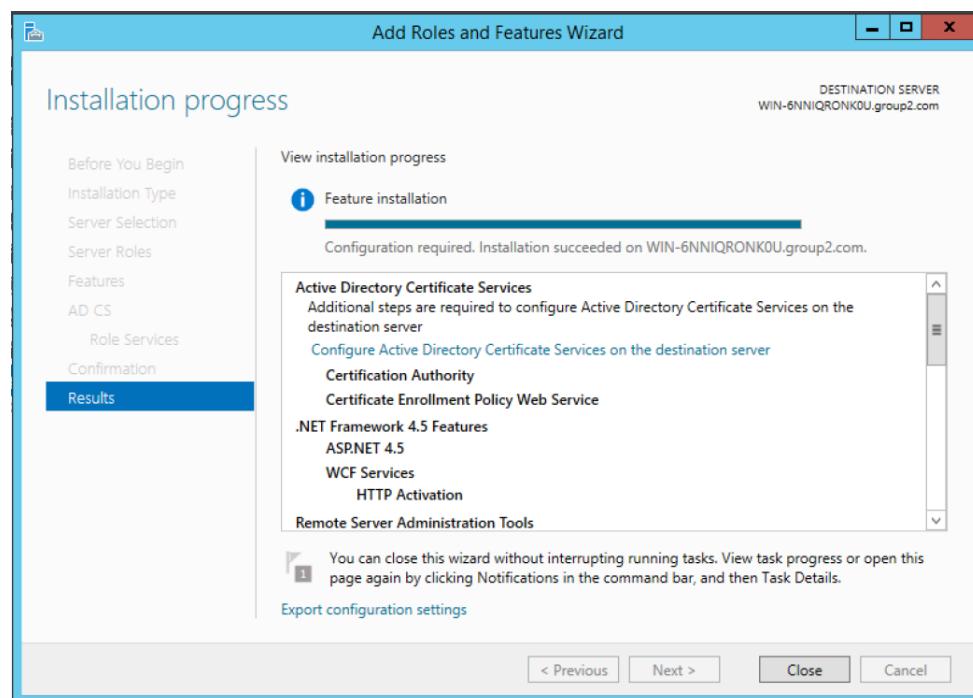


Figure 109: Installation completed

**Step 10:** In the dashboard click AD CS, it will show a warning message. Then, click More options.

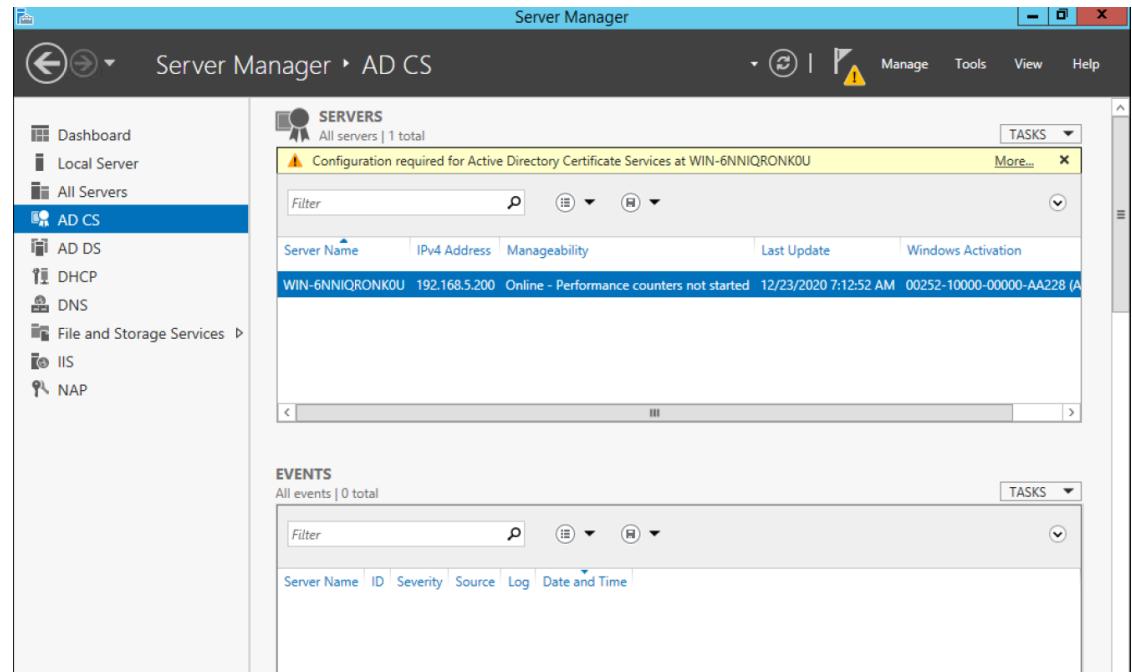


Figure 110: AD CS Showing a warning message

**Step 11:** All Server Task Details and Notifications window will appear, click “Configure Active Directory Certificate Services”.

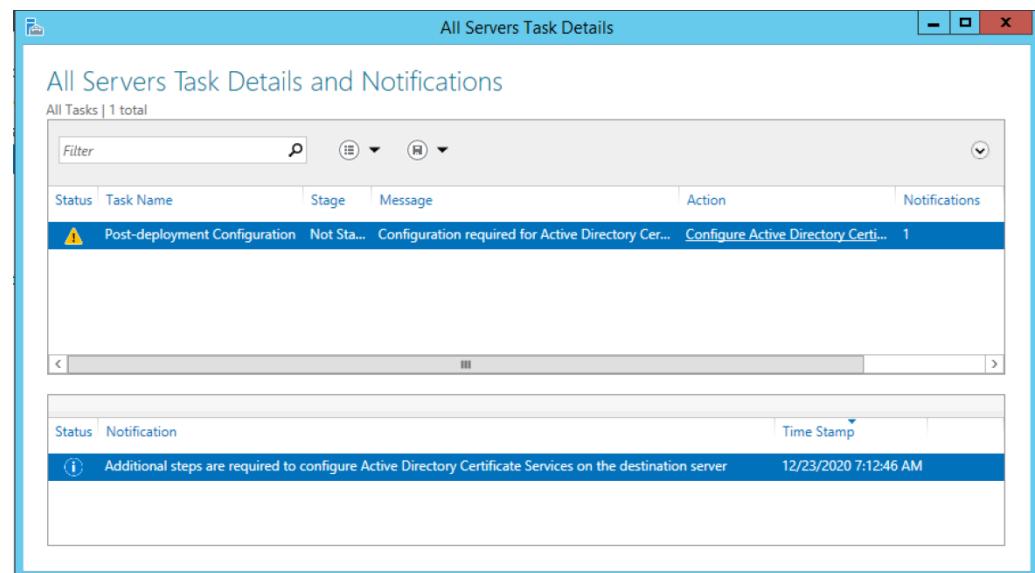


Figure 111: Click “Configure Active Directory Certificate Services”

**Step 12:** AD CS configuration wizard appears in the credentials option; click Next.

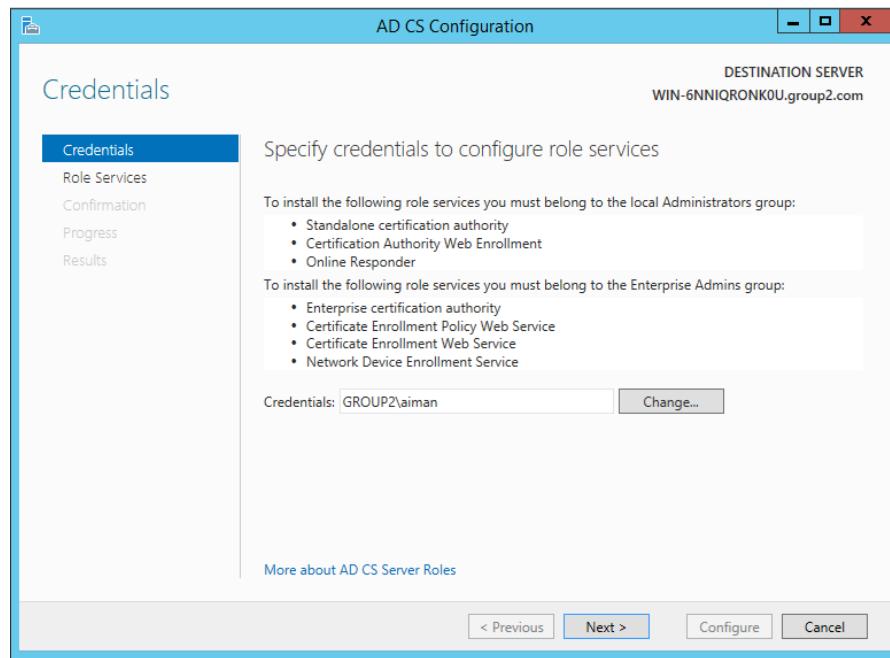


Figure 112: Credentials of AD CS

**Step 13:** In role services, select the **Certificate Enrollment Policy Web Service** to configure and click **Next**.

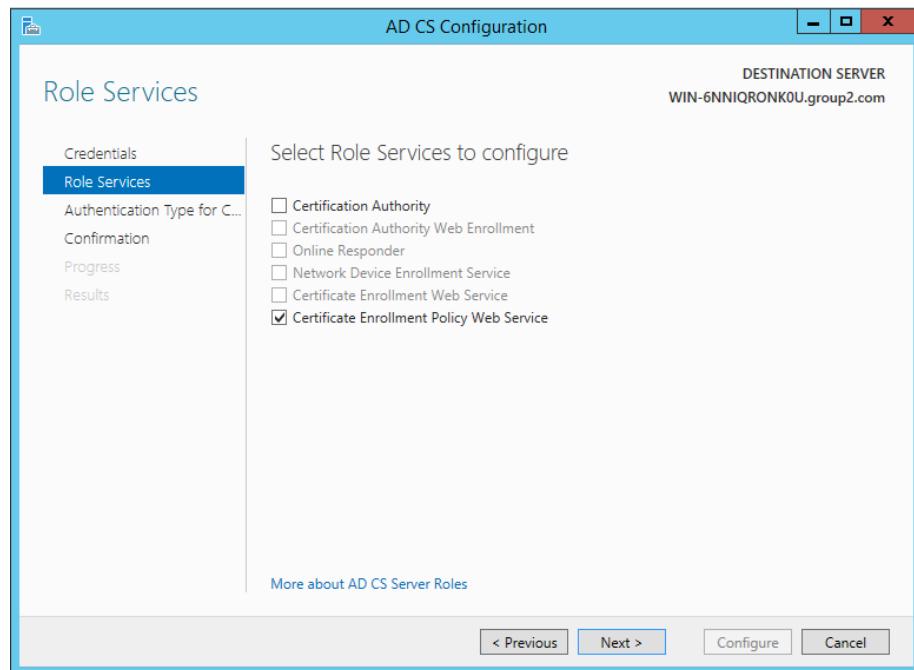
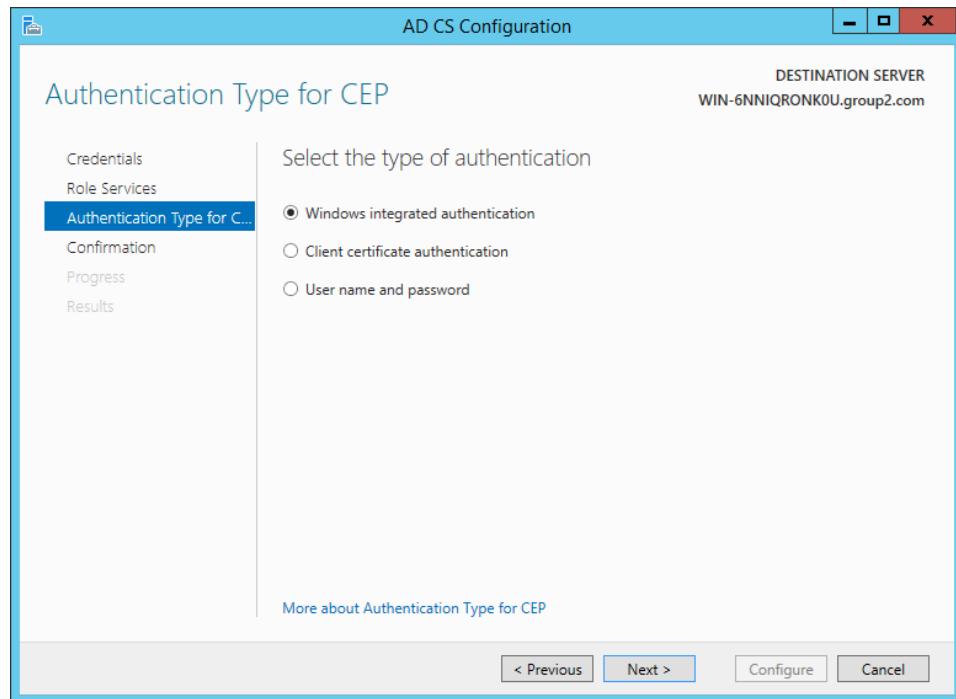


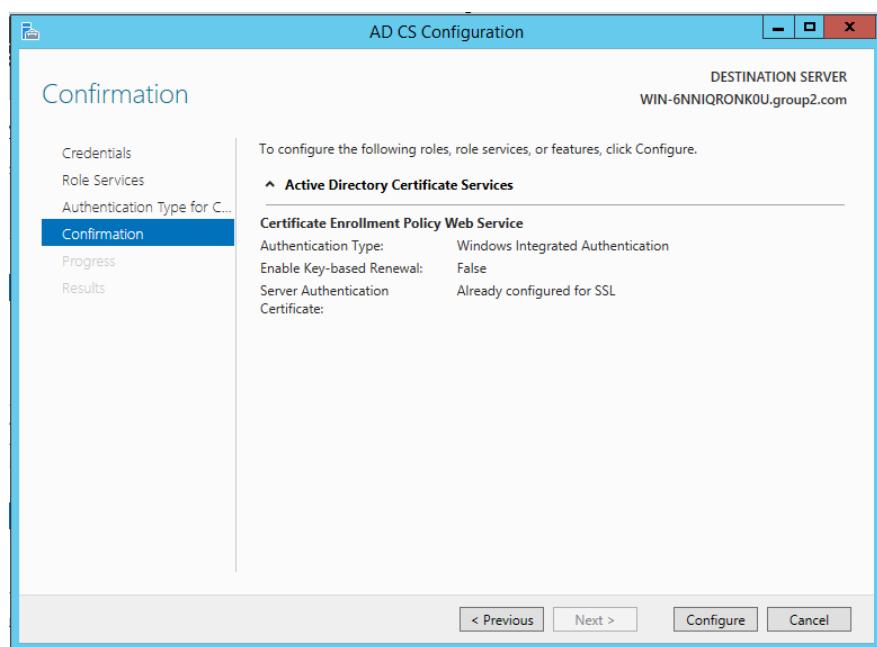
Figure 113: Select Certificate Enrollment Policy Web Service

**Step 14:** In the Authentication window, click **Windows integrated authentication** and click **Next**.



*Figure 114: Click Windows integrated authentication*

**Step 15:** In the confirmation tab hit the configure option.



*Figure 115: AD CS configuration confirmation*

**Step 16:** Finally, in the result tab you can see the selected and configured features.

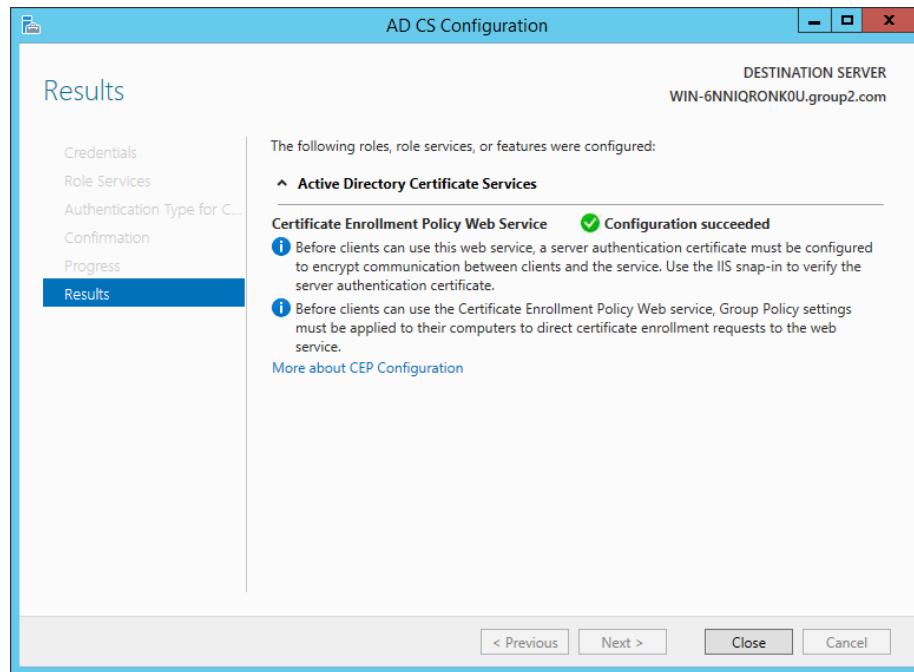


Figure 116: Result tab

**Step 17:** In role services, select the **Certificate Authority** to configure and click **Next** as this service has been missed to configured at previous step.

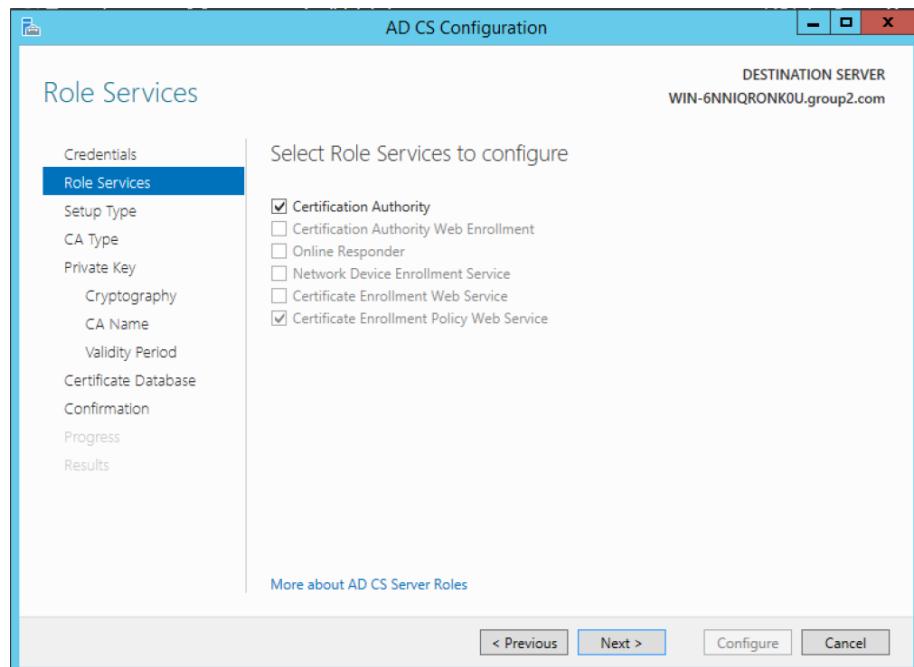


Figure 117: Select Certification Authority

**Step 18:** Select **Enterprise CA** when specify the setup type of the CA.

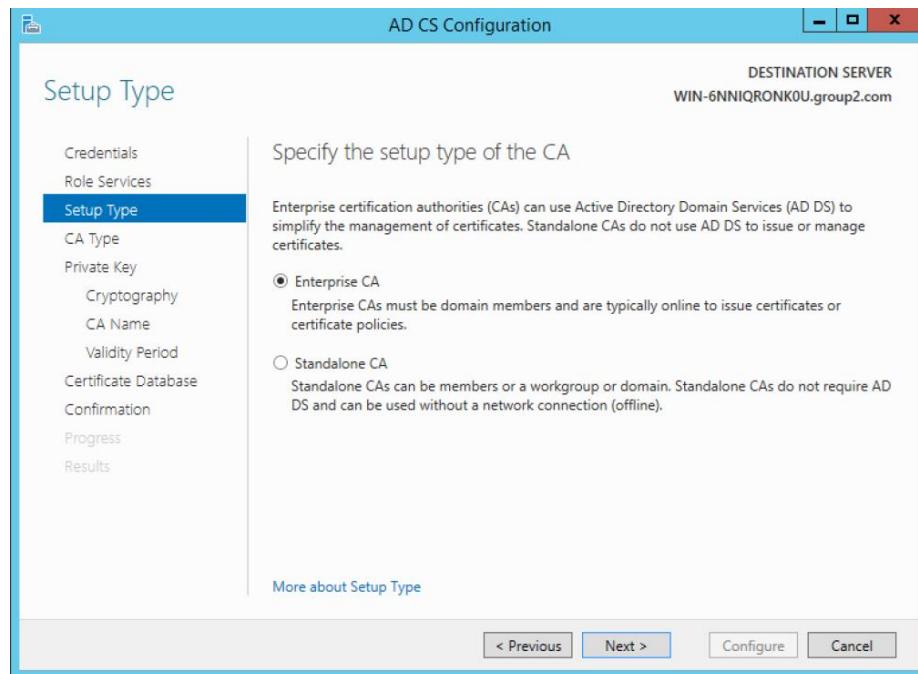


Figure 118: Select Enterprise CA

**Step 19:** Select **RAS#Microsoft Software Key Storage Provider** as a cryptographic provider and **SHA1** as the hash algorithm with default key length.

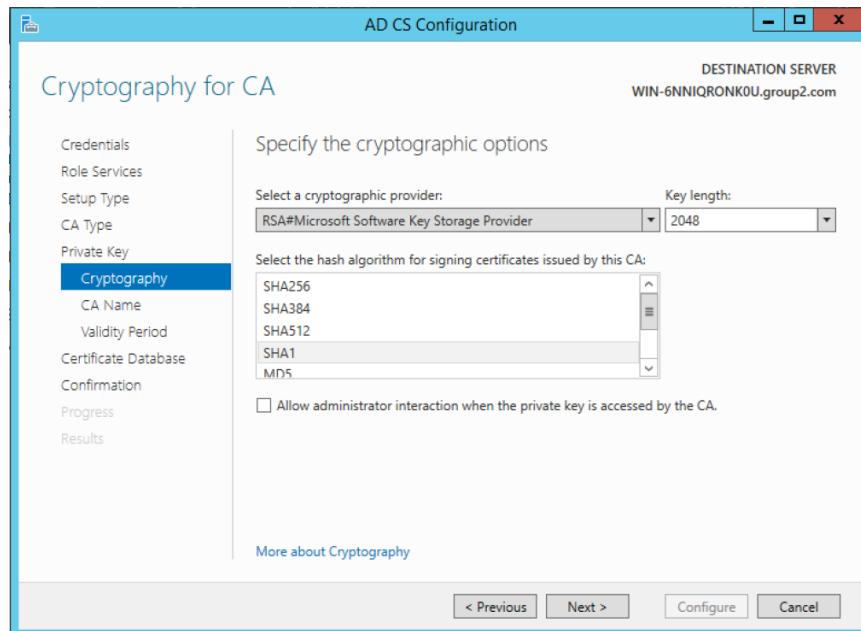


Figure 119: Select RAS#Microsoft Software Key Storage Provider, SHA1 with key length 2048

**Step 20:** Use the default settings when specify the name of the CA.

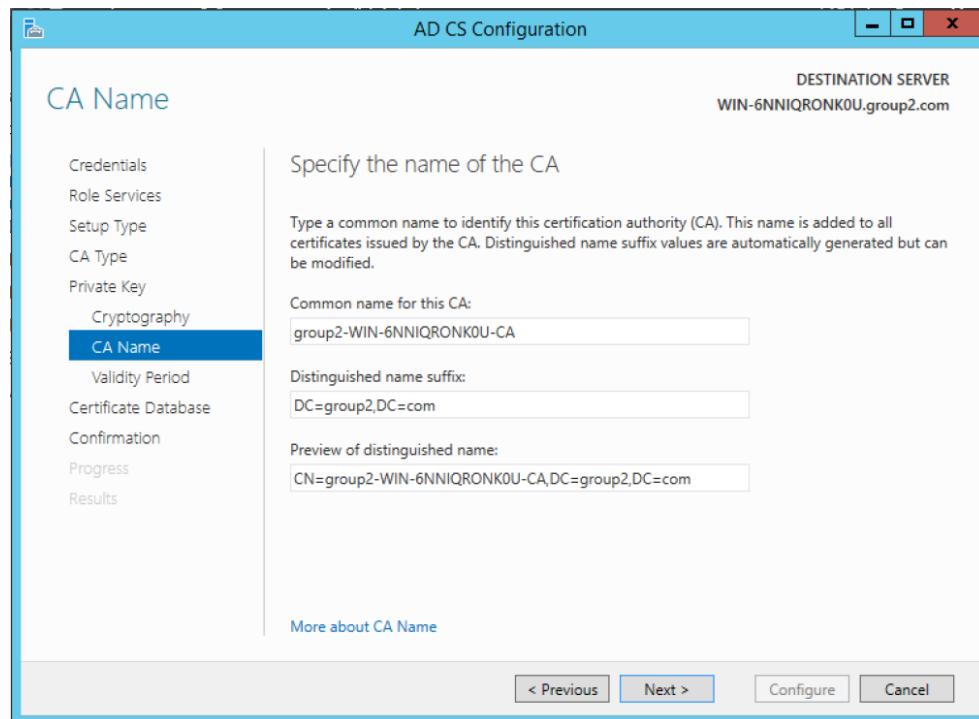


Figure 120: Specify the name of the CA

**Step 21:** Set 5 years when specify the validity period.

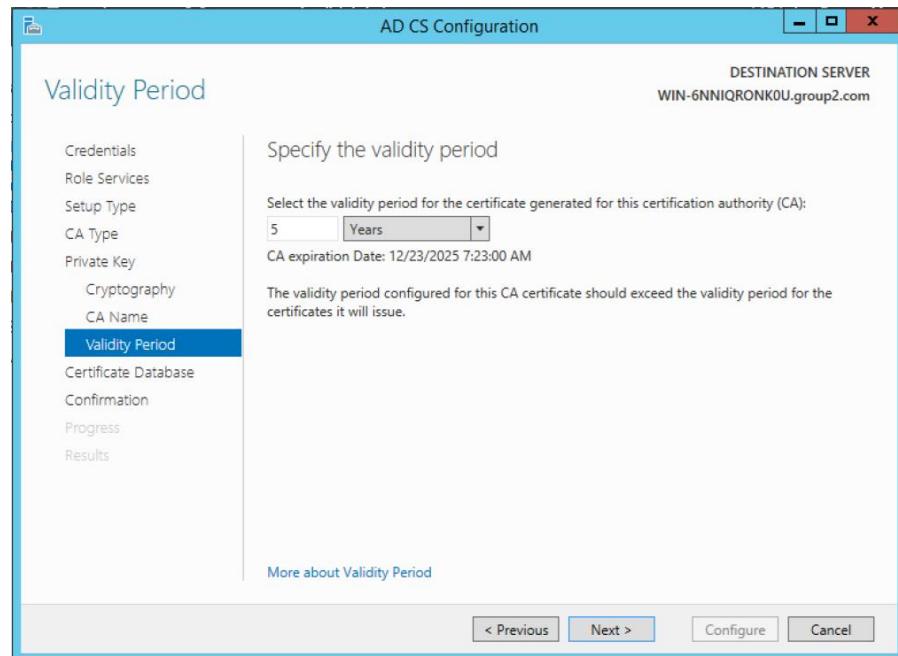


Figure 121: Specify the validity period

**Step 22:** Use the default settings when specify the database locations.

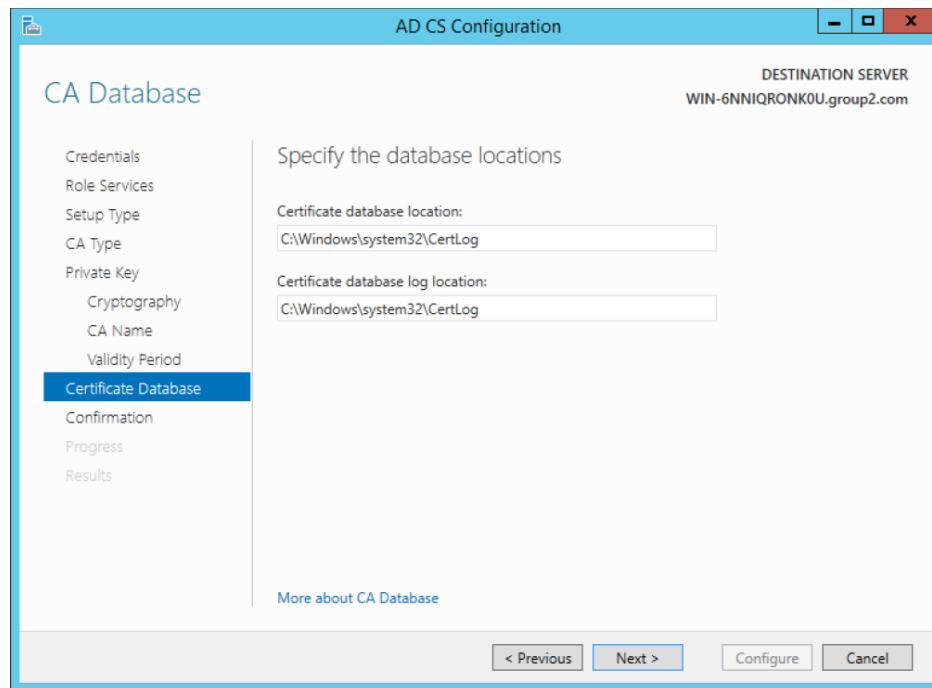


Figure 122: Specify the validity period

**Step 23:** Hit the configure option in the confirmation tab.

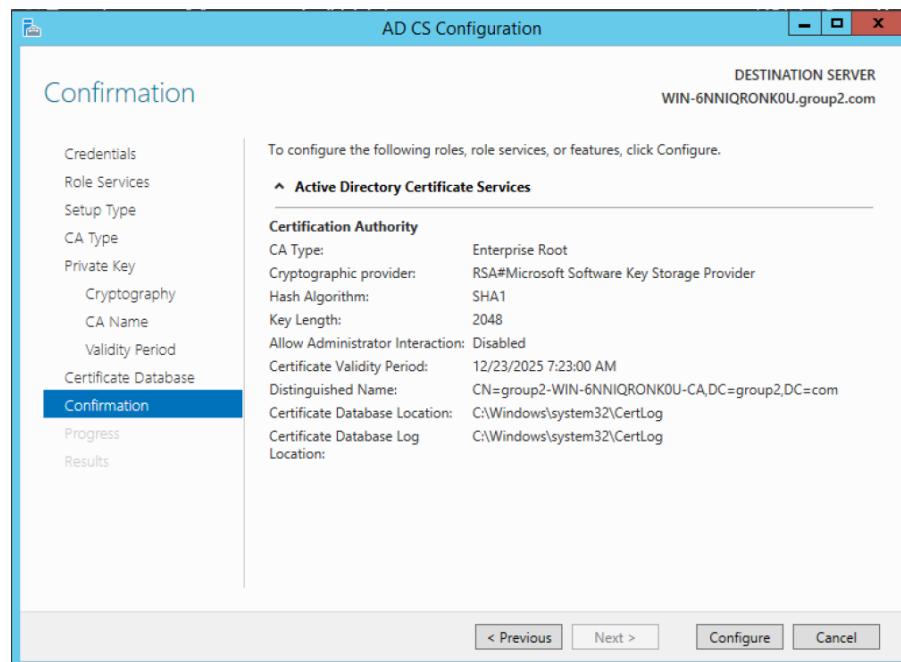


Figure 123: Confirmation tab for AD CS

**Step 24:** You can see the selected and configured features in the result tab.

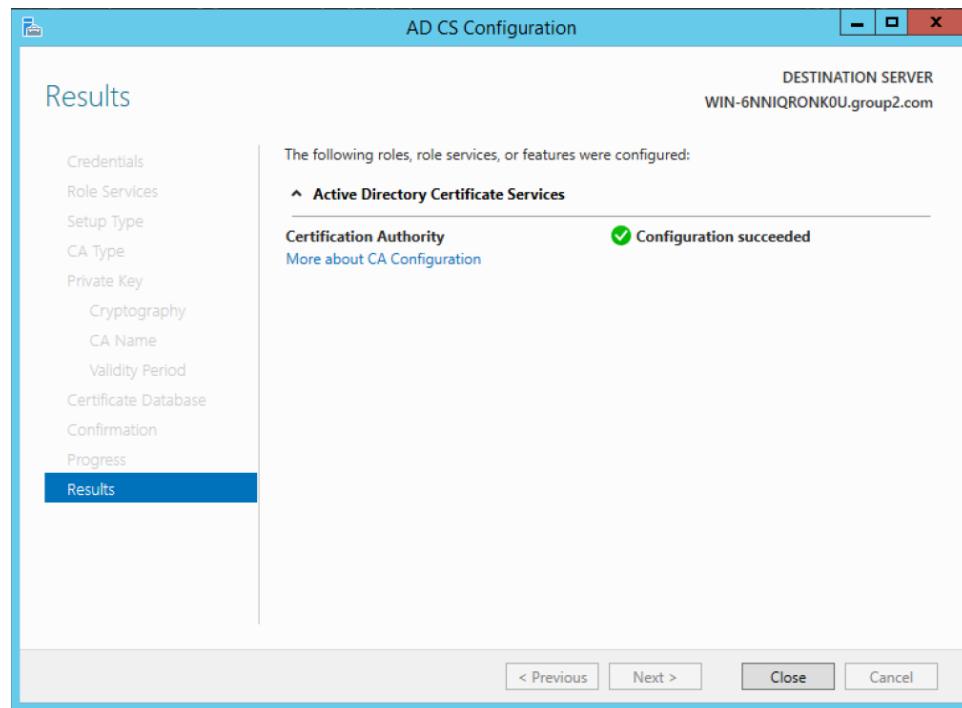


Figure 124: Result tab for AD CS

**Step 25: Create Domain Certification.** First, go to IIS Manager and select Server Certificates.

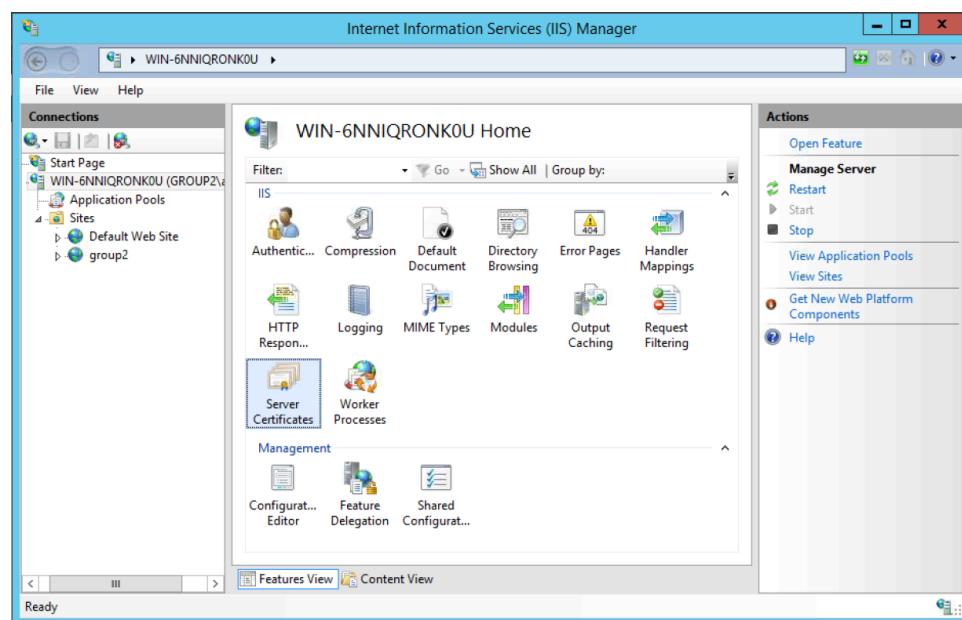


Figure 125: Server Certificates

**Step 26:** Select to create Domain Certificate.

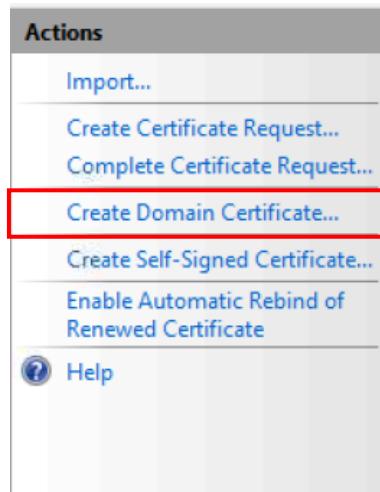


Figure 126: Create Domain Certificates

**Step 27:** Fill in the required information for the certificate and click **Next**.

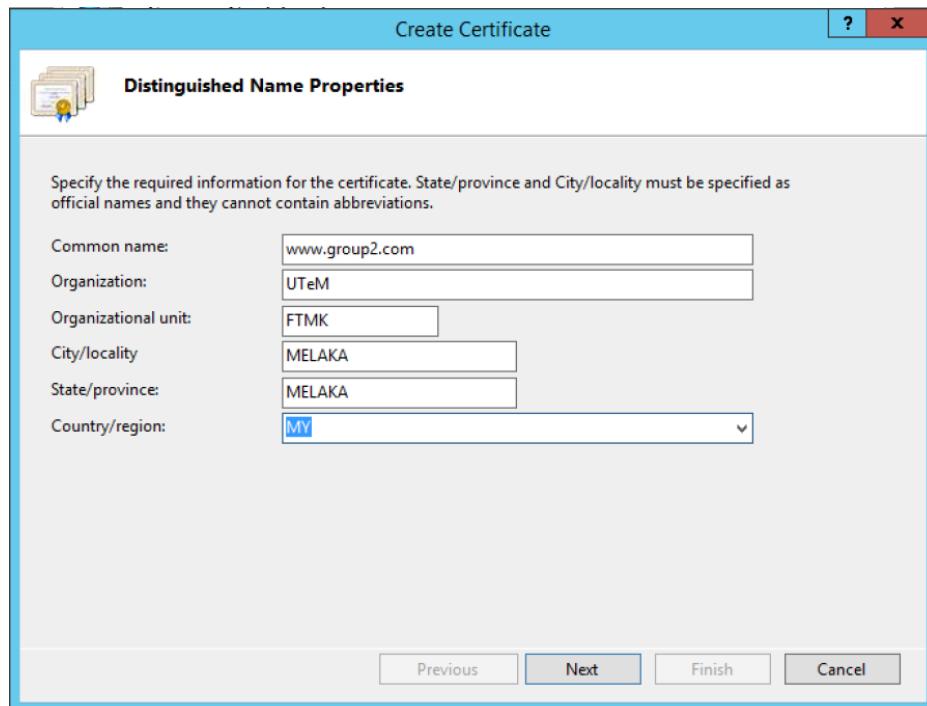


Figure 127: Fill in information for certificate

**Step 28:** Select the Online Certification Authority and fill in the Friendly name.

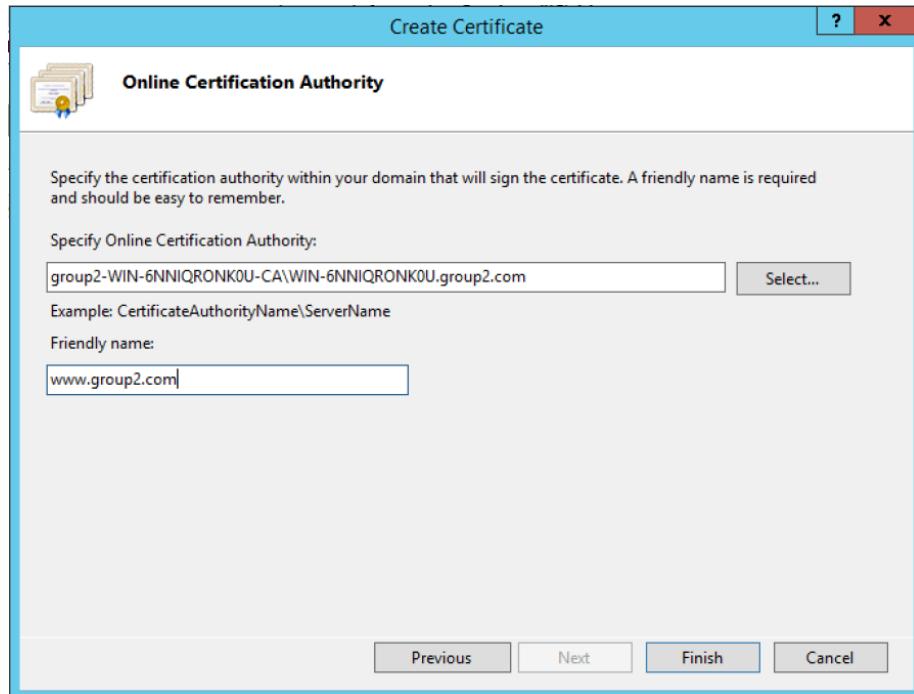


Figure 128: Select Online Certification Authority & fill in the Friendly name.

**Step 29:** The server certificate is created.

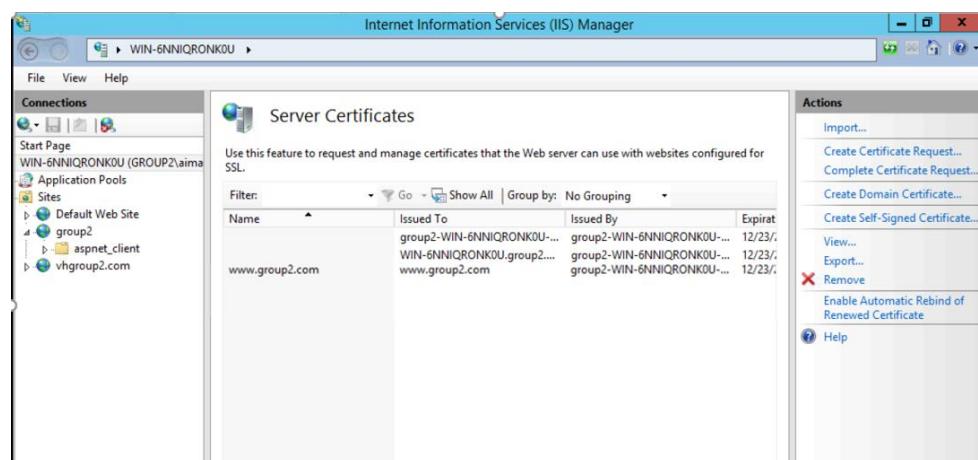


Figure 129: List of Certificate

**Step 30:** Add Site **Binding** and select type **https** for SSL. Choose SSL Certificate that had been created before.

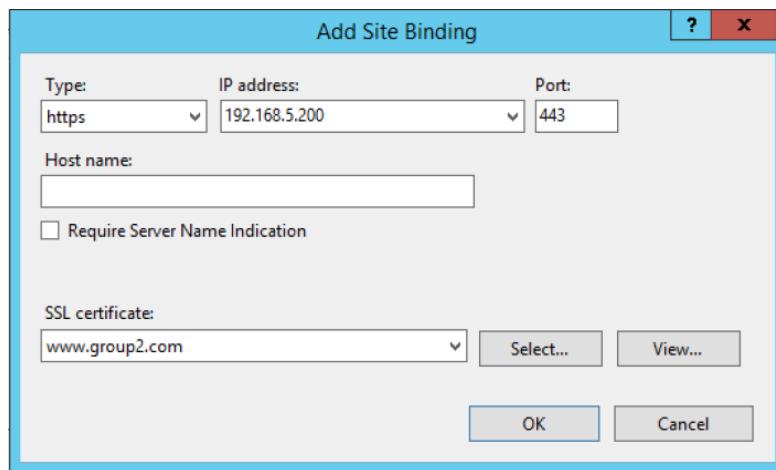


Figure 130: Add site binding for SSL

**Step 31:** Go to SSL Settings to change SSL setting,

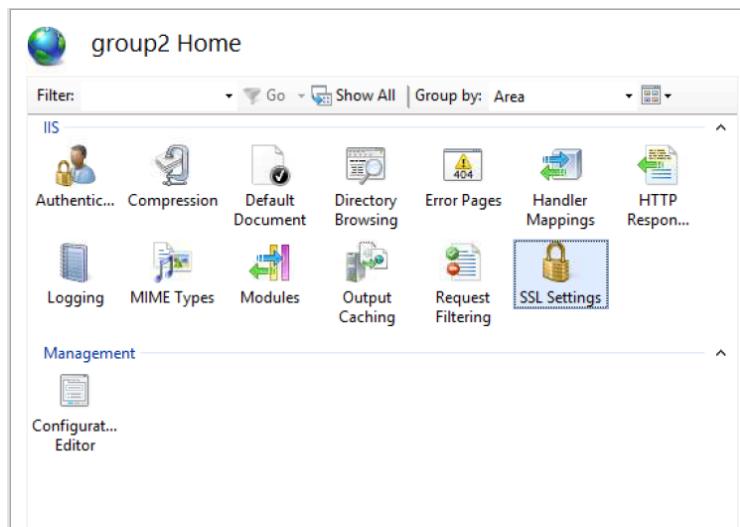


Figure 131: SSL settings

**Step 32:** Untick **Require SSL** and **Ignore** client certificate, the click **Apply** to save the changes.

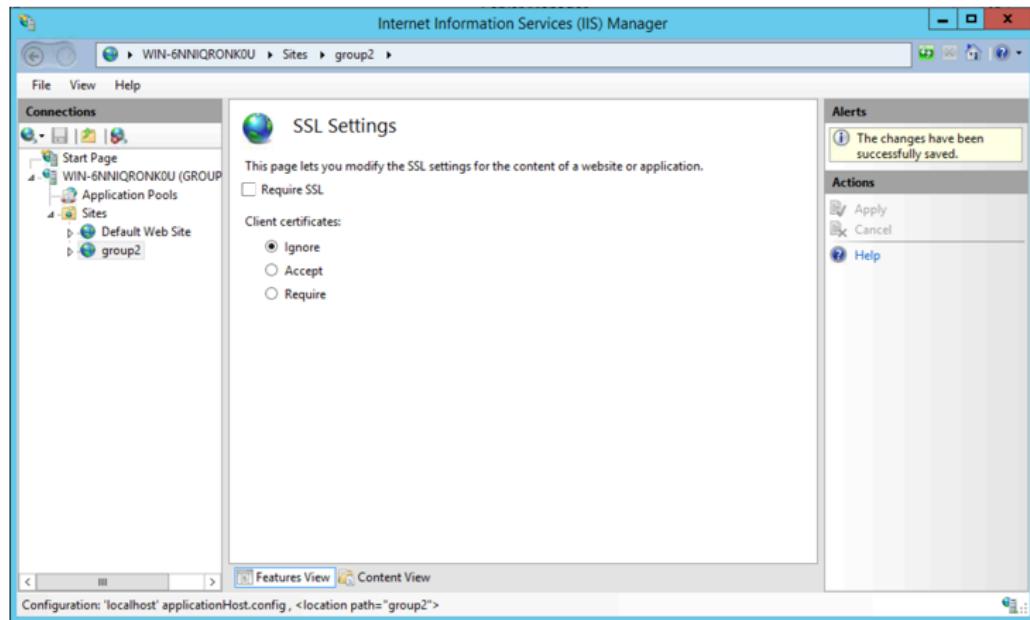


Figure 132: SSL Settings

## Virtual Hosting

**Step 1:** Open IIS manager and right click at **Sites**. Then, select **Add Website** to add a new website.

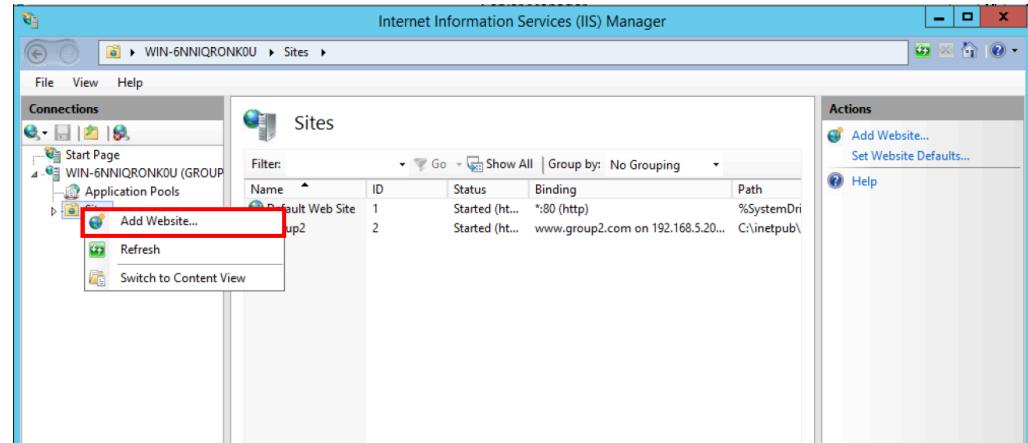


Figure 133: Adding new website at IIS manager

**Step 2:** Fill the site name with virtual hosting name and all the detail required.

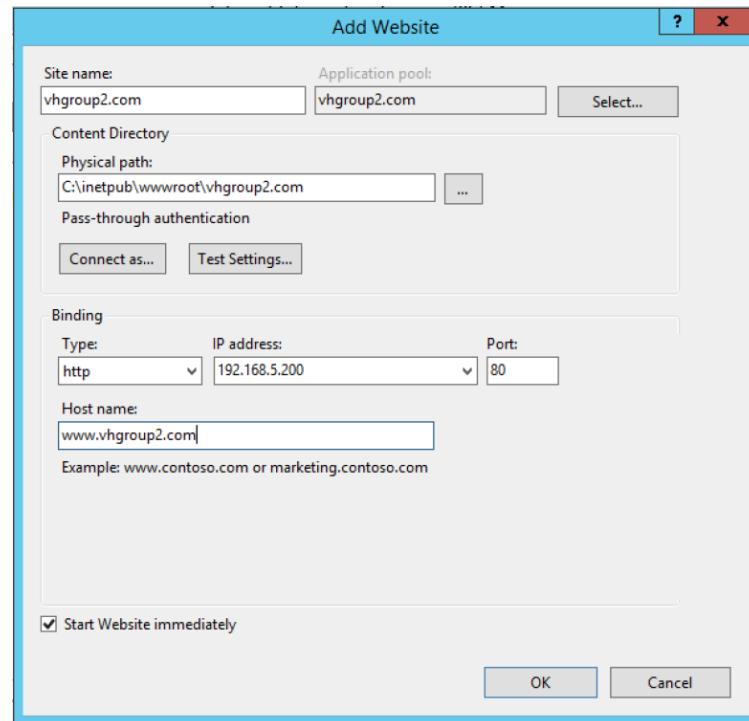


Figure 134: Add new website

**Step 3:** Go **This PC > Local Disk (C:) > inetpub > wwwroot**. Create a folder named ‘vhgroup2’ and move in the default html file as well as the involved photo inside the folder.

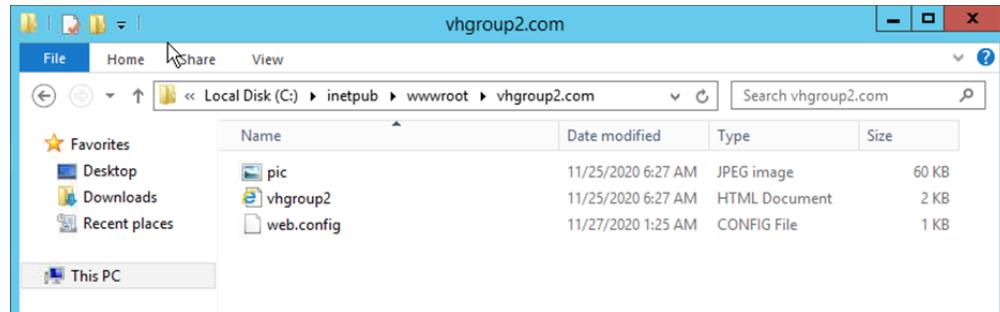


Figure 135: Creating vhgroup2 directory with the vhgroup2.html file

**Step 4:** Add a Default document for the website by select **Default Document**.

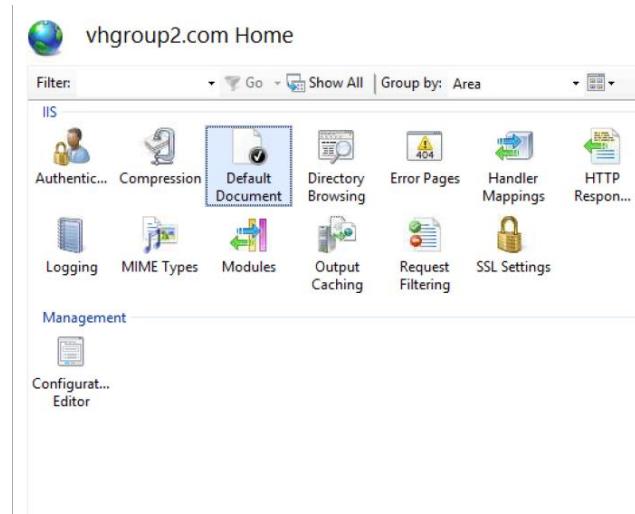


Figure 136: Add new Default Document

**Step 5:** Add new html file with the file name called **vhgroup2.html** and click **OK**.

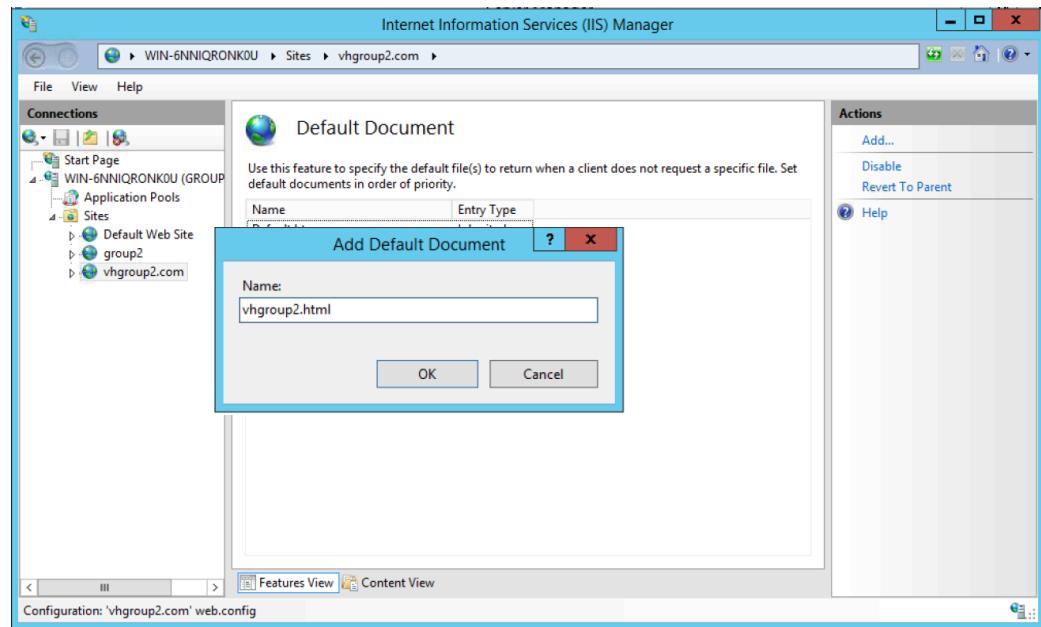


Figure 137: Default html file for vhgroup2.com

**Step 6:** Create a new zone in **Forward Lockup Zones** by right click it and select **New Zone** in DNS manager.

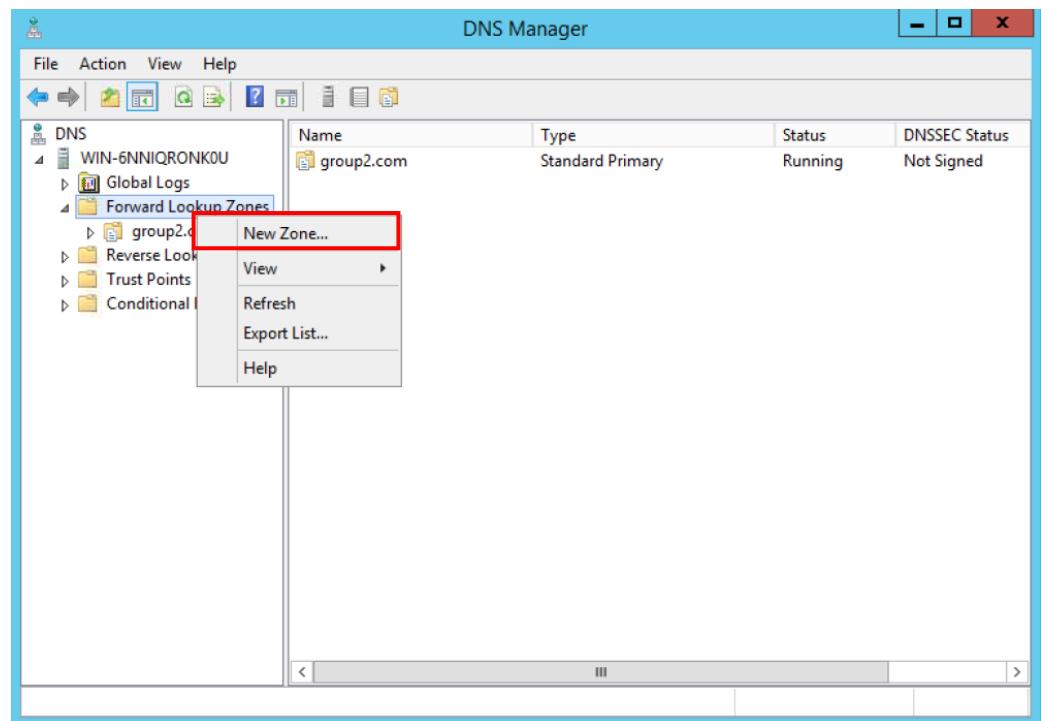


Figure 138: Creating new zone

**Step 7:** Click **Next**.



Figure 139: Create new zone in forward lockup zones in DNS manager

**Step 8:** Choose **primary zone** and tick to store zone in active directory. Then, click **Next**.

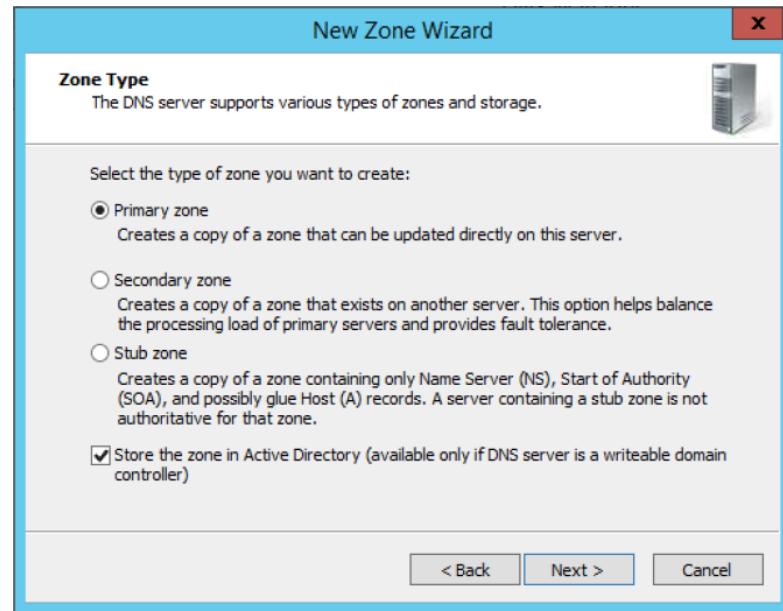


Figure 140: Choosing primary zone

**Step 9:** Choose domain: group2.com when New Zone Wizard ask how you want zone data replicated. Then, click Next.

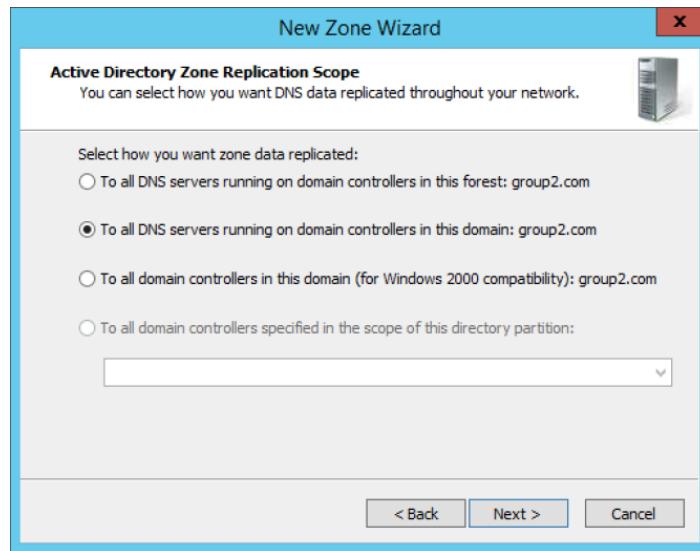


Figure 141: Choosing domain:group2.com in wizard for Web

**Step 10:** Create new zone name.

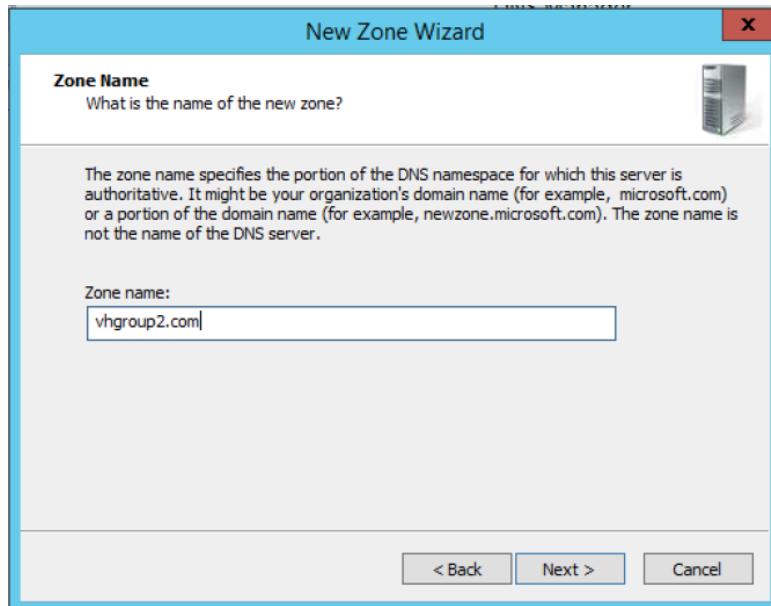


Figure 142: Creating new zone name

**Step 11:** Choose **Allow both nonsecure and Secure Dynamic Updates** as the type of dynamic updates.

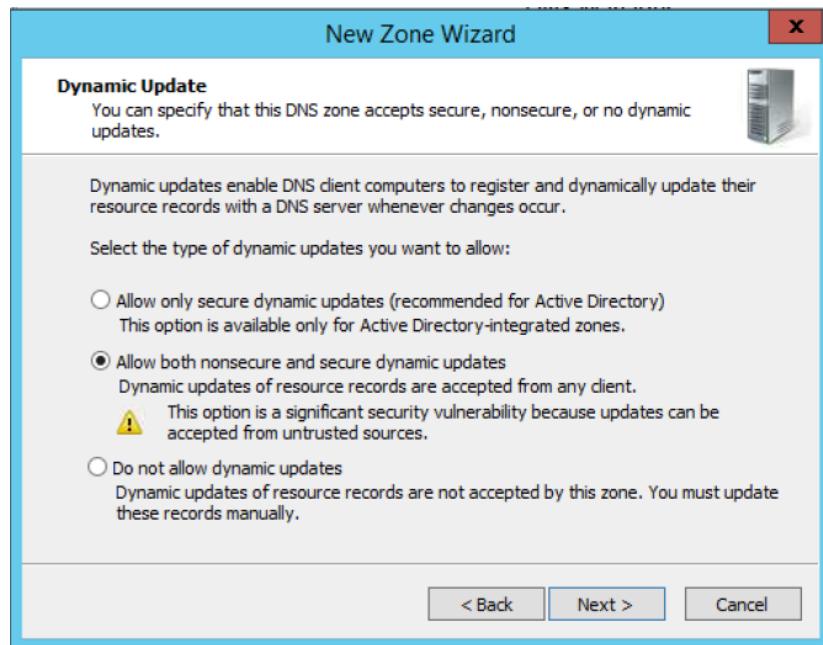


Figure 143: Choosing dynamic update

**Step 12:** New zone wizard created successfully and click **Finish**.

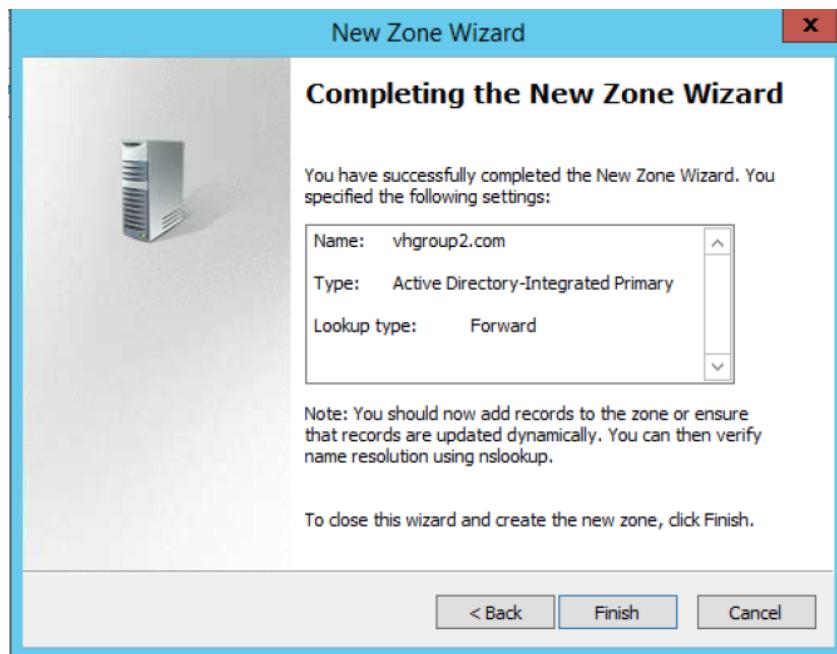


Figure 144: Completing the New Zone wizard

**Step 13:** Create new host by right click the **vhgroup2.com** zone and select the **New host (A Or AAA)**.

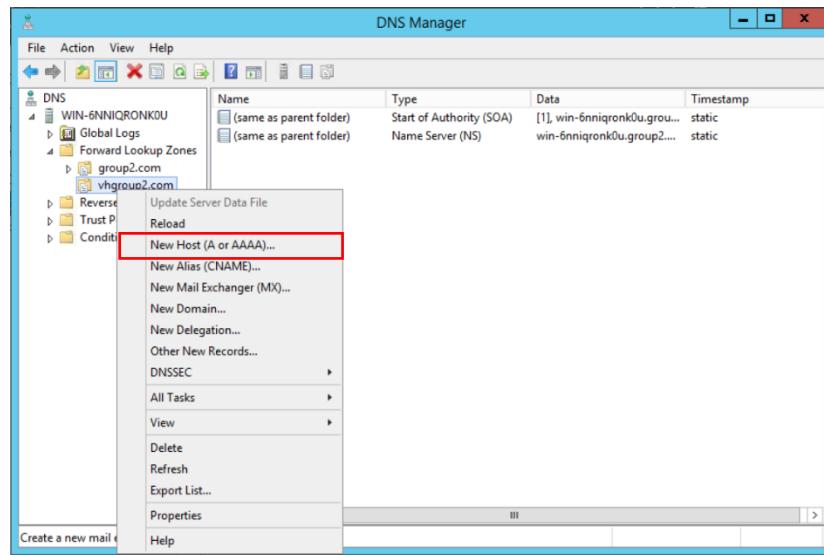


Figure 145: Adding host

**Step 14:** Enter the ip address **192.168.5.200** and click the **Add Host**.

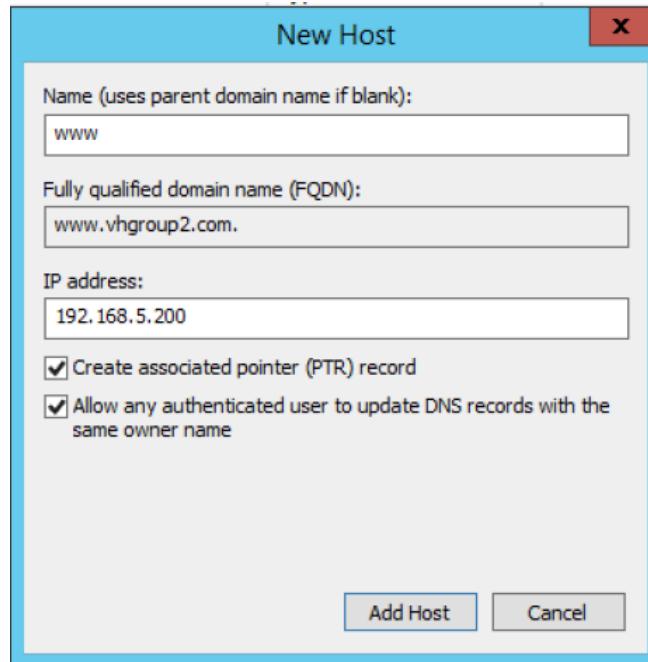
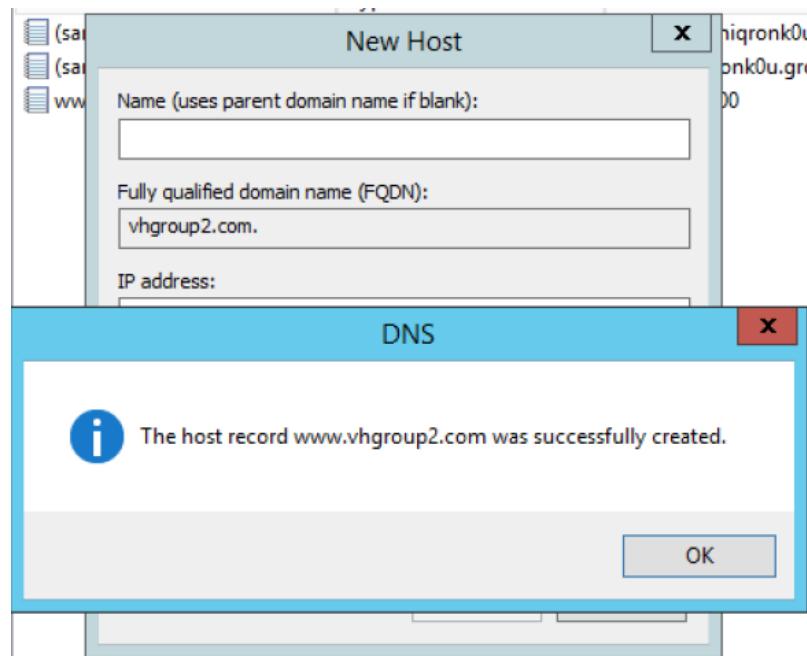


Figure 146: Entering ip address in new host

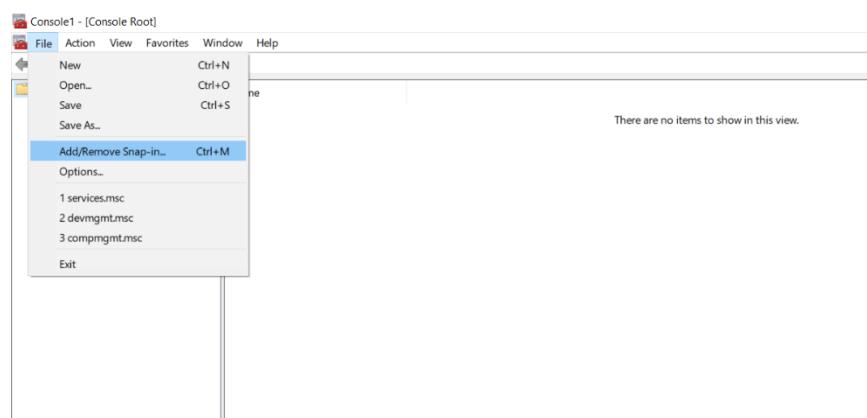
**Step 15:** Host created and click **OK**.



*Figure 147: Host created*

**Step 16:** To trust the Domain Certificate, go to **Microsoft Management Console (MMC)**.

**Step 17:** Click **File** and select **Add/Remove Snap-in**.



*Figure 148: Click File and select Add/ Remove Snap-in*

**Step 18:** Select Certificates in Available snap-ins window. Then, click Add.

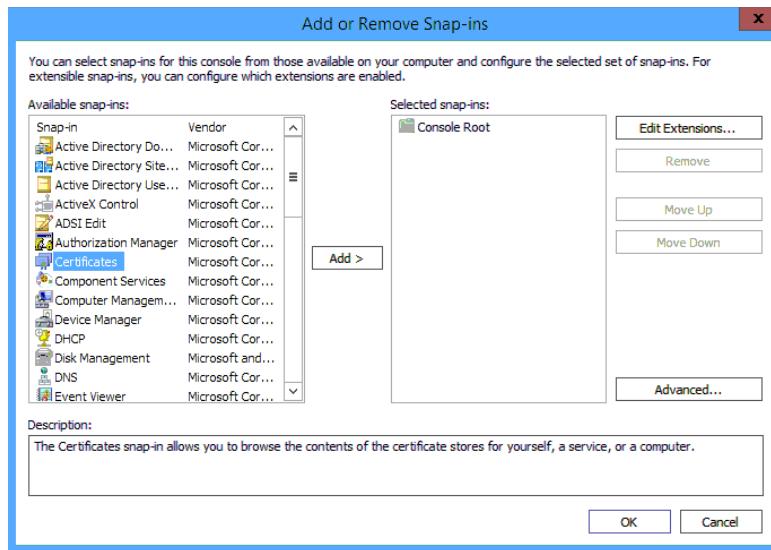


Figure 149: Select Certificates and click Add

**Step 19:** Choose My user account.

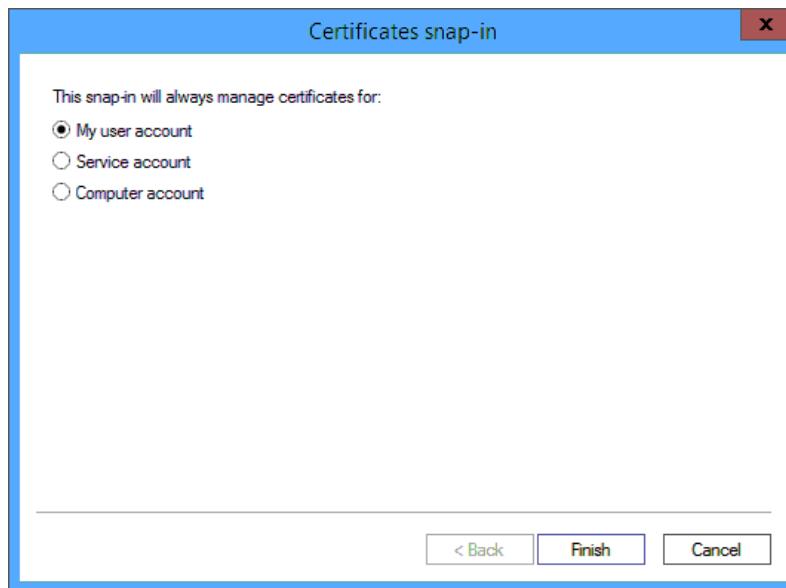


Figure 150: Choose My user account

**Step 20:** Click **OK** after add snap-ins.

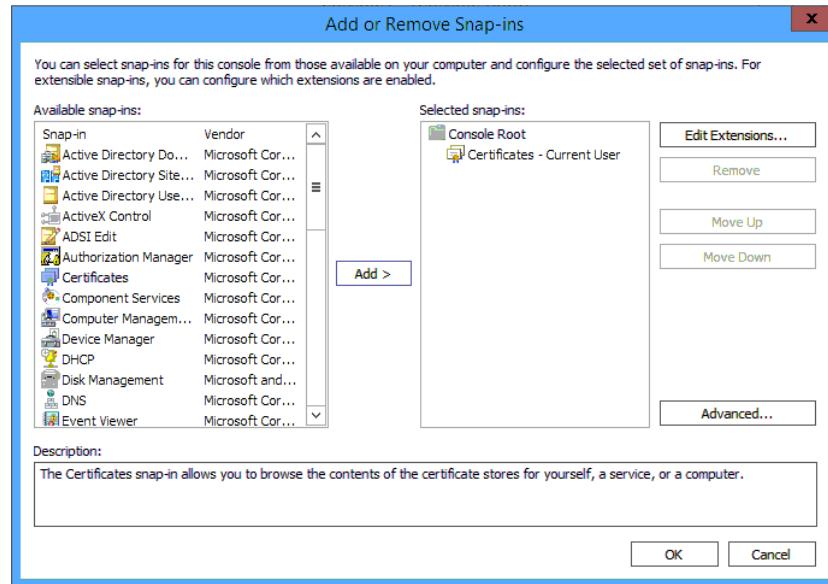


Figure 151: Selected Snap-ins

**Step 21:** Find the cerificate that want to trust and right-click on it. Then, export it by selecting **All Tasks** and click **Export**.

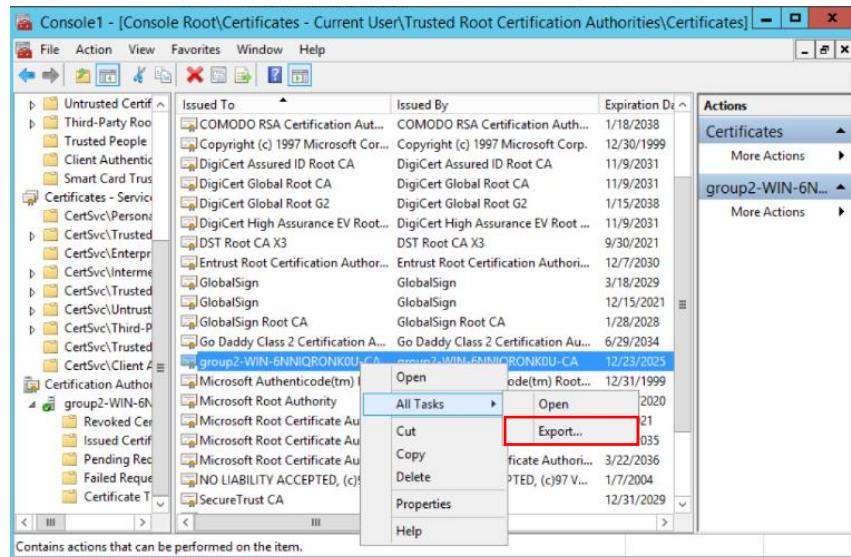


Figure 152: Export the certificate that want to trust

**Step 22:** Click **Next** when the Certificate Export Wizard prompted.

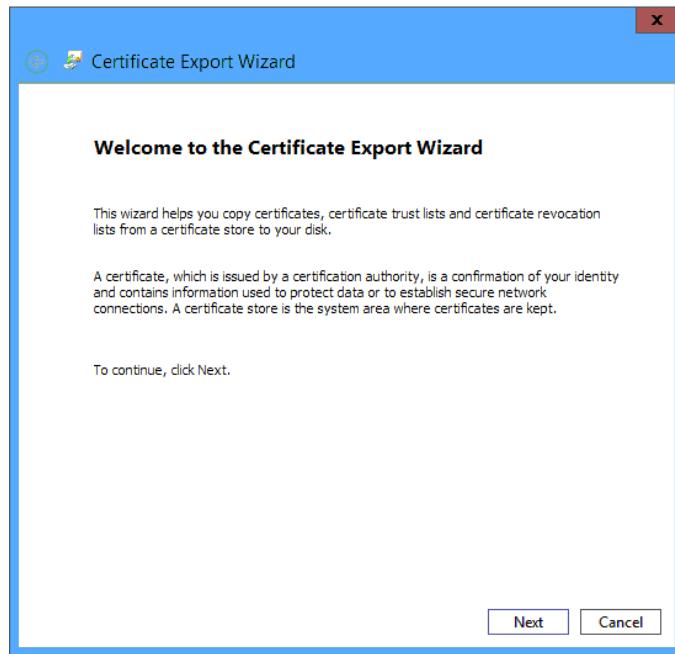


Figure 153: Certificate Export Wizard

**Step 23:** Choose **DER encoded binary X.509 (.CER)** as export file format.

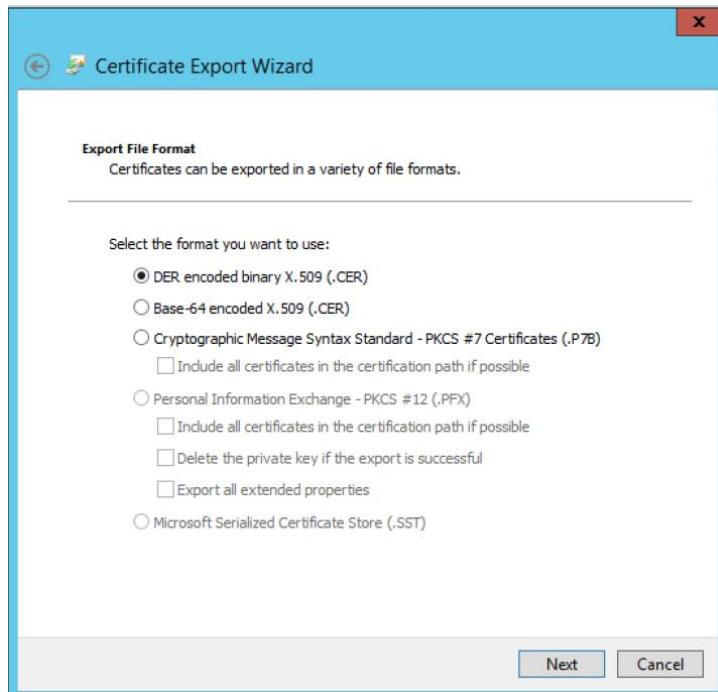


Figure 154: Export file format

**Step 24:** Fill in the name of the file that want to export.

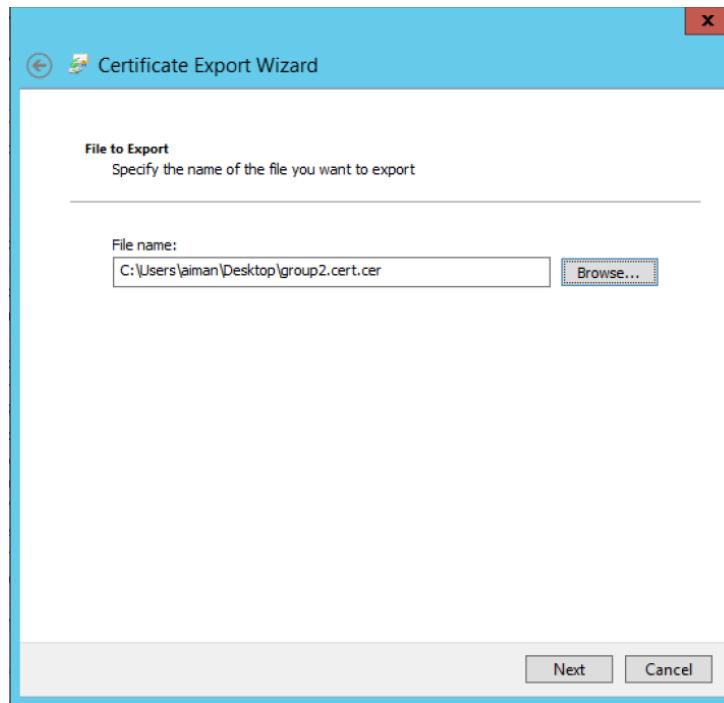


Figure 155: Name of the exported file

**Step 25:** Click **Finish** after completing the certificate export wizard.

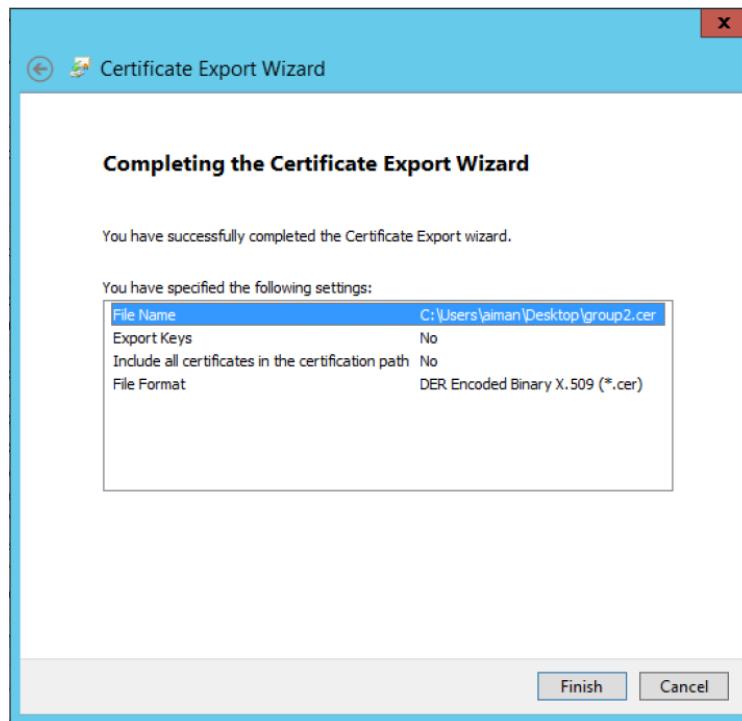


Figure 156: Completing the certificate export wizard

**Step 26:** Click **OK** on the window that informs the export was successful.

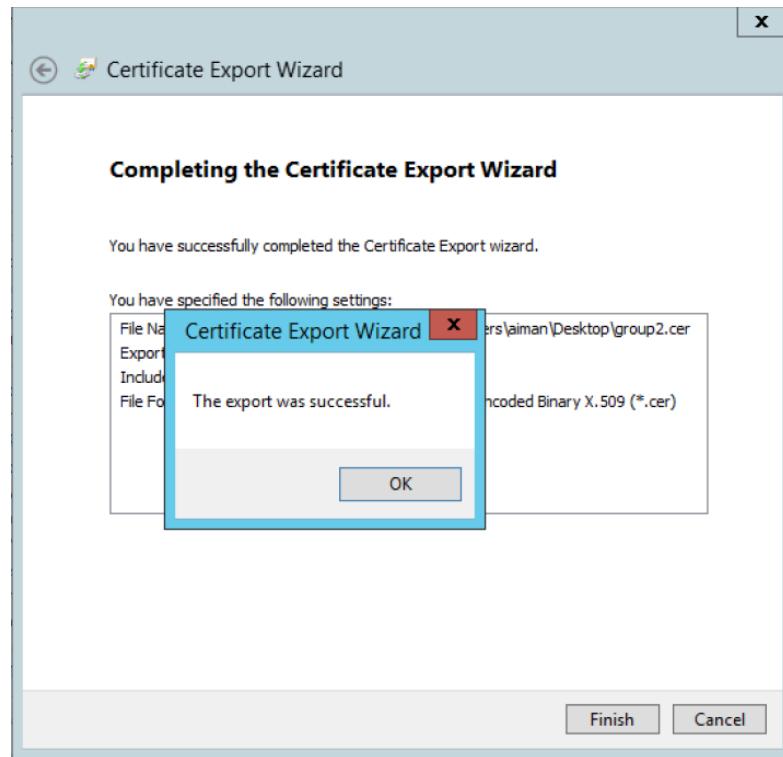


Figure 157: Export was successful

**Step 27:** Create a folder called SharedCert in the C drive (C:).

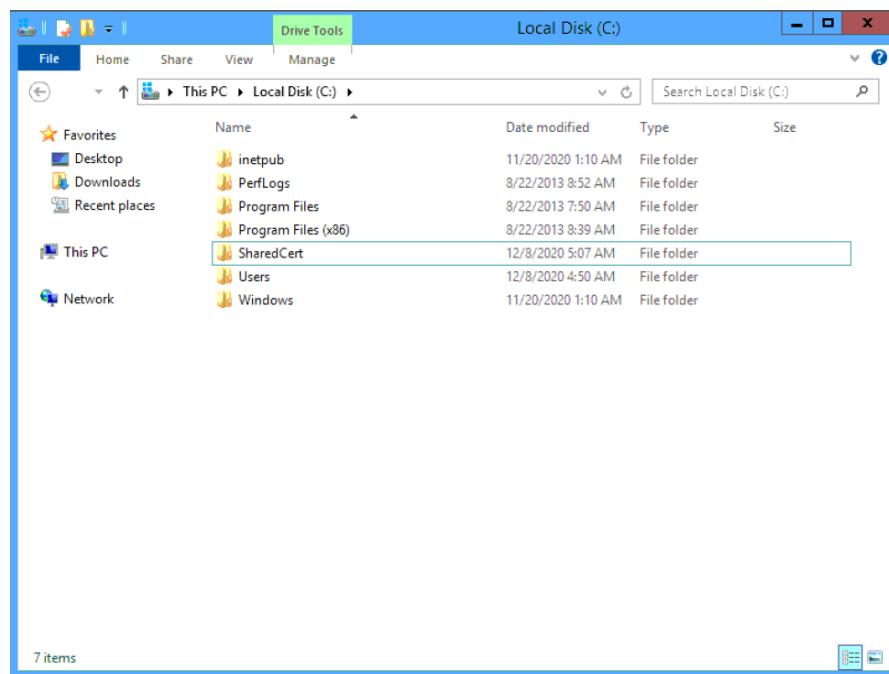


Figure 158: Creating SharedCert folder

**Step 28:** Drag or move the exported certificate to the SharedCert folder.

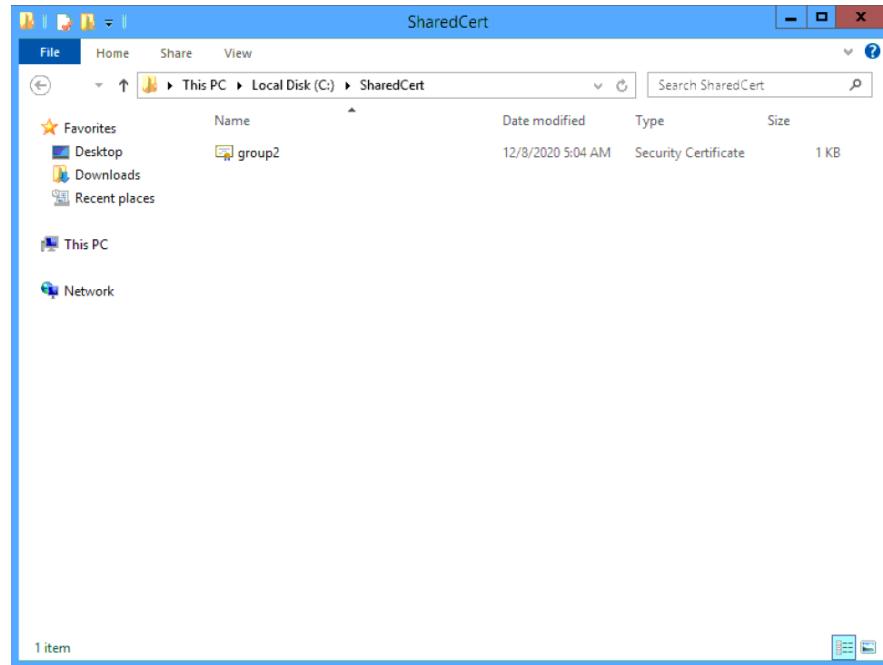


Figure 159: Move the exported certificate to the SharedCert folder

**Step 29:** Open **Group Policy Management**. Then, right-click on the domain and select **Create a GPO in this domain, and Link it here...**

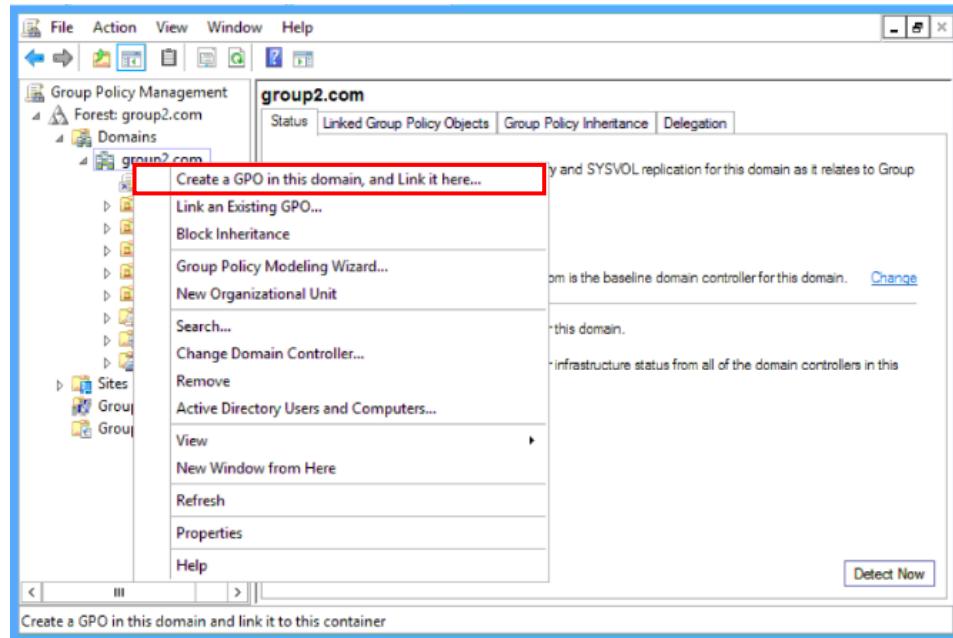


Figure 160: Create a GPO in this group2.com

**Step 30:** Fill in the name of the new GPO.

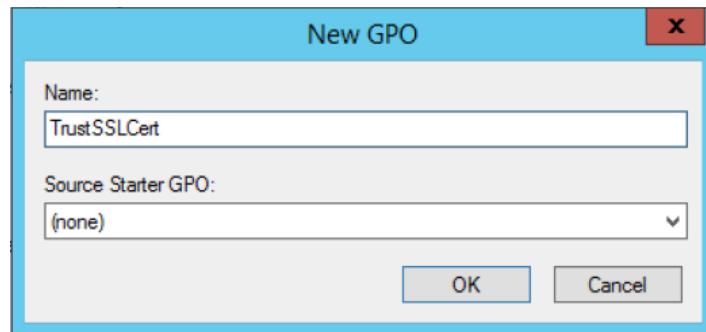


Figure 161: TrustSSLCert as name of new GPO

**Step 31:** Right-click on the **TrustDomain** and select **Edit** to open Group Policy Management Editor. Then, click Window Settings and select **Security Settings**.

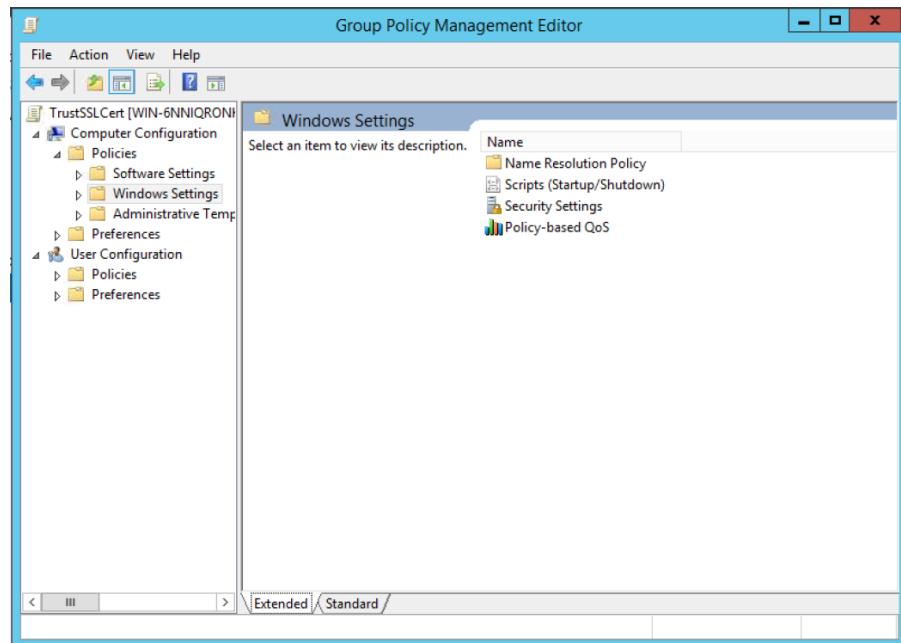


Figure 162: Windows Settings of policy

### Step 32: Select Public Key Policies.

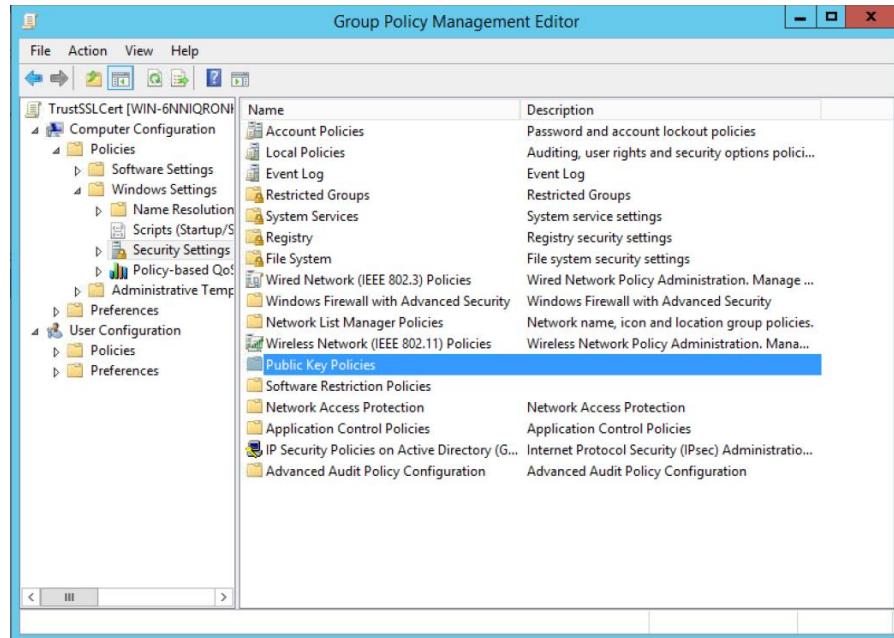


Figure 163: Security settings of Windows settings

### Step 33: Select Trusted Root Certification Authorities.

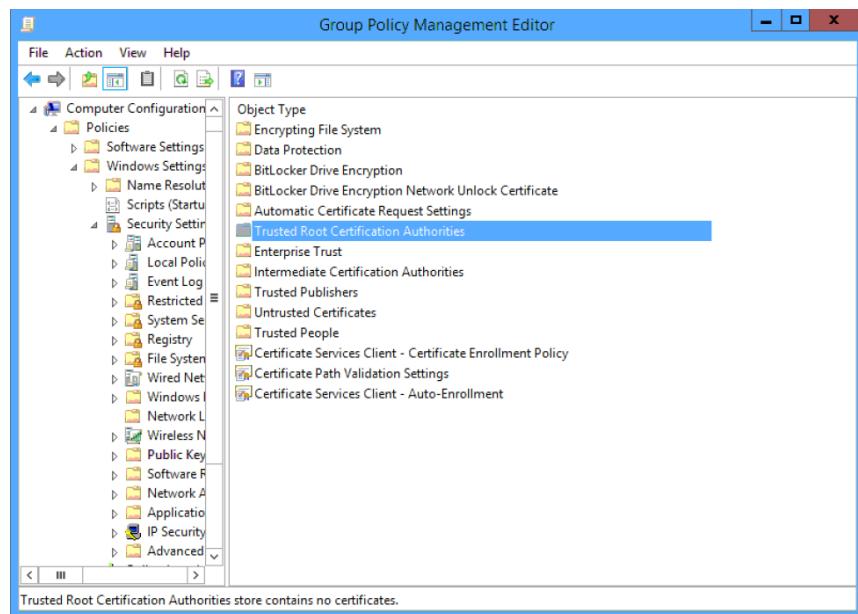


Figure 164: Selecting Trusted Root Certification Authorities in security settings

**Step 34:** Right-click on the blank and select **import**.

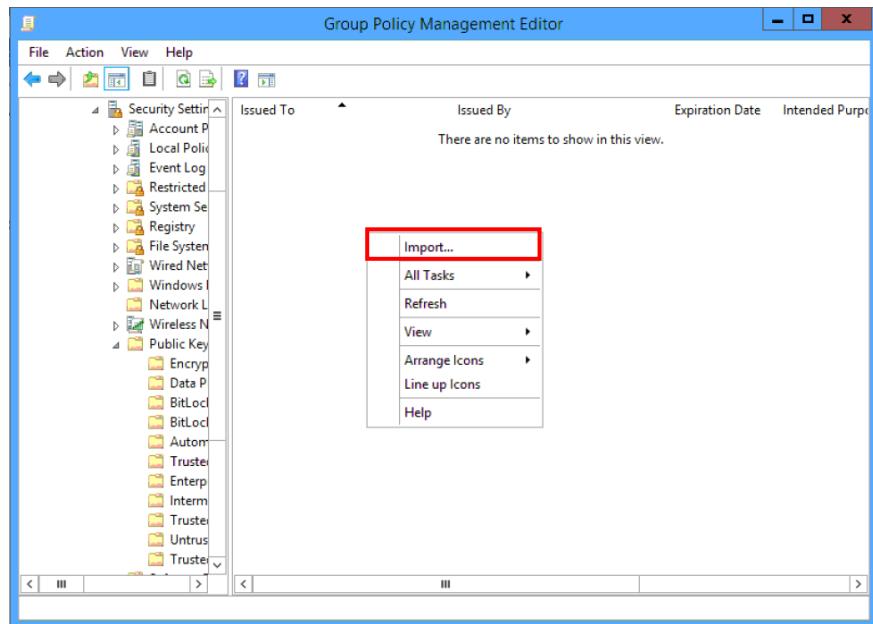


Figure 165: Selecting import

**Step 35:** Click **Next** on the Certificate Import Wizard.

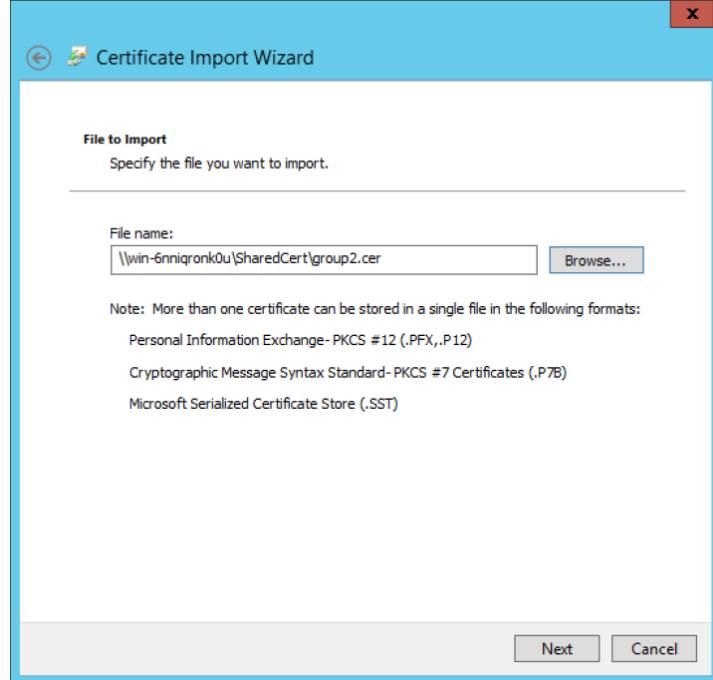
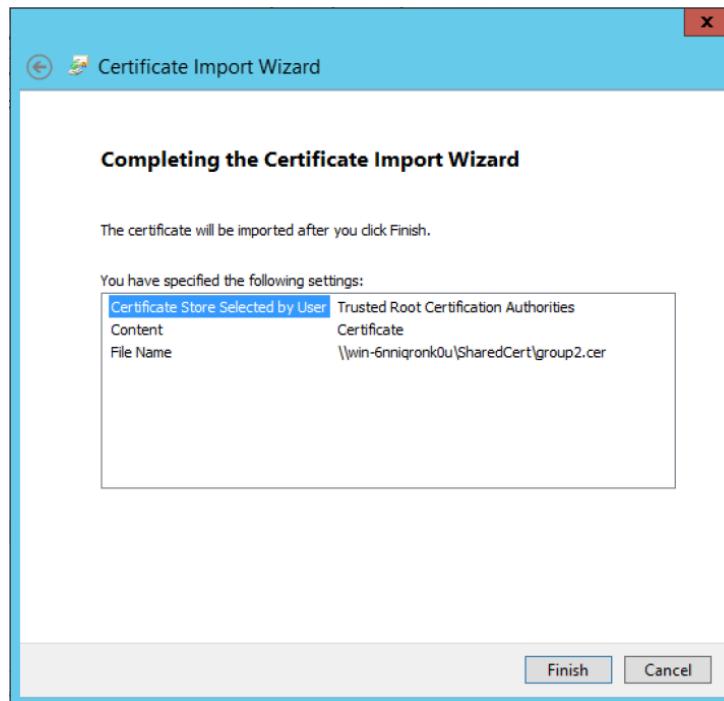


Figure 166: Specify the file want to export

**Step 36:** Click **Finish** after completing the certificate import wizard.

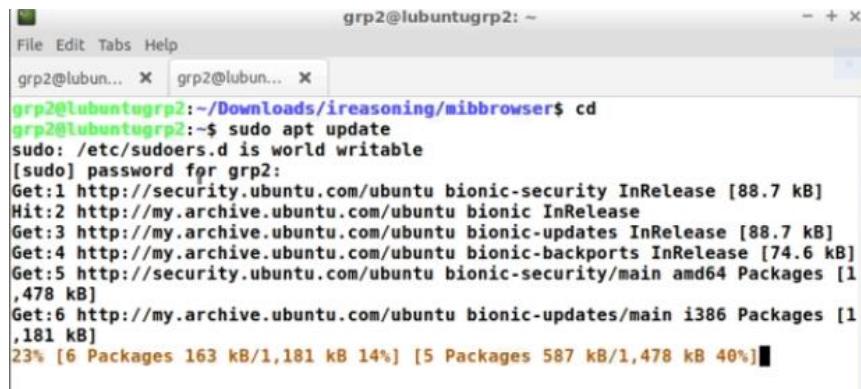


*Figure 167: completing the certificate import wizard*

### 5.3.9 NETWORK MONITORING SYSTEM

For the network monitoring system, we choose Nagios Core to monitor the network. Nagios Core can monitor Network bandwidth usage, packet loss rate, interface error rate, high CPU or memory utilization and many more. Below is the step on how to install and configure Nagios Core on Ubuntu.

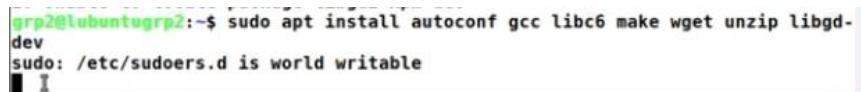
#### Step 1: Update the package list



```
grp2@lubuntugrp2:~$ sudo apt update
[sudo] password for grp2:
Get:1 http://security.ubuntu.com/ubuntu bionic-security InRelease [88.7 kB]
Hit:2 http://my.archive.ubuntu.com/ubuntu bionic InRelease
Get:3 http://my.archive.ubuntu.com/ubuntu bionic-updates InRelease [88.7 kB]
Get:4 http://my.archive.ubuntu.com/ubuntu bionic-backports InRelease [74.6 kB]
Get:5 http://security.ubuntu.com/ubuntu bionic-security/main amd64 Packages [1,478 kB]
Get:6 http://my.archive.ubuntu.com/ubuntu bionic-updates/main i386 Packages [1,181 kB]
23% [6 Packages 163 kB/1,181 kB 14%] [5 Packages 587 kB/1,478 kB 40%]
```

Figure 168 apt update

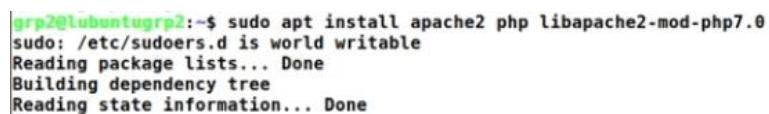
#### Step 2: Install the prerequisite packages necessary for building Nagios and Nagios plugins



```
grp2@lubuntugrp2:~$ sudo apt install autoconf gcc libc6 make wget unzip libgd-dev
[sudo] password for grp2:
```

Figure 169 Installing Nagios

#### Step 3: Installing Apache, PHP 7 and all necessary modules on Ubuntu.



```
grp2@lubuntugrp2:~$ sudo apt install apache2 php libapache2-mod-php7.0
[sudo] password for grp2:
Reading package lists... Done
Building dependency tree
Reading state information... Done
```

Figure 170 Installing Apache

#### Step 4: Enable apache to start on boot



```
grp2@lubuntugrp2:~$ sudo systemctl enable apache2.service
[sudo] password for grp2:
Synchronizing state of apache2.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable apache2
```

Figure 171 Start the Apache

#### Step 5: Downloading Nagios Core tar archive

```
@lubuntugrp2:~$ wget https://assets.nagios.com/downloads/nagioscore/releases/nagios-4.4.6.tar.gz -P /tmp  
21-01-08 03:22:15-- https://assets.nagios.com/downloads/nagioscore/releases/nagios-4.4.6.tar.gz  
lving assets.nagios.com (assets.nagios.com)... 72.14.181.71, 2600:3c00::f0  
1ff:fedf:b821  
fecting to assets.nagios.com (assets.nagios.com)|72.14.181.71|:443... conne
```

Figure 172 Downloading Nagios Core archive

**Step 6:** Extracting the archive directory

```
grp2@lubuntugrp2:~$ cd /tmp  
grp2@lubuntugrp2:/tmp$ tar xzf nagios-4.4.6.tar.gz
```

Figure 173 Extracting the file

**Step 7:** Run the configure script which will check the system for missing libraries and binaries and prepare the Nagios source code for the build process

```
grp2@lubuntugrp2:/tmp$ cd nagios-4.4.6/  
grp2@lubuntugrp2:/tmp/nagios-4.4.6$ ./configure --with-httpd-conf=/etc/apache2/sites-enabled
```

Figure 174 Run the configure file

**Step 8:** Start the compilation process

```
grp2@lubuntugrp2:/tmp/nagios-4.4.6$ make all
```

Figure 175 Starting the compilation

**Step 9:** Creating Nagios user and group

```
grp2@lubuntugrp2:/tmp/nagios-4.4.6$ sudo make install-groups-users  
grp2@lubuntugrp2:/tmp/nagios-4.4.6$ sudo usermod -aG nagios www-data
```

Figure 176 Creating user & group

**Step 10:** Installing Nagios service configuration files

```
grp2@lubuntugrp2:/tmp/nagios-4.4.6$ sudo make install-daemoninit
```

Figure 177 Installing configuration file

**Step 11:** Installing and configure permissions on the directory

```
grp2@lubuntugrp2:/tmp/nagios-4.4.6$ sudo make install-commandmode
```

Figure 178 Configure permission

**Step 12:** Installing Apache configuration files for Nagios web interface

```
grp2@lubuntugrp2:/tmp/nagios-4.4.6$ sudo make install-webconf
```

Figure 179 Configuration for web interfaces

**Step 13:** Enabling Apache rewrite and CGI modules

```
|grp2@lubuntugrp2:/tmp/nagios-4.4.6$ sudo a2enmod rewrite cgi
```

Figure 180 Enable Apache

#### Step 14: Setup Nagios Apache authentication

```
|grp2@lubuntugrp2:/tmp/nagios-4.4.6$ sudo htpasswd -c /usr/local/nagios/etc/htpasswd.users nagiosadmin  
sudo: /etc/sudoers.d is world writable  
New password: ■
```

Figure 181 Setup authentication

#### Step 15: Setting the ownership of the Nagios Apache authentication configuration file to web-server user

```
|grp2@lubuntugrp2:/tmp/nagios-4.4.6$ sudo chown www-data.www-data /usr/local/nagios/etc/htpasswd.users  
|grp2@lubuntugrp2:/tmp/nagios-4.4.6$ sudo chmod 640 /usr/local/nagios/etc/htpasswd.users
```

Figure 182 Setting ownership

#### Step 16: Restarting the Apache

```
|grp2@lubuntugrp2:/tmp/nagios-4.4.6$ systemctl restart apache2
```

Figure 183 Restart Apache

#### Step 17: Starting Nagios Core service and check the status

```
|grp2@lubuntugrp2:/tmp/nagios-4.4.6$ systemctl start nagios.service  
|grp2@lubuntugrp2:/tmp/nagios-4.4.6$ systemctl status nagios.service
```

Figure 184 Starting Nagios

### Step 18: Installing Nagios Plugins and extracting the file

```
grp2@lubuntugrp2:~$ wget https://nagios-plugins.org/download/nagios-plugins-2.3.3.tar.gz -P /tmp/  
grp2@lubuntugrp2:~$ cd /tmp  
grp2@lubuntugrp2:/tmp$ tar xzf nagios-plugins-2.3.3.tar.gz  
grp2@lubuntugrp2:/tmp$ cd nagios-plugins-2.3.3/  
grp2@lubuntugrp2:/tmp/nagios-plugins-2.3.3$ ./configure --with-nagios-user=nagios --with-nagios-group=nagios
```

Figure 185 Installing Nagios plugins

### Step 19: The frontend interface for Nagios Core

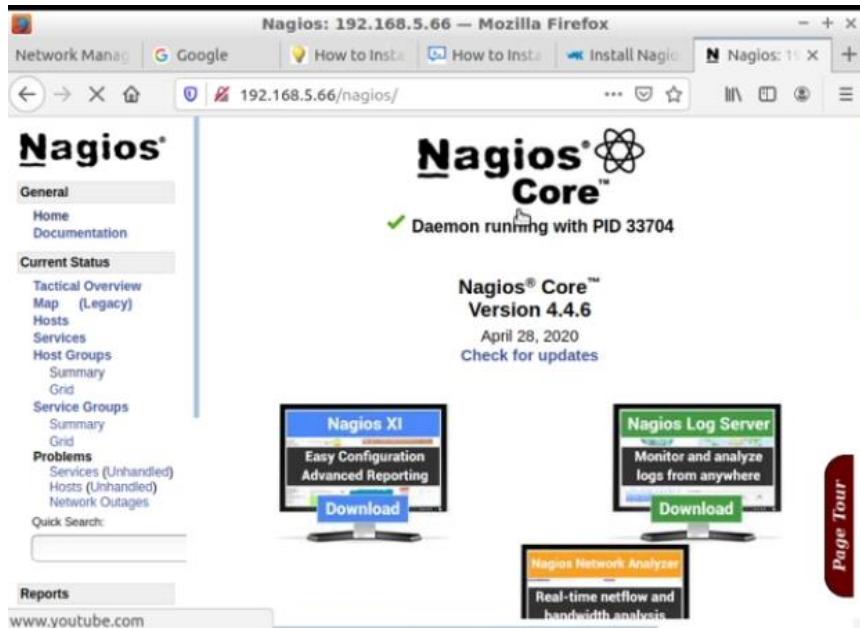


Figure 186 Frontend interface

### 5.3.10 AAA (AUTHENTICATION AUTHORIZATION AND ACCOUNTING) USING RADIUS

**Step 1:** Open Active Directory User and Computer and create a new group as follows.

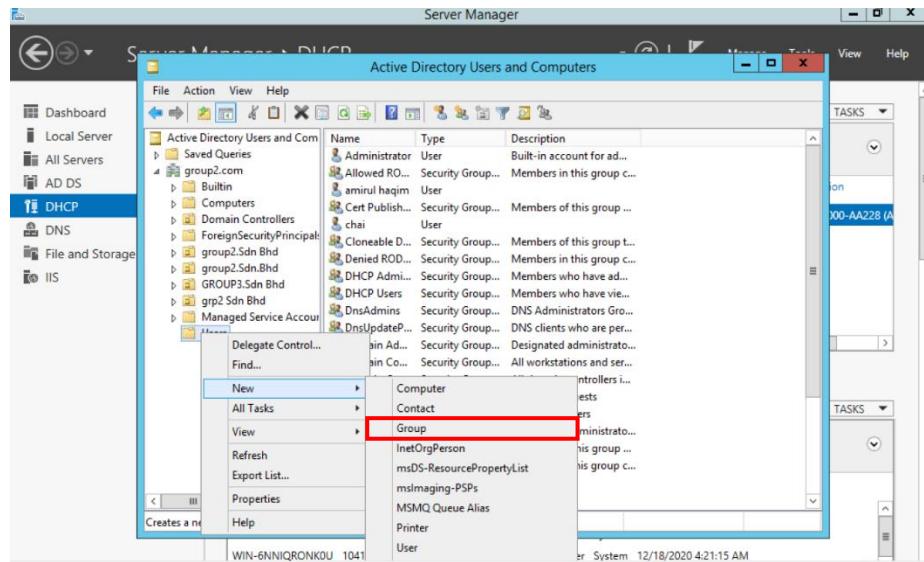


Figure 187: Creating new group

**Step 2:** Create ‘wkspgroup2’ group for Radius users who have the privilege level 15.

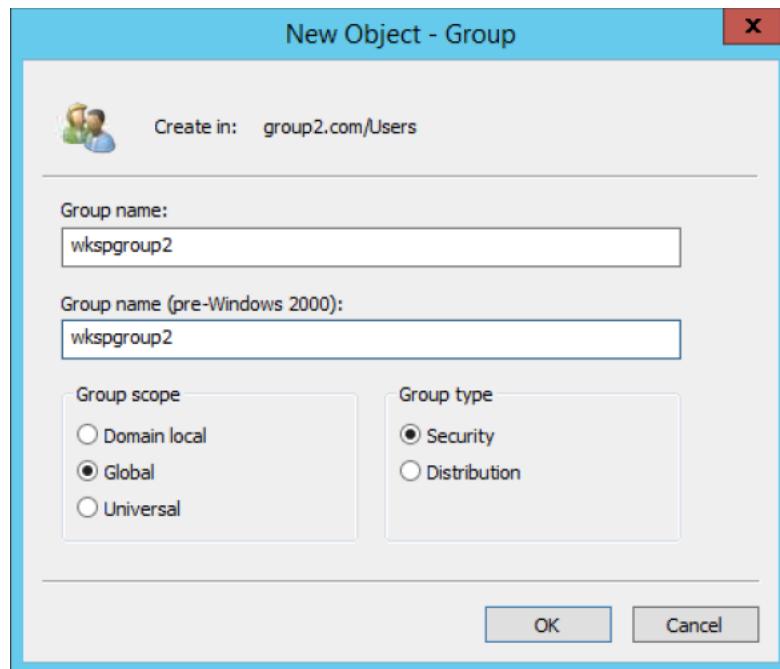


Figure 188: Filling in the name of the new group

**Step 3:** Assign the **Domain Admins** to the group **wkshgroup2** by right clicking at the group and choose add to group option.

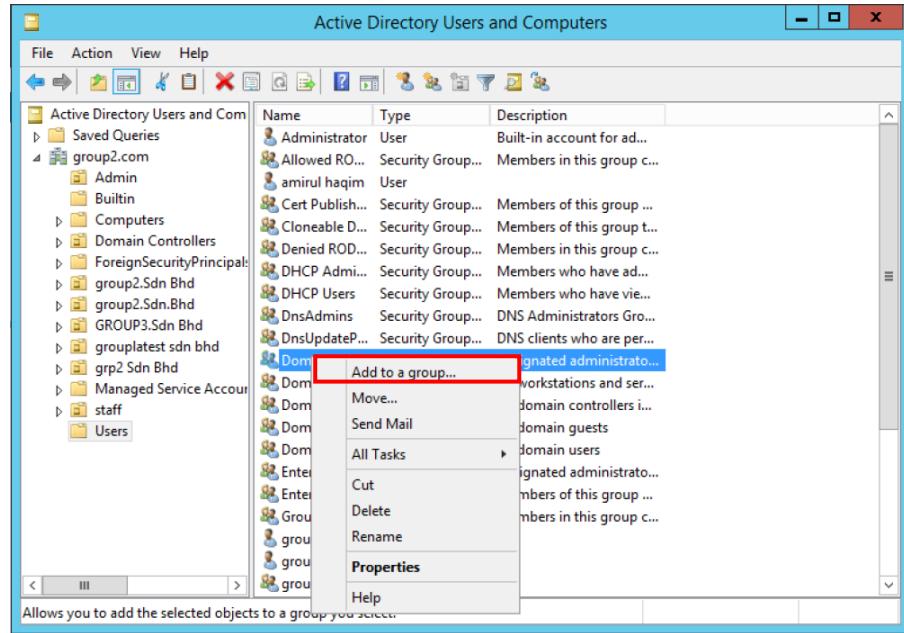


Figure 189: Adding user to a group

**Step 4:** To assign the user to the group, type the group name in the text area and click **Check Names**. Error message will pop up if the group does not exist.

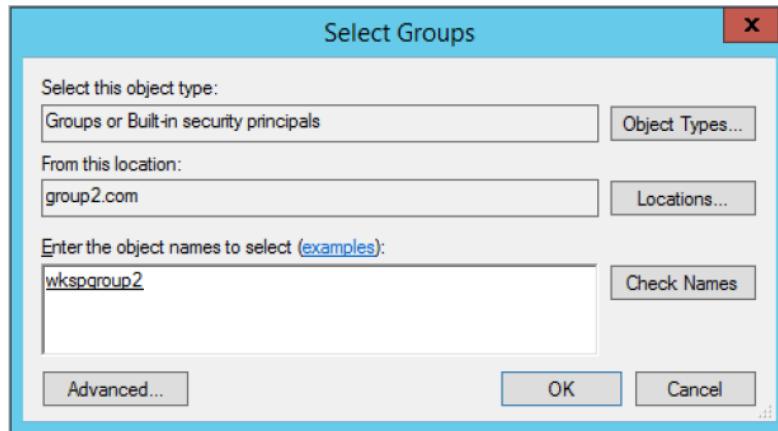


Figure 190: Selecting group

**Step 5:** The group will now have user in its members list. **Domain Admins** users were added into wkspgroup2. Then, click **OK** on the group properties.

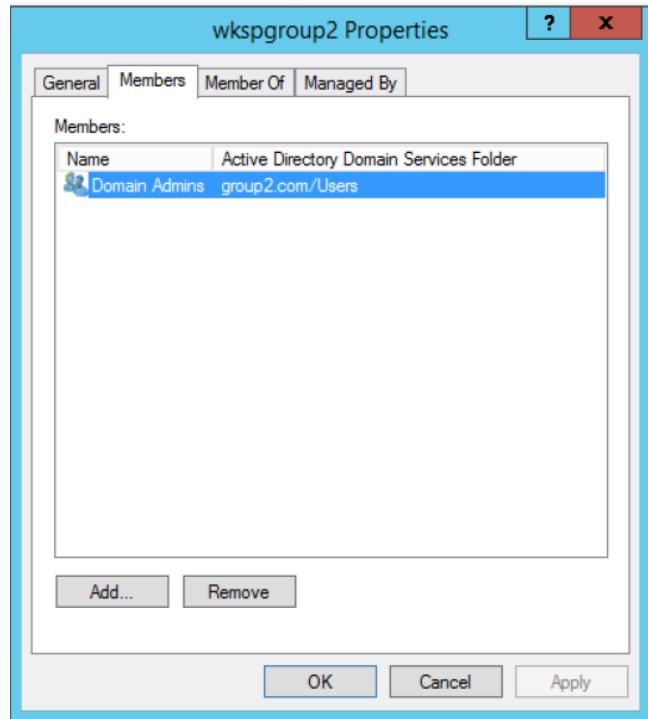


Figure 191: Domain Admins are the member of wkspgroup2

**Step 6:** Go to **Server Manager** to install Network Policy Service. Click on **Tools** and select **Add Roles and Features**.

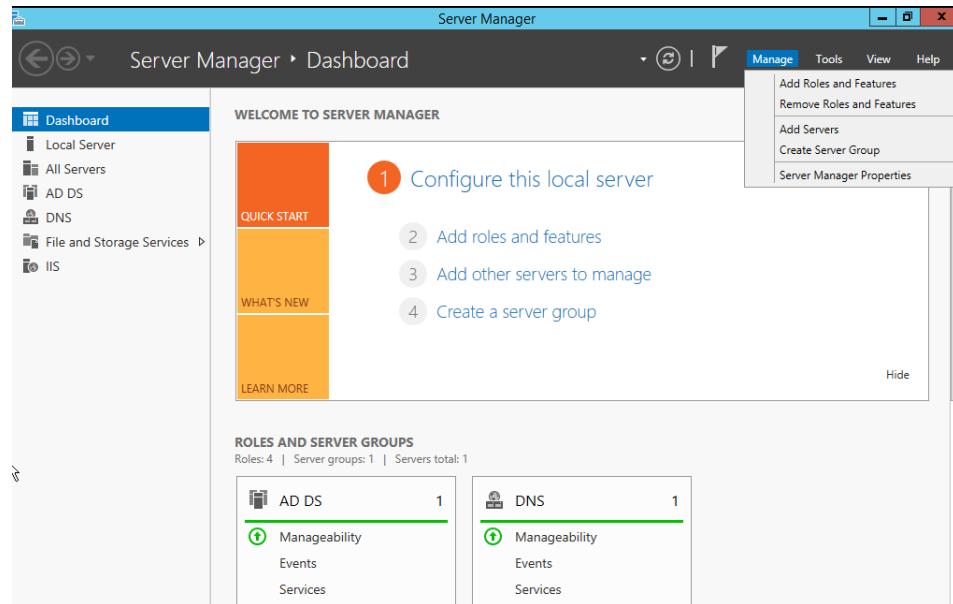


Figure 192: Server Manager

**Step 7:** Click **Next** at the installation wizard.

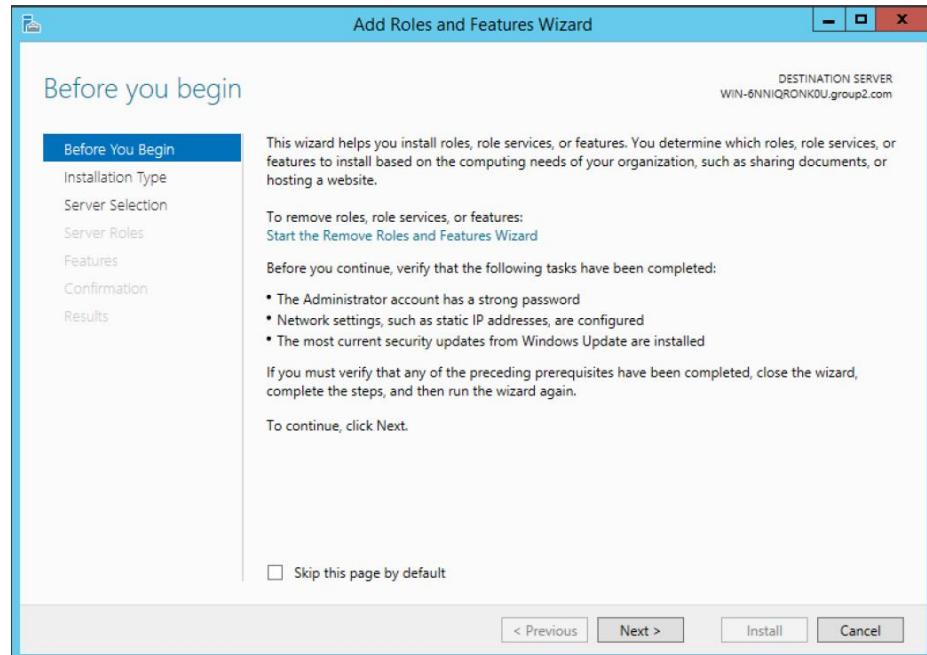


Figure 193: Add Roles and Features

**Step 8:** Select **Role-based or feature-based Installation type** when select installation type.

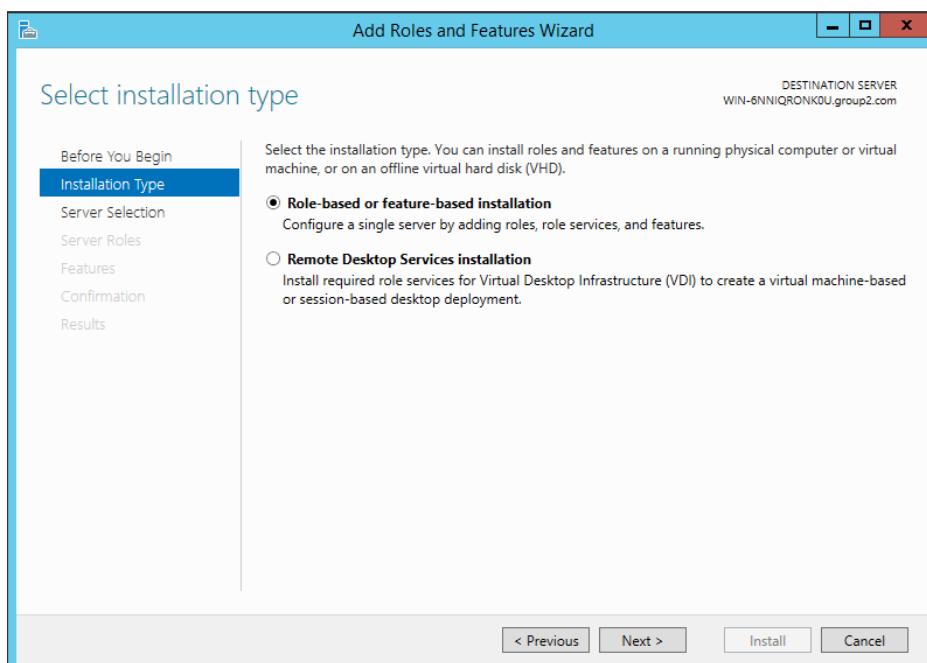


Figure 194: Selection installation type

**Step 9:** Tick **Select the local server from the server pool** and click next to proceed.

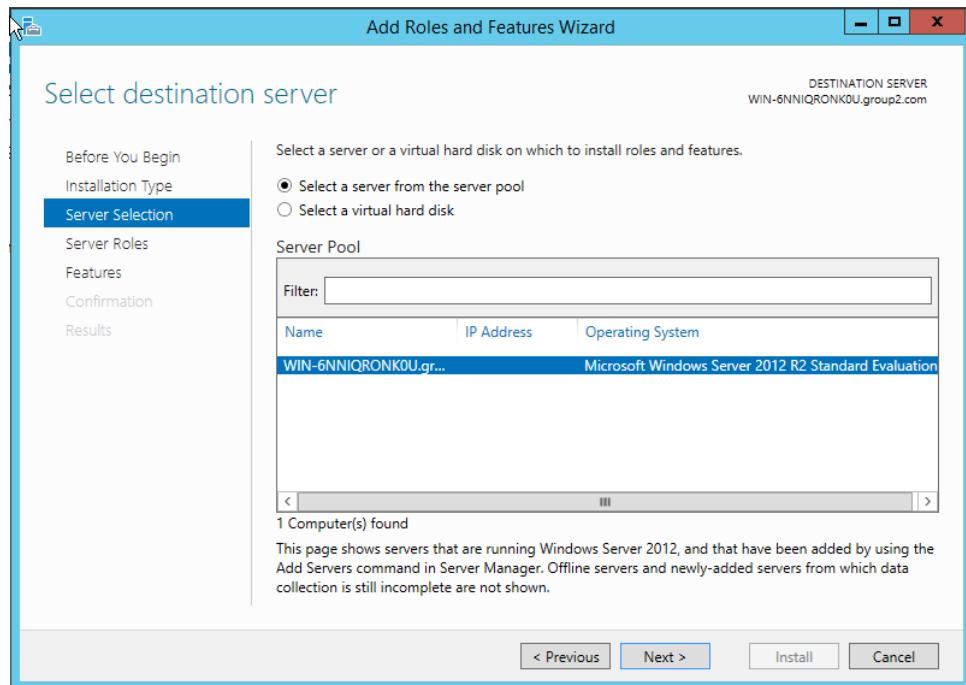


Figure 195: Add destination server

**Step 10:** In the Server Roles section, select **Network Policy and Access Services** and click **Next**.

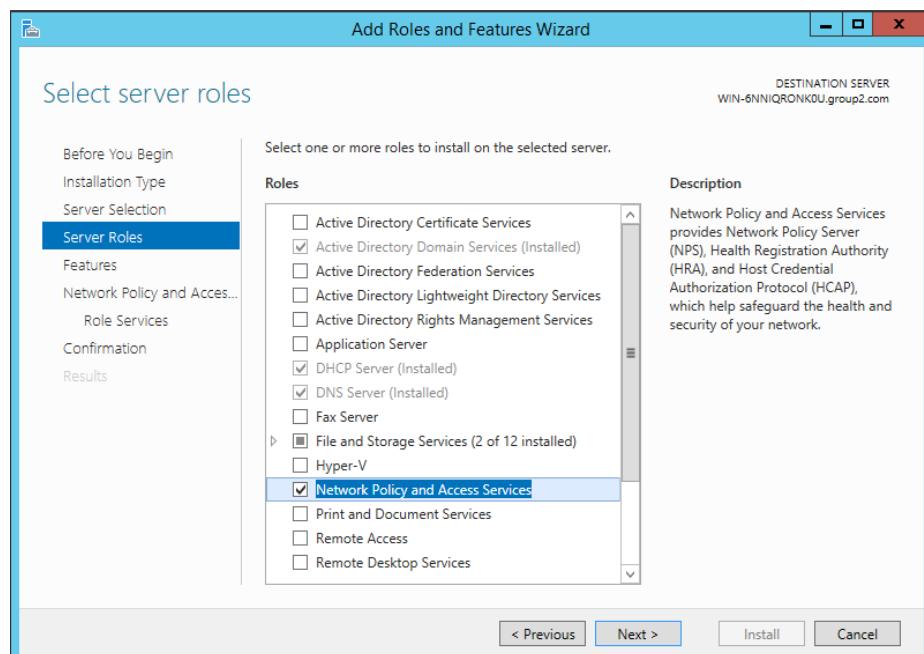


Figure 196: Selecting Network Policy and Access Services

**Step 11:** Click **Next** at the features section of the installation process as there is no additional features required for this project.

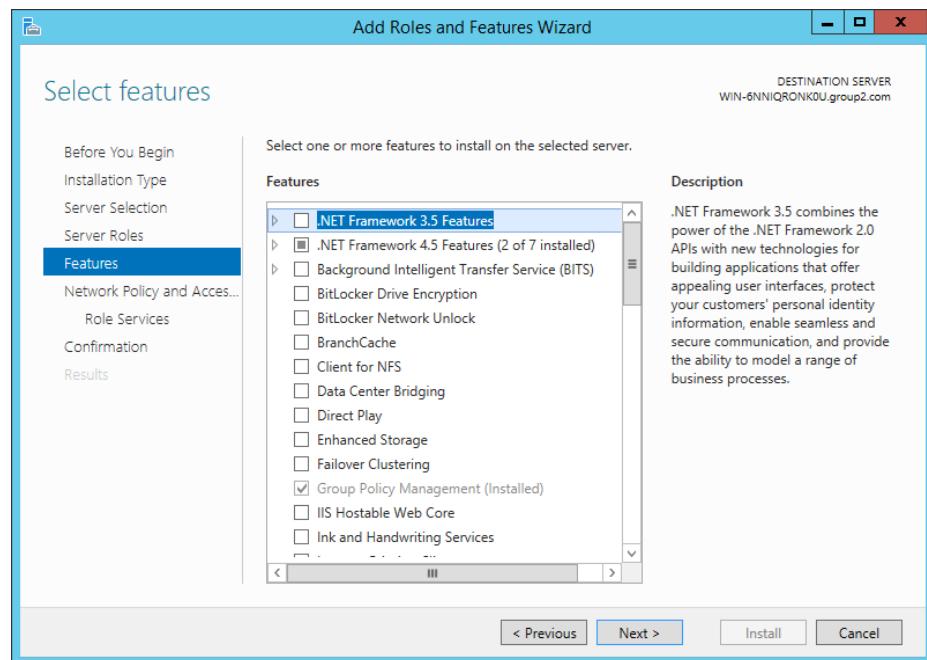


Figure 197: Selecting features

**Step 12:** Click **Next** for the **Network Policy and Access Services** section.

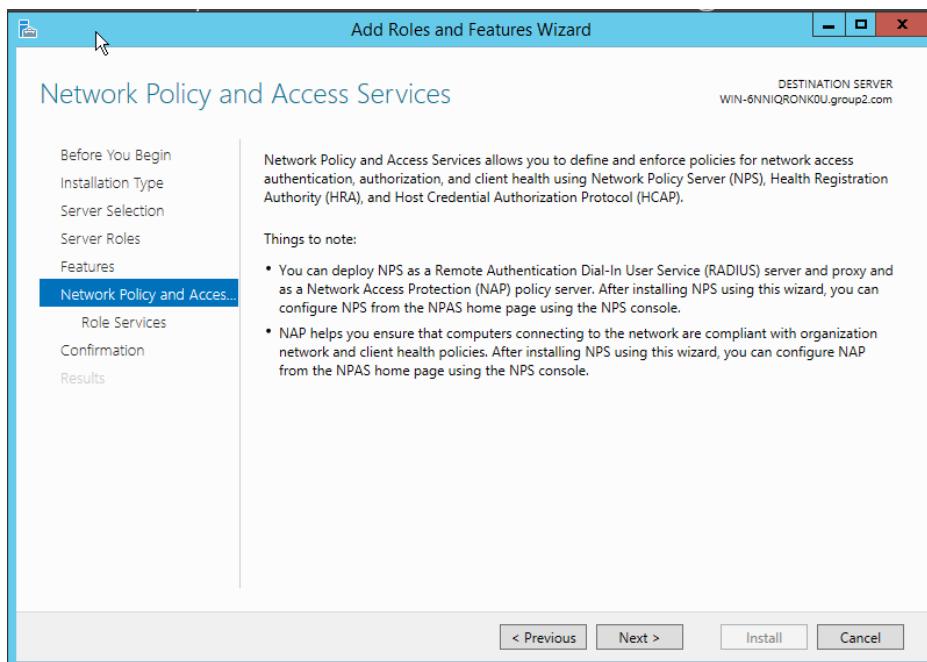


Figure 198: Overview of Network Policy and Access Services

**Step 13:** Select the **Network Policy Server** when select the Role Services. Then, click **Next** to proceed to the next step for installation.

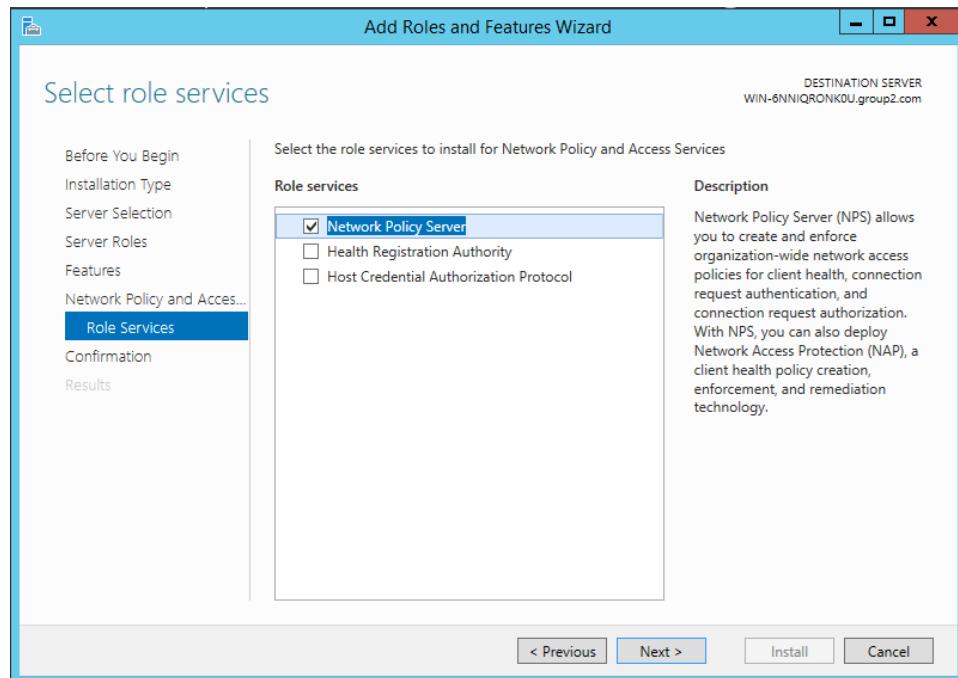


Figure 199: Selecting Network Policy Server

**Step 14:** Tick the **Restart the destination server automatically if required** and click **Install** for the installation process begins.

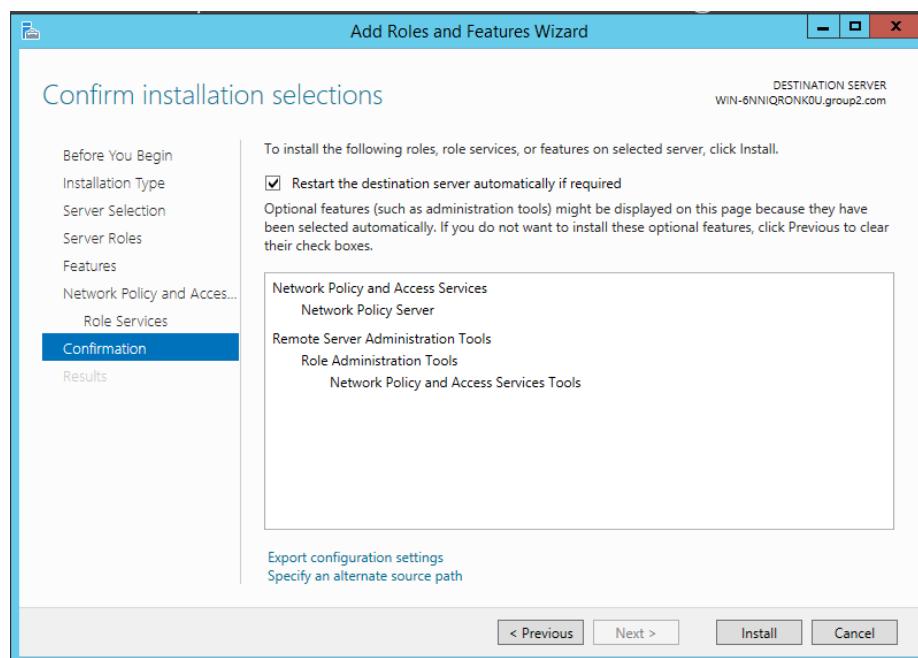


Figure 200: Confirm installation selections

**Step 15:** The installation process will complete in few minutes.

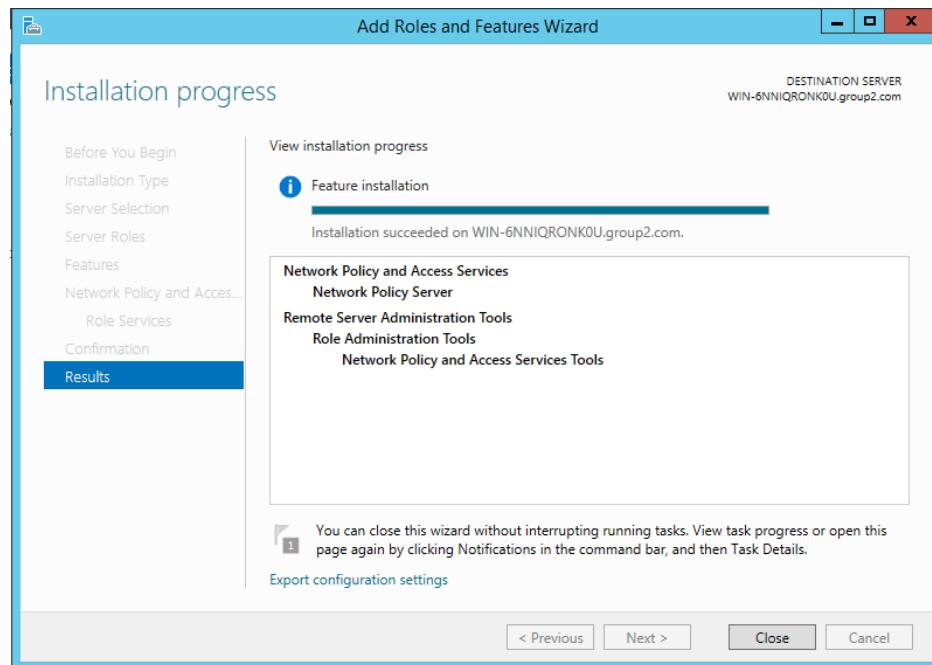


Figure 201: Complete installation process

**Step 16:** Go to Server Manager and click on Tools. Then, select the **Network Policy Server** that has been installed.

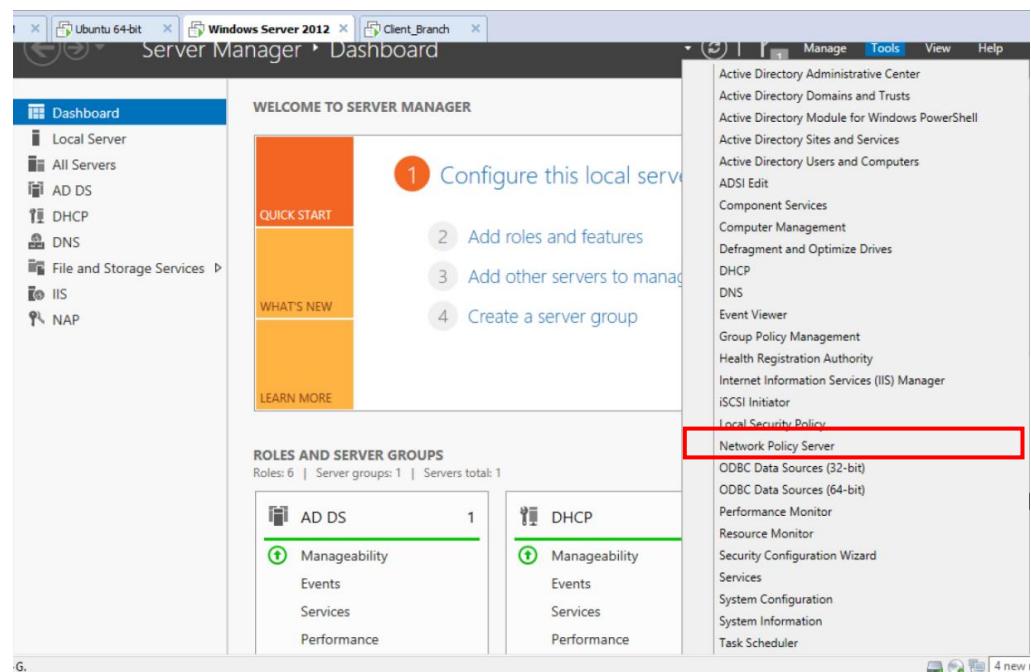


Figure 202: Navigate to Network Policy Server

**Step 17:** Right click the NPS (local) and select **Register server in Active Directory**.

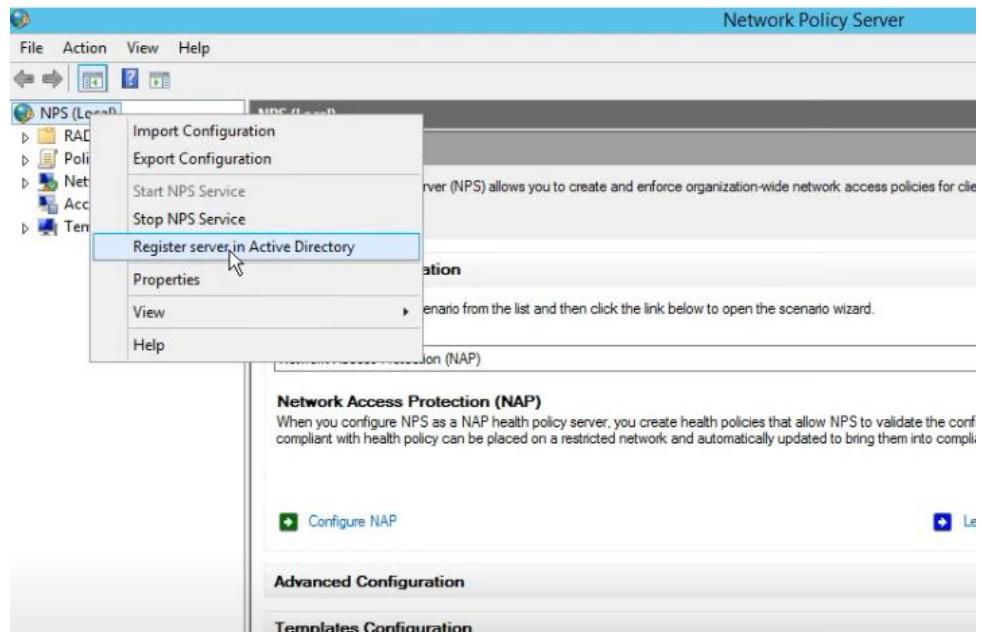


Figure 203: Register servers in Active Directory

**Step 18:** To create new RADIUS client, right click **Radius Clients** at the left column and select **New** to create a new Radius Client.

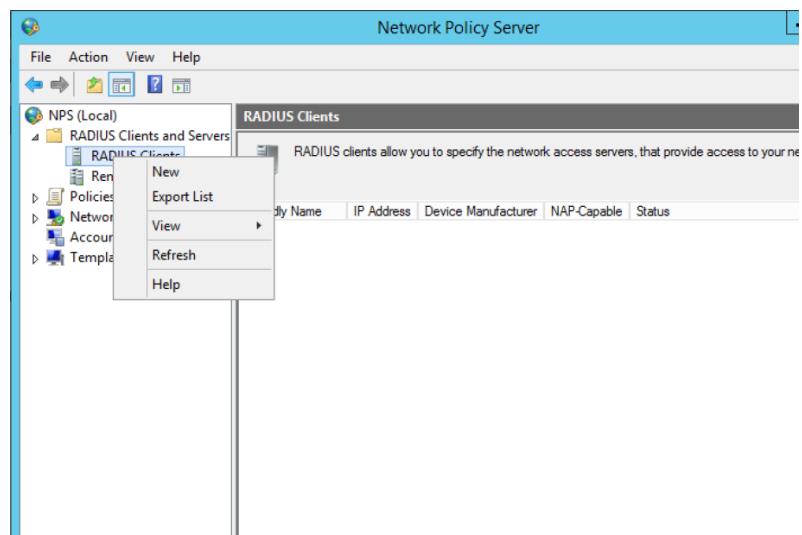


Figure 204: Adding Radius Client

**Step 19:** Enter the friendly name for the client, ip address of the **RouterHQ** router (default gateway of the radius server) and the shares key at the windows.

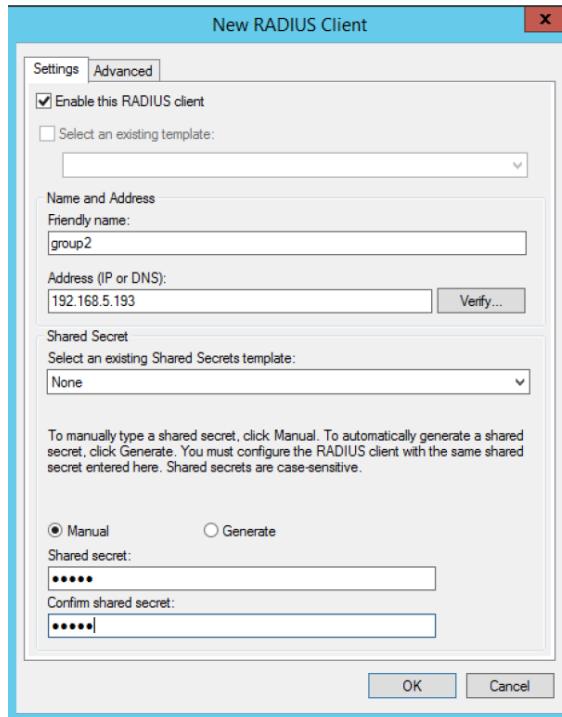


Figure 205: Creating a new Radius Client

**Step 20:** Click on the **Advance** tab and select **Cisco** as the vendor name of Radius Client.

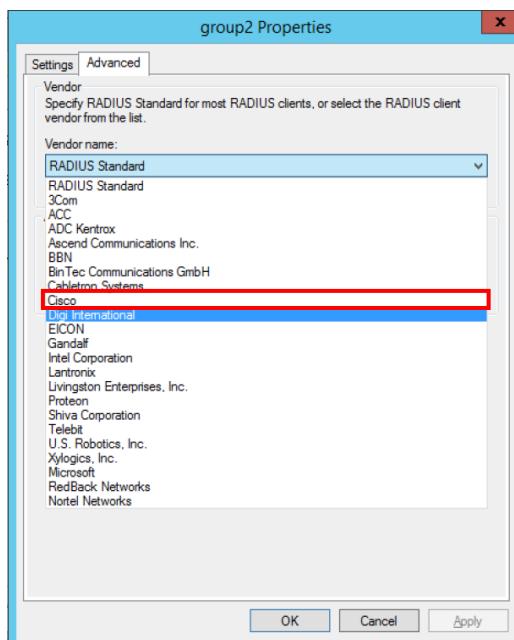


Figure 206: Selecting vendor name of the Radius Client in Advanced tab

**Step 21:** After selecting the vendor of the Radius Client, click **Apply** and **OK**.

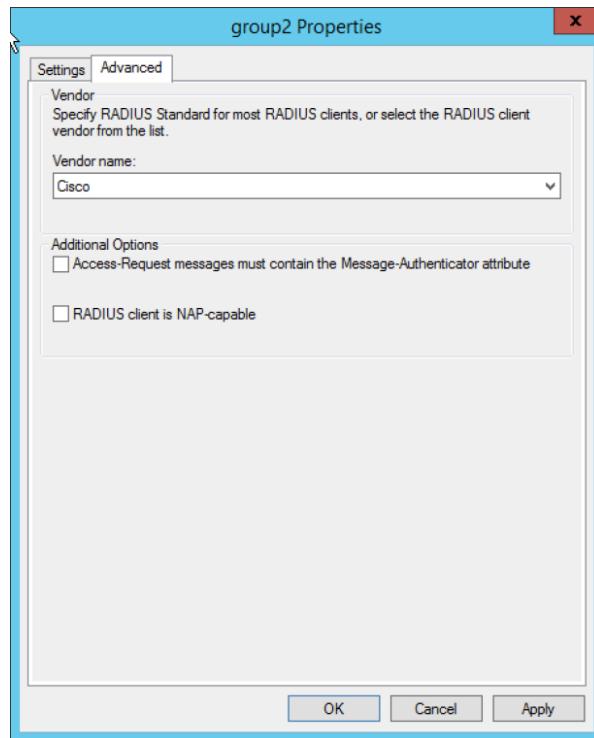


Figure 207: Selecting Cisco as the vendor name

**Step 22:** The Radius Client with friendly name **group2** is successfully created.

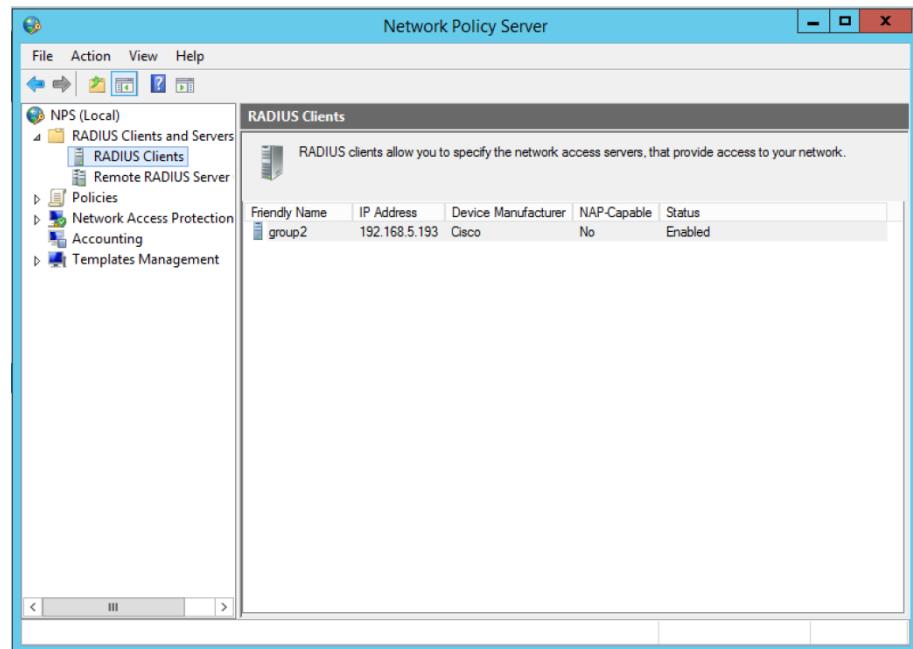


Figure 208: Complete creating a Radius Client

**Step 23:** Expanding the Policy at the left column and right-click on the **Connection Request Policies**. Then, select **New**.

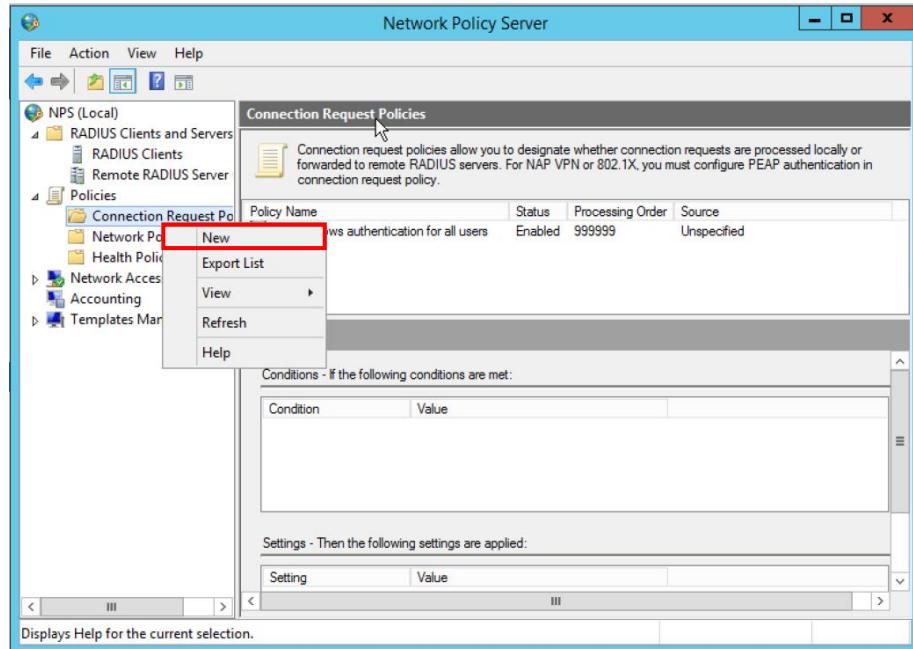


Figure 209: Creating a new Connection Request Policy

**Step 24:** Fill in the policy name and choose **Unspecified** as type of network access server. Then, click **Next**.

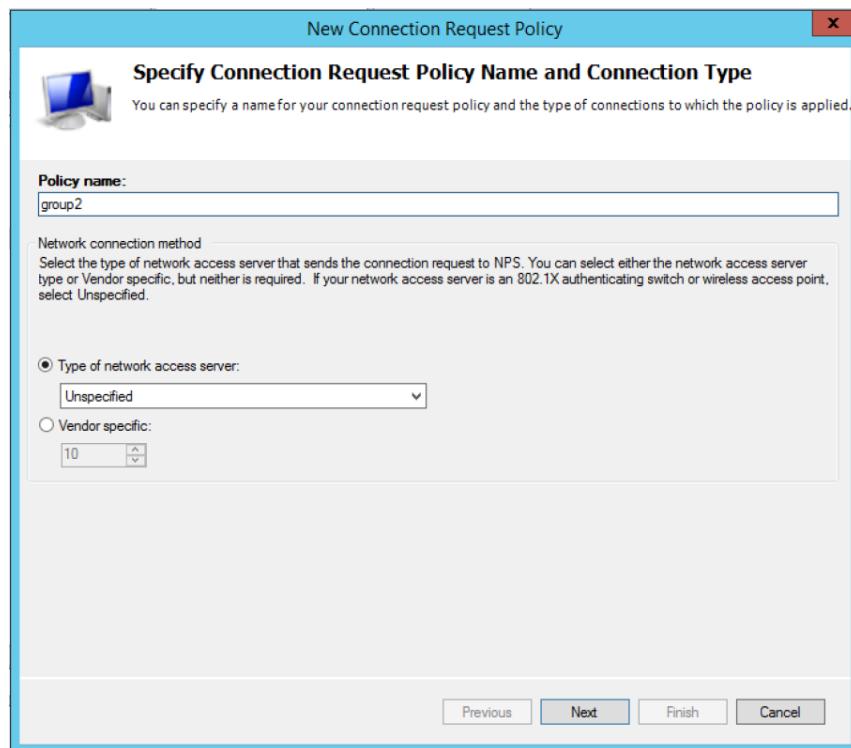


Figure 210: Filling in policy name

**Step 25:** Select **Client Friendly Name** and click **Add**.

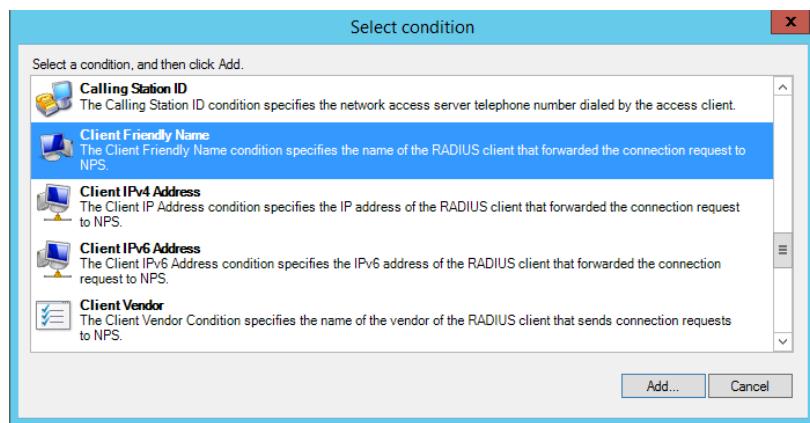


Figure 211: Selecting a condition

**Step 26:** Fill in the **Client Friendly Name**.

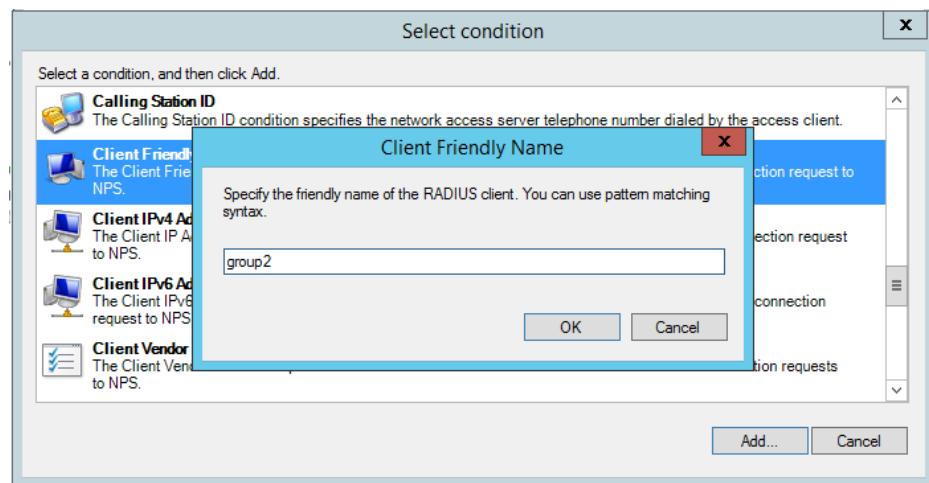


Figure 212: Filling in Client Friendly Name

**Step 27:** Use the default settings and click **Next**.

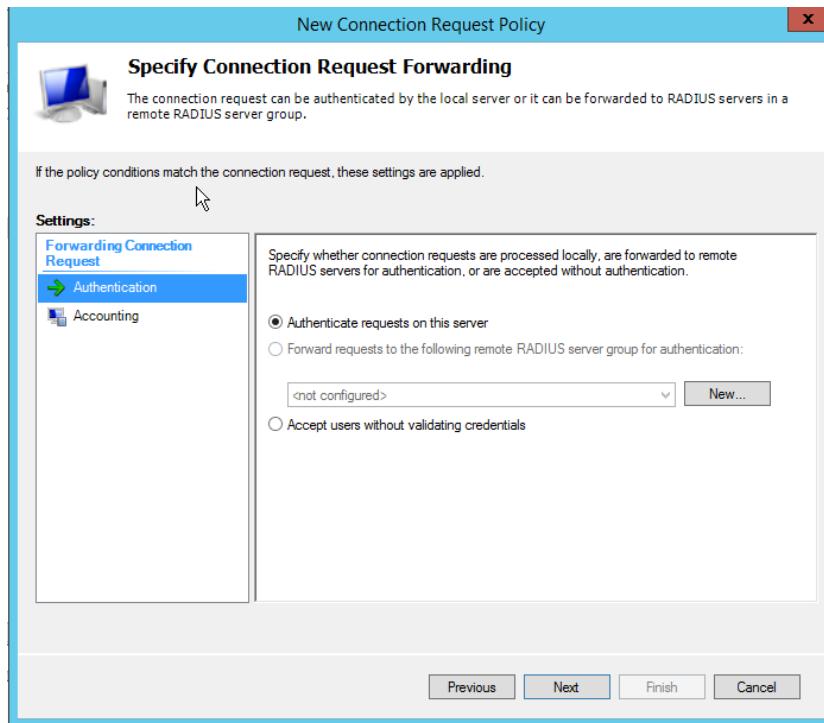


Figure 213: Authentication setting of Specify Connection Request Forwarding

**Step 28:** Click **Next** to proceed with the default settings.

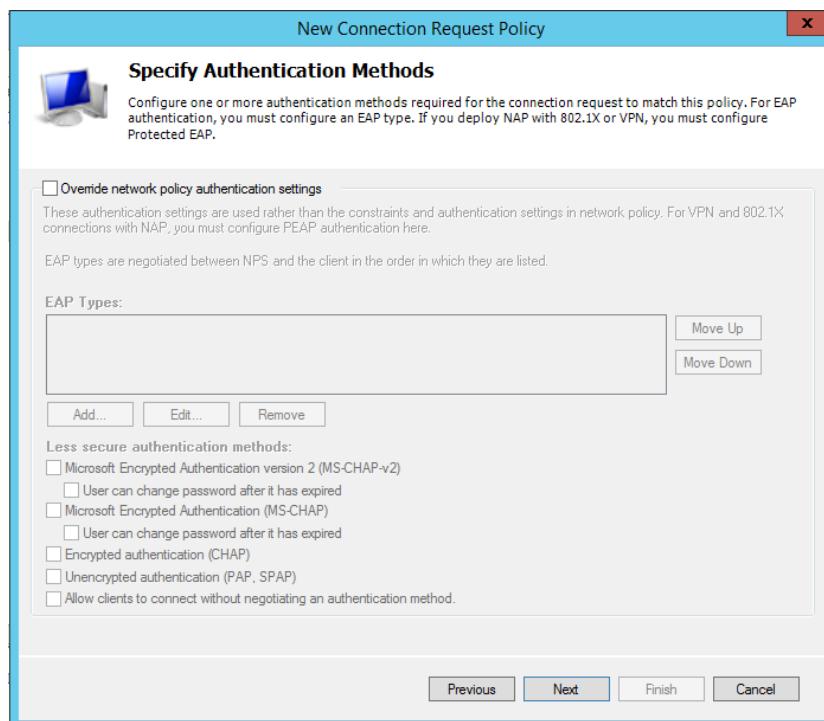
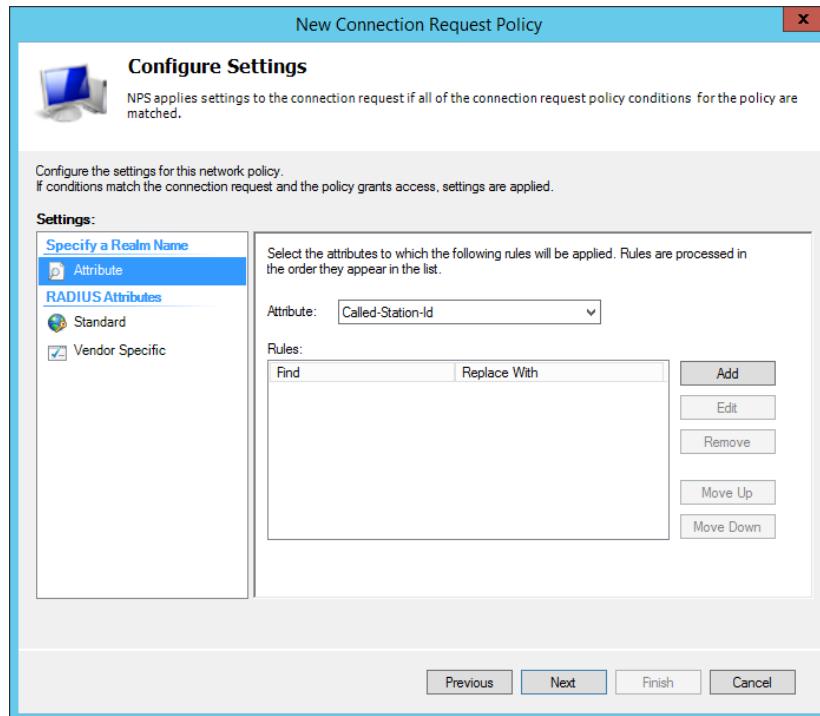


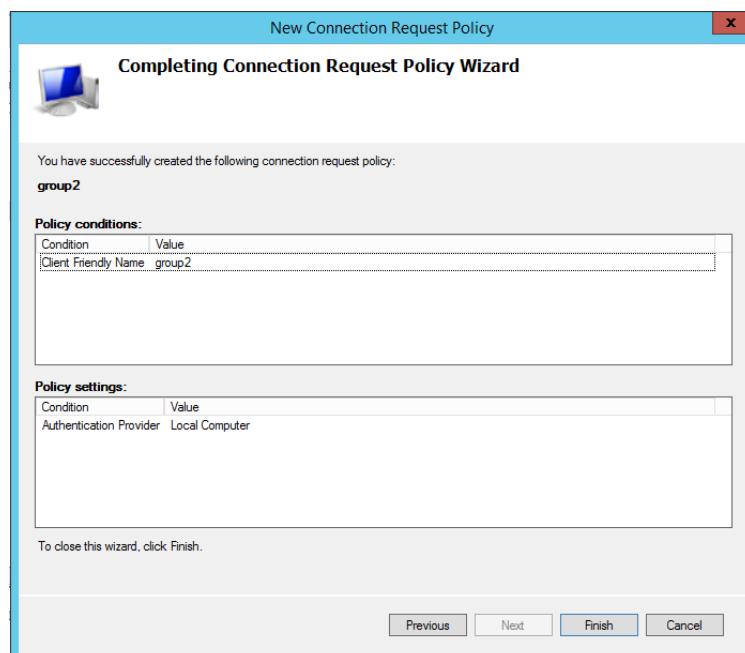
Figure 214: Continue with default setting

**Step 29:** Click **Next** to proceed with the default settings.



*Figure 215: Continue with default setting*

**Step 30:** Click **Finish** on the window that shows the overview of the connection request policy to complete the process.



*Figure 216: Overview of the connection request policy*

**Step 31:** The Connection Request Policy is successfully created.

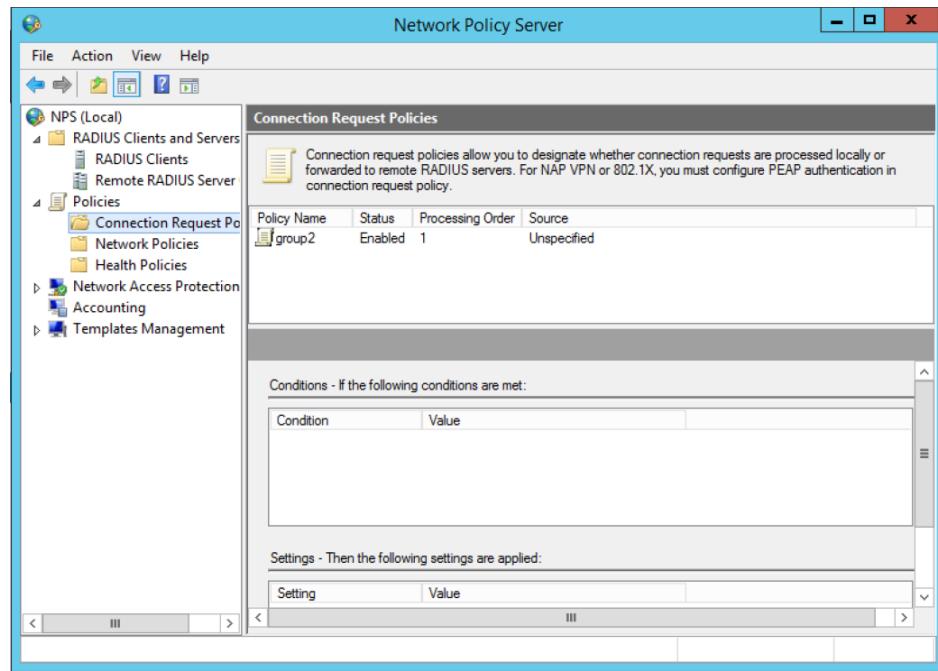


Figure 217: Successfully create Connection Request Policy

**Step 32:** Right click on the Network Policy and select New.

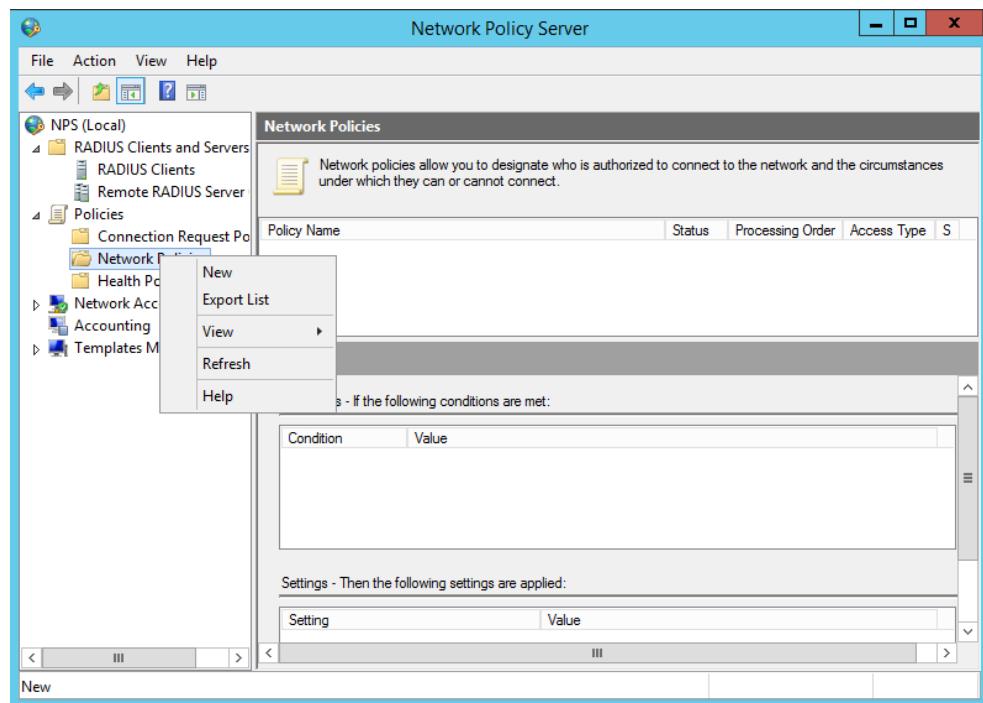


Figure 218: Creating Network Policy

**Step 33:** Specify the name of the policy that will be created and choose **Unspecified** as type of network access server. Then, click **Next**.

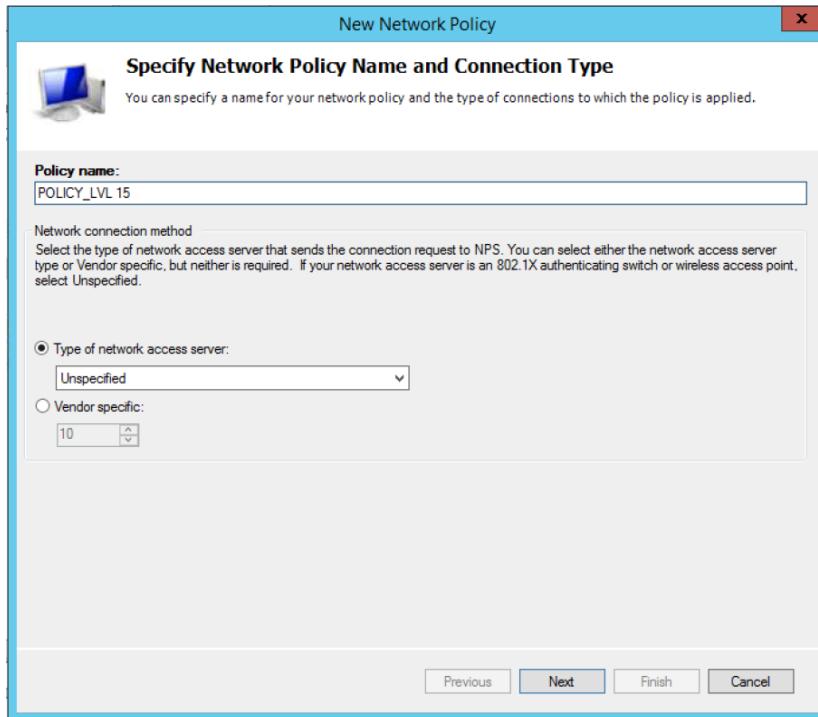


Figure 219: Filling in Network Policy name

**Step 34:** Specify the new condition for the policy by clicking **Add**.

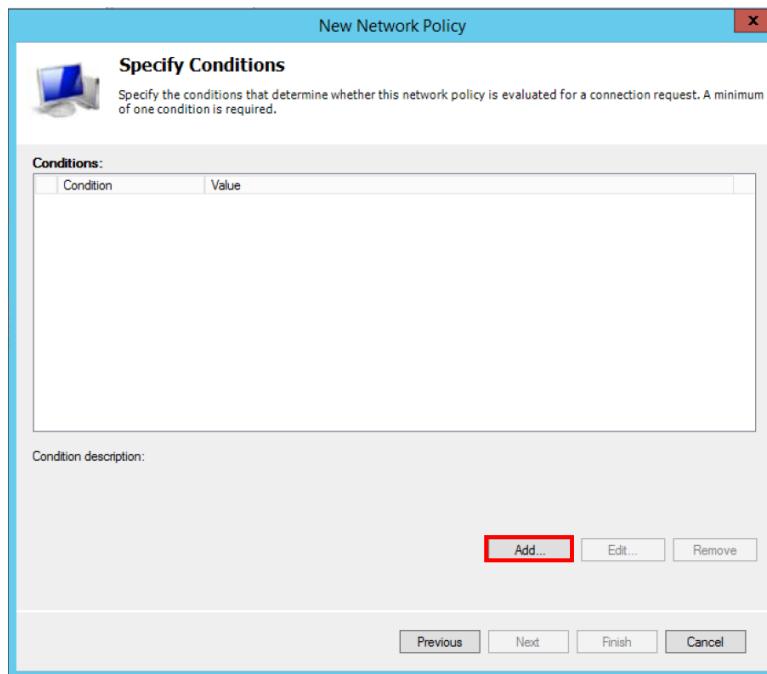


Figure 220: Adding a new condition

**Step 35:** Select the condition that will be used. Choose **User Group** and click **Add** since there are created user and group before this.

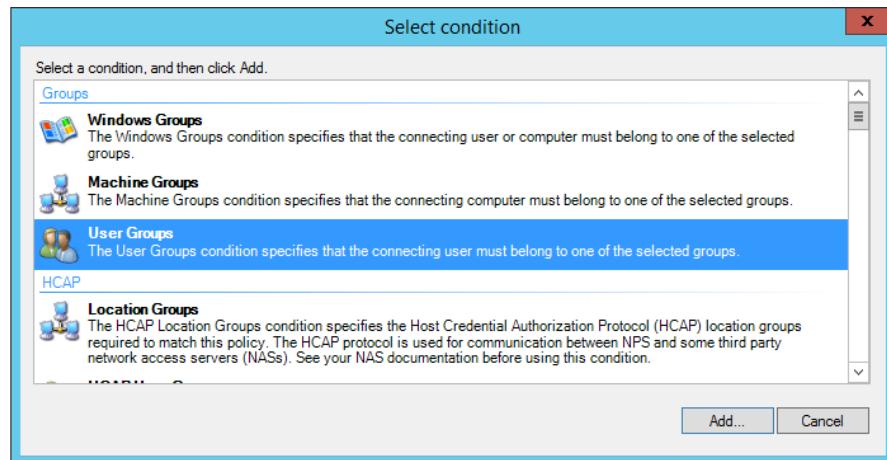


Figure 221: Selecting a condition

**Step 36:** Click **Add Groups** again.

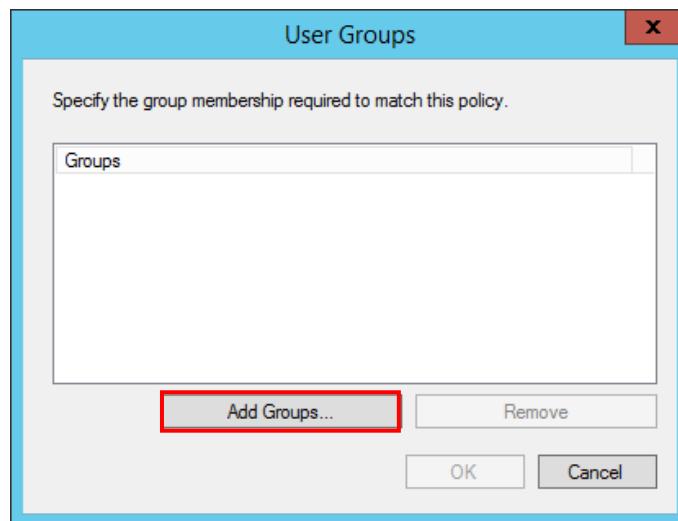


Figure 222: Adding user groups

**Step 37:** Type in group name in the text area provided. Click **Check Names** to make sure the group already created.

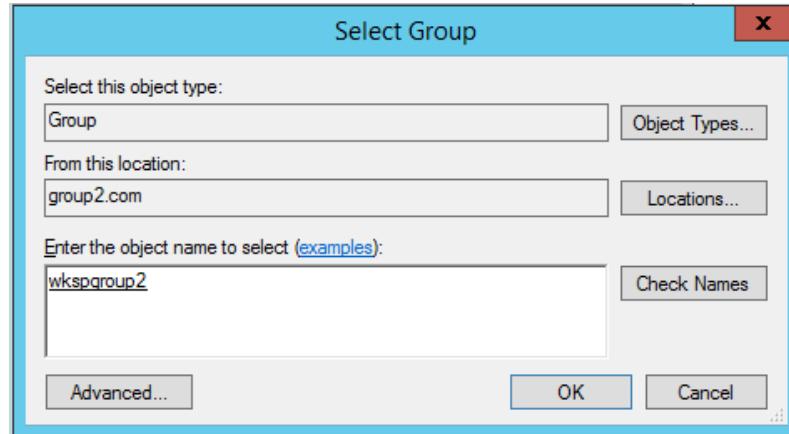


Figure 223: Selecting group

**Step 38:** There is a condition in the list after adding the group. Then, click **Next**.

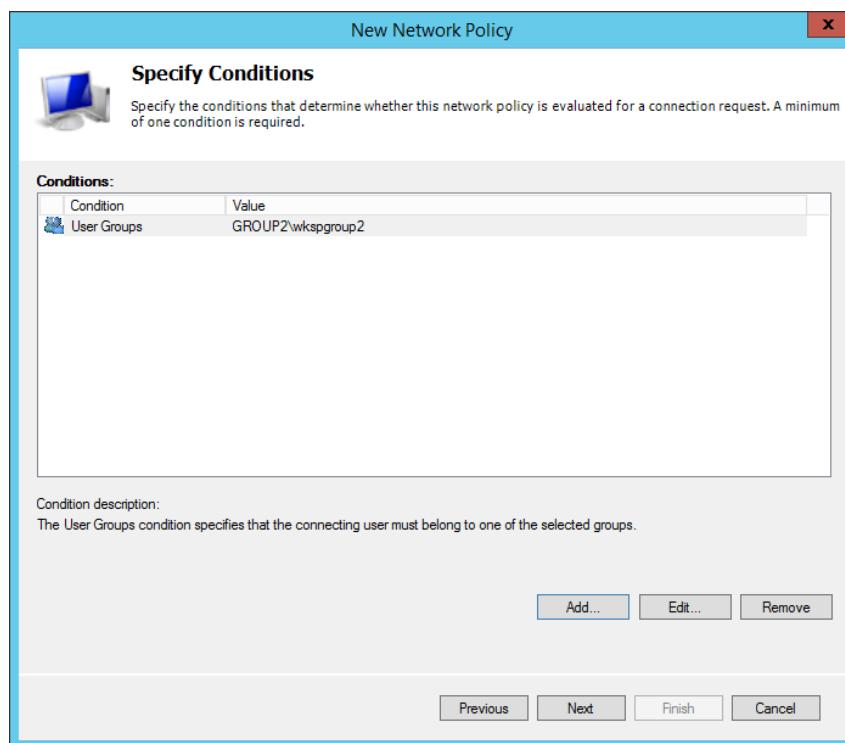


Figure 224: Successfully adding a condition

**Step 39:** Select **Access Granted** for specify Access permission. Then, click **Next**.

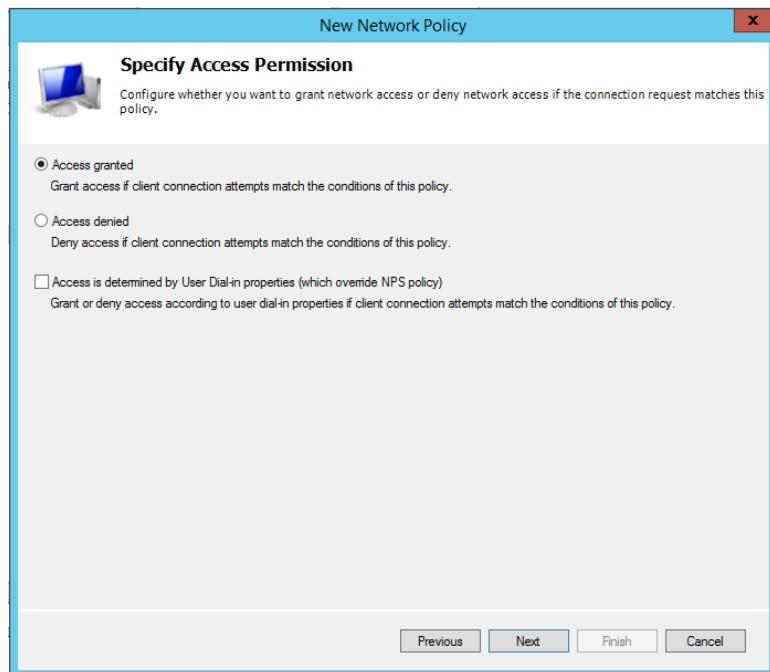


Figure 225: Selecting Access granted

**Step 40:** In the Configure Authentication Methods, tick all the authentication method. Then, click **Next**.

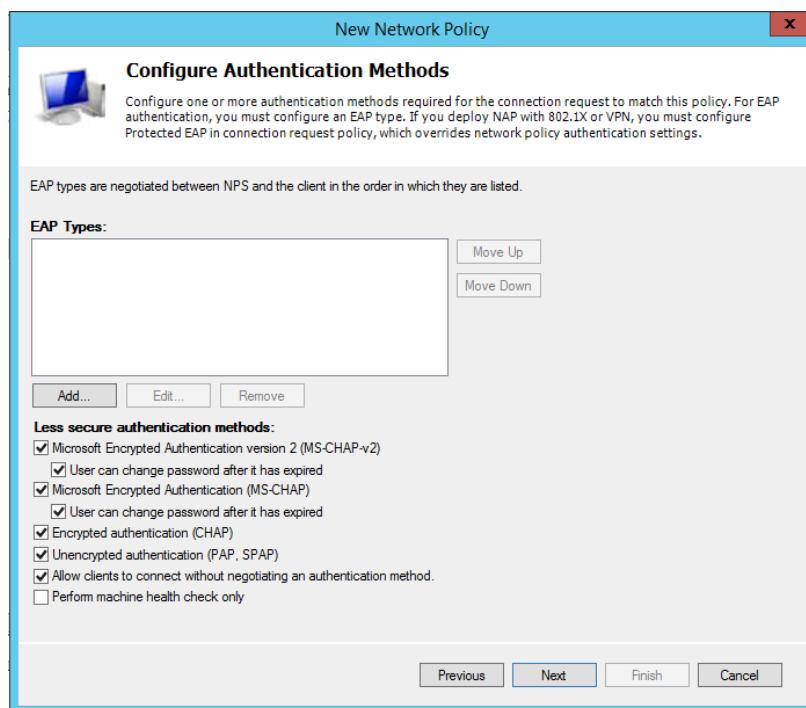


Figure 226: Selecting less secure authentication methods

**Step 41:** Click **Next** on the configure constrain window as there is no constrain required in this project.

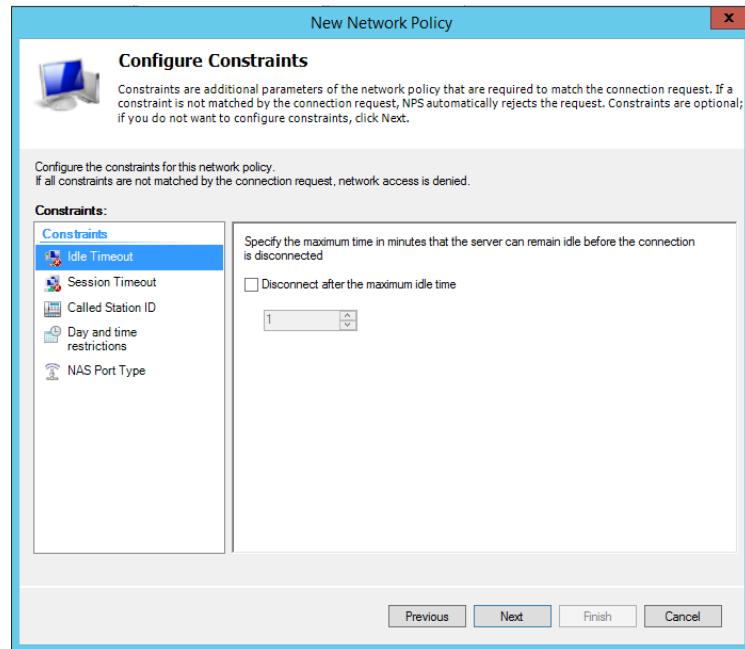


Figure 227: Continue with default setting

**Step 42:** At Standard Attribute, delete the Framed-Protocol PPP.

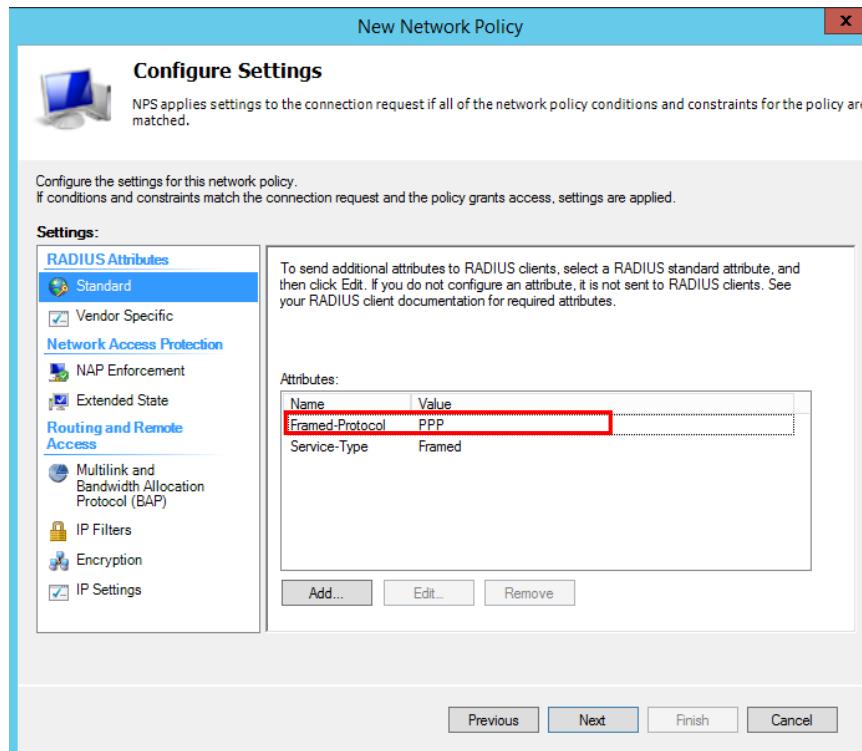


Figure 228: Deleting Framed-Protocol PPP at Standard attribute

**Step 43:** Click the **Service-Type** and select **Edit**.

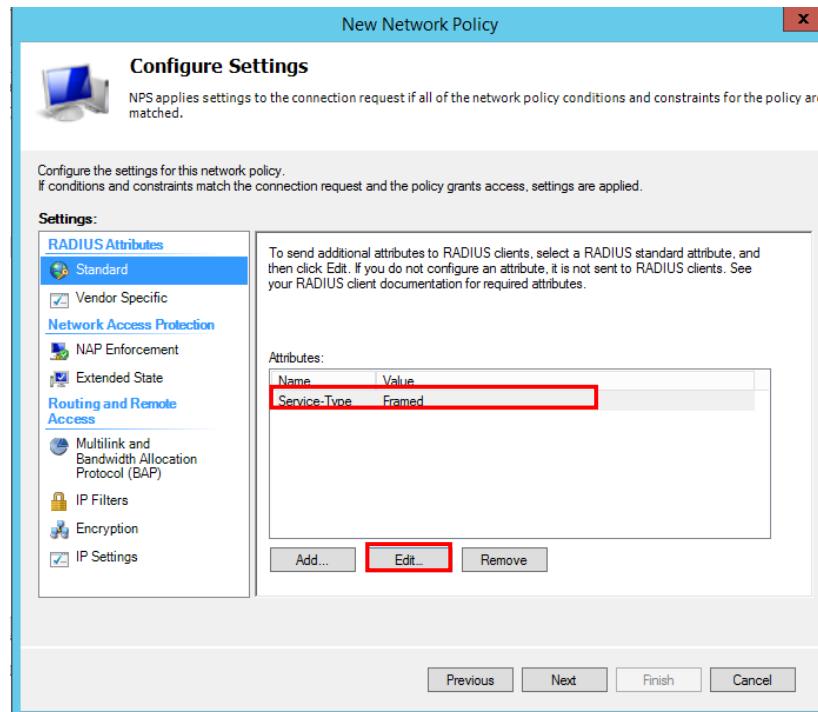


Figure 229: Editing Service-Type on Standard attribute

**Step 44:** In the attribute information, select **Others** and select **Login** which will be the value used by the server to pass to the RADIUS client.

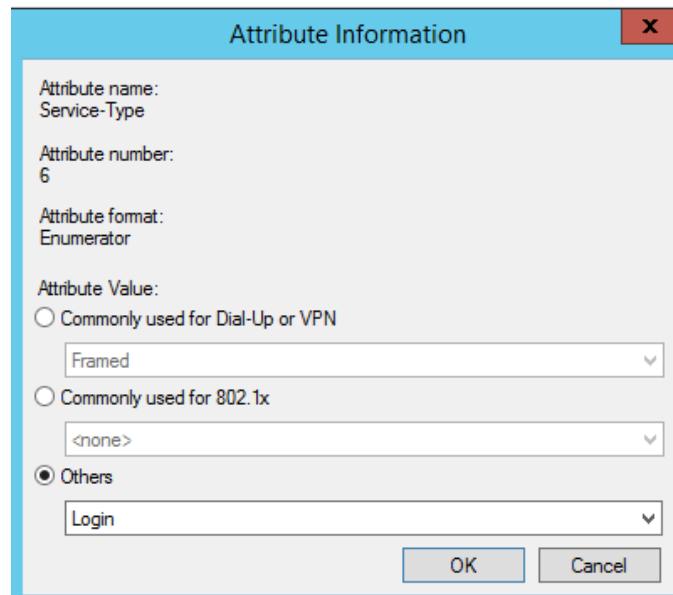


Figure 230: Select Login at Attribute information

**Step 45:** Go to **Vendor Specific** at the left column of the configure settings. Then, click Add.

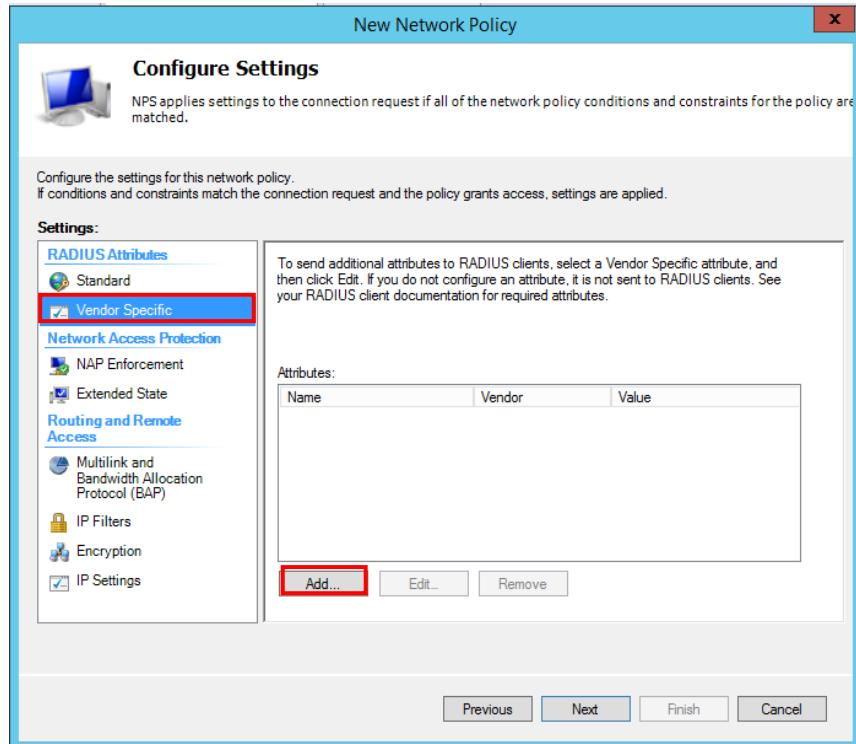


Figure 231: Adding Vendor Specification

**Step 46:** Choose **Cisco** at the **Vendor** drop down and select **Cisco-AV-Pair** at **Attributes** to select Vendor Specific RADIUS Server. Then, click **Add**.

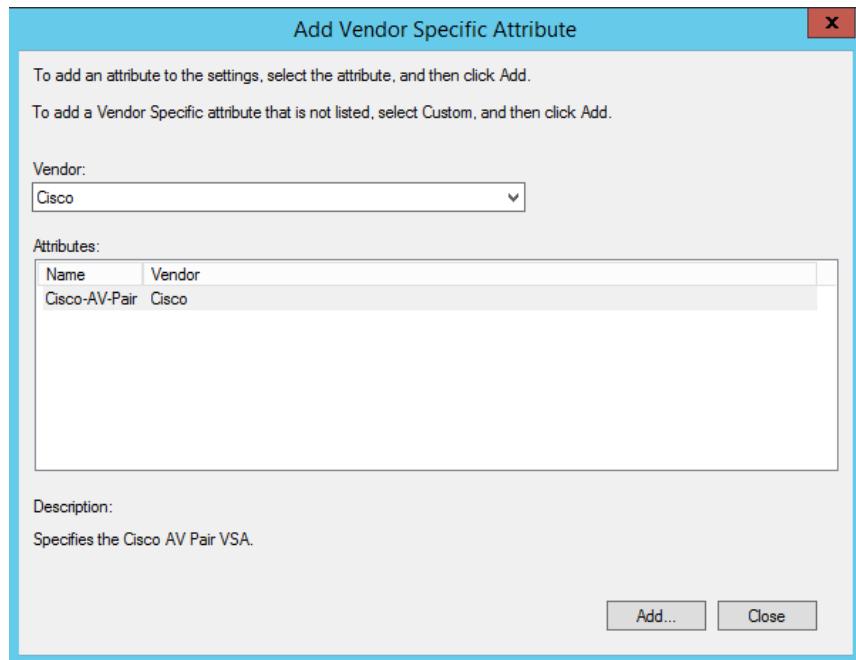


Figure 232: Adding Vendor specific Attribute

**Step 47:** Click **Add** on the **Attribute Information** window.

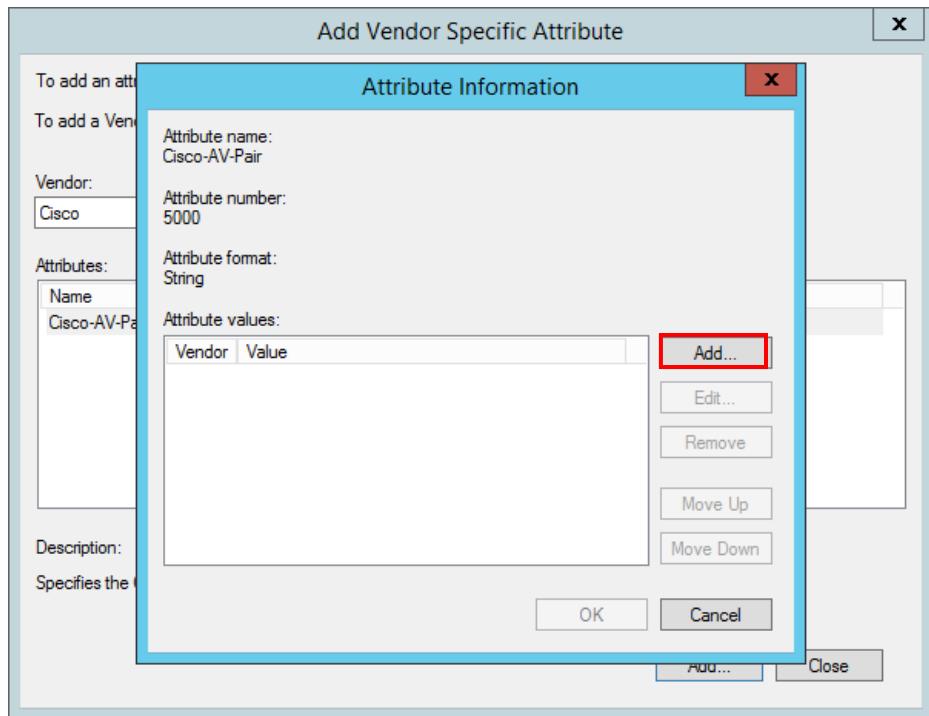


Figure 233: Adding Vendor Attribute information

By default, there are three privilege levels on the router.

- privilege level 1 = non-privileged (prompt is router>), the default level for logging in
- privilege level 15 = privileged (prompt is router#), the level after going into enable mode
- privilege level 0 = seldom used, but includes 5 commands: disable, enable, exit, help, and logout

**Step 48:** Type ‘shell:priv-lvl=15’ as the attribute value and then click OK.

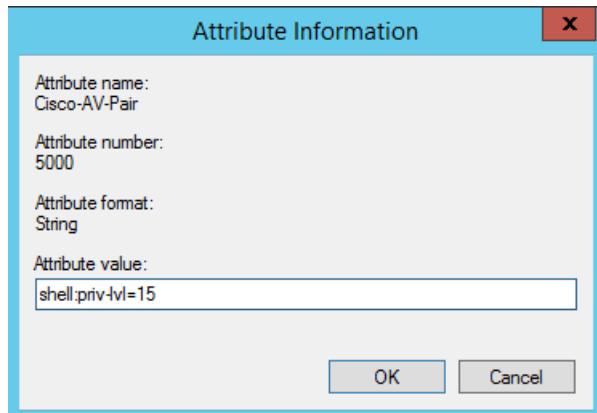


Figure 234: Filling in Vendor Specification

**Step 49:** Click **Finish** on the window that shows the overview of the new network policy to complete the process.

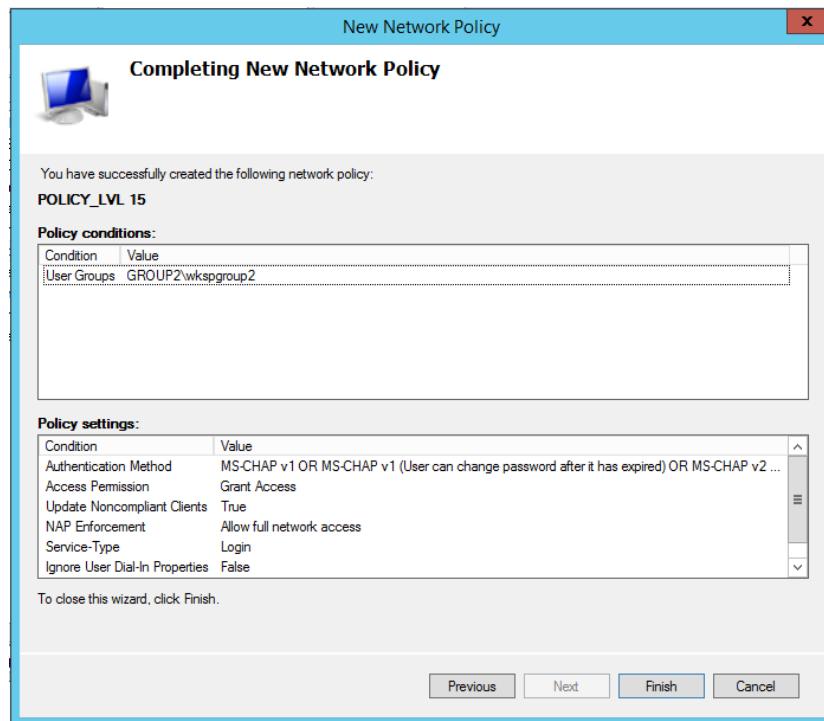


Figure 235: Overview of a New Network Policy

**Step 50:** The new network policy is successfully created.

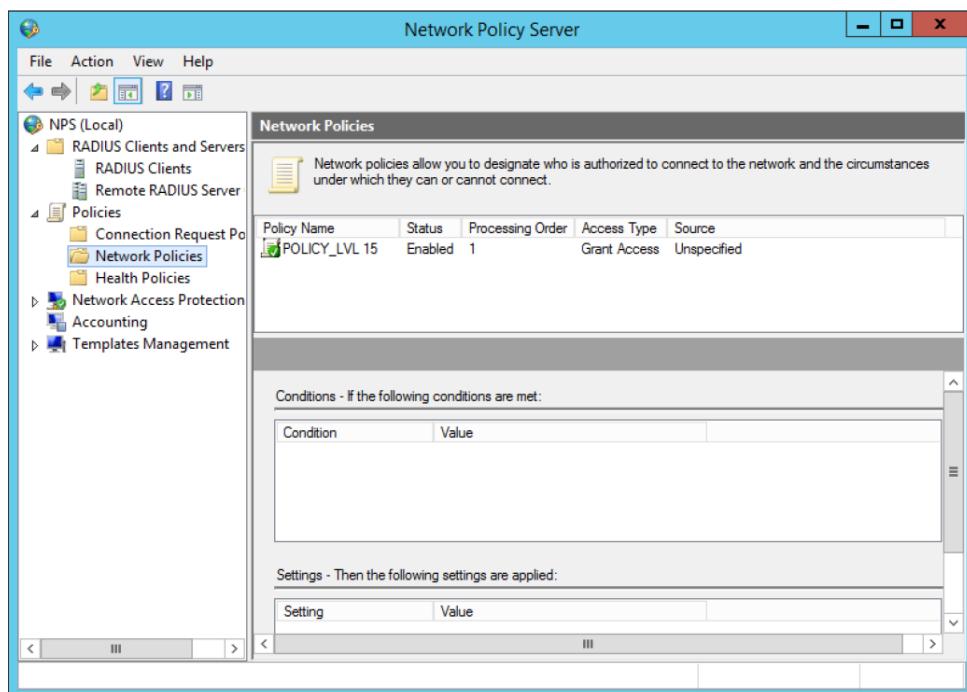


Figure 236: Successful create a New Network Policy

**Step 51:** Go to the Accounting tab, click on **Configure Accounting**.

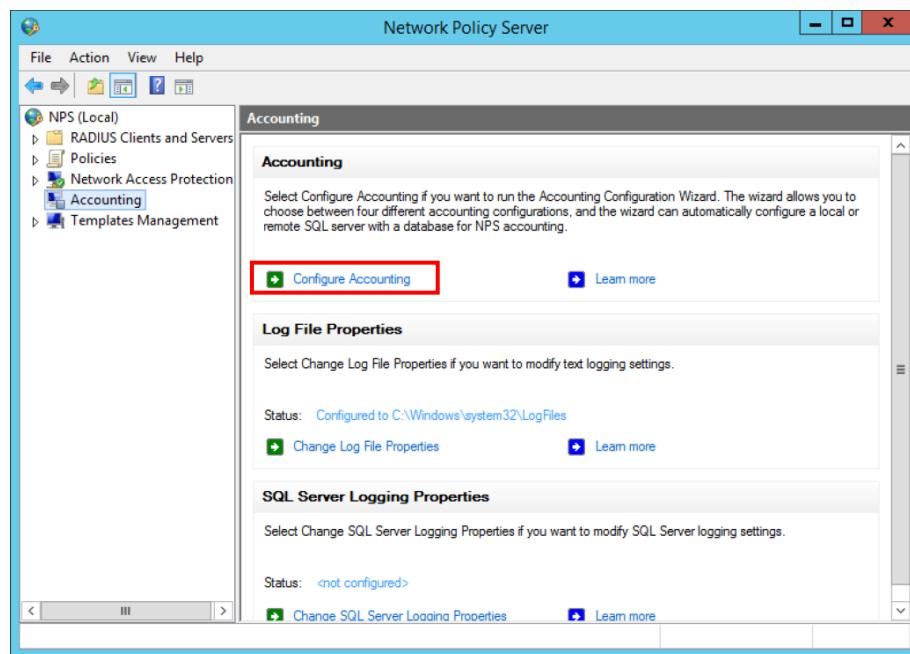


Figure 237: Configure Accounting in Network Policy Server

**Step 52:** Click **Next** on the Introduction page of the **Accounting Configuration Wizard**.

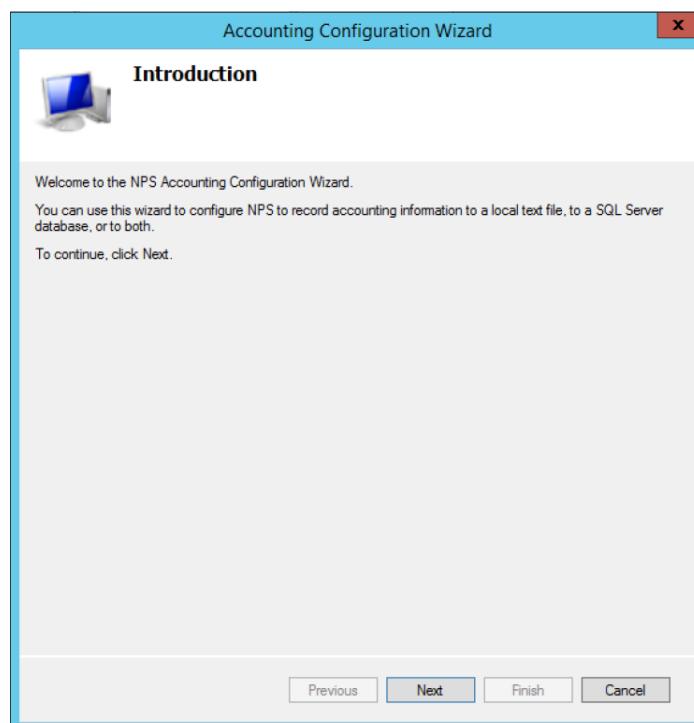


Figure 238: Introduction in Accounting configuration

**Step 53:** Tick **Log to a text file on the local computer** when select Accounting Options. Then, click next.

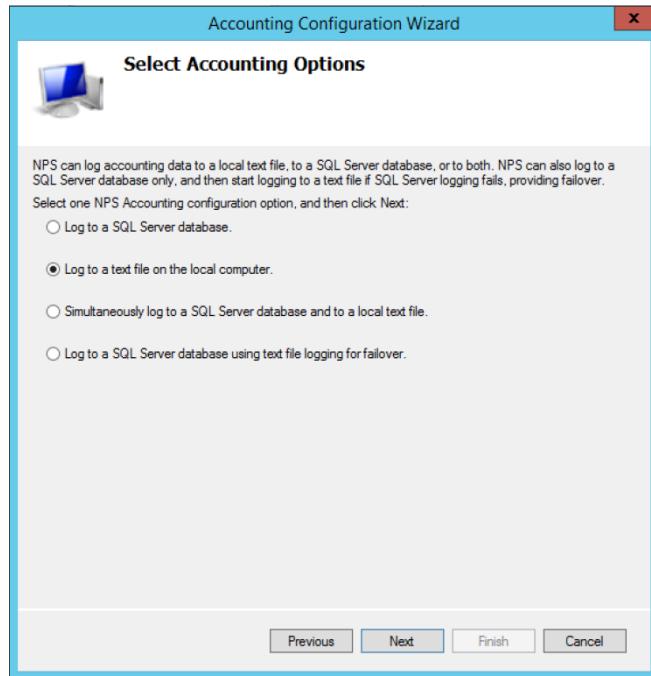


Figure 239: Select Accounting option

**Step 54:** Pick all the option for Logging Information. Then, specify a location for the log file. Tick the options to discard connection requests if logging fails. Then, click **Next**.

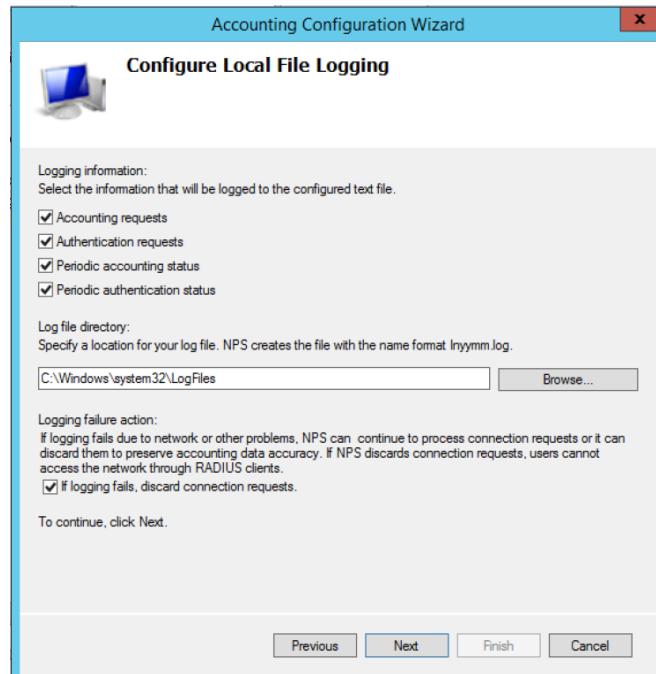


Figure 240: Configure file logging

**Step 55:** Click **Next** on the **Summary** page about Accounting Configuration.

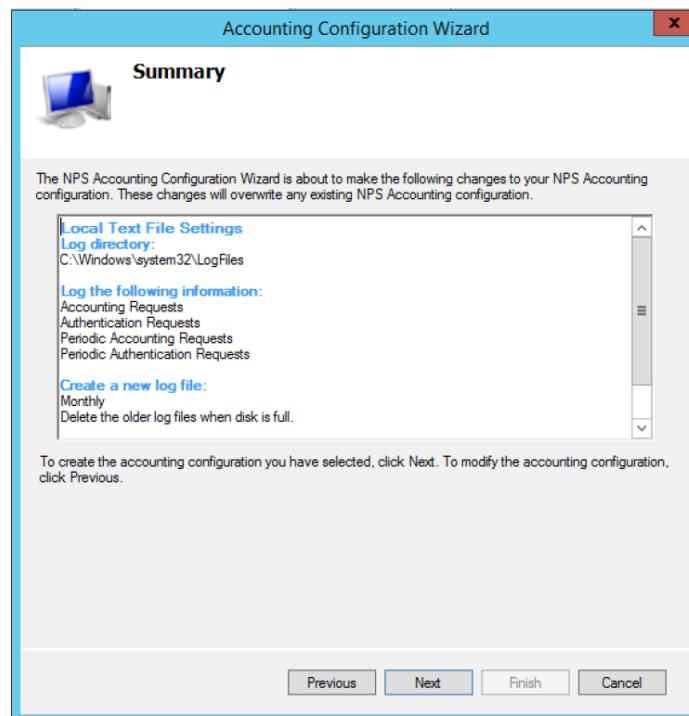


Figure 241: Summary page for Accounting Configuration

**Step 56:** Click **Close** on the Conclusion page.

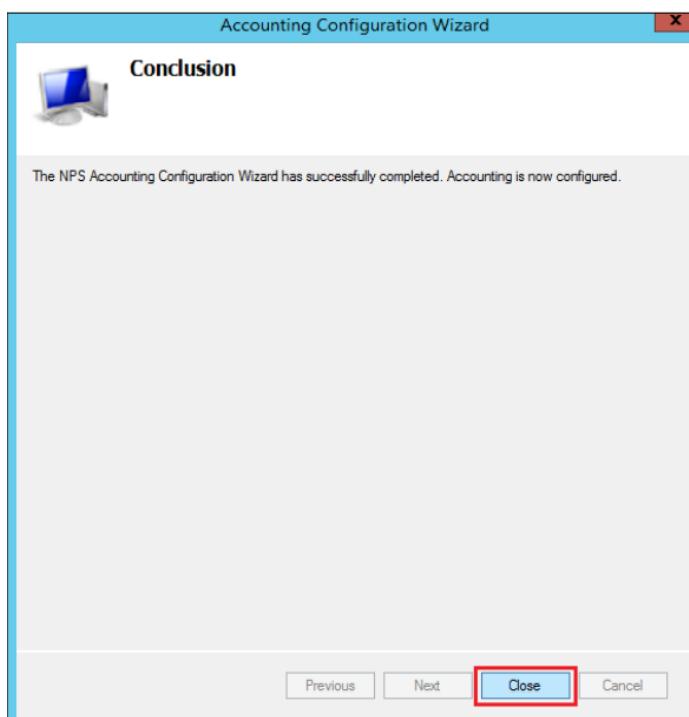
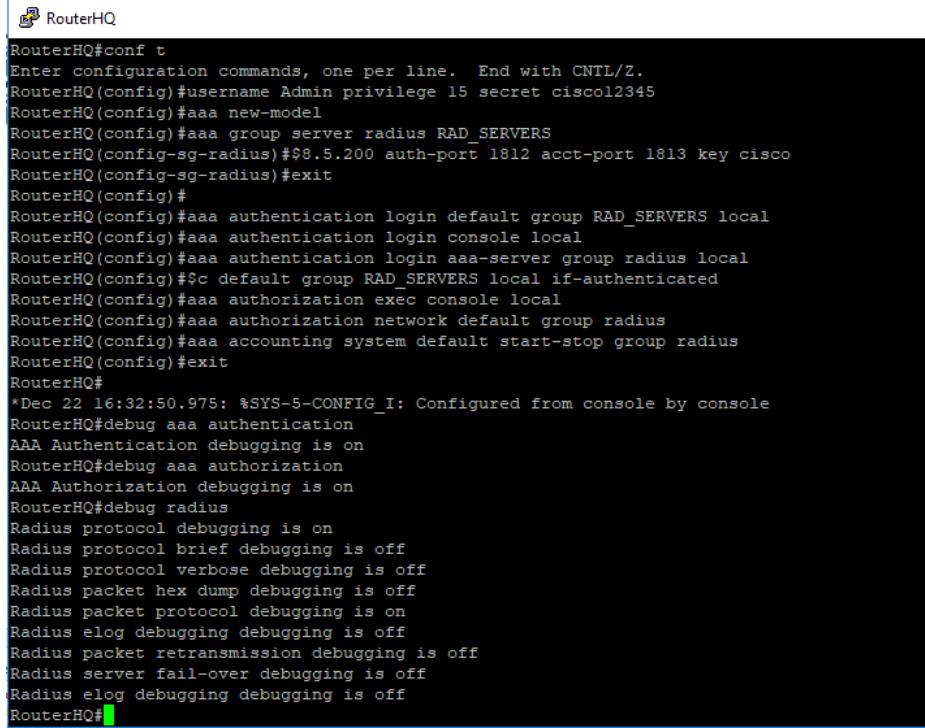


Figure 242: Conclusion Page for Accounting Configuration

**Step 57:** Open the console of RouterHQ router and then enter this command to configure authentication and authorization as below:



```
RouterHQ#conf t
Enter configuration commands, one per line. End with CNTL/Z.
RouterHQ(config)#username Admin privilege 15 secret cisco12345
RouterHQ(config)#aaa new-model
RouterHQ(config)#aaa group server radius RAD_SERVERS
RouterHQ(config-sg-radius)#$8.5.200 auth-port 1812 acct-port 1813 key cisco
RouterHQ(config-sg-radius)#exit
RouterHQ(config)#
RouterHQ(config)#aaa authentication login default group RAD_SERVERS local
RouterHQ(config)#aaa authentication login console local
RouterHQ(config)#aaa authentication login aaa-server group radius local
RouterHQ(config)#{<c> default group RAD_SERVERS local if-authenticated
RouterHQ(config)#aaa authorization exec console local
RouterHQ(config)#aaa authorization network default group radius
RouterHQ(config)#aaa accounting system default start-stop group radius
RouterHQ(config)#exit
RouterHQ#
*Dec 22 16:32:50.975: %SYS-5-CONFIG_I: Configured from console by console
RouterHQ#debug aaa authentication
AAA Authentication debugging is on
RouterHQ#debug aaa authorization
AAA Authorization debugging is on
RouterHQ#debug radius
Radius protocol debugging is on
Radius protocol brief debugging is off
Radius protocol verbose debugging is off
Radius packet hex dump debugging is off
Radius packet protocol debugging is on
Radius elog debugging debugging is off
Radius packet retransmission debugging is off
Radius server fail-over debugging is off
Radius elog debugging debugging is off
RouterHQ#
```

Figure 243: Configuration in putty for aaa new model, Authentication & Authorization

**Step 58:** Exit **enable** mode. Then, login using the username and password of the member under group wkspgroup2. After that, type in command to configure for accounting as below.



```
Username: ziging
Password:

RouterHQ#conf t
Enter configuration commands, one per line. End with CNTL/Z.
RouterHQ(config)#aaa accounting system default start-stop group radius
RouterHQ(config)#aaa group server radius RAD_SERVER
RouterHQ(config-sg-radius)#server name SERVER1
RouterHQ(config-sg-radius)#server name SERVER2
RouterHQ(config-sg-radius)#exit
RouterHQ(config)#radius server SERVER1
RouterHQ(config-radius-server)#key cisco
RouterHQ(config-radius-server)#exit
Warning: Address not yet configured.
RouterHQ(config)#$2.168.5.200 auth-port 1645 acct-port 1646 key cisco
  Warning: The CLI will be deprecated soon
  'radius-server host 192.168.5.200 auth-port 1645 acct-port 1646 key cisco'
  Please move to 'radius server <name>' CLI.
RouterHQ(config)#radius-server host 192.168.5.200 key cisco
```

Figure 244: Configuration in putty for Accounting

### 5.3.11 VLAN & PORT SECURITY

#### VLAN Security

VLAN Security is to assign different VLAN to ensure there is no communication between VLAN. Besides, when attacker attack VLAN, it will prevent further damage to another VLAN. Another function of VLAN security is switch all the unused port to a new VLAN and change the status to suspend in other to blocked unauthorized personal to access to the network. A suspended VLAN will not allow any traffic being sending in or out.

Create a new VLAN and name it.

```
SwitchHQ(config)#vlan 15
SwitchHQ(config-vlan)#name unusedport
SwitchHQ(config-vlan)#int range gi1/0 -3, gi2/0 -1
SwitchHQ(config-if-range)#
SwitchHQ(config-if-range)#
SwitchHQ(config-if-range)#switchport mode access
SwitchHQ(config-if-range)#switchport access vlan 15
SwitchHQ(config-if-range)#ex
```

Figure 245: Assign Port to VLAN

Go to VLAN 15 and state it as suspends.

```
SwitchHQ(config)#vlan 15
SwitchHQ(config-vlan)#state suspend
SwitchHQ(config-vlan)#ex
```

Figure 246: Change status

```
SwitchHQ#sh vlan br

VLAN Name                               Status      Ports
---- -----
1   default                             active
10  vlan_server                         active     Gi0/1, Gi0/2, Gi0/3
15  unusedport                          suspended  Gi1/0, Gi1/1, Gi1/2, Gi1/3
                                         Gi2/0, Gi2/1
20  vlan_client                         active
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
SwitchHQ#
```

Figure 247: Show VLAN

## **Port Security**

Run command *show port-security* to check if there are any port have been configured.

Use command below to secure port gi0/1, gi0/2 by using command switchport port-security mac-address sticky.

```
SwitchHQ(config)#int gi0/1
SwitchHQ(config-if)#switchport host
switchport mode will be set to access
spanning-tree portfast will be enabled
channel group will be disabled

SwitchHQ(config-if)#switchport port-security
SwitchHQ(config-if)#switchport port-security maximum 1
SwitchHQ(config-if)#switchport port-security violation shutdown
SwitchHQ(config-if)#switchport port-security mac-address sticky
SwitchHQ(config-if) #
```

Figure 248: Configure Port for Windows Server

```
SwitchHQ(config)#int gi0/2
SwitchHQ(config-if)#switchport host
switchport mode will be set to access
spanning-tree portfast will be enabled
channel group will be disabled

SwitchHQ(config-if)#switchport port-security maximum 1
SwitchHQ(config-if)#switchport port-security violation shutdown
SwitchHQ(config-if)#switchport port-security mac-address sticky
```

Figure 249: Configure Port for Ubuntu Server

### 5.3.12 IDS WITH PORT MIRRORING

#### Part A: Installation Snort

First, we need to install all the tools required for building software

```
root@lubuntugrp2:~# sudo apt-get install build-essential  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
The following packages were automatically installed and are no longer required
```

Figure 250: Install all tools

Install all Snort pre-requisites that are available from the Ubuntu repositories.

```
root@lubuntugrp2:~# sudo apt-get install -y libcap-dev libpcre3-dev libdumbnet  
-dev  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
The following packages were automatically installed and are no longer required
```

Figure 251: Install all Installing libpcre3-dev

```
root@lubuntugrp2:~# sudo apt-get install -y zlib1g-dev liblzma-dev openssl lib  
ssl-dev  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done
```

Figure 252: Installing zlib1g-dev

Install *Snort DAQ Prerequisites*. *Bison* and *flex* are the requirement for Snort DAQ installation.

```
root@lubuntugrp2:~# sudo apt-get install flex bison  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
The following packages were automatically installed and are no longer required
```

Figure 253: Installing bison flex

Create a separate directory in which will install tar packages of snort and Snort DAQ. Then change working directory to newly created directory.

```
root@lubuntugrp2:~# mkdir ~snort_src  
root@lubuntugrp2:~# cd ~snort_src
```

Figure 254: Make and change directory

Download and install latest version of DAQ. Snort use something call Data Acquisition library (DAQ) to make abstract calls to packet capture libraries. Download the latest DAQ source package from the Snort website with wget command.

```
root@lubuntugrp2:~/snort_src# wget https://www.snort.org/downloads/snort/daq-2.0.7.tar.gz
--2020-12-13 23:52:58--  https://www.snort.org/downloads/snort/daq-2.0.7.tar.gz
Resolving www.snort.org (www.snort.org)... 104.18.139.9, 104.18.138.9, 2606:4700::6812:8b09, ...
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/000/015/642/original/daq-2.0.7.tar.gz?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Am
```

Figure 255: Download DAQ

After downloaded it, type command “tar -xvzf daq2.0.7.tar.gz” to extract the file.

```
root@lubuntugrp2:~/snort_src# tar xvzf daq-2.0.7.tar.gz
daq-2.0.7/
daq-2.0.7/config.h.in
```

Figure 256: Extract file

Change into the new directory with command “cd daq-2.0.7”. Next, type command “./configure”, “make” and “sudo make install” to compile the program and then finally install DAQ.

```
root@lubuntugrp2:~/snort# cd daq-2.0.7
root@lubuntugrp2:~/snort/daq-2.0.7# ./configure && make && sudo make install
```

Figure 257: Configure, make & make install command

Installing Snort. Change back to download folder. Then download Snort source code with wget, use the latest version number from Snort website.

```
root@lubuntugrp2:~/snort/daq-2.0.7# wget https://www.snort.org/downloads/snort/snort-2.9.17.tar.gz
--2020-12-31 23:15:38--  https://www.snort.org/downloads/snort/snort-2.9.17.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.
```

Figure 258: Installing Snort latest version

Once install is complete, extract the source file.

```
root@lubuntugrp2: ~/snort_src# tar xvzf snort -2.9.17.tar.gz  
snort-2.9.17/
```

Figure 259: Extract file

Change into the new directory. Then configure the installation with sourcefire mode enabled.

```
root@lubuntugrp2:~/snort# cd snort-2.9.17  
root@lubuntugrp2:~/snort/snort-2.9.17# ./configure --enable-sourcefire && make  
&& sudo make install
```

Figure 260: Enabling sourcefire

## Part B: Configure Snort

It will need to setup Snort for our system, includes editing some configuration files, downloading rules that Snort need to follow and taking Snort for a test run.

Start with updating shared libraries.

```
root@lubuntugrp2:~/snort/snort-2.9.17# sudo ldconfig
```

Figure 261: Updating libraries

Create a Soft Link for Snort binary. Then, to run Snort safely without root access, we should create a new unprivileged user and a new user group for the daemon to run under.

```
root@lubuntugrp2:~/snort/snort-2.9.17# sudo ln -s /usr/local/bin/snort /usr/sbin/snort  
root@lubuntugrp2:~/snort/snort-2.9.17# sudo groupadd snort  
sudo: /etc/sudoers.d is world writable  
groupadd: group 'snort' already exists  
root@lubuntugrp2:~/snort/snort-2.9.17# sudo useradd snort -r -s /sbin/nologin  
-c SNORT_IDS -g snort
```

Figure 262: Creating user and group

Create folder structure to house the snort configuration.

```
root@lubuntugrp2:~/snort/snort-2.9.17# sudo mkdir /etc/snort  
root@lubuntugrp2:~/snort/snort-2.9.17# sudo mkdir /etc/snort/rules  
root@lubuntugrp2:~/snort/snort-2.9.17# sudo mkdir /etc/snort/rules/iplists  
root@lubuntugrp2:~/snort/snort-2.9.17# sudo mkdir /etc/snort/preproc_rules  
root@lubuntugrp2:~/snort/snort-2.9.17# sudo mkdir /usr/local/lib/snort_dynamic  
rules  
root@lubuntugrp2:~/snort/snort-2.9.17# sudo mkdir /var/log/snort
```

Figure 263: Creating folder

Create new files for the white and black lists as well as the local rules.

```
root@lubuntugrp2:~/snort/snort-2.9.17# sudo touch /etc/snort/rules/iplists/black_list.rules
root@lubuntugrp2:~/snort/snort-2.9.17# sudo touch /etc/snort/rules/iplists/white_list.rules
root@lubuntugrp2:~/snort/snort-2.9.17# sudo touch /etc/snort/rules/local.rules
```

Figure 264: Creating folder in rules

Change the permission for new directories.

```
root@lubuntugrp2:~/snort/snort-2.9.17# sudo chmod -R 5775 /etc/snort
sudo: /etc/sudoers.d is world writable
root@lubuntugrp2:~/snort/snort-2.9.17# sudo chmod -R 5775 /var/log/snort
sudo: /etc/sudoers.d is world writable
root@lubuntugrp2:~/snort/snort-2.9.17# sudo chmod -R 5775 /usr/local/lib/snort_dynamicrules
sudo: /etc/sudoers.d is world writable
root@lubuntugrp2:~/snort/snort-2.9.17# sudo chown -R snort:snort /etc/snort
sudo: /etc/sudoers.d is world writable
You have new mail in /var/mail/root
root@lubuntugrp2:~/snort/snort-2.9.17# sudo chown -R snort:snort /var/log/snort
```

Figure 265: Creating list and change permission

Copy the configuration files from the source to our configuration directory.

```
root@lubuntugrp2:~/snort/snort-2.9.17/etc# sudo cp *.conf* /etc/snort
sudo: /etc/sudoers.d is world writable
You have new mail in /var/mail/root
root@lubuntugrp2:~/snort/snort-2.9.17/etc# sudo cp *.map /etc/snort
```

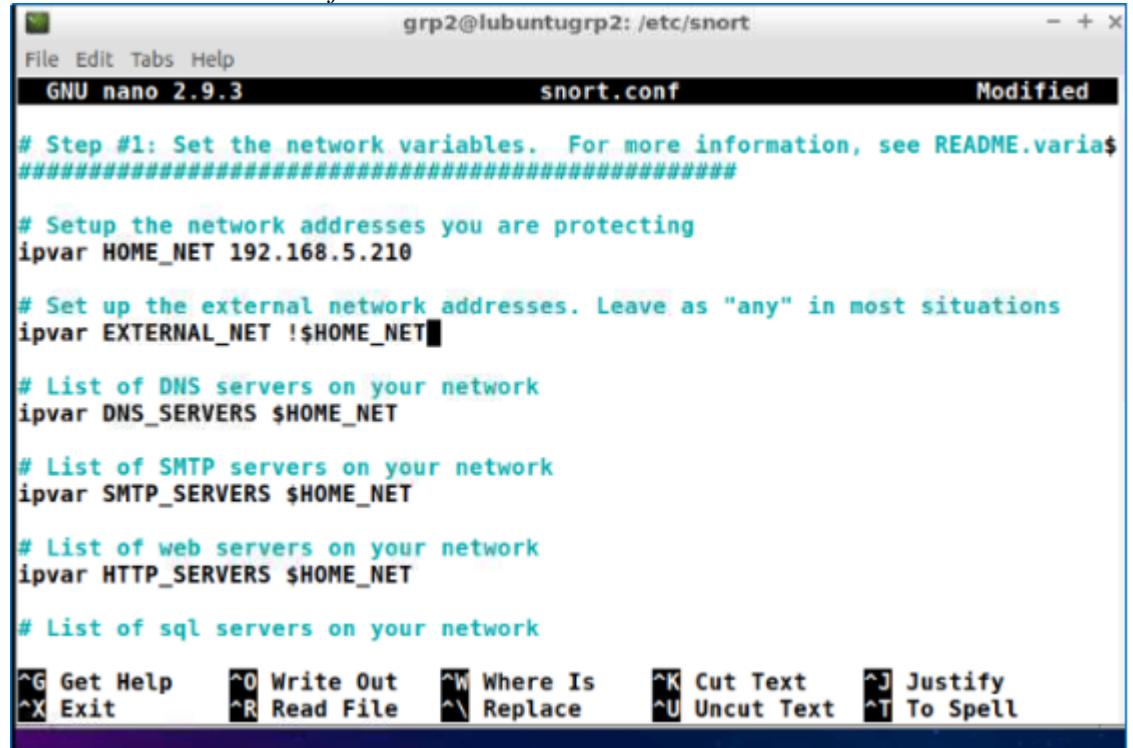
Figure 266: Copying configuration

Then use “snort -V” to verify snort.

```
root@lubuntugrp2:~/snort/snort-2.9.17# snort -V
      _.-> Snort! <*-_
      o"- )~ Version 2.9.17 GRE (Build 199)
      '--- By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
      m
      Copyright (C) 2014-2020 Cisco and/or its affiliates. All rights reserved.
      Copyright (C) 1998-2013 Sourcefire, Inc., et al.
      Using libpcap version 1.8.1
      Using PCRE version: 8.39 2016-06-14
      Using ZLIB version: 1.2.11
```

Figure 267: Verify Snort

Update snort.conf. Edit the snort.conf to modify a few parameters. Type `sudo nano /etc/snort/snort.conf`



```
grp2@lubuntugrp2: /etc/snort
File Edit Tabs Help
GNU nano 2.9.3          snort.conf          Modified

# Step #1: Set the network variables. For more information, see README.varia$#####
#####ipvar HOME_NET 192.168.5.210

# Setup the network addresses you are protecting
ipvar HOME_NET 192.168.5.210

# Set up the external network addresses. Leave as "any" in most situations
ipvar EXTERNAL_NET !$HOME_NET

# List of DNS servers on your network
ipvar DNS_SERVERS $HOME_NET

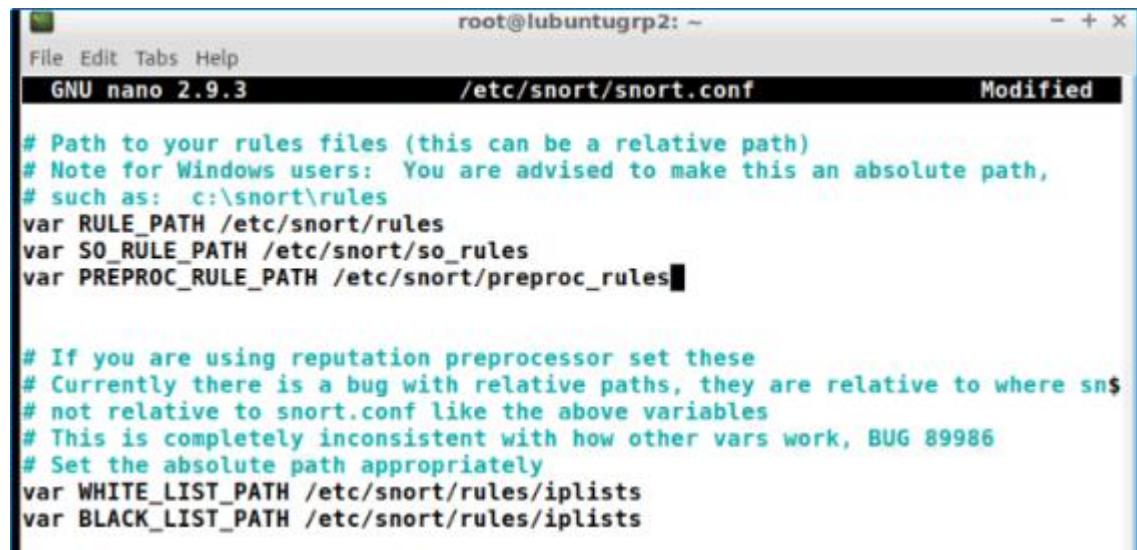
# List of SMTP servers on your network
ipvar SMTP_SERVERS $HOME_NET

# List of web servers on your network
ipvar HTTP_SERVERS $HOME_NET

# List of sql servers on your network

^G Get Help    ^O Write Out   ^W Where Is   ^K Cut Text   ^J Justify
^X Exit        ^R Read File    ^M Replace    ^U Uncut Text  ^T To Spell
```

Figure 268: Protected IP



```
root@lubuntugrp2: ~
File Edit Tabs Help
GNU nano 2.9.3          /etc/snort/snort.conf          Modified

# Path to your rules files (this can be a relative path)
# Note for Windows users: You are advised to make this an absolute path,
# such as: c:\snort\rules
var RULE_PATH /etc/snort/rules
var SO_RULE_PATH /etc/snort/so_rules
var PREPROC_RULE_PATH /etc/snort/preproc_rules

# If you are using reputation preprocessor set these
# Currently there is a bug with relative paths, they are relative to where snort.conf is located
# not relative to snort.conf like the above variables
# This is completely inconsistent with how other vars work, BUG 89986
# Set the absolute path appropriately
var WHITE_LIST_PATH /etc/snort/rules/iplists
var BLACK_LIST_PATH /etc/snort/rules/iplists
```

Figure 269: Modifying path to rules

Scroll down to the bottom of the file and find the list of included rule sets.

Uncomment the output snort to log file.

```
root@lubuntugrp2: ~
File Edit Tabs Help
GNU nano 2.9.3          /etc/snort/snort.conf          Modified

priority whitelist, \
nested_ip inner, \
whitelist $WHITE_LIST_PATH/white_list.rules, \
blacklist $BLACK_LIST_PATH/black_list.rules

#####
# Step #6: Configure output plugins
# For more information, see Snort Manual, Configuring Snort - Output Modules
#####

# unified2
# Recommended for most installs
output unified2: filename merged.log, limit 128, nostamp, mpls_event_types, vs

# Additional configuration for specific types of installs
# output alert_unified2: filename snort.alert, limit 128, nostamp
# output log_unified2: filename snort.log, limit 128, nostamp

# syslog

^G Get Help    ^O Write Out   ^W Where Is    ^K Cut Text    ^J Justify
^X Exit        ^R Read File   ^A Replace     ^U Uncut Text  ^T To Spell
```

Figure 270: Output Snort to log file

```
root@lubuntugrp2: ~
File Edit Tabs Help
GNU nano 2.9.3          /etc/snort/snort.conf          Modified

# Step #7: Customize your rule set
# For more information, see Snort Manual, Writing Snort Rules
#
# NOTE: All categories are enabled in this conf file
#####

# site specific rules
include $RULE_PATH/local.rules
include $RULE_PATH/community.rules

#include $RULE_PATH/app-detect.rules
#include $RULE_PATH/attack-responses.rules
#include $RULE_PATH/backdoor.rules
#include $RULE_PATH/bad-traffic.rules
#include $RULE_PATH/blacklist.rules
#include $RULE_PATH/botnet-cnc.rules
#include $RULE_PATH/browser-chrome.rules
#include $RULE_PATH/browser-firefox.rules

^G Get Help    ^O Write Out   ^W Where Is    ^K Cut Text    ^J Justify
^X Exit        ^R Read File   ^A Replace     ^U Uncut Text  ^T To Spell
```

Figure 271: Uncomment any rules available

After done with the configuration, save the changes and exit. Test the snort.conf. Type sudo snort -T -c /etc/snort/snort.conf to validate Snort Rules. It should get “Snort successfully validated the configuration!”.

```

root@lubuntugrp2: /etc/snort
File Edit Tabs Help
Using PCRE version: 8.39 2016-06-14
Using ZLIB version: 1.2.11

Rules Engine: SF_SNORT_DETECTION_ENGINE Version 3.1 <Build 1>
Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
Preprocessor Object: SF_SIP Version 1.1 <Build 1>
Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Preprocessor Object: SF_DCERPC2 Version 1.0 <Build 3>
Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
Preprocessor Object: SF_GTP Version 1.1 <Build 1>
Preprocessor Object: SF_SSH Version 1.1 <Build 3>
Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>
Preprocessor Object: appid Version 1.1 <Build 5>
Preprocessor Object: SF_SMTP Version 1.1 <Build 9>
Preprocessor Object: SF_S7COMMPLUS Version 1.0 <Build 1>
Preprocessor Object: SF_POP Version 1.0 <Build 1>
Preprocessor Object: SF_SDF Version 1.1 <Build 1>
Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>
Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>

Snort successfully validated the configuration!
Snort exiting
root@lubuntugrp2:/etc/snort#

```

Figure 272: Output testing snort

Creating a custom Snort rule to test Snort. Add custom detection rule alert on incoming ICMP connections to the local.rules -file. Open local rules with

#sudo nano /etc/snort/rules/local.rules.

```

root@lubuntugrp2: /etc/snort
File Edit Tabs Help
GNU nano 2.9.3          /etc/snort/rules/local.rules          Modified
alert icmp any any -> $HOME_NET any (msg:"icmp test"; sid:10000001;
rev:1; classtype:icmp-event;)

```

Figure 273: Inserting rules

We can add any rules using this format:

action protocol source\_ip port\_source -> destination\_ip port\_destination  
(msg:"comment"; sid:unique id values; rev:as rules version number;)

The rules consist of the following parts:

1. Action for traffic matching the rule, alert in this case.
2. Traffic protocol like TCP, UDP or ICMP.
3. Source address and port, simply marked as any to include all addresses and ports.
4. Destination address and port, \$HOME\_NET as declared in the configuration and any for port.

- Some additional bits :
- ✓ log message
  - ✓ unique rules identifier
  - ✓ rule version number
  - ✓ Save the local.rules by ‘ctrl O’ and exit

### Configure Port Mirror

**Step 1:** Type “config t”

**Step 2:** monitor session 1 source interface gi0/0

**Step 3:** monitor session 1 destination interface gi0/3

**Step 4:** Check the source and destination port at monitor session 1. Type “sh monitor session 1” to test port mirror has been set up.

```
Switch#Q#sh monitor session 1
Session 1
-----
Type : Local Session
Source Ports :
    Both : Gi0/0
Destination Ports : Gi0/3
Encapsulation : Native
```

Figure 274: Verify the monitor session has created

```
Switch#Q#
Switch#Q#sh int status
Port      Name          Status       Vlan     Duplex   Speed  Type
Gi0/0                connected   trunk    a-full   auto   RJ45
Gi0/1                connected   10      a-full   auto   RJ45
Gi0/2                connected   10      a-full   auto   RJ45
Gi0/3                monitoring  1      a-full   auto   RJ45
Gi1/0                connected   15      a-full   auto   RJ45
Gi1/1                connected   20      a-full   auto   RJ45
Gi1/2                connected   21      a-full   auto   RJ45
```

Figure 275: Show status port

### 5.3.13 SAMBA

**Step 1:** Update the server with command *apt-get update*

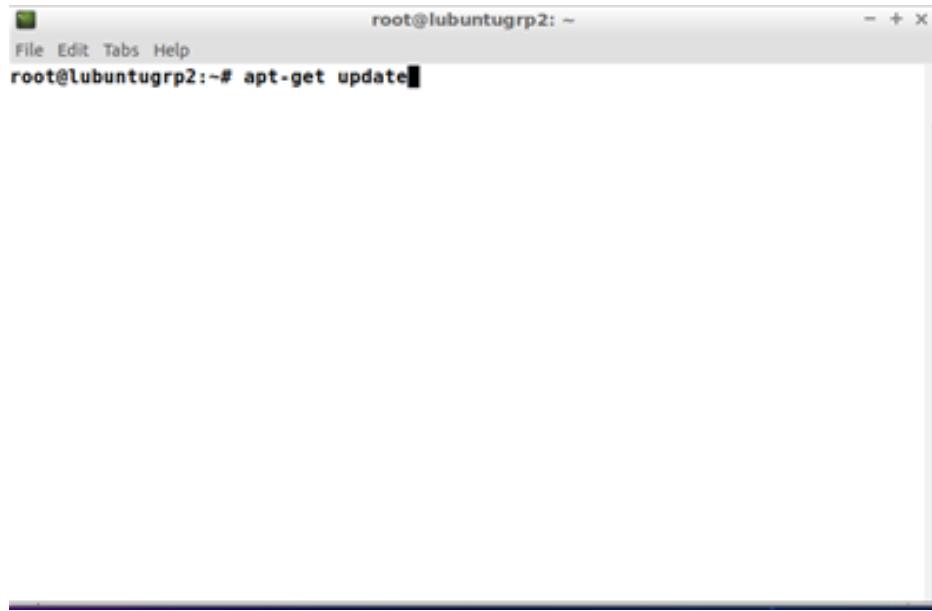
A screenshot of a terminal window titled "root@lubuntugrp2: ~". The window has standard Linux terminal icons at the top. The text area contains the command "root@lubuntugrp2:~# apt-get update" followed by a cursor. The background of the window is white.

Figure 276 : Update the server

**Step 2:** Upgrade the server with command *apt-get upgrade*

A screenshot of a terminal window titled "root@lubuntugrp2: ~". The window has standard Linux terminal icons at the top. The text area contains the command "root@lubuntugrp2:~# apt-get upgrade" followed by a cursor. The background of the window is white.

Figure 277 : Upgrade the server

**Step 3:** Install samba and some packages with command ***apt-get install samba samba-common samba-libs libpam-winbind nautilus-share samba-client***



A screenshot of a terminal window titled "root@lubuntugrp2: ~". The window has standard Linux terminal icons at the top. The text inside the terminal shows the command "root@lubuntugrp2:~# apt-get install samba sambam-common samba-libs libpam-winbind nautilus-sharee samba-client" followed by a carriage return. The terminal is set against a light gray background.

Figure 278 : Installation of samba and some packages in Lubuntu

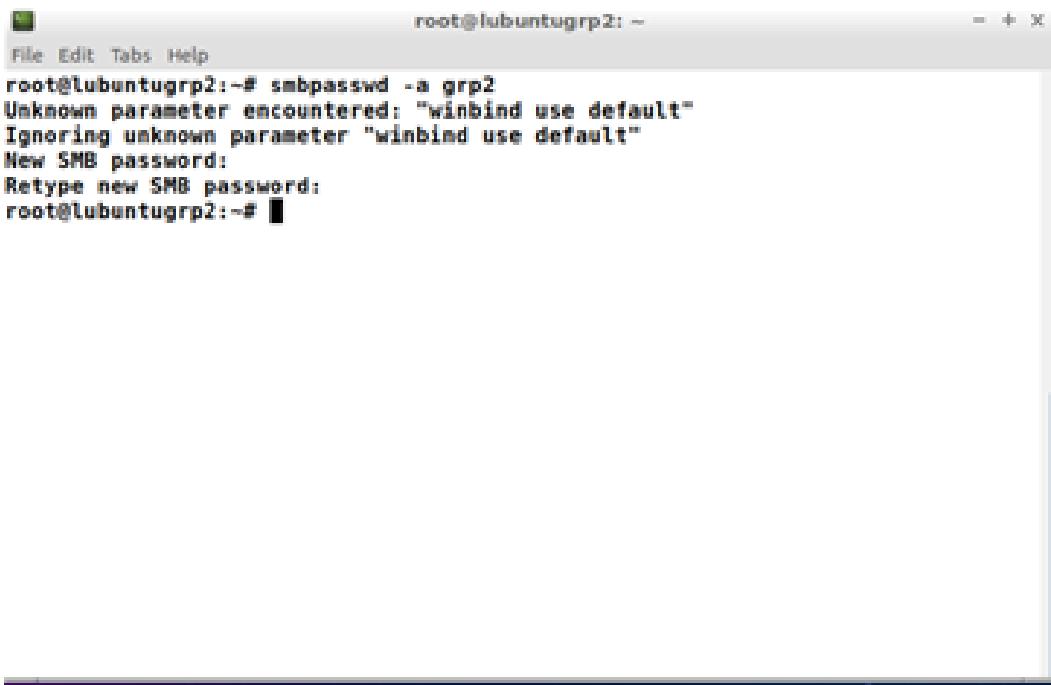
**Step 4:** Add a user for Lubuntu account or use an existing user using command ***useradd grp2***



A screenshot of a terminal window titled "root@lubuntugrp2: ~". The window has standard Linux terminal icons at the top. The text inside the terminal shows the command "root@lubuntugrp2:~# useradd grp2" followed by a carriage return. The terminal is set against a light gray background.

Figure 279 : Addition of new user for samba service

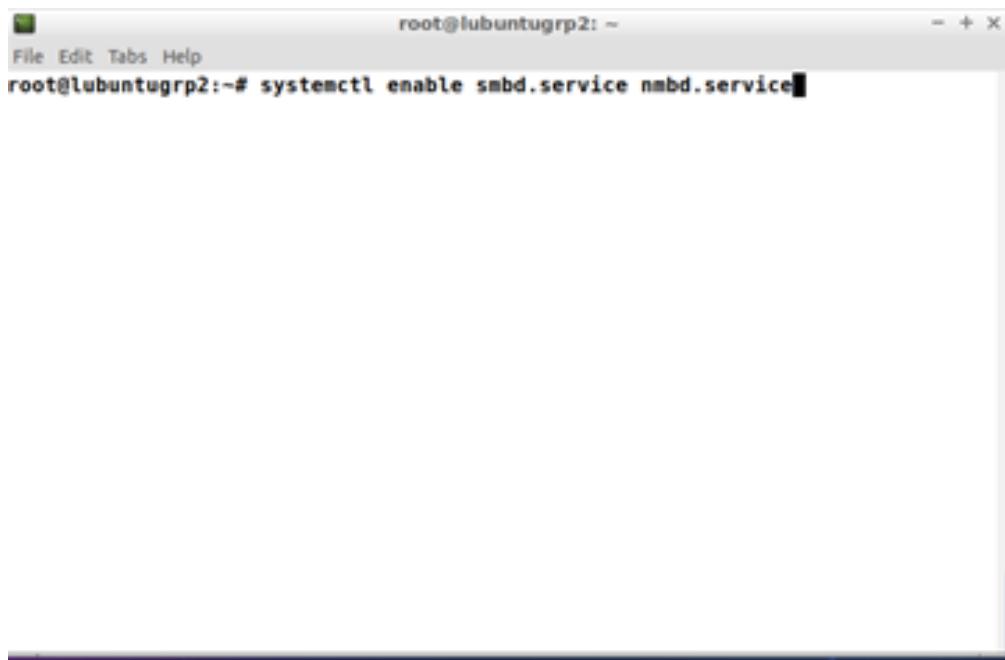
**Step 5:** Create a user for samba using command ***smbpasswd -a grp2***



```
root@lubuntugrp2:~# smbpasswd -a grp2
Unknown parameter encountered: "winbind use default"
Ignoring unknown parameter "winbind use default"
New SMB password:
Retype new SMB password:
root@lubuntugrp2:~#
```

Figure 280 : Create a samba account

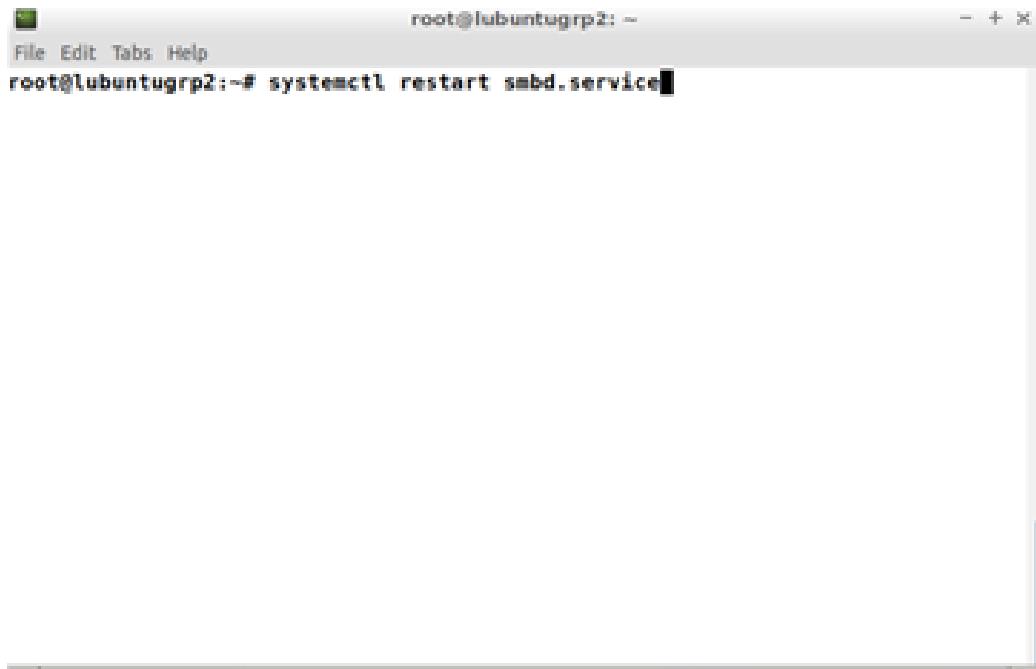
**Step 6:** Enable the smbd service and nmbd service using command ***systemctl enable smbd.service nmbd.service***



```
root@lubuntugrp2:~# systemctl enable smbd.service nmbd.service
```

Figure 281 : Enable the samba service

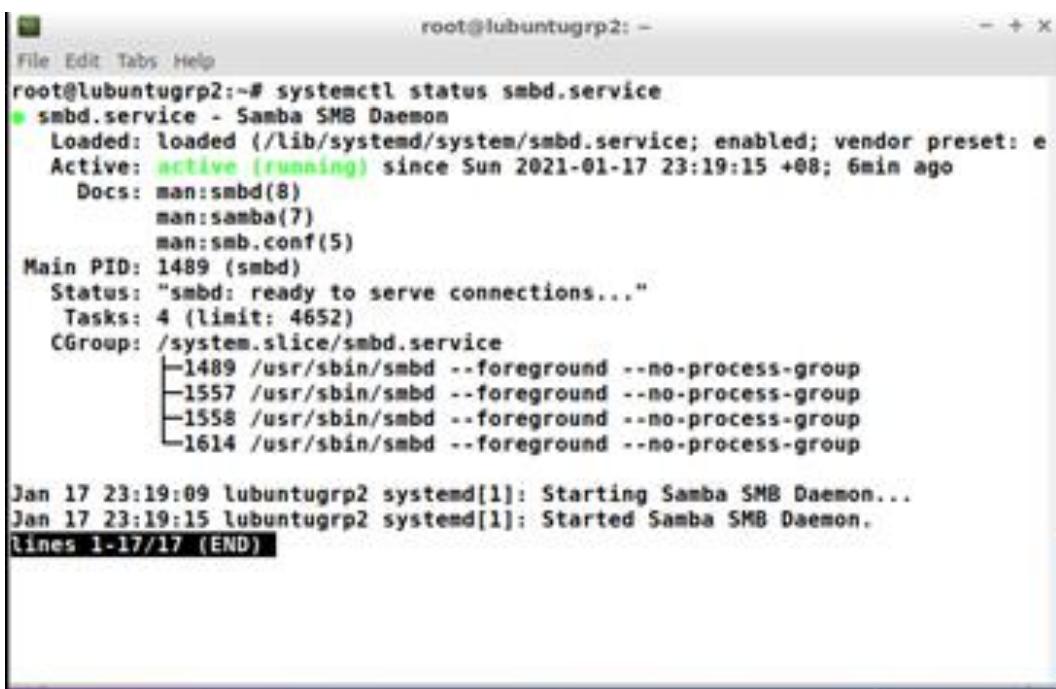
**Step 7:** Restart the smbd service and nmbd service using command ***systemctl restart smbd.service nmbd.service***



```
root@lubuntugrp2: ~
File Edit Tabs Help
root@lubuntugrp2:~# systemctl restart smbd.service
```

Figure 282 : Restart the samba service

**Step 8:** Check the smbd service using command *systemctl status smbd.service*

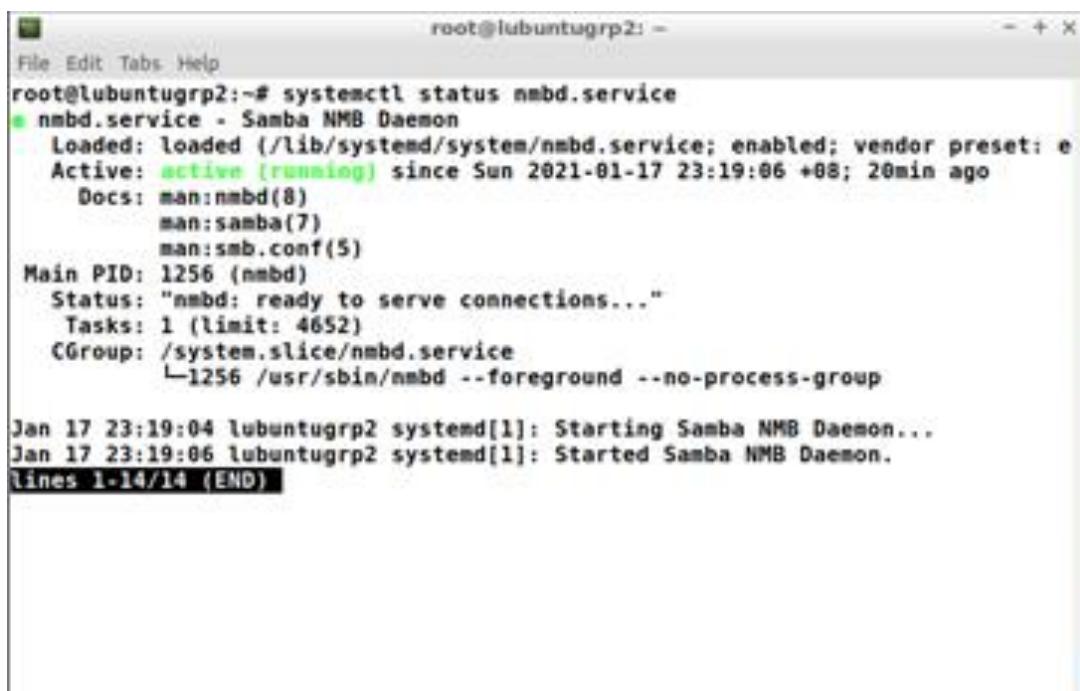


```
root@lubuntugrp2: ~
File Edit Tabs Help
root@lubuntugrp2:~# systemctl status smbd.service
● smbd.service - Samba SMB Daemon
  Loaded: loaded (/lib/systemd/system/smbd.service; enabled; vendor preset: e
  Active: active (running) since Sun 2021-01-17 23:19:15 +08; 6min ago
    Docs: man:smbd(8)
          man:samba(7)
          man:smb.conf(5)
  Main PID: 1489 (smbd)
    Status: "smbd: ready to serve connections..."
      Tasks: 4 (limit: 4652)
     CGroup: /system.slice/smbd.service
             └─1489 /usr/sbin/smbd --foreground --no-process-group
                  ├─1557 /usr/sbin/smbd --foreground --no-process-group
                  ├─1558 /usr/sbin/smbd --foreground --no-process-group
                  └─1614 /usr/sbin/smbd --foreground --no-process-group

Jan 17 23:19:09 lubuntugrp2 systemd[1]: Starting Samba SMB Daemon...
Jan 17 23:19:15 lubuntugrp2 systemd[1]: Started Samba SMB Daemon.
lines 1-17/17 (END)
```

Figure 283 : Status checking for the samba service ( smbd )

**Step 9:** Check the nmbd service using command `systemctl status smbd.service`



```
root@lubuntugrp2:~# systemctl status nmbd.service
● nmbd.service - Samba NMB Daemon
   Loaded: loaded (/lib/systemd/system/nmbd.service; enabled; vendor preset: e
   Active: active (running) since Sun 2021-01-17 23:19:06 +08; 20min ago
     Docs: man:nmbd(8)
           man:samba(7)
           man:smb.conf(5)
 Main PID: 1256 (nmbd)
   Status: "nmbd: ready to serve connections..."
      Tasks: 1 (limit: 4652)
     CGroup: /system.slice/nmbd.service
             └─1256 /usr/sbin/nmbd --foreground --no-process-group

Jan 17 23:19:04 lubuntugrp2 systemd[1]: Starting Samba NMB Daemon...
Jan 17 23:19:06 lubuntugrp2 systemd[1]: Started Samba NMB Daemon.
lines 1-14/14 (END)
```

Figure 284 : Status checking for the samba service ( nmbd )

**Step 10:** Create a folder called NetShare



Figure 285 : Creation of a folder for samba service

**Step 11:** Open the samba configuration file using command ***nano /etc/samba/smb.conf***

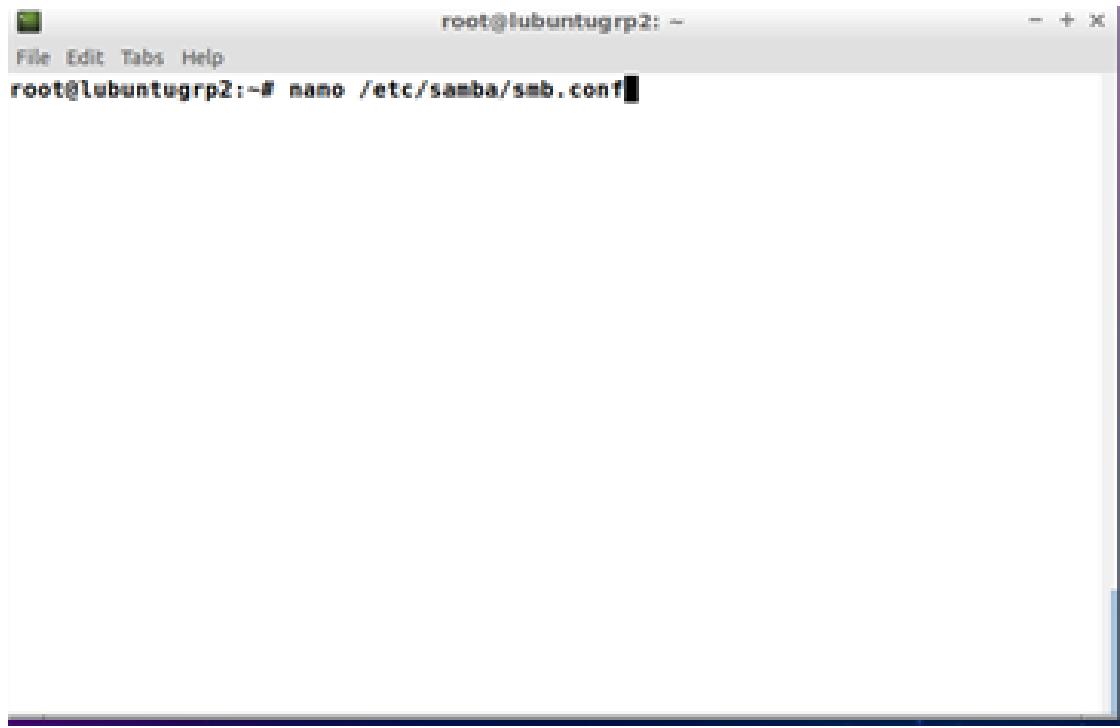


Figure 286 : Opening the samba configuration file

**Step 12:** Edit the samba configuration file using lines as shown in the figure below

```
root@lubuntugrp2:~# nano /etc/samba/smb.conf

[global]
security = user
password server = WIN-6NNIQRONKOU.group2.com
realm = GROUP2.COM
bindip config * : range = 16777216-33554431
template homedir = /home/%D/%U
template shell = /bin/bash
winbind use default = true
winbind offline logon = false

#client ipc signing = auto

^G Get Help   ^O Write Out   ^M Where Is   ^X Cut Text   ^J Justify
^X Exit      ^R Read File    ^I Replace    ^U Uncut Text  ^T To Spell
```

The screenshot shows the contents of the /etc/samba/smb.conf file in the nano editor. It includes global settings like security, password server, realm, and template definitions. It also includes a client ipc section with a signing setting. At the bottom, there are standard nano editor key bindings for various functions like getting help (^G), writing out (^O), and exiting (^X).

Figure 287 : Configuration of samba ( Part 1 )

```
root@lubuntugrp2: ~
File Edit Tabs Help
GNU nano 2.9.3          /etc/samba/smb.conf

# to the drivers directory for these users to have write rights in it
; write list = root, @lpadmin

[MySharing]

comment = My sharing folders sharing
path    = /home/grp2/sharing
read only = no
guest ok = no
valid users = grp2,admin,nonadmin
write list = grp2,admin

(grp2)
comment = grp2 files
path    = /home/grp2/NetShare
valid users = @"group2\Domain Users"
force group = "domain user"
writeable = yes
read only = no

^G Get Help   ^O Write Out   ^K Where Is   ^X Cut Text   ^J Justify
^X Exit      ^R Read File   ^U Replace   ^U Uncut Text  ^T To Spell
```

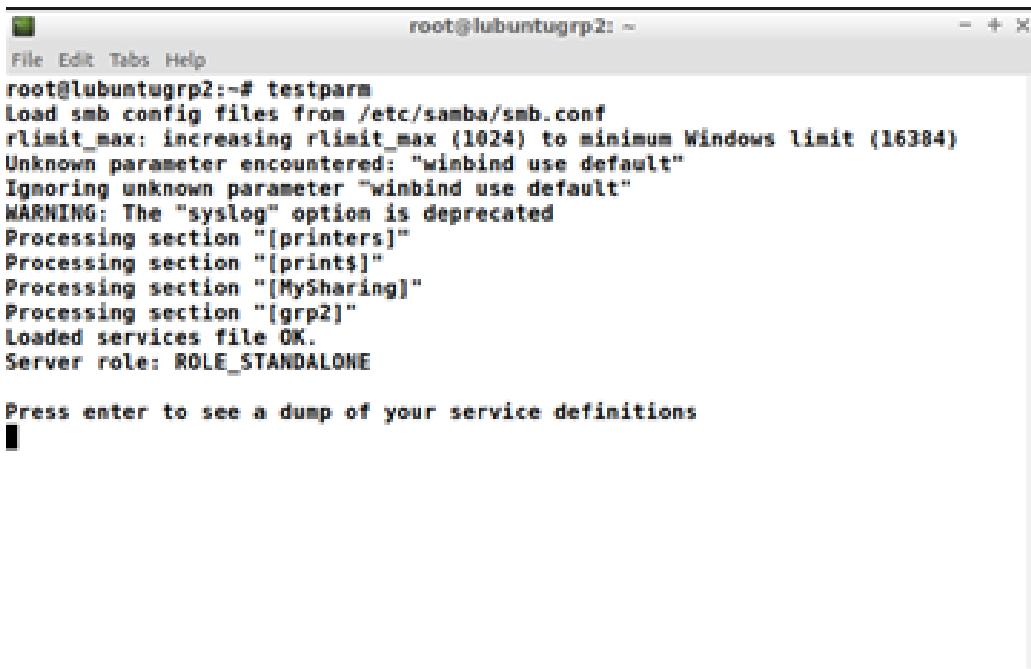
Figure 288 : Configuration of samba ( Part 2 )

### Step 13: Enable the sharing for the folder



Figure 289 : Enabling the folder for sharing

**Step 14:** Test the samba configuration for the sharing using command ***testparm***



```
root@lubuntugrp2:~# testparm
Load smb config files from /etc/samba/smb.conf
rlimit_max: increasing rlimit_max (1024) to minimum Windows limit (16384)
Unknown parameter encountered: "winbind use default"
Ignoring unknown parameter "winbind use default"
WARNING: The "syslog" option is deprecated
Processing section "[printers]"
Processing section "[print$]"
Processing section "[MySharing]"
Processing section "[grp2]"
Loaded services file OK.
Server role: ROLE_STANDALONE

Press enter to see a dump of your service definitions
[ ]
```

*Figure 290 : Testing of the samba configuration file*

### 5.3.14 LINUX SERVER HARDENING

#### Ubuntu Server Hardening

##### Step 1: Keep Linux Server Updates

Step 1(a): Update and upgrade for the system to get the latest packages. Click yes for all the update packages.

```
grp2@lubuntugrp2:~$ sudo apt-get update
sudo: /etc/sudoers.d is world writable
[sudo] password for grp2:
Hit:1 http://my.archive.ubuntu.com/ubuntu bionic InRelease
Get:2 http://security.ubuntu.com/ubuntu bionic-security InRelease [88.7 kB]
Get:3 http://my.archive.ubuntu.com/ubuntu bionic-updates InRelease [88.7 kB]
Get:4 http://my.archive.ubuntu.com/ubuntu bionic-backports InRelease [74.6 kB]
Get:5 http://security.ubuntu.com/ubuntu bionic-security/main amd64 Packages [1,499 kB]
Get:6 http://my.archive.ubuntu.com/ubuntu bionic-updates/main i386 Packages [1,189 kB]
Get:7 http://my.archive.ubuntu.com/ubuntu bionic-security/main amd64 Packages [1,835 kB]
Get:8 http://security.ubuntu.com/ubuntu bionic-security/main i386 Packages [888 kB]
Get:9 http://security.ubuntu.com/ubuntu bionic-security/main amd64 DEP-11 Meta
data [49.0 kB]
Get:10 http://security.ubuntu.com/ubuntu bionic-security/universe amd64 DEP-11
Metadata [59.4 kB]
Get:11 http://security.ubuntu.com/ubuntu bionic-security/multiverse amd64 DEP-
11 Metadata [2,464 B]
Get:12 http://my.archive.ubuntu.com/ubuntu bionic-updates/main amd64 DEP-11 Me
tadata [295 kB]
Get:13 http://my.archive.ubuntu.com/ubuntu bionic-updates/universe amd64 Packa
```

Figure 291 : Update for the system

```
grp2@lubuntugrp2:~$ sudo apt-get upgrade
sudo: /etc/sudoers.d is world writable
Reading package lists... Done
Building dependency tree
Reading state information... Done
Calculating upgrade... Done
The following packages have been kept back:
  linux-generic linux-headers-generic linux-image-generic
The following packages will be upgraded:
  adcli firefox firefox-locale-en ghostscript ghostscript-x libgs9
  libgs9-common libipa-hbac0 libnss-sss libopenexr22 libpl1-kit0 libpam-sss
  libproxy1-plugin-gsettings libproxy1-plugin-networkmanager libproxy1v5
  libssasl2-2 libssasl2-modules libssasl2-modules-db
  libssasl2-modules-gssapi-mit libsss-certmap0 libsss-idmap0
  libsss-nss-idmap0 libsss-simpleifp0 libsss-sudo libwvpack1 linux-libc-dev
  pl1-kit pl1-kit-modules python-apt-common python-sss python3-apt
  python3-distupgrade python3-sss sssd sssd-ad sssd-ad-common sssd-common
  sssd-dbus sssd-ipa sssd-krb5 sssd-krb5-common sssd-ldap sssd-proxy
  sssd-tools tzdata ubuntu-release-upgrader-core ubuntu-release-upgrader-gtk
  update-notifier update-notifier-common xdg-utils
50 upgraded, 0 newly installed, 0 to remove and 3 not upgraded.
Need to get 69.4 MB of archives.
After this operation, 144 kB disk space will be freed.
Do you want to continue? [Y/n] y
```

Figure 292 : Upgrade for the system

Step 1(b): Install package for allowing system to automatically update.

```
root@lubuntugrp2:~# apt-get install unattended-upgrades
Reading package lists... Done
Building dependency tree
Reading state information... Done
Suggested packages:
  bsd-mailx needrestart
The following NEW packages will be installed:
  unattended-upgrades
0 upgraded, 1 newly installed, 0 to remove and 3 not upgraded.
Need to get 41.7 kB of archives.
After this operation, 418 kB of additional disk space will be used.
Get:1 http://my.archive.ubuntu.com/ubuntu bionic-updates/main amd64 unattended-upgrades all 1.lubuntul.18.04.14 [41.7 kB]
Fetched 41.7 kB in 2s (26.8 kB/s)
Preconfiguring packages ...
Selecting previously unselected package unattended-upgrades.
(Reading database ... 191497 files and directories currently installed.)
Preparing to unpack .../unattended-upgrades_1.lubuntul.18.04.14_all.deb ...
Unpacking unattended-upgrades (1.lubuntul.18.04.14) ...
Setting up unattended-upgrades (1.lubuntul.18.04.14) ...

Creating config file /etc/apt/apt.conf.d/50unattended-upgrades with new version
Created symlink /etc/systemd/system/multi-user.target.wants/unattended-upgrade
```

Figure 293 : Install auto-update package

Step 1(c): Change directory into **/etc/apt/apt.conf.d**. Make configuration on config file (50unattended-upgrades). Save and close the file.



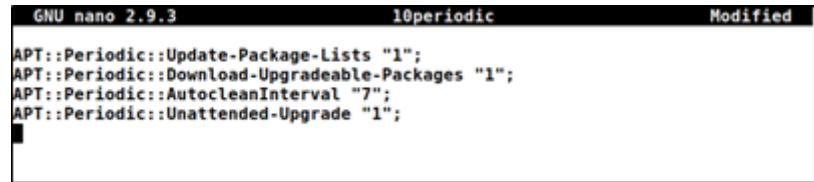
```
GNU nano 2.9.3          50unattended-upgrades

// Automatically upgrade packages from these (origin:archive) pairs
//
// Note that in Ubuntu security updates may pull in new dependencies
// from non-security sources (e.g. chromium). By allowing the release
// pocket these get automatically pulled in.
Unattended-Upgrade::Allowed-Origins {
    "${distro_id}:${distro_codename}";
    "${distro_id}:${distro_codename}-security";
    // Extended Security Maintenance; doesn't necessarily exist for
    // every release and this system may not have it installed, but if
    // available, the policy for updates is such that unattended-upgrades
    // should also install from here by default.
    "${distro_id}ESMAApps:${distro_codename}-apps-security";
    "${distro_id}ESM:${distro_codename}-infra-security";
    "${distro_id}:${distro_codename}-updates";
    // "${distro_id}:${distro_codename}-proposed";
    // "${distro_id}:${distro_codename}-backports";
};

[ Read 92 lines ]
^G Get Help      ^O Write Out      ^W Where Is      ^K Cut Text      ^J Justify
^X Exit          ^R Read File       ^\ Replace       ^U Uncut Text    ^T To Spell
```

Figure 294 : Editing configuration file (50unattended-upgrades)

Step 1(d): Editing config file (10periodic) to enable automatic updates. Save and close the file.



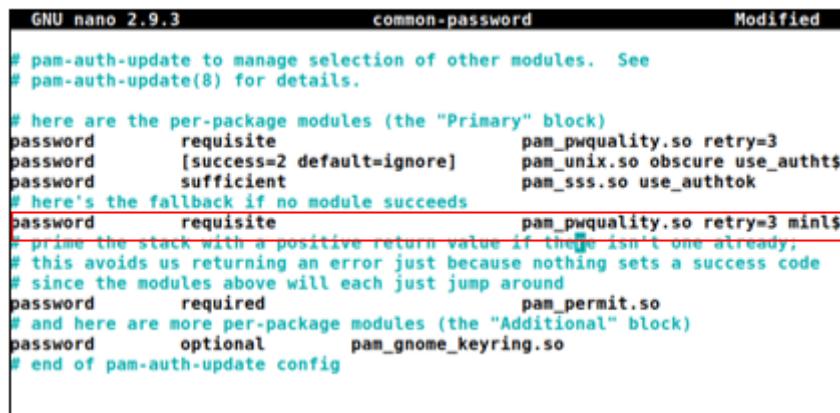
```
GNU nano 2.9.3          10periodic          Modified
APT::Periodic::Update-Package-Lists "1";
APT::Periodic::Download-Upgradeable-Packages "1";
APT::Periodic::AutocleanInterval "7";
APT::Periodic::Unattended-Upgrade "1";
```

Figure 295 : Configuration on config file (10periodic)

The above configuration updates the package list, downloads, and installs available upgrades every day. The local download archive is cleaned every week.

## Step 2: Password Policy

Step 2(a): Change directory to **/etc/pam.d** and use any text editor to open the **common - password** configuration file for Pluggable Authentication Modules(PAM) services.



```
GNU nano 2.9.3          common-password          Modified
# 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      requisite          pam_pwquality.so retry=3
password      [success=2 default=ignore]    pam_unix.so obscure use_auth$#
password      sufficient         pam_sss.so use_authok
# here's the fallback if no module succeeds
password      requisite          pam_pwquality.so retry=3 minl$#
# 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 296 : Update common-password config file

```

GNU nano 2.9.3           common-password          Modified
# 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      requisite          pam_pwquality.so retry=3
password      [success=2 default=ignore]    pam_unix.so obscure use_authent$ 
password      sufficient         pam_sss.so use_authentok

# here's the fallback if no module succeeds
s3 minlen=10 dcredit=-1 ucredit=-1 lcredit=-1

# 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

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

```

Figure 297 : Update common-password config file

Step 2(b): Set a maximum of 3 attempts for getting an acceptable password, a 8 character of minimum length, a requirement that the password contain at least one each of digit, lower-case character, and upper-case character. Then, save and close the file.

Step 2(c): Change directory to **/etc/** and use any text editor to open the **login.defs** configuration file. Under Linux password related utilities and config files comes from shadow password suite. The **/etc/login.defs** file defines the site-specific configuration for this suite.

Step 2(d): Edit the **login.defs** configuration file. Save and close the file.

```

GNU nano 2.9.3           login.defs            Modified
KILLCHAR      025
UMASK        022

#
# Password aging controls:
#
# PASS_MAX_DAYS  Maximum number of days a password may be used.
# PASS_MIN_DAYS  Minimum number of days allowed between password chang$ 
# PASS_WARN_AGE   Number of days warning given before a password expire$ 

PASS_MAX_DAYS 60
PASS_MIN_DAYS 5
PASS_WARN_AGE 14

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

```

Figure 298 : Update login.defs file

This will force every user to change their password once every 2 months and send out a warning message 14 days prior to password expiration.

Step 2(e): Change specify user password expiration

```
root@lubuntugrp2:~# chage -m 5 -M 60 -W 14 -I 30 grp2
```

*Figure 299 : Change specify user (grp2) password expiration*  
This user(grp2) password will be expired on specific date.

Command:

```
sudo chage -m 5 -M 60 -W 14 -I 30 username
```

-m = minimum of 5 days between password change

-M = Maximum of 60 days between password change

-W = set expiration warning days to 14 days

-I = set password inactive after expiration to 30 days For more information use **chage –help**

Step 3: Set Permission on Sensitive System File

Step 3(a): Open Terminal and type in following command. Set only root has permission on these sensitive system files.

```

root@lubuntugrp2:~# cd /var/log
root@lubuntugrp2:/var/log# chmod 0700 wtmp
root@lubuntugrp2:/var/log# cd /etc/
root@lubuntugrp2:/etc# chmod 0755 /etc/profile
root@lubuntugrp2:/etc# chmod 0700 /etc/hosts
root@lubuntugrp2:/etc#

```

*Figure 300 : Change system files permission*

- **/var/log/wtmp** show login and logout info.
- **/etc/profile** contains Linux system wide environment and startup programs. Usually used to set PATH variable, user limits, and other settings for user. It only runs for login shell.
- **/etc/hosts** hosts file is a plain text file that all operating systems use to translate hostnames into IP addresses.
- **chmod 0755** (chmod a+rwx,g-w,o-w,ug-s,-t) sets permissions so that, (U)ser / owner can read, write and execute. (G)roup can read and execute but cannot write. (O)thers can read and execute but cannot write.
- **chmod 0700** (chmod a+rwx,g-rwx,o-rwx,ug-s,-t) sets permissions so that, (U)ser / owner can read, write and execute. (G)roup cannot read, write and execute. (O)thers cannot read, write and execute.

#### Step 4: Set Permission on User File

Step 4(a): Open Terminal and type in following command.

```

root@lubuntugrp2:/etc# chmod 0644 /etc/fstab
root@lubuntugrp2:/etc# chmod 0644 /etc/passwd
root@lubuntugrp2:/etc# chmod 0400 /etc/shadow
root@lubuntugrp2:/etc# chmod 0644 /etc/group
root@lubuntugrp2:/etc# chmod 0644 /etc/sudoers
root@lubuntugrp2:/etc# ■

```

*Figure 301 : Change permission on user accessible file*

- **/etc/fstab** is a list of file systems to be mounted at BOOT time.
- **/etc/passwd** stores essential information, required during login to the system. This file is owned by the root user and must be readable by all the users, but only the root user has writable permissions.

- **/etc/shadow** file stores actual password in encrypted format for user's account with additional properties related to user password.
- **/etc/group** is a text file which defines the groups to which users belong under Linux and UNIX operating system.
- **/etc/sudoers**. The sudoers file is a file Linux and Unix administrators use to allocate system rights to system users. This allows the administrator to control who does what.
- **chmod 0644** (`chmod a+rwx,u-x,g-wx,o-wx,ug-s,-t`) sets permissions so that, (U)ser / owner can read and write but cannot execute. (G)roup can read but cannot write and execute. (O)thers can read but cannot write and execute.
- **chmod 0400** (`chmod a+rwx,u-wx,g-rwx,o-rwx,ug-s,-t`) sets permissions so that, (U)ser / owner can read but cannot write and execute. (G)roup cannot read, write and execute. (O)thers cannot read, write and execute.

Step 5: Use multiple tools to discover on network port

Step 5(a): Use **netstat** as a command line tool for monitoring network connections both incoming and outgoing traffic. **Netstat** is one of the most basic network services debugging tools, shows what ports are open and whether any programs are listening on ports. Study on each listening port and disable those unused port. Discovered that the cups printing is opened. So, we decided to close this service.

Active Internet connections (only servers)						
Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State	PID/Program name
tcp	0	0	127.0.0.53:53	0.0.0.0:*	LISTEN	594/systemd-resolv
tcp	0	0	0.0.0.0:22	0.0.0.0:*	LISTEN	1054/sshd
tcp	0	0	127.0.0.1:631	0.0.0.0:*	LISTEN	874/cupsd
tcp	0	0	0.0.0.0:25	0.0.0.0:*	LISTEN	1394/master
tcp	0	0	0.0.0.0:445	0.0.0.0:*	LISTEN	1431/smbd
tcp	0	0	0.0.0.0:993	0.0.0.0:*	LISTEN	1199/dovecot
tcp	0	0	0.0.0.0:5666	0.0.0.0:*	LISTEN	1245/nrpe
tcp	0	0	0.0.0.0:139	0.0.0.0:*	LISTEN	1431/smbd
tcp	0	0	192.168.5.66:5357	0.0.0.0:*	LISTEN	1123/python3
tcp	0	0	0.0.0.0:143	0.0.0.0:*	LISTEN	1199/dovecot
tcp	0	0	0.0.0.0:111	0.0.0.0:*	LISTEN	591/rpcbind
tcp6	0	0	:::22	:::*	LISTEN	1054/sshd
tcp6	0	0	:::631	:::*	LISTEN	874/cupsd
tcp6	0	0	:::25	:::*	LISTEN	1394/master

Figure 302 : Discover listening port

tcp6	0	0	:::445	:::*	LISTEN	1431/smbd
tcp6	0	0	:::993	:::*	LISTEN	1199/dovecot
tcp6	0	0	:::5666	:::*	LISTEN	1245/nrpe
tcp6	0	0	:::139	:::*	LISTEN	1431/smbd
tcp6	0	0	fe80::20c:29ff:fe3:5357	:::*	LISTEN	1123/python3
tcp6	0	0	:::143	:::*	LISTEN	1199/dovecot
tcp6	0	0	:::111	:::*	LISTEN	591/rpcbind
tcp6	0	0	:::80	:::*	LISTEN	1355/apache2

Figure 303 : Discover listening port

Command:

netstat -tlpn

-t: scan for TCP

-l: display listening server sockets

-p: display PID/Program name for sockets

-n: display numeric port number, do not resolve names.

Step 5(b): Install **Nmap** ("Network Mapper") as a tool for network exploration and security auditing. It was designed to rapidly scan large networks, although it works fine against single hosts. Nmap is commonly used for security audits, many systems and network administrators find it useful for routine tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime.

```
root@lubuntugrp2:~# sudo apt-get install nmap
sudo: /etc/sudoers.d is world writable
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
liblinear3
Suggested packages:
liblinear-tools liblinear-dev ndiff
The following NEW packages will be installed:
liblinear3 nmap
0 upgraded, 2 newly installed, 0 to remove and 3 not upgraded.
Need to get 5,213 kB of archives.
After this operation, 24.1 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 liblinear3 amd64 2
.1.0+dfsg-2 [39.3 kB]
Get:2 http://my.archive.ubuntu.com/ubuntu bionic/main amd64 nmap amd64 7.60-1u
buntu5 [5,174 kB]
32% [2 nmap 1,378 kB/5,174 kB 27%]                                         207 kB/s 18s■
```

Figure 304 : Installing Nmap

Step 5(e): Discover all opened port with command **nmap -p- <IP address of Linux server>**. Study on each opened port and identify which port is not needed and disable that port.

```
root@lubuntugrp2:~# nmap -p- 192.168.5.210
Starting Nmap 7.60 ( https://nmap.org ) at 2021-01-13 03:55 +08
Nmap scan report for mail.group2.com (192.168.5.210)
Host is up (0.000010s latency).
Not shown: 65525 closed ports
PORT      STATE SERVICE
25/tcp    open  smtp
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
143/tcp   open  imap
445/tcp   open  microsoft-ds
993/tcp   open  imaps
2222/tcp  open  EtherNetIP-1
5357/tcp  open  wsdapi
5666/tcp  open  nrpe

Nmap done: 1 IP address (1 host up) scanned in 6.64 seconds
```

Figure 305 : Discovered port on Nmap

Command **nmap -p <IP address of Linux server>**

-p- : used to scan all the port on the provided IP addresses.

## Step 6: Disable Unnecessary Services and Port

Step 6(a): To disable unnecessary service and port. Use **service <program names/packages> stop**. From discovering the network port, found an unnecessary service which is CUPS service. CUPS is a common UNIX printing system which allows a computer to act as a print server

```
root@lubuntugrp2:~# cd /etc
root@lubuntugrp2:/etc# service cups stop
root@lubuntugrp2:/etc# systemctl disable cups
Synchronizing state of cups.service with SysV service script with /lib/systemd
/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install disable cups
Removed /etc/systemd/system/sockets.target.wants/cups.socket.
Removed /etc/systemd/system/multi-user.target.wants/cups.path.
root@lubuntugrp2:/etc# █
```

Figure 306 : Stop CUPS services

## Step 7: Use Linux Firewall

Step 7(a): UFW (Ubuntu Firewall) is a simple, easy-to-use, front-end interface to manage Linux iptables firewall. Iptables rules are complicated and UFW is designed to make things less complicated for administrators. Installation for UFW application.

```
root@lubuntugrp2:~# apt install ufw
Reading package lists... Done
Building dependency tree
Reading state information... Done
ufw is already the newest version (0.36-0ubuntu0.18.04.1).
0 upgraded, 0 newly installed, 0 to remove and 3 not upgraded.
root@lubuntugrp2:~# █
```

Figure 307 : Installation of UFW

Step 7(b): Enable access to the port used by SSH which is port 2222 by using command **ufw allow ssh**.

```
root@lubuntugrp2:~# cd /etc/ssh  
root@lubuntugrp2:/etc/ssh# ufw allow 2222/tcp
```

Figure 308 : Allow ssh port

Step 7(c): Reload the firewall so changes reflect immediately.

```
root@lubuntugrp2:~# ufw reload  
WARN: /etc/default is world writable!  
WARN: /etc is world writable!  
WARN: / is world writable!  
WARN: /etc/ufw is world writable!  
WARN: /etc/ufw/applications.d is world writable!  
WARN: /lib/ufw is world writable!  
WARN: /lib is world writable!  
WARN: /usr/sbin is world writable!  
WARN: /usr is world writable!  
Firewall reloaded
```

Figure 309 : Reload UFW

Step 7(d): Set automatically enable for firewall service permanently.

```
root@lubuntugrp2:~# systemctl enable ufw  
Synchronizing state of ufw.service with SysV service script with /lib/systemd/  
systemd-sysv-install.  
Executing: /lib/systemd/systemd-sysv-install enable ufw  
root@lubuntugrp2:~# █
```

Figure 310 : Enable UFW

### 5.3.15 IPSEC VPN SERVER

#### SoftEther VPN Server Installation

Step 1 : Access to <https://www.softether.org/5-download> and select **Download** button.

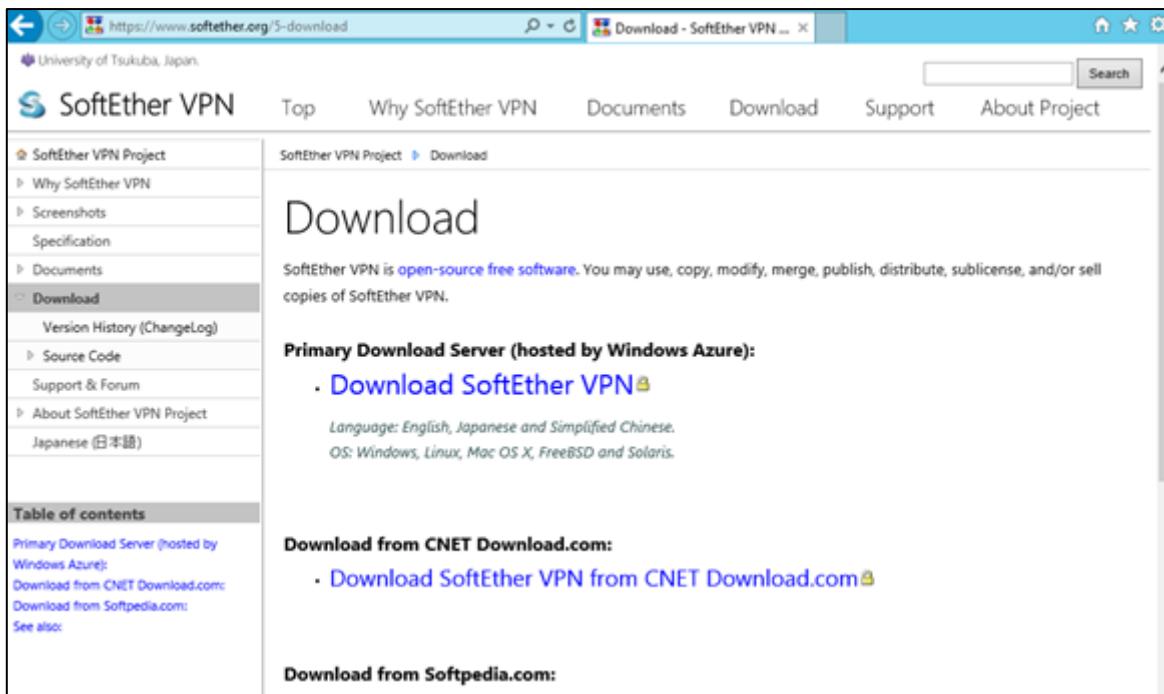


Figure 311 : Go to website and click download

Step 2 : Select **Download SoftEther VPN**.



Figure 312 : Download SoftEther VPN

Step 3 : Select the Software, Component, Platform and CPU according to your requirement and begin to download.

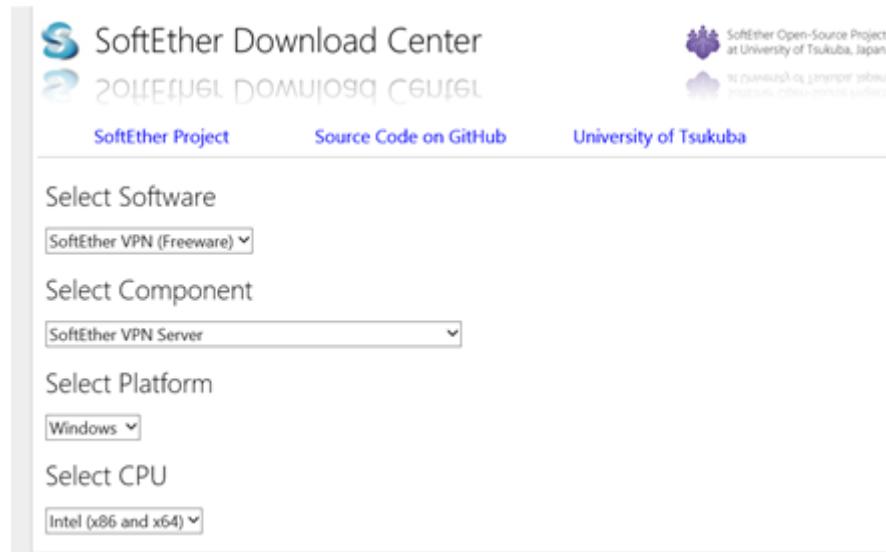


Figure 313 : Choose requirement

Step 4 : Execute the installer that have been downloaded. A Welcome Page will be shown and click **Next**.



Figure 314 : Download section

Step 5 : Then, select **SoftEther VPN Server** and select Next.

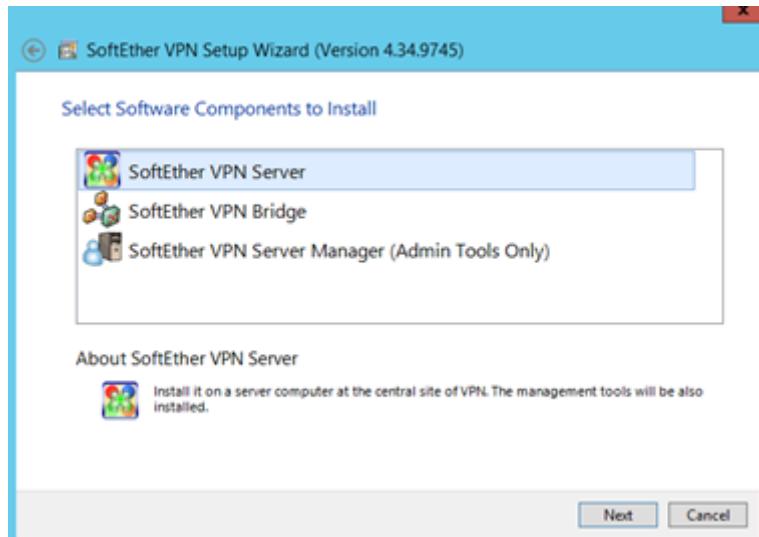


Figure 315 : Choose software component to install

Step 6 : Tick **Agree** to the User License Agreement and select **Next**.

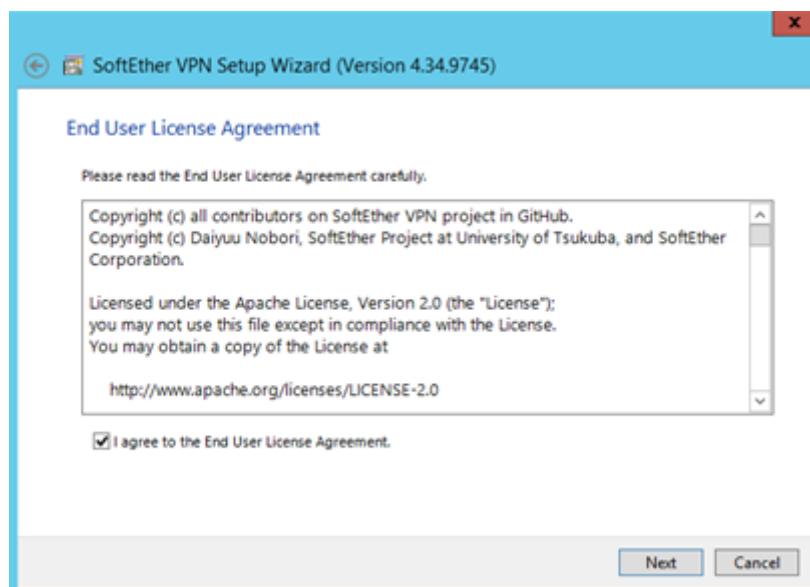


Figure 316 : Agree to End user Agreement

Step 7 : Click **Next** to proceed to select file path to store SoftEther VPN Server.

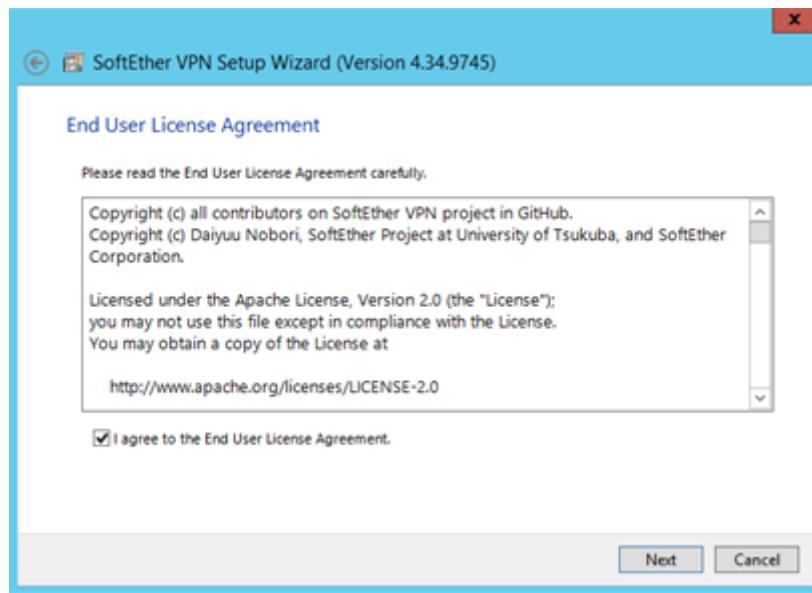


Figure 317 : Important Notice

Step 8 : Select the file path that you wish to store SoftEther VPN Server file and select **Next**.

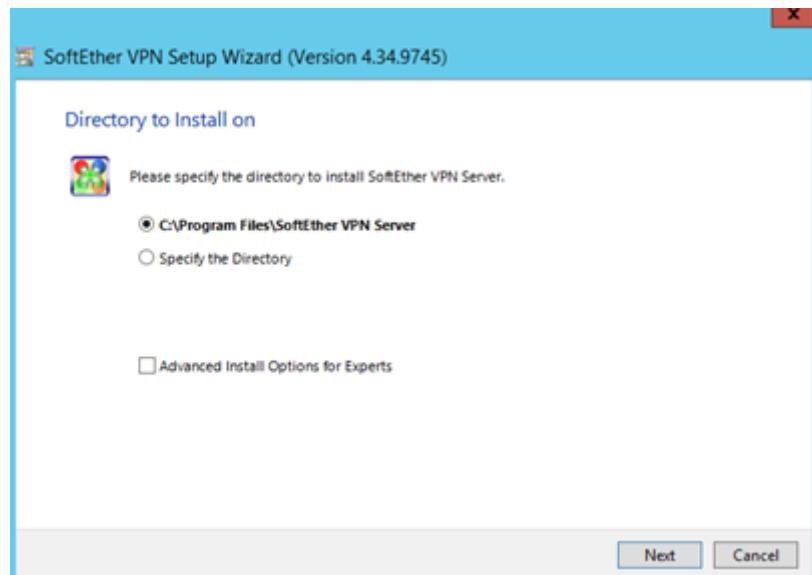


Figure 318 : Path Selection

Step 9 : Then, select **Next** and wait for the SoftEther VPN Server installation to complete and click **Finish**.

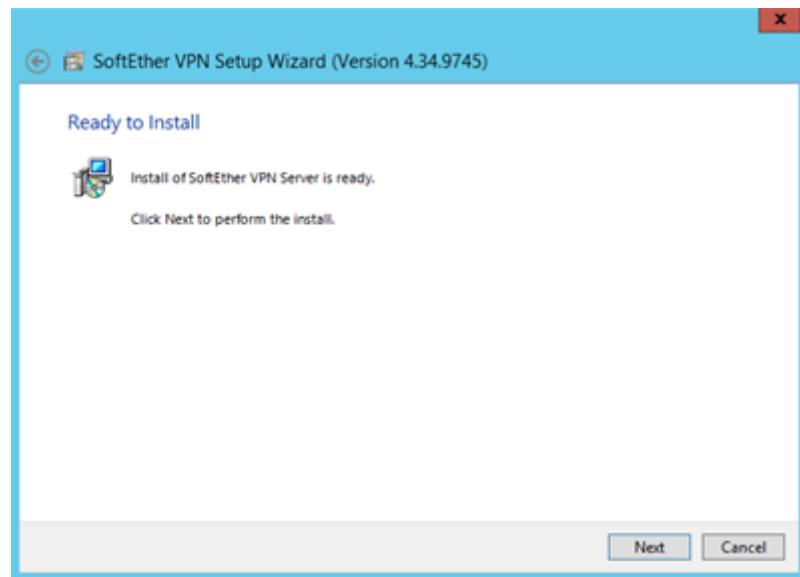


Figure 319 : Wait for installation

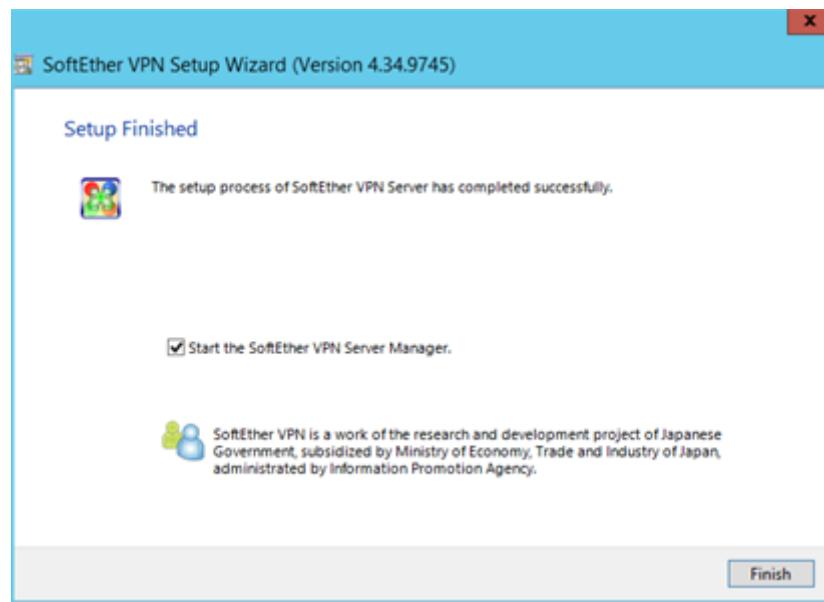


Figure 320 : Finish installation

Step 10 : Open the SoftEther VPN Server Manager. Then. select the **localhost(This server)** option and select **Edit Setting** to change the configuration.



Figure 321: Select local host

## Configuration of SoftEther VPN Server

Step 1 : Modify the **Setting Name** and use the **port 5555** by default. Remember to check the **“Connect to Localhost”** boxes for easy troubleshooting. Other options remain the same and select **OK**.

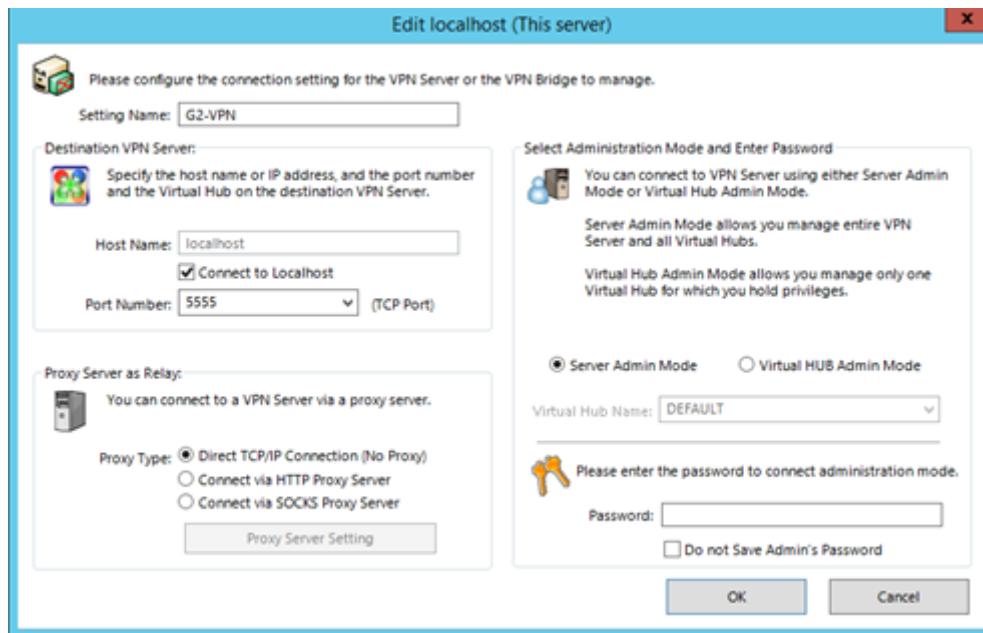


Figure 322 : Set up local host

Step 2 : Click on **Connect** button at bottom right section. Set the administrator password and hit **OK**.



Figure 323 : Set administrator password

Step 3 : Next, a SoftEther VPN Server/Bridge Easy Setup window will pop out. Tick the **Remote Access VPN Server, Site-to-site VPN Server or VPN Bridge** and select **Next**. Then, select **Next** on the new pop up window.

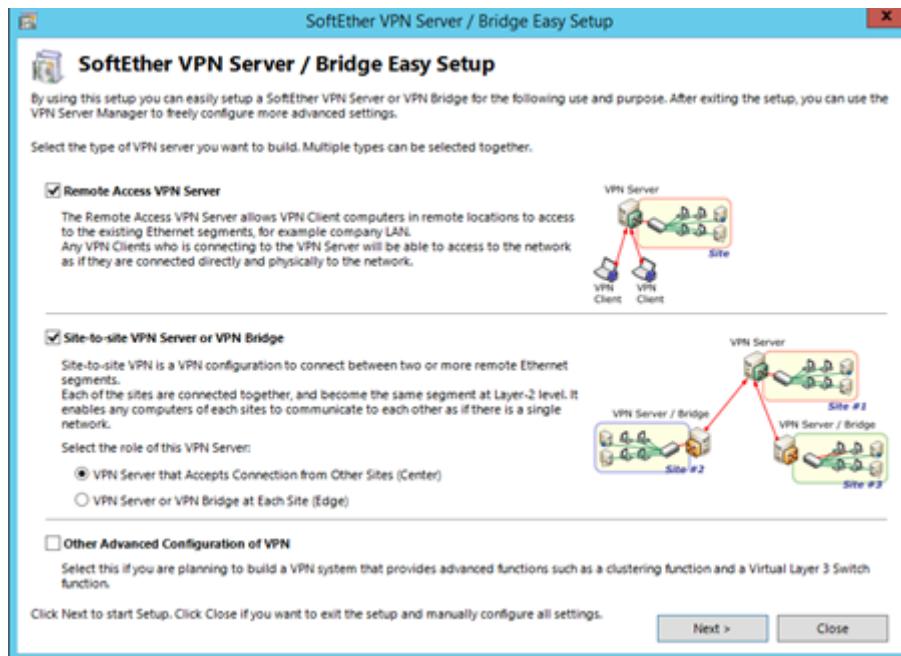


Figure 324 : Set up bridge



Figure 325 : Set up confirmation notice

Step 4 : Setup for the Virtual Hub Name and select **OK**.

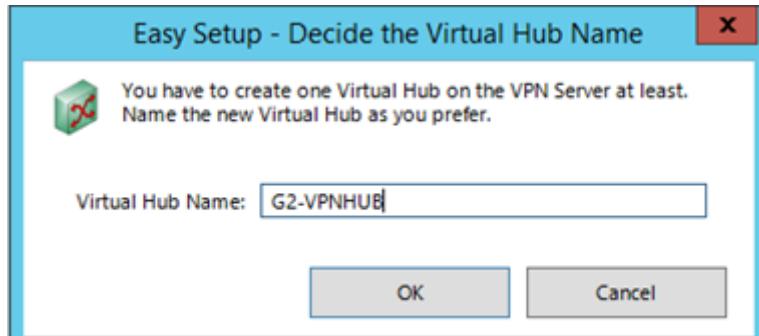


Figure 326 : Setup Virtual Hub Name

Step 5 : Disable VPN Azure Services and press **OK**.

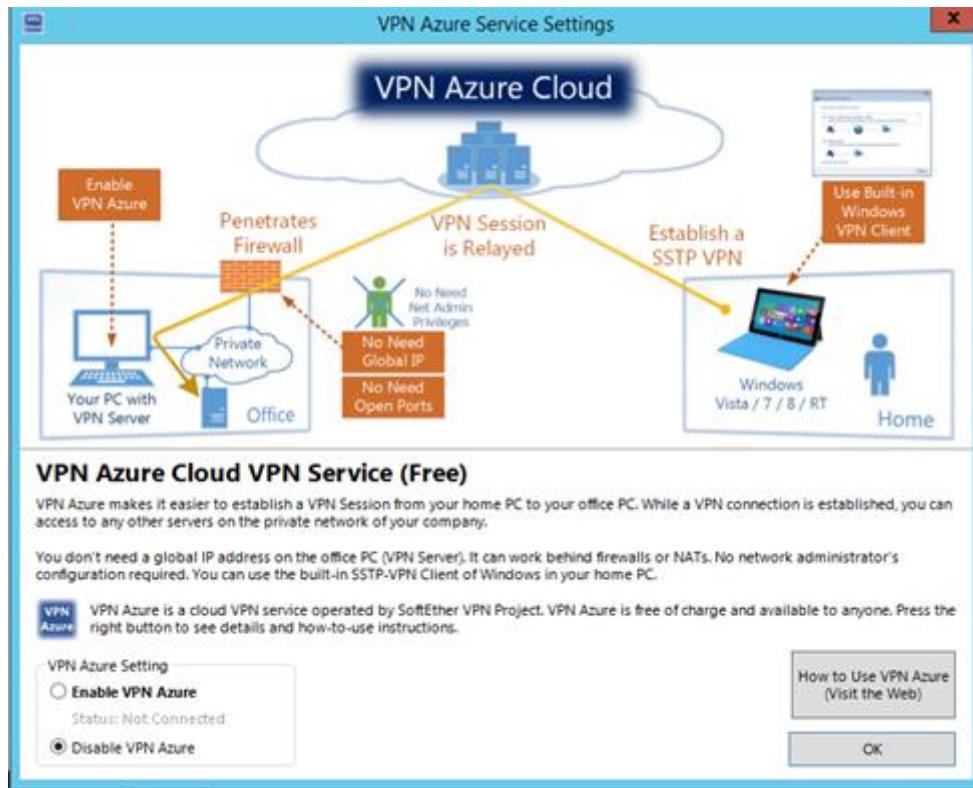


Figure 327 : Disable VPN Azure Services

Step 6 : Select **Create Users** button and create a new user. Modify the Auth Type to **Password Authentication** for easy management and set a new password for the user. After finish modifying, and select **OK** button to create new user.

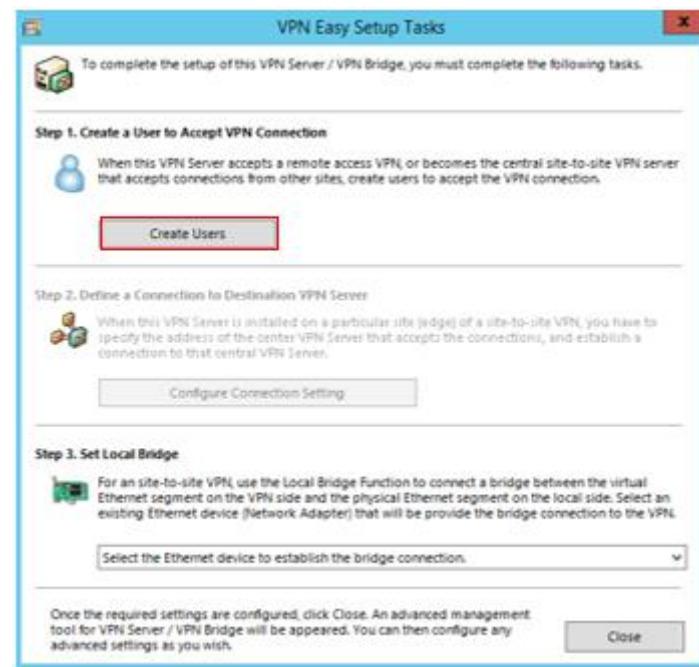


Figure 328 : Create a new user

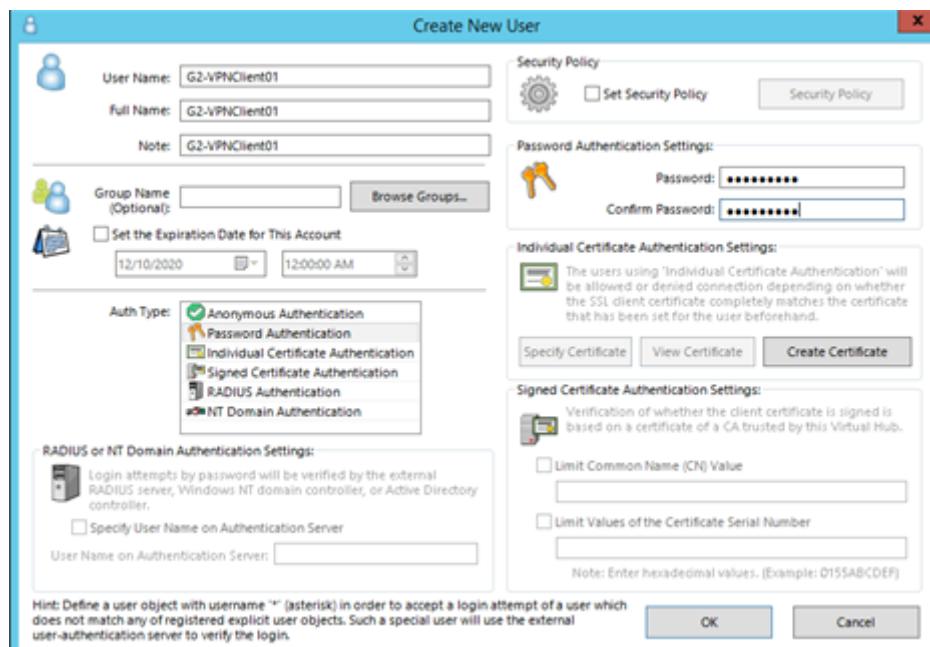


Figure 329 : Set up new user

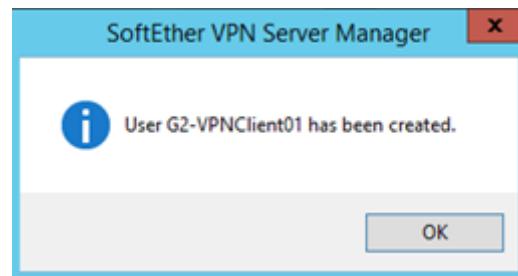
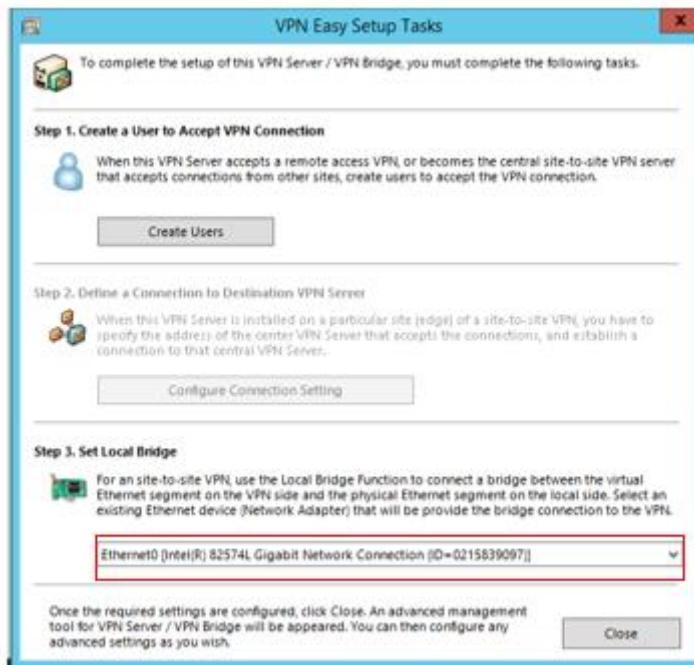


Figure 330 : Confirmation alert of user created

Manage Users						
Virtual Hub "G2-VPNHUB" has the following users.						
User Name	Full Name	Group Name	Description	Auth Method	Num Logins	Last Login
G2-VPNClient01	G2-VPNClient01	-	G2-VPNClient01	Password Auth...	0	(None)
<button>New</button> <button>Edit</button> <button>View User Info</button> <button>Remove</button> <button>Refresh</button> <button>Exit</button>						

Figure 331: Manage user

Step 7 : Exit from the Manage User window. Set Local Bridge with the desired NIC to use and close the window.



*Figure 332 : Set up local bridge*

Step 8 : After finishing setup for Local Bridge, click on virtual hub name and select **Management of Virtual Hub** and chose **Virtual NAT and Virtual DHCP Server (SecureNAT)**.



*Figure 333 : Manage Virtual Hub*

Step 9 ; Next, select **Enable SecureNAT** and click **OK** to proceed. It is crucial as it will provide IP address to the user. Click **OK** then close Management of Virtual Hub windows.

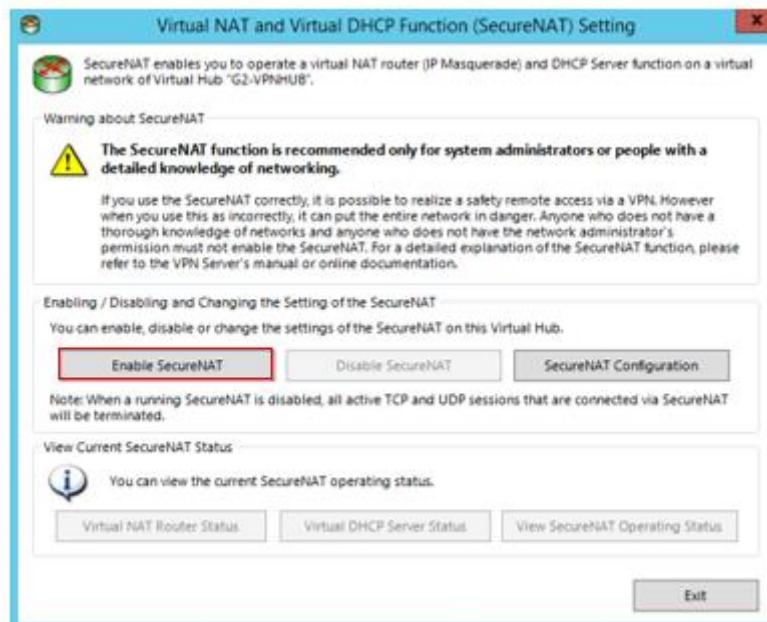


Figure 334 : Enable SecureNAT

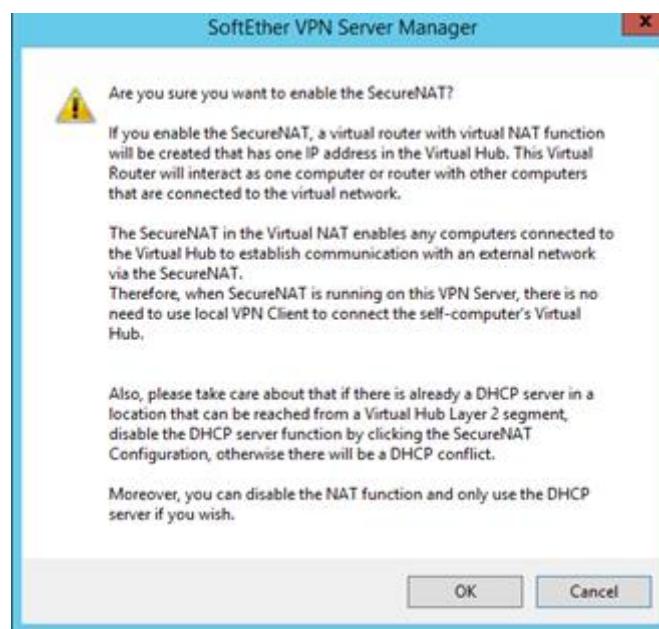


Figure 335 : Enable SecureNAT alert

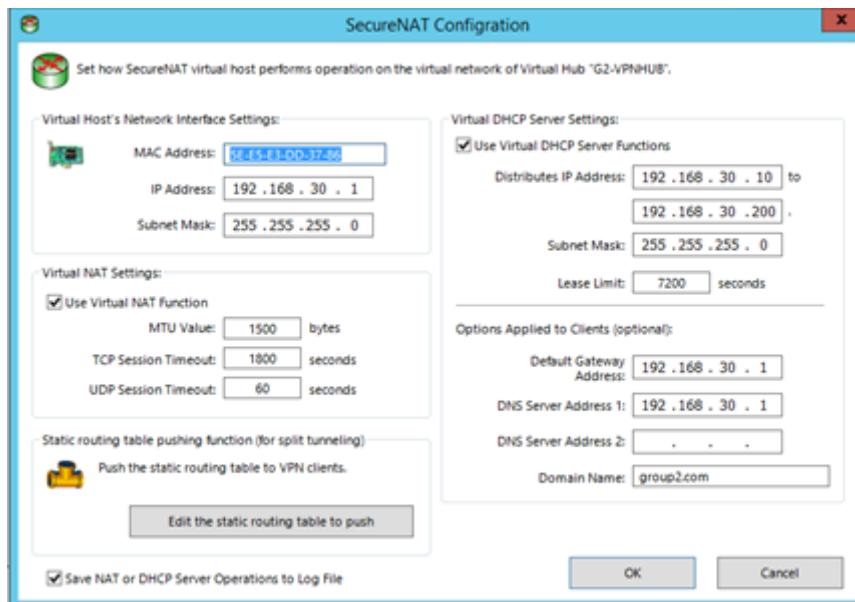


Figure 336 : Ip address provided by SecureNAT

Step 10 : Go back to the Manage VPN Server section, select **Encryption and Network** option.



Figure 337 : Select **Encryption and Network**

Step 11 : Change Encryption Algorithm Name to AES128-SHA and select OK.

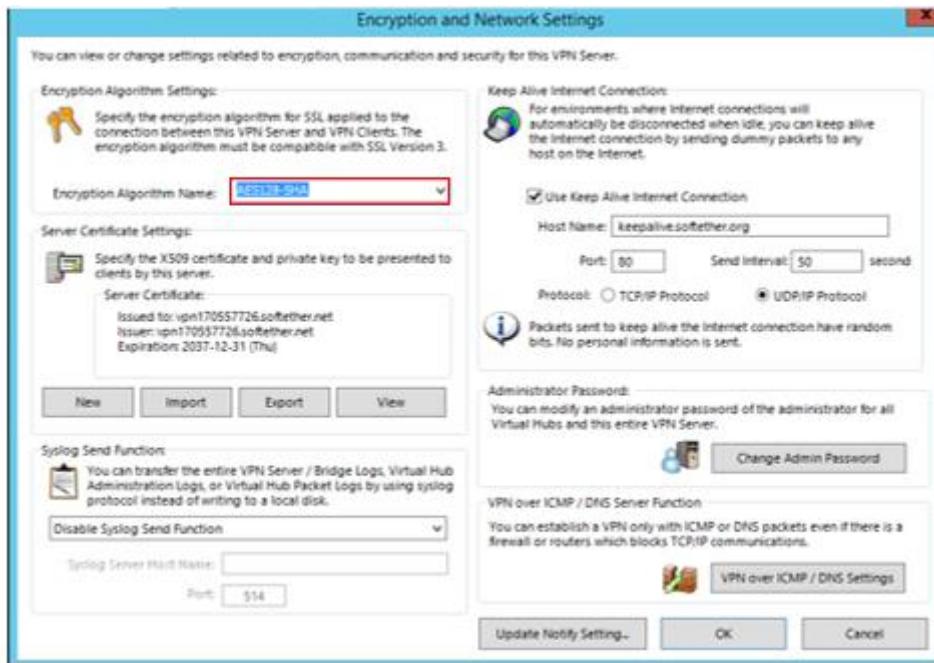


Figure 338 : Modify encryption algorithm name

Step 12 : Go back to Manager VPN Server Section, select IPsec / L2TP Setting.



Figure 339 : Select IPsec / L2TP Setting

Step 13 : The Virtual Hub is created and the VPN server is ready to be connected.



Figure 340 : Virtual Hub is created

## SoftEther VPN Client Installation

Step 1 : Access to <https://www.softether.org/5-download> and select Download button.

The screenshot shows the 'Download - SoftEther VPN ...' page of the SoftEther VPN website. The URL in the address bar is <https://www.softether.org/5-download>. The page has a navigation menu on the left with options like Top, Why SoftEther VPN, Documents, Download, Support, and About Project. The 'Download' option is currently selected. The main content area is titled 'Download' and contains text about the open-source nature of the software and its availability on Windows Azure. It features a prominent red-bordered 'Download SoftEther VPN' button. Below this, there are sections for 'Download from CNET Download.com:' and 'Download from Softpedia.com:', each with a corresponding download link.

Figure 341 : Go to website and click download

Step 2 : Select **Download SoftEther VPN**.

The screenshot shows the official SoftEther VPN download page. It features a large "Download" button at the top left. Below it, a note states that SoftEther VPN is open-source free software. A section titled "Primary Download Server (hosted by Windows Azure)" contains a link to "Download SoftEther VPN". This link is described as being in English, Japanese, and Simplified Chinese, and available for Windows, Linux, Mac OS X, FreeBSD, and Solaris. Another section, "Download from CNET Download.com:", also provides a link to download the software.

Figure 342 : Download SoftEther VPN

Step 3 : Select the Software, Component, Platform and CPU according to your requirement and begin to download.

The screenshot shows a user interface for selecting download requirements. It includes dropdown menus for "Select Software" (set to "SoftEther VPN (Freeware)"), "Select Component" (set to "SoftEther VPN Client"), "Select Platform" (set to "Windows"), and "Select CPU" (set to "Intel (x86 and x64)"). Below these, a "Download Files (72)" section lists a single item: "SoftEther VPN Client (Ver 4.30, Build 9696, beta)". This item has a note about its network functions and a warning about anti-virus software. It also includes a "Release Date: 2019-07-08 <Latest Build>" link, a "What's new (ChangeLog)" link, and details about supported languages (English, Japanese, Simplified Chinese) and operating systems (Windows, Intel x86 and x64).

Figure 343 : Choose requirement

Step 4 : Execute the installer that have been downloaded. A Welcome Page will be shown and click **Next**.

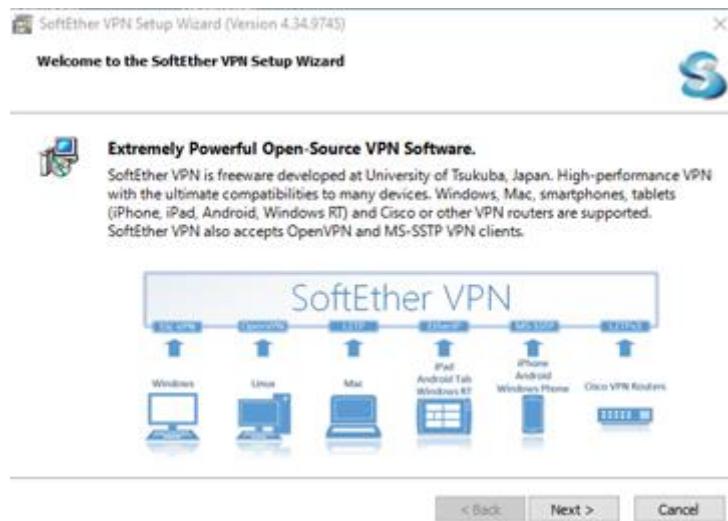


Figure 344 : Download section

Step 5 : Then, select **SoftEther VPN Client** and select Next.

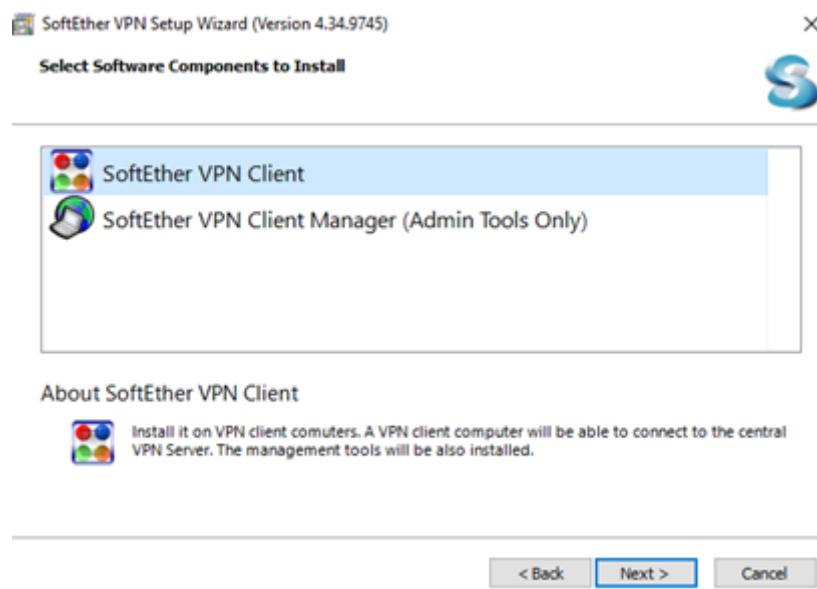


Figure 345 : Choose software component to install

Step 6 : Tick **Agree** to the User License Agreement and select **Next**.

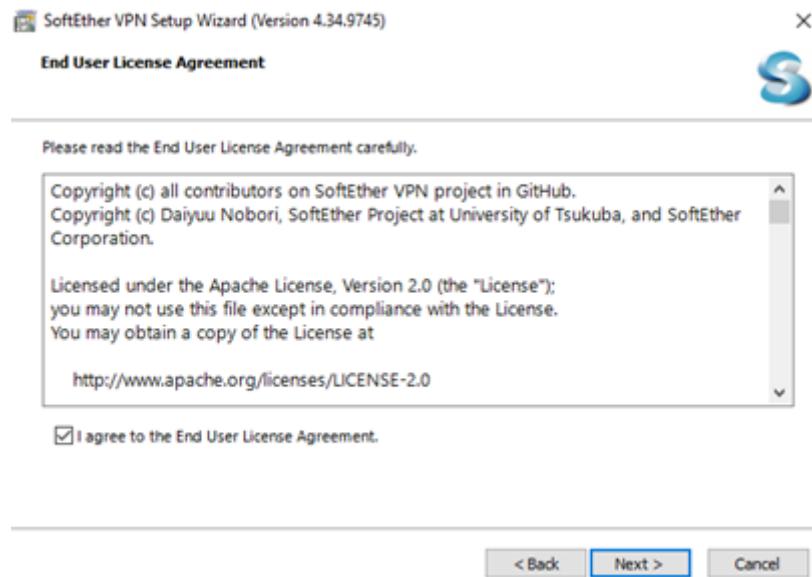


Figure 346 : Agree to End user Agreement

Step 7 : Click **Next** to proceed to select file path to store SoftEther VPN Server.

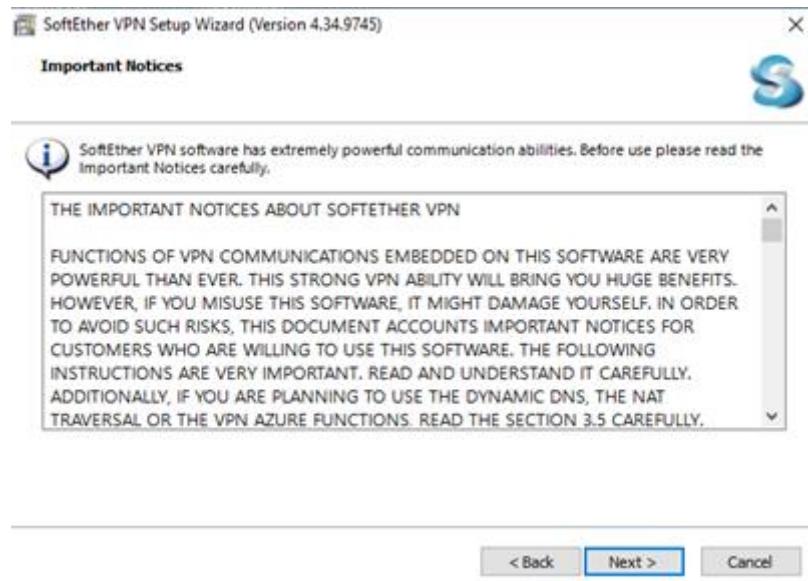


Figure 347 : Important Notice

Step 8 : Select the file path that you wish to store SoftEther VPN Server file and select **Next**.

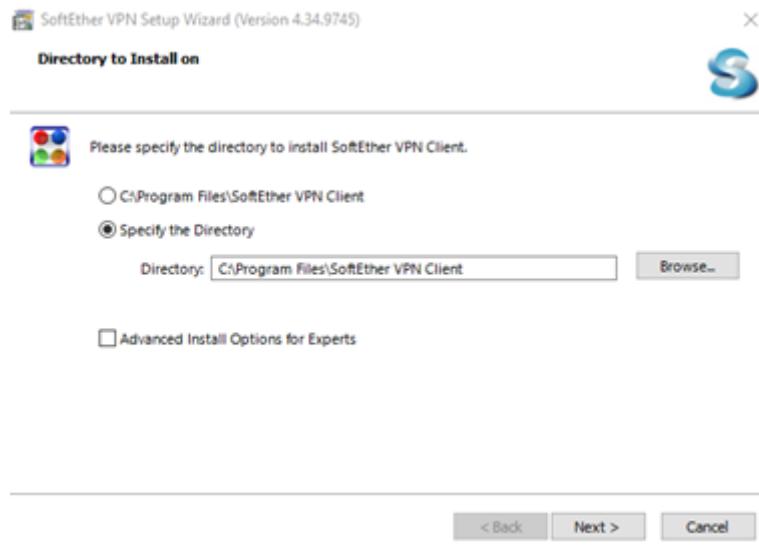


Figure 348 : Path Selection

Step 9 : Then, select **Next** and wait for the SoftEther VPN Server installation to complete and click **Finish**.

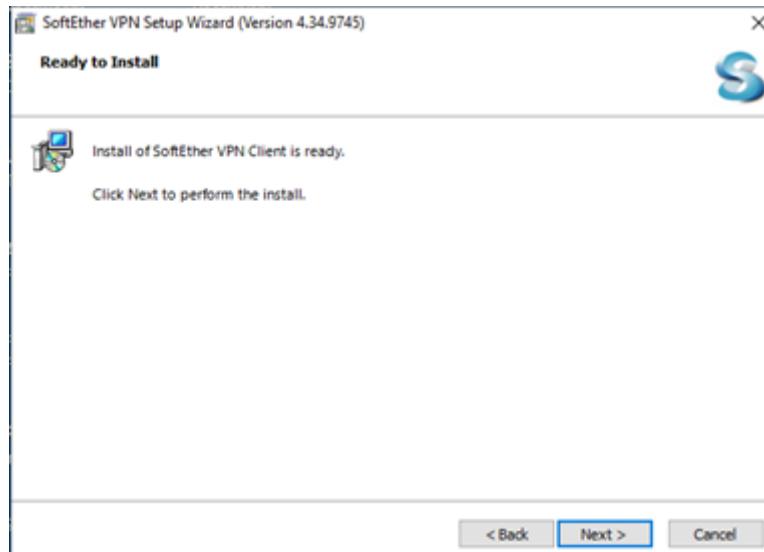


Figure 349 : Wait for installation

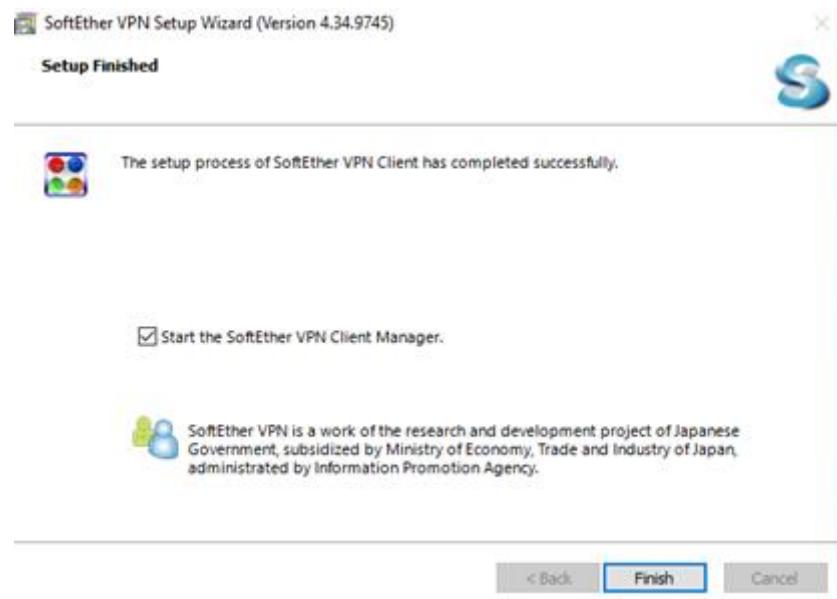


Figure 350 : Finish installation

## Configuration of SoftEther VPN Client on Client HQ

Step 1 : Open the SoftEther VPN Client Manager. Select Add VPN Connection and Hit Yes.

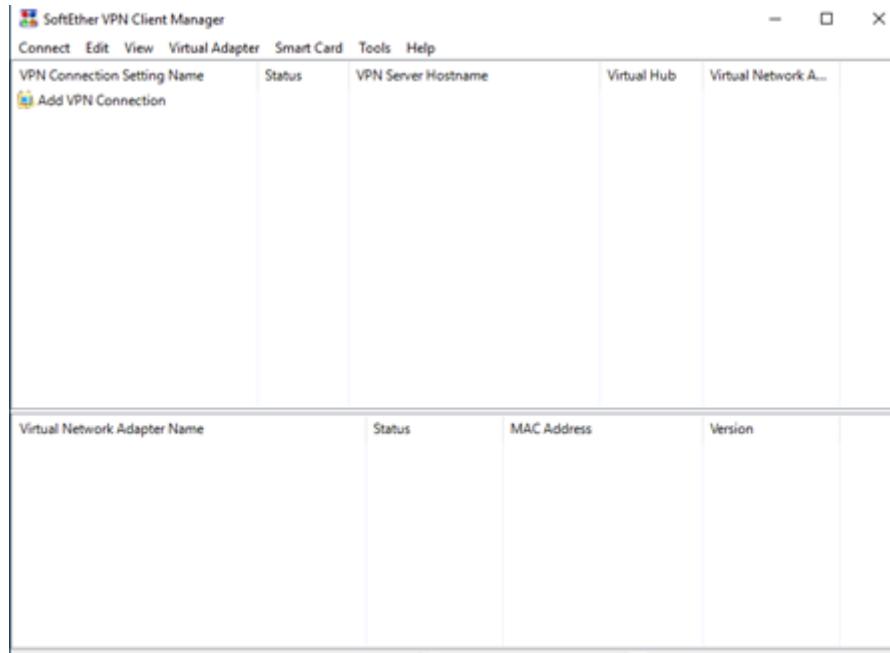
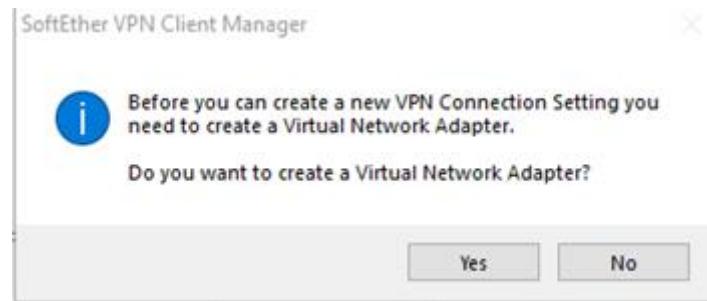
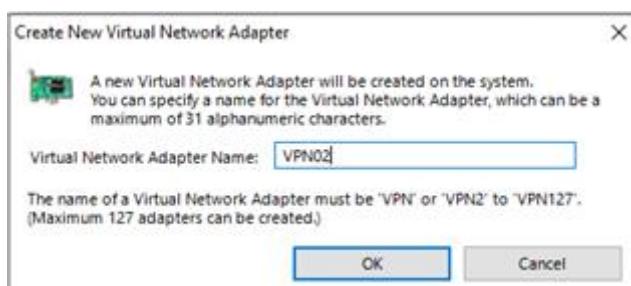


Figure 351 : GUI of SoftEther VPN Client Manager



*Figure 352 : Create new Virtual Network Adapter*

Step 2 : Change the name as ( VPN02 ). Click OK button.



*Figure 353 : Set up Virtual Network Adapter name*

Step 3 : Then, a new virtual network adapter name will appear on bottom section with mac address, status and other information.

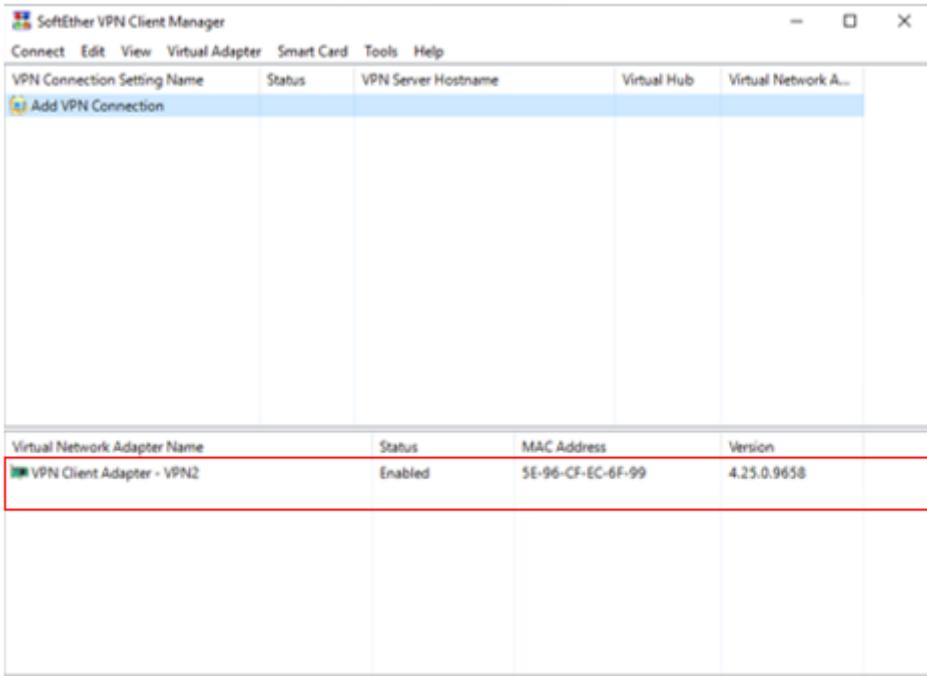


Figure 354 : New virtual network adapter

Step 4 : Next, select Add VPN Connection again, a New VPN Connection Setting Properties window will pop out. Change the Setting Name as ( G2-VPNConnect ), Host Name as < SoftEther VPN Server IP Address >, Port 5555 and Virtual Hub name as ( G2-VPNHUB ). On User Authentication Settings, change Auth Type to Standard Password Authentication and insert the username ( G2-VPNClient01 ) and password that want to be login. Lastly, click the OK button.

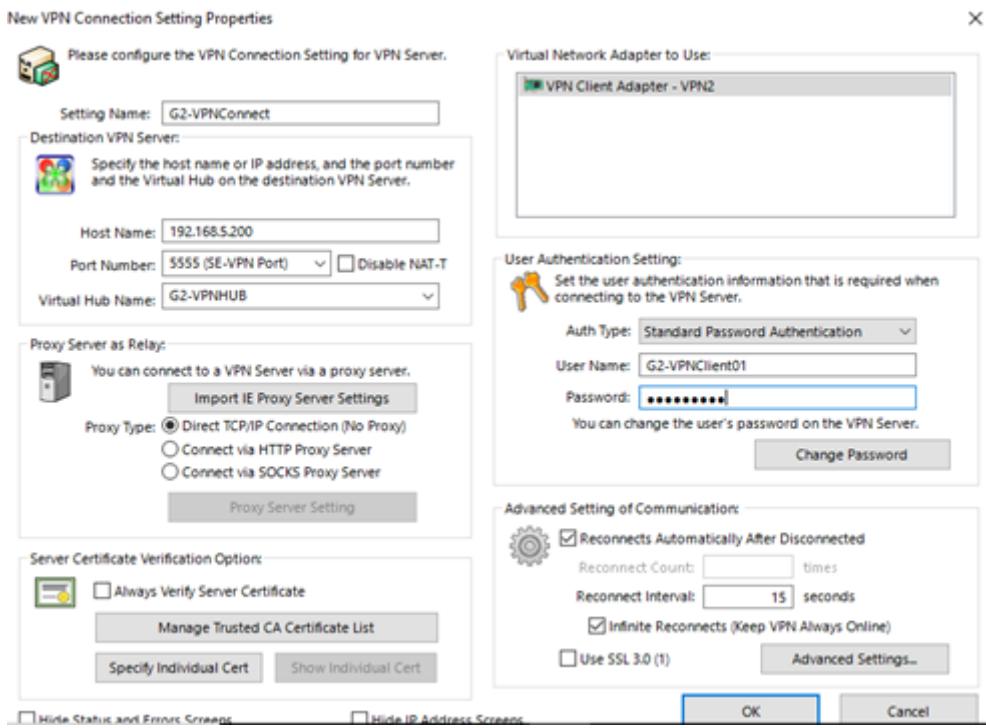


Figure 355 : Set up VPN Connection

Step 5 : Success to create a New VPN Connection.

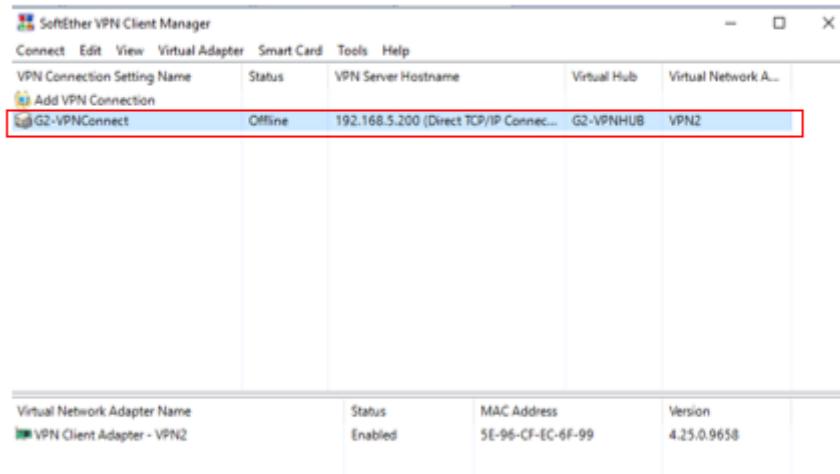


Figure 356 : VPN Connection created

## Configuration of SoftEther VPN Client on Client Branch

Step 1 : Open the SoftEther VPN Client Manager. Select Add VPN Connection and Hit Yes.

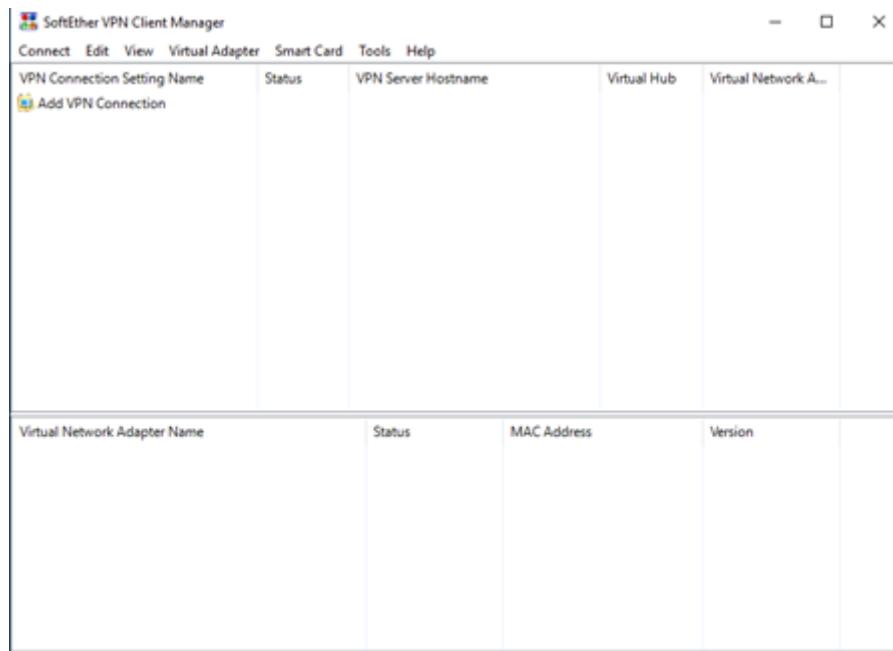


Figure 357 : GUI of SoftEther VPN Client Manager



Figure 358 : Create new Virtual Network Adapter

Step 2 : Change the name as ( VPN03 ). Click OK button.



Figure 359 : Set up Virtual Network Adapter name

Step 3 : Then, a new virtual network adapter name will appear on bottom section with mac address, status and other information.

Virtual Network Adapter Name	Status	MAC Address	Version
VPN Client Adapter - VPN3	Enabled	5E-08-F5-F4-F2-0A	4.25.0.9658

SoftEther VPN Client Manager Not Connected SoftEther VPN Client Build 9745

Figure 360 : New virtual network adapter

Step 4 : Next, select Add VPN Connection again, a New VPN Connection Setting Properties window will pop out. Change the Setting Name as ( G2-VPNConnect ), Host Name as < SoftEther VPN Server IP Address >, Port 5555 and Virtual Hub name as ( G2-VPNHUB ). On User Authentication Settings, change Auth Type to Standard Password Authentication and insert the username ( G2-VPNClient01 ) and password that want to be login. Lastly, click the OK button.

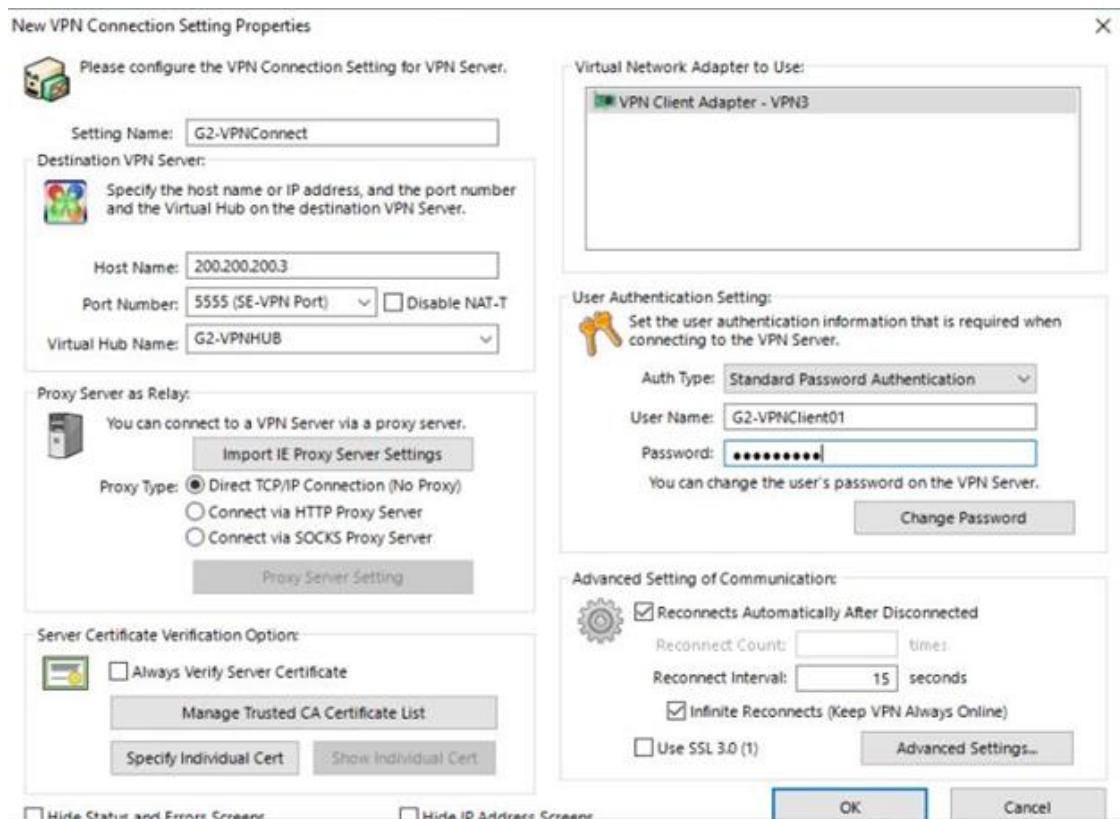


Figure 361 : Set up VPN Connection

Step 5 : Success to create a New VPN Connection.

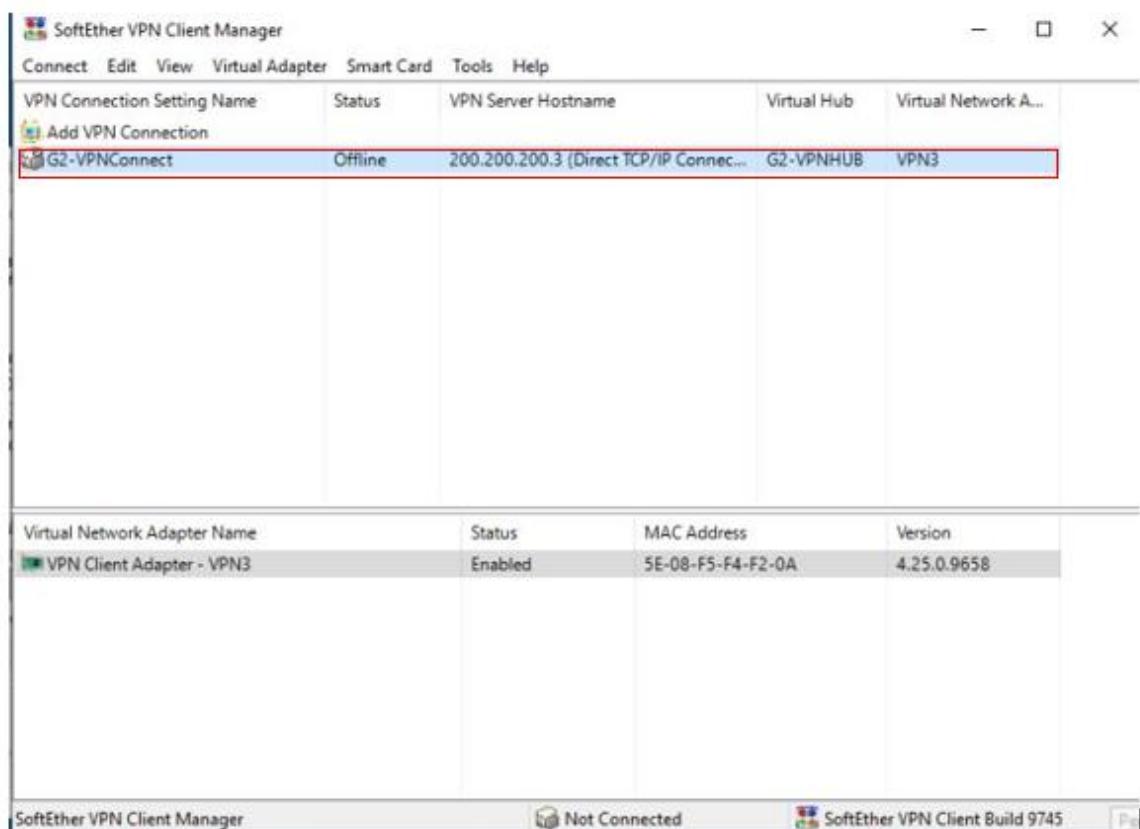


Figure 362 : VPN Connection created

### 5.3.16 USER AUTHENTICATION BY INTEGRATING AD WITH LINUX

Step 1 : Update the server with the command ***apt-get update***



A screenshot of a terminal window titled "root@lubuntugrp2: ~". The window has standard Linux window controls (minimize, maximize, close) at the top right. The menu bar includes "File", "Edit", "Tabs", and "Help". The main area of the terminal shows the command "root@lubuntugrp2:~# apt-get update" entered by the user. The terminal is currently empty, indicating no output has been displayed.

Figure 363 : Lubuntu Server Update

Step 2 : Upgrade the server with the command ***apt-get upgrade***



A screenshot of a terminal window titled "root@lubuntugrp2: ~". The window has standard Linux window controls (minimize, maximize, close) at the top right. The menu bar includes "File", "Edit", "Tabs", and "Help". The main area of the terminal shows the command "root@lubuntugrp2:~# apt-get update" entered by the user. The terminal is currently empty, indicating no output has been displayed.

Figure 364 : Lubuntu Server Upgrade

Step 3 : Download the PowerBroker Identity Services (PBIS) package from GitHub

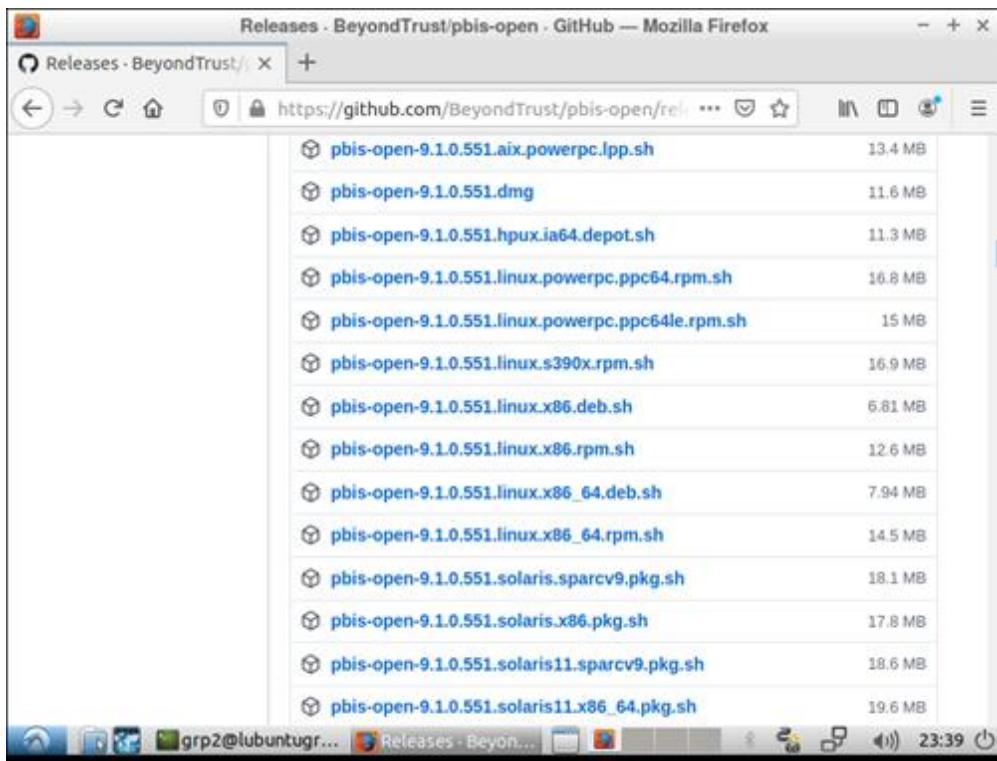


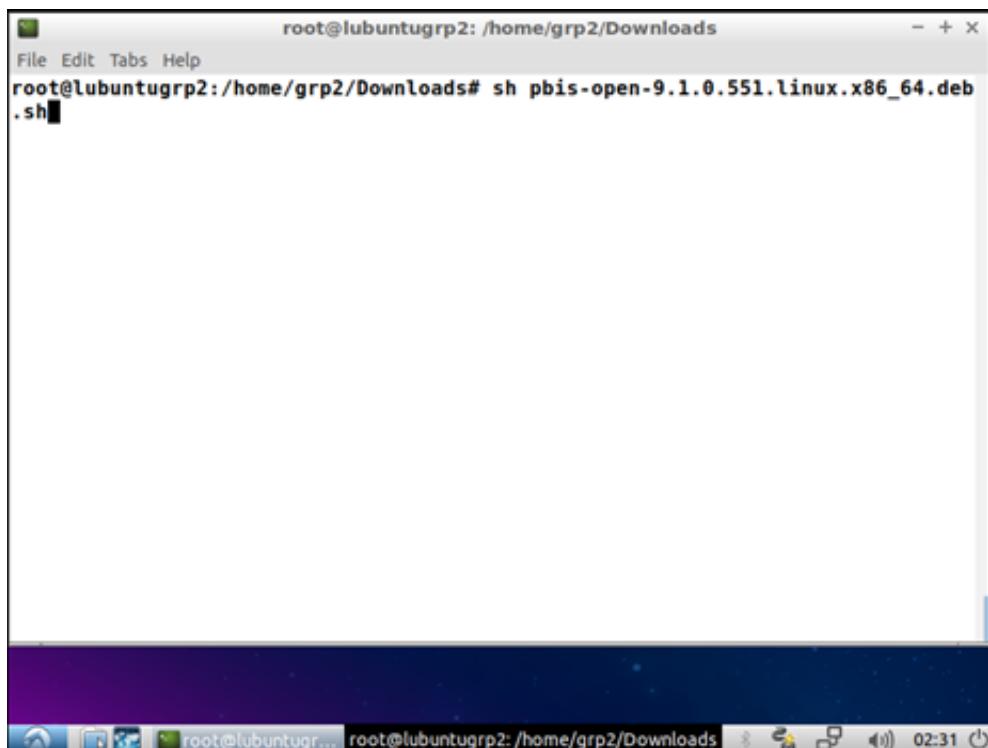
Figure 365 : Download the PBIS from GitHub

Step 4 : Change the permission for downloaded PBIS package into read, write and execute permission with command **chmod 777 pbis-open-9.1.0.551.linux.x86\_64.deb.sh**

```
root@lubuntugrp2: /home/grp2/Downloads
File Edit Tabs Help
root@lubuntugrp2:/home/grp2/Downloads# chmod 777 pbis-open-9.1.0.551.linux.x86_64.deb.sh
```

Figure 366 : Permission changes for downloaded PBIS package

Step 5 : Install the PBIS with command `sh pbis-open-9.1.0.551.linux.x86_64.deb.sh`



A terminal window titled "root@lubuntugrp2: /home/grp2/Downloads". The command entered is "sh pbis-open-9.1.0.551.linux.x86\_64.deb.sh". The window shows a progress bar at the bottom.

Figure 367 : Installation of PBIS

Step 6 : Create an Active Directory group named group2IntegrateAD which will integrate with Linux and add and include some users in the group in Windows Server

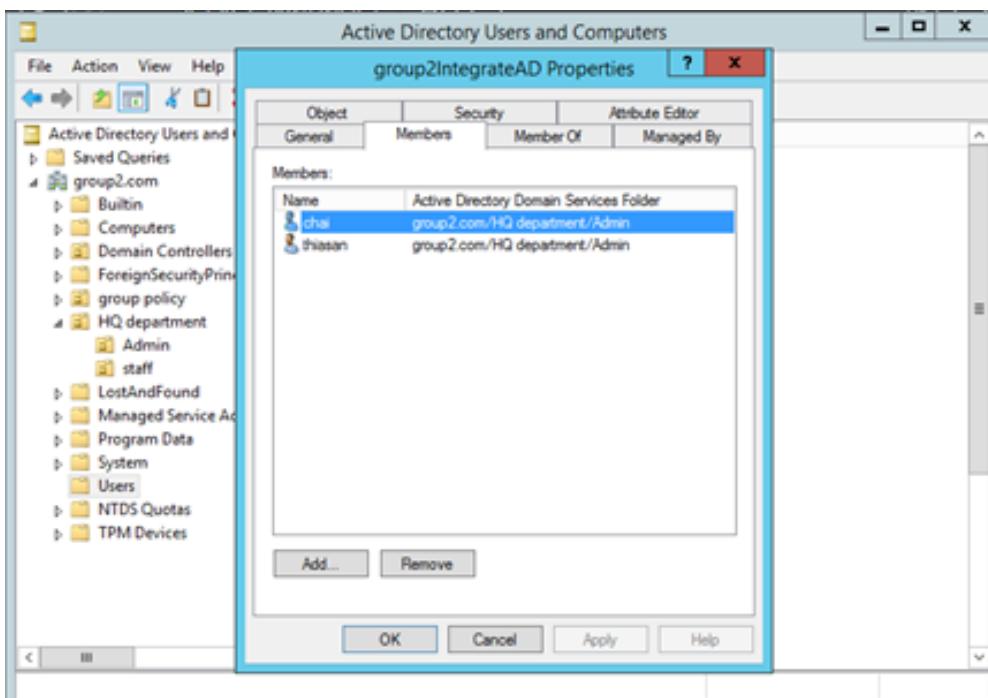
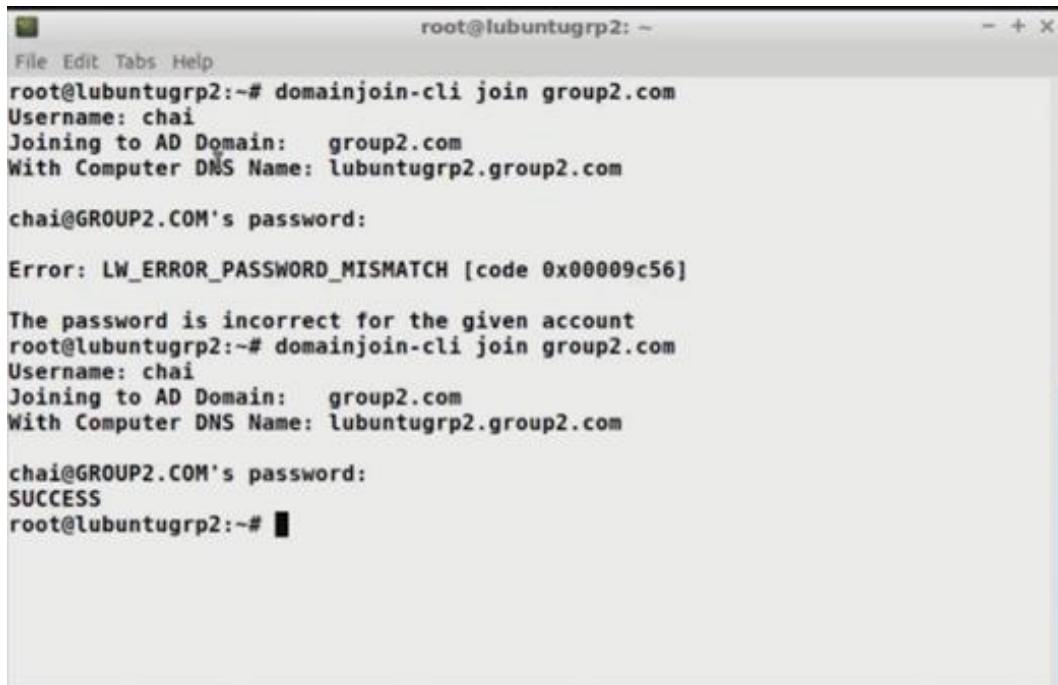


Figure 368 : AD group with users created

Step 7 : Join the Lubuntu system with Windows Active Directory to integrate the Active Directory with the created user with command ***domainjoin-cli join group2.com***

A “SUCCESS” message will be shown if the domain join is success



The image shows a terminal window titled "root@lubuntugrp2: ~" with a gray header bar containing "File Edit Tabs Help". The main area of the terminal displays the following command and its execution:

```
root@lubuntugrp2:~# domainjoin-cli join group2.com
Username: chai
Joining to AD Domain: group2.com
With Computer DNS Name: lubuntugrp2.group2.com

chai@GROUP2.COM's password:

Error: LW_ERROR_PASSWORD_MISMATCH [code 0x000009c56]

The password is incorrect for the given account
root@lubuntugrp2:~# domainjoin-cli join group2.com
Username: chai
Joining to AD Domain: group2.com
With Computer DNS Name: lubuntugrp2.group2.com

chai@GROUP2.COM's password:
SUCCESS
root@lubuntugrp2:~# ■
```

Figure 369 : Domain Joining Between Lubuntu server and Windows Active Directory

Step 8 : Setup the Active Directory login settings with the commands

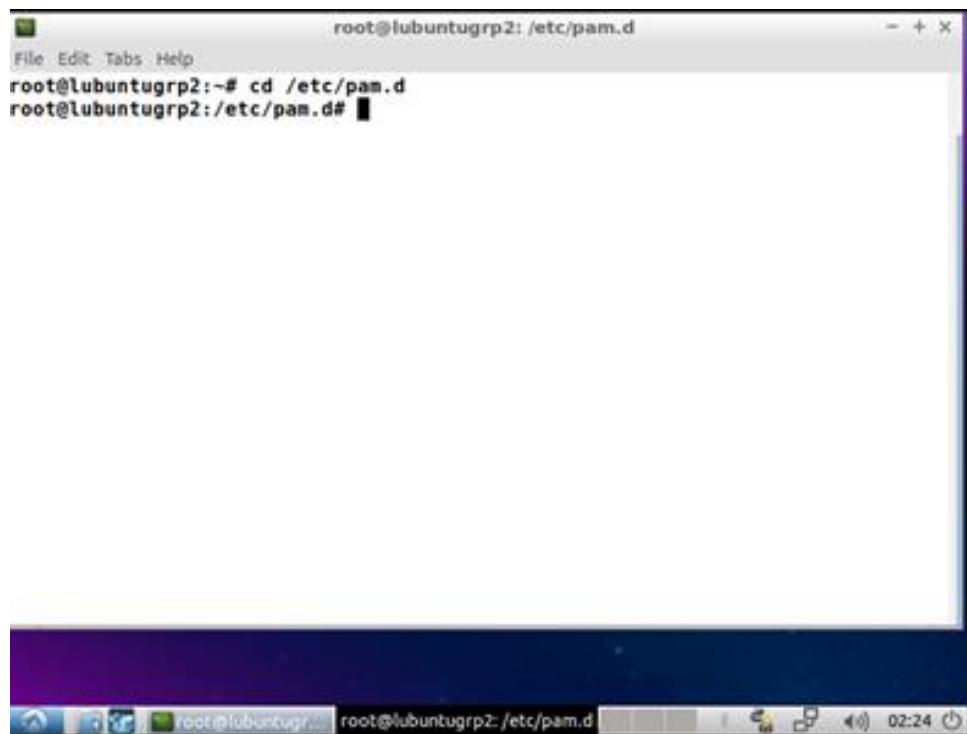
```
./config UserDomainPrefix group2.com  
./config AssumeDefaultDomain True  
./config LoginShellTemplate /bin/bash  
./config HomeDirTemplate %H/%D/%U  
./config RequireMembershipOf group2.com\group2IntegrateAD
```

The screenshot shows a terminal window titled "root@lubuntugrp2: /etc/pam.d". The terminal displays the following text:

```
File Edit Tabs Help  
aiman@GROUP2.COM's password:  
Warning: System restart required  
Your system has been configured to authenticate to Active Directory for the  
first time. It is recommended that you restart your system to ensure that  
all applications recognize the new settings.  
  
SUCCESS  
root@lubuntugrp2:~# cd /opt/pbis/bin  
root@lubuntugrp2:/opt/pbis/bin# sudo domainjoin-cli join group2.com  
Username: aiman  
Joining to AD Domain: group2.com  
With Computer DNS Name: lubuntugrp2.group2.com  
  
aiman@GROUP2.COM's password:  
SUCCESS  
root@lubuntugrp2:/opt/pbis/bin# ./config UserDomainPrefix group2.com  
root@lubuntugrp2:/opt/pbis/bin# ./config AssumeDefaultDomain True  
root@lubuntugrp2:/opt/pbis/bin# ./config LoginShellTemplate /bin/bash  
root@lubuntugrp2:/opt/pbis/bin# ./config HomeDirTemplate %H/%D/%U  
root@lubuntugrp2:/opt/pbis/bin# ./config RequireMembershipOf group2.com\group2IntegrateAD  
root@lubuntugrp2:/opt/pbis/bin# cd /etc/pam.d/  
root@lubuntugrp2:/etc/pam.d# nano common-session  
root@lubuntugrp2:/etc/pam.d# █
```

Figure 370 : Login Settings

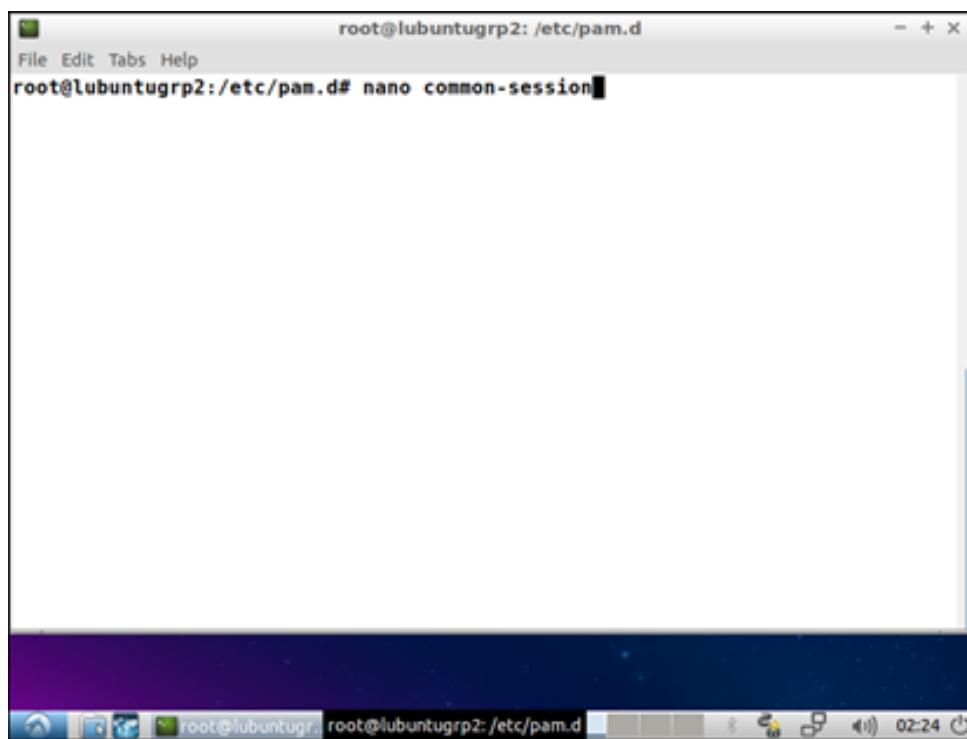
Step 9 : Change to the pam.d directory with command ***cd /etc/pam.d***



A screenshot of a terminal window titled "root@lubuntugrp2: /etc/pam.d". The window shows the command "root@lubuntugrp2:~# cd /etc/pam.d" being typed. The terminal is running on a Lubuntu desktop environment, as indicated by the window title and the desktop icons visible in the background.

Figure 371 : Change to pam.d directory

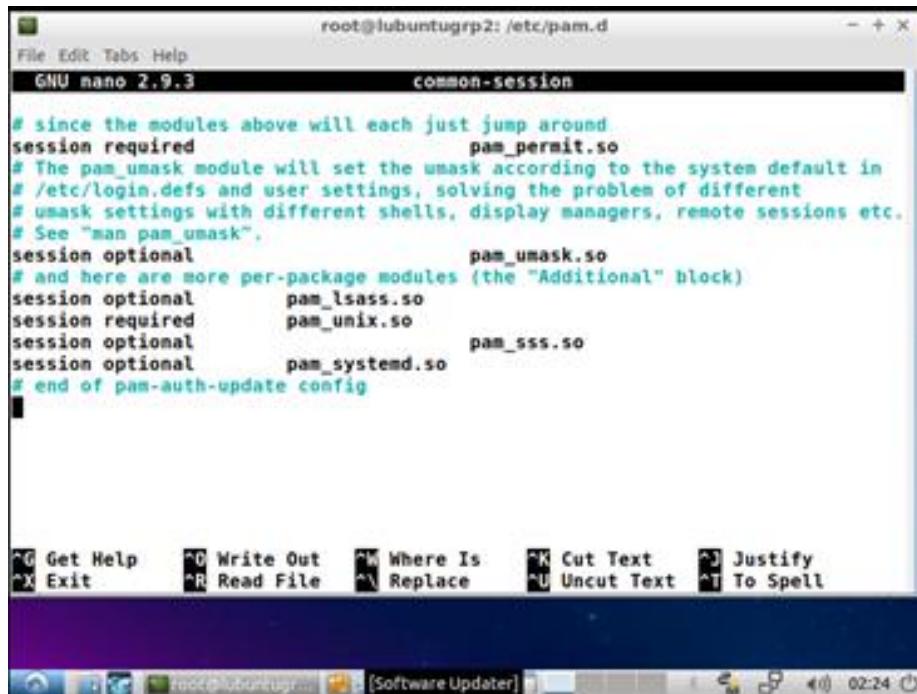
Step 10 : Open the pam.d common-session file with command ***nano common-session***



A screenshot of a terminal window titled "root@lubuntugrp2: /etc/pam.d". The window shows the command "root@lubuntugrp2:/etc/pam.d# nano common-session" being typed. The terminal is running on a Lubuntu desktop environment, as indicated by the window title and the desktop icons visible in the background.

Figure 372 : Open the common-session configuration file

Step 11 : Edit the common-session configuration file with adding the line as shown in the figure below

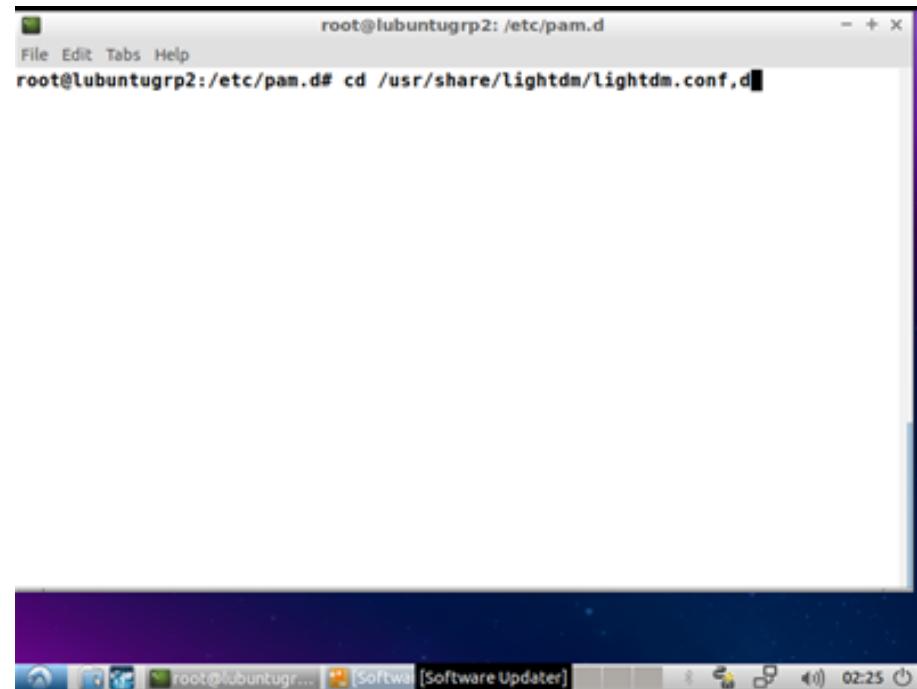


```
root@lubuntugrp2: /etc/pam.d
File Edit Tabs Help
GNU nano 2.9.3           common-session

# 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 optional           pam_lsass.so
session required            pam_unix.so
session optional            pam_sss.so
session optional            pam_systemd.so
# end of pam-auth-update config
```

Figure 373 : Edited common-session configuration file

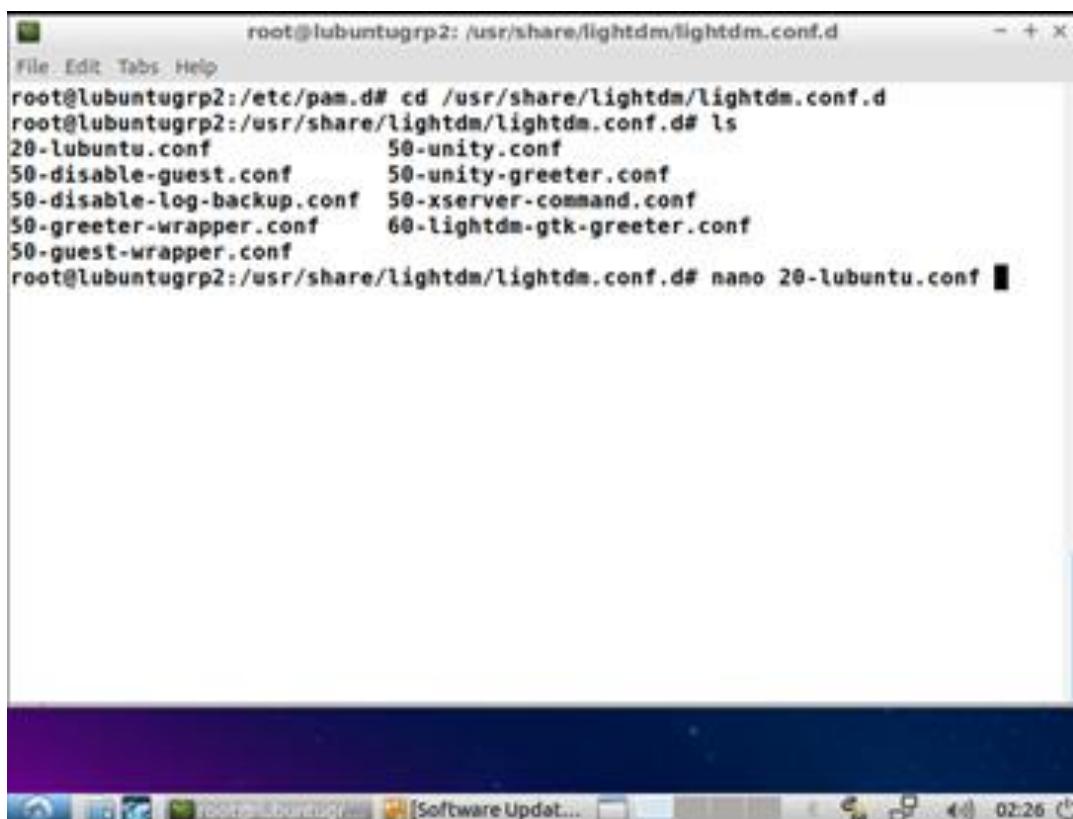
Step 12 : Change to the lightdm.conf.d directory with command **cd /usr/share/lightdm/lightdm.conf.d**



```
root@lubuntugrp2: /etc/pam.d
File Edit Tabs Help
root@lubuntugrp2:/etc/pam.d# cd /usr/share/lightdm/lightdm.conf.d
```

Figure 374 : Change directory to lightdm.conf.d

Step 13 : Open the configuration file with command ***nano 20-lubuntu.conf***



```
root@lubuntugrp2: /usr/share/lightdm/lightdm.conf.d - + x
File Edit Tabs Help
root@lubuntugrp2:/etc/pam.d# cd /usr/share/lightdm/lightdm.conf.d
root@lubuntugrp2:/usr/share/lightdm/lightdm.conf.d# ls
20-lubuntu.conf      50-unity.conf
50-disable-guest.conf 50-unity-greeter.conf
50-disable-log-backup.conf 50-xserver-command.conf
50-greeter-wrapper.conf 60-lightdm-gtk-greeter.conf
50-guest-wrapper.conf
root@lubuntugrp2:/usr/share/lightdm/lightdm.conf.d# nano 20-lubuntu.conf ■
```

*Figure x : Open lightdm.conf.d configuration file*

Step 14 : Edit the configuration file with command

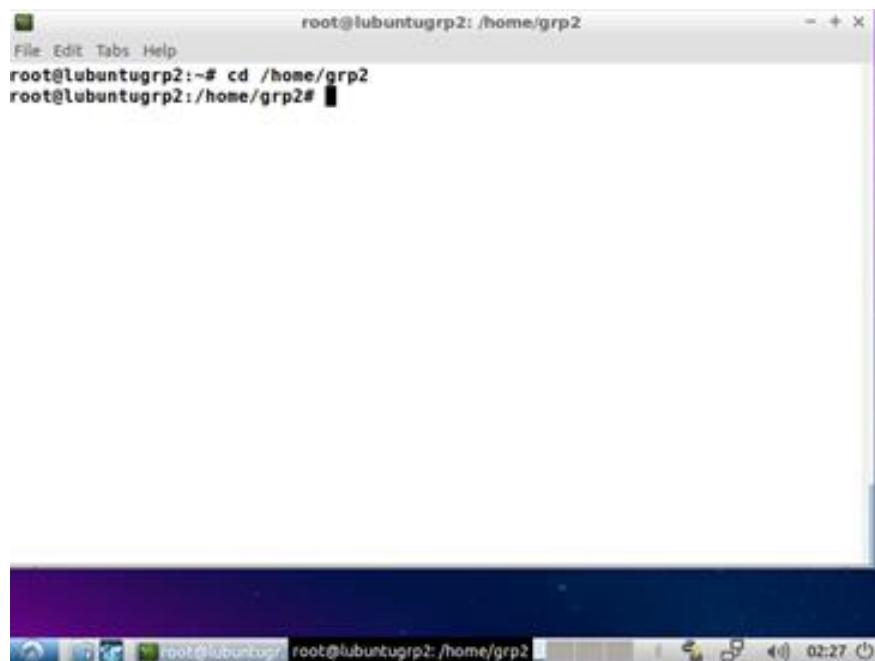
```
user-session=Lubuntu  
allow-guest=false  
greeter-show-manual-login=true
```



```
[Seat:*]  
user-session=Lubuntu  
allow-guest=false  
greeter-show-manual-login=true
```

Figure 375 : Configured lightdm.conf.d configuration file

Step 15 : Change to the home directory of the user `cd /home/grp2`



```
root@lubuntugrp2:~# cd /home/grp2  
root@lubuntugrp2:/home/grp2#
```

Figure 376 : Change the directory file to /home/grp2

Step 16 : Open the sudoers file with command **visudo**

(This is to enable integrated Active Directory Users to have and use sudo permission)

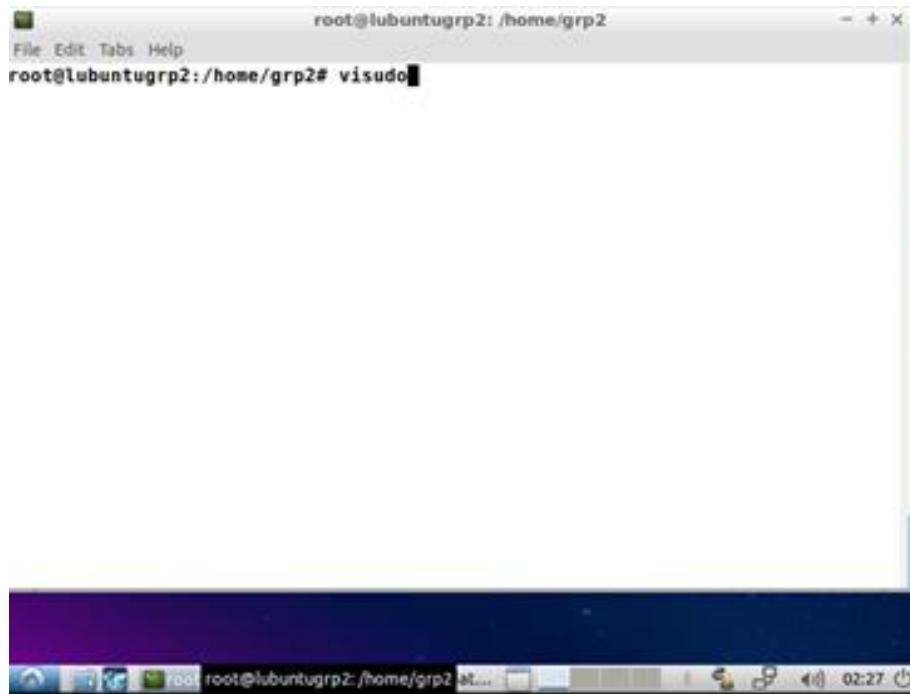


Figure 377 : Open the sudoers configuration file

Step 17 : Edit and update the permission in the configuration file as shown in figure below

```
# Members of the admin group may gain root privileges
%admin  ALL=(ALL)    ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL)  ALL
%GROUP2\group2integratead  ALL=(ALL:ALL)    ALL

# See sudoers(5) for more information on "#include" directives:
#include /etc/sudoers.d
```

The screenshot shows a terminal window with the title "root@lubuntugrp2: /home/grp2". The window displays the contents of the "/etc/sudoers.tmp" file, which contains the configuration for the sudoers file. It includes sections for the "admin" group and the "GROUP2\group2integratead" group, both allowing all users to run any command as root. A "#include /etc/sudoers.d" directive is also present. The bottom of the window shows a menu bar with various keyboard shortcuts for navigating the text editor.

Figure 378 : Configured sudoers configuration file

Step 18 : Save the configuration file and login with integrated Active Directory users accounts

### 5.3.17 WINDOWS SERVER HARDENING

Step 1 : Open Security Configuration Wizard ( Start > Administrative Tools > Security Configuration Wizard )

This is welcoming page of Security Configuration Wizard. Click next.



Figure 379 : Welcome Page of Security Configuration Wizard

Step 2 : Select Create a new security policy and click Next.

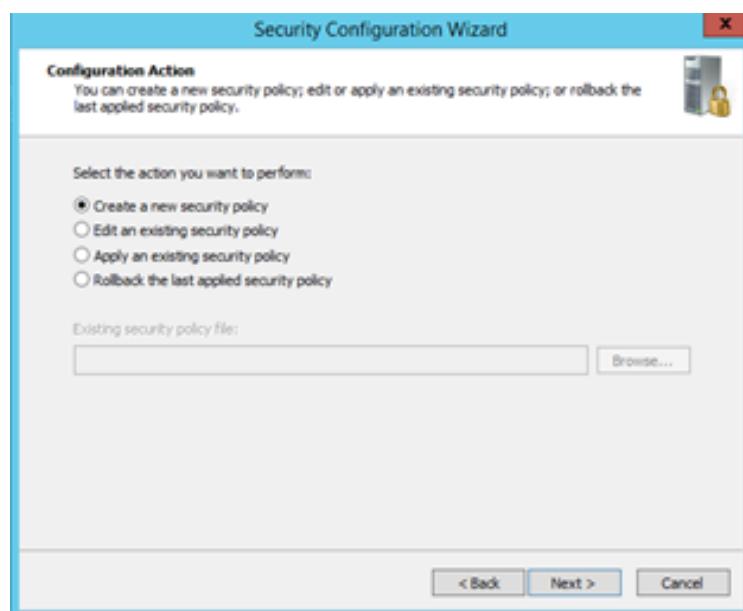


Figure 380 : Configuration Action Tab

Step 3 : Insert the Server Name and click Next.



Figure 381 : Server Selection Tab

Step 4 : Wait until the process complete and click Next.

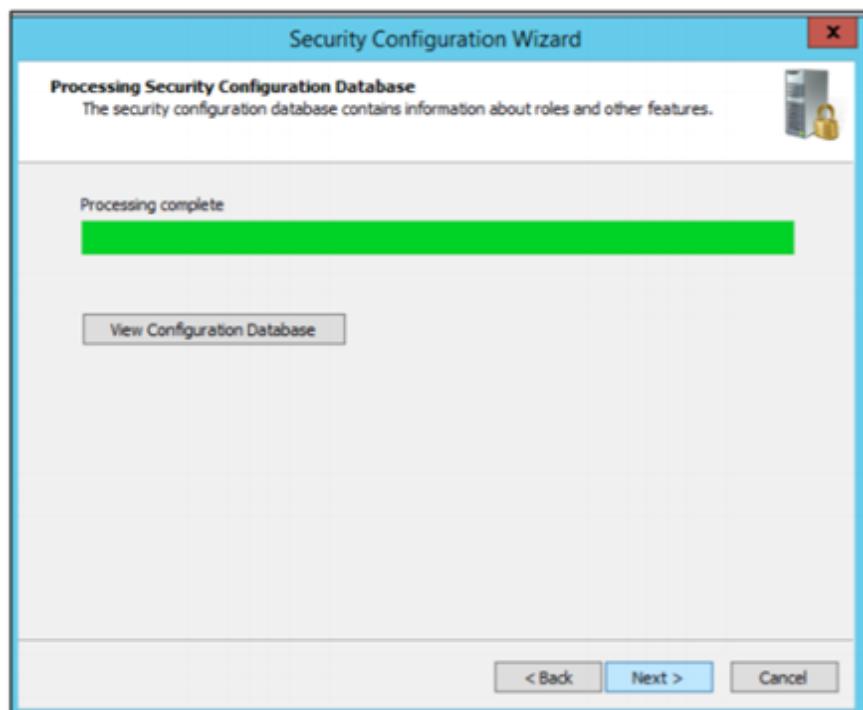


Figure 382 : Completion of Process Tab

Step 5 : This is the welcome page of the Role- Based Service Configuration. Click Next.

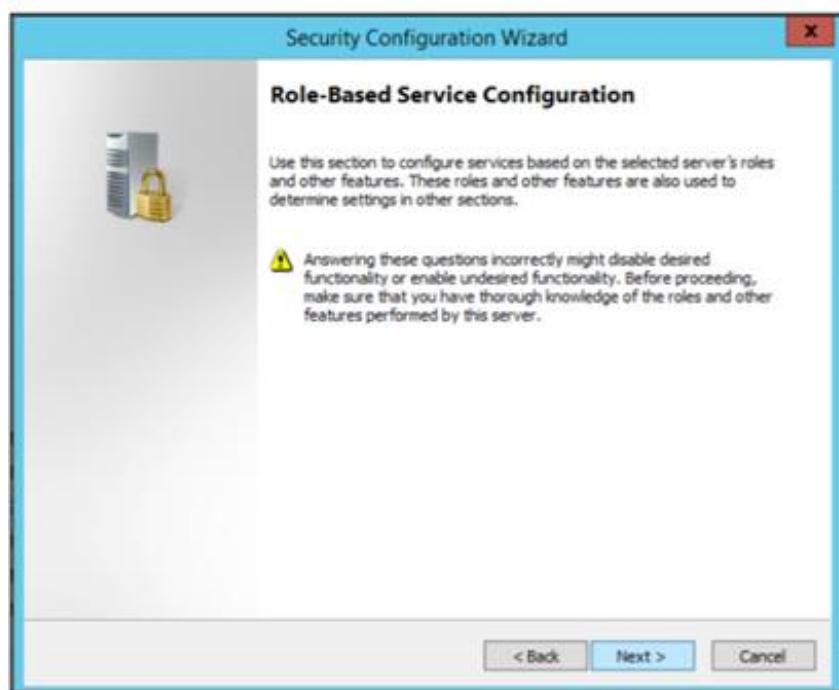


Figure 383 : Welcome Tab of Role-Based Service Configuration

Step 6 : Select the server roles that the server will perform. Click Next.

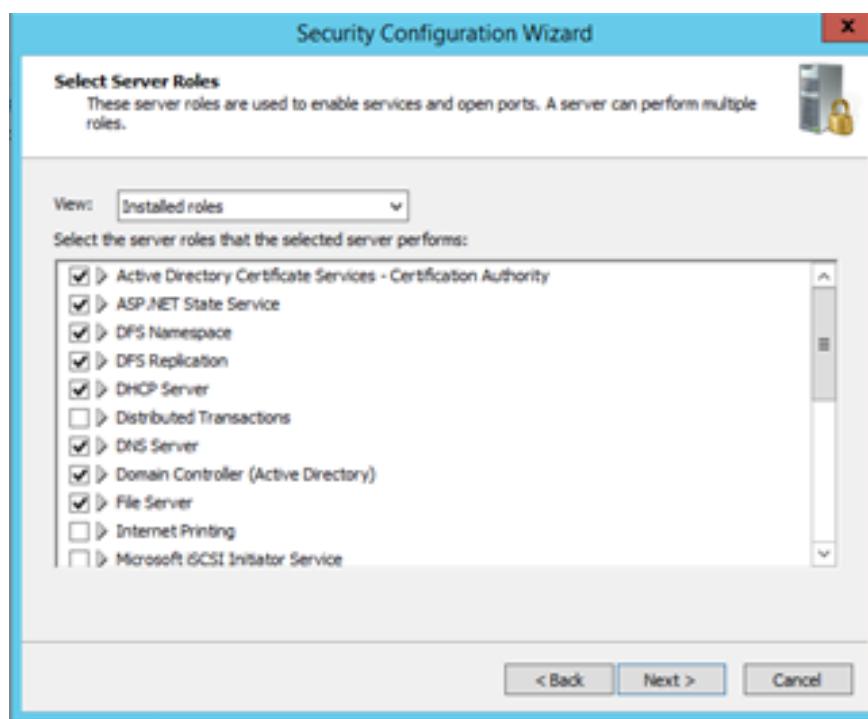


Figure 384 : Server Roles Lists Tab

Step 7 : Select the client features that the server will perform. Click Next.

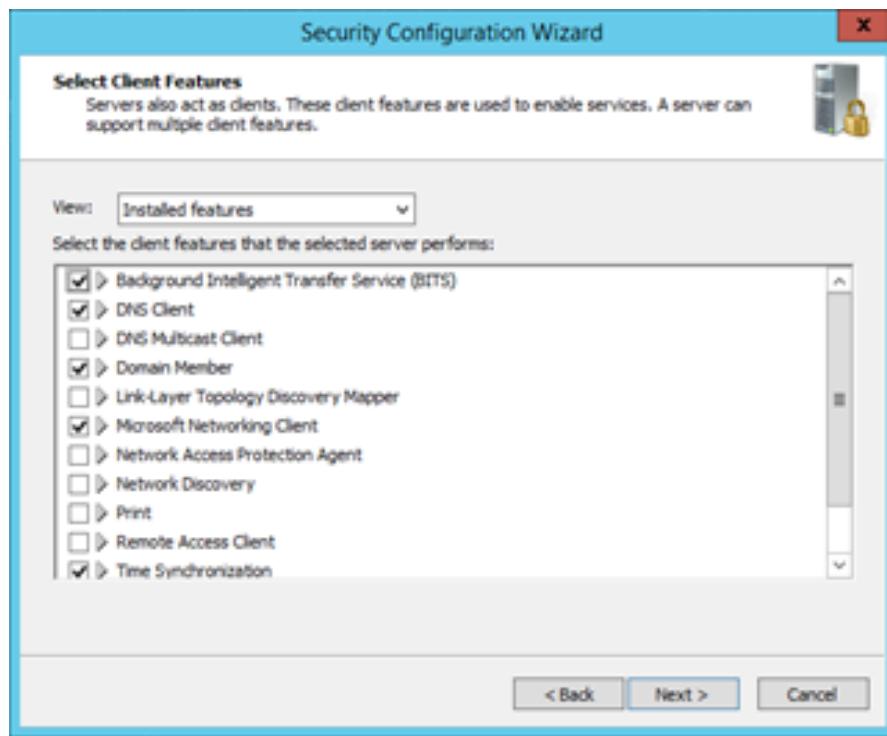


Figure 385 : Client Features Lists Tab

Step 8 : Select the options used to administrate the server. Click Next.

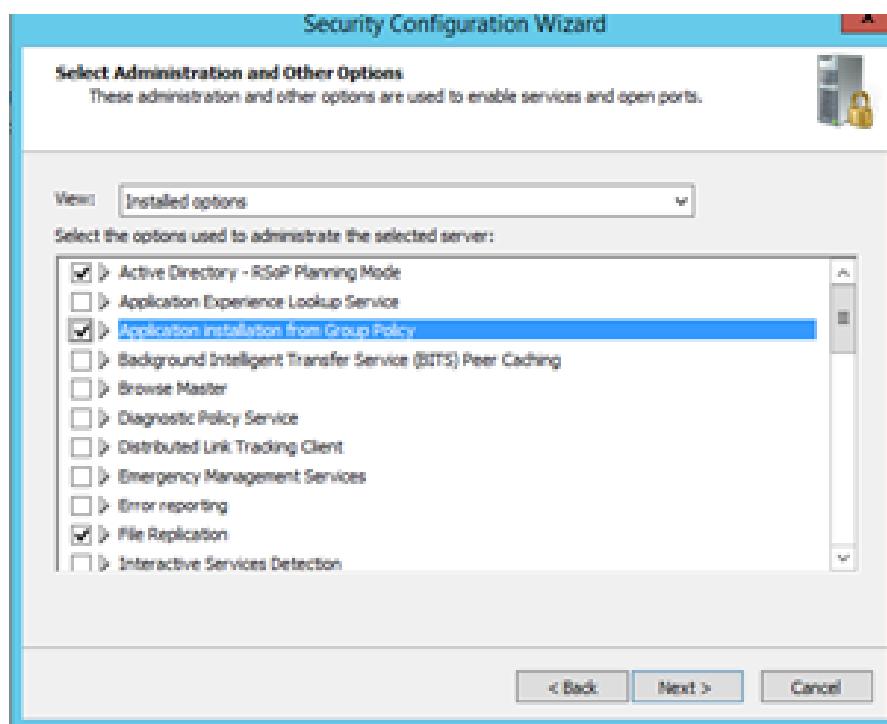


Figure 386 : Administration and Other Options Lists Tab

Step 9 : Select the Do not change the startup mode of the service. Click Next.



Figure 387 : Handling Unspecified Services Tab

Step 10 : Confirm the service changes. Click Next.

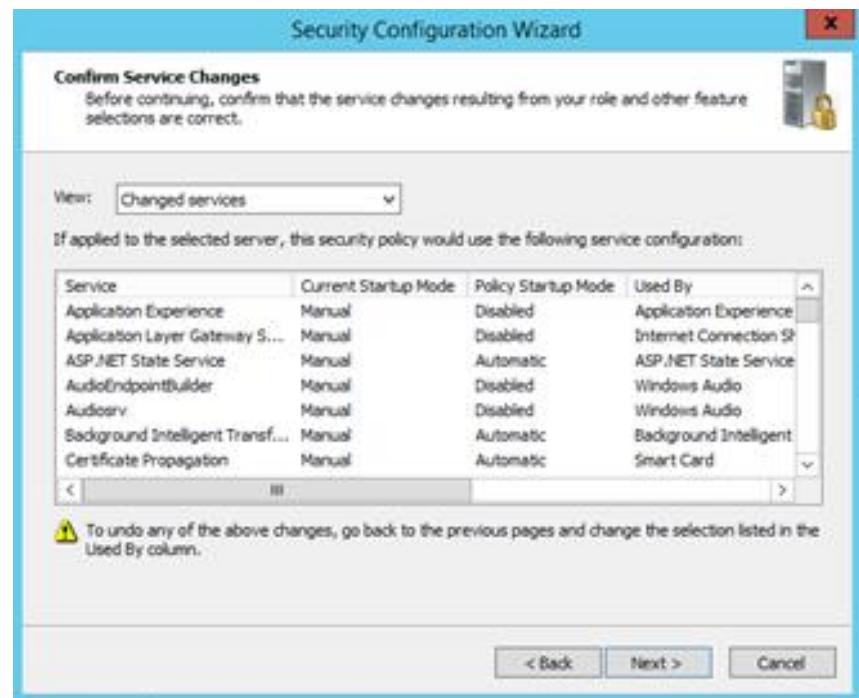


Figure 388 : Confirmation of Service Changes List Tab

Step 11 : This is the welcome page of Network Security. Click Next.



Figure 389 : Welcome page of Network Security Tab

Step 12 : Select the network security rules. Click Next.

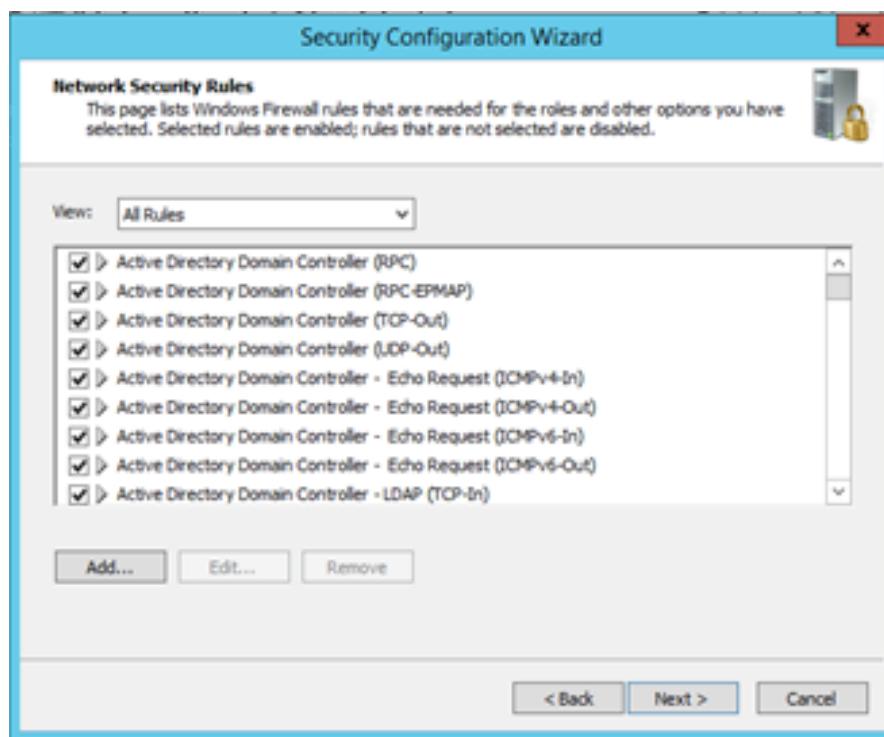


Figure 390 : Network Security Rules Lists Tab

Step 13 : This is the welcome page of Registry Settings. Click Next.



Figure 391 : Welcome page of Registry Settings Tab

Step 14 : Select the attributes that needed for the Server Message Block (SMB) Security Signatures. Click Next.



Figure 392 : SMB Security Signatures Requirement Tab

Step 15 : Determine whether LDAP Signing is require or not by the security policy. Click Next.



Figure 393 : LDAP Signing Requirement Tab

Step 16 : Select the Domain Accounts as the methods the selected user to authenticate with remote computers. Click Next.

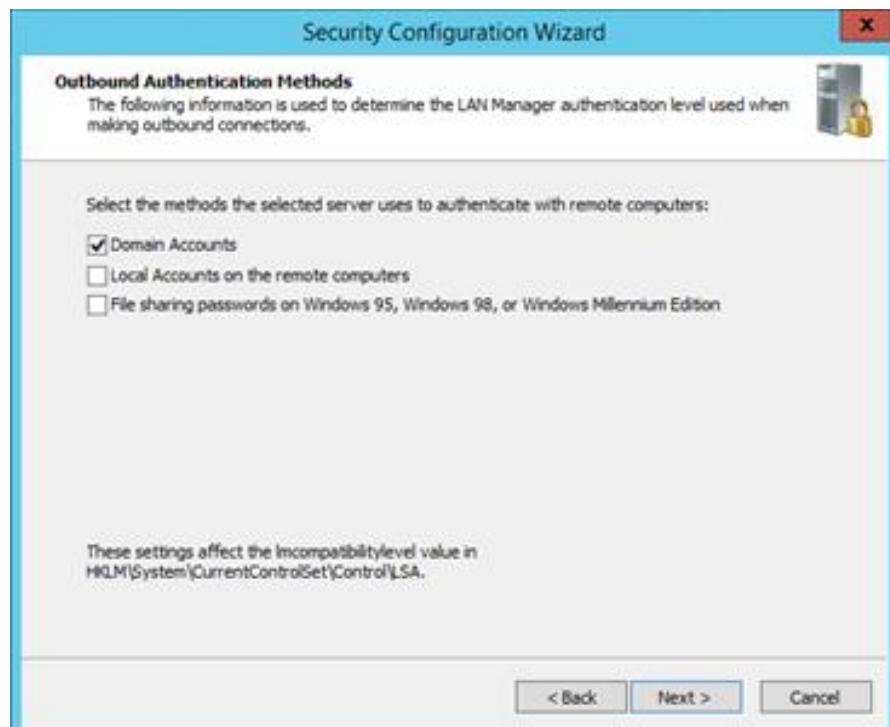


Figure 394 : Outbound Authentication Methods Tab

Step 17 : Select Windows NT 4.0 Service Pack 6a or later operating systems. Click Next.

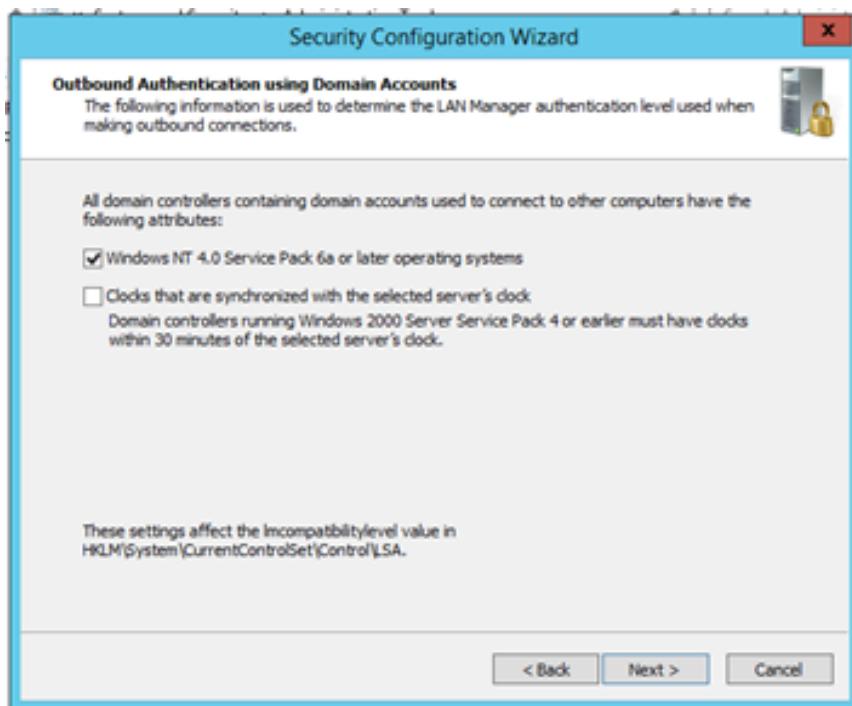


Figure 395 : Attributes Selection of Outbound Authentication using Domain Accounts Tab

Step 18 : This is summary of registry settings. Click Next.

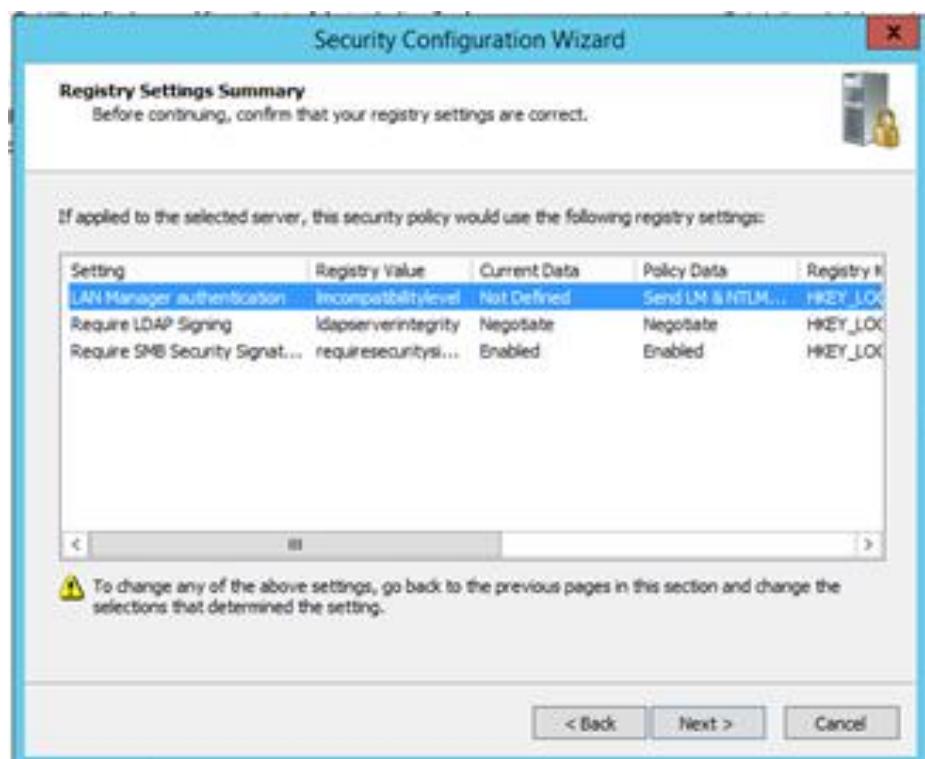


Figure 396 : Summary of Registry Settings Tab

Step 19 : This is welcome page of Audit Policy. Click Next.

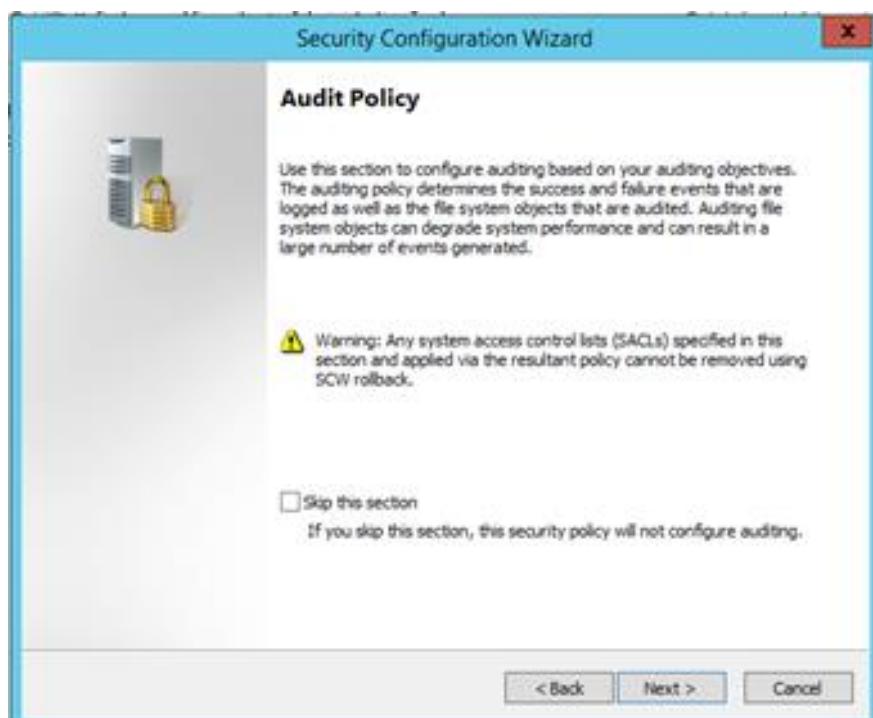


Figure 397 : Welcome page for Audit Policy Tab

Step 20 : Select Audit successful and unsuccessful activities. Click Next.



Figure 398 : Selection of auditing objectives of System Audit Policy Tab

Step 21 : This is summary of Audit Policy. Click Next.

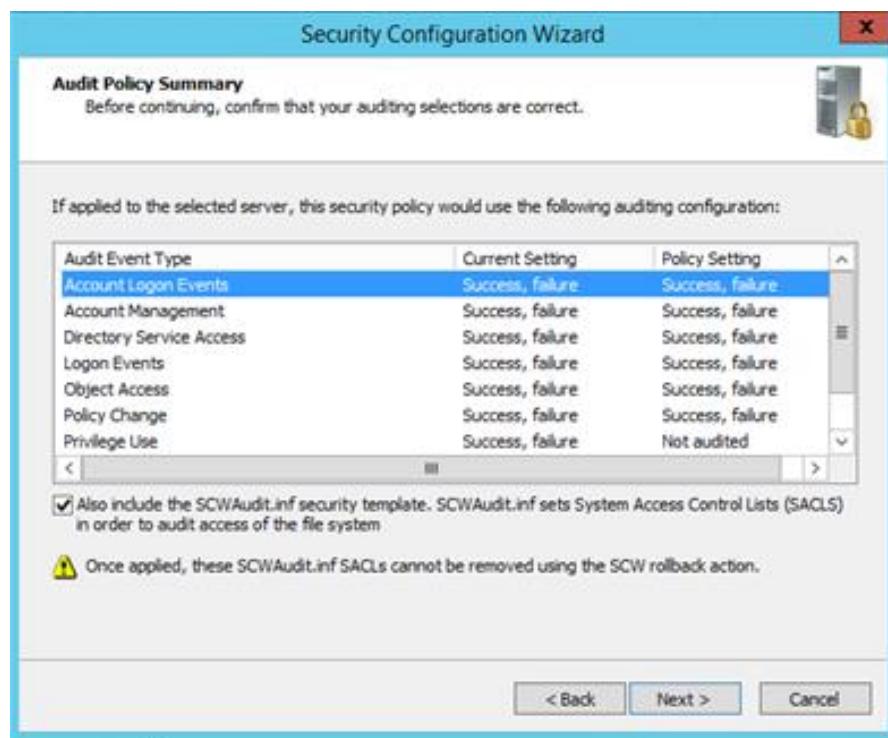


Figure 399 : Summary of Audit Policy Tab

Step 22 : This is page that shows the Security Policy has been save. Click Next.

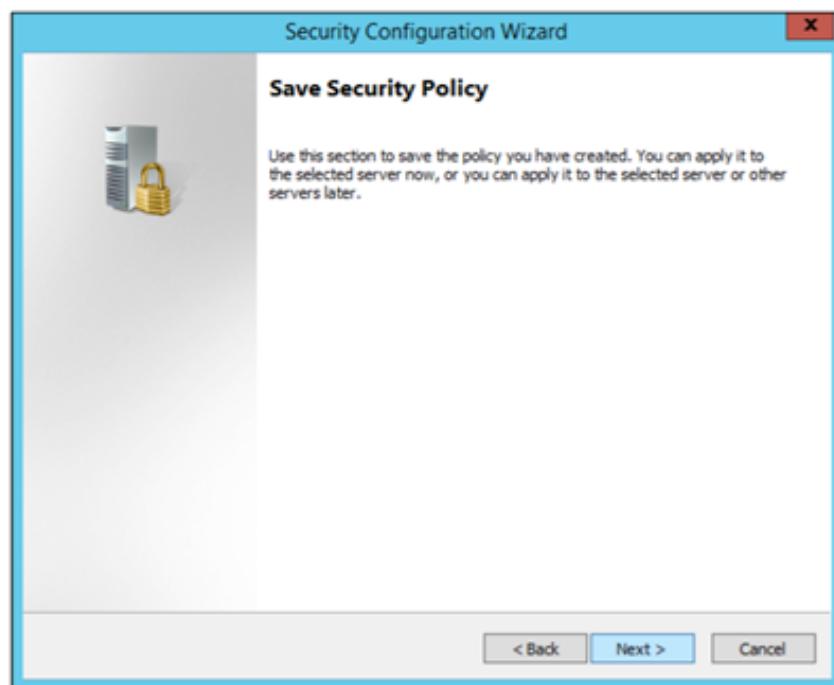


Figure 400 : Security Policy Tab To Save The Policy

Step 23 : Save the file using an appropriate name and location for the security policy file.  
Click Next.

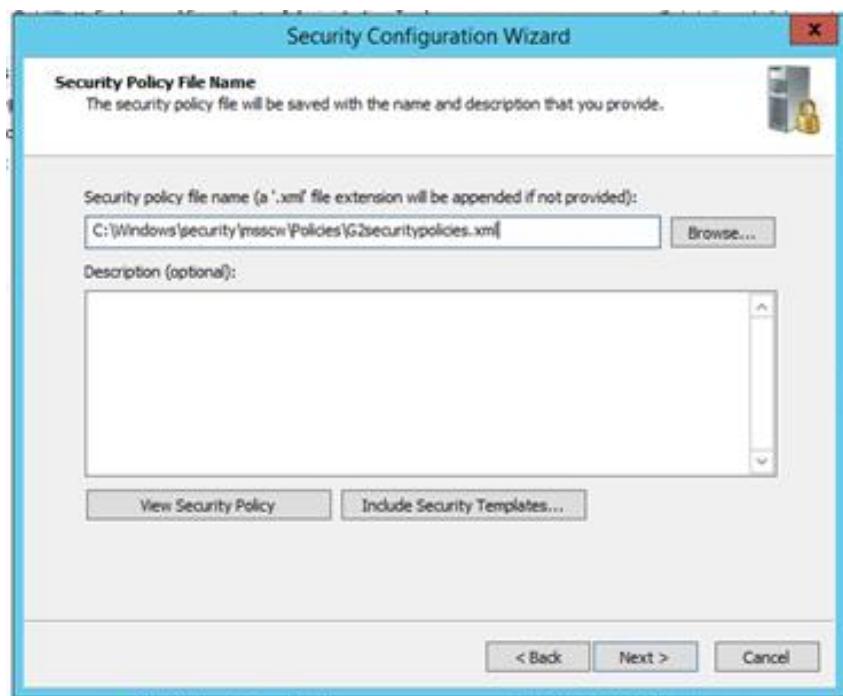


Figure 401 : File Saving for Security Policy File Name and File Location Tab

Step 24 : Wait until the process complete. Click Next.

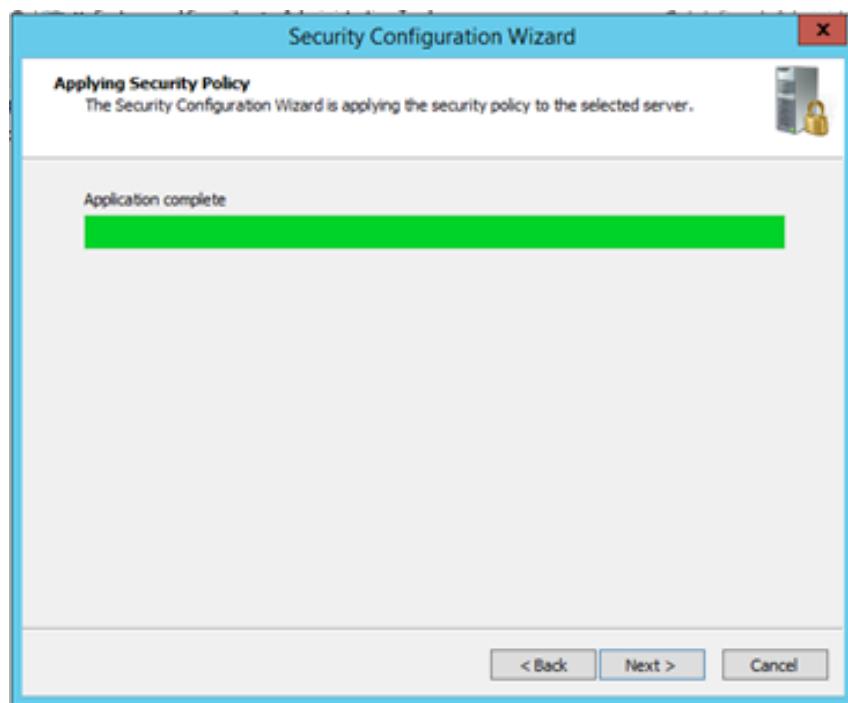


Figure 402 : Application Completion for Security Policy Tab

Step 25 : This is page that shows Security Configuration Wizard has been configured successfully. Click Finish.



Figure 403 :Completion of Security Configuration Wizard Tab

# CHAPTER 6: TESTING

## 6.1 INTRODUCTION

By using various methods and different tools, all the services we have can be used and accessed. This chapter will demonstrate how the services that had been set up and configured can be used. The testing is also to ensure that the function of the services is effectively up and running. Testing is the practice of making objective judgments regarding the extent to which the system meets, exceeds, or fails to meet stated objectives. In other words, testing is about risk control.

## 6.2 SERVICES TESTING

### 6.2.1 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.

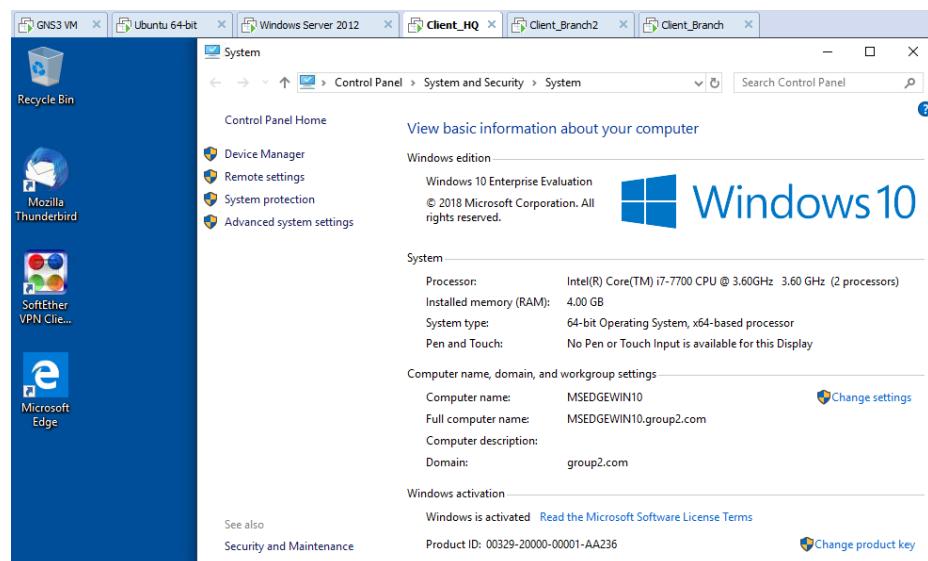


Figure 404 : System Properties

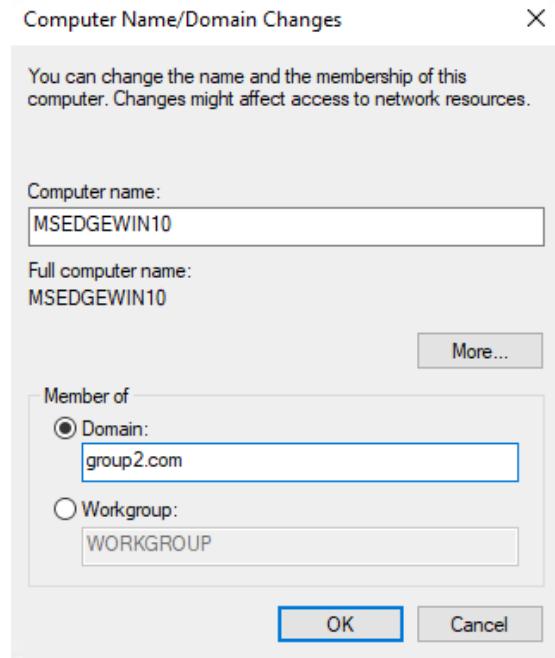


Figure 405 : Changes client to Domain

**Step 2 :** A username and password are require as a security purpose. Then, click ok.

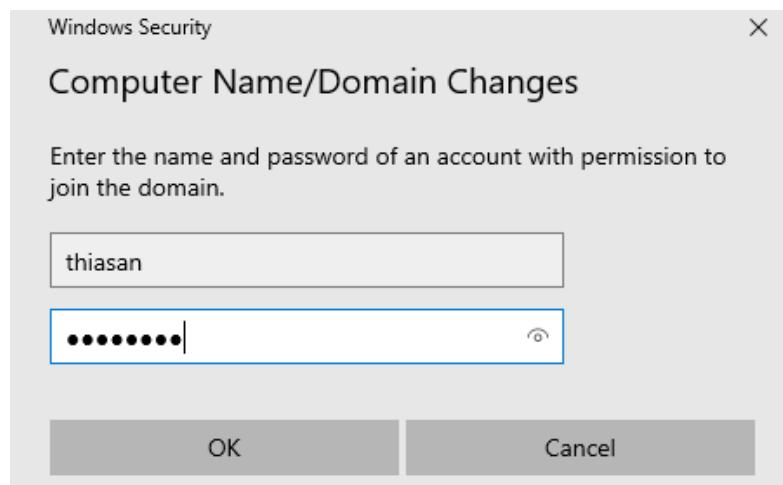


Figure 406 : Windows Security

**Step 3 :** To see whether the domain is success or not, a message will appear says that “Welcome to the group2.com domain”. After that, the system need to be restart in order to change it to domain.

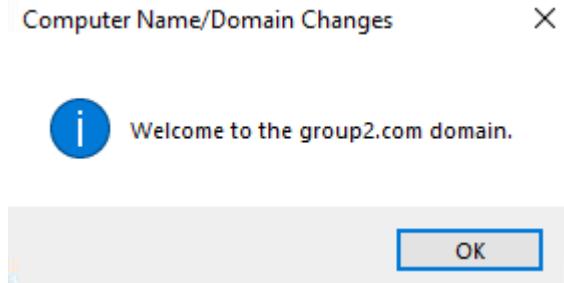


Figure 407 : Computer Name/Domain Changes

**Step 4 :** At pc client, enter the user as thiasan. Before the policy enable, the password must have 8 character in the desktop.

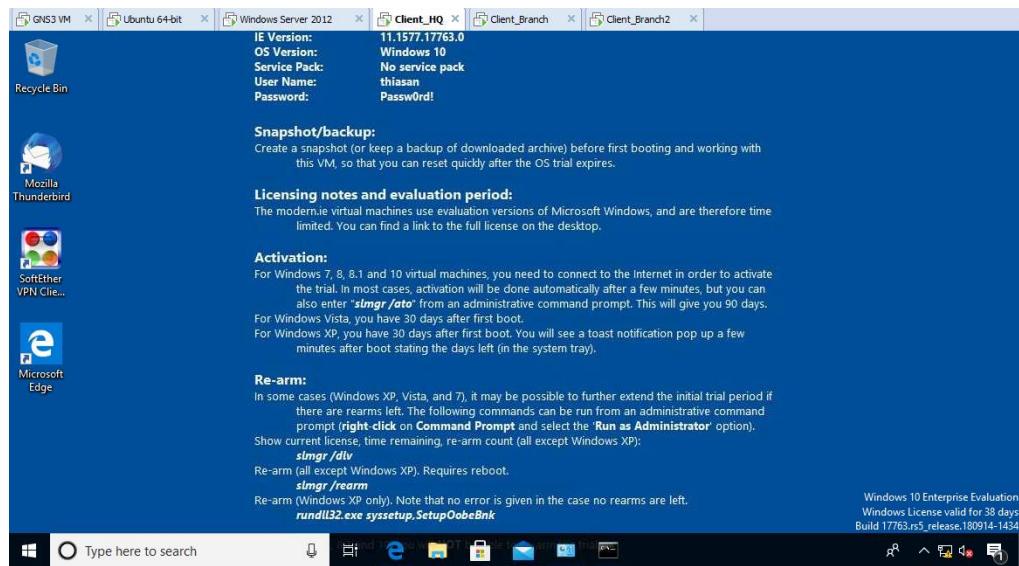


Figure 408 : Before The Policy is Enable

**Step 5 :** After the policy is enable by configure in the Group Policy Management Editor, if password did not same with policy will pop out notification

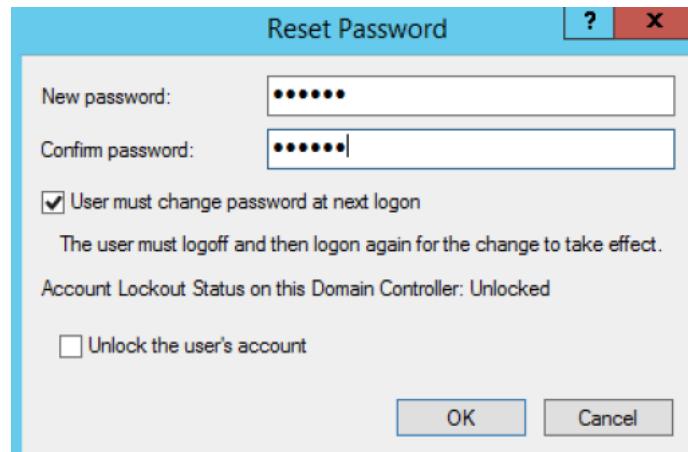


Figure 409

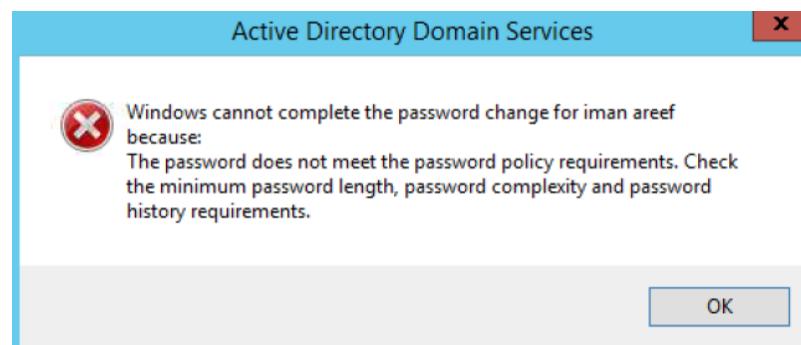
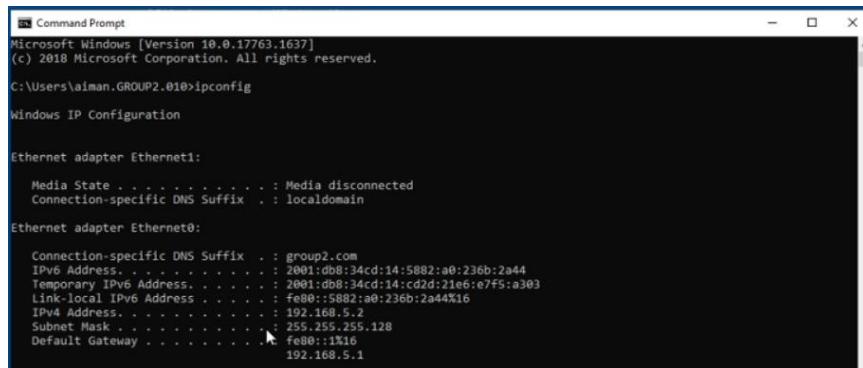


Figure 410 : After The Policy is Enable

## 6.2.2 DHCP IPv4 & IPV6

**Step 1:** On Client HQ, open CMD and type ipconfig



```
Command Prompt
Microsoft Windows [Version 10.0.17763.1637]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\aiman.GROUP2.010>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet1:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . : localdomain

Ethernet adapter Ethernet0:
  Connection-specific DNS Suffix . : group2.com
  IPv6 Address . . . . . : 2001:db8:34cd:14:5882:a0:236b:2a44
  Temporary IPv6 Address . . . . . : 2001:db8:34cd:14:cdd2:21e6:e7f5:a303
  Link-local IPv6 Address . . . . . : fe80::5882:a0:236b:2a44%16
  IPv4 Address . . . . . : 192.168.5.2
  Subnet Mask . . . . . : 255.255.255.128
  Default Gateway . . . . . : fe80::1%16
                                         192.168.5.1
```

Figure 411 : ipconfig on client HQ

**Step 2:** Go to Window Server and it will display that the client gets the DHCP IPv4 from the server.

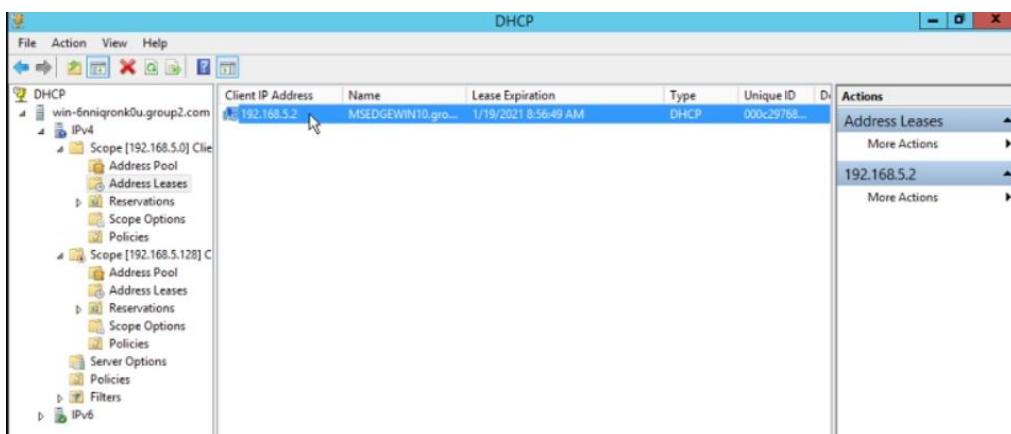
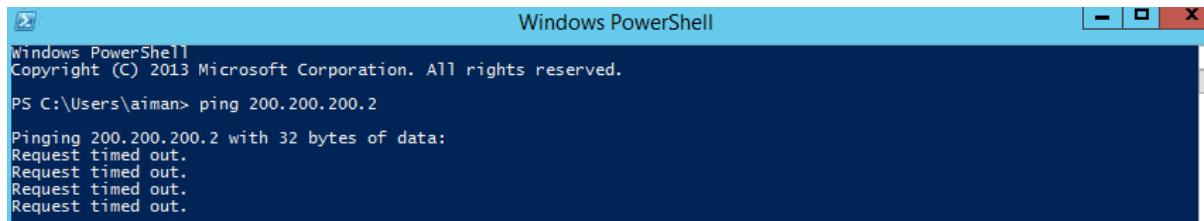


Figure 412 : Lease expiration

## 6.2.3 DYNAMIC ROUTING & NAT

### 6.2.3.1 DYNAMIC ROUTING



```
Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

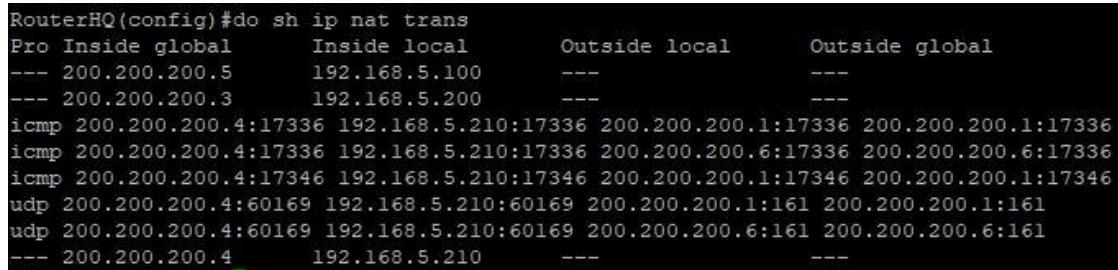
PS C:\Users\aiman> ping 200.200.200.2

Pinging 200.200.200.2 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

Figure 413 : Ping Public IP Address

### 6.2.3.2 NAT

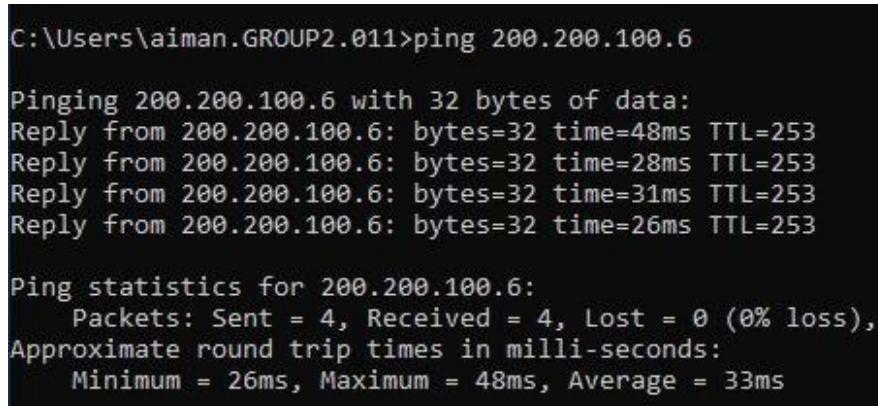
**Step 1:** Show mapping inside global/local and outside global/local by using command “*show ip nat translation*”.



```
RouterHQ(config)#do sh ip nat trans
Pro Inside global      Inside local      Outside local      Outside global
--- 200.200.200.5      192.168.5.100    ---              ---
--- 200.200.200.3      192.168.5.200    ---              ---
icmp 200.200.200.4:17336 192.168.5.210:17336 200.200.200.1:17336 200.200.200.1:17336
icmp 200.200.200.4:17336 192.168.5.210:17336 200.200.200.6:17336 200.200.200.6:17336
icmp 200.200.200.4:17346 192.168.5.210:17346 200.200.200.1:17346 200.200.200.1:17346
udp 200.200.200.4:60169 192.168.5.210:60169 200.200.200.1:161 200.200.200.1:161
udp 200.200.200.4:60169 192.168.5.210:60169 200.200.200.6:161 200.200.200.6:161
--- 200.200.200.4      192.168.5.210    ---              ---
```

Figure 414 : NAT translation

**Step 2:** Testing connection by ping public IP neighbor using command “*ping*”.



```
C:\Users\aiman.GROUP2.011>ping 200.200.100.6

Pinging 200.200.100.6 with 32 bytes of data:
Reply from 200.200.100.6: bytes=32 time=48ms TTL=253
Reply from 200.200.100.6: bytes=32 time=28ms TTL=253
Reply from 200.200.100.6: bytes=32 time=31ms TTL=253
Reply from 200.200.100.6: bytes=32 time=26ms TTL=253

Ping statistics for 200.200.100.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 26ms, Maximum = 48ms, Average = 33ms
```

Figure 415 : Ping Public IP Address

#### 6.2.4 IPSEC SITE-TO-SITE TUNNELING

**Step 1:** Show details information about the tunnel.

```
RouterHQ#sh int Tunnel 0
Tunnel0 is up, line protocol is up
  Hardware is Tunnel
  Internet address is 2.2.2.1/24
  MTU 17878 bytes, BW 100 Kbit/sec, DLY 50000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 200.200.200.2, destination 200.200.100.6
  Tunnel protocol/transport IPSEC/IP
  Tunnel TTL 255
  Tunnel transport MTU 1438 bytes
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Tunnel protection via IPsec (profile "group2_profile")
  Last input never, output never, output hang never
  Last clearing of "show interface" counters 02:05:37
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer
--More--
```

Figure 416 : Details about Tunnel

**Step 2:** Show details information about the session.

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

Interface: Tunnel0
Session status: UP-ACTIVE
Peer: 200.200.100.6 port 500
  IKEv1 SA: local 200.200.200.2/500 remote 200.200.100.6/500 Active
  IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
    Active SAs: 2, origin: crypto map
```

Figure 417 : Session information

**Step 3:** Show that the tunnel is active.

```
RouterHQ#sh crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst          src          state      conn-id status
200.200.200.2  200.200.100.6  QM_IDLE      1001 ACTIVE

IPv6 Crypto ISAKMP SA
```

*Figure 418 : Tunnel Status*

**Step 4:** Ping to beside group router to our router.

```
RouterHQ#ping 192.168.5.129 source 192.168.5.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.5.129, timeout is 2 seconds:
Packet sent with a source address of 192.168.5.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/28/56 ms
```

*Figure 419 : Ping status*

### 6.2.5 ACCESS CONTROL LIST

**STEP 1:** Try to remote windows server from client using telnet, it can't be remote.

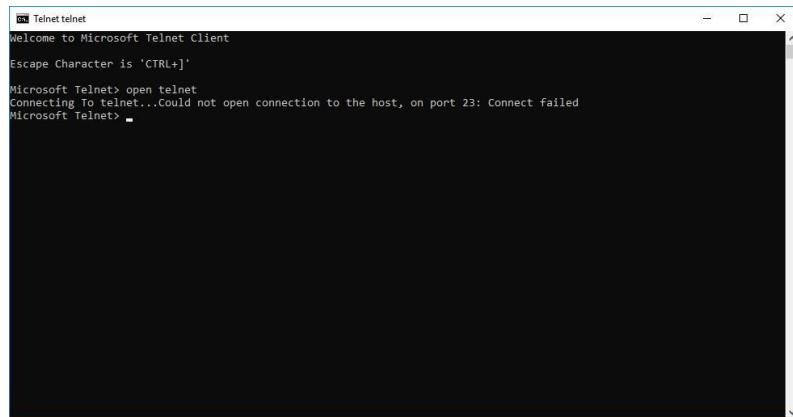


Figure 420 : TELNET testing

## 6.2.6 DOMAIN NAME SYSTEM

### In Windows Server

Use the command “*nslookup*” to verify that DNS servers are running. The “*nslookup*” command is a network utility program that is used to collect information about servers on the Internet.

**Step 1:** Open Windows Powershell and type nslookup. If it is successful, it will display the information.

```
PS C:\Users\aiman> nslookup
Default Server: win-6nniqronk0u.group2.com
Address: 2001:db8:34cd:15::3

> group2.com
Server: win-6nniqronk0u.group2.com
Address: 2001:db8:34cd:15::3

Name: group2.com
Addresses: 2001:db8:34cd:15::3
          2001:db8:34cd:15:58e4:362c:7882:c552
          192.168.5.200

> lubuntugrp2.group2.com
Server: win-6nniqronk0u.group2.com
Address: 2001:db8:34cd:15::3

Name: lubuntugrp2.group2.com
Address: 192.168.5.210

> 192.168.5.210
Server: win-6nniqronk0u.group2.com
Address: 2001:db8:34cd:15::3

Name: lubuntugrp2.group2.com
Address: 192.168.5.210

> 192.168.5.200
Server: win-6nniqronk0u.group2.com
Address: 2001:db8:34cd:15::3

Name: win-6nniqronk0u.group2.com
Address: 192.168.5.200

> www.group2.com
Server: win-6nniqronk0u.group2.com
Address: 2001:db8:34cd:15::3

Name: www.group2.com
Address: 192.168.5.200
```

Figure 421 : nslookup result

## In Client

**Step 2:** Open command prompt and type nslookup. If it is successful, it will display the information.

```
C:\Users\aiman.GROUP2.014>nslookup
Default Server: win-6nniqronk0u.group2.com
Address: 192.168.5.200

> group2.com
Server: win-6nniqronk0u.group2.com
Address: 192.168.5.200

Name: group2.com
Addresses: 2001:db8:34cd:15::3
           2001:db8:34cd:15:58e4:362c:7882:c552
           192.168.5.200

> lubuntugrp2.group2.com
Server: win-6nniqronk0u.group2.com
Address: 192.168.5.200

Name: lubuntugrp2.group2.com
Address: 192.168.5.210

> www.group2.com
Server: win-6nniqronk0u.group2.com
Address: 192.168.5.200

Name: www.group2.com
Address: 192.168.5.200

> 192.168.5.200
Server: win-6nniqronk0u.group2.com
Address: 192.168.5.200

Name: win-6nniqronk0u.group2.com
Address: 192.168.5.200
```

*Figure 422 : nslookup result*

### 6.2.7 LINUX EMAIL SERVER

**Step 1:** Using the server IP address (192.168.5.210) to navigate to the RainLoop mail page. Then, login to RainLoop webmail client with an email account.

Username: [chong@mail.group2.com](mailto:chong@mail.group2.com)

Password: grp2

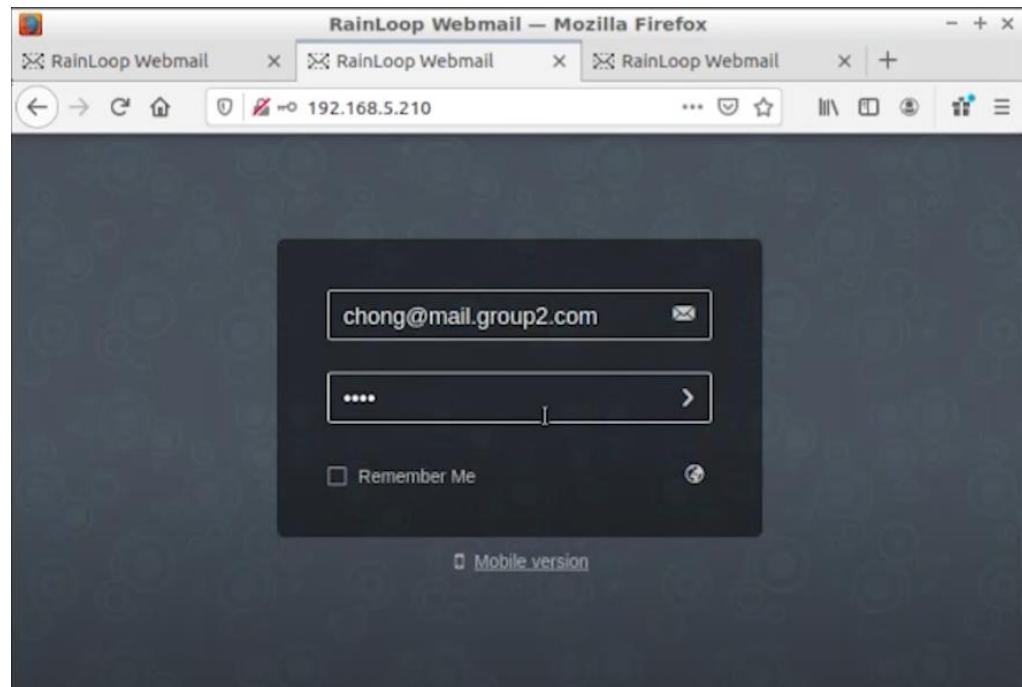


Figure 423: Login to RainLoop Webmail Client

**Step 2:** After login successful, create an email and send to another webmail client account for testing purpose.

To: [thiasan@mail.group2.com](mailto:thiasan@mail.group2.com)

From: [chong@mail.group2.com](mailto:chong@mail.group2.com)

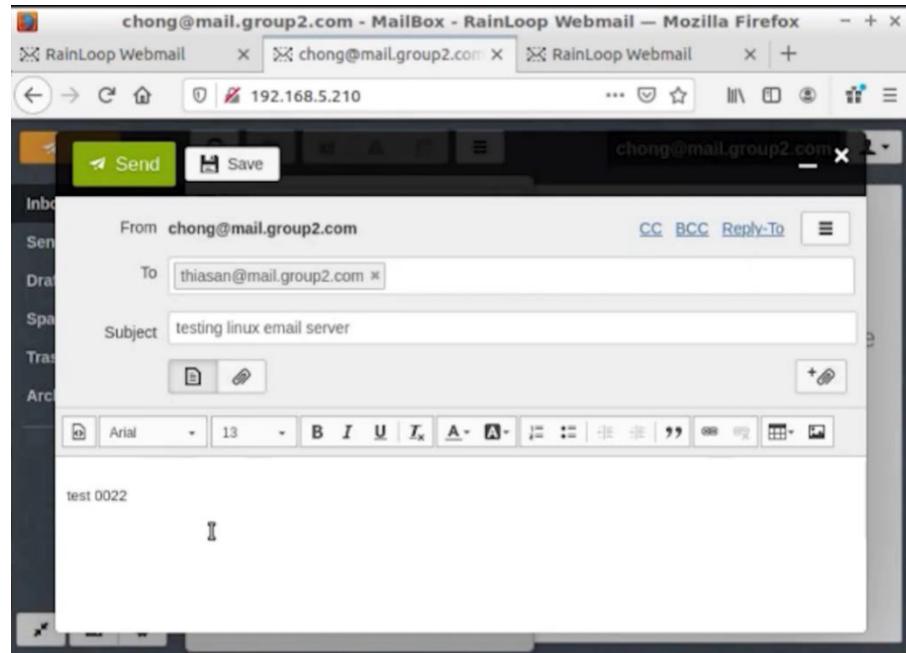


Figure 424: Compose and send email in RainLoop Webmail

**Step 3:** Navigate to **Sent** page to check for the sent email.

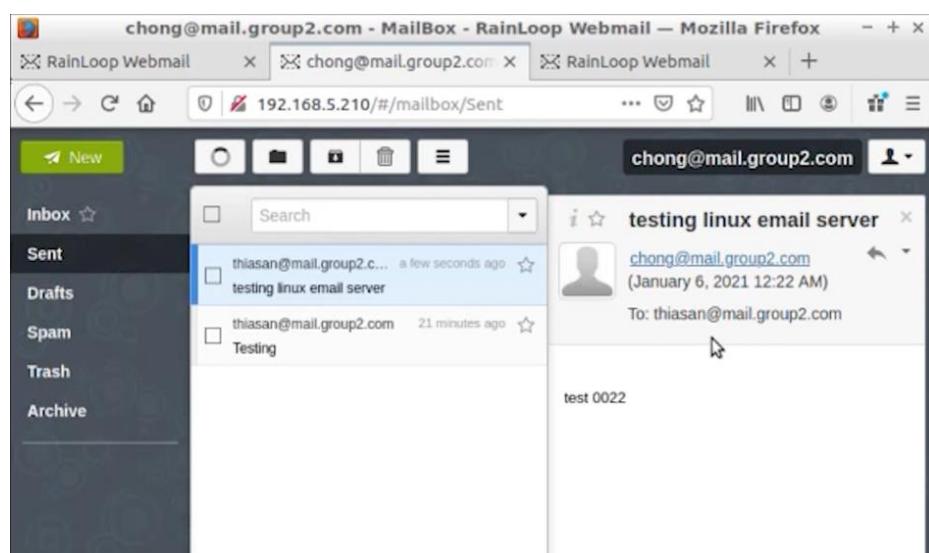
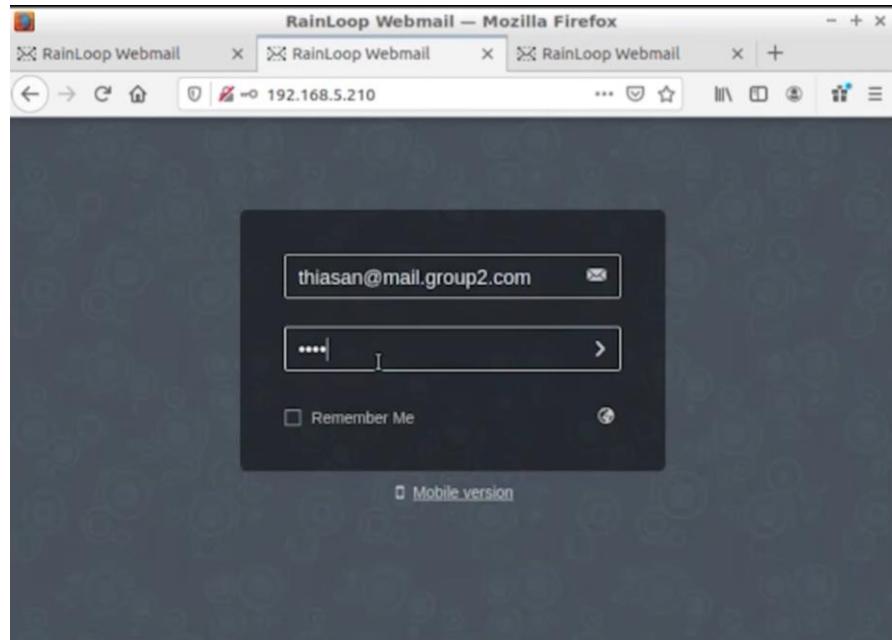


Figure 425: Email is sent successfully

**Step 4:** Login to the recipient email account to check the inbox.

Username: [thiasan@mail.group2.com](mailto:thiasan@mail.group2.com)

Password: grp2



*Figure 426: Login to another mail account*

**Step 5:** Navigate to **Inbox** to check for the received email.

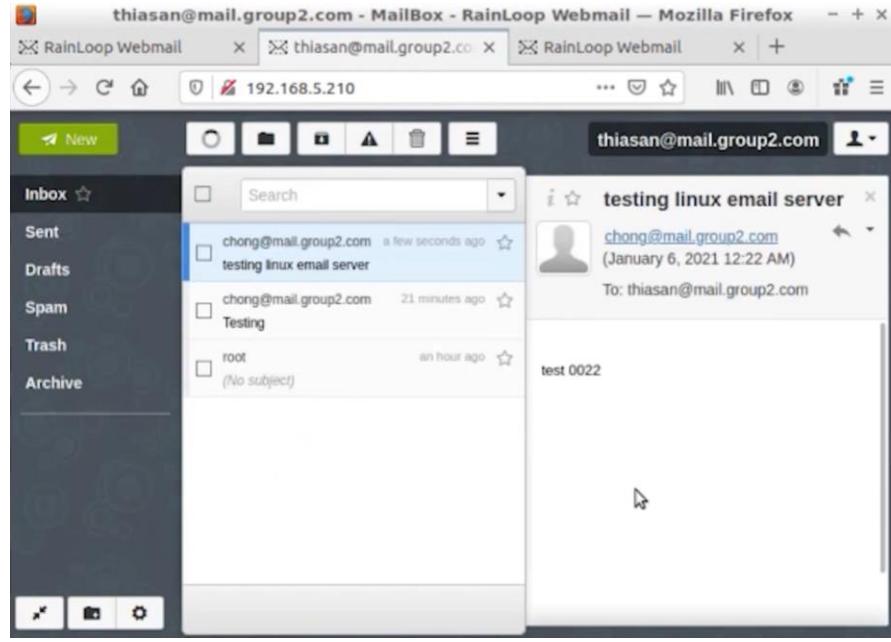


Figure 427: Recipient have received the email

**Step 6:** Navigate to browser at clientHQ and access to the RainLoop mail page using the IP address (192.168.5.210).

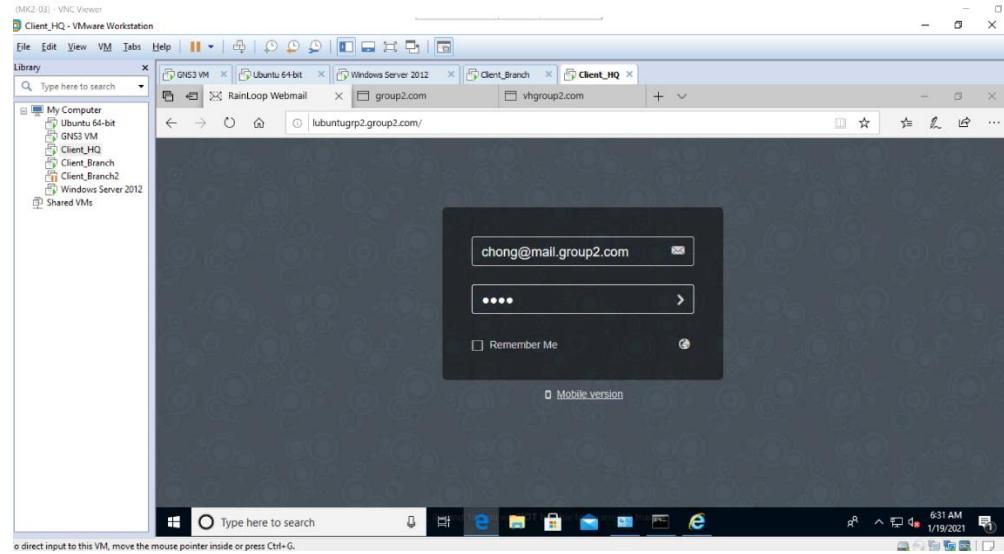


Figure 428: RainLoop main page at ClientHQ

## 6.2.8 WEB, SSL & VIRTUAL HOSTING

### Testing Web

**Step 1:** Open group website using <http://www.group2.com>.

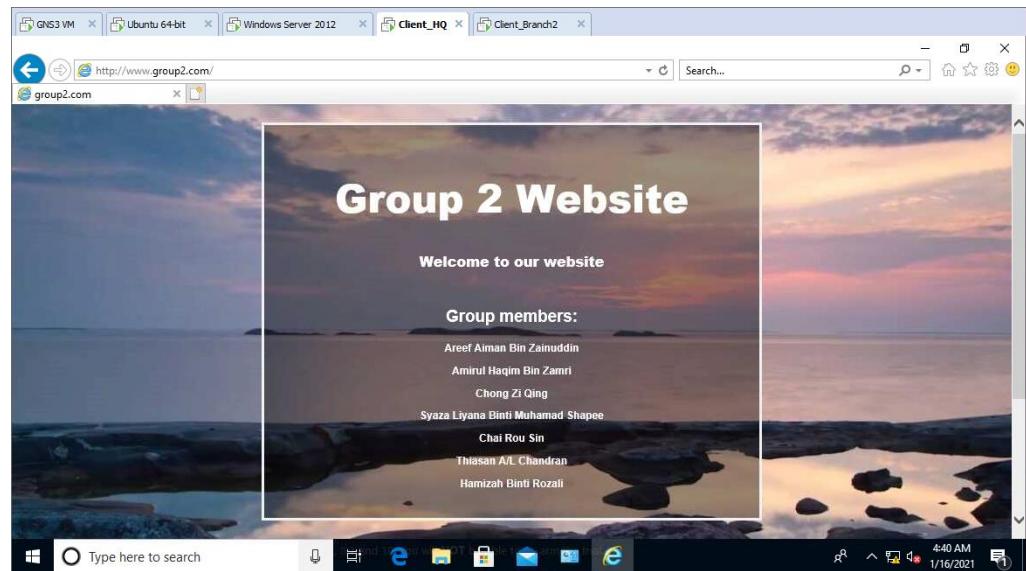


Figure 429: Group website

### Testing SSL

**Step 1:** Open group website with SSL using <https://www.group2.com>.

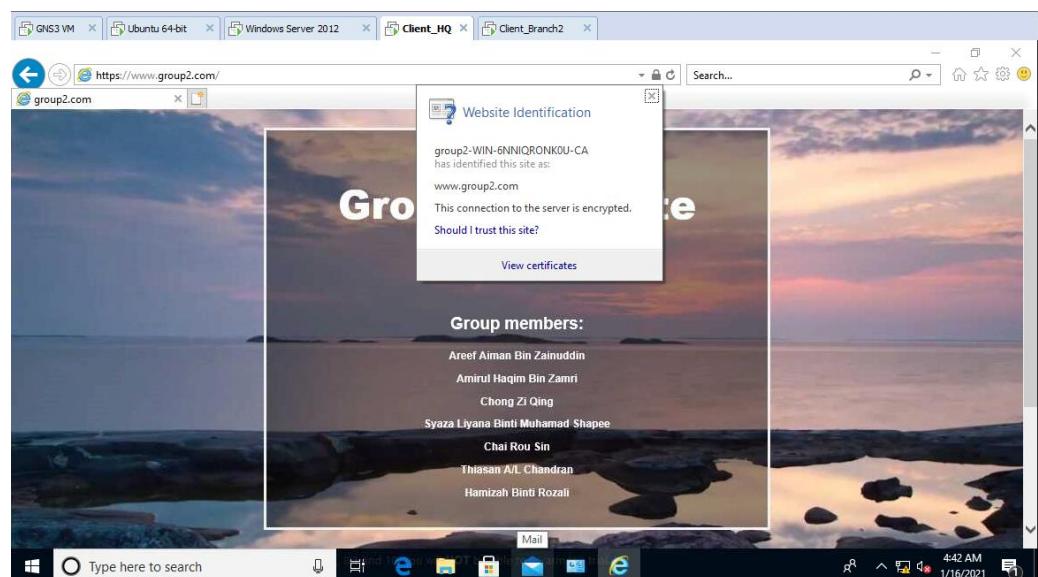


Figure 430: Group website with SSL

## Testing Virtual Hosting

Step 1: Open the website for virtual host using http://www.vhgroup2.com.



Figure 431: Virtual hosting website

## 6.2.9 NETWORK MONITORING SYSTEM

### Step 1: Stopping the DHCP service

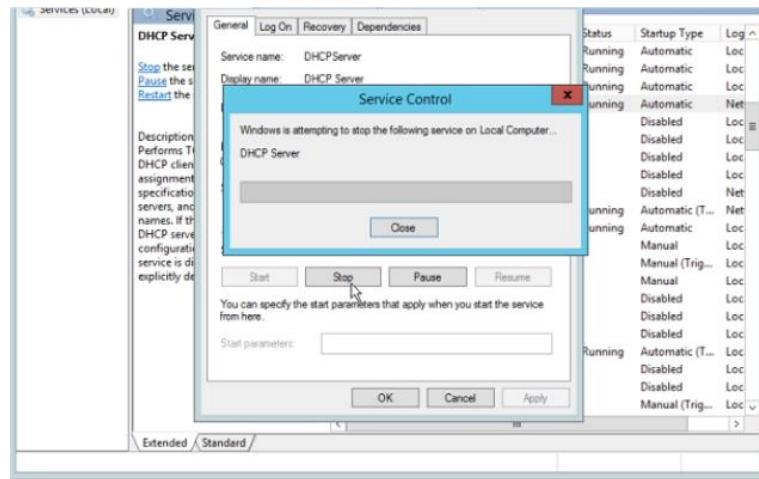


Figure 432 Stop DHCP service

**Step 2:** The Nagios Core show the status for DHCP is critical because it cannot monitor the service when the DHCP service is stopped

A screenshot of the Nagios Core web interface. The main page displays the 'Current Status' of hosts and services. On the left, there's a sidebar with links like 'Home', 'Documentation', 'Tactical Overview', 'Hosts', 'Services', 'Host Groups', 'Service Groups', 'Reports', and 'Problems'. The 'Problems' section is expanded, showing a table of service status. One entry for 'DHCP Server' under host 'WIN-6HNIQRONKGU' is highlighted in red and labeled 'CRITICAL'. Other entries in the table include 'Active Directory Domain Services', 'C:\ Drive Space', 'CPU Load', 'DNS Server', and 'Memory Usage', all of which are currently 'OK'. The Nagios logo is at the top left, and the URL in the browser is '192.168.5.210/nagios/'.

Figure 433 DHCP service status

**Step 3:** Starting the DHCP service on Windows Server

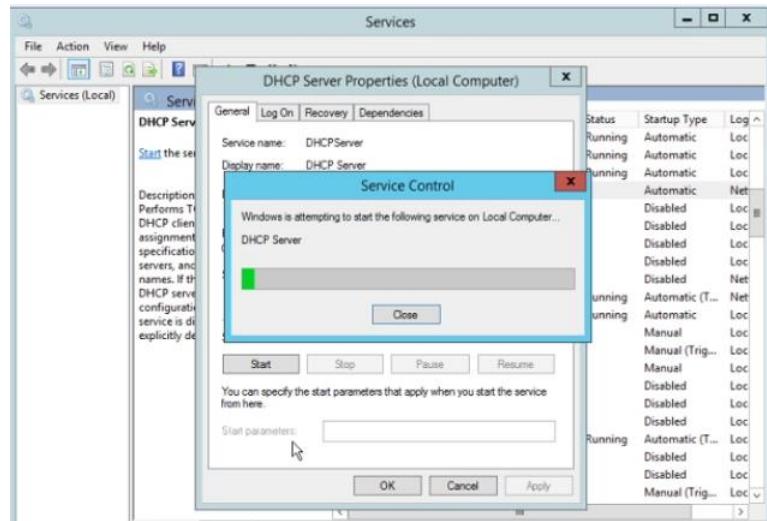


Figure 434 Starting DHCP service

**Step 4:** the DHCP status on Nagios Core is ok because it can monitor the DHCP service after it is started or up

Service	Status	Last Check	Downtime	Critical
C:\ Drive Space	OK	01-15-2021 16:10:52	0d 6h 26m 19s	1/3
CPU Load	OK	01-15-2021 16:16:39	0d 6h 30m 47s	1/3
DHCP Server	OK	01-15-2021 16:17:08	0d 0h 0m 19s	1/3
DNS Server	OK	01-15-2021 16:17:08	0d 0h 36m 56s	1/3
Memory Usage	OK	01-15-2021 16:09:54	0d 6h 27m 17s	1/3
NSClient++ Version	OK	01-15-2021 16:11:33	0d 6h 26m 7s	1/3

Figure 435 DHCP service status

**Step 5:** The status of monitored network device

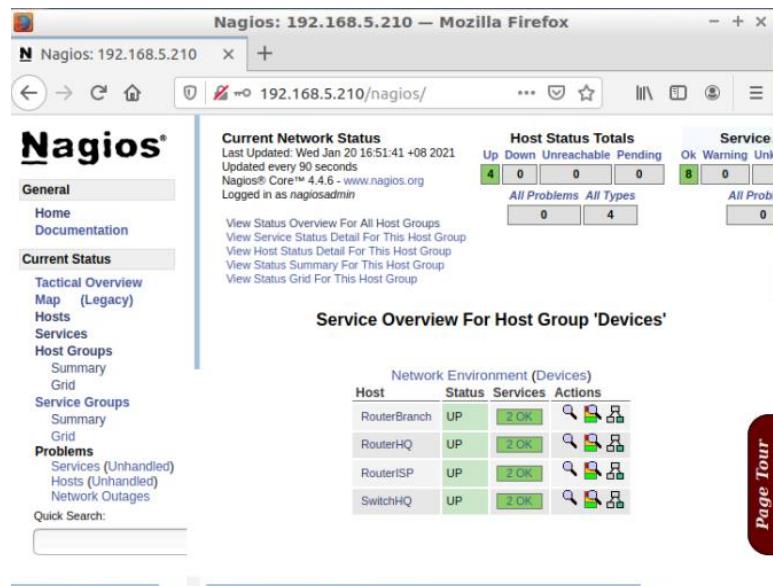


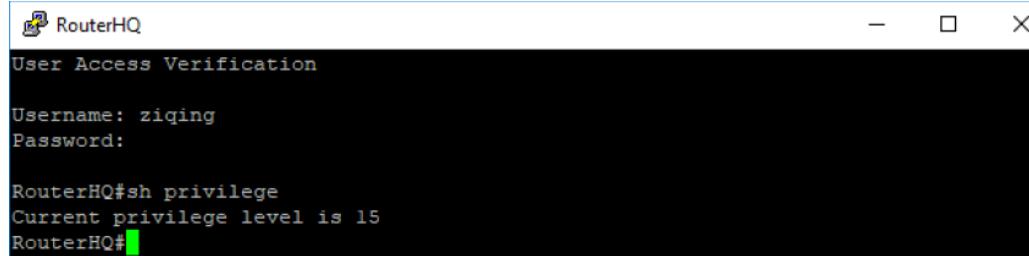
Figure 436 Monitored network device status

### 6.2.10 AAA (AUTHENTICATION AUTHORIZATION AND ACCOUNTING) USING RADIUS

**Step 1:** Enter enable model using AD user account (password and usernames). The configuration for radius server is successful if the authentication passed. Then, insert command to show the privileges that you have insert.

Username: ziqing

Password: Abcd1234



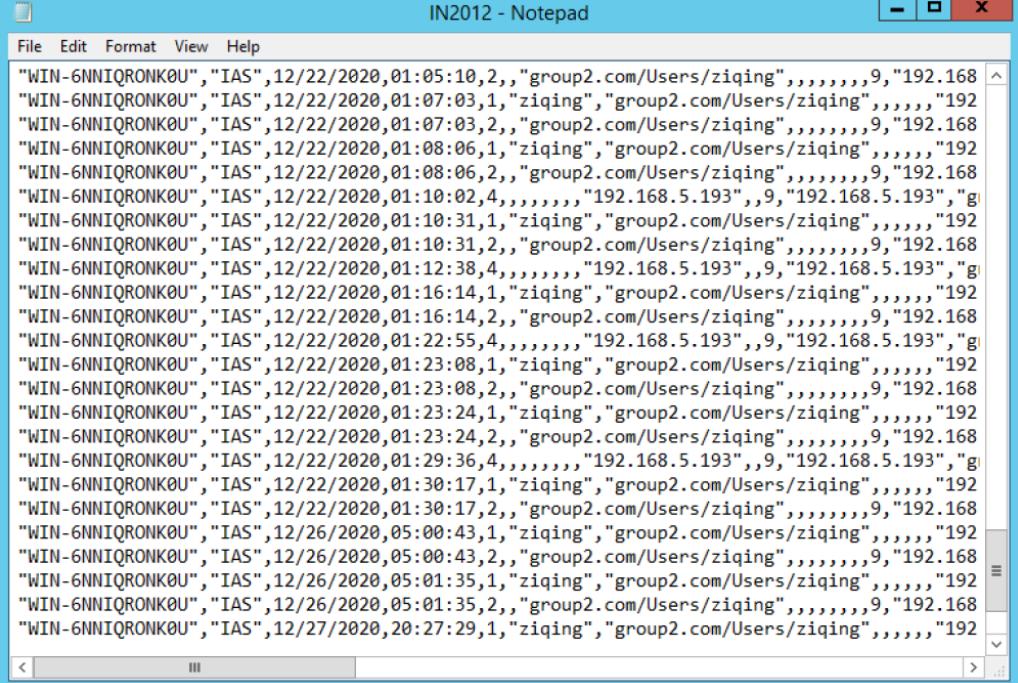
```
RouterHQ
User Access Verification

Username: ziqing
Password:

RouterHQ#sh privilege
Current privilege level is 15
RouterHQ#
```

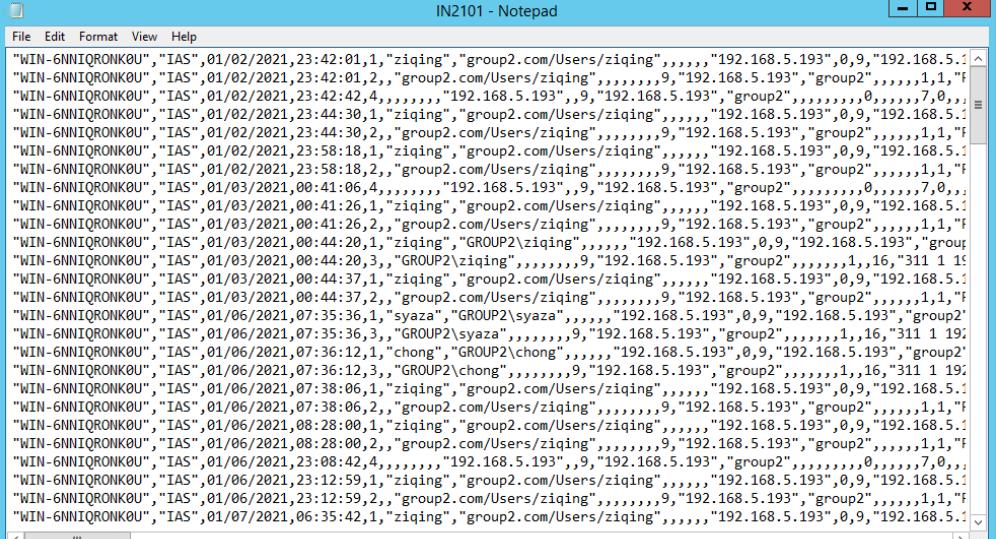
Figure 437: Enter username and password in router

**Step 2:** For Accounting, the logging information are saved in the lnyymm.log file.



```
IN2012 - Notepad
File Edit Format View Help
"WIN-6NNIQRONKOU","IAS",12/22/2020,01:05:10,2,"group2.com/Users/ziqing",,,,"192.168.5.193",0,9,"192.168.5.193"
"WIN-6NNIQRONKOU","IAS",12/22/2020,01:07:03,1,"ziqing","group2.com/Users/ziqing",,,,"192.168.5.193"
"WIN-6NNIQRONKOU","IAS",12/22/2020,01:07:03,2,"group2.com/Users/ziqing",,,,"192.168.5.193"
"WIN-6NNIQRONKOU","IAS",12/22/2020,01:08:06,1,"ziqing","group2.com/Users/ziqing",,,,"192.168.5.193"
"WIN-6NNIQRONKOU","IAS",12/22/2020,01:08:06,2,"group2.com/Users/ziqing",,,,"192.168.5.193"
"WIN-6NNIQRONKOU","IAS",12/22/2020,01:10:02,4,,,"192.168.5.193",,9,"192.168.5.193"
"WIN-6NNIQRONKOU","IAS",12/22/2020,01:10:31,1,"ziqing","group2.com/Users/ziqing",,,,"192.168.5.193"
"WIN-6NNIQRONKOU","IAS",12/22/2020,01:10:31,2,"group2.com/Users/ziqing",,,,"192.168.5.193"
"WIN-6NNIQRONKOU","IAS",12/22/2020,01:12:38,4,,,"192.168.5.193",,9,"192.168.5.193"
"WIN-6NNIQRONKOU","IAS",12/22/2020,01:16:14,1,"ziqing","group2.com/Users/ziqing",,,,"192.168.5.193"
"WIN-6NNIQRONKOU","IAS",12/22/2020,01:16:14,2,"group2.com/Users/ziqing",,,,"192.168.5.193"
"WIN-6NNIQRONKOU","IAS",12/22/2020,01:22:55,4,,,"192.168.5.193",,9,"192.168.5.193"
"WIN-6NNIQRONKOU","IAS",12/22/2020,01:23:08,1,"ziqing","group2.com/Users/ziqing",,,,"192.168.5.193"
"WIN-6NNIQRONKOU","IAS",12/22/2020,01:23:08,2,"group2.com/Users/ziqing",,,,"192.168.5.193"
"WIN-6NNIQRONKOU","IAS",12/22/2020,01:23:24,1,"ziqing","group2.com/Users/ziqing",,,,"192.168.5.193"
"WIN-6NNIQRONKOU","IAS",12/22/2020,01:23:24,2,"group2.com/Users/ziqing",,,,"192.168.5.193"
"WIN-6NNIQRONKOU","IAS",12/22/2020,01:29:36,4,,,"192.168.5.193",,9,"192.168.5.193"
"WIN-6NNIQRONKOU","IAS",12/22/2020,01:30:17,1,"ziqing","group2.com/Users/ziqing",,,,"192.168.5.193"
"WIN-6NNIQRONKOU","IAS",12/22/2020,01:30:17,2,"group2.com/Users/ziqing",,,,"192.168.5.193"
"WIN-6NNIQRONKOU","IAS",12/26/2020,05:00:43,1,"ziqing","group2.com/Users/ziqing",,,,"192.168.5.193"
"WIN-6NNIQRONKOU","IAS",12/26/2020,05:00:43,2,"group2.com/Users/ziqing",,,,"192.168.5.193"
"WIN-6NNIQRONKOU","IAS",12/26/2020,05:01:35,1,"ziqing","group2.com/Users/ziqing",,,,"192.168.5.193"
"WIN-6NNIQRONKOU","IAS",12/26/2020,05:01:35,2,"group2.com/Users/ziqing",,,,"192.168.5.193"
"WIN-6NNIQRONKOU","IAS",12/27/2020,20:27:29,1,"ziqing","group2.com/Users/ziqing",,,,"192.168.5.193
```

Figure 438: IN2012.log



```
IN2101 - Notepad
File Edit Format View Help
"WIN-6NNIQRONKOU","IAS",01/02/2021,23:42:01,1,"ziqing","group2.com/Users/ziqing",,,,"192.168.5.193",0,9,"192.168.5.193"
"WIN-6NNIQRONKOU","IAS",01/02/2021,23:42:01,2,"group2.com/Users/ziqing",,,,"192.168.5.193"
"WIN-6NNIQRONKOU","IAS",01/02/2021,23:42:42,4,,,"192.168.5.193",,9,"192.168.5.193"
"WIN-6NNIQRONKOU","IAS",01/02/2021,23:44:30,1,"ziqing","group2.com/Users/ziqing",,,,"192.168.5.193",0,9,"192.168.5.193"
"WIN-6NNIQRONKOU","IAS",01/02/2021,23:44:30,2,"group2.com/Users/ziqing",,,,"192.168.5.193"
"WIN-6NNIQRONKOU","IAS",01/02/2021,23:58:18,1,"ziqing","group2.com/Users/ziqing",,,,"192.168.5.193",0,9,"192.168.5.193"
"WIN-6NNIQRONKOU","IAS",01/02/2021,23:58:18,2,"group2.com/Users/ziqing",,,,"192.168.5.193"
"WIN-6NNIQRONKOU","IAS",01/03/2021,00:41:06,4,,,"192.168.5.193",,9,"192.168.5.193"
"WIN-6NNIQRONKOU","IAS",01/03/2021,00:41:26,1,"ziqing","group2.com/Users/ziqing",,,,"192.168.5.193",0,9,"192.168.5.193"
"WIN-6NNIQRONKOU","IAS",01/03/2021,00:41:26,2,"group2.com/Users/ziqing",,,,"192.168.5.193",0,9,"192.168.5.193"
"WIN-6NNIQRONKOU","IAS",01/03/2021,00:44:20,1,"ziqing","GROUP2ziqing",,,,"192.168.5.193",0,9,"192.168.5.193"
"WIN-6NNIQRONKOU","IAS",01/03/2021,00:44:20,3,"GROUP2ziqing",,,,"192.168.5.193",0,9,"192.168.5.193"
"WIN-6NNIQRONKOU","IAS",01/03/2021,00:44:37,1,"ziqing","group2.com/Users/ziqing",,,,"192.168.5.193",0,9,"192.168.5.193"
"WIN-6NNIQRONKOU","IAS",01/03/2021,00:44:37,2,"group2.com/Users/ziqing",,,,"192.168.5.193",0,9,"192.168.5.193"
"WIN-6NNIQRONKOU","IAS",01/06/2021,07:35:36,1,"syaza","GROUP2syaza",,,,"192.168.5.193",0,9,"192.168.5.193"
"WIN-6NNIQRONKOU","IAS",01/06/2021,07:35:36,3,"GROUP2syaza",,,,"192.168.5.193",0,9,"192.168.5.193"
"WIN-6NNIQRONKOU","IAS",01/06/2021,07:35:36,6,"chong","GROUP2chong",,,,"192.168.5.193",0,9,"192.168.5.193"
"WIN-6NNIQRONKOU","IAS",01/06/2021,07:36:12,1,"chong","GROUP2chong",,,,"192.168.5.193",0,9,"192.168.5.193"
"WIN-6NNIQRONKOU","IAS",01/06/2021,07:36:12,3,"GROUP2chong",,,,"192.168.5.193",0,9,"192.168.5.193"
"WIN-6NNIQRONKOU","IAS",01/06/2021,07:38:06,1,"ziqing","group2.com/Users/ziqing",,,,"192.168.5.193",0,9,"192.168.5.193"
"WIN-6NNIQRONKOU","IAS",01/06/2021,07:38:06,2,"group2.com/Users/ziqing",,,,"192.168.5.193",0,9,"192.168.5.193"
"WIN-6NNIQRONKOU","IAS",01/06/2021,08:28:00,1,"ziqing","group2.com/Users/ziqing",,,,"192.168.5.193",0,9,"192.168.5.193"
"WIN-6NNIQRONKOU","IAS",01/06/2021,08:28:00,2,"group2.com/Users/ziqing",,,,"192.168.5.193",0,9,"192.168.5.193"
"WIN-6NNIQRONKOU","IAS",01/06/2021,23:08:42,4,,,"192.168.5.193",,9,"192.168.5.193"
"WIN-6NNIQRONKOU","IAS",01/06/2021,23:12:59,1,"ziqing","group2.com/Users/ziqing",,,,"192.168.5.193",0,9,"192.168.5.193"
"WIN-6NNIQRONKOU","IAS",01/06/2021,23:12:59,2,"group2.com/Users/ziqing",,,,"192.168.5.193",0,9,"192.168.5.193"
"WIN-6NNIQRONKOU","IAS",01/07/2021,06:35:42,1,"ziqing","group2.com/Users/ziqing",,,,"192.168.5.193",0,9,"192.168.5.193"
```

Figure 439: IN2101.log

## 6.2.11 LAYER 2 SECURITY VLAN & PORT SECURITY

### VLAN Security

Then view the VLAN table to ensure all the unused port is in the right VLAN.

VLAN Name	Status	Ports
1 default	active	
10 vlan_server	active	Gi0/1, Gi0/2, Gi0/3
15 unusedport	suspended	Gi1/0, Gi1/1, Gi1/2, Gi1/3 Gi2/0, Gi2/1
20 vlan_client	active	
1002 fddi-default	act/unsup	
1003 token-ring-default	act/unsup	
1004 fddinet-default	act/unsup	
1005 trnet-default	act/unsup	

Figure 440: VLAN brief

### Port Security

Used command show port security to display list of port which is have been assigned and their security action.

Secure Port (Count)	MaxSecureAddr (Count)	CurrentAddr (Count)	SecurityViolation (Count)	Security Action (Count)
Gi0/1 1		1	0	Shutdown
Gi0/2 10		3	0	Shutdown
-----				
Total Addresses in System (excluding one mac per port) : 2				
Max Addresses limit in System (excluding one mac per port) : 4096				

Figure 441: Summary of shutdown ports

To display port security information about specific interface, used command show port-security interface gi0/1.

SwitchHQ#sh port-security int gi0/1
Port Security : Enabled
Port Status : Secure-up
Violation Mode : Shutdown
Aging Time : 0 mins
Aging Type : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses : 1
Total MAC Addresses : 1
Configured MAC Addresses : 0
Sticky MAC Addresses : 1
Last Source Address:Vlan : 0050.56c0.0004:10
Security Violation Count : 0

Figure 442: To display port security information

To display port security information about specific interface, used command show port-security interface gi0/2.

```
SwitchHQ#sh port-security int gi0/2
Port Security          : Enabled
Port Status            : Secure-up
Violation Mode        : Shutdown
Aging Time             : 0 mins
Aging Type             : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses : 10
Total MAC Addresses   : 2
Configured MAC Addresses : 0
Sticky MAC Addresses  : 2
Last Source Address:Vlan : 000c.2933.44a8:10
Security Violation Count : 0

SwitchHQ#
```

Figure 443: To display port security information

### 6.2.12 IDS WITH PORT MIRRORING

#### Part A: Snort Testing

Verify Snort Installation:

Enter the command: \$ snort -V

```
root@lubuntugrp2:~/snort/snort-2.9.17# snort -V
      _--> Snort! <--_
   o"   )~ Version 2.9.17 GRE (Build 199)
     '   By Martin Roesch & The Snort Team: http://www.snort.org/contact#tea
m
Copyright (C) 2014-2020 Cisco and/or its affiliates. All rights res
erved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using libpcap version 1.8.1
Using PCRE version: 8.39 2016-06-14
Using ZLIB version: 1.2.11
```

Figure 444: Verify installation

Enter the command : sudo snort -T -c /etc/snort/snort.conf

```
root@lubuntugrp2: /etc/snort
File Edit Tabs Help
Using PCRE version: 8.39 2016-06-14
Using ZLIB version: 1.2.11

Rules Engine: SF_SNORT_DETECTION_ENGINE Version 3.1 <Build 1>
Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
Preprocessor Object: SF_SIP Version 1.1 <Build 1>
Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Preprocessor Object: SF_DCERPC2 Version 1.0 <Build 3>
Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
Preprocessor Object: SF_GTP Version 1.1 <Build 1>
Preprocessor Object: SF_SSH Version 1.1 <Build 3>
Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>
Preprocessor Object: appid Version 1.1 <Build 5>
Preprocessor Object: SF_SMTP Version 1.1 <Build 9>
Preprocessor Object: SF_S7COMMPLUS Version 1.0 <Build 1>
Preprocessor Object: SF_POP Version 1.0 <Build 1>
Preprocessor Object: SF_SDF Version 1.1 <Build 1>
Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>
Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>

Snort successfully validated the configuration!
Snort exiting
root@lubuntugrp2:/etc/snort#
```

Figure 445: Snort successfully validated.

## Part B: Port Mirror Testing

Ensure you in root user.

Change the interface into port mirror.

```
root@lubuntugrp2:~# snort -A console -i ens38 -u snort -g snort -c /etc/snort/snort.conf
```

Figure 446: Run command snort

Now that Snort is running and listening on ens38.

```
Commencing packet processing (pid=36163)
01/19-23:23:43.184303  [**] [1:10000001:1] icmp test [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 192.168.5.211 -> 192.168.5.210
01/19-23:23:46.692564  [**] [1:10000001:1] icmp test [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 192.168.5.211 -> 192.168.5.210
01/19-23:23:50.716525  [**] [1:10000001:1] icmp test [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 192.168.5.211 -> 192.168.5.210
01/19-23:23:54.711581  [**] [1:10000001:1] icmp test [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 192.168.5.211 -> 192.168.5.210
01/19-23:23:59.206896  [**] [1:10000001:1] icmp test [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 192.168.5.211 -> 192.168.5.210
01/19-23:24:02.722097  [**] [1:10000001:1] icmp test [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 192.168.5.211 -> 192.168.5.210
01/19-23:24:06.703950  [**] [1:10000001:1] icmp test [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 192.168.5.211 -> 192.168.5.210
01/19-23:24:10.585226  [**] [1:10000001:1] icmp test [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 192.168.5.211 -> 192.168.5.210
01/19-23:24:14.589476  [**] [1:10000001:1] icmp test [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 192.168.5.211 -> 192.168.5.210
```

Figure 447: Snort alert

Open the log files to ensure the data is recorded.

Type *snort -r /var/log/snort/snort.log*. \*press tab\*

```
root@lubuntugrp2: ~
File Edit Tabs Help
TCP TTL:63 TOS:0x0 ID:13807 IplLen:20 DgmLen:60 DF
Seq: 0xC2C8D00
** END OF DUMP
=====

WARNING: No preprocessors configured for policy 0.
01/19-23:24:34.969898 192.168.5.211 -> 192.168.5.210
ICMP TTL:255 TOS:0x0 ID:36659 IplLen:20 DgmLen:56
Type:5 Code:1 REDIRECT HOST NEW GW: 192.168.5.200
** ORIGINAL DATAGRAM DUMP:
192.168.5.210:49272 -> 192.168.5.200:12489
TCP TTL:63 TOS:0x0 ID:34181 IplLen:20 DgmLen:60 DF
Seq: 0xB39F12D5
** END OF DUMP
=====

WARNING: No preprocessors configured for policy 0.
01/19-23:24:38.967775 192.168.5.211 -> 192.168.5.210
ICMP TTL:255 TOS:0x0 ID:36663 IplLen:20 DgmLen:56
Type:5 Code:1 REDIRECT HOST NEW GW: 192.168.5.200
** ORIGINAL DATAGRAM DUMP:
192.168.5.210:49280 -> 192.168.5.200:12489
TCP TTL:63 TOS:0x0 ID:17883 IplLen:20 DgmLen:60 DF
Seq: 0x284375E9
```

Figure 448: Log file shown

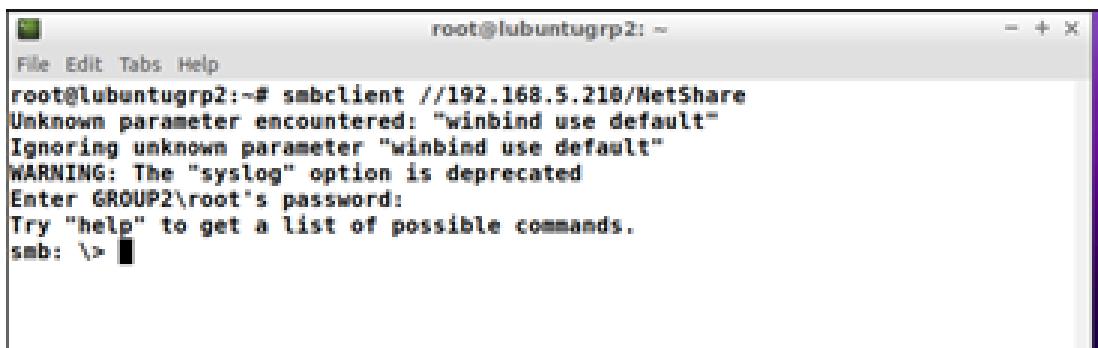
### 6.2.13 SAMBA AND SAMBA SECURITY SERVICES

#### Lubuntu Server

**Step 1:** Make sure Client can ping Lubuntu Server

**Step 2:** Enable the sharing from the Lubuntu (Samba) Server using command

**smbclient //192.168.5.210/NetShare**



```
root@lubuntugrp2:~# smbclient //192.168.5.210/NetShare
Unknown parameter encountered: "winbind use default"
Ignoring unknown parameter "winbind use default"
WARNING: The "syslog" option is deprecated
Enter GROUP2\root's password:
Try "help" to get a list of possible commands.
smb: \> 
```

Figure 449 : Samba folder sharing enabled

#### Client HQ

**Step 3:** Add a network location from client HQ

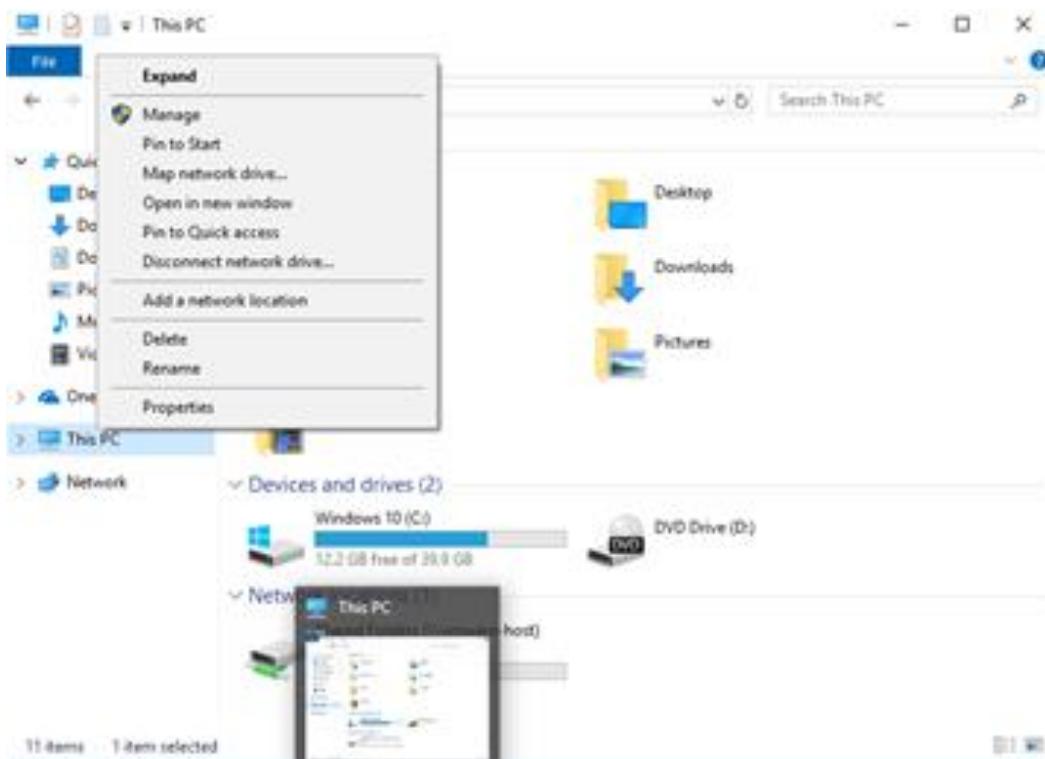


Figure 450 : Add a network location

**Step 4:** Click Next

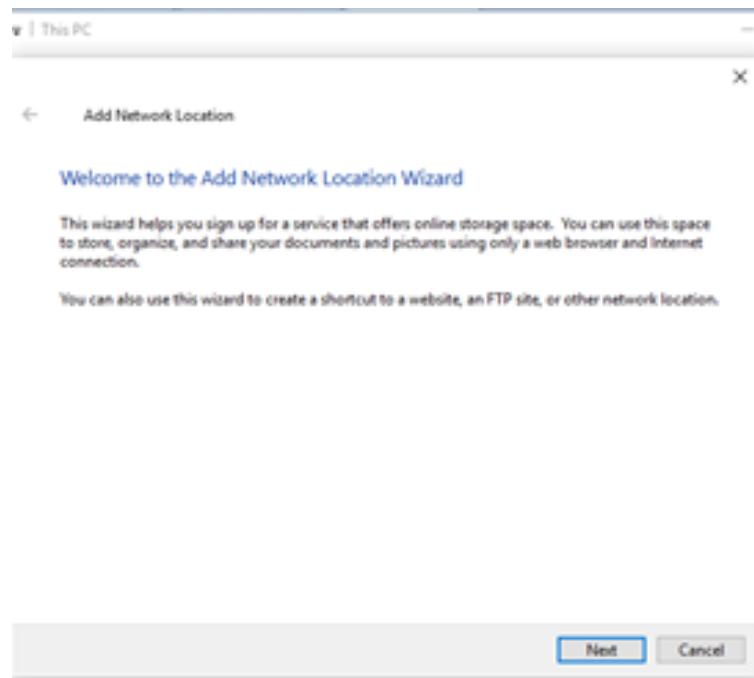


Figure 451 : Welcome page of add network location wizard

**Step 5:** Make sure the Internet connection is on and click the option as shown in the figure below and click next

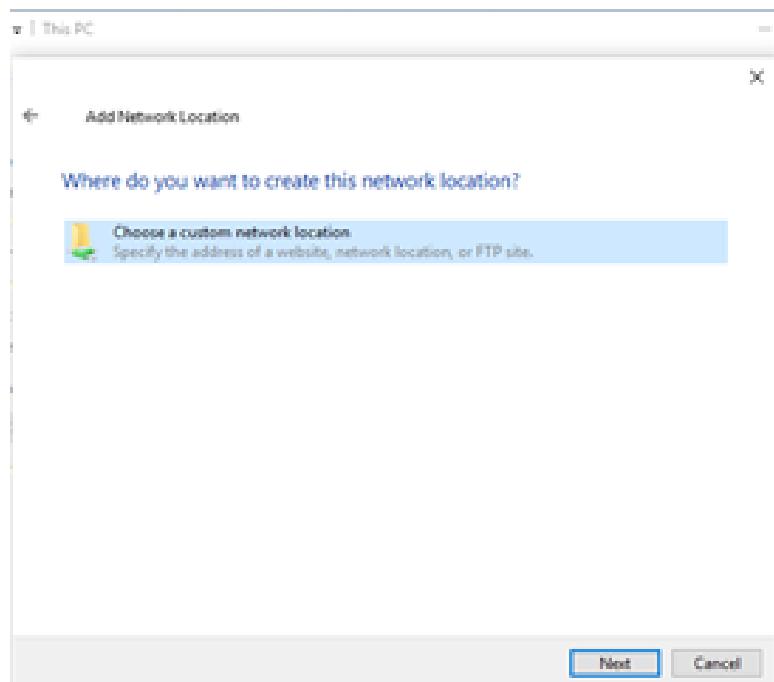


Figure 452 : Option to choose a custom network location

**Step 6:** Access the sharing from the Lubuntu (Samba) Server using command <\\192.168.5.210\NetShare> and click next.

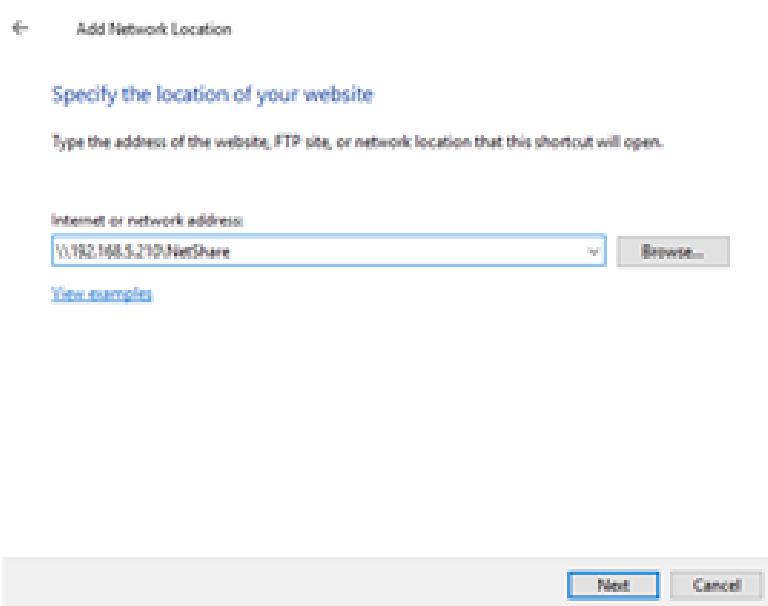


Figure 453 : Typed samba location address

**Step 7:** Click next.

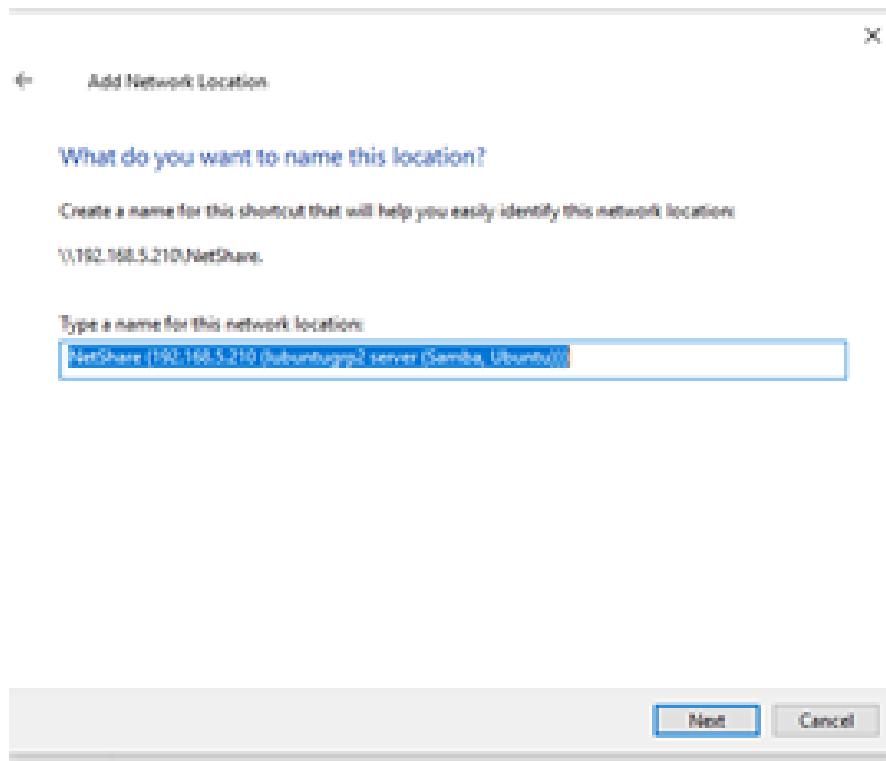


Figure 454 : Name for the samba shared network location

**Step 8:** Click Finish.

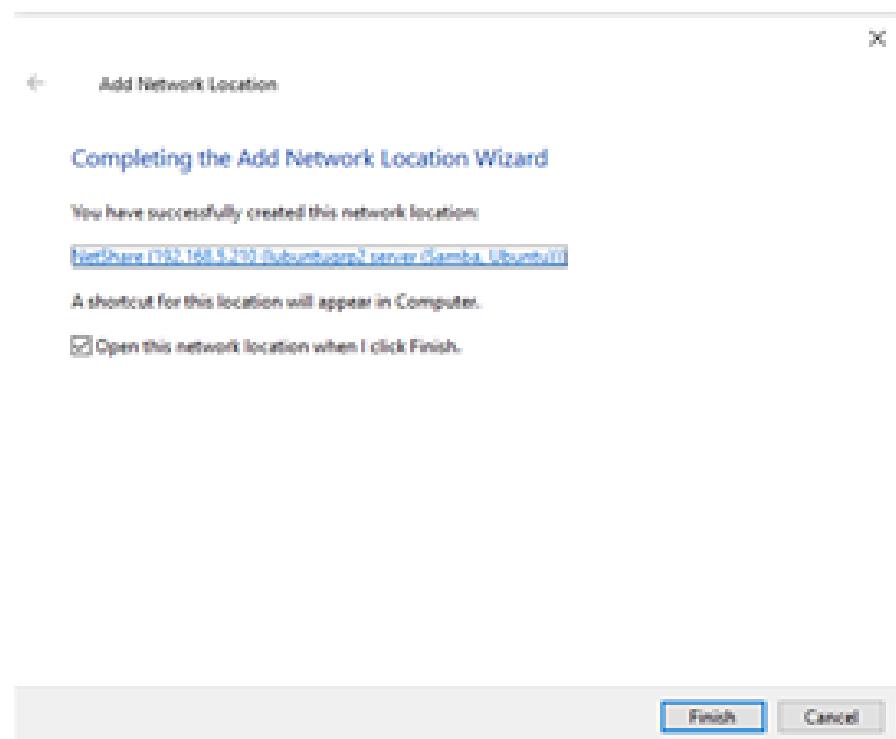


Figure 455 : Completion of adding network location wizard

**Step 9:** Now all the files and folders on NetShare are accessible.

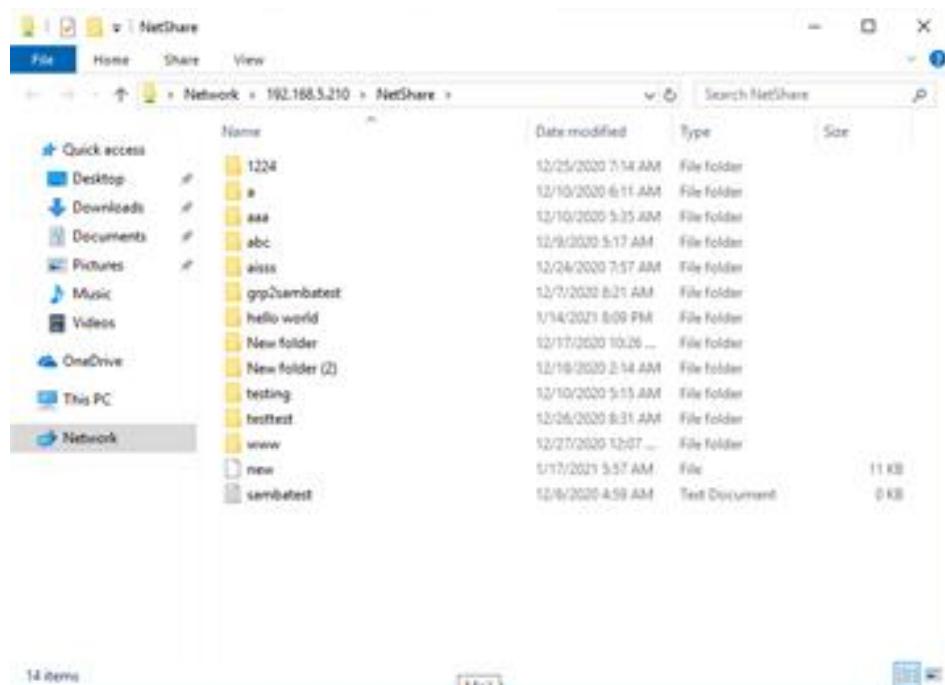


Figure 456 : Folders and files created in samba share

**Step 10:** Click the IP address on the bar above to see all the shared folders from Samba Server.

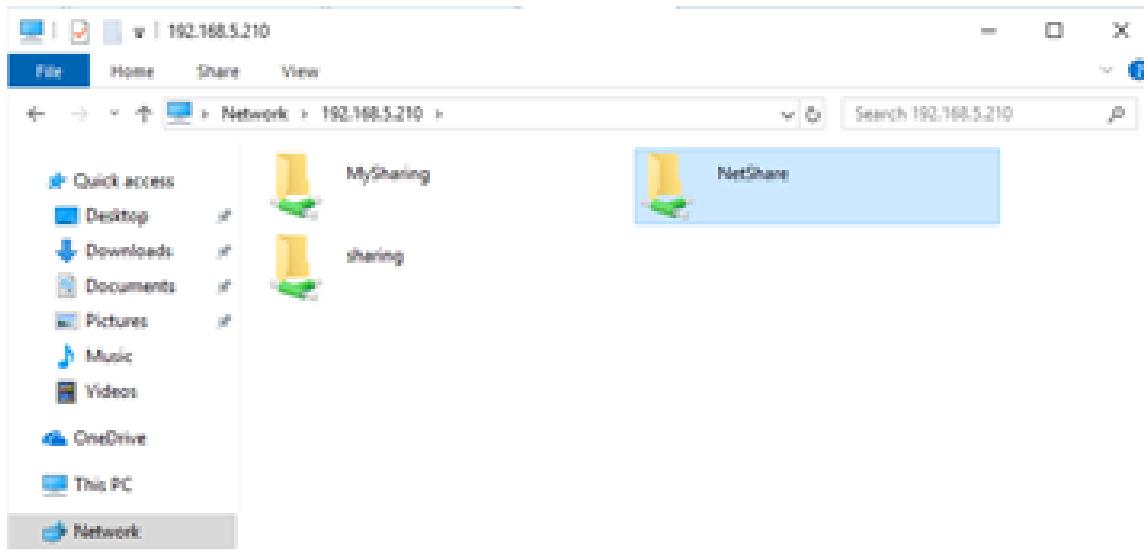


Figure 457 : All shared folders lists

**Step 11:** Some Sharing required credential which is part of Samba Security Features.

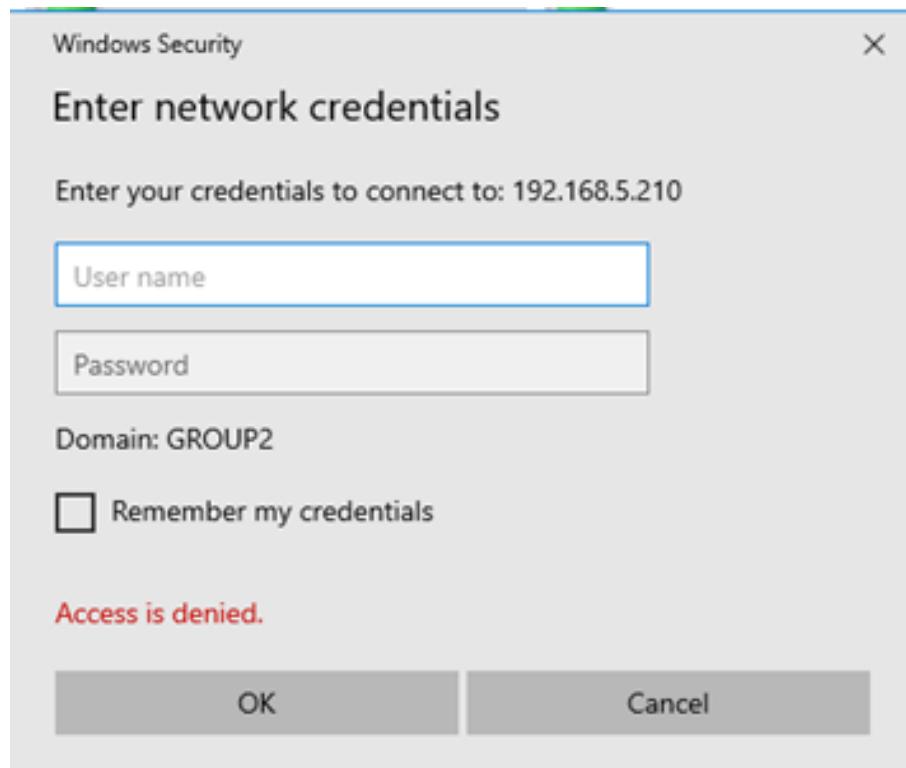


Figure 458 : Network credentials requirement for security purpose

**Step 12:** Some sharing restricted and denied the logged user from modify the files or folders which is part of Samba Security Features.

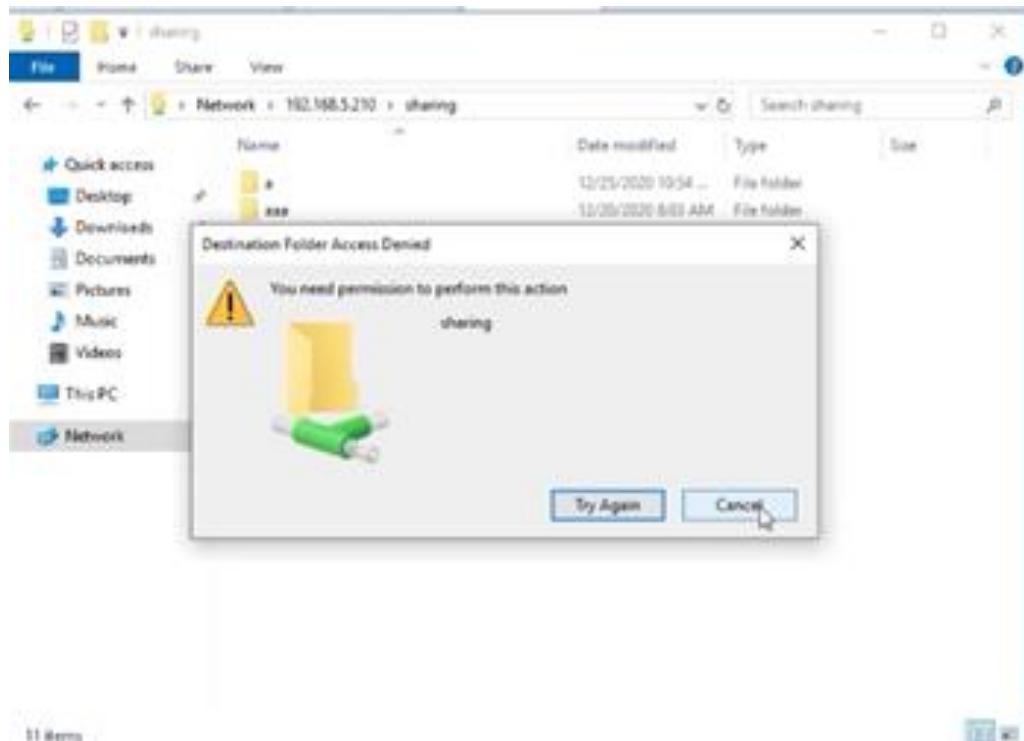


Figure 459 : Restricted action warning

## 6.2.14 LINUX SERVER HARDENING AND VULNERABILITY REPORT

**Step 1:** To verify every software and application is up to date.

```
root@lubuntugrp2:/etc/profile.d# apt-get update
Get:1 http://security.ubuntu.com/ubuntu bionic-security InRelease [88.7 kB]
Hit:2 http://my.archive.ubuntu.com/ubuntu bionic InRelease
Get:3 http://security.ubuntu.com/ubuntu bionic-security/main amd64 DEP-11 Meta
data [48.9 kB]
Get:4 http://my.archive.ubuntu.com/ubuntu bionic-updates InRelease [88.7 kB]
Get:5 http://security.ubuntu.com/ubuntu bionic-security/universe amd64 DEP-11
Metadata [59.5 kB]
Get:6 http://security.ubuntu.com/ubuntu bionic-security/multiverse amd64 DEP-1
1 Metadata [2,464 kB]
Get:7 http://my.archive.ubuntu.com/ubuntu bionic-backports InRelease [74.6 kB]
Get:8 http://my.archive.ubuntu.com/ubuntu bionic-updates/main amd64 DEP-11 Met
adata [294 kB]
Get:9 http://my.archive.ubuntu.com/ubuntu bionic-updates/universe amd64 Packag
es [1,700 kB]
Get:10 http://my.archive.ubuntu.com/ubuntu bionic-updates/universe i386 Packag
es [1,549 kB]
Get:11 http://my.archive.ubuntu.com/ubuntu bionic-updates/universe amd64 DEP-1
1 Metadata [288 kB]
Get:12 http://my.archive.ubuntu.com/ubuntu bionic-updates/multiverse amd64 DEP
-11 Metadata [2,468 kB]
Get:13 http://my.archive.ubuntu.com/ubuntu bionic-backports/universe amd64 DEP
-11 Metadata [9,288 kB]
Fetched 4,207 kB in 5s (792 kB/s)
Reading package lists... Done
root@lubuntugrp2:/etc/profile.d#
```

Figure 460 : Verify application up to date

**Step 2:** Check Password Policy

**Step 2(a):** Open terminal and type **passwd** to change password for the user.

```
root@lubuntugrp2:/etc/profile.d# apt-get update
Get:1 http://security.ubuntu.com/ubuntu bionic-security InRelease [88.7 kB]
Hit:2 http://my.archive.ubuntu.com/ubuntu bionic InRelease
Get:3 http://security.ubuntu.com/ubuntu bionic-security/main amd64 DEP-11 Meta
data [48.9 kB]
Get:4 http://my.archive.ubuntu.com/ubuntu bionic-updates InRelease [88.7 kB]
Get:5 http://security.ubuntu.com/ubuntu bionic-security/universe amd64 DEP-11
Metadata [59.5 kB]
Get:6 http://security.ubuntu.com/ubuntu bionic-security/multiverse amd64 DEP-1
1 Metadata [2,464 kB]
Get:7 http://my.archive.ubuntu.com/ubuntu bionic-backports InRelease [74.6 kB]
Get:8 http://my.archive.ubuntu.com/ubuntu bionic-updates/main amd64 DEP-11 Met
adata [294 kB]
Get:9 http://my.archive.ubuntu.com/ubuntu bionic-updates/universe amd64 Packag
es [1,700 kB]
Get:10 http://my.archive.ubuntu.com/ubuntu bionic-updates/universe i386 Packag
es [1,549 kB]
Get:11 http://my.archive.ubuntu.com/ubuntu bionic-updates/universe amd64 DEP-1
1 Metadata [288 kB]
Get:12 http://my.archive.ubuntu.com/ubuntu bionic-updates/multiverse amd64 DEP
-11 Metadata [2,468 kB]
Get:13 http://my.archive.ubuntu.com/ubuntu bionic-backports/universe amd64 DEP
-11 Metadata [9,288 kB]
Fetched 4,207 kB in 5s (792 kB/s)
Reading package lists... Done
root@lubuntugrp2:/etc/profile.d#
```

Figure 461 : Verify password change

**Step 2(b):** Open terminal and type **chage -l username** to check for password age.

```
root@lubuntugrp2:~# chage -l grp2
Last password change : Nov 06, 2020
Password expires      : Jan 05, 2021
Password inactive     : Feb 04, 2021
Account expires       : never
Minimum number of days between password change : 5
Maximum number of days between password change : 60
Number of days of warning before password expires : 14
```

Figure 462 : Verify for password age

**Step 3:** Check permission on System Files

```
root@lubuntugrp2:~# cd /var/log
root@lubuntugrp2:/var/log# ls -al | grep wtmp
-rwx----- 1 root          utmp          82560 Jan 12 23:58 wtmp
-rw-r--r--. 1 root          utmp          430848 Dec 31 23:06 wtmp.1
root@lubuntugrp2:/var/log# cd /etc
root@lubuntugrp2:/etc# ls -al | grep profile
-rwxr-xr-x. 1 root root    581 Apr  9 2018 profile
drwxrwxrwx. 2 root root    4096 Jan 13 03:33 profile.d
root@lubuntugrp2:/etc# ls -al | grep hosts
drwxrwxrwx. 4 root root    4096 Nov  7 01:00 ghostsscript
-rwx----- 1 root root    352 Jan  5 23:30 hosts
-rw-r--r--. 1 root root    411 Nov  7 01:02 hosts.allow
-rw-r--r--. 1 root root    711 Nov  7 01:02 hosts.deny
-rw-r--r--. 1 root root    316 Dec 29 23:57 hosts.lwidentity.bak
-rw-r--r--. 1 root root    191 Nov 27 23:48 hosts.lwidentity.orig
```

Figure 463 : Verify on system file permission

**Step 4:** Check permission on User Files

```
root@lubuntugrp2:/etc# ls -al | grep fstab
-rw-r--r--. 1 root root    655 Dec 10 16:45 fstab
root@lubuntugrp2:/etc# ls -al | grep passwd
-rw-r--r--. 1 root root    2920 Jan  8 04:00 passwd
-rw-r--r--. 1 root root    2872 Jan  8 03:26 passwd-
root@lubuntugrp2:/etc# ls -al | grep shadow
-rw-r--r--. 1 root shadow   1014 Jan  8 04:00 gshadow
-rw-r--r--. 1 root shadow   998 Jan  8 03:27 gshadow-
-r----- 1 root shadow   2124 Jan 13 03:28 shadow
-rw-r--r--. 1 root shadow   2124 Jan  8 04:00 shadow-
root@lubuntugrp2:/etc# ls -al | grep group
-rw-r--r--. 1 root root    1231 Jan  8 04:00 group
-rw-r--r--. 1 root root    1212 Jan  8 03:27 group-
root@lubuntugrp2:/etc# ls -al | grep sudoers
-rw-r--r--. 1 root root    806 Dec 22 00:10 sudoers
drwxrwxrwx. 2 root root    4096 Nov 26 13:53 sudoers.d
root@lubuntugrp2:/etc#
```

Figure 464 : Verify on users accessible file permission

**Step 5:** Check on network port and verify on CUPS port is closed

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State	PID/Program name
tcp	0	0	127.0.0.53:53	0.0.0.0:*	LISTEN	594/systemd-resolv
tcp	0	0	0.0.0.0:25	0.0.0.0:*	LISTEN	1394/master
tcp	0	0	0.0.0.0:445	0.0.0.0:*	LISTEN	1431/smbd
tcp	0	0	0.0.0.0:993	0.0.0.0:*	LISTEN	1199/dovecot
tcp	0	0	0.0.0.0:5666	0.0.0.0:*	LISTEN	1245/nrpe
tcp	0	0	0.0.0.0:139	0.0.0.0:*	LISTEN	1431/smbd
tcp	0	0	192.168.5.66:5357	0.0.0.0:*	LISTEN	1123/python3
tcp	0	0	0.0.0.0:2222	0.0.0.0:*	LISTEN	1054/sshd
tcp	0	0	0.0.0.0:143	0.0.0.0:*	LISTEN	1199/dovecot
tcp	0	0	0.0.0.0:111	0.0.0.0:*	LISTEN	591/rpcbind
tcp6	0	0	:::25	:::*	LISTEN	1394/master
tcp6	0	0	:::445	:::*	LISTEN	1431/smbd
tcp6	0	0	:::993	:::*	LISTEN	1199/dovecot
tcp6	0	0	:::5666	:::*	LISTEN	1245/nrpe

tcp6	0	0	:::139	:::*	LISTEN	1431/smbd
tcp6	0	0	fe80::20c:29ff:fe3:5357	:::*	LISTEN	1123/python3
tcp6	0	0	:::2222	:::*	LISTEN	1054/sshd
tcp6	0	0	:::143	:::*	LISTEN	1199/dovecot
tcp6	0	0	:::111	:::*	LISTEN	591/rpcbind
tcp6	0	0	:::80	:::*	LISTEN	1355/apache2

Figure 465 : CUPS port closed

**Step 6:** Disable unnecessary services and port and verify on disabled CUPS services.

```
root@lubuntugrp2:~# service cups status
● cups.service - CUPS Scheduler
  Loaded: loaded (/lib/systemd/system/cups.service; disabled; vendor preset: enabled)
    Active: inactive (dead)
      Docs: man:cupsd(8)

Jan 12 23:56:42 lubuntugrp2 systemd[1]: Started CUPS Scheduler.
Jan 13 03:57:01 lubuntugrp2 systemd[1]: Stopping CUPS Scheduler...
Jan 13 03:57:01 lubuntugrp2 systemd[1]: Stopped CUPS Scheduler.
root@lubuntugrp2:~#
```

Figure 466 : Display disabled service

**Step 7:** Verify on allowed port and services. Verify on UFW status.

```
root@lubuntugrp2:~# ufw status
WARN: /etc/default is world writable!
WARN: /etc is world writable!
WARN: / is world writable!
WARN: /etc/ufw is world writable!
WARN: /etc/ufw/applications.d is world writable!
WARN: /lib/ufw is world writable!
WARN: /lib is world writable!
WARN: /usr/sbin is world writable!
WARN: /usr is world writable!
Status: active

To                         Action      From
--                         -----      ----
80                         ALLOW       Anywhere
2222/tcp                   ALLOW       Anywhere
80 (v6)                    ALLOW       Anywhere (v6)
2222/tcp (v6)              ALLOW       Anywhere (v6)

root@lubuntugrp2:~#
```

*Figure 467 : Display allow port, services and UFW status*

## 6.2.15 IPSEC VPN SERVER FOR REMOTE EMPLOYEES

### Client HQ in Window Server

#### Testing on Internal Network

**Step 1:** Open the SoftEther VPN Client Manager and test for the connection.

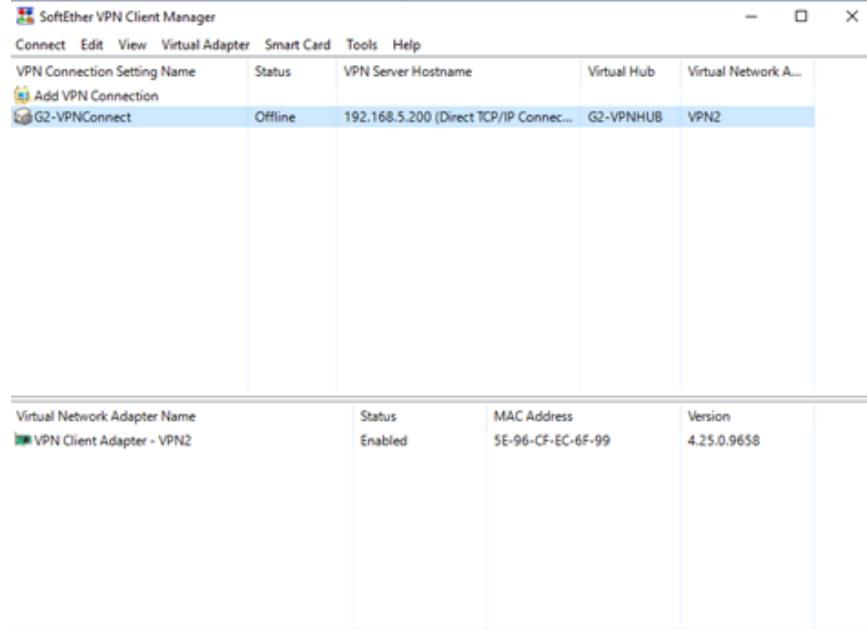


Figure 468 : GUI of SoftEther VPN Client Manager

**Step 2:** Select VPN Connection (G2-VPNConnect) and select Connect.

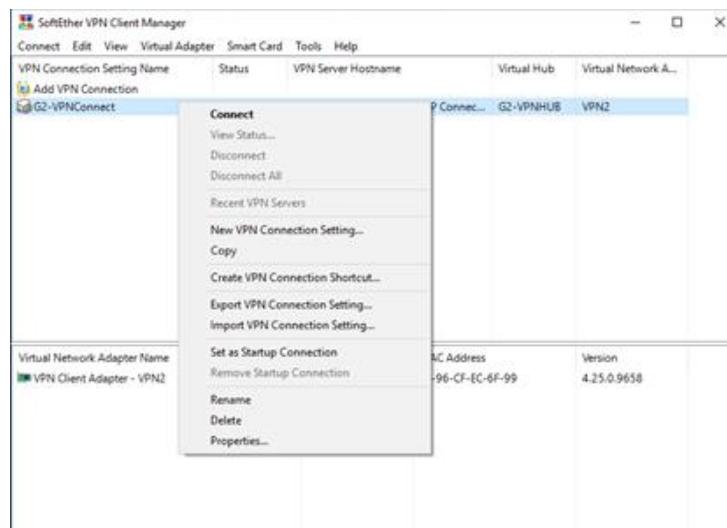


Figure 469 : Connect to VPN

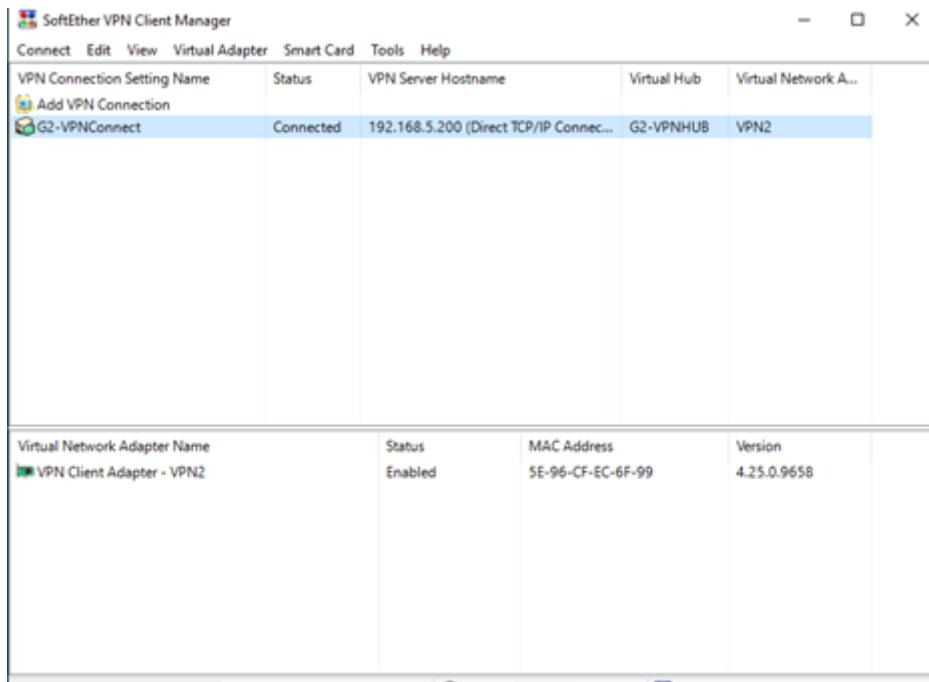


Figure 470 : Connected to VPN

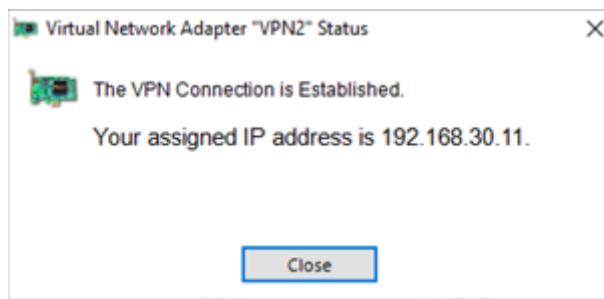


Figure 471 : Connection successful

**Step 3:** Go to SoftEther VPN Server Manager machine and verify the VPN connection.

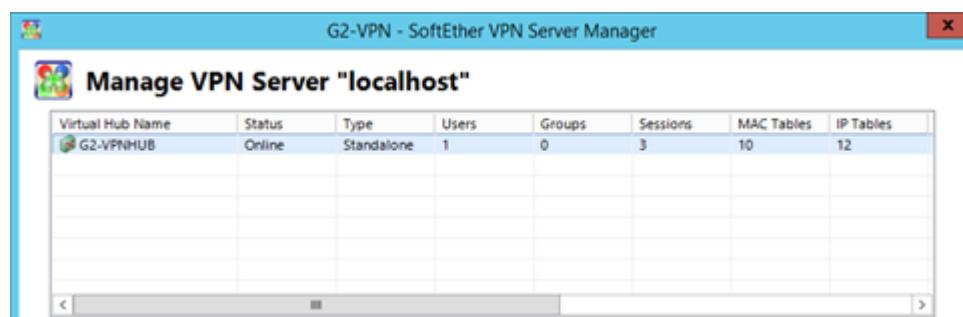


Figure 472 : Verify VPN Connection

**Step 4:** Open command prompt and enter command ipconfig /all to verify the ip address assigned by SoftEther VPN.

```
Unknown adapter VPN2 - VPN Client:

Connection-specific DNS Suffix . : group2.com
Description . . . . . : VPN Client Adapter - VPN2
Physical Address . . . . . : 5E-96-CF-EC-6F-99
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::7114:6c6f:ff6:64e3%28(PREFERRED)
IPv4 Address. . . . . : 192.168.30.11(PREFERRED)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Wednesday, December 9, 2020 1:44:08 AM
Lease Expires . . . . . : Wednesday, December 9, 2020 3:44:07 AM
Default Gateway . . . . . : 192.168.30.1
DHCP Server . . . . . : 192.168.30.1
DHCPv6 IAID . . . . . : 475961039
DHCPv6 Client DUID. . . . . : 00-01-00-01-27-50-A4-47-00-0C-29-76-8A-E2
DNS Servers . . . . . : 192.168.30.1
NetBIOS over Tcpip. . . . . : Enabled
```

Figure 473 : Verify IP address

### **Testing on External Network at Client Branch**

**Step 1:** Open the SoftEther VPN Client Manager and test for the connection.

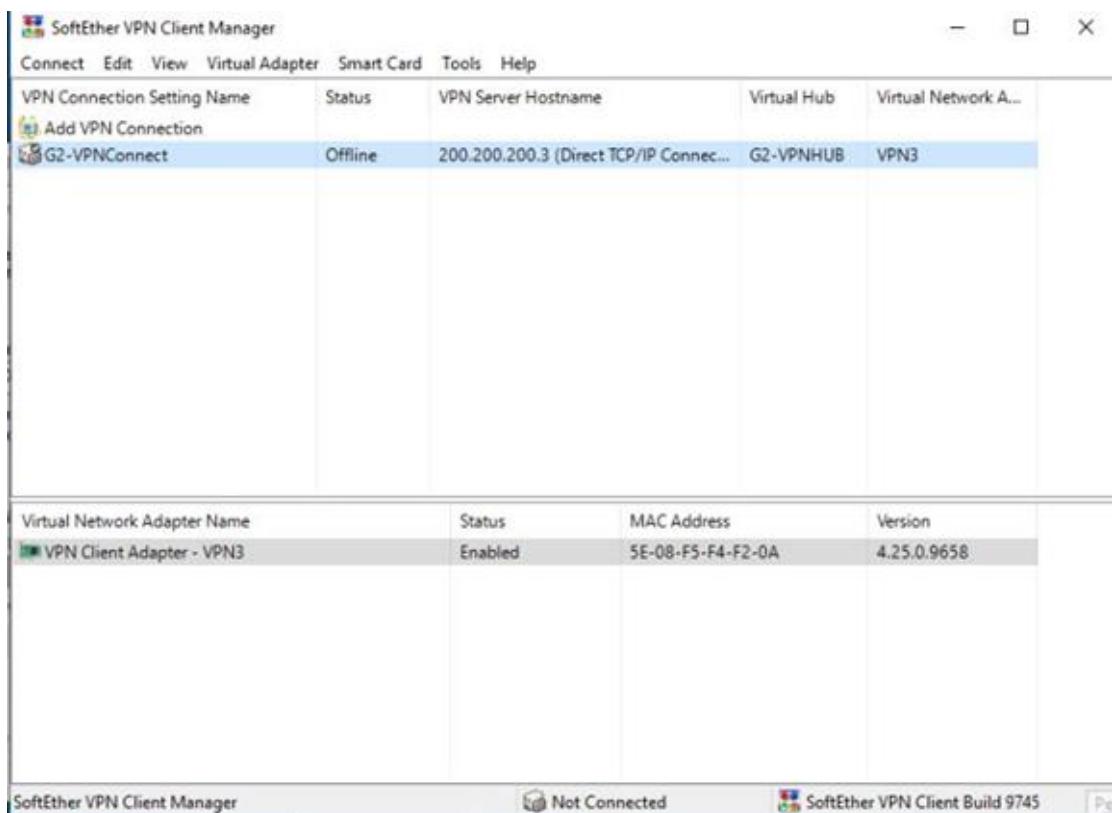


Figure 474 : GUI of SoftEther VPN Client Manager

**Step 2:** Select VPN Connection (G2-VPNConnect) and select Connect.

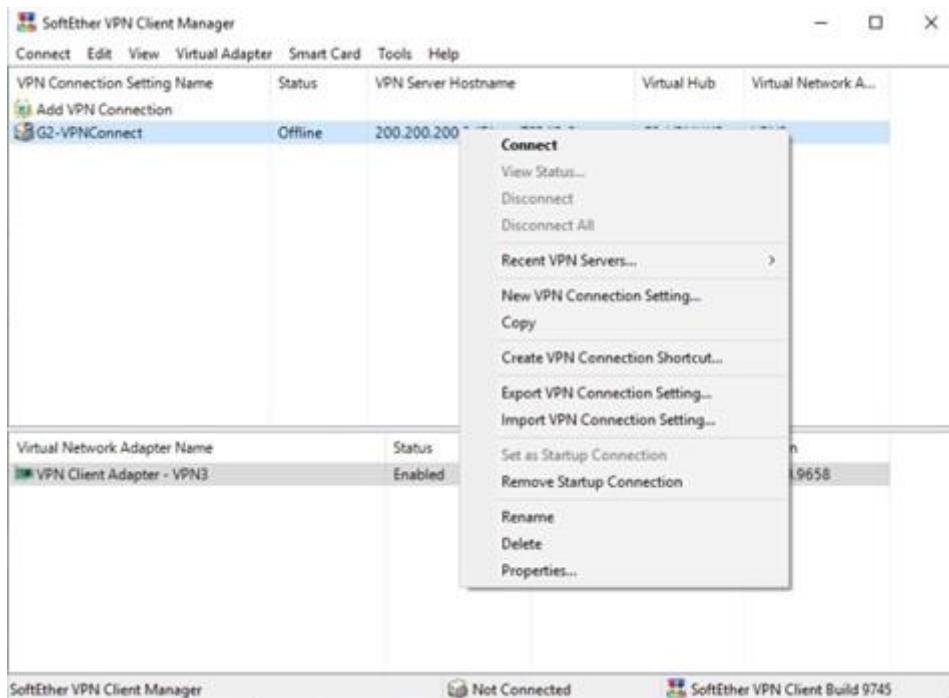


Figure 475 : Connect to VPN

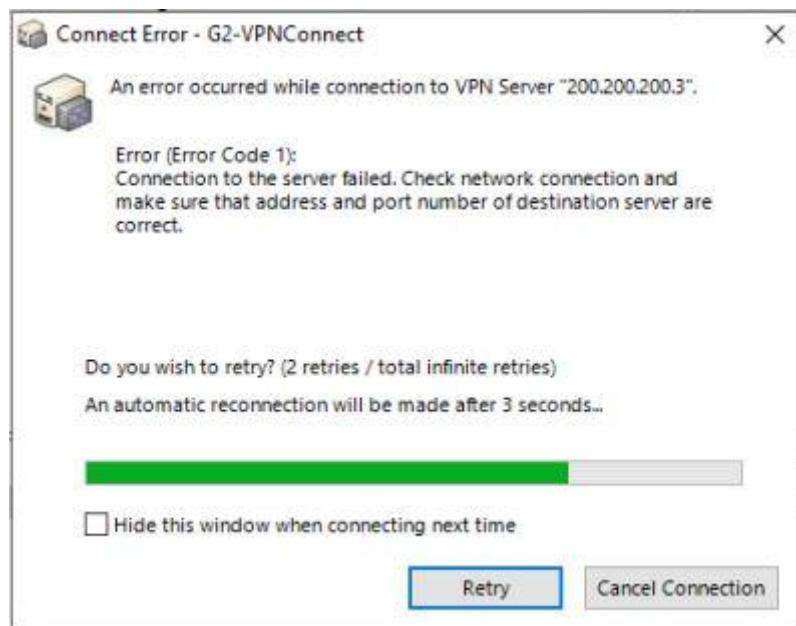
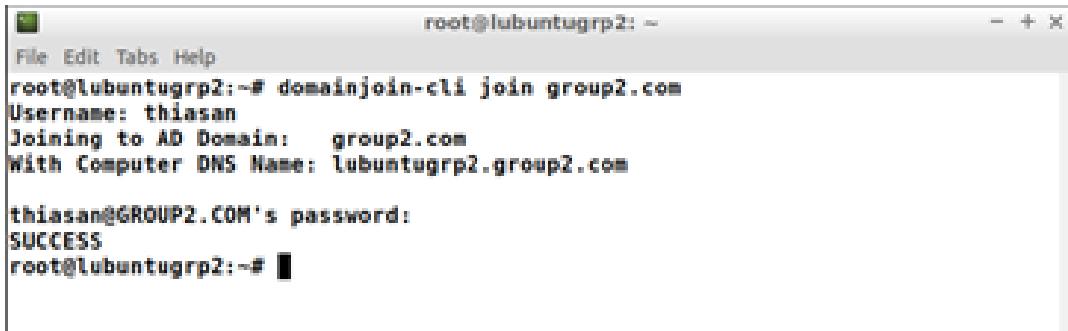


Figure 476 : Fail connected to VPN

**Problem:** The connection from SoftEther VPN Client Manager at Client Branch to Windows Server is fail. Therefore, public IP address of Windows server is not success assigned to the Client Branch.

### 6.2.16 USER AUTHENTICATION BY INTEGRATING AD WITH LINUX

**Step 1:** Open Lubuntu terminal and join the domain using command ***domainjoin-cli join group2.com***



```
root@lubuntugrp2: ~# domainjoin-cli join group2.com
Username: thiasan
Joining to AD Domain: group2.com
With Computer DNS Name: lubuntugrp2.group2.com

thiasan@GROUP2.COM's password:
SUCCESS
root@lubuntugrp2: ~#
```

Figure 477 : Domain join connection with domain Group2.com

**Step 2:** Log in from the login area with registered Active Directory user account. Select Other as account user and type ***username@DOMAIN\_NAME*** username box and type in the user's password.

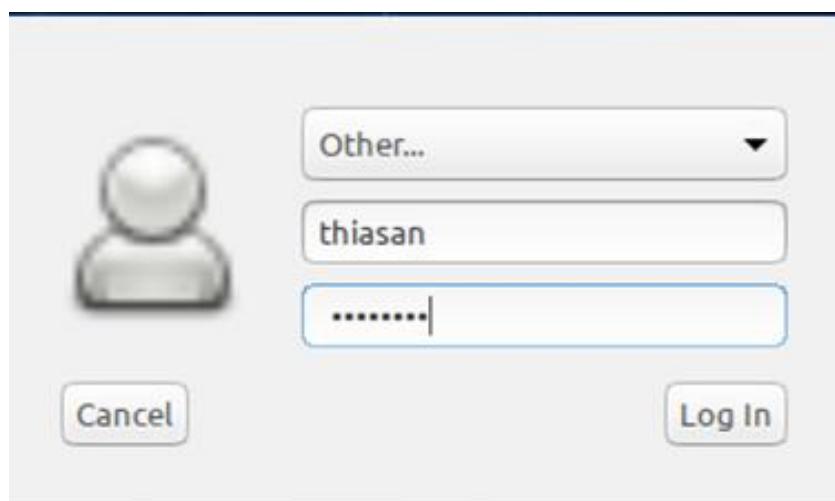


Figure 478 : Log in using registered user in Active Directory

**Step 3:** Check for the username in the terminal



The screenshot shows a terminal window titled 'Emulator'. The title bar displays the session information: 'GROUP2\thiasan@lubuntugrp2: ~'. The menu bar includes 'File', 'Edit', 'Tabs', and 'Help'. The command prompt is shown as 'GROUP2\thiasan@lubuntugrp2:~\$'. The terminal window is currently empty, indicating no output from the command.

Figure 479 : Logged username in terminal

**Step 4:** Check user home directory with command ***pwd***



The screenshot shows a terminal window titled 'Emulator'. The title bar displays the session information: 'GROUP2\thiasan@lubuntugrp2: ~'. The menu bar includes 'File', 'Edit', 'Tabs', and 'Help'. The command prompt is shown as 'GROUP2\thiasan@lubuntugrp2:~\$'. The user runs the command 'pwd' which outputs '/home/GROUP2/thiasan'. Then, the user runs 'ls' to list the contents of their home directory, which includes 'Desktop', 'Downloads', 'Maildir', 'Pictures', 'Templates', 'Documents', 'examples.desktop', 'Music', 'Public', and 'Videos'. The terminal window is currently empty, indicating no output from the command.

Figure 480 : Checking of user's home directory ( Successful )

**Step 5:** Switch to Windows Server and check the connected Lubuntu Server computer

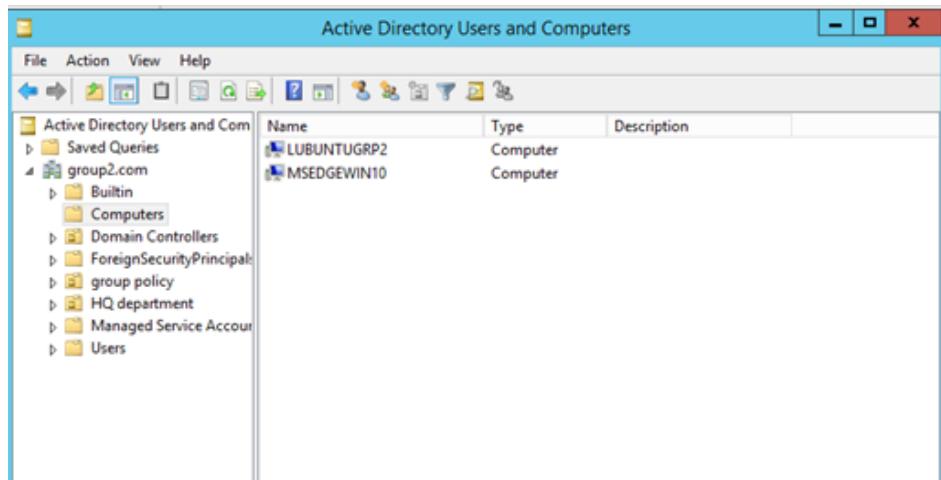


Figure 481 : Connected Lubuntu Server in Active Directory

**Step 6:** Log in using unregistered users under the group and check for verification

```
root@lubuntugrp2: ~
File Edit Tabs Help
root@lubuntugrp2:~# domainjoin-cli join group2.com
Username: thiasan
Joining to AD Domain: group2.com
With Computer DNS Name: lubuntugrp2.group2.com

thiasan@GROUP2.COM's password:
SUCCESS
root@lubuntugrp2:~# domainjoin-cli join group2.com
Username: try
Joining to AD Domain: group2.com
With Computer DNS Name: lubuntugrp2.group2.com

try@GROUP2.COM's password:
Error: ERROR_ACCESS_DENIED [code 0x00000005]

Access is denied
root@lubuntugrp2:~# ■
```

Figure 482 : Invalid user denied from login

**Step 7:** Leave the domain if want to disconnect the domain join using command  
**domainjoin-cli leave**

```
root@lubuntugrp2: ~
File Edit Tabs Help
root@lubuntugrp2:~# domainjoin-cli join group2.com
Username: thiasan
Joining to AD Domain: group2.com
With Computer DNS Name: lubuntugrp2.group2.com

thiasan@GROUP2.COM's password:
SUCCESS
root@lubuntugrp2:~# domainjoin-cli leave
Leaving AD Domain: GROUP2.COM
SUCCESS
root@lubuntugrp2:~# ■
```

Figure 483 : Leave domain

## 6.2.17 WINDOWS SERVER HARDDENING AND VULNERABILITY REPORT

Step 1: Check all required settings.

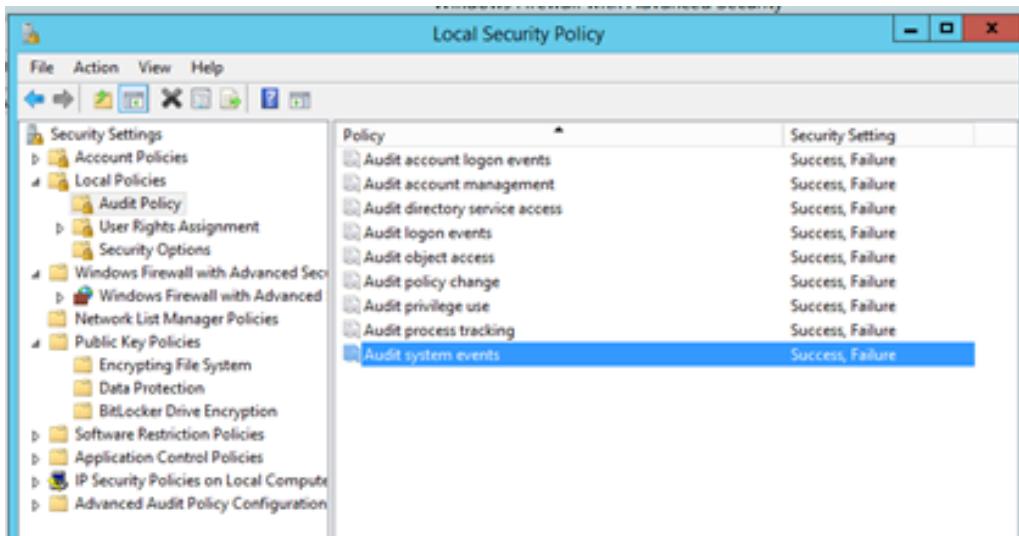


Figure 484 : Audit Policy checking

Step 2: Check Firewall overview after enabling.

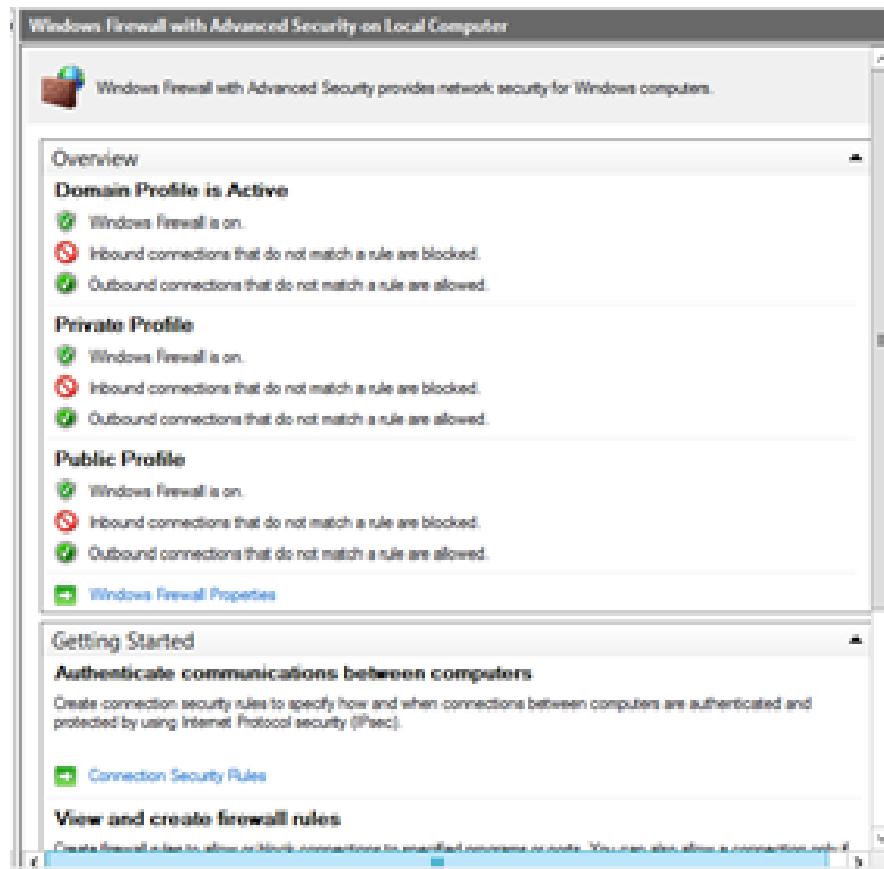


Figure 485 : Firewall Overview settings checking

**Step 3:** Check the password policy.

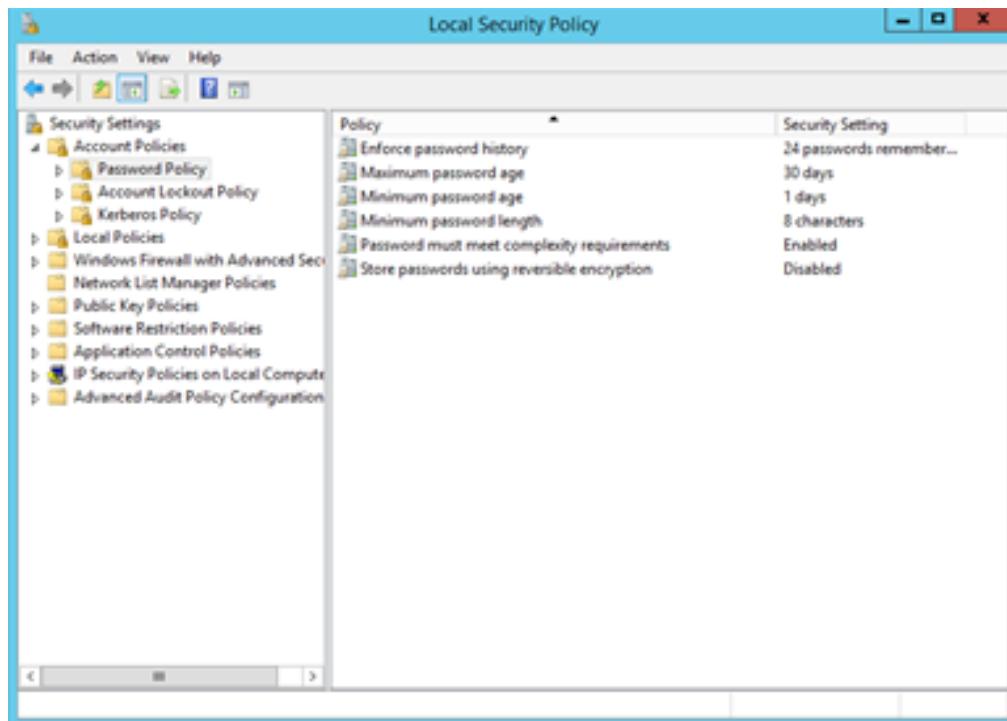


Figure 486 : Password Policy Checking

**Step 4:** Check the Account Lockout Policy

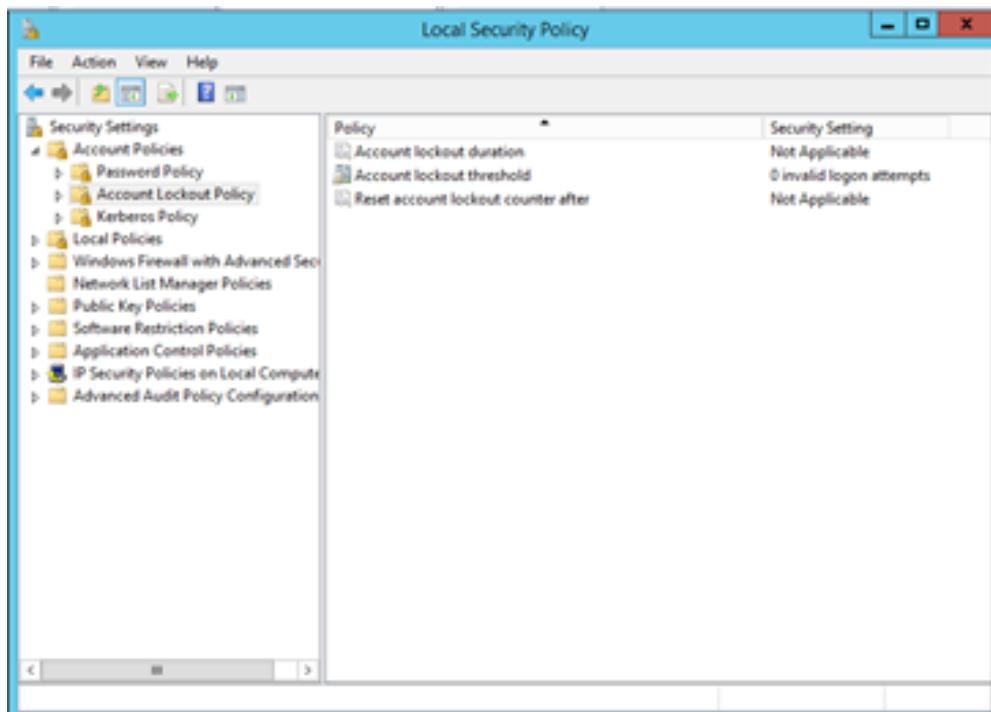


Figure 487 : Account Lockout Policy checking

### Step 5: Check the Kerberos Policy

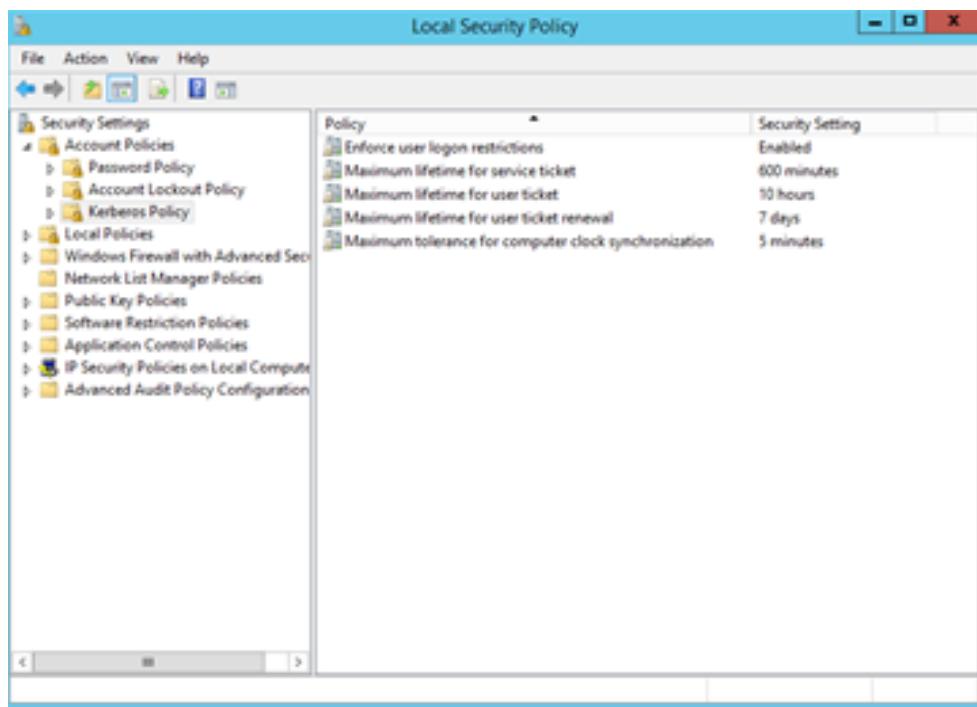


Figure 488 : Kerberos Policy checking

### **6.3 CONCLUSION**

There is various testing for the installation and configuration of the services to ensure that their services are already up and running smoothly. The part of testing is therefore very critical for troubleshooting if any issue is found. A test error is a useful one for a learner to learn and be more experienced in these services. However, by using the testing, all services are up and running smoothly, so we make it into the documentation.

# **CHAPTER 7: CONCLUSION**

## **7.1 INTRODUCTION**

A couple of things has been studied over these past few weeks, such as a way to set up, install, manage, and troubleshoot and all the basic services in this Workshop. The prerequisite for industrial training is all the lessons gained from this Workshop. Defining, implementing, and managing this workshop, starting from the selection of a leader from the beginning to the end of the project to lead this project. This workshop's general output is appropriate. Many of the services were effectively completed by our group before the due date. Tasks were assigned equally to each participant and a schedule was established to control their flow.

This network is a combination of network and security. All the services are included in this network to manage and monitor the infrastructure of the network services. Through carrying out this project, we are very thankful to acquire all the knowledge and experience to be prepared for our industrial training.

## **7.2 PROJECT ADVANTAGES**

Implementing this project has a lot of advantages. The most important part of this project is to have computer networking and security experience in the working environment. In essence, this project also offers other benefits, which are as follows:

- 1) Able to design the network infrastructure for this project.
- 2) Able to install and configure these services.
- 3) Able to configure, monitor, and maintain a simple network.
- 4) Able to understand the methods to set up a network and to deal with the VNC server.
- 5) To troubleshoot and overcome any problems during the setup of the services.
- 6) Able to know more about the configuration and functions of services installed in the Windows Server 2019, Debian, Linux Ubuntu.
- 7) Able to develop a simple networking system to allow communication between computers and server on a different platform.
- 8) Increase the communication between network students and security students in developing a decent network environment.

### **7.3 PROJECT DISADVANTAGES**

Implementing this project also has its disadvantages. The project disadvantages are as follows:

- 1) Lack of knowledge about some services done by other group members.
- 2) The server provided to do this project causing problems thus it complicates the development of the project.
- 3) The students have to spend much time setting up the network.
- 4) The software that has been provided for this project is less stable compared to hardware network equipment that we supposedly use for this project.

### **7.4 PROJECT LIMITATION**

These constraints keep us from achieving the project's full potential. We had to adapt and work harder to succeed because of this constraint. Such limitations are as follows:

- 1) Do not have an incentive and a chance to explore to implement some wired equipment technology.
- 2) There is no good, secure and stable state of the virtual network computing provided to each group.
- 3) There are restrictions on the number of remote computers we can control and the number of people you can use the VNC at one time.
- 4) No immersive tutorial is available. Figuring it out can be challenging and stressful if the students do not know how to use it.

## **7.5 CONCLUSION**

Upon completion of this Workshop 2, we are provided with the Virtual Network Computing (VNC) server. Hence, we are required to be able to install, configure, set up, track and manage our network. We used the operating systems such as Lubuntu 18.04 LTS and Microsoft Windows Server 2012.

Also, we learned to set up some security configurations in workshop 2, such as server hardening, port security, access control list (ACL), and so on, to increase the security level of our network and secure the network from unauthorized access or hacking. To allow the concepts of knowledge we learned during the lecture to be applied, such as Local Area Network (LAN), Wide Area Network (WAN), Network Analysis and Design, Data Communication and Networking, etc.

In short, this project is a very good introduction to real-world and industrial training for us, and at the end of this project, we can complete all the tasks provided and successfully set up the network. From our supervisor and co-supervisor, we learned and understood the services. We are very grateful and we thank them for guiding us to the successful completion of the workshop.

**Auditor's Security  
Hardening Checklist  
for  
GROUP 2**

## **APPENDIX A**

### **Windows Server Hardening**

#### **Windows Server 2012 R2 Hardening Checklist – Group 2**

##### **Server Information**

<b>IP Address</b>	<b>192.168.5.200</b>
<b>Machine Name</b>	<b>WIN-6NNIQRONKOU.group2.com</b>
<b>Date</b>	<b>24 / 1 / 2021</b>

Step	✓	To Do
<b>Preparation and Installation</b>		
1	✓	Install Nmap to scan ports that are opened before Windows Server Hardening
2	✓	Consider using the Security Configuration Wizard to assist in hardening the host
<b>Service Packs and Hotfixes</b>		
3	✓	Install the latest service packs and hotfixes from Microsoft.
4	✓	Enable automatic notification of patch availability.

<b>Step</b>	<b>√</b>	<b>To Do</b>
<b>User Account Policies</b>		
5	√	Set minimum password length.
6	√	Enable password complexity requirements.
7	√	Configure account lockout policy.
<b>User Rights Assignment</b>		
8	√	Restrict the ability to access this computer from the network to Administrators and Authenticated Users.
9	√	Do not grant any users the 'act as part of the operating system' right. (Default)
10	√	Restrict local logon access to Administrators.
11	√	Deny guest accounts the ability to logon as a service, a batch job, locally, or via RDP.
<b>Security Settings</b>		
12		Disable the guest account.
13		Require Ctrl+Alt+Del for interactive logins
14		Configure machine inactivity limit to protect idle interactive sessions
<b>Network Access Controls</b>		

<b>Step</b>	√	<b>To Do</b>
15	√	Disable anonymous SID/Name translation. (Default)
16	√	Do not allow anonymous enumeration of SAM accounts. (Default)
17	√	Do not allow everyone permissions to apply to anonymous users. (Default)
18	√	Require the "Classic" sharing and security model for local accounts. (Default)
<b>Network Security Settings</b>		
19	√	Enable the Windows Firewall in all profiles (domain, private, public). (Default)
20	√	Configure the Windows Firewall in all profiles to block inbound traffic by default. (Default)
<b>Active Directory Domain Member Security Settings</b>		
21	√	Digitally encrypt or sign secure channel data (always). (Default)
22	√	Digitally encrypt secure channel data (when possible). (Default)
23	√	Digitally sign secure channel data (when possible). (Default)
24	√	Require strong (Windows 2000 or later) session keys.
<b>Audit Policy Settings</b>		
25	√	Configure Account Logon audit policy.

<b>Step</b>	√	<b>To Do</b>
26	√	Configure Account Management audit policy.
27	√	Configure Logon/Logoff audit policy.
28	√	Configure Policy Change audit policy.
29	√	Configure Privilege Use audit policy.
<b>Additional Security Protection</b>		
30	√	Disable or uninstall unused services.
31	√	Disable or delete unused users.
32	√	Configure file system permissions.
<b>Additional Steps</b>		
33	√	Set the system date/time and configure it to synchronize against campus time servers.
34	√	Install and enable anti-virus software.
35	√	Configure anti-virus software to update daily.
<b>Physical Security</b>		
36	√	set a BIOS/firmware password to prevent alterations in system start up settings.

<b>Step</b>	<b>√</b>	<b>To Do</b>
37	√	Do not allow the system to be shut down without having to log on. (Default)
38	√	Configure a screen-saver to lock the console's screen automatically if the host is left unattended.

Windows hardening checklist Group 5 is referring to The University of Texas at Austin Windows server 2012 R2 hardening checklist.

Reference: WINDOWS SERVER 2012 R2 HARDENING CHECKLIST.

<https://security.utexas.edu/os-hardening-checklist/windows-2016>

## APPENDIX B

### Linux Server Hardening Checklist

Set Permissions on Sensitive System File	
Configuration Files	
<b>System Files</b>	
<b>Ubuntu</b>	
Attribute	Settings
/etc/profile	<b>0755</b>
/etc/hosts	<b>0700</b>
/var/log/wtmp	<b>0700</b>
<b>Users Files</b>	
<b>Ubuntu</b>	
Attribute	Settings
/etc/fstab	<b>0644</b>
/etc/passwd	<b>0644</b>
/etc/shadow	<b>0400</b>
/etc/group	<b>0644</b>
/etc/sudoers	<b>0644</b>

Task	Before	After
<b>Software and Updates</b>		
Click Updates in Ubuntu Search Bar	X	/
Change from weekly to daily in automatically in automatically check for updates bar	X	/
Change from download automatically to download and install automatically in when there are security updates bar	X	/
Check for updates	X	/
<b>Terminal</b>		
Check password expiration with sudo chage -l (username)	X	/
Change password expiration with sudo chage -M (max days) -I (days inactive) -W (days for warning) (username)	X	/
Open nano /etc/pam.d/common- password-change min length of the password	X	/

Install Nmap	X	
Scan ports with Nmap (Penetration test before)	X	/
Disable CUPS service (for printing)	X	/
Upgrade Bash	X	/
Set security limits	X	/
Scan ports with Nmap (Penetration test after)	X	/

## APPENDIX C

### AUDIT CHECK LIST

<b>Reference</b>	<b>Audit area, objective and question</b>		<b>Results</b>	
	<b>Checklist</b>	<b>Section</b>	<b>Audit Question</b>	<b>Findings</b>
<b>1.0 SECURITY POLICY</b>				
<b>1.1 Security Policy</b>				
1.1.1 Security policy document		Whether there exists a security policy, which is approved by the supervisor, published and communicated as appropriate to all users.  Whether it states the management commitment and set out the organizational approach to managing information security.	Security policy is done in final report.	C
1.1.2 Review and evaluation		Whether the Security policy has an owner, who is responsible for its maintenance and review according to a defined review process.	Security policy have owner which is Group 2 users.	C

	<p>Whether the process ensures that a review takes place in response to any changes affecting the basis of the original assessment,</p> <p>Example: significant security incidents, new vulnerabilities or changes to organisational or technical infrastructure.</p>		
<b>2.0 ORGANISATIONAL SECURITY</b>			
<b>2.1 Information security infrastructure</b>			
2.1.1 Management information security forum	Whether there is a management forum to ensure there is a clear direction and visible management support for security initiatives within the organization.	Briefing about workshop 2 and having group discussion.	C
2.1.2 Information security coordination	Whether there is a cross-functional forum of management representatives from relevant parts of the organization to coordinate the implementation of information security controls.	Discuss of VLSM, Routing & NAT	C
2.1.3 Authorisation process for information processing facilities	Whether there is a management authorisation process in place for any new information processing facility. This should include all new facilities such as software.	Authorisation at all server, router and switch.	C
2.1.4 Independent review of information security	Whether the implementation of security policy is reviewed independently on regular basis. This is to provide assurance that organizational practices properly reflect the policy, and that it is feasible and effective.	Review by all members.	C
<b>2.2 Security of third party access</b>			

2.2.1 Identification of risks from third party access	Whether risks from third party access are identified and appropriate security controls implemented.  Whether the types of accesses are identified, classified and reasons for access are justified.	ACL is implemented.	C
<b>3.0 PERSONNEL SECURITY</b>			
<b>3.1 Security in job definition and Resourcing</b>			
3.1.1 Including security in job responsibilities	Whether security roles and responsibilities as laid in Organisation's information security policy is documented where appropriate. This should include general responsibilities for implementing or maintaining security policy as well as specific responsibilities for protection of particular assets, or for extension of particular security processes or activities.	Security policy is done in final report.	C
<b>4.0 COMMUNICATIONS AND OPERATIONS MANAGEMENT</b>			
<b>4.1 Operational Procedure and responsibilities</b>			
4.1.1 Segregation of duties	Whether duties and areas of responsibility are separated in order to reduce opportunities for unauthorized modification or misuse of information or services.	Services are divided to each member.	C
<b>4.2 System planning and acceptance</b>			
4.2.1 Capacity Planning	Whether the capacity demands are monitored and projections of future capacity requirements are made.	Capacity are monitored.	C

	This is to ensure that adequate processing power and storage are available.		
4.2.2 System acceptance	Whether System acceptance criteria are established for new information systems, upgrades and new versions. Whether suitable tests were carried out prior to acceptance.	System acceptance criteria are established.	C
<b>4.3 Housekeeping</b>			
4.3.1 Information back-up	Whether Back-up of essential business information such as production server, critical network components, configuration backup etc., were taken regularly.	Always backup	C
<b>4.4 Exchange of Information and software</b>			
4.4.1 Security of Media in transit	Whether security of media while being transported taken into account.  Whether the media is well protected from unauthorised access, misuse or corruption.	Samba	C
<b>4.5 Network Management</b>			
4.5.1 Network Control	Whether there exist any special controls to safeguard confidentiality and integrity of data processing over the public network and to protect the connected systems.  Example: Virtual Private Networks and another encryption.	VPN	C
<b>5.0 ACCESS CONTROL</b>			
<b>5.1 User Responsibilities</b>			

5.1.1 Password use	Whether there are any guidelines in place to guide users in selecting and maintaining secure passwords.	Password length = 8 or more character, must include number, must include lower case and upper case, set the password never expired.	C
5.1.2 Unattended user equipment	Whether the users and contractors are made aware of the security requirements and procedures for protecting unattended equipment, as well as their responsibility to implement such protection.  Example: Logoff when session is finished or set up auto log off, terminate sessions when finished etc.,	Provided to all server, router and switch	C
<b>5.2 Network Access Control</b>			
5.2.1 Segregation in networks	Whether the network (where third parties need access to information system) is segregated using perimeter security mechanisms such as firewalls.	Internal firewall such as Routing & NAT  External firewall such as ACL	C
5.2.2 Network routing control	Whether there exists any network control to ensure that computer connections and information flows do not breach the access control policy of the business applications. This is often essential for networks shared with non-organisations users.	Routing & NAT	C

	Whether the routing controls are based on the positive source and destination identification mechanism. Example: Network Address Translation (NAT).	Routing & NAT	C
5.2.3 Security of network services	Whether the organisation, using public or private network service does ensure that a clear description of security attributes of all services used is provided.	Routing & NAT	C
<b>5.3 Operating system access control</b>			
5.3.1 User identification and authorisation	Whether unique identifier is provided to every user such as operators, system administrators and all other staff including technical. The generic user accounts should only be supplied under exceptional circumstances where there is a clear business benefit. Additional controls may be necessary to maintain accountability.	All member has identification and is authorized.	C
	Whether the authentication method used does substantiate the claimed identity of the user; commonly used method: Password that only the user knows.	Users are authenticated	C
5.3.2 Password management system	Whether there exists a password management system that enforces various password controls such as: individual password for accountability, enforce password changes, store passwords in encrypted form, not display passwords on screen etc.,	Password is implemented in all equipment	C
<b>5.4 Monitoring system access and use</b>			

5.4.1 Event logging	Whether audit logs recording exceptions and other security relevant events are produced and kept for an agreed period to assist in future investigations and access control monitoring.	Accounting in RADIUS server	C
5.4.2 Monitoring system use	Whether procedures are set up for monitoring the use of information processing facility. The procedure should ensure that the users are performing only the activities that are explicitly authorised.	Monitored by Nagios Core and IDS	C

## 6.0 SYSTEM DEVELOPMENT AND MAINTENANCE

### 6.1 Cryptographic controls

6.1.1 Encryption	Whether encryption techniques were used to protect the data. Whether assessments were conducted to analyse the sensitivity of the data and the level of protection needed.	SSH, enable secret in router and switch.	C
6.1.2 Key management	Whether there is a management system in place to support the organisation's use of cryptographic techniques such as Secret key technique and Public key technique.	The shared key in RADIUS server is same with shared key in configuration of authentication using radius server – AAA	C
	Whether the Key management system is based on agreed set of standards, procedures and secure methods.	Yes	C

### 6.2 Security in development and support process

6.2.1 Outsourced software development	Whether there are controls in place over outsourcing software. The points to be noted includes: Licensing arrangements, escrow arrangements, contractual requirement for quality assurance, testing before installation to detect Trojan code etc.,	VPN (SoftEther)	C
<b>7.0 COMPLIANCE</b>			
<b>7.1 Aspects of Services Continuity Management</b>			
7.1.1 Testing, maintaining and reassessing services	Whether services are tested regularly to ensure that they are up to date and effective	Services are tested	C
<b>7.2 Compliance with legal requirements</b>			
7.2.1 Identification of applicable legislation	Whether all relevant statutory, regulatory and contractual requirements were explicitly defined and documented for each information system. Whether specific controls and individual responsibilities to meet these requirements were defined and documented.	Were defined and documented in final report.	C
7.2.2 Intellectual property rights (IPR)	Whether proprietary software products are supplied under a license agreement that limits the use of the products to specified machines. The only exception might be for making own back-up copies of the software.	VPN (SoftEther)	C
7.2.3 Data protection and privacy of personal information	Whether there is a management structure and control in place to protect data and privacy of personal information.	Password is encrypted and protected.	C

7.2.4 Collection of evidence	Whether the process involved in collecting the evidence is in accordance with legal and industry best practise.	Accounting log in RADIUS server.	C
<b>7.3 Reviews of Security Policy and technical compliance</b>			
7.3.1 Compliance with security policy	Whether all areas within the organisation is considered for regular review to ensure compliance with security policy, standards and procedures.	Security policy is documented in final report.	C
7.3.2 Technical compliance checking	Whether information systems were regularly checked for compliance with security implementation standards.	Harden Linux Server, Harden Window Server	C
<b>7.4 System audit considerations</b>			
7.4.1 System audit controls	Whether audit requirements and activities involving checks on operational systems should be carefully planned and agreed to minimise the risk of disruptions to workshop.	Yes	C
7.4.2 Protection of system audit tools	Whether access to system audit tools such as software or data files are protected to prevent any possible misuse or compromise.	Yes	C

## APPENDIX D

No	Task	Week														
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	Assigning students to Supervisors	█														
2	Briefing of Workshop 2		█													
3	Proposal preparation. Device setup			█	█											
4	Students submit proposal to Supervisors			█	█	█										
5	Project Implementation (Progress 1)				█	█	█									
6	Project Implementation (Progress 2)						█	█	█	█	█					
7	Project Implementation (Progress 3)											█	█	█		
8	Video and Poster preparation												█			
9	Students submit video and poster to Supervisors												█	█		
9	Project Demonstration & Presentation													█		
10	Final Submission of Final Report, Peer Assessment Report and Log Book														█	